НАЦІОНАЛЬНЕ АГЕНТСТВО ІЗ ЗАБЕЗПЕЧЕННЯ ЯКОСТІ ВИЩОЇ ОСВІТИ

ВІДОМОСТІ
про самооцінювання освітньої програми

Заклад вищої освіти	**Київський національний університет імені Тараса Шевченка**
Освітня програма	**20270 Кібербезпека**
Рівень вищої освіти	**Бакалавр**
Спеціальність	**125 Кібербезпека**

Відомості про самооцінювання є частиною акредитаційної справи, поданої до Національного агентства із забезпечення якості вищої освіти для акредитації зазначеної вище освітньої програми. Відповідальність за підготовку і зміст відомостей несе заклад вищої освіти, який подає програму на акредитацію.

Детальніше про мету і порядок проведення акредитації можна дізнатися на вебсайті Національного агентства – https://naqa.gov.ua/

Використані скорочення:

ID	ідентифікатор
ВСП	відокремлений структурний підрозділ
ЄДЕБО	Єдина державна електронна база з питань освіти
ЄКТС	Європейська кредитна трансферно-накопичувальна система
ЗВО	заклад вищої освіти
ОП	освітня програма

Загальні відомості

1. Інформація про ЗВО (ВСП ЗВО)

Реєстраційний номер ЗВО у ЄДЕБО	**41**
Повна назва ЗВО	**Київський національний університет імені Тараса Шевченка**
Ідентифікаційний код ЗВО	**02070944**
ПІБ керівника ЗВО	**Бугров Володимир Анатолійович**
Посилання на офіційний веб-сайт ЗВО	**https://knu.ua**

2. Посилання на інформацію про ЗВО (ВСП ЗВО) у Реєстрі суб'єктів освітньої діяльності ЄДЕБО

https://registry.edbo.gov.ua/university/41

3. Загальна інформація про ОП, яка подається на акредитацію

ID освітньої програми в ЄДЕБО	**20270**
Назва ОП	**Кібербезпека**
Галузь знань	**12 Інформаційні технології**
Спеціальність	**125 Кібербезпека**
Спеціалізація (за наявності)	*відсутня*
Рівень вищої освіти	**Бакалавр**
Тип освітньої програми	**Освітньо-професійна**
Вступ на освітню програму здійснюється на основі ступеня (рівня)	**Повна загальна середня освіта, Фаховий молодший бакалавр, ОКР «молодший спеціаліст», Молодший бакалавр**
Структурний підрозділ (кафедра або інший підрозділ), відповідальний за реалізацію ОП	**Кібербезпеки та захисту інформації**
Інші навчальні структурні підрозділи (кафедра або інші підрозділи), залучені до реалізації ОП	**кафедра іноземних мов математичних факультетів; кафедра новітньої історії України; кафедра української філософії і культури; кафедра теоретичних основ високих технологій; кафедра екології та зоології; кафедра політології; кафедра філософії та методології науки; кафедра економічного менеджменту та підприємництва; кафедра фізики**
Місце (адреса) провадження освітньої діяльності за ОП	**Факультет інформаційних технологій Київського національного університету імені Тараса Шевченка, вул. Богдана Гаврилишина, 24, м. Київ, Україна, 04116**
Освітня програма передбачає присвоєння професійної кваліфікації	*не передбачає*
Професійна кваліфікація, яка присвоюється за ОП (за наявності)	***відсутня***
Мова (мови) викладання	**Українська**
ID гаранта ОП у ЄДЕБО	**168831**
ПІБ гаранта ОП	**Браіловський Микола Миколайович**
Посада гаранта ОП	**доцент**
Корпоративна електронна адреса гаранта ОП	**brailovskyim@knu.ua**
Контактний телефон гаранта ОП	**+38(067)-429-20-56**
Додатковий телефон гаранта ОП	*відсутній*

Форми здобуття освіти на ОП	Термін навчання
очна денна	3 р. 10 міс.

4. Загальні відомості про ОП, історію її розроблення та впровадження

Для забезпечення потреб ринку України у висококваліфікованих фахівцях з інформаційної і кібербезпеки та відповідно до програми розвитку Київського національного університету імені Тараса Шевченка на 2012-2020 роки (https://science.knu.ua/documents/rozvytok/Progran_Univ_2020.pdf, стор. 5) у 2013 році було створено кафедру кібербезпеки та захисту інформації. У 2014 році університет отримав ліцензії на підготовку здобувачів вищої освіти першого рівня «бакалавр» за напрямами підготовки: 6.170101 «Безпека інформаційно-комунікаційних систем» і 6.170103 «Управління інформаційною безпекою».
Освітню програму «Кібербезпека» було розроблено у 2018 році робочою групою у складі: доц. Браіловський М.М., проф. Оксіюк О.Г., проф. Бабенко Т.В., доц. Пархоменко І.І., доц. Лукова-Чуйко Н.В. Розглянуто та затверджено на засіданні Вченої ради Київського національного університету 25.06.2018 року та введено в дію наказом ректора 20.09 2018 року. Після введення Стандарту вищої освіти України першого бакалаврського рівня, галузі знань 12 - Інформаційні технології, спеціальності 125 "Кібербезпека", що був затверджений та введений в дію наказом Міністерства освіти і науки України 04.10.2018 р. № 1074 була розроблена нова редакція ОП, яка затверджена на засіданні Вченої ради Київського національного університету 03.12.2018 року (протокол №7) та введено в дію наказом ректора 12 лютого 2019 року № 144-32.
З метою врахування вимог часу, побажань представників кластерів інформаційної безпеки (ІБ) та інформаційних технологій (ІТ) («Інженерно-технічного центру Хай-Тек бюро», «Українські спеціальні системи», ДССЗЗІ, випускників кафедри, які працюють за фахом у державних структурах, приватних компаніях та інших зацікавлених осіб), у 2021 році програму було оновлено та затверджено на засіданні Вченої ради Київського національного університету імені Тараса Шевченка від 29.12.2021 р. (протокол № 10) та введена в дію наказом ректора № 160-32 від 23.03.2022р. (ОПИС ОСВІТНЬО-ПРОФЕСІЙНОЇ ПРОГРАМИ 2022 – Кафедра кібербезпеки та захисту інформації (knu.ua)

5. Інформація про контингент здобувачів вищої освіти на ОП станом на 1 жовтня поточного навчального року у розрізі форм здобуття освіти та набір на ОП (кількість здобувачів, зарахованих на навчання у відповідному навчальному році сумарно за усіма формами здобуття освіти)

Рік навчання	Навчальний рік, у якому відбувся набір здобувачів відповідного року навчання	Обсяг набору на ОП у відповідному навчальному році	Контингент студентів на відповідному році навчання станом на 1 жовтня поточного навчального року	У тому числі іноземців
			ОД	*ОД*
1 курс	2022 - 2023	115	110	0
2 курс	2021 - 2022	106	107	1
3 курс	2020 - 2021	70	71	1
4 курс	2019 - 2020	67	66	1

Умовні позначення: ОД – очна денна; ОВ – очна вечірня; З – заочна; Дс – дистанційна; М – мережева; Дл – дуальна.

6. Інформація про інші ОП ЗВО за відповідною спеціальністю

Рівень вищої освіти	Інформація про освітні програми
початковий рівень (короткий цикл)	*програми відсутні*
перший (бакалаврський) рівень	**33300 Кібербезпека (на основі ОКР молодшого спеціаліста)** **20270 Кібербезпека** **1074 Безпека інформаційних і комунікаційних систем** **49755 Кібербезпека (на основі ОПС фахового молодшого бакалавра)** **19160 Безпека інформаційних і комунікаційних систем (мова навчання російська)/Безопасность информационных и коммуникационных систем** **2092 Управління інформаційною безпекою**
другий (магістерський) рівень	**20271 Кібербезпека**
третій (освітньо-науковий/освітньо-творчий) рівень	**37141 Кібербезпека**

7. Інформація про площі приміщень ЗВО станом на момент подання відомостей про самооцінювання, кв. м.

	Загальна площа	Навчальна площа
Усі приміщення ЗВО	542665	67681
Власні приміщення ЗВО (на праві власності, господарського відання або оперативного управління)	542665	67681
Приміщення, які використовуються на іншому праві, аніж право власності, господарського відання або оперативного управління (оренда, безоплатне користування тощо)	0	0
Приміщення, здані в оренду	2485	0

Примітка. Для ЗВО із ВСП інформація зазначається:
- щодо ОП, яка реалізується у базовому ЗВО – без урахування приміщень ВСП;
- щодо ОП, яка реалізується у ВСП – лише щодо приміщень даного ВСП.

8. Документи щодо ОП

Документ	Назва файла	Хеш файла
Освітня програма	*ОПП_125_Кібербезпека_2022.pdf*	bTCVYf+I5b2zLyZjnG7c+du5Ws5pxe3rE/EhveyXXeU=
Освітня програма	*ОПП_125_Кібербезпека_2019.pdf*	Wa3TsIYLgO1tiWuqkDz8hJcqAwpHnpJCwWs/95SNvAo=
Навчальний план за ОП	*НП_125_Кібербезпека_2022.pdf*	8LlTwXp+R1U47dLxvSSVU4s5kz0bQaZxgbX+2loTiyA=
Навчальний план за ОП	*НП_125_Кібербезпека_2019.pdf*	e1ljAlmXJul19JeuMmIaXucKrcc0HtaYFSUQXbFy/OU=
Рецензії та відгуки роботодавців	*Рецензія_ОПП_2022_Гнатюк.pdf*	rCMb9aCrMIQ2oMWULjwNt23LyOkLlQgbQeVtgRo1SnA=
Рецензії та відгуки роботодавців	*Рецензія ОПП_2022_Кохановський.pdf*	as8CSyLT76mwALZsdfQQIy8qfXKt0FleAGKHzQGmjNk=
Рецензії та відгуки роботодавців	*Рецензія ОПП_Алгоритм.pdf*	aU9B+ofKw4Wjy//VbkhXGXgsxO3ddRbuHHAO6QtykgI=

1. Проектування та цілі освітньої програми

Якими є цілі ОП? У чому полягають особливості (унікальність) цієї програми?

Метою ОП “Кібербезпека” є підготовка фахівців, здатних розв’язувати спеціалізовані задачі і практичні проблеми у галузі інформаційної безпеки та використовувати, і впроваджувати технології інформаційної та/або кібербезпеки. Унікальність ОП “Кібербезпека” полягає у освоєнні здобувачами вищої освіти найсучасніших компонентів у галузі кібербезпеки (квантова криптологія, безпека хмарних технологій тощо). При розробці ОП “Кібербезпека” проєктною групою враховано досвід розробки аналогічних програм вітчизняними та закордонними закладами вищої освіти - НТУ України «КПІ імені Ігоря Сікорського», Національного авіаційного університету, Київського університету імені Б. Грінченка, Stanford University (США), а також досвід отриманий членами робочої групи в процесі реалізації міжнародних професійних програм USAID (United States Agency for International Development). Про унікальність ОП “Кібербезпека” також свідчить широкий спектр місць працевлаштування випускників - індустрія ІБ та ІТ, силові структури, банківські установи.

Продемонструйте, із посиланням на конкретні документи ЗВО, що цілі ОП відповідають місії та стратегії ЗВО

Метою освітньої програми є підготовка фахівців здатних розв’язувати спеціалізовані задачі і практичні проблеми у галузі інформаційної безпеки та використовувати і впроваджувати технології інформаційної та кібербезпеки, в цілому відповідає місії Університету. Відповідно до «Стратегічного плану розвитку Університету на період 2018-2025 року» (https://knu.ua/pdfs/official/Development-strategic-plan-22-12-12.pdf) основні функції, покладені на Університет і які визначають його місію, стосуються формування національної еліти України, підготовки висококваліфікованих кадрів для наукових, освітніх та виробничих українських та міжнародних установ, сприяння європейській та євроатлантичній інтеграції України, гармонійному входженню у світовий економічний простір як рівноправного партнера, вироблення рекомендацій органам державної влади для прийняття ефективних управлінських рішень у процесі реагування на економічні, екологічні, політичні, соціальні та військові виклики, повоєнне відновлення.

Опишіть, яким чином інтереси та пропозиції таких груп заінтересованих сторін (стейкхолдерів) були враховані під час формулювання цілей та програмних результатів навчання ОП:
- здобувачі вищої освіти та випускники програми

ОП “Кібербезпека” і її редакції формувався на основі аналізу результатів опитування здобувачів вищої освіти, щодо наповненості освітніх компонент аналізу результатів обговорення наповнення освітніх компонент з випускними курсами ОП “Кібербезпека” (https://kbzi.knu.ua/speek_bak/) та https://kbzi.knu.ua/an_spek_bak/).

- роботодавці

До обговорення ОП “Кібербезпека” були залучені роботодавці, перш за все, фахівці ДССЗЗІ та провідних ІБ та ІТ компаній міста Києва («Інженерно-технічного центру Хай-Тек бюро», «Українські спеціальні системи», ТОВ “ЕПАМ СИСТЕМЗ”, “B2B-рішення”, ТОВ "Софтпром Солюшнз", ТОВ "МТІ", ТОВ "Ел-Консалтинг", KPMG). Пропозиції роботодавців стосувалися пріоритетів ОК, поглиблення теоретичних знань та практичних вмінь у галузі кібербезпеки (особливо в розрізі протидії гібридній війні в кіберпросторі), вмінню застосовувати отримані знання на робочому місці, відповідності ОП “Кібербезпека” потребам особистості та суспільства, сприянню конкурентоспроможності випускників на ринку праці. Зазначені пропозиції роботодавців були враховані в процесі перегляду ОП “Кібербезпека”.

- академічна спільнота

Думки та пропозиції академічної спільноти були враховані при формулюванні цілей, компетентностей та програмних результатів навчання. Обговорення відбувалися на засіданнях проєктної групи та засіданнях кафедри кібербезпеки та захисту інформації. Науково-педагогічні працівники кафедри організовують та беруть активну участь у щорічних міжнародних науково-практичних конференціях «Проблеми кібербезпеки інформаційно-телекомунікаційних систем» (PCSITS) і «Інформаційні технології та впровадження» (IT&I), де кафедра має свою секцію Cyberspace Protection Technologies.
До цього наукового заходу долучається широке коло провідних фахівців в галузі інформаційної та кібербезпеки з України та з закордону (матеріали конференції IT&I індексуються в наукометричних базах).
Також відбувається активна взаємодія з міжнародною академічною спільнотою в галузі кібербезпеки в рамках сумісної роботи над міжнародними проєктами Erasmus+KA2, USAID «Кібербезпека критично важливої інфраструктури України», Еразмус+, напрям Жан Моне «Інтеграція рамок та політик кібербезпеки ЄС в Україні» тощо.

- інші стейкхолдери

Іншими стейкхолдерами є територіальна громада м. Києва та інших регіонів України економічний розвиток яких, у тому числі залежить від кваліфікації людського капіталу, чому значною мірою сприяє Київський національний університет імені Тараса Шевченка.
Реалізація ОП “Кібербезпека” сприяє зміцненню обороноспроможності країни в кіберпросторі внаслідок збільшення кількості висококваліфікованих фахівців, які працевлаштовуються на різних об'єктах інформаційної діяльності примножуючи й розвиваючи тим самим економіку міста та регіону.

Продемонструйте, яким чином цілі та програмні результати навчання ОП відбивають тенденції розвитку спеціальності та ринку праці

Ринок праці вимагає висококваліфікованих фахівців в галузі кібербезпеки та захисту інформації. За інформацією Національного інституту стратегічних досліджень в Україні спостерігається дефіцит фахівців у сфері кібербезпеки (https://niss.gov.ua/doslidzhennya/informaciyni-strategii/kiberbezpeka-v-umovakh-rozgortannya-chetvertoi-promislovoi). Спектр вимог ринку до фахових компетентностей фахівців з кібербезпеки, в умовах гібридної війни, є досить різноманітним – знання законодавчої та нормативно-правової бази в галузі інформаційної безпеки, захист інформації на апаратному та програмному рівнях, криптозахист, захист мереж, тощо. Існуючі потреби суспільства та ринку відображені у змісті навчальних дисциплін, таких як: «Нормативно-правове забезпечення інформаційної безпеки», «Системи технічного захисту інформації», «Криптографічні системи захисту інформації», «Захист інформації в інформаційних системах та мережах» та ін. Ці потреби відображені у ПРН 7, 14, 16, 18, 27, 35,47,48 50 ОП“Кібербезпека”. Всі сучасні тенденції базуються на знаннях ключових засад інформаційної безпеки з кожного напрямку і враховані в програмних результатах навчання за ОП “Кібербезпека”.
Кореляція розвитку спеціальності, програмних результатів за цією ОП “Кібербезпека” та ринку праці досягається внаслідок тісної співпраці з роботодавцями, плідної роботи над міжнародними програмами (USAID тощо), використання в навчальному процесі таких платформ, як RangeForce, Hack The Box тощо.

Продемонструйте, яким чином під час формулювання цілей та програмних результатів навчання ОП було враховано галузевий та регіональний контекст

Галузевий та регіональний контекст при розробленні ОП “Кібербезпека” врахований через аналіз пропозицій працедавців, значну частину яких становлять ІТ та ІБ компанії міста та регіону. Роботодавці зацікавлені в висококваліфікованих фахівцях, які мають наступні компетентностей: вміти проєктувати, впроваджувати, супроводжувати інформаційно-комунікаційні системи, системи управління інформаційною безпекою, системи управління подіями ІБ, комплексні системи захисту інформації, оцінювати рівень захищеності інформаційних ресурсів підприємства на базі сучасних моделей, методів і засобів захисту інформації. На базі цього аналізу та обговорень на засіданнях проєктної групи та кафедри формувалися обов'язкові компоненти ОП “Кібербезпека”, що

забезпечують результати навчання.

Продемонструйте, яким чином під час формулювання цілей та програмних результатів навчання ОП було враховано досвід аналогічних вітчизняних та іноземних програм

Формуванню цієї ОП “Кібербезпека” передував аналіз освітніх програм за спеціальністю 125 “Кібербезпека” закладів вищої освіти, що знаходяться у відкритому доступі. Було проаналізовано ОП «Системи, технології та математичні методи кібербезпеки» НТУ України «КПІ імені Ігоря Сікорського», «Системи та технології кібербезпеки» Національного авіаційного університету, «Безпека інформаційних та комунікаційних систем» Київського університету імені Б. Грінченка, «Кібербезпека» Харківського національного університету ім. В.Н. Каразіна, програм з кібербезпеки університету Стенфорда (https://online.stanford.edu/explore?type=program&filter%5B0%5D=topic%3A1057&keywords=&items_per_page=12). Кожна з ОП має свою специфіку, що визначається науковими школами університетів, де ці програми реалізовані, але ОП мають і спільні характеристики, зокрема ті, що відображають сучасні досягнення в галузі кібербезпеки та захисту інформації (безпека Web-застосунків, захист інформаційно-комунікаційних систем, криптографічні методи захисту тощо). В результаті аналізу зазначених ОП та враховуючи регіональну специфіку в ОП “Кібербезпека” були включені актуальні ОК, наприклад, “Управління інформаційною безпекою” (ОК18), “Системи електронного підпису та управління ключами”(ОК29) та інші.

Продемонструйте, яким чином ОП дозволяє досягти результатів навчання, визначених стандартом вищої освіти за відповідною спеціальністю та рівнем вищої освіти

Стандарт вищої освіти за спеціальністю 125 “Кібербезпека” галузі знань 12 Інформаційні технології для першого (бакалаврського) рівня вищої освіти затверджено 04.10.2018 (Наказ МОН України № 1074 від 04.10.2018). Оскільки, до складу проєктної групи з розробки ОП входили два розробники Стандарту (представники кафедри КБЗІ проф. Оксіюк О.Г. і проф. Бабенко Т.В.) це дозволило повністю імплементувати його вимоги в ОП “Кібербезпека” починаючи з 2018 року.
Освітні компоненти ОП сформовано так, щоб вони забезпечували відповідні компетентності ОП та ПРН. ОК забезпечують теоретичні знання, практичні уміння й навички, які забезпечать можливість ефективного розв’язання комплексних сучасних задач у сфері кібербезпеки, в умовах стрімких змін у ландшафті загроз, та відповідних методах, засобах протидії та забезпечення безпеки, технологічного розвитку засобів кібербезпеки.

Якщо стандарт вищої освіти за відповідною спеціальністю та рівнем вищої освіти відсутній, поясніть, яким чином визначені ОП програмні результати навчання відповідають вимогам Національної рамки кваліфікацій для відповідного кваліфікаційного рівня?

Стандарт вищої освіти України для першого (бакалаврського) рівня вищої освіти галузі знань 12 «Інформаційні технології» спеціальності 125 «Кібербезпека» затверджений та введений в дію наказом Міністерства освіти і науки України від 04.10.2018 № 1074 (https://mon.gov.ua/storage/app/media/vishcha-osvita/2022/Standarty.Vyshchoyi.Osvity/Zatverdzheni.Standarty/01/31/125-Kiberbezpeka-bak.31.01.22.pdf)

2. Структура та зміст освітньої програми

Яким є обсяг ОП (у кредитах ЄКТС)?

240

Яким є обсяг освітніх компонентів (у кредитах ЄКТС), спрямованих на формування компетентностей, визначених стандартом вищої освіти за відповідною спеціальністю та рівнем вищої освіти (за наявності)?

180

Який обсяг (у кредитах ЄКТС) відводиться на дисципліни за вибором здобувачів вищої освіти?

60

Продемонструйте, що зміст ОП відповідає предметній області заявленої для неї спеціальності (спеціальностям, якщо освітня програма є міждисциплінарною)?

Зміст ОП “Кібербезпека” розкривається через включені до неї ОК і повністю відповідає предметній області спеціальності 125 “Кібербезпека” та має чітку структуру. ОК логічно взаємопов'язані в систему, та в сукупності забезпечують досягнення заявлених в ОП “Кібербезпека” цілей та програмних результатів навчання. Відповідність ОП “Кібербезпека” предметній області заявленої для неї спеціальності демонструється через об'єкти, цілі, інструменти та інші компоненти ОП “Кібербезпека”. Освітні компоненти ОП “Кібербезпека” охоплюють всі об'єкти та процеси, що впливають на забезпечення кібербезпеки: об'єкти інформаційної діяльності включаючи об'єкти критичної інформаційної інфраструктури, комп'ютерні, автоматизовані, інформаційно-телекомунікаційні,

інформаційно-комунікаційні, інформаційні ресурси і технології, системи управління інформаційними технологіями й системи управління інформаційною безпекою, процеси управління інформаційною та кібербезпекою об'єктів інформаційної діяльності, що підлягають захисту. ОК ОП “Кібербезпека” формують засади для обґрунтованого використання сучасних парадигм, концепцій, принципів, підходів та технологічних рішень для побудови систем інформаційної/кібербезпеки для заданого рівня гарантій та прогнозування очікуваних результатів їх впровадження та експлуатації.
ОП “Кібербезпека” має достатній набір ОК, у тому числі й, для успішної підготовки кваліфікаційної роботи бакалавра. ОК професійного блоку дозволяють забезпечити підготовку висококваліфікованого конкурентоспроможного фахівця в галузі кібербезпеки та захисту інформації.

Яким чином здобувачам вищої освіти забезпечена можливість формування індивідуальної освітньої траєкторії?

Структура ОП “Кібербезпека” забезпечує можливість для формування індивідуальної освітньої траєкторії, зокрема через індивідуальний вибір дисциплін здобувачами вищої освіти, в обсязі передбаченому Стандартом вищої освіти України для першого (бакалаврського) рівня спеціальності 125 «Кібербезпека». Процедура вибору здобувачами вищої освіти індивідуальної освітньої траєкторії регламентується Положенням про організацію освітнього процесу в Київському національному університеті імені Тараса Шевченка (https://knu.ua/pdfs/official/Polozhennia-pro-organizatsiyu-osvitniogo-procesu-11_04_2022.pdf), Положення про порядок реалізації студентами Київського Національного університету імені Тараса Шевченка права на вільний вибір навчальних дисциплін» (http://senate.univ.kiev.ua/?p=855). Можливість формування індивідуальної освітньої траєкторії відображається в індивідуальних навчальних планах студентів та передбачає можливість індивідуального вибору навчальних дисциплін в межах передбачених ОП “Кібербезпека” та навчальним планом (в обсязі не менше 25 % від загальної кількості кредитів ЄТКС) з дотриманням послідовності їх вивчення відповідно до структурно-логічної схеми підготовки фахівця.

Яким чином здобувачі вищої освіти можуть реалізувати своє право на вибір навчальних дисциплін?

Право на вибір навчальних дисциплін студенти можуть реалізувати відповідно до Положення про порядок реалізації студентами Київського Національного університету імені Тараса Шевченка права на вільний вибір навчальних дисциплін» (http://senate.univ.kiev.ua/?p=855). Вибір навчальних дисциплін студент здійснює в процесі формування свого індивідуального плану навчання у межах, що передбачені ОП “Кібербезпека” та робочим навчальним планом з дотриманням послідовності їх вивчення відповідно до структурно-логічної схеми підготовки фахівця. Вибіркові навчальні дисципліни індивідуального плану студента формуються з блоків вибіркових навчальних дисциплін ОП.
Вибіркові навчальні дисципліни, що внесені до індивідуального навчального плану студента, є обов'язковими для вивчення. Запис студентів на вивчення блоків вибіркових дисциплін та окремих вибіркових дисциплін проводиться за їх письмовими заявами та з використанням онлайн-кабінету автоматизованої системи «ТРИТОН» (https://student.triton.knu.ua/).

Опишіть, яким чином ОП та навчальний план передбачають практичну підготовку здобувачів вищої освіти, яка дозволяє здобути компетентності, необхідні для подальшої професійної діяльності

Проведення практики здобувачів вищої освіти в Університеті регламентується “Положенням про проведення практики студентів” (http://surl.li/bjvpv). Практична підготовка здобувачів за ОП передбачає формування фахових компетентностей зі спеціальності, що є необхідними для їх професійної діяльності. Ці компетентності здобувачі отримують під час проведення практичних та лабораторних робіт в межах окремих ОК. Також ОП передбачені проєктно-технологічна та науково-дослідна практика. Метою яких є набуття професійних навичок за ОП, поглиблення, закріплення та систематизація знань, у тому числі з інформаційно-аналітичної, проєктної, діагностичної, дослідницької та консалтингової діяльності у сфері ІТ та ІБ на основі роботи конкретного підприємства, формування у здобувачів вмінь для прийняття професійних, обґрунтованих, самостійних рішень в реальних виробничих умовах, збір необхідних матеріалів для виконання бакалаврської роботи. Здобувачам забезпечується вільний вибір місця проходження практики. Університет підтримує зв'язки з підприємствами та організаціями, що є потенційними базами практик, та створює умови для реалізації змісту практик, зокрема з ТОВ “ЕРАМ СИСТЕМЗ”, “B2B-рішення”, ТОВ "Авалекс Сольюшнз" та ін. Саме потреби роботодавців визначають цілі і завдання практичної підготовки. У щоденнику проходження практики фіксується оцінка роботи здобувача вищої освіти, а підприємство надає офіційний відгук, що в сукупності дозволяє забезпечувати зворотний зв'язок з базами практик.

Продемонструйте, що ОП дозволяє забезпечити набуття здобувачами вищої освіти соціальних навичок (soft skills) упродовж періоду навчання, які відповідають цілям та результатам навчання ОП результатам навчання ОП

ОП “Кібербезпека” дозволяє здобувачами вищої освіти опанувати комплекс соціальних/універсальних навичок (soft skills), що вимагаються від сучасного фахівця. Серед soft skills, що формуються ОП “Кібербезпека” є формування компетентностей креативного мислення, уміння формулювати власну думку та приймати рішення, здатність брати на себе відповідальність і працювати в критичних умовах, вміння залагоджувати конфлікти, працювати в команді, здатність реалізовувати свої права й обов'язки, як члена суспільства, усвідомлювати цінність громадянського суспільства та його сталого розвитку. Соціальні навички (soft skills) формуються всіма ОК ОП “Кібербезпека”, але насамперед їх формують такі ОК, як «Українська та зарубіжна культура», «Філософія», «Соціально-політичні студії», «Вибрані розділи трудового права й основ підприємницької діяльності», «Іноземна мова». Поглиблення соціальних

навичок також досягається шляхом вивчення вибіркових ОК, практики за темою дипломної бакалаврської роботи, її виконання та захисту, під час виконання яких здобувач вищої освіти отримує компетентності з виявлення, аналізу, перевірки, оцінювання повноти та правдивості інформації, формування обґрунтованих професійних суджень та прийняття обґрунтованих рішень.

Яким чином зміст ОП ураховує вимоги відповідного професійного стандарту?

На час розробки ОП, що акредитується, професійний стандарт відсутній. Проєкт нової редакції ОП, в якому врахований професійний стандарт «Фахівець сфери захисту інформації» знаходиться в процесі розробки.

Який підхід використовує ЗВО для співвіднесення обсягу окремих освітніх компонентів ОП (у кредитах ЄКТС) із фактичним навантаженням здобувачів вищої освіти (включно із самостійною роботою)?

В Київському національному університеті імені Тараса Шевченка організація освітнього процесу регламентується "Положенням про організацію освітнього процесу" (https://www.univ.kiev.ua/pdfs/official/Polozhennia-pro-organizatsiyu-osvitniogo-procesu-11_04_2022.pdf)
В положенні зазначено, що організація освітнього процесу здійснюється відповідно до Європейської кредитної трансферно-накопичувальної системи (ЄКТС). ЄКТС базується на визначенні навчального навантаження здобувача вищої освіти, що є необхідним для досягнення очікуваних результатів навчання та обліковується в кредитах ЄКТС (обсяг одного кредиту становить 30 годин). Частка аудиторного та позааудиторного навантаження, що визначається у відсотках, становить структуру кредиту. Рекомендована структура кредиту ЄКТС в Університеті для першого бакалаврського рівня, як правило, 50% аудиторних занять. Відповідно до Положення про організацію освітнього процесу" обсяг самостійної (позааудиторної) роботи з кожної дисципліни визначено в навчальному плані ОП "Кібербезпека", а її зміст в робочій навчальній програмі дисципліни та навчально методичних матеріалах до неї.

Якщо за ОП здійснюється підготовка здобувачів вищої освіти за дуальною формою освіти, продемонструйте, яким чином структура освітньої програми та навчальний план зумовлюються завданнями та особливостями цієї форми здобуття освіти

За даною ОП "Кібербезпека" підготовка здобувачів вищої освіти за дуальною формою освіти не здійснюється.

3. Доступ до освітньої програми та визнання результатів навчання

Наведіть посилання на веб-сторінку, яка містить інформацію про правила прийому на навчання та вимоги до вступників ОП

https://vstup.knu.ua/

Поясніть, як правила прийому на навчання та вимоги до вступників ураховують особливості ОП?

Правила прийому на навчання за ОП "Кібербезпека" враховують особливості програми та повністю відповідають умовам прийому на навчання для здобуття першого (бакалаврського) рівня вищої освіти МОН України. Умови вступу бакалаврів та перелік необхідних для вступу документів розміщені на офіційному сайті університету у розділі "Вступ на бакалавра" за посиланням https://vstup.knu.ua/#Section211. Правила прийому на навчання для здобуття ступеня бакалавра з ОП "Кібербезпека" враховує особливості ОП, зокрема для вступу необхідно три сертифікати ЗНО: 1) українська мова;2) математика; 3) один зі списку (історія України, іноземна мова, біологія, географія, фізика, хімія). Детальніше за посиланням https://vstup.knu.ua/images/2022/NMT_ZNO_vstup.pdf

Яким документом ЗВО регулюється питання визнання результатів навчання, отриманих в інших ЗВО? Яким чином забезпечується його доступність для учасників освітнього процесу?

Питання визнання результатів навчання, отриманих в інших ЗВО регулюються документами, що розміщені у вільному доступі на інформаційних ресурсах Університету:
Положення про організацію освітнього процесу у Київському національному університеті імені Тараса Шевченка введене в дію Наказом Ректора від 31 серпня 2018 року за №716-32 (п.11) (https://knu.ua/pdfs/official/Polozhennia-pro-organizatsiyu-osvitniogo-procesu-11_04_2022.pdf);
Положення про порядок реалізації права на академічну мобільність Київського національного університету імені Тараса Шевченка від 29.06.2016 р. (http://mobility.univ.kiev.ua/?page_id=804&lang=uk);
Порядок поновлення та переведення здобувачів вищої освіти (студентів, слухачів, курсантів) у Київському національному університеті імені Тараса Шевченка (http://vstup.univ.kiev.ua/userfiles/files/instruction.pdf);
Наказ Ректора від 12.07.2016 року за №603-22 "Про затвердження Порядку проведення в Київському національному університеті імені Тараса Шевченка атестації для визнання здобутих кваліфікацій, результатів навчання та періодів навчання в системі вищої освіти, здобутих на тимчасово окупованій території України після 20 лютого 2014 року. http://nmc.univ.kiev.ua/docs/Nakaz_atestaciya_PK_2016.jpg

Опишіть на конкретних прикладах практику застосування вказаних правил на відповідній ОП (якщо

такі були)?

Прикладом практики застосування вказаних правил на ОП “Кібербезпека” є зарахування здобувача вищої освіти на навчання за контрактом Наказ № 3843-33 від 07.10.2021 р. відповідно до якого академічну різницю, що склала 30 кредитів було включено до його індивідуально навчального плану з граничним терміном її ліквідації до 01.11.2021р.

Яким документом ЗВО регулюється питання визнання результатів навчання, отриманих у неформальній освіті? Яким чином забезпечується його доступність для учасників освітнього процесу?

Після набрання чинності наказу Міністерства освіти і науки України за №130 від 16 березня 2022 року «Про затвердження порядку визнання у вищій та фаховій передвищій освіті результатів навчання, здобутих шляхом неформальної та/або інформальної освіти» (Положення-про-валідацію1.pdf (univ.kiev.ua).
Проте за результатами зверненням Студентського парламенту Університету з метою забезпечення прав студентів на якісну освіту під час запровадження карантинних заходів, пов’язаних із коронавірусною інфекцією COVID-19 було прийнято рішення (розпорядження №056/642 від 2.06.2020 р.) щодо зарахування результатів навчання, підтверджених сертифікатами, наприклад, з платформи Coursera for Campus (http://www.univ.kiev.ua/news/10974) тощо.
Питання визнання результатів навчання за наданим студентом сертифікатом приймається викладачем відповідної дисципліни, обговорюється та затверджується на засіданні кафедри. Надані здобувачем вищої освіти сертифікати дають можливість йому отримати певну кількість балів за визначені в РНП дисципліни види робіт. Університет не обмежує права здобувачів вищої освіти на розвиток компетентностей поза освітніми програмами шляхом неформального та/або інформального навчання в Університеті і за його межами, сам розробляє і пропонує такі програми.

Опишіть на конкретних прикладах практику застосування вказаних правил на відповідній ОП (якщо такі були)

Практики застосування вказаних правил на ОП “Кібербезпека” не було.

4. Навчання і викладання за освітньою програмою

Продемонструйте, яким чином форми та методи навчання і викладання на ОП сприяють досягненню програмних результатів навчання? Наведіть посилання на відповідні документи

Навчання на ОП “Кібербезпека” проводиться за денною (очною) формою навчання (тривалість навчання - 3 роки 10 місяців і 2 роки 10 місяців за скороченим циклом підготовки). Досягнення програмних результатів навчання на ОП “Кібербезпека” досягається внаслідок поєднання таких форм навчання, як лекційні заняття, практичні роботи, лабораторні заняття, семінарські заняття, виконання курсових робіт, самостійної роботи, проходження практик на об'єктах інформаційної діяльності. Викладання здійснюється з широким використанням мультимедійних засобів та спеціалізованого програмного забезпечення. Здобувачам вищої освіти надається доступ до інформаційних та методичних матеріалів кожної освітньої компоненти, а саме доступна інформація про робочу програму навчальної дисципліни, перелік рекомендованої літератури, систему оцінювання знань, глосарій, лекційні, методичні матеріали, тестові завдання для самоконтролю тощо (https://kbzi.knu.ua/).
Інформація про методи навчання і викладання, що застосовуються на ОП “Кібербезпека” для кожної ОК деталізовано в таблиці 3.

Продемонструйте, яким чином форми і методи навчання і викладання відповідають вимогам студентоцентрованого підходу? Яким є рівень задоволеності здобувачів вищої освіти методами навчання і викладання відповідно до результатів опитувань?

Форми і методи навчання в Київському національному університеті імені Тараса Шевченка регламентовані «Положенням про організацію освітнього процесу» (https://knu.ua/pdfs/official/Polozhennia-pro-organizatsiyu-osvitniogo-procesu-11_04_2022.pdf) яке ґрунтується на студентоцентрованому підході. Відповідно до цього Положення навчання і викладання в Університеті здійснюються за такими формами й методами: навчальні заняття, виконання індивідуальних завдань, самостійна робота, практична підготовка, контрольні заходи. Види навчальних занять: лекції, лабораторні роботи, практичні роботи, семінарські, індивідуальні, консультації. На кожен навчальний рік проєктна група на основі навчального плану за ОП “Кібербезпека” розробляє робочий план, що конкретизує перелік освітніх компонентів і види занять, їх обсяг і форми контролю за семестрами. Кожен здобувач вищої освіти, починаючи з другого курсу, має можливість формувати власну освітню траєкторію.
Навчаючись за ОП “Кібербезпека” здобувачі освіти мають можливість формувати власну освітню траєкторію, обираючи дисципліни вільного вибору, місце проходження практик, тематику індивідуальних завдань, курсових робіт, випускної кваліфікаційної роботи. За результатами анонімних опитувань більшість здобувачів вищої освіти задоволені результатами організації освітнього процесу на ОП “Кібербезпека”.
Результати опитувань оприлюднені на офіційному сайті випускової кафедри (https://kbzi.knu.ua/speek_bak/).

Продемонструйте, яким чином забезпечується відповідність методів навчання і викладання на ОП принципам академічної свободи

Методи навчання і викладання на ОП “Кібербезпека” відповідають принципам академічної свободи. Наприклад, відповідно до “Положення про організацію освітнього процесу” (https://knu.ua/pdfs/official/Polozhennia-pro-organizatsiyu-osvitniogo-procesu-11_04_2022.pdf) лектор зобов'язаний дотримуватись робочої програми навчальної дисципліни щодо тем лекцій, але не обмежується в питаннях тлумачення навчального матеріалу, послідовності його викладення, формах і засобах донесення його до студентів. Можливе проведення лекцій у формах: інформаційні, проблемні, візуальні, бінарні, лекції-провокації, лекції-конференції, лекції-консультації, лекції-дискусії тощо, також у формі вебінарів з використанням інформаційно-комунікаційних систем (мережі Інтернет). Під час проведення лабораторних, практичних, семінарських занять передбачено постановку та обговорення загальної проблеми, розв'язання завдань з їх обговоренням.
Академічна свобода здобувачів вищої освіти також забезпечується шляхом формування індивідуальної освітньої траєкторії, гарантією свободи пошуку та поширення інформації при проведенні досліджень, вільним вибором тематики курсових та кваліфікаційних робіт, баз практики, можливістю участі в академічній мобільності, можливістю поширювати результати своїх досліджень на конференціях, участі в конкурсах та олімпіадах тощо.

Опишіть, яким чином і у які строки учасникам освітнього процесу надається інформація щодо цілей, змісту та очікуваних результатів навчання, порядку та критеріїв оцінювання у межах окремих освітніх компонентів *

Відповідно до “Положення про організацію освітнього процесу” (https://knu.ua/pdfs/official/Polozhennia-pro-organizatsiyu-osvitniogo-procesu-11_04_2022.pdf) для кожної навчальної дисципліни, що входить в ОП “Кібербезпека” є розроблена робоча програма, в якій викладено зміст навчальної дисципліни, її послідовність, форми вивчення, форми поточного і семестрового контролю, результати навчання, основні і додаткові літературні джерела. Здобувач має можливість ознайомитися з РНП на сайті кафедри (https://kbzi.knu.ua/bakalavr/). Інформація оновлюється щорічно перед початком вступної кампанії й доступна потенційним абітурієнтам і здобувачам вищої освіти при формуванні індивідуальної освітньої траєкторії.
Крім того, на початку семестру лектор та викладачі-асистенти (при проведенні лабораторних, практичних та семінарських занять) детально роз'яснюють здобувачам освіти порядок та критерії оцінювання запланованих окремих видів робіт та форм контролю.

Опишіть, яким чином відбувається поєднання навчання і досліджень під час реалізації ОП

Відповідно до “Положення про організацію освітнього процесу” https://knu.ua/pdfs/official/Polozhennia-pro-organizatsiyu-osvitniogo-procesu-11_04_2022.pdf) в Київському національному університеті імені Тараса Шевченка науково-дослідна робота студентів здійснюється за такими основними напрямами: 1) науково-дослідна робота в освітньому процесі; 2) науково-дослідна робота студентів у поза навчальний час; 3) науково-організаційні заходи – конференції, конкурси, олімпіади тощо. В ОП “Кібербезпека” заплановані і реалізуються в освітньому процесі всі види науково-дослідної роботи здобувачів. Про результативність поєднання навчання і наукових досліджень свідчать публікації і презентації наукових доробок студентів на престижних наукових міжнародних конференціях, матеріали яких індексуються в науковометричних базах, зокрема: 1) Lukova-Chuiko N., Fesenko A., Papirna H., Gnatyuk S. Threat hunting as a method of protection against cyber threats CEUR Workshop Proceedingsthis link is disabled, 2021; 2) Viktoriia H., Hnatienko H., Babenko, T. An intelligent model to assess information systems security level Proceedings of the 2021 5th World Conference on Smart Trends in Systems Security and Sustainability, WorldS4 2021; 3) Grechko V., Babenko T., Myrutenko L. Secure software developing recommendations 2019 IEEE International Scientific-Practical Conference: Problems of infocommunications Science and Technology, PICS Proceedings, 2019; 4) Shestak Y., Toliupa S., Shevchenko A., Torchylo A., Onyigwang O.J. Data Processing Centre's Cyberattack Protection Directions on the Base of Neural Network Algorithms CEUR Workshop Proceedings 2022; 5) Buchyk S., Lukova-Chuiko N., Toliupa S., Piatyhor V., Buchyk O. Diceware Password Generation Algorithm Modification based on Pseudo-Random Sequences CEUR Workshop Proceedingsthis link is disabled, 2021 тощо.
Студент Губський О на другому всеукраїнському конкурсі наукових робіт зайняв друге місце. Тема роботи «Інтелектуальні моделі класифікації подій кібербезпеки». Дипломом І ступеню відзначено В. Солодовник на Міжнародній студентській олімпіаді «Шляхи та механізми захисту інформаційного простору України від шкідливих інформаційно-психологічних впливів». Значна кількість студентів, що навчаються за ОП “Кібербезпека” систематично беруть участь в роботі щорічної конференції «Проблеми кібербезпеки інформаційно-телекомунікаційних систем» (PCSITS). Детальніше за посиланням (https://kbzi.knu.ua/pcsits/).

Продемонструйте, із посиланням на конкретні приклади, яким чином викладачі оновлюють зміст навчальних дисциплін на основі наукових досягнень і сучасних практик у відповідній галузі

Зміст навчальних дисциплін переглядається та оновлюється викладачами ОП “Кібербезпека” не рідше чим один раз на рік відповідно до “Положення про організацію освітнього процесу” (https://knu.ua/pdfs/official/Polozhennia-pro-organizatsiyu-osvitniogo-procesu-11_04_2022.pdf).
Моніторинг передбачає оцінювання відповідності ОП “Кібербезпека” і її ОК сучасним науковим досягненням в галузі кібербезпеки, тенденціям розвитку економіки й суспільства, змінам потреб роботодавців, здобувачів вищої освіти та інших стейкхолдерів. Наприклад, були оновлені РНП з дисциплін: “Квантова криптологія” на основі наукових напрацювань у сфері квантових методів захисту інформації (доц. А. Фесенко); “Захист інформації в інформаційних системах та мережах” на основі напрацювань з оцінки ризиків інформаційної безпеки в розподілених системах (проф. Бабенко), “Управління інформаційною безпекою” на основі наукових напрацювань з управління інцидентами кібербезпеки (проф. Толюпа). В рамках міжнародної програми USAID “Кібербезпека об'єктів критичної інфраструктури України” викладачі ОП “Кібербезпека” оновили РНП дисциплін: “Інформаційні системи та мережі”, “Управління інформаційною безпекою”, “Інформаційні технології в кіберпросторі”, “Кіберпростір та протидія кіберзлочинності”, “Криптографічні системи захисту інформації”.

Опишіть, яким чином навчання, викладання та наукові дослідження у межах ОП пов'язані із інтернаціоналізацією діяльності ЗВО

Навчання, викладання, наукові дослідження в межах ОП пов'язані з підходами щодо інтернаціоналізації, які реалізує Університет. Згідно "Положення про порядок реалізації права на академічну мобільність у КНУ імені Тараса Шевченка" НПП ОП та здобувачі вищої освіти мають право на академічну мобільність, що може бути реалізоване на підставі міжнародних договорів про співробітництво в галузі освіти і науки, міжнародних програм та проєктів, договорів про співробітництво між Університетом або його основними структурними підрозділами та вітчизняними/іноземними закладами вищої освіти (науковими установами), а також може бути реалізоване зацікавленною особою з власної ініціативи, що підтримана адміністрацією Університету, в якому він постійно навчається або працює.
З метою поглиблення інтеграції в український та міжнародний освітньо-науковий простір, підвищення якості освіти та результативності наукових досліджень такі викладачі ОП як: проф. Н. Лукова-Чуйко, проф. С. Бучик, проф. В. Наконечний, доц. А. Фесенко, доц. Л. Мирутенко, ас. С. Даков пройшли наукові закордонні стажування за програмами, що відповідають профілю ОП (https://kbzi.knu.ua/quality/). Використання потенціалу наукової бібліотеки ім. М. Максимовича (http://surl.li/bfyqd) в комплексі з науковими стажуваннями та підвищенням кваліфікації НПП ОП (https://kbzi.knu.ua/quality/) дозволяє забезпечити адаптацію отриманих здобувачами вищої освіти результатів навчання для потенційного використання практично в будь-якій країні.

5. Контрольні заходи, оцінювання здобувачів вищої освіти та академічна доброчесність

Опишіть, яким чином форми контрольних заходів у межах навчальних дисциплін ОП дозволяють перевірити досягнення програмних результатів навчання?

Детальний опис контрольних заходів, які можуть бути застосовані у межах навчальних дисциплін ОП, наведено у «Положенні про організацію освітнього процесу у Київському національному університеті імені Тараса Шевченка» (https://knu.ua/pdfs/official/Polozhennia-pro-organizatsiyu-osvitniogo-procesu-11_04_2022.pdf). та «Положення про порядок оцінювання знань студентів при кредитно-модульній системі організації навчального процесу у Київському національному університеті імені Тараса Шевченка» (http://www.nmc.univ.kiev.ua/docs/POLOJENNIA-2010-1.doc). Згідно положень оцінювання результатів навчання здійснюється на принципах об'єктивності, системності, плановості, єдності вимог, відкритості, прозорості, економічності, доступності та зрозумілості методики оцінювання, урахування індивідуальних можливостей студентів. Контрольні заходи поділяються на такі категорії: поточний контроль та підсумковий контроль. Поточний контроль результатів навчання здійснюється під час проведення практичних, лабораторних та семінарських занять, його метою є перевірка рівня знань здобувача та набутих ним вмінь і навичок, які визначаються відповідною РНП. Форми поточного контролю, їх оцінка в балах та критерії оцінювання визначаються у відповідності зі специфікою дисципліни та фіксуються у РНП.
Для підсумкового контролю дисциплін ОП передбачені такі форми контролю як іспит або залік. Зазначені форми контрольних заходів у межах освітніх компонентів ОП є чіткими, зрозумілими, надають можливість встановити досягнення здобувачем ПРН.
Критерієм успішного опанування студентом ОК є досягнення ним мінімальних порогових значень оцінок за кожним запланованим результатом навчання та мінімального порогового рівня оцінки за ОК загалом. Мінімальний пороговий рівень оцінки визначається відповідною РНП. Мінімальний пороговий рівень оцінки становить 60% від максимально можливої кількості балів. Здобувач освіти може бути недопущений до підсумкового оцінювання, якщо під час семестру він не досяг мінімального порогового рівня оцінки.
Наведені форми контролю та підхід до оцінювання дозволяють перевірити рівень досягнення усіх запланованих результатів навчання та оцінити рівень теоретичних знань і практичних навичок здобувачів освіти.

Яким чином забезпечуються чіткість та зрозумілість форм контрольних заходів та критеріїв оцінювання навчальних досягнень здобувачів вищої освіти?

Чіткість та зрозумілість форм контрольних заходів та оцінювання знань здобувачів вищої освіти на ОП «Кібербезпека» забезпечується шляхом визначення необхідних понять, принципів та підходів у розділі 7 «ОЦІНЮВАННЯ РЕЗУЛЬТАТІВ НАВЧАННЯ», «Положення про організацію освітнього процесу у Київському національному університеті імені Тараса Шевченка» https://knu.ua/pdfs/official/Polozhennia-pro-organizatsiyu-osvitniogo-procesu-11_04_2022.pdf) та подальшій деталізації їх у відповідній РНП освітнього компоненту. Зокрема у РНП прописуються форми поточного та підсумкового контролів, процедура організації оцінювання, критерії оцінювання, наводиться детальна схема формування оцінки та шкала відповідності оцінок. РНП оприлюднені на сайті кафедри (https://kbzi.knu.ua/bakalavr/).
Для додаткового роз'яснення форм та процедури контрольних заходів здобувачі освіти можуть звернутися до викладача, як особисто, так і через засоби комунікації (електронна пошта, телефон, месенджер), контакти надаються на першому занятті

Яким чином і у які строки інформація про форми контрольних заходів та критерії оцінювання доводяться до здобувачів вищої освіти?

Інформація про форми контрольних заходів та критерії оцінювання для кожного ОК ОП наводиться у РНП ОП та навчальному плані, які доступні на сайті кафедри (https://kbzi.knu.ua/). Документи оприлюднюються на сайті кафедри впродовж тижня після їх затвердження. Викладач на першому занятті інформує студентів про форми

контрольних заходів та їх терміни, а також надає усі необхідні роз'яснення щодо дисципліни. Графік навчального процесу з наведеними термінами підсумкового контролю публікуються на сайті факультету (http://fit.univ.kiev.ua/for-students/session-schedule) перед початком навчального року. Також у графіку навчального процесу наведені терміни проведення практики.
Графік навчального процесу визначає календарні терміни теоретичного навчання і практичної підготовки, семестрового контролю, ліквідації академічної заборгованості, підготовки кваліфікаційних робіт, атестації здобувачів освіти. Графік навчального процесу затверджується проректором з науково-педагогічної роботи і розміщується на сайті факультету ІТ (http: //fit.univ.kiev.ua/for-students/session-schedule).

Яким чином форми атестації здобувачів вищої освіти відповідають вимогам стандарту вищої освіти (за наявності)?

Відповідно до вимог Стандарту вищої освіти України першого бакалаврського рівня, галузі знань 12 - Інформаційні технології, спеціальності 125 "Кібербезпека" ОП передбачає атестацію у формі єдиного державного кваліфікаційного іспиту.
Додатково розробниками ОП передбачено захист випускної кваліфікаційної роботи.
На атестацію виноситься сукупність знань, умінь, навичок, компетентностей, набутих особою у процесі навчання за ОП.
До атестації допускаються студенти, які виконали всі вимоги програми підготовки.
Тематика випускних робіт обговорюється та затверджується на засіданні кафедри кібербезпеки.
Рекомендації до вибору тем, структури роботи, змістовного наповнення розділів роботи та правила оформлення висвітлені у методичних рекомендаціях до виконання випускної кваліфікаційної роботи для отримання освітнього ступеня «бакалавр» спеціальності 125 «Кібербезпека» (https://kbzi.knu.ua/diplom_bak/).
Регламент виконання випускних кваліфікаційних робіт доводиться до відома студентів перед початком дипломного проєктування.
Перед захистом всі роботи перевіряються на плагіат, до матеріалів роботи долучається довідка про проходження такої перевірки. На ОП «Кібербезпека» відсоток унікальності кваліфікаційних робіт у середньому за різними роками становить 85-95%.

Яким документом ЗВО регулюється процедура проведення контрольних заходів? Яким чином забезпечується його доступність для учасників освітнього процесу?

Процедура проведення контрольних заходів регулюється:
1) «Положенням про організацію освітнього процесу у Київського Національного університету імені Тараса Шевченка» (розділи 4, 7 та інше) (https://www.knu.ua/pdfs/official/Polozhennia-pro-organizatsiyu-osvitniogo-procesu-11_04_2022.pdf)
2) «Положення про порядок створення та організацію роботи Екзаменаційної комісії у Київському національному університеті імені Тараса Шевченка» від 3 листопада 2014 року (http://nmc.univ.kiev.ua/docs/Polojennya%20pro%20DEK.doc);
3) «Положення про систему забезпечення якості освіти та освітнього процесу в Київському національному університеті імені Тараса Шевченка» (https://knu.ua/pdfs/official/Quality-assurance-system-of-education-and-educational-process.pdf);
4) «Тимчасовий порядок проведення заліково-екзаменаційної сесії та підсумкової атестації з використанням технологій дистанційного навчання у Київському національному університеті імені Тараса Шевченка» (http://nmc.univ.kiev.ua/docs/Poryadok%20zal_ekz%20sesii%20dyst_techn.pdf), яке діє під час карантину і воєнного стану.
Усі вказані вище документи є оприлюдненими на сайтах та доступні для всіх учасників освітнього процесу.

Яким чином ці процедури забезпечують об'єктивність екзаменаторів? Якими є процедури запобігання та врегулювання конфлікту інтересів? Наведіть приклади застосування відповідних процедур на ОП

Об'єктивність та неупередженість екзаменаторів забезпечується відповідно до пунктів 7.1.7-7.1.8. «Положенням про організацію освітнього процесу у Київського Національного університету імені Тараса Шевченка» (розділи 4,7 та інше) (https://www.knu.ua/pdfs/official/Polozhennia-pro-organizatsiyu-osvitniogo-procesu-11_04_2022.pdf):
1) оцінювання під час іспитів проводиться комісією, яка включає як мінімум двох викладачів;
2) оцінювачі мають право не брати участь в оцінюванні у випадку виникнення конфлікту інтересів;
3) результати семестрового оцінювання зберігаються впродовж одного року, що дозволяє, перевірити об'єктивність оцінювання. При проведенні оцінювання з використанням засобів інформаційно-комунікаційних технологій здійснюється відеофіксація всієї процедури проведення оцінювання.
Процедури запобігання та врегулювання конфлікту інтересів регламентуються «Положенням про систему забезпечення якості освіти та освітнього процесу в Київському національному університеті імені Тараса Шевченка», «Положенням про організацію освітнього процесу у Київського Національного університету імені Тараса Шевченка», (https://www.knu.ua/pdfs/official/Polozhennia-pro-organizatsiyu-osvitniogo-procesu-11_04_2022.pdf), «Порядок вирішення конфліктних ситуацій у Київському національному університеті імені Тараса Шевченка» (http://www.univ.kiev.ua/pdfs/official/Procedure-for-resolving-conflict-situations-in-University.pdf).
На ОП конфліктних ситуацій під час оцінювання зафіксовано не було.

Яким чином процедури ЗВО урегульовують порядок повторного проходження контрольних заходів? Наведіть приклади застосування відповідних правил на ОП

Регулювання порядку повторного проходження контрольних заходів наведено у «Положення про організацію освітнього процесу у Київському національному університеті імені Тараса Шевченка» (https://knu.ua/pdfs/official/Quality-assurance-system-of-education-and-educational-process.pdf), а саме у пункті 7.3 «Повторне складання семестрового контролю». Згідно з положенням, повторне проходження контрольних заходів можливе лише у випадку отримання незадовільної оцінки. Здобувачу освіти, який одержав під час семестрового контролю не більше двох незадовільних оцінок, дозволяється ліквідувати академічну заборгованість до початку наступного семестру. Повторне складання іспитів/заліків допускається не більше двох разів із кожної дисципліни: перший раз – викладачу, другий – комісії, яка створюється деканом факультету. Для перескладання академічних заборгованостей складається графік, який оприлюднюється на сайті факультету заздалегідь.
На ОП всі випадки повторного проходження контрольних заходів здійснюються відповідно до нормативних документів Київського Національного університету імені Тараса Шевченка.
За І сем. 2022-2023 н.р. з дисципліни «Теорія інформації та кодування» було організовано повторне складання заліку для 2 здобувачів. Згідно з нормативними документами було організовано перше перескладання викладачу 27.12.2022 (за його результатами залік склав 1 здобувач, 1 отримав «не зараховано») та друге перескладання комісії 11.01.2023. Комісія складалася з трьох викладачів, один з них – в.о. завідувача кафедри.

Яким чином процедури ЗВО урегульовують порядок оскарження процедури та результатів проведення контрольних заходів? Наведіть приклади застосування відповідних правил на ОП

Порядок оскарження процедури та результатів проведення контрольних заходів регулюється наступними документами:
Положення про організацію освітнього процесу у Київському національному університеті імені Тараса Шевченка (розділ 4, 8 та інші): (https://knu.ua/pdfs/official/Polozhennia-pro-organizatsiyu-osvitniogo-procesu-11_04_2022.pdf).
Положення про порядок створення та організацію роботи Екзаменаційної комісії в Київському національному університеті імені Тараса Шевченка від 3 листопада 2014 року:
(nmc.univ.kiev.ua/docs/Polojennya%20pro%20DEK.doc).
Зокрема, поточний контроль оскаржується впродовж тижня після оголошення результатів контролю, а семестровий контроль оскаржується в день його оголошення.
Підсумкова атестація може бути оскаржена впродовж 12 годин наступного робочого дня, що слідує за днем оголошення результатів, поданням апеляції на ім'я ректора.
Випадків оскарження результатів контрольних заходів за даною ОП «Кібербезпека» не було.

Які документи ЗВО містять політику, стандарти і процедури дотримання академічної доброчесності?

Поняття академічної доброчесності на ОП «Кібербезпека» регламентується «Етичним кодексом університетської спільноти» (https://www.knu.ua/pdfs/official/ethical-code/Ethical-code-of-the-university-community.pdf), введено у п.1. «Положення про організацію освітнього процесу у Київському національному університеті імені Тараса Шевченка» (https://www.knu.ua/pdfs/official/Polozhennia-pro-organizatsiyu-osvitniogo-procesu-11_04_2022.pdf).
У підрозділах 9.8, 10.7 та окремих підпунктах розділів 7 і 8 визначені види порушень і відповідальність здобувачів освіти та НПП.
Політика та стандарти доброчесності здобувачів вищої освіти описані в п. 5 «Етичного кодексу університетської спільноти» та п.9.8. «Положення про організацію освітнього процесу у Київському національному університеті імені Тараса Шевченка». Процедури дотримання академічної доброчесності регламентуються п.4.2 та п.5.3 «Положення про систему забезпечення якості освіти та освітнього процесу в Київському національному університеті імені Тараса Шевченка (https://knu.ua/pdfs/official/Quality-assurance-system-of-education-and-educational-process.pdf), «Положення про систему виявлення та запобігання академічному плагіату у Київському національному університеті імені Тараса Шевченка» (http://senate.univ.kiev.ua/?p=1352), «Положення про забезпечення дотримання академічної доброчесності у Київському національному університеті імені Тараса Шевченка» (http://senate.univ.kiev.ua/?p=2104).

Які технологічні рішення використовуються на ОП як інструменти протидії порушенням академічної доброчесності?

Відповідно до "Положення про систему виявлення та запобігання академічному плагіату у Київському національному університеті імені Тараса Шевченка" (https://knu.ua/pdfs/official/Detection-and-prevention-of-academic-plagiarism-in-University.pdf) всі кваліфікаційні роботи ОП «Кібербезпека» на етапі допуску до захисту підлягають обов'язковій перевірці на плагіат системою виявлення плагіату Unicheck (https://unicheck.com).
26 квітня 2018 року Київський національний університет імені Тараса Шевченка уклав Договір про співпрацю із компанією «Антиплагіат».
Відповідальним за перевірку кваліфікаційних робіт на кафедрі є к.т.н. Шестак Я.В., якій наукові керівники надсилають готові студентські роботи. Після захисту кваліфікаційні роботи передаються в репозиторій бібліотеки Київського національного університету імені Тараса Шевченка
(https://ir.library.knu.ua/knurepo/handle/123456789/82).
Також задля запобігання можливості порушення академічної доброчесності теми курсових та кваліфікаційних робіт формулюються індивідуально для кожного здобувача освіти.

Яким чином ЗВО популяризує академічну доброчесність серед здобувачів вищої освіти ОП?

На кафедрі КБЗІ популяризується неухильне дотримання принципів і норм етичного кодексу університетської спільноти. Куратори груп та викладачі проводять зі здобувачів вищої освіти обговорення видів порушення академічної доброчесності.

На сайті кафедри оприлюднені матеріали щодо перевірки кваліфікаційних робіт бакалавра на плагіат (https://kbzi.knu.ua/final_certification_bak/).
Крім того, академічна доброчесність популяризується шляхом постійних роз'яснень основних вимог, щодо академічної доброчесності, інформування здобувачів вищої освіти про проушення принципів академічної доброчесності, недопущення випадків плагіату, фальсифікацій та обману, пояснення відповідальності за порушення академічної доброчесності. Університет є учасником проєкту «Ініціатива академічної доброчесності та якості освіти» (Academic Integrity and Quality Initiative – Academic IQ).
Крім того, популяризацію академічної доброчесності проводить студентське самоврядування (згідно «Положення про студентське самоврядування») та студпарламент (http://sp.knu.ua).

Яким чином ЗВО реагує на порушення академічної доброчесності? Наведіть приклади відповідних ситуацій щодо здобувачів вищої освіти відповідної ОП

При виявленні порушень академічної доброчесності на ОП керуються «Положенням про систему виявлення та запобігання академічному плагіату у Київському національному університеті імені Тараса Шевченка» та «Положенням про організацію освітнього процесу у Київському національному університеті імені Тараса Шевченка». Види реагування зазначені у п. 9.8.3 «Положення про організацію освітнього процесу у Київському національному університеті імені Тараса Шевченка», а саме: повторне проходження оцінювання; повторне проходження відповідного освітнього компонента ОП «Кібербезпека»; відрахування з Університету; позбавлення академічної стипендії; позбавлення наданих Університетом пільг з оплати навчання. Відповідно до пункту 9.8.5. «Положення про організацію освітнього процесу у Київському Національному університеті імені Тараса Шевченка» порядок встановлення фактів порушення академічної доброчесності визначено Вченою Радою з урахуванням вимог ЗУ «Про освіту». Здобувач освіти, щодо якого розглядається питання про порушення академічної доброчесності, має право: ознайомитися з усіма матеріалами перевірки та подати до них зауваження; надавати усні та письмові пояснення або відмовитися від надання будь-яких пояснень, брати участь у дослідженні доказів порушення академічної доброчесності; знати про дату, час і місце та бути присутнім під час розгляду питання про встановлення факту порушення академічної доброчесності та притягнення його до академічної відповідальності; оскаржити рішення про притягнення до академічної відповідальності.

6. Людські ресурси

Яким чином під час конкурсного добору викладачів ОП забезпечується необхідний рівень їх професіоналізму?

Оголошення конкурсу на заміщення вакантних посад публікується у газеті «Сучасна освіта України» та на сайті Університету (http://senate.univ.kiev.ua/?cat=9).
Забезпечення необхідного рівня професіоналізму викладачів здійснюється шляхом дотримання чітко визначеної прозорої процедури конкурсного відбору. Основним критерієм є професіоналізм претендента: відповідність його освіти посаді; наявність наукових і вчених звань; стаж науково-педагогічної діяльності; рівень науково-теоретичного рівня викладання дисциплін; авторство підручників, посібників тощо; публікаційна активність. Необхідний рівень професіоналізму викладачів забезпечується відповідністю викладачів ОП «Кібербезпека» кваліфікаційним вимогам, визначеними ліцензійними умовами провадження освітньої діяльності.
Обговорення кандидатур претендентів на заміщення вакантних посад професорів, доцентів, асистентів проводиться трудовим колективом кафедри, вченою радою факультету, Вченою радою Університету (для професорів та завідувачів кафедр).
Наразі кваліфікація НПП кафедри, залучених для викладання на ОП «Кібербезпека», забезпечує досягнення визначених ОП програмних результатів навчання та відповідає вимогам.

Опишіть, із посиланням на конкретні приклади, яким чином ЗВО залучає роботодавців до організації та реалізації освітнього процесу

Процедура залучення фахівців-практиків та роботодавців регламентована Статутом Київського національного університету імені Тараса Шевченка (наказ від 18.22.2022, №1061), а також в Університеті створено Раду роботодавців (http://surl.li/dexqf), затверджене Положення про ради роботодавців (https://cutt.ly/hVcD1wS), наказ ректора No832-32 від 26.10.2021 р. врегульовує питання організації експертних рад роботодавців при факультетах для спеціальності (групи спеціальностей). Університет активно залучає ІБ-компанії для діалогу щодо формування ОП «Кібербезпека» та РНП ОК, наприклад: "ДССЗЗІ"; "B2B-рішення"; ТОВ "ЕРАМ СИСТЕМЗ", ТОВ "Авалекс Сольюшнз", ТОВ "МТІ", ТОВ "Ел-Консалтинг", KPMG (детальніше за посиланням: (https://kbzi.knu.ua/2023/01/26/kr_st_p9098/) та керівництва виробничими практиками.

Опишіть, із посиланням на конкретні приклади, яким чином ЗВО залучає до аудиторних занять на ОП професіоналів-практиків, експертів галузі, представників роботодавців

Університет забезпечує можливість залучення професіоналів практиків (експертів галузі, представників роботодавців) до викладання, керівництва практикою і кваліфікаційними роботами шляхом зарахування на частину ставки і погодинної оплати їх праці, а також за сумісництвом. Фахівцям-практикам надається дозвіл на читання лекцій незалежно від наявності у них наукового ступеню. Наприклад, директор ТОВ "B2B-рішення" А. Бігдан, директор ТОВ «ІТЦ Хайтек Бюро» О.Гребенюк, директор ТОВ "Акксон Софт" О.Курінний

(https://kbzi.knu.ua/2023/02/07/stholder_p2359)

Опишіть, яким чином ЗВО сприяє професійному розвиткові викладачів ОП? Наведіть конкретні приклади такого сприяння

Можливості для підвищення кваліфікації зокрема створюють Інститут післядипломної освіти (http://www.ipe.knu.ua/), Відділ академічної мобільності Київського національного університету імені Тараса Шевченка (http://mobility.univ.kiev.ua/?page_id=2&lang=uk), Відділ міжнародних зв'язків (http://international.knu.ua/).
Університет є засновником платформи «KNU Professionals» для фахового розвитку НПП та підвищення рівня педагогічної майстерності і щорічно організовує курс KNU Teach Week (https://www.facebook.com/KNUprofessionals).
Для підвищення кваліфікації викладачів на факультеті функціонують мережеві академії Cisco (https://kbzi.knu.ua/cisco/), та USAID/RangeForce (https://kbzi.knu.ua/usaid/) в яких мають можливість навчатися та сертифікуватися як здобувачі вищої освіти, так і викладачі кафедри.

Продемонструйте, що ЗВО стимулює розвиток викладацької майстерності

Університет є учасником програми вдосконалення викладання у вищій освіті України та проєкту: «Якісне навчання через якісне викладання» метою якого є покращення якості викладання навчальних дисциплін та підвищення ефективності навчального процесу за допомогою впровадження сучасних методик і технік.
Стимулюванню викладацької майстерності сприяє Наказ Ректора № 71-32 від 31.01.2014р. «Про затвердження Положення про стимулювання співробітників Київського Національного університету імені Тараса Шевченка за результатами наукової діяльності», розпорядження ректора «Про створення комісії з матеріального заохочення» від 10.12.2018р. за №113 (http://science.univ.kiev.ua/news/official/3247/).
З метою підвищення майстерності, засвоєння нових засобів навчання в Університеті проводяться тренінги для співробітників. Зокрема, у 2020 р. відбувся тренінг з цифрової трансформації для викладачів кафедри та факультету від виконавців проєкту програми Erasmus+ КА2 «dComFra» (http://fit.univ.kiev.ua/erasmus-ka2-dcomfra), USAID (https://kbzi.knu.ua/usaid/).
До матеріального стимулюванням розвитку викладацької майстерності НПП можна віднести щорічне відзначення кращих викладачів факультету (http://fit.univ.kiev.ua/best-lecturers) (матеріальне заохочення), доплати за вчене звання та науковий ступінь, преміювання за результатами публікаційної активності. До нематеріального заохочення відноситься висунення НПП на відзнаки МОН та НАНУ.

7. Освітнє середовище та матеріальні ресурси

Продемонструйте, яким чином фінансові та матеріально-технічні ресурси (бібліотека, інша інфраструктура, обладнання тощо), а також навчально-методичне забезпечення ОП забезпечують досягнення визначених ОП цілей та програмних результатів навчання?

Створена матеріально-технічна база (МТБ) на факультеті інформаційних технологій відповідає сучасним вимогам щодо забезпечення комп'ютерною технікою, програмним забезпеченням, аудиторним фондом тощо. Лекційні аудиторії укомплектовані мультимедійними проєкторами, лабораторії – сучасною комп'ютерною технікою, підключенням до Internet. Студентам доступні бібліотечні фонди наукової та методичної літератури, електронний каталог наукових джерел та on-line доступ до фахової літератури. Наукова бібліотека ім. М. Максимовича надає відкритий доступ до електронних ресурсів (https://goo.su/IHR), повнотекстової платформи Springer Nature (https://goo.su/A8j) та сучасної наукової періодики.
МТБ дозволяє опановувати навчальні матеріали з використанням сучасних програмних засобів та середовищ, забезпечує доступ до фахової літератури, дозволяє проводити аналіз сучасних наукових публікацій та виконувати власні програмні експерименти за напрямками досліджень, що в цілому забезпечує досягнення визначених ОП «Кібербезпека» цілей та програмних результатів.
Описи ОП «Кібербезпека», робочі програми дисциплін доступні для студентів на сайті кафедри (https://kbzi.knu.ua/opp_2022/). Розроблені викладачами навчально-методичні комплекси систематично оновлюються та відповідають цілям та програмним результатам навчання. Для забезпечення ефективності навчання в умовах сьогодення на факультеті впроваджено використання освітніх платформ зокрема Microsoft Teams, Moodle та інші.

Продемонструйте, яким чином освітнє середовище, створене у ЗВО, дозволяє задовольнити потреби та інтереси здобувачів вищої освіти ОП? Які заходи вживаються ЗВО задля виявлення і врахування цих потреб та інтересів?

Створене в Університеті освітнє середовище вибудоване на принципах забезпечення якісної сучасної освіти та безпечних умов навчання, побуту, дозвілля. Всі інформаційні ресурси, потрібні для навчання, викладацької, наукової діяльності в межах ОП «Кібербезпека» є у вільному доступі викладачів і студентів, що забезпечується відповідною ІТ-інфраструктурою (системою Triton, WEB-ресурси кафедри, бібліотечні фонди тощо). Проводяться фахові наукові конференції та семінари, що надає можливість студентам викласти свої наукові ідеї та результати, отримати оцінку та поради фахівців. Діє програма академічної мобільності, що забезпечує можливість навчання та стажування у провідних університетах світу. Представники студентського самоврядування входять до складу

керівних органів університету, що сприяє дотриманню прав й інтересів здобувачів. В університеті працює Інститут кураторства. Для забезпечення умов повноцінного та змістовного дозвілля студентів функціонують Молодіжний центр культурно-естетичного виховання (https://goo.su/wYE), спорткомплекс, гуртки. Проводяться щорічні моніторингові опитування UNIDOS (http://unidos.univ.kiev.ua/) для виявлення потреб, інтересів та рівня задоволеності здобувачів навчальним процесом, культурно-соціальною сферою, матеріально-технічним, інформаційним забезпеченням, рівнем науково-дослідної роботи, виявлення недоліків в організації провадження освітньої діяльності. Результати опитувань аналізуються керівництвом університету та факультетів і, в разі необхідності, вживаються необхідні заходи.

Опишіть, яким чином ЗВО забезпечує безпечність освітнього середовища для життя та здоров'я здобувачів вищої освіти (включаючи психічне здоров'я)?

Стратегічний план розвитку Університету на період 2018-2025 року, затверджений Вченою радою Університету 25 червня 2018 року, містить заходи з соціально-педагогічного супроводу для забезпечення сприятливих умов навчання (http://senate.univ.kiev.ua/?p=742). Університет забезпечує дотримання "Правил внутрішнього розпорядку Київського національного університету імені Тараса Шевченка" (https://goo.su/9FDW), "Положення про студентське містечко та студентський гуртожиток Київського національного університету імені Тараса Шевченка", "Правил внутрішнього розпорядку в студентських гуртожитках університету" (https://studmisto.knu.ua/documents/regulation-documents/257-pravyla-vnutrishnoho-rozporiadku), також гарантуються належні умови праці та навчання відповідно до вимог законодавства про охорону праці. Проводяться інструктажі з техніки безпеки на лабораторних заняттях і перед практиками.
Служба психологічної підтримки університету (https://psyservice.knu.ua/, https://t.me/psy_service_knu) забезпечує можливість отримання фахової допомоги всіма учасниками освітнього процесу. За необхідності є можливість отримати спеціалізовану медичну допомогу фахівців Інституту психіатрії Університету.
Університетська клініка забезпечує проведення профілактичних оглядів та пропонує широкий спектр медичних послуг.

Опишіть механізми освітньої, організаційної, інформаційної, консультативної та соціальної підтримки здобувачів вищої освіти? Яким є рівень задоволеності здобувачів вищої освіти цією підтримкою відповідно до результатів опитувань?

З метою забезпечення освітньої підтримки здобувачів та сприяння їх професійному росту в Київському національному університеті імені Тараса Шевченка і на факультеті інформаційних технологій, зокрема, запроваджено ряд механізмів освітньої, організаційної, інформаційної та консультативної підтримки. Освітня підтримка здобувачів передбачає в рамках викладання дисциплін проведення навчальних занять, практичної підготовки, виконання індивідуальних самостійних робіт, контрольних заходів, консультацій. Необхідні освітні матеріали доступні в бібліотеці університету та електронній бібліотеці (https://goo.su/yiu) тощо.
Крім освітньої підтримки на факультеті студентам надають допомогу: центр по роботі зі студентами, відділ академічної мобільності, відділ сприяння працевлаштуванню та роботі з випускниками (http://jobs.knu.ua), спорткомплекс, Молодіжний центр культурно-естетичного виховання (https://goo.su/HzH), Центр комунікацій (https://goo.su/bez), Наукове товариство студентів та аспірантів (http://ntsa.univ.kiev.ua/), Навчальна лабораторія соціологічних та освітніх досліджень. Власна університетська клініка забезпечує консультації та допомогу з питань здоров`я. Діє психологічна служба університету.
Вирішення організаційних питань на факультеті покладено на деканат, завідувачів та фахівців кафедр, кураторів груп. Актуальна інформація щодо всіх питань діяльності факультету та кафедри висвітлюється на інформаційних стендах, дошках об'яв та відповідних інтернет-ресурсах. Інструментами інформаційної підтримки є сайти (https://www.knu.ua/), телеграм-канал PRAVDA inn-KNU, (http://fit.univ.kiev.ua), (https://kbzi.knu.ua). Науково-педагогічні працівники кафедри забезпечують інформаційно-консультативну підтримку здобувачів, що реалізована у формі планових консультацій в ході навчання та позааудиторний час, індивідуальних on-line консультацій. Активним виразником проблем і помічником у вирішення широкого кола питань є студентське самоврядування. Скарг та нарікань від здобувачів щодо усіх видів підтримки не надходило.
Результати опитувань здобувачів ОП «Кібербезпека» свідчать про переважне задоволення такою підтримкою.

Яким чином ЗВО створює достатні умови для реалізації права на освіту особами з особливими освітніми потребами? Наведіть посилання на конкретні приклади створення таких умов на ОП (якщо такі були)

Відповідно до Положення про організацію освітнього процесу у Київському національному університеті імені Тараса Шевченка (п.12.3.8) Університет забезпечує учасникам освітнього процесу (у т. ч. іноземним громадянам і здобувачам освіти з особливими потребами) безперешкодний доступ до навчально-методичного забезпечення, бібліотечних ресурсів, наукометричних баз даних, надання їм фахової консультаційної підтримки, тощо, а також належне технічне оснащення аудиторного фонду та гуртожитків, надає підтримку випускникам у працевлаштуванні.
Інші документи, які регламентують створення умов для реалізації права на освіту особами з особливими освітніми потребами:
1. Концепція розвитку інклюзивної освіти "Університету рівних можливостей" (http://www.univ.kiev.ua/pdfs/equal-opportunities/Concept-of-inclusive-education-development.pdf).
2. Пам'ятка про правила комунікації із людьми з інвалідністю (http://www.univ.kiev.ua/pdfs/equal-opportunities/Pamyatka-pro-pravyla-komunikaciyi-iz-lyudmy-z-invalidnistyu.pdf).
3. Порядок супроводу осіб з інвалідністю (http://www.univ.kiev.ua/pdfs/equal-opportunities/Poryadok-suprovodu-osib-z-invalidnistyu.pdf).
Статутом Київського Національного університету імені Тараса Шевченка (https://www.univ.kiev.ua/pdfs/statut/statut-

22-11-28.pdf) закріплене право здобувача освіти на «спеціальний навчально-реабілітаційний супровід і вільний доступ до інфраструктури Університету, відповідно до медико-соціальних показань за наявності обмежень життєдіяльності, зумовлених станом здоров'я.

Яким чином у ЗВО визначено політику та процедури врегулювання конфліктних ситуацій (включаючи пов'язаних із сексуальними домаганнями, дискримінацією та корупцією)? Яким чином забезпечується їх доступність політики та процедур врегулювання для учасників освітнього процесу? Якою є практика їх застосування під час реалізації ОП?

У Київському національному університеті імені Тараса Шевченка діє ряд документів щодо визначення політики та процедур врегулювання конфліктних ситуацій (включаючи пов'язаних із сексуальними домаганнями, дискримінацією та корупцією), а саме:
1. Положення про організацію освітнього процесу у Київському національному університеті імені Тараса Шевченка (https://goo.su/SKw).
2. Порядок вирішення конфліктних ситуацій у Київському національному університеті імені Тараса Шевченка (https://goo.su/Pta) введений в дію наказом Ректора N105-32 від 14.02.2020 р.
3. Заходи щодо запобігання та протидії корупції (https://goo.su/b76j).
4. Антикорупційна програма (https://goo.su/09O).
5. Етичний кодекс університетської спільноти (https://goo.su/muq).
Діє Положення про Постійну комісію Вченої ради з питань етики (https://goo.su/yOU).
Вся необхідна інформація є у відкритому доступі. Серед здобувачів вищої освіти з метою ознайомлення останніх з чинними процедурами вирішення конфліктних ситуацій у Київському національному університеті імені Тараса Шевченка на рівні факультету, кафедри, освітніх програм, кураторів груп ведеться на систематичній основі інформаційно-роз'яснювальна робота.
У разі виникнення конфліктних ситуацій здобувач вищої освіти звертається до куратора академічної групи та завідувача кафедри. З метою аналізу та формування подальшого плану дій з подолання негативного явища проводяться спільні засідання та обговорення проблем з участю завідувача кафедри, куратора групи, гарантом ОП «Кібербезпека» та студентами. Будь-який учасник освітнього процесу має можливість скористатися телефоном або поштовою скринькою довіри як на рівні університету, так і на рівні факультету і кафедри (https://kbzi.knu.ua/location/). За результатами Комплексної перевірки факультету 2019 р. не було виявлено жодного натяку на будь-яку корупційну складову, що було оголошено на Вченій раді та опубліковано у відповідному звіті на сайті факультету (https://goo.su/9FE1).
Випадків конфліктних ситуацій пов'язаних із сексуальними домаганнями, корупцією або дискримінацією на ОП, що акредитується не зафіксовано.

8. Внутрішнє забезпечення якості освітньої програми

Яким документом ЗВО регулюються процедури розроблення, затвердження, моніторингу та періодичного перегляду ОП? Наведіть посилання на цей документ, оприлюднений у відкритому доступі в мережі Інтернет

Процедури розроблення, затвердження, моніторингу та періодичного перегляду освітньої програми ОП «Кібербезпека» регулюються наступними документами:
1. Положення про організацію освітнього процесу у Київському національному університеті імені Тараса Шевченка (https://www.knu.ua/pdfs/official/Polozhennia-pro-organizatsiyu-osvitniogo-procesu-11_04_2022.pdf).
2. Наказ ректора №158-32 від 05.03.2018 року "Про затвердження тимчасового порядку розроблення, розгляду і затвердження освітніх (освітньо-професійних, освітньо-наукових) програм" (http://nmc.univ.kiev.ua/docs/Poryadok_OP.pdf).
3. Наказ ректора №729-32 від 11.08.2017 р. "Про запровадження в освітній та інформаційний процес форм опису освітньо-професійної (освітньо-наукової) програми, структурних вимог до інформаційного пакета, форм робочої навчальної програми дисципліни і форми представлення інформації про кваліфікацію науково-педагогічного працівника" (http://nmc.univ.kiev.ua/docs/Nakaz_Form_Doc-729-32_11-08-2017.pdf) (з додатками).
4. Наказ ректора №601-32 від 08.07.2019 року "Про затвердження Тимчасового порядку розгляду пропозицій щодо внесення змін до описів ступеневих освітніх програм" (http://nmc.univ.kiev.ua/docs/Tymchasovyi%20poryadok%20vnesennya%20zmin%20do%20OOP.pdf).
5. Положення про систему забезпечення якості освіти та освітнього процесу в Київському національному університеті імені Тараса Шевченка (https://www.knu.ua/pdfs/official/Quality-assurance-system-of-education-and-educational-process.pdf)

Опишіть, яким чином та з якою періодичністю відбувається перегляд ОП? Які зміни були внесені до ОП за результатами останнього перегляду, чим вони були обґрунтовані?

Згідно до Положенням про організацію освітнього процесу (https://www.knu.ua/pdfs/official/Polozhennia-pro-organizatsiyu-osvitniogo-procesu-11_04_2022.pdf) моніторинг та періодичний перегляд ОП «Кібербезпека» проводиться не рідше ніж раз на рік. Підстави для внесення змін до затверджених описів ОП, ініціатори та порядок внесення пропозицій, їх оформлення та оприлюднення визначаються у «Положення про систему забезпечення якості освіти та освітнього процесу в Київському національному університеті імені Тараса Шевченка (https://knu.ua/pdfs/official/Quality-assurance-system-of-education-and-educational-process.pdf)
У 2022 році була підготовлена нова редакція ОП, що враховувала зміни в Стандарту вищої освіти України першого

бакалаврського рівня, галузі знань 12 - Інформаційні технології, спеціальності 125 “Кібербезпека” від 13.01.2022, згідно з Концепцією вивчення іноземних мов студентами неспеціалізованих факультетів/інститутів Київського національного університету імені Тараса Шевченка №196-32 від 10.03.2020 р., а також враховувала результати обговорення ОП зі здобувачами та стейкхолдерами за участі представників ІБ та ІТ-компаній. Зокрема в новій редакції ОП в якості форми атестації введений єдиний державний комплексний іспит зі спеціальності, оновлено вибіркові компоненти тощо. Також внесені відповідні зміни до навчального плану.

Продемонструйте, із посиланням на конкретні приклади, як здобувачі вищої освіти залучені до процесу періодичного перегляду ОП та інших процедур забезпечення її якості, а їх позиція береться до уваги під час перегляду ОП

Відповідно до «Положення про систему забезпечення якості освіти та освітнього процесу в Київському національному університеті імені Тараса Шевченка (https://knu.ua/pdfs/official/Quality-assurance-system-of-education-and-educational-process.pdf) звернення здобувачів освіти або результати опитування здобувачів освіти, які навчаються на ОП «Кібербезпека», є підставою для ініціювання пропозицій щодо внесення змін до затверджених описів ОП «Кібербезпека». Кафедрою та факультетом інформаційних технологій проводяться щорічні опитування студентів щодо якості організації освітнього процесу на ОП «Кібербезпека», студенти та випускники можуть подавати також свої пропозиції щодо внесення змін до опису ОП «Кібербезпека», до робочих програм освітніх компонентів, форм та методів навчання, викладання, оцінювання тощо, безпосередньо НПП, що залучені до викладання на ОП, гаранту освітньої програми, завідувачу кафедри або надсилати свої пропозиції через сайт кафедри (https://kbzi.knu.ua/bakalavr/). Отримані пропозиції розглядаються та обговорюються на засіданні кафедри, за рішенням кафедри виносяться до розгляду до науково-методичної комісії факультету та вченої ради факультету за встановленою в Університету процедурою.

Яким чином студентське самоврядування бере участь у процедурах внутрішнього забезпечення якості ОП

Положення про Студентське самоврядування Університету (https://goo.su/9feR) регулює участь студентів у заходах щодо забезпечення якості вищої освіти, студенти можуть вносити пропозиції щодо змісту навчальних планів і програм та організації навчального процесу, інших питань життєдіяльності Університету; звертатися до адміністрації з пропозиціями щодо їх вирішення; виносити на розгляд адміністрації питання, що потребують відповідних рішень; брати участь у вирішенні конфліктних ситуацій, делегувати своїх представників до робочих органів (Науково-методична рада університету, вчена рада факультету, Вчена Рада Університету, науково-методична комісія факультету). Згідно з «Положення про систему забезпечення якості освіти та освітнього процесу в Київському національному університеті імені Тараса Шевченка (https://knu.ua/pdfs/official/Quality-assurance-system-of-education-and-educational-process.pdf) до суб’єктів, що можуть ініціювати зміни до освітніх програм, віднесені органи студентського самоврядування.
Студентське самоврядування факультету ініціює проведення опитувань серед студентів (https://goo.su/Bgs), асоціація випускників факультету ставить на меті брати участь в розробці та реалізації освітніх програм (https://goo.su/9Jf). Представники студентського самоврядування є членами вченої ради факультету та науково-методичної комісії факультету, тому мають можливість активно брати участь в обговоренні пропонованих змін, а також, як представники студспільноти факультету, бути їх ініціаторами.

Продемонструйте, із посиланням на конкретні приклади, як роботодавці безпосередньо або через свої об’єднання залучені до процесу періодичного перегляду ОП та інших процедур забезпечення її якості

Положенням про ради роботодавців у Київському національному університеті імені Тараса Шевченка (https://goo.su/VmB) визначено, що одним з основних завдань ради роботодавців є внесення пропозицій в процесі розробки/перегляду освітніх програм. Крім того, однією з підстав щодо внесення змін до описів чинний освітніх програм відповідно до «Положення про систему забезпечення якості освіти та освітнього процесу в Київському національному університеті імені Тараса Шевченка (https://knu.ua/pdfs/official/Quality-assurance-system-of-education-and-educational-process.pdf).
Кафедрою кібербезпеки та захисту інформації та гарантом ОП «Кібербезпека» проводяться постійні консультації з “ДССЗЗІ”, “B2B-рішення”, “ЕРАМ ”ТОВ "Софтпром Солюшнз", ТОВ "МТІ", ТОВ "Ел-Консалтинг", KPMG та ін.), з представниками наукових установ та академічної спільноти з метою насичення ОК ОП «Кібербезпека» сучасними науковими досягненнями в галузі кібербезпеки та захисту інформації (https://kbzi.knu.ua/2021/09/29/k_s_sreak_cs_p4443/).

Опишіть практику збирання та врахування інформації щодо кар’єрного шляху та траєкторій працевлаштування випускників ОП

На факультеті інформаційних технологій створено асоціацію випускників факультету (http://fit.univ.kiev.ua/асоціація-випускників-фіту).
Випускники факультету залучаються до проведення «Днів відкритих дверей», «Дня факультету» та інших культурно-масових заходів.
Викладачі кафедри кібербезпеки та захисту інформації, куратори студентських груп підтримують контакти з випускниками, дізнаються інформацію про їх кар’єрний ріст та траєкторію працевлаштування. Випускники також діляться своїми враженнями про сильні та слабкі сторони освітньої програми. Пропозиції випускників аналізуються та розглядаються на засіданні кафедри. Кафедра кібербезпеки та захисту інформації, факультет інформаційних технологій та Університет інформує та допомагає випускникам у працевлаштуванні. На сайті http://job.univ.kiev.ua

публікуються вакансії для випускників. Під час проведення «Дня факультету» у випускників є можливість ознайомитися з можливостями працевлаштування, що сприятиме їх кар'єрному росту.

Які недоліки в ОП та/або освітній діяльності з реалізації ОП були виявлені у ході здійснення процедур внутрішнього забезпечення якості за час її реалізації? Яким чином система забезпечення якості ЗВО відреагувала на ці недоліки?

Якщо під час реалізації ОП виявляються недоліки, внесення змін здійснюється у відповідності до процедури, що визначена у «Положення про систему забезпечення якості освіти та освітнього процесу в Київському національному університеті імені Тараса Шевченка (https://knu.ua/pdfs/official/Quality-assurance-system-of-education-and-educational-process.pdf).
Гарант освітньої програми, аналізуючи інформацію про рівень успішності здобувачів освіти за освітніми компонентами програми, результати опитувань здобувачів освіти, рекомендації роботодавців та інших стейкхолдерів, досвід вітчизняних та закордонних ЗВО, ситуацію на ринку праці та сучасні тенденції розвитку ІТ-галузі тощо, може ініціювати внесення змін до ОП «Кібербезпека».
В 2022 р. було затверджено нову редакцію ОП «Кібербезпека», в якій було усунуто певні недоліки які були виявлені в процесі провадження ОП «Кібербезпека», зокрема: було забезпечено поглиблене вивчення блоку фундаментальних дисциплін. Після внесення зазначених змін, що дозволили врахувати сучасні тенденції в ІТ та ІБ секторах (введення 6 професійних стандартів) проєктною групою розробляється нова редакція ОП «Кібербезпека».

Продемонструйте, що результати зовнішнього забезпечення якості вищої освіти беруться до уваги під час удосконалення ОП. Яким чином зауваження та пропозиції з останньої акредитації та акредитацій інших ОП були враховані під час удосконалення цієї ОП?

При реалізації ОП «Кібербезпека» були враховані рекомендації експертної комісії що проводила попередню акредитацію, а саме:
1. Вдосконалено наповнення офіційного сайту (https://kbzi.knu.ua/educational_methodical_materials/) навчально-методичними матеріалами, що забезпечують програмні результати освітньої програми;
2. Покращено показники з міжнародних стажувань НПП кафедри, а саме: проф. Н. Лукова-Чуйко проф. С. Бучик, проф. В. Наконечний, доц. А. Фесенко, доц. Л. Мирутенко, ас. С. Даков пройшли наукові закордонні стажування за програмами, що відповідають профілю ОП «Кібербезпека» (https://kbzi.knu.ua/quality/);
3. На кафедрі, що забезпечує підготовку на ОП «Кібербезпека» запроваджено проведення щорічної міжнародної науково-практичної конференції «Проблеми кібербезпеки інформаційно-телекомунікаційних систем» (PCSITS) (https://kbzi.knu.ua/pcsits/);
4. До реалізації освітнього процесу з ОП «Кібербезпека» були залучені: д.т.н. професор Гнатюк С.О (читання лекцій з “Квантової криптології” https://kbzi.knu.ua/2023/02/27/visiting_professor_hnatiuk/), директора ТОВ “B2B рішення” А. Бігдан тощо;
5. Оновлені договори щодо баз практик (https://kbzi.knu.ua/our_partners/).

Опишіть, яким чином учасники академічної спільноти змістовно залучені до процедур внутрішнього забезпечення якості ОП?

Учасники академічної спільноти Київського національного університету імені Тараса Шевченка - керівництво, НПП, наукові співробітники, здобувачі освіти - залучаються до процедур внутрішнього забезпечення якості ОП «Кібербезпека» на етапах розроблення, затвердження, моніторингу та періодичного перегляду ОП «Кібербезпека», а також в процесі її реалізації шляхом рецензування і публічного обговорення на засіданнях, нарадах, семінарах, робочих зустрічах.
НПП проводять та взаємовідвідують відкриті заняття, рецензії на які також обговорюються на засіданнях кафедри. Науково-методичною комісією факультету проводиться внутрішнє рецензування навчально-методичних розробок НПП.
На кафедрі проводяться попередні захисти випускних кваліфікаційних робіт студентів, зовнішнє рецензування кваліфікаційних робіт.
З метою вдосконалення освітнього контенту, форм, методів викладання та оцінювання проводяться консультації з представниками академічної спільноти з інших навчальних закладів України (НТУ України «КПІ імені Ігоря Сікорського», Національний авіаційний університет, Національний університет «Львівська політехніка» та ін.).
НПП кафедри є членами професійних об'єднань та асоціацій.

Опишіть розподіл відповідальності між різними структурними підрозділами ЗВО у контексті здійснення процесів і процедур внутрішнього забезпечення якості освіти

Відповідно до Положення про систему забезпечення якості освіти та освітнього процесу в Київському національному університеті імені Тараса Шевченка (https://cutt.ly/7Cnzfne) відповідальність між різними структурними підрозділами Університету у контексті здійснення процесів і процедур внутрішнього забезпечення якості освіти розподілена так:
1 рівень - здобувачі освіти та їх ініціативні групи, до прав яких належить ініціювання і моніторинг пов’язаний з інформаційним супроводом здобувачів освіти, їх академічною та неакадемічною підтримкою
2 рівень - кафедри, гаранти, проєктні групи, НПП, роботодавці, що відповідають за реалізацію ОП, її моніторинг, ініціювання змін
3 рівень - структурні підрозділи, які здійснюють освітню діяльність: факультети, їх керівники і заступники, вчена рада, НМК, групи забезпечення навчального процесу, навчально-допоміжний персонал, органи студентського самоврядування, галузеві ради роботодавців. На цьому рівні здійснюється контроль за реалізацією ОП і її

адміністрування
4 рівень - загальноуніверситетські структурні підрозділи, що відповідають за реалізацію заходів із забезпечення якості освіти (НМЦ, відділ атестації науково-педагогічних працівників та ін.) На цьому рівні розроблюються та приймаються загальноуніверситетські рішення, документи тощо.
5 рівень - Наглядова Рада, Ректор, Вчена рада, НМК Університету. Це рівень прийняття стратегічних рішень, що визначають політику провадження освітньої діяльності та забезпечення якості освітнього процесу, затверджуються всі нормативно-правові акти Університету

9. Прозорість і публічність

Якими документами ЗВО регулюється права та обов'язки усіх учасників освітнього процесу? Яким чином забезпечується їх доступність для учасників освітнього процесу?

Права та обов'язки усіх учасників освітнього процесу регулюються документами:
Статут Київського національного університету імені Тараса Шевченка (https://www.univ.kiev.ua/pdfs/statut/statut-22-11-28.pdf).
Положення про організацію освітнього процесу у Київському національному університеті імені Тараса Шевченка (https://knu.ua/pdfs/official/Polozhennia-pro-organizatsiyu-osvitniogo-procesu-11_04_2022.pdf).
Положення про систему забезпечення якості освіти та освітнього процесу в Київському національному університеті імені Тараса Шевченка (https://www.univ.kiev.ua/pdfs/official/Quality-assurance-system-of-education-and-educational-process.pdf).
Етичний кодекс університетської спільноти (https://www.knu.ua/pdfs/official/ethical-code/Ethical-code-of-the-university-community.pdf).
Порядок вирішення конфліктних ситуацій у Київському національному університеті імені Тараса Шевченка (https://www.knu.ua/pdfs/official/Procedure-for-resolving-conflict-situations-in-University.pdf).
Положення про гаранта освітньої програми в Київському національному університеті імені Тараса Шевченка (http://senate.univ.kiev.ua/?p=1678).
Правила внутрішнього розпорядку у студентських гуртожитках Київського національного університету імені Тараса Шевченка (https://studmisto.knu.ua/management/documents/regulation-documents/257-pravyla-vnutrishnoho-rozporiadku).
Договір про навчання та договір про надання платної освітньої послуги для підготовки фахівців.

Наведіть посилання на веб-сторінку, яка містить інформацію про оприлюднення на офіційному веб-сайті ЗВО відповідного проекту з метою отримання зауважень та пропозиції заінтересованих сторін (стейкхолдерів). Адреса веб-сторінки

Документація розміщена на офіційному сайті кафедри КБЗІ
https://kbzi.knu.ua/speek_prof_progr/

Наведіть посилання на оприлюднену у відкритому доступі в мережі Інтернет інформацію про освітню програму (включаючи її цілі, очікувані результати навчання та компоненти)

Документація розміщена на офіційному сайті кафедри КБЗІ
ОП "Кібербезпека" – https://kbzi.knu.ua/opp_2022

11. Перспективи подальшого розвитку ОП

Якими загалом є сильні та слабкі сторони ОП?

Сильні сторони:
1. ОП "Кібербезпека" надає здобувачам освіту в інноваційній та наукомісткій галузі інформаційних технологій - кібербезпека, яка є однією з ключових трансформаційних технологій оборони, економіки, державного управління в Україні та світі.
2. ОП "Кібербезпека" вдало поєднує фундаментальну підготовку в області інформаційних технологій, комп'ютерних наук, програмування і ґрунтовну підготовку за напрямками досліджень в області захисту інформації та кібербезпеки за індивідуальною освітньою траєкторією. Все це у сукупності забезпечує високий попит на ОП "Кібербезпека" у здобувачів освіти (високий конкурс, високі середні бали ЗНО вступників порівняно з іншими аналогічними ОП).
3. ОП "Кібербезпека" орієнтована на підготовку кіберфахівців з урахуванням сучасних світових тенденцій з інтелектуалізації інформаційного простору, під час провадження ОП "Кібербезпека" здійснюється постійний моніторинг потенційного ринку праці, використовуються ресурси компаній-партнерів Університету таких, як "ДССЗЗІ", "B2B-рішення", "ЕРАМ "ТОВ "Софтпром Солюшнз", ТОВ "МТІ", ТОВ "Ел-Консалтинг", KPMG та ін. Як наслідок випускники ОП "Кібербезпека" затребувані на ринку праці в Україні та закордоном.
4. При розробці та під час провадження ОП "Кібербезпека" постійно здійснюється моніторинг підходів до реалізації освітньої діяльності за аналогічними освітніми програмами вітчизняних та закордонних ЗВО, зокрема НТУ України «КПІ імені Ігоря Сікорського», НУ «Львівська політехніка», Державний торговельно-економічний університет тощо.

5. Викладання більшості освітніх компонентів здійснюється висококваліфікованими фахівцями, які у своїй практичній діяльності займаються розробкою та впровадженням новітніх технологій, постійно працюють над підвищенням свого професійного рівня та викладацької майстерності, а саме: проходять стажування в провідних фахових компаніях та провідних університетах України та ЕС (проф. Н. Лукова-Чуйко проф. С. Бучик, проф. В. Наконечний, доц. А. Фесенко, доц. Л. Мирутенко, ас. С.Даков), беруть участь в програмах підвищення кваліфікації щодо розбудови системи забезпечення якості освіти.
Слабкі сторони:
1. Низький відсоток залучення представників фахових компаній та лекторів з іноземних університетів до викладання на освітній програмі.
2. Невисока умотивованість здобувачів вищої освіти до науково-дослідної роботи та орієнтація на швидке набуття практичних навичок для працевлаштування під час навчання.

Якими є перспективи розвитку ОП упродовж найближчих 3 років? Які конкретні заходи ЗВО планує здійснити задля реалізації цих перспектив?

Подальший розвиток ОП “Кібербезпека” буде проводитись із врахуванням сучасних тенденцій розвитку кібербезпеки та захисту інформації, міжнародного освітнього простору в сфері комп'ютерних наук як відповідь на виклики ринку праці. На найближчі 3 років можна визначити такі напрямки для реалізації:
1) Провести модифікацію системи вільного вибору студентів в рамках ОП “Кібербезпека”, перейти від вибору блоками дисциплін до вибору з каталогу курсів.
2) Продовжити роботу з вдосконалення робочих програм з метою актуалізації теоретичного та практичного змісту освіти, методів та технологій навчання з врахуванням сучасних трендів розвитку як галузі інформаційних технологій, так і вищої освіти та пропозицій різних груп стейкхолдерів.
3) Ширше залучати до роботи на ОП “Кібербезпека” лекторів з іноземних університетів та представників провідних галузевих кампаній.
4) Продовжити роботу по вдосконаленню навчально-методичного забезпечення освітніх компонентів з використанням сучасних інформаційних технологій представлення навчального матеріалу та розвитку єдиної навчальної онлайн-платформи.
5) Налагодити сталу зворотну комунікацію успішних випускників зі здобувачами освіти ОП “Кібербезпека”.

Запевнення

Запевняємо, що уся інформація, наведена у відомостях та доданих до них матеріалах, є достовірною.

Гарантуємо, що ЗВО за запитом експертної групи надасть будь-які документи та додаткову інформацію, яка стосується освітньої програми та/або освітньої діяльності за цією освітньою програмою.

Надаємо згоду на опрацювання та оприлюднення цих відомостей про самооцінювання та усіх доданих до них матеріалів у повному обсязі у відкритому доступі.

Додатки:

Таблиця 1. Інформація про обов’язкові освітні компоненти ОП

Таблиця 2. Зведена інформація про викладачів ОП

Таблиця 3. Матриця відповідності програмних результатів навчання, освітніх компонентів, методів навчання та оцінювання

***

Шляхом підписання цього документа запевняю, що я належним чином уповноважений на здійснення такої дії від імені закладу вищої освіти та за потреби надам документ, який посвідчує ці повноваження.

Документ підписаний кваліфікованим електронним підписом/кваліфікованою електронною печаткою.

Інформація про КЕП

ПІБ:

Дата:

Таблиця 1. Інформація про обов'язкові освітні компоненти ОП

Назва освітнього компонента	Вид компонента	Силабус або інші навчально-методичні матеріали		Якщо освітній компонент потребує спеціального матеріально-технічного та/або інформаційного забезпечення, наведіть відомості щодо нього*
		Назва файла	Хеш файла	
Кваліфікаційна робота бакалавра	підсумкова атестація	*ОК30.pdf*	oqeEnnnzrAGU6/yGFe5YqwANQJ0XUspcr9KSDwlqXQU=	*Спеціального МТЗ не потребує*
Науково-дослідна практика	практика	*ОК22.pdf*	qK3ABQKoniEtffg4ZISD4icMLY6QmLMZw52SP3xSTus=	*Спеціального МТЗ не потребує*
Проектно-технологічна практика	практика	*ОК21.pdf*	QyASDtJeFJQRpNeSBz4SIOf6LyLCoMYUbgSZyobIeGQ=	*Спеціального МТЗ не потребує*
Інформаційні технології в кіберпросторі	навчальна дисципліна	*ОК5.pdf*	hKeHzfso6F+uzxR4FmLPqGI9nIVqYC1ZQMtTgip8scw=	*Спеціального МТЗ не потребує*
Іноземна мова	навчальна дисципліна	*ОК23.pdf*	YstQ28zwyJpsXiVE8FL8M4wwcZuF97tqP6xbf/Zw65A=	*Спеціального МТЗ не потребує*
Філософія	навчальна дисципліна	*ОК3.pdf*	9Q/V1C+bdWhq/g7vy1rexKGGibpbv6Y73KzCihnrV4E=	*Спеціального МТЗ не потребує*
Українська та зарубіжна культура	навчальна дисципліна	*ОК2.pdf*	5PGUFQ71tikX2yfyE1VuIOPPweMp3Wqmoqgc9c/q+nQ=	*Спеціального МТЗ не потребує*
Комплексні системи захисту інформації	навчальна дисципліна	*ОК16.pdf*	uqyfP5ueiuhrHKoPkJlFJWlcJeUDmPJ6d6Lhs9cif4g=	*Програмно-апартний комплекс DigiScan. Скануючий приймач AOR8200*
Спеціальні математичні методи в інформаційній та кібербезпеці	навчальна дисципліна	*ОК4.pdf*	Uu17cMrIsfjJfZVLoju6QNsJQD9V/aZiSXSMya445sc=	*Спеціального МТЗ не потребує*
Соціально-політичні студії	навчальна дисципліна	*ОК31.pdf*	QDYVFKEsAwQhLA1OaJ8NH2kVYTV8SpvFZb15vpiKwA8=	*Спеціального МТЗ не потребує*
Захист інформації в інформаційних системах та мережах	навчальна дисципліна	*ОК19.pdf*	u0HEv33YZmbbNQe3Fn7FUkx6ddrwzYjk4a/4T+NqGuk=	*ауд. 204, 205; Virtual Box, Microsoft Teams, C/C++, RangeForce. Python, Go.*
Безпека банківських технологій	навчальна дисципліна	*ОК29.pdf*	W4v/rZeL/rned+DJzslvBClQBywhlC9sMQhFmT6DdZk=	*TrendMicro Smart Protection, IBM QRadar, Forescout CounterACT*
Криптографічні системи захисту інформації	навчальна дисципліна	*ОК15.pdf*	1HNOW5U378W92grlptHPIqbd56Tm/Xd5gW1nGl+L+oY=	*Спеціального МТЗ не потребує*
Теорія інформації та кодування	навчальна дисципліна	*ОК14.pdf*	yvzJE35YwxnRLs1LAqkOPXLQZUUSTW/EiaNW4zKal0s=	*Спеціального МТЗ не потребує*
Інформаційні системи та мережі	навчальна дисципліна	*ОК13.pdf*	lPS1PXssJZlWZxdVzIz+7BrrFodoaTX10GQP00NMCUo=	*ауд. 204, 205 – Virtual Box, Microsoft Teams, C/C++, RangeForce. Python, Go*
Комп'ютерна графіка та мультимедійні технології	навчальна дисципліна	*ОК26.pdf*	guB855qobfb78ZQ3ANRpNaAXkyvm+QXu8FyLmxFuLzs=	*Спеціального МТЗ не потребує*
Науковий образ світу	навчальна дисципліна	*ОК25.pdf*	Ddyy6y+AF6g5d52uTgGM346K+UrAohkEvH/q4Yuo1tg=	*Спеціального МТЗ не потребує*

Вступ до університетських студій	навчальна дисципліна	*ОК1.pdf*	cgMW5NPQGxplRtVo8qU6Y1PPmiMHgODDfITVfDXYQHk=	*Спеціального МТЗ не потребує*
Фізика	навчальна дисципліна	*ОК6.pdf*	VBStRFEZazZ7HqyNsvsj6WK9Ys5UVV/WNuCP1ue79gc=	*Спеціального МТЗ не потребує*
Національна та інформаційна безпека держави	навчальна дисципліна	*ОК7.pdf*	23u/LiE0EfkO4JO3Yh593TGIAy6xWD1Wn0IHVRJUCK8=	*Спеціального МТЗ не потребує*
Кіберпростір та протидія кіберзлочинності	навчальна дисципліна	*ОК20.pdf*	c3TWCnu4C3xqSzldteXFYPLDw5ERiUvm4fPHBF5wsV8=	*Спеціального МТЗ не потребує*
Основи алгоритмізації та програмування	навчальна дисципліна	*ОК27.pdf*	WpFj7p6EtoztxDz8q4JVvOsjrTDpyHusTHfElbRzc4M=	*ауд. 204, 205 – Intel Core I5; 3,2 GHz; ОЗУ 8 GB, HDD 1TB; ауд. 205, інтернет 10 Мбіт/сек на ПК; ОС Windows 10, Microsoft 365, Microsoft Teams, Microsoft Visual Studio 2019 C++.*
Вступ до кібернетичної безпеки	навчальна дисципліна	*ОК28.pdf*	xsYlDdrkFg5L3O1rQCs5yHsHES9yEWSItSJpTMwaulE=	*Спеціального МТЗ не потребує*
Вибрані розділи трудового права і основ підприємницької діяльності	навчальна дисципліна	*ОК17.pdf*	hyupTTpL2l96Czg0QO786/p/2Xdm8eXgZnqHPU0Pk6A=	*Спеціального МТЗ не потребує*
Основи екології	навчальна дисципліна	*ОК33.pdf*	UW5XsqUHPFHaP67QyX/WUcea1PT4U6hP8cVYS2tdP+c=	*Спеціального МТЗ не потребує*
Операційні системи та їх захист	навчальна дисципліна	*ОК8.pdf*	RVU3HGwGLi6f+fD6PDnyW4WdGSDgjVyXNIOzfo4VHoY=	*ауд. 204, 205 – віртуальне середовище типу VMWare, Oracle VirtualBox, ОС Linux.*
Технології програмування захищених систем	навчальна дисципліна	*ОК9.pdf*	O1Oqm92a3aHPbPWgKojUbKChEYA3VfUbL09ec22bhrI=	*ауд. 204, 205 – Microsoft 365, Microsoft Teams, Microsoft Visual Studio 2019, C++, RangeForce.*
Сигнали та процеси в системах технічного захисту інформації	навчальна дисципліна	*ОК10.pdf*	2aAEpRhyQ45DlytoG32h9N2bb/I4EKwLV9gL43+i7tk=	*ауд. 204, 205 – Microsoft 365, доступ до сервісу www.falstad.com/circuit/*
Електроніка та мікросхемотехніка	навчальна дисципліна	*ОК11.pdf*	paDdcSOOvV1sSLfrQ4rwc7rd+AwJ9TFbZeaqRSxuUlI=	*ауд. 204, 205 – Microsoft 365, доступ до сервісу www.falstad.com/circuit/*
Архітектура комп'ютерних систем	навчальна дисципліна	*ОК12.pdf*	+FE7SzeDZGSdCwx1Co8iNfAe7jQ1tDdYQcRq/zBvYkI=	*ауд. 204, 205 – Програми для тестування компонентів ПК: Aida 64, CPUZ, OCCP; MemTest, Victoria HDD/SSD, HDD Scan. Обладнання для вимірювання напруги Мультиметр – вольтметр для вимірювання постійної напруги.*
Управління інформаційною безпекою	навчальна дисципліна	*ОК18.pdf*	lF0pftQ/oukqGwA68JwpjKrsjaBoAtuhn5V60Cm9bRQ=	*Програмний комплекс SearchInform, SIEM IBM QRadar, Trend Micro Apex One, Wallix Bastion.*
Математичні основи в інформаційній та кібербезпеці	навчальна дисципліна	*ОК24.pdf*	/Id2RPgWgaC7luG+N5zCoF3BDteLOwcl2WPzTTEVohM=	*Спеціального МТЗ не потребує*

* наводяться відомості, як мінімум, щодо наявності відповідного матеріально-технічного забезпечення, його достатності для реалізації ОП; для обладнання/устаткування – також кількість, рік введення в експлуатацію, рік останнього ремонту; для програмного забезпечення – також кількість ліцензій та версія програмного забезпечення

Таблиця 2. Зведена інформація про викладачів ОП

ID викладача	ПІБ	Посада	Структурний підрозділ	Кваліфікація викладача	Стаж	Навчальні дисципліни, що їх викладає викладач на ОП	Обґрунтування
289511	Левінець Руслан Петрович	Асистент, Основне місце роботи	Історичний факультет	Диплом кандидата наук ДК 029024, виданий 11.05.2005	7	Вступ до університетських студій	Освіта та науковий ступінь відповідають тематиці дисципліни. Викладач є асистентом кафедри новітньої історії України Історичного факультету Київського національного університету імені Тараса Шевченка. Автор дисертаційного дослідження на тему: «Життєвий шлях та науково громадська діяльність В.Я.Шульгіна (1821-1878 рр.)», присвяченого в.о. екстраординарного професора кафедри всесвітньої історії університету Св. Володимира Шульгіну Віталію Яковичу
400478	Коренєва Наталя Олексіївна	Доцент, Основне місце роботи	Економічний факультет	Диплом бакалавра, Академія муніципального управління, рік закінчення: 2001, спеціальність: 0501 Економіка і підприємництво, Диплом магістра, Київський національний університет імені Тараса Шевченка, рік закінчення: 2003, спеціальність: 050106 Облік і аудит, Диплом кандидата наук ДК 050299, виданий 28.04.2009, Атестат доцента 12ДЦ 039196, виданий 26.06.2014	8	Вибрані розділи трудового права і основ підприємницької діяльності	Освіта та науковий ступінь відповідають тематиці дисципліни, наукова робота пов'язана з тематикою дисципліни. Член постійних спеціалізованих вчених рад Д26.001.23 при Київському національному університеті імені Тараса Шевченка та Д26.159.01 при Інституті фізики НАН України. Науковий керівник держбуджетної теми 19БФ051-05 (2019-2021); член редакційної колегії з фізики твердого тіла журнала Open Physics De Gruyter, Springer (2007-2017) 2018 рецензент журналів: APS (Physical Review B та Physical Review Letters), AIP (Applied Physics Letters, Journal of Applied Physics, Review of Scientific Instruments), IOP (Nanotechnology, Journal of Physics D, Semiconductor Science and Technology), Physica B, Nanoscale Research Letters, PLOS ONE, Optical Materials, Journal of Industrial and Engineering Chemistry. Публікації за тематикою

							дисципліни: 1. Подолян А.О., Коротченков О.О. Фізика низькорозмірних напівпровідників. Генерація та рекомбінація нерівноважних носіїв заряду. Фотоелектричний ефект // Вінниця: ТОВ “Твори”, 2018 (4 друк. арк.); Напівпровідникові гетероструктури та нанокомпозити на основі кремнію та оксиду цинку: сонохімічний синтез та фізичні властивості. Наукова монографія / О.О. Коротченков, А.Б. Надточій, М.І. Закіров, М.В. Ісаєв, А.Г. Кузьмич, М.О. Боровий – Київ–Вінниця: ТОВ “Твори”, 2018. – 218 с. ISBN 978-617-7706-25-9. 2. Enhancing the Seebeck effect in Ge/Si through the combination of interfacial design features / A. Nadtochiy, V. Kuryliuk, V. Strelchuk, O. Korotchenkov, P.-W. Li, S.-W. Lee // Scientific Reports. – 2019. – Vol. 9, doi.org/10.1038/s41598-019-52654-z; 3. Enhanced terahertz conductivity in ultra-thin gold film deposited onto (3-mercaptopropyl) trimethoxysilane (MPTMS)-coated Si substrates / Y. Lee, D. Kim, J. Jeong, J. Kim, V. Shmid, O. Korotchenkov, P. Vasa, Y.-M. Bahk, D.-S. Kim // Scientific Reports. – 2019. – Vol. 9, article 15025 (7 pp.); 4. Sonochemical modification of SiGe layers for photovoltaic applications / A. Nadtochiy, O. Korotchenkov, V. Schlosser // Physica Status Solidi (a). – 2019. – Vol. 216, Issue 17, article 1900154 (9 pp.); 5. Improving photoelectric energy conversion by structuring Si surfaces with Ge quantum dots / V. Shmid, V. Kuryliuk, A. Nadtochiy, O. Korotchenkov, P.-W. Li // Proceedings of the

							2019 IEEE 39th International Conference on Electronics and Nanotechnology, ELNANO. – 2019. – P. 92–96; 6. Epoxy filled with bare and oxidized multi-layered graphene nanoplatelets: a comparative study of filler loading impact on thermal properties / B. Gorelov, A. Gorb, A. Nadtochiy, D. Starokadomsky, V. Kuryliuk, N. Sigareva, S. Shulga, V. Ogenko, O. Korotchenkov, O. Polovina // Journal of Material Science. – 2019. – Vol. 54, Issue 12, P. 9247–9266; 7. Charge-carrier relaxation in sonochemically fabricated dendronized CaSiO3–SiO2–Si nanoheterostructures / R. Savkina, A. Smirnov, S. Kirilova, V. Shmid, A. Podolian, A. Nadtochiy, V. Odarych, O. Korotchenkov // Applied Nanoscience. – 2019. – Vol. 9, Issue 5, P. 1047-1056; 8. Фотоелектричні властивості плівок SiGe, покритих шарами аморфного та полікристалічного кремнію / V. Shmid, A. Podolian, A. Nadtochiy, O. Korotchenkov, B. Romanyuk, V. Melnik, V. Popov, O. Kosulya // Укр. фіз. журн. – 2019. – т. 64, №5, С. 413–422; 9. Enhanced photoresponse of Ge/Si nanostructures by combining amorphous silicon deposition and annealing/ R. Savkina, A. Smirnov, S. Kirilova, V. Shmid, A. Podolian, A. Nadtochiy, V. Odarych, O. Korotchenkov // Applied Nanoscience. – 2019. – Vol. 9, Issue 5, P. 1047-1056; 10. A simple sonochemical synthesis of nanosized ZnO from zinc acetate and sodium hydroxide / M.I. Zakirov, M.P. Semen'ko, O.A. Korotchenkov // Journal of Applied Physics – 2018. – Vol. 124, Issue 9, P. 095703 (7 pp) 11. Фото-електричні властивості кремнієвих структур із нанокомпозитним

							епоксидно-полімерним шаром / В.І. Шмід, С.П. Назаров, А.О. Подолян, А.Б. Надточій, О.О. Коротченков // Ж. нано- електрон. фіз.– 2018. – т. 10, №2, С. 02024 (6 с.)
337194	Мирутенко Лариса Вікторівна	доцент, Основне місце роботи	Факультет інформаційних технологій	Диплом спеціаліста, Сумський державний педагогісний інститут імені А.С. Макаренка, рік закінчення: 1999, спеціальність: , Диплом кандидата наук ДК 043333, виданий 26.06.2017, Атестат доцента АД 006549, виданий 07.12.2020	17	Інформаційні технології в кіберпросторі	Освіта та науковий ступінь відповідають тематиці дисципліни. Відомості про підвищення кваліфікації: 1. Повний курс навчання по роботі з обладнанням для модернізації Комплексу прийому та обробки інформації з телефонних мереж зв'язку «Курс-6», ТОВ Криптон-М, сертифікат №54-2018, 31 жовтня 2018 р. 2. Стажування на кафедрі комп'ютеризованих систем захисту інформації Навчально-наукового інституту комп'ютерних інформаційних технологій Національного авіаційного університету, довідка від 20.12.2018 № 0302/4075. 3. Certificate of completion Cyber-Physical System Security within the 2021 Cybersecuriti Summer Training Program under the USAID Project. 14 june - 23 july 2021. Публікації за тематикою дисципліни: 1. Yuliia STEPANENKO, Valeriia SOLODOVNIK, Andriy FESENKO, Larysa MYRYTENKO SECURE PASSWORD STORAGE WITH CRYPTOGRAPHIC HASH FUNCTION / XII International conference of students, phd-students and young scientists "Engineer of XXI century", Bielsko-Biała, Poland, 2021. 2. Hnatiienko, H., Kiktev, N., Babenko, T.,Desiatko, A., Myrutenko, L./ Prioritizing Cybersecurity Measures with Decision Support Methods Using Incomplete Data

							//CEUR Workshop Proceedings,2021, 3241, pp. 169–180 (SCOPUS) 3. Shestak Y., Valeriia SOLODOVNIK., Myrutenko L. ALGORITHM OF LOAD BALANCE OPTIMIZATION ON HARDWARE RESOURCES OF INFORMATION SYSTEMS. Projekt interdyscyplinarny projektem XXI wieku. Bielsko-Biala: Wydawnictwo Naukowe Akademii Techniczno – Humanistycznej w Bielsku-Bialej, 2020. P. 193-198 4. V. Grechko, T. Babenko, і L. Myrutenko, «БЕЗПЕЧНЕ ПРОГРАМНЕ ЗАБЕЗПЕЧЕННЯ, ЩО РОЗРОБЛЯЄ РЕКОМЕНДАЦІЇ», Кібербезпека: освіта, наука, техніка, вип. 2, вип. 6, с. 82-93, Груд 2019. 5. Мирутенко Л. В. Система оцінки якості дистанційної освіти в Україні: основні проблеми і задачі / Лариса Вікторівна Мирутенко. // Системи обробки інформації : збірник наукових праць. – Х.: Харківський університет Повітряних Сил імені Івана Кожедуба, 2016. – Вип. 3(140). – С. 260 – 263
369164	Козуб Любов Степанівна	Доцент, Основне місце роботи	Навчально-науковий інститут філології	Диплом спеціаліста, Тернопільський державний педагогічний університет імені В.Гнатюка, рік закінчення: 1999, спеціальність: , Диплом кандидата наук ДК 031169, виданий 15.12.2005, Атестат доцента 12ДЦ 022699, виданий 21.05.2009	20	Іноземна мова	Освіта та науковий ступінь відповідають тематиці дисципліни, наукова робота пов'язана з тематикою дисципліни. Робоча програма навчальної дисципліни «Іноземна мова (англійська)» для студентів 1-4 курсів, галузь знань 12 «Інформаційні технології», спеціальність 125 «Кібербезпека», освітня програма «Кібербезпека», освітній рівень: бакалавр (17 кредитів). Навчальний рік 2022-2025. Публікації за тематикою дисципліни: 1. Козуб Л.С. (2018). Лексико-стилістичні засоби передачі чужого мовлення в електронних засобах масової інформації.

							Актуальні питання гуманітарних наук: зб наук. пр Дрогобицького державного педагогічного університету імені І. Франка. Дрогобич: Вид. дім Гельветика. Вип. 20. 78-81. 2. Козуб Л.С. (2018). Роль інтонації в змістовій структурі інформаційного тексту. Матеріали круглого столу «Сучасні тенденції фонетичних досліджень» (26-27 квітня). Київ: Нац. тех. ун-т України «КПІ ім. І. Сікорського». С. 91-93. 3. Козуб Л.С. (2019). The role of prosodic means in realizing the pragmatic effect / Роль просодичних засобів у реалізації прагматичного ефекту. «Міжнародний філологічний часопис». Vol. 10, № 2. P. 45-50.Козуб Л.С. (2019). Специфіка прагматичного спрямування емотивних текстів. Міжнародний філологічний часопис». Vol. 10, № 3. P. 26-31. 4. Kozub L., Valigura O., Monashnenko A. (2020). Prosody of English Television Advertising: Sociolinguistic Features And Pragmatic Potential / Просодія англомовної телевізійної реклами: соціолінгвістичні особливості та прагматичний потенціал. Euromentor Journal Studies About Education. Volume XI, № 1. Bucuresti: Pro Universitaria, P. 13-38. 5. Kozub L., Valigura O., Sieriakova I. (2020). Computer Technologies in Acoustic Analysis of English Television Advertising / Комп'ютерні технології в акустичному аналізі англомовної телевізійної реклами. Arab World English Journal. Special Issue on Call (6). 38-48. DOI: https://dx.doi.org/10.24093/awej/call6.3 6. Kozub L., Valigura O., Parashchuk V. (2020). Phonetic Portrait of an English-

							Ukrainian Bilingual: Prosodic Parameters in Academic Discourse / Фонетичний портрет англо-українського білінгва: просодичні параметри академічному дискурсі. Arab World English Journal (AWEJ). Special Issue on the English Language in Ukrainian Context. 16-25. DOI: https://dx.doi.org/10.24093/awej/elt3.2 7. Kozub L. (2021). Online Learning Resources and Tools in Interactive EFL Teaching / Онлайн-ресурси та інструменти в інтерактивному навчанні англійської як іноземної мови. XIII International Scientific and Practical Conference "Development of Modern Science: Theory, Methology, Practice" (March, 18-19). Madrid, Spain. 175-176. 8. Kozub L. (2021). Political Correctness in Modern English Media / Політична коректність в сучасних англомовних засобах масової інформації. XXVI International Scientific and Practical Conference "Topical Issues of Practice and Science" (May, 18-21). London, Great Britain. 556-557. 9. Kozub L., Pylypenko O. (2021). Foreign Language Teaching of Ukrainian University Students in a Distance Learning Environment / Викладання іноземної мови студентам українських університетів у середовищі дистанційного навчання. Arab World English Journal (AWEJ) Volume 12(3). 375-384 DOI:https://dx.doi.org/10.24093/awej/vol12no3.26 10. Computer Technologies in Acoustic Analysis of English Television Advertising (Web of Science, Texas, Malaysia) 11. Phonetic Portrait of an English-Ukrainian Bilingual: Prosodic Parameters in Academic Discourse (Web of Science, Texas,

							Malaysia) 12. Foreign Language Teaching of Ukrainian University Students in a Distance Learning Environment (Web of Science, Texas, Malaysia) 13. Kozub L., Stepanechko O. (2022). Effectiveness of the Inquiry-Based Method in English Language Teaching of Ukrainian University Students Through Technology-Enabled Learning. Arab World English Journal, 13 (3). 2022. 368- 377. 14. DOI: https://dx.doi.org/10.24093/awej/vol13no3.24
26046	Комар Олена Вікторівна	доцент, Основне місце роботи	Філософський факультет	Диплом спеціаліста, Київський національний університет імені Тараса Шевченка, рік закінчення: 2000, спеціальність: 030101 Філософія, Диплом кандидата наук ДК 027482, виданий 09.02.2005, Атестат доцента 12ДЦ 022857, виданий 22.12.2009	21	Філософія	Освіта та науковий ступінь відповідають тематиці дисципліни, наукова робота пов'язана з тематикою дисципліни. Публікації за тематикою дисципліни: 1. Філософія: хрестоматія для бакалаврів фіз-мат. і природн. спеціальностей. У 2 т. Т.1. Філософська пропедевтика / авт.-упоряд. І.С. Добронравова, О.В. Руденко, О.В.Комар та ін.; заг. ред. І.С. Добронравової, О.В. Руденко. – 2-ге вид., доп. – К.: ВПЦ «Київський університет», 2020.- 879 с. 2. Філософія: хрестоматія для бакалаврів фіз-мат. і природн. спеціальностей. У 2 т. Т. 2. Теоретична та практична філософія / авт.-упоряд. І.С. Добронравова, О.В. Руденко, О.В.Комар та ін.; заг. ред. І.С. Добронравової, О.В. Руденко. – 2-ге вид., доп. – К.: ВПЦ «Київський університет», 2020.- 543 с. 3. Методологія та організація наукових досліджень : навч. посіб. для студ.-магістр. усіх спец. / за ред. І.С.Добронравової (ч. 1), О.В.Руденко (ч. 2). - К. : ВПЦ "Київський університет", 2018. - 607 с. (С. 80-119, С 149-156, С. 240-254, С. 409-445.).

							4. Філософія науки: підручник. / за ред. І.С. Добронравової. – К.: ВПЦ «Київський університет», 2018. – 255 с. (З Добронравова І.С., Сидоренко Л.І., Комар О.В. та ін.). Розділ 7.1-7.3. 5. Новітня філософія науки: підруч. для студ. філос. ф-тів і аспірантів 6. І.С. Добронравова, Т.М. Білоус, О.В. Комар - К.: Логос, 2009. 7. Новітня західна філософія науки. Підручник. 8. І.С. Добронравова, Т.М. Білоус, О.В. Комар - К.: Вид. ПАРАПАН, 2008. 9. Добронравова І., Горбунова Л., Комар О. Освіта для майбутнього: роздуми над ювілейною доповіддю Римського клубу / Філософія освіти. № 4, 2018. С. 70-99. 10. В. Кебуладзе, О. Комар, А. Леонов Переклад як (не)порозуміння. Термінологічна дискусія. What is it like to be a zombie? / Філософська думка. – № 1, 2016. – С. 83-111 11. Комар О. Постнекласична епістемологія: нові тенденції// Людина в складному світі / Збірка наукових праць Суми: Університетська книга, 2017. – С. 238-248. 12. Комар О. Тесеєві мандри свідомості Філософська думка. – № 2, 2016. – С. 57-70. 13. Komar O. Neuroethics in Philosophy and Science // The Days of Science of the Faculty of Philosophy – 2019. International Scientific Conference, April 23-24, 2019. Kyiv: Publishing center “Kyiv University”, 2019. – P. 51-52. 14. Комар О. Нейроетика та елліністичні філософські рецепти щастя / Щастя та сучасне суспільство: збірник матеріалів міжнародної наукової конференції. - Львів: Сполом, 2021. - С. 153-1157. 15. Комар О. Графемно-колірна синестезія:

							нейрологічний палімпсест чи когнітивна метафоризація? Матеріали XVI Міжнародної науково-практичної конференції "Психолінгвістика в сучасному світі - 2021" (Переяслав, 16-17 грудня, 2021 р.). Том 16 (2021). Стажування та сертифікати про підвищення кваліфікації: 1. Наукове стажування у Бібліотеці імені М. Максимовича (лютий – травень 2021). 2. Сертифікат про завершення курсу підвищення кваліфікації та розвитку компетентностей викладачів KNU TEACH WEEK, 01.03.2021. 3. Сертифікат про завершення курсу «Зміцнення викладання та організаційного управління в університетах», платформа Prometheus, 23.04.2021. 4. Сертифікат про завершення курсу «English for Career /Англійська для кар'єрного зростання», університет Пенсильванії, платформа Prometheus, 03.05.2021.
95218	Бежнар Ганна Петрівна	доцент, Основне місце роботи	Філософський факультет	Диплом спеціаліста, Київський національний університет імені Тараса Шевченка, рік закінчення: 2001, спеціальність: 040301 Політологія, Диплом кандидата наук ДК 028438, виданий 13.04.2005	15	Українська та зарубіжна культура	Освіта та науковий ступінь відповідають тематиці дисципліни, наукова робота пов'язана з тематикою дисципліни. 1. Візуальні дослідження в контексті теорії та історії культури: навч. посіб. / І. І. Маслікова, О. Ю. Павлова, А. М. Тормахова та ін.; заг. ред. В. І. Панченко. К. : ВПЦ "Київський університет", 2021. С. 410-418. 2. Українська та зарубіжна культура: навчально-методичний комплекс для студентів ННЦ «Інститут біології та медицини». К.: Оперативна дільниця філософського факультету КНУ імені Тараса Шевченка, 2020. 44 с.

							3. Теорія масової культури: навчально-методичний комплекс для студентів спеціальності «культурологія». К.: Оперативна дільниця філософського факультету КНУ імені Тараса Шевченка, 2020. 40 с. 4. Теорія масової культури: курс лекцій Навчальний посібник [електронне видання]. К. 2020. Режим доступу: http://philosophy.univ.kiev.ua/uploads/editor/Files/Kafedry/Ukrainian_philosophy/МК_Бежнар.pdf Публікації за тематикою дисципліни: 1. Ensuring the on the beginning metaphilosophy: «Antique Project». Laplage in Journal, 7(Extra-A), 2021. p.19-25. (Omelchenko, V. ., Semykras, V. ., Turenko, V. ., Zarytska, O.)
402049	Лаптєв Олександр Анатолійович	доцент, Основне місце роботи	Факультет інформаційних технологій	Диплом доктора наук ДД 010230, виданий 24.09.2020, Диплом кандидата наук ДК 013189, виданий 13.02.2002, Атестат старшого наукового співробітника (старшого дослідника) АС 004851, виданий 15.12.2005	41	Комплексні системи захисту інформації	Освіта та науковий ступінь відповідають тематиці дисципліни, наукова робота пов'язана з тематикою дисципліни. Керівник науково дослідної роботи Київського національного університету імені Тараса Шевченка: «Методи та засоби виявлення несанкціонованого розповсюдження інформації в умовах інформаційного протиборства». РН 0121U113291 від 12.10.2021 (10.2021-10.2025) Відомості про підвищення кваліфікації: Міністерство освіти і науки України. Державний університет телекомунікацій. Тема: Системи технічного захисту інформації. Навчальний час 120 годин, чотири кредита ЄКТS. Сертифікат про підвищення кваліфікації № СТ 38855349/081-19 від 26.04.2019. Міністерство освіти і науки України. Волинський національний університет Лесі

							Українки, кафедра загальної математики та методики навчання інформатики. Сертифікат про підвищення кваліфікації № 176/21 серія н/с. Науково-практичний семінар "Інформаційні технології в науці та освіті". Загальна кількість годин - 108. Certificate of completion Audit and Risk Management within the 2021 Cybersecuriti Summer Training Program under the USAID Project. 14 june - 23 july. Навчання на курсах "Advanced Malware" within the 2022 Cybersecurity Summer Instructor Training Program under the USAID Cybersecurity for Critical Infrastructure in Ukraine Activity. 11 July – 31 August 2022. Наявність виданого підручника чи навчального посібника (включаючи електронні) або монографії (загальним обсягом не менше 5 авторських аркушів), в тому числі видані у співавторстві (обсягом не менше 1,5 авторського аркуша на кожного співавтора). 1.Лаптєв О.А. Методологічні основи автоматизованого пошуку цифрових засобів негласного отримання інформації. – К. Міленіум. 2020 – 326 с. УДК 004.056.53. ISBN 987-966-8063-79-3. http://www.library.hneu.edu.ua/new_books/28; http://www.dut.edu.ua/ru/lib/1/category/96/view/2162 2. Serhii Yevseiev, Volodymir Ponomarenko, Oleksandr Laptiev, Oleksandr Milov and others/ Synergy of building cybersecurity systems. Kharkiv. Publisher PC TECHNOLOGY CENTER. 2021 – 188 с. 18,8 ум.друк.арк./власний внесок 3,3 авторських аркушів. ISBN 978-617-7319-31-2 (on-line). ISBN 978-

							617-7319-32-9 (print). DOI: https://doi.org/10.15587/978-617-7319-31-2 https://monograph.com.ua/pctc/catalog/book/64 3. Лаптєв О.А., Кузавков В.В., Хорошко В.О. «Системи пошуку засобів негласного здобуття акустичної інформації» – К. Міленіум. 2023 – 282 с. Підручник. https://www.researchgate.net/publication/368925556_SISTEMI_POSUKU_ZASOBIV_NEGLASNOGO_ZDOBUTTA_AKUSTICNOI_INFORMACII 4.О.А.Лаптєв, В.В.Собчук, О.М. Станжицький, Н.В Лукова-Чуйко. A comprehensive method of evaluating the effectiveness of the distance learning system in higher education institutions. In book : education, science, research during martial law. Collective monograph. Riga, Latvia : «Baltija Publishing», November 14, 2022. 374 p. (pp.209-231). DOI: https://doi.org/10.30525/978-9934-26-247-0-9 http://www.baltijapublishing.lv/omp/index.php/bp/catalog/book/261/7247/15075-1 Публікації за тематикою дисципліни: 1. Laptiev Oleksandr, Shuklin German, Savchenko Vitalii, Barabash Oleg, MusienkoAndrii and Haidur Halyna, The Method of Hidden Transmitters Detection based on the Differential Transformation Model. International Journal of Advanced Trends in Computer Science and Engineering (IJATCSE) Volume 8 No. 6 .November - December 2019. Scopus Indexed - ISSN 2278 – 3091. pp.2840 – 2846. DOI: 10.30534/ijatcse/2019/26862019. 0,8 ум.друк.арк./власний внесок 0,17 авторських аркушів, 2. Lubov Berkman, Oleg Barabash, Olga Tkachenko , Andri Musienko, Oleksand Laptiev, Ivanna Salanda. The Intelligent

							Control System for infocommunication networks. International Journal of Emerging Trends in Engineering Research (IJETER) Volume 8. No. 5, May 2020. Scopus Indexed - ISSN 2347 – 3983. P.1920 – 1925. DOI:10.30534/ijeter/2020/73852020. 0,6 ум.друк.арк./власний внесок 0,13 авторських аркушів, 3. Vitalii Savchenko, Oleh Ilin, Nikolay Hnidenko, Olga Tkachenko, Oleksander Laptiev, Svitlana Lehominova, Detection of Slow DDoS Attacks based on User's Behavior Forecasting. International Journal of Emerging Trends in Engineering Research (IJETER) Volume 8. No. 5, May 2020. Scopus Indexed - ISSN 2347 – 3983. P.2019 – 2025. DOI:10.30534/ijeter/2020/90852020. 0,6 ум.друк.арк./власний внесок 0,15 авторських аркушів, 4. Barabash Oleg, Laptiev Oleksand, Tkachev Volodymyr, Maystrov Oleksii, Krasikov Oleksandr, Polovinkin Igor. The Indirect method of obtaining Estimates of the Parameters of Radio Signals of covert means of obtaining Information. International Journal of Innovative Technology and Exploring Engineering (IJITEE), Volume 8. No. 8, August 2020.Scopus Indexed- ISSN: 2278–3075. P4133 – 4139. DOI:10.30534/ijeter/2020/73852020. 0,6 ум.друк.арк./власний внесок 0,15 авторських аркушів, 5. Serhii Yevseiev, Roman Korolyov, Andrii Tkachov, Oleksandr Laptiev, Ivan Opirskyy, Olha Soloviova. Modification of the algorithm (OFM) S-box, which provides increasing crypto resistance in the post-quantum period. International Journal of Advanced Trends in Computer Science and Engineering (IJATCSE) Volume 9. No. 5, September-Oktober 2020. pp. 8725-8729 Scopus. DOI:

							10.30534/ijatcse/2020/261952020. 0,8 ум.друк.арк./власний внесок 0,15 авторських аркушів, 6. Oleg Barabash, Oleksandr Laptiev, Oksana Kovtun, Olga Leshchenko, Kseniia Dukhnovska, Anatoliy Biehun. The Method dynavic TF-IDF. International Journal of Emerging Trends in Engineering Research (IJETER), Volume 8. No. 9, September 2020. pp 5712-5718. Scopus. DOI:10.30534/ijeter/2020/130892020. 0,6 ум.друк.арк./власний внесок 0,157 авторських аркушів, 7. Serhii Yevseiev, Oleksandr Laptiev, Sergii Lazarenko, Anna Korchenko, Iryna Manzhul. Modeling the protection of personal data from trust and the amount of information on social networks. Number 1 (2021), «EUREKA: Physics and Engineering» pp.24–31. Scopus. DOI:10.21303/2461-4262.2021.001615. 0,7 ум.друк.арк./власний внесок 0,2 авторських аркушів, 8. Korchenko A.O., Breslavskyi V.O., Yevseiev S.P, Zhumangalieva N.K., Zvarych A.O., Kazmirchuk S.V., Kurchenko O.A., Laptiev O.A., Severinov O. V.,. Tkachuk S. S. Development of a method for construction of linguistic standards for multicriterial evaluation of HONEYPOT efficiency. Eastern-European journal of enterprise technologies. Vol.1№2 (109), 2021 pp. 14–23. ISSN (print)1729 - 3774. ISSN (on-line) 1729-4061. Scopus. DOI: 10.15587/1729-4061.2021.225346. 0,9 ум.друк.арк./власний внесок 0,15 авторських аркушів, 9. O.Svynchuk, O. Barabash, J.Nikodem, R. Kochan, O. Laptiev. Image compression using fractal functions. Fractal and Fractional, 2021, 5(2), 31.pp.1-14. DOI:10.3390/fractalfract5020031 - 14 Apr 2021. Web of Science Core Collection 1,4 ум.друк.арк./власний

							внесок 0,2 авторських аркушів, 10. Oleksandr Laptiev, Vitalii Savchenko, Andrii Pravdyvyi, Ivan Ablazov, Rostyslav Lisnevskyi, Oleksandr Kolos, Viktor Hudyma. Method of Detecting Radio Signals using Means of Covert by Obtaining Information on the basis of Random Signals Model. International Journal of Communication Networks and Information Security (IJCNIS), Vol. 13, No. 1, 2021. pp.48-54. Scopus. 0,7 ум.друк.арк./власний внесок 0,15 авторських аркушів, 11. Laptiev O., Savchenko V., Kotenko A., Akhramovych V., Samosyuk V., Shuklin G., Biehun A. Method of Determining Trust and Protection of Personal Data in Social Networks. International Journal of Communication Networks and Information Security (IJCNIS), Vol. 13, No. 1, 2021. pp.15-21. Scopus. https://www.researchgate.net/publication/349366774_Method_of_determining_the_protection_of_personal_data_from_trust_in_social_networks. 0,6 ум.друк.арк./власний внесок 0,15 авторських аркушів. 12. Zamrii I., Sobchuk V., Laptiev O., Savchenko V., Shkapa V., Kovalenko V. and Kotok V. Fractal Functions and Their Application to Source Data Coding. ARPN Journal of Engineering and Applied Sciences. Vol. 17, No. 4, 2022. pp. 424 – 435. Scopus. 13. Roman Kyrychok, Oleksandr Laptiev, Rostyslav Lisnevsky, Valeri Kozlovsky, Vitaliy Klobukov. Development of a method for checking vulnerabilities of a corporate network using bernstein transformations. Eastern-European journal of enterprise technologies. Vol.1№9 (115), 2022 pp. 93–101. ISSN (print)1729 - 3774. ISSN (on-line) 1729-4061. DOI: 10.15587/1729-4061.2022.253530.

							Scopus. 14. Volodymyr Petrivskyi, Viktor Shevchenko, Serhii Yevseiev, Oleksandr Milov,Oleksandr Laptiev,Oleksii Bychkov, Vitalii Fedoriienko, Maksim Tkachenko, Oleg Kurchenko, Ivan Opirsky. Development of a modification of the method for constructing energy-efficient sensor networks using static and dynamic sensors. Eastern-European journal of enterprise technologies. Vol.1№9 (115), 2022 pp. 15–23. ISSN (print) 1729 - 3774. ISSN (on-line) 1729-4061. DOI: 10.15587/1729-4061.2022.252988 Scopus. 15. Лукова-Чуйко Н.В., Лаптєв О.А., Барабаш О.В., Мусієнко А.П., Ахрамович В.М. Метод розрахунку захисту персональних даних з урахуванням комплексу специфічних параметрів соціальних мереж. Збірник наукових праць Військового інституту Київського національного університету імені Тараса Шевченка. Київ: ВІКНУ, 2022. № 76. С. 54 – 68. https://doi.org/10.17721/2519-481X/2022/76-05 16. Беркман Л.Н., Барабаш О.В., Ткаченко О.М., Мусієнко А.П., Лаптєв О.А., Свинчук О.В. Інтелектуальна система управління для інфокомунікаційних мереж. Системи управління навігації і зв'язку. Том 3. №69. 2022. С 54–59. https://doi.org/10.26906/SUNZ.2022.3 17. Лаптєв О.А., Бучик С.С., Савченко В.А., Наконечний В.С. , Михальчук І.І, Шестак Я.В., Виявлення та блокування повільних ddos-атак за допомогою прогнозування поведінки користувача. Наукоємні технології. Інформаційні технології, кібербезпека. Том 55 № 3 (2022) стр.184-

							192. DOI: 10.18372/2310-5461.55.16908 18. Serhii Yevseiev, Khazail Rzayev, Oleksandr Laptiev, Ruslan Hasanov, Oleksandr Milov, Bahar Asgarova, Jale Camalova, Serhii Pohasii. Development of a hardware cryptosystem based on a random number generator with two types of entropy sources. Eastern-European journal of enterprise technologies. Vol.5№9 (119), 2022 pp. 6–16. ISSN (print) 1729 - 3774. ISSN (on-line) 1729-4061. DOI: 10.15587/1729-4061.2022.265774 Scopus.
431509	Мусієнко Андрій Петрович	професор, Сумісництво	Факультет інформаційних технологій	Диплом спеціаліста, Державний університет телекомунікацій, рік закінчення: 2017, спеціальність: 7.05090302 телекомунікаційні системи та мережі, Диплом магістра, Волинський національний університет імені Лесі Українки, рік закінчення: 2008, спеціальність: 080101 Математика, Диплом доктора наук ДД 008556, виданий 23.04.2019, Диплом кандидата наук ДК 017621, виданий 21.11.2013, Атестат доцента АД 004997, виданий 02.07.2020	7	Спеціальні математичні методи в інформаційній та кібербезпеці	Освіта та науковий ступінь відповідають тематиці дисципліни. Публікації за тематикою дисципліни: 5. Musienko, A., Sobchuk, V., Barabash, O., Kopiika, O., Zamrii, I., (2019). Fraktal and differential properties of the inversor of digits of Qs-representation of real number.Understanding Complex Systems, 79–95. (Scopus). https://www.scopus.com/record/display.uri?eid=2-s2.0-85058941299&origin=resultslist&sort=plf-f 6. Musienko, A., Dakhno, N., Barabash, O., Shevchenko, H., Leshchenko, O., (2020). Modified Gradient Method for K-positive Operator Models for Unmanned Aerial Vehicle Control. 2020 IEEE 6th International Conference on Methods and Systems of Navigation and Motion Control, MSNMC 2020 - Proceedings, 81–84. (Scopus). https://www.scopus.com/record/display.uri?eid=2-s2.0-85097643340&origin=resultslist&sort=plf-f 7. Musienko, A., Sobchuk, V., Barabash, O., Tverdenko, H., Lukova-Chuiko, N. (2020). The Assessment of the Quality of Functional Stability of the Automated Control System with Hierarchic Structure. 2020 IEEE 2nd International

Conference on System Analysis and Intelligent Computing. (Scopus). https://www.scopus.com/record/display.uri?eid=2-s2.0-85097156326&origin=resultslist&sort=plf-f
8. Musienko, A., Barabash, O., Svynchuk, O., Sobchuk, V. (2021). Adaptive accumulation and diagnostic information systems of enterprises in energy and industry sectors. E3S Web of Conferences. (Scopus). https://www.scopus.com/record/display.uri?eid=2-s2.0-85104416246&origin=resultslist&sort=plf-f
9. Musienko, A., Sobchuk, V., Olimpiyeva, Y., Sobchuk, A. (2021). Ensuring the properties of functional stability of manufacturing processes based on the application of neural networks. CEUR Workshop Proceedings,106–116. (Scopus). https://www.scopus.com/record/display.uri?eid=2-s2.0-85104006288&origin=resultslist&sort=plf-f
10. Musienko, A., Barabash, O., Hohoniants, S., Rudenko, Y., Klochko, A. (2021). Comprehensive methods of evaluation of efficiency of distance learning system functioning. International Journal of Computer Network and Information Security, 13(1), 16–28. (Scopus). https://www.scopus.com/record/display.uri?eid=2-s2.0-85101294862&origin=resultslist&sort=plf-f
11. Musienko, A., Sobchuk, V., Barabash, O., Svynchuk, O. (2022). Adaptive accumulation and diagnostic information systems of enterprises in energy and industry sectors. E3S Web of Conferences. (Scopus). https://www.scopus.com/record/display.uri?eid=2-s2.0-85104416246&origin=resultslist&sort=plf-f
12. Musienko, A., Sobchuk, V., Barabash, O., Kozlovskyi, V., Shcheblanin, Y. (2022). Evaluation of efficiency of applications of

							functionally sustainable generealized information system of the enterprise. HORA 2022 - 4th International Congress on Human-Computer Interaction, Optimization and Robotic Applications, Proceedings. (Scopus). https://www.scopus.com/record/display.uri?eid=2-s2.0-85133966844&origin=resultslist&sort=plf-f&featureToggles=FEATURE_NEW_DOC_DETAILS_EXPORT:1,FEATURE_EXPORT_REDESIGN:0
337163	Телешун Ярослав Сергійович	асистент, Основне місце роботи	Філософський факультет	Диплом бакалавра, Київський національний університет імені Тараса Шевченка, рік закінчення: 2013, спеціальність: 040301 Політологія, Диплом магістра, Київський національний університет імені Тараса Шевченка, рік закінчення: 2015, спеціальність: 8.03010401 політологія, Диплом кандидата наук ДК 049769, виданий 18.12.2018	2	Соціально-політичні студії	Освіта та науковий ступінь відповідають тематиці дисципліни. Дисертація «Фінансово-політичні групи в нестабільному інституційному середовищі» на здобуття наукового ступеня кандидата політичних наук за спеціальністю 23.00.02 – політичні інститути і процеси була достроково захищена на спеціалізованій вченій раді 19 листопада 2018 р. Публікації за тематикою дисципліни: Телешун, Я. С. “ГЛОБАЛЬНА КОРУПЦІЯ” – ФЕНОМЕН XXI СТОЛІТТЯ. Вісник Харківського національного університету імені В.Н. Каразіна. Серія “Питання політології”; 38, 22-34. Відомості про підвищення кваліфікації: Диплом Аріельского університету в Самарії (Держава Ізраїль) про закінчення спецкурсу «Політична структура і публічне управління»(Political Structure and Public Administration). 2016 р.
101846	Бабенко Тетяна Василівна	професор, Основне місце роботи	Факультет інформаційних технологій	Диплом доктора наук ДД 007055, виданий 03.12.2008, Диплом кандидата наук КН 009601, виданий 21.12.1995, Атестат	30	Захист інформації в інформаційних системах та мережах	Освіта та науковий ступінь відповідають тематиці дисципліни, наукова робота пов'язана з тематикою дисципліни. Публікації за тематикою дисципліни: 1. Babenko, T.,Hnatiienko, H.,

				доцента ДЦ 000404, виданий 27.04.2000, Атестат професора 12ПР 008558, виданий 28.03.2013			Bigdan, A. /Model for determining the protection level of a complex system // CEUR Workshop Proceedings, 2022, 3132, pp. 156–165 (SCOPUS) 2. Hnatiienko, H., Kiktev, N., Babenko, T.,Desiatko, A., Myrutenko, L./ Prioritizing Cybersecurity Measures with Decision Support Methods Using Incomplete Data //CEUR Workshop Proceedings,2021, 3241, pp. 169–180 (SCOPUS) 3. Панченко М., Бігдан А., Бабенко Т., Тимофєєв Д. Виявлення аномалій інформаційної безпеки на основі аналізу ентропії інформаційної системи. Енергетика і автоматика. 2022. №1. С.72-81 4. Detection of sql injection attack using neural networks Hubskyi, O., Babenko, T., Myrutenko, L., Oksiiuk, O. Advances in Intelligent Systems and Computing, 2021, 1265 AISC, стр. 277–286. (SCOPUS) 5. Modeling of the integrated quality assessment system of the information security management system Babenko, T., Hnatiienko, H., Vialkova, V. CEUR Workshop Proceedings, 2021, 2845, стр. 75–84. 6. Modeling of critical nodes in complex poorly structured organizational systems Babenko, T., Hnatiienko, H., Ignisca, V., Iavich, M. CEUR Workshop Proceedings, 2021, 2915, стр. 92–101. 7. Determining key risks for modern distributed information systems Palko, D., Hnatienko, H., Babenko, T., Bigdan, A. CEUR Workshop Proceedings, 2021, 3018, стр. 81–100. 8. Babenko, T., Hnatiienko, H., Vialkova, V. Modeling of information security system and automated assessment of the integrated quality of the impact of controls on the functional stability of the organizational system // Selected

Papers of the XX International Scientific and Practical Conference "Information Technologies and Security" (ITS 2020), Kyiv, Ukraine, December 10, 2020 / CEUR Workshop Proceedings, 2021, 2859, pp. 188–198.
9. Hrechko Viktoriia; Hrygorii Hnatienko; Tetiana Babenko. An intelligent model to assess information systems security level // 2021 Fifth World Conference on Smart Trends in Systems Security and Sustainability (WorldS4), London, United Kingdom, 29-30 July 2021/ Date Added to IEEE Xplore: 19 August 2021, Pp 128 – 133, DOI: 10.1109/WorldS451998.2021.9514019.
10. Babenko, T., Hnatiienko, H., Vialkova, V. Modeling of the integrated quality assessment system of the information security management system / CEUR Workshop Proceedings, Volume 2845, 2021, Pages 75-84 // 7th International Conference ""Information Technology and Interactions"", IT and I 2020; Kyiv; Ukraine; 2 December 2020 through 3 December 2020; Code 168286.
11. Vialkova Vira, Linetskyi Artem, Babenko Tetiana, Myrutenko Larysa /Eliminating privilage escalation to root in containers running on kubernetes// Scientific & practical cyber security journal (SPCSJ) № 1. [Electronic journal]. URL: https://journal.scsa.ge/wp-content/uploads/2020/04/11-41-spcsj.pdf
12. Babenko Tetiana, Hnatiienko Grygorii, Vialkova Vira, Bigdan Andrii / Intellectual model for classification of network cybersecurity events// in the Proceedings International Workshop on Cyber Hygiene, Kyiv, Ukraine, November 30, 2020.Ukraine.
13. Babenko Tetiana, Hnatiienko Grygorii,

							Vialkova Vira /Modeling of the integrated quality assessment system of the information security management system// Proccedings “Information Technology and Interactions” (IT&I-2020) 2-3 December, 2020, Kyiv. 14. Т.В. Бабенко, Г.М. Гнатієнко, В.І. Вялкова / Моделювання системи інформаційної безпеки та автоматизована оцінка інтегральної якості впливу контролів на функціональну стійкість організаційної системи// в XX Міжнародній науково-практичній конференції «Інформаційні технології та безпека» (ІТБ-2020). Інститут проблем реєстрації інформації НАН України, 10 грудня 2020 року, Київ 15. O. Hubskyi, T. Babenko, L.Myrutenko, O. Oksiiuk. Detection of SQL Injection Attack Using Neural Networks. In: Shkarlet S., Morozov A., Palagin A. (eds) Mathematical Modeling and Simulation of Systems (MODS'2020). MODS 2020. Advances in Intelligent Systems and Computing, vol. 1265. Springer, Cham. 16. Dmitry Palko, Tetiana Babenko, Larysa Myrutenko and Andrii Bigdan Model of information security critical incident risk assessment. IEEE International Conference on Problems of Infocommunications Science and Technology, (PIC S&T 2020) for October, 6-9 in Kharkiv, Ukraine. 17. Secure software developing recommendations Grechko, V., Babenko, T., Myrutenko, L. 2019 IEEE International Scientific-Practical Conference: Problems of Infocommunications Science and Technology, PIC S and T 2019 - Proceedings, 2019, стр. 45–50, 9061529. 18. Бабенко Т.В,

							Толюпа С.В., Гречко В.В. Проблеми використання SSL/TSL Захист інформації, Том 19, N 4 жовтень-грудень 2017 с 298-305 19. T. Babenko S. Toliu[a Kovalova LVQ models of DDOS attacks identification14 th International Conference on Advanced Trends in Radioelectronics, Telecommunications and Computer Engineering, IEEE Lviv, 21 february 2018 Відомості про підвищення кваліфікації: 1. ТОВ "РДЛ". Сертифікат про повний курс навчання по роботі зі Шлюзом законного перехоплення для PS core компанії Huawei серія №012/2018 з 1 вересня по 1 листопада 2018 р. 2. Довідка про стажування 01-1/2700 15.01.2021 НТУ «КПІ» (180 год)
101846	Бабенко Тетяна Василівна	професор, Основне місце роботи	Факультет інформаційних технологій	Диплом доктора наук ДД 007055, виданий 03.12.2008, Диплом кандидата наук КН 009601, виданий 21.12.1995, Атестат доцента ДЦ 000404, виданий 27.04.2000, Атестат професора 12ПР 008558, виданий 28.03.2013	30	Безпека банківських технологій	Освіта та науковий ступінь відповідають тематиці дисципліни, наукова робота пов'язана з тематикою дисципліни. Публікації за тематикою дисципліни: 1. Babenko, T.,Hnatiienko, H., Bigdan, A. /Model for determining the protection level of a complex system // CEUR Workshop Proceedings, 2022, 3132, pp. 156–165 (SCOPUS) 2. Hnatiienko, H., Kiktev, N., Babenko, T.,Desiatko, A., Myrutenko, L./ Prioritizing Cybersecurity Measures with Decision Support Methods Using Incomplete Data //CEUR Workshop Proceedings,2021, 3241, pp. 169–180 (SCOPUS) 3. Панченко М., Бігдан А., Бабенко Т., Тимофєєв Д. Виявлення аномалій інформаційної безпеки на основі аналізу ентропії інформаційної системи. Енергетика і автоматика. 2022. №1. С.72-81 4. Detection of sql injection attack using

							neural networks Hubskyi, O., Babenko, T., Myrutenko, L., Oksiiuk, O. Advances in Intelligent Systems and Computing, 2021, 1265 AISC, стр. 277–286. (SCOPUS) 5. Modeling of the integrated quality assessment system of the information security management system Babenko, T., Hnatiienko, H., Vialkova, V. CEUR Workshop Proceedings, 2021, 2845, стр. 75–84. 6. Modeling of critical nodes in complex poorly structured organizational systems Babenko, T., Hnatiienko, H., Ignisca, V., Iavich, M. CEUR Workshop Proceedings, 2021, 2915, стр. 92–101. 7. Determining key risks for modern distributed information systems Palko, D., Hnatienko, H., Babenko, T., Bigdan, A. CEUR Workshop Proceedings, 2021, 3018, стр. 81–100. 8. Babenko, T., Hnatiienko, H., Vialkova, V. Modeling of information security system and automated assessment of the integrated quality of the impact of controls on the functional stability of the organizational system // Selected Papers of the XX International Scientific and Practical Conference "Information Technologies and Security" (ITS 2020), Kyiv, Ukraine, December 10, 2020 / CEUR Workshop Proceedings, 2021, 2859, pp. 188–198. 9. Hrechko Viktoriia; Hrygorii Hnatienko; Tetiana Babenko. An intelligent model to assess information systems security level // 2021 Fifth World Conference on Smart Trends in Systems Security and Sustainability (WorldS4), London, United Kingdom, 29-30 July 2021/ Date Added to IEEE Xplore: 19 August 2021, Pp 128 – 133, DOI: 10.1109/WorldS451998.2021.9514019. 10. Babenko, T., Hnatiienko, H.,

							Vialkova, V. Modeling of the integrated quality assessment system of the information security management system / CEUR Workshop Proceedings, Volume 2845, 2021, Pages 75-84 // 7th International Conference ""Information Technology and Interactions"", IT and I 2020; Kyiv; Ukraine; 2 December 2020 through 3 December 2020; Code 168286. 11. Vialkova Vira, Linetskyi Artem, Babenko Tetiana, Myrutenko Larysa /Eliminating privilage escalation to root in containers running on kubernetes// Scientific & practical cyber security journal (SPCSJ) № 1. [Electronic journal]. URL: https://journal.scsa.ge/wp-content/uploads/2020/04/11-41-spcsj.pdf 12. Babenko Tetiana, Hnatiienko Grygorii, Vialkova Vira, Bigdan Andrii / Intellectual model for classification of network cybersecurity events// in the Proceedings International Workshop on Cyber Hygiene, Kyiv, Ukraine, November 30, 2020.Ukraine. 13. Babenko Tetiana, Hnatiienko Grygorii, Vialkova Vira /Modeling of the integrated quality assessment system of the information security management system// Proccedings “Information Technology and Interactions” (IT&I-2020) 2-3 December, 2020, Kyiv. 14. Т.В. Бабенко, Г.М. Гнатієнко, В.І. Вялкова / Моделювання системи інформаційної безпеки та автоматизована оцінка інтегральної якості впливу контролів на функціональну стійкість організаційної системи// в XX Міжнародній науково-практичній конференції «Інформаційні технології та безпека» (ІТБ-2020). Інститут

							проблем реєстрації інформації НАН України, 10 грудня 2020 року, Київ 15. O. Hubskyi, T. Babenko, L.Myrutenko, O. Oksiiuk. Detection of SQL Injection Attack Using Neural Networks. In: Shkarlet S., Morozov A., Palagin A. (eds) Mathematical Modeling and Simulation of Systems (MODS'2020). MODS 2020. Advances in Intelligent Systems and Computing, vol. 1265. Springer, Cham. 16. Dmitry Palko, Tetiana Babenko, Larysa Myrutenko and Andrii Bigdan Model of information security critical incident risk assessment. IEEE International Conference on Problems of Infocommunications Science and Technology, (PIC S&T 2020) for October, 6-9 in Kharkiv, Ukraine. 17. Secure software developing recommendations Grechko, V., Babenko, T., Myrutenko, L. 2019 IEEE International Scientific-Practical Conference: Problems of Infocommunications Science and Technology, PIC S and T 2019 - Proceedings, 2019, стр. 45–50, 9061529. 18. Бабенко Т.В, Толюпа С.В., Гречко В.В. Проблеми використання SSL/TSL Захист інформації, Том 19, N 4 жовтень-грудень 2017 с 298-305 19. T. Babenko S. Toliu[a Kovalova LVQ models of DDOS attacks identification14 th International Conference on Advanced Trends in Radioelectronics, Telecommunications and Computer Engineering, IEEE Lviv, 21 february 2018 Відомості про підвищення кваліфікації: 1. ТОВ "РДЛ". Сертифікат про повний курс навчання по роботі зі Шлюзом законного перехоплення для PS core компанії Huawei серія №012/2018 з 1 вересня по 1 листопада 2018 р. 2. Довідка про

							стажування 01-1/2700 15.01.2021 НТУ «КПІ» (180 год)
109324	Фесенко Андрій Олексійович	доцент, Основне місце роботи	Факультет інформаційних технологій	Диплом магістра, Національний авіаційний університет, рік закінчення: 2011, спеціальність: 000007 Адміністративний менеджмент у сфері захисту інформації з обмеженим доступом, Диплом кандидата наук ДК 044565, виданий 11.10.2017	8	Криптографічні системи захисту інформації	Освіта та науковий ступінь відповідають тематиці дисципліни, наукова робота пов'язана з тематикою дисципліни. Автор понад 70 наукових публікацій за профілем кафедри (з них: 30 у періодичних наукових фахових виданнях, 18 публікацій включені до наукометричної бази Scopus: h-індекс в Scopus 5), автор розділів в 4 колективних монографіях. Відомості про підвищення кваліфікації: 1. Implementing Cisco Collaboration Devices (CICD) 1.0, CISCO, Certificate number: 112275, August 23, 2019; 2. Криптографічний захист інформації Криптосистеми та засоби криптографічного захисту, НТУУ «КПІ ім. І.Сікорського» ПК№02070921/004903-19 від 24.05.2019; 3. Обладнання комплексу прийому та обробки інформації з телефонних мереж зв'язку «Курс-6» ТОВ «Криптон-М» 2018 рік № 55-2018, 31.10.2018; 4. Побудова захищених комп'ютерних мереж, Національний авіаційний університет, Б/Н, 15.12.2018 5. Навчання на курсах "Foundations of Computer and Network Security" within the 2022 Cybersecurity Summer Instructor Training Program under the USAID Cybersecurity for Critical Infrastructure in Ukraine Activity. 11 July – 31 August 2022. 6. Educational & Scientific Internship Program on Methods and means of data protection in the conditions of cyber warfare at Vocational Training Center in Nowy Sącz (Centrum Kształcenia Zawodowego w Nowym Sączu), 15.12.2022 - 30.01.2023, 180 hours. Публікації за

							тематикою дисципліни: 1. Сучасні технології нейролінгвістичного програмування / [В. М. Петрик, С. О. Гнатюк, А. О. Фесенко та ін.]. – Київ: Центр учбової літератури, 2020. – 200 с. – (978-611-01-2069-2). 2. A. Fesenko, H. Papirna// Scientific and Practical Cyber Security Journal (SPCSJ) 2(2):13-17 Scientific Cyber Security Association (SCSA), 2018, pp. 13- 17 3. Novel certification method for quantum random number generators Novel certification method for quantum random number generators Iavich, M., Kuchukhidze, T., Gnatyuk, S., Fesenko, A. International Journal of Computer Network and Information Security, 2021, 13(3), стр. 28–38 4. Diagnosis of Rail Circuits by Means of Fiber-Optic Cable Mgebrishvili, N., Iavich, M., Moiseev, G., Fesenko, A., Dorozhynskyy, S. Lecture Notes on Data Engineering and Communications Technologies, 2021, 83, стр. 127–137 5. Threat hunting as a method of protection against cyber threats Lukova-Chuikoa, N., Fesenkoa, A., Papirnaa, H., Gnatyukb, S. CEUR Workshop Proceedings, 2021, 2833, стр. 103–113 6. Improvement of Merkle Signature Scheme by Means of Optical Quantum Random Number Generators Iavich, M., Gagnidze, A., Iashvili, G., ...Arakelian, A., Fesenko, A. Advances in Intelligent Systems and Computing, 2021, 1247 AISC, стр. 440–453
337194	Мирутенко Лариса Вікторівна	доцент, Основне місце роботи	Факультет інформаційних технологій	Диплом спеціаліста, Сумський державний педагогісний інститут імені А.С. Макаренка, рік закінчення: 1999, спеціальність:	17	Теорія інформації та кодування	Освіта та науковий ступінь відповідають тематиці дисципліни. Відомості про підвищення кваліфікації: 1. Повний курс навчання по роботі з обладнанням для модернізації

				, Диплом кандидата наук ДК 043333, виданий 26.06.2017, Атестат доцента АД 006549, виданий 07.12.2020			Комплексу прийому та обробки інформації з телефонних мереж зв'язку «Курс-6», ТОВ Криптон-М, сертифікат №54-2018, 31 жовтня 2018 р. 2. Стажування на кафедрі комп'ютеризованих систем захисту інформації Навчально-наукового інституту комп'ютерних інформаційних технологій Національного авіаційного університету, довідка від 20.12.2018 № 0302/4075. 3. Certificate of completion Cyber-Physical System Security within the 2021 Cybersecuriti Summer Training Program under the USAID Project. 14 june - 23 july 2021. Публікації за тематикою дисципліни: 1. Yuliia STEPANENKO, Valeriia SOLODOVNIK, Andriy FESENKO, Larysa MYRYTENKO SECURE PASSWORD STORAGE WITH CRYPTOGRAPHIC HASH FUNCTION / XII International conference of students, phd-students and young scientists "Engineer of XXI century", Bielsko-Biała, Poland, 2021. 2. Hnatiienko, H., Kiktev, N., Babenko, T.,Desiatko, A., Myrutenko, L./ Prioritizing Cybersecurity Measures with Decision Support Methods Using Incomplete Data //CEUR Workshop Proceedings,2021, 3241, pp. 169–180 (SCOPUS) 3. Shestak Y., Valeriia SOLODOVNIK., Myrutenko L. ALGORITHM OF LOAD BALANCE OPTIMIZATION ON HARDWARE RESOURCES OF INFORMATION SYSTEMS. Projekt interdyscyplinarny projektem XXI wieku. Bielsko-Biala: Wydawnictwo Naukowe Akademii Techniczno – Humanistycznej w Bielsku-Bialej, 2020. P. 193-198 4. V. Grechko, T.

							Babenko, і L. Myrutenko, «БЕЗПЕЧНЕ ПРОГРАМНЕ ЗАБЕЗПЕЧЕННЯ, ЩО РОЗРОБЛЯЄ РЕКОМЕНДАЦІЇ», Кібербезпека: освіта, наука, техніка, вип. 2, вип. 6, с. 82-93, Груд 2019. 5. Мирутенко Л. В. Система оцінки якості дистанційної освіти в Україні: основні проблеми і задачі / Лариса Вікторівна Мирутенко. // Системи обробки інформації : збірник наукових праць. – Х.: Харківський університет Повітряних Сил імені Івана Кожедуба, 2016. – Вип. 3(140). – С. 260 – 263
101846	Бабенко Тетяна Василівна	професор, Основне місце роботи	Факультет інформаційних технологій	Диплом доктора наук ДД 007055, виданий 03.12.2008, Диплом кандидата наук КН 009601, виданий 21.12.1995, Атестат доцента ДЦ 000404, виданий 27.04.2000, Атестат професора 12ПР 008558, виданий 28.03.2013	30	Інформаційні системи та мережі	Освіта та науковий ступінь відповідають тематиці дисципліни, наукова робота пов'язана з тематикою дисципліни. Публікації за тематикою дисципліни: 1. Yuliia Kovaleva, Tetiana Babenko, Vira Ignisca Models and Methods of Wireless decentralized network for energy monitoring of critical infrastructure facilitates. Scientific & practical cyber security journal (SPCSJ) № [Electronic journal]. MODELS AND METHODS OF WIRELESS DECENTRALIZED NETWORKS FOR ENERGY MONITORING OF CRITICAL INFRASTRUCTURE FACILITIES | Scientific and practical cyber security journal (scsa.ge). 2. Y. Kovalova, T. Babenko, L.Myrutenko, O. Oksiiuk. Optimization of lifetime in wireless monitoring networks. International Journal of Computing, 19(2).– 2020.– С. 267-272. 3. Babenko Tetiana, Hnatiienko Grygorii, Vialkova Vira /Modeling of information security system and automated expert assessment of integral quality of system functional stability// in the X Inter-University

							Conference “Engineer of the 21st Century". 11 December 2020 at the University of Bielsko-Biała (ATH) in Bielsko-Biała, Poland. 4. Babenko, T., Hnatiienko, H., Ignisca, V., Iavich, M. Modeling of critical nodes in complex poorly structured organizational systems // Proceedings of the 26th International Conference on Information Society and University Studies (IVUS 2021), Kaunas, Lithuania, April 23, 2021 / CEUR Workshop Proceedings, 2021, 2915, pp. 92–101.
37474	Толюпа Сергій Васильович	професор, Основне місце роботи	Факультет інформаційних технологій	Диплом доктора наук ДД 000091, виданий 10.11.2011, Диплом кандидата наук КН 012091, виданий 10.12.1996, Атестат доцента ДЦ 005016, виданий 20.06.2002, Атестат професора 12ПР 008351, виданий 25.01.2013	44	Управління інформаційною безпекою	Освіта та науковий ступінь відповідають тематиці дисципліни. Відомості про підвищення кваліфікації: 1. ТОВ «ДЕПС СЕЛЮШЕНЗ». Сертифікат про підвищення кваліфікації серія DP №000131 від 31.12.2020р. 2. Certificate of completion Incident response within the 2021 Cybersecuriti Summer Training Program under the USAID Project. 3. Навчання на курсах USAID Project “ Cybersecurity for Critical Infrastructure in Ukraine” (за програмою «Malware Analysis») 18 October – 1 December 2021. 4. Навчання на курсах USAID Project "Audit and Risk Management" within the 2022 Cybersecurity Summer Instructor Training Program under the USAID Cybersecurity for Critical Infrastructure in Ukraine Activity. 11 July – 31 August 2022 Навчальні посібники та монографії: 1. Толюпа С.В., Бучик С.С., Лукова-Чуйко Н.В., Фесенко А.О. Системи технічного захисту інформації. . Навчальний посібник. - К.: Формат, 2022. – 386 с. 2. Толюпа С.В., Браіловський М.М., Наконечний В.С., Сайко В.Г. Мікропроцесорні системи на

							мікроконтролерах. Навчальний посібник. – К: КНУ імені Тараса Шевченка, 2022. – с. 298. 3. Толюпа С.В., Політанський Р.Л., Лісінський В.В. Управління інформаційною безпекою. Навчальний посібник. За заг. ред. Толюпи С.В. – Чернівці. ЧНУ імені Юрія Федь-ковича. 2021р. – с. 486. 4. Лукова-Чуйко Н.В. Системи виявлення вторгнень та функціональна стійкість розподілених інформаційних систем до кібернетичних загроз. // Н.В. Лукова-Чуйко, В.С. Наконечний, Толюпа С.В., М.М. Браіловський // Монографія К.: Формат, 2021. – 407 с. 5. Наконечний В.С. Методи та засоби підвищення ефективності функціонування радіотехнічних систем розпізнавання багатопозиційного базування. / В.С. Наконечний, С.В. Толюпа, В.А. Дружинін, Н.В. Лукова-Чуйко. // Монографія. Київ. - К.: Формат. 2019. – 237 с. 6. Браіловський М.М., Толюпа С.В., Наконечний В.С., Методика виявлення та протидії кібернетичним атакам на інформаційні системи. / Наукоємні технології в інфокомунікаціях: обробка, захист та передача інформації. Монграфія Під заг. Радакцією В.М. Безрука, В.В. Баранніка. – Х.: ХНУРЕ., 2018. – с. 310-327 7. Толюпа С.В., Оксіюк О.Г, Вялкова В.І. Захист об’єктів інформаційної діяльності. . Навчальний посібник. – К.: “МП Леся”, 2018. – 312с. 8. Політанський Л.Ф., Політанський Р.Л., Толюпа С.В., Лісінський В.В. Технології комплексного захисту інформації в кіберпросторі. Навчальний посібник.

							За заг. ред. Л.Ф. Політанського. – Чернівці. ЧНУ імені Юрія Федьковича. 2018р. – с. 204. 9. Бойко Ю.М., Дружинін В.А., Толюпа С.В. Теоретичні аспекти підвищення завадостійкості й ефективності обробки сигналів в радіотехнічних пристроях та засобах телекомунікаційних систем за наявності завад. Монографія. – К.: НТУУ «КПІ ім. І. Сікорського», 2018. – 229с. 10. Бараннік В.В. Наукоємні технології в інфокумунікаціях: обробка, захист та передача інформації: монографія / під загальною редакцією В.М. Безрука, В.В. Баранніка. – Х.: ФОП Бровін О.В., 2018. – 328 с. Публікації за тематикою дисципліни: 1. Khusainov, P., Toliupa, S., Bakanov, V., Shtanenko, S. Substantial formulation of the task of improving the information model of decision-making in the prompt (crisis) response to cyber incidents. Proceedings - 16th International Conference on Advanced Trends in Radioelectronics, Telecommunications and Computer Engineering, TCSET 2022, 2022, стр. 287–290. 2. Pliushch, O., Toliupa, S., Kravchenko, Y., Rybydajlo, A. Pulse-forming Network with Improved Form of the Pulse. Proceedings - 16th International Conference on Advanced Trends in Radioelectronics, Telecommunications and Computer Engineering, TCSET 2022, 2022, стр. 314–318. 3. Toliupa, S., Buchyk, S., Nakonechnyi, V., ...Parkhomenko, I., Lukova-Chuiko, N. Building an Intrusion Detection System in Critically Important Information Networks with Application of Data Mining Methods. Proceedings - 16th International

							Conference on Advanced Trends in Radioelectronics, Telecommunications and Computer Engineering, TCSET 2022, 2022, стр. 128–133. 4. Shtanenko, S., Samokhvalov, Y., Toliupa, S., Silko, O. Increasing survivability of technological systems based on the technology of programmable logic device. CEUR Workshop Proceedingsthis link is disabled, 2022, 3132, стр. 237–245. 5. Zhurakovskyi, B., Toliupa, S., Druzhynin, V., Bondarchuk, A., Stepanov, M. Calculation of Quality Indicators of the Future Multiservice Network. Book Chapter. Lecture Notes in Electrical Engineeringthis link is disabled, 2022, 831, стр. 197–209. 6. Saiko, V., Toliupa, S., Nakonechnyi, V., Brailovskyi, M., Domrachev, V. Model of Increase of Spectral Efficiency of Use of Frequency Resource of Low-Orbit System with Architecture of the Distributed Satellite. Book Chapter. Lecture Notes in Electrical Engineeringthis link is disabled, 2022, 831, стр. 410–423. 7. Сергій Толюпа, Іван Пархоменко, Людмила Терейковська, Володимир Кваснiков Побудова систем виявлення кібератак за допомогою прихованої марківської моделі. Науковий журнал НУ "Чернігівська політехніка" Технічні науки та технології , 2021. №1(23) – с. 89-96. (Фахове видання) 8. С.Толюпа, І. Пархоменко, С. Штаненко. Модель системи протидії вторгненням в інформаційних системах. Інфокомунікаційні технології та електронна інженерія. №1. 2021. С. 86-95. 9. Самохвалов Юрій, Толюпа Сергій, Штаненко Сергій. Забезпечення кібербезпеки АСУ ТП шляхом застосування ПЛІС технології.

							Безпека інформаційних систем і технологій. №1. 2021. С. 45-54. 10. Толюпа С.В., Білецький В.С. Атаки аутентифікації та авторизації на web-ресурси. Вісник інженерної академії України. №2. – 2017. – с.98-104. 11. Serhii Toliupa , Oleksandr Pliushch , Ivan Parkhomenko. Побудова систем виявлення атак в інформаційних мережах на нейромережевих структурах. Електронне фахове наукове видання "Кібербезпека: освіта, наука, техніка" том 2 №10. 2020. с. 169-183. 12. Толюпа С. В., Пархоменко І. І., Кириленко А. І., Вадис К. А. «Захист корпоративної інформації на мобільних пристроях.», Збірник наукових праць «Моделювання та інформаційні системи в економіці», КНЕУ, 2020. №99 — С. 151 – 161. 13. Толюпа С. В., Одарченко Р. С., Пархоменко І. І., Даков С.Ю. «Виявлення атак в корпоративній мережі за допомогою правил нечіткої логіки», Наукоємні технології. – К.:НАУ, 2020. – № 4 (48). – С 470-477. 14. Lada Slipachuk, Serhii Toliupa and Volodymyr Nakonechnyi. The Process of the Critical Infrastructure Cyber Security Management using the Integrated System of the National Cyber Security Sector Management in Ukraine. 3rd IEEE International Conference On Advanced Information and Communication Technologies (AICT) – 2019. Lviv, Ukraine. Scopus. 15. Serhii Toliupa, Hanna Shvedova and Ivan Parkhomenko. Security and Regulatory Aspects of the Critical Infrastructure Objects Functioning and Cyberpower Level Assesment. 3rd IEEE International Conference On

							Advanced Information and Communication Technologies (AICT) – 2019. Lviv, Ukraine. Scopus. 16. Sergey Toliupa, Ihor Tereikovskiy, Ivan Dychka, Liudmyla Tereikovska and Alexander Trush. The Method of Using Production Rules in Neural Network Recognition of Emotions by Facial Geometry. 3rd IEEE International Conference On Advanced Information and Communication Technologies (AICT) – 2019. Lviv, Ukraine. Scopus. 17. Serhii Toliupa, Liudmyla Tereikovska, Ihor Tereikovskyi, Oleksandr Korystin, Volodymyr Nakonechnyi. One-periodic template marks model of normal behavior of the safety parameters of information systems networking resources. International Scientific-Practical Conference Problems of Infocommunications Science and Technology (PIC S&T) 2019 Ukraine. Scopus. 18. Nakonechnyi V. Toliupa S. Tereshchenko I., Tereshchenko A. Branch Information technologies of Quality Management. IEEE International Scientific-Practical Conference «Problems of Infocommunications. Science and Technology» (PIC S&T-2018), Kharkov (Ukraine), 9 – 12 October 2018. Scopus. – c. 156-159. 19. Ihor Tereikovskiy, Serhii Toliupa, Ivan Parkhomenko and Liudmyla Tereikovska. Markov model of normal conduct template of computer systems network objects. 14th International Conference. Advanced trends in radioelecttronics, telecommunications and comhuter engineering TCSET-2018. 20-524/02/18/ Славське. P. 345-353. Scopus 20. Tetiana Babenko, Serhii Toliupa and Yuliia Kovalova. Title:

							LVQ models of DDOS attacks identification. 14th International Conference Advanced trends in radioelecttronics, telecommunications and comhuter engineering TCSET-2018. 20-24/02/18/ Славське. P. 186-191. Scopus 21. Volodymyr Saiko, Volodymyr Nakonechnyi, Serhii Toliupa and Mykola Brailovskyi. Method for determining optimal transparency windows for mobile 5th generation. 14th International Conference advanced trends in radioelecttronics, telecommunications and comhuter engineering TCSET-2018. 20-24/02/18/ Славське. P. 198-203. Scopus 22. Volodymyr Saiko, Serhii Toliupa, Volodymyr Nakonechnyi and Serhii Dakov. The method for reducing probability of incorrect data reception in radio channels of terahertz frequency range. 14th International Conference Advanced trends in radioelecttronics, telecommunications and comhuter engineering TCSET-2018. 20-24/02/18/ Славське. P. 408-411. Scopus; 1. Довбешко С.В., Толюпа С.В., Труш О.В. Додатковий захистний код, обфускований віртуальною машиною. Науково-технічний журнал “Сучасний захист інформації”.– №3. 2018. С. 84-92. 23. Довбешко С.В., Толюпа С.В., Шестак Я.В. Застосування методів інтелектуального аналізу даних для побудови систем виявлення атак. Науково-технічний журнал “Сучасний захист інформації”.– №1. 2019. С. 56-62. 24. Толюпа С.В., Пархоменко І.І., Коноваленко А.Д. Аналіз вразливостей локальних бездротових мереж та способи їх захисту від можливих атак.

							Вісник інженерної академії України. №3. – 2018. с. 72 – 76.
187783	Коротченков Олег Олександрович	професор, Основне місце роботи	Фізичний факультет	Диплом спеціаліста, Київський ордена Леніна державний університет ім.і Т.Г. Шевченка, рік закінчення: 1980, спеціальність: , Диплом доктора наук ДД 001040, виданий 12.01.2000, Атестат професора ПР 002464, виданий 23.10.2003	36	Фізика	Освіта та науковий ступінь відповідають тематиці дисципліни, наукова робота пов'язана з тематикою дисципліни. Член постійних спеціалізованих вчених рад Д26.001.23 при Київському національному університеті імені Тараса Шевченка та Д26.159.01 при Інституті фізики НАН України. Науковий керівник держбуджетної теми 19БФ051-05 (2019-2021); член редакційної колегії з фізики твердого тіла журнала Open Physics De Gruyter, Springer (2007-2017) 2018 рецензент журналів: APS (Physical Review B та Physical Review Letters), AIP (Applied Physics Letters, Journal of Applied Physics, Review of Scientific Instruments), IOP (Nanotechnology, Journal of Physics D, Semiconductor Science and Technology), Physica B, Nanoscale Research Letters, PLOS ONE, Optical Materials, Journal of Industrial and Engineering Chemistry. Публікації за тематикою дисципліни: 1. Подолян А.О., Коротченков О.О. Фізика низькорозмірних напівпровідників. Генерація та рекомбінація нерівноважних носіїв заряду. Фотоелектричний ефект // Вінниця: ТОВ “Твори”, 2018 (4 друк. арк.); Напівпровідникові гетероструктури та нанокомпозити на основі кремнію та оксиду цинку: сонохімічний синтез та фізичні властивості. Наукова монографія / О.О. Коротченков, А.Б. Надточій, М.І. Закіров, М.В. Ісаєв, А.Г. Кузьмич, М.О. Боровий – Київ–Вінниця: ТОВ “Твори”, 2018. – 218 с. ISBN 978-617-7706-25-9.

							2. Enhancing the Seebeck effect in Ge/Si through the combination of interfacial design features / A. Nadtochiy, V. Kuryliuk, V. Strelchuk, O. Korotchenkov, P.-W. Li, S.-W. Lee // Scientific Reports. – 2019. – Vol. 9, doi.org/10.1038/s41598-019-52654-z; 3. Enhanced terahertz conductivity in ultra-thin gold film deposited onto (3-mercaptopropyl) trimethoxysilane (MPTMS)-coated Si substrates / Y. Lee, D. Kim, J. Jeong, J. Kim, V. Shmid, O. Korotchenkov, P. Vasa, Y.-M. Bahk, D.-S. Kim // Scientific Reports. – 2019. – Vol. 9, article 15025 (7 pp.); 4. Sonochemical modification of SiGe layers for photovoltaic applications / A. Nadtochiy, O. Korotchenkov, V. Schlosser // Physica Status Solidi (a). – 2019. – Vol. 216, Issue 17, article 1900154 (9 pp.); 5. Improving photoelectric energy conversion by structuring Si surfaces with Ge quantum dots / V. Shmid, V. Kuryliuk, A. Nadtochiy, O. Korotchenkov, P.-W. Li // Proceedings of the 2019 IEEE 39th International Conference on Electronics and Nanotechnology, ELNANO. – 2019. – P. 92–96; 6. Epoxy filled with bare and oxidized multi-layered graphene nanoplatelets: a comparative study of filler loading impact on thermal properties / B. Gorelov, A. Gorb, A. Nadtochiy, D. Starokadomsky, V. Kuryliuk, N. Sigareva, S. Shulga, V. Ogenko, O. Korotchenkov, O. Polovina // Journal of Material Science. – 2019. – Vol. 54, Issue 12, P. 9247–9266; 7. Charge-carrier relaxation in sonochemically fabricated dendronized $CaSiO_3$–SiO_2–Si nanoheterostructures / R. Savkina, A. Smirnov, S. Kirilova, V. Shmid, A.

							Podolian, A. Nadtochiy, V. Odarych, O. Korotchenkov // Applied Nanoscience. – 2019. – Vol. 9, Issue 5, P. 1047-1056; 8. Фотоелектричні властивості плівок SiGe, покритих шарами аморфного та полікристалічного кремнію / V. Shmid, A. Podolian, A. Nadtochiy, O. Korotchenkov, B. Romanyuk, V. Melnik, V. Popov, O. Kosulya // Укр. фіз. журн. – 2019. – т. 64, №5, С. 413–422; 9. Enhanced photoresponse of Ge/Si nanostructures by combining amorphous silicon deposition and annealing/ R. Savkina, A. Smirnov, S. Kirilova, V. Shmid, A. Podolian, A. Nadtochiy, V. Odarych, O. Korotchenkov // Applied Nanoscience. – 2019. – Vol. 9, Issue 5, P. 1047-1056; 10. A simple sonochemical synthesis of nanosized ZnO from zinc acetate and sodium hydroxide / M.I. Zakirov, M.P. Semen'ko, O.A. Korotchenkov // Journal of Applied Physics – 2018. – Vol. 124, Issue 9, P. 095703 (7 pp) 11. Фото-електричні властивості кремнієвих структур із нанокомпозитним епоксидно-полімерним шаром / В.І. Шмід, С.П. Назаров, А.О. Подолян, А.Б. Надточій, О.О. Коротченков // Ж. нано- електрон. фіз.– 2018. – т. 10, №2, С. 02024 (6 с.)
168831	Браіловський Микола Миколайович	доцент, Основне місце роботи	Факультет інформаційних технологій	Диплом кандидата наук ДК 020523, виданий 08.10.2003, Атестат доцента 02ДЦ 002476, виданий 21.10.2004	25	Національна та інформаційна безпека держави	Освіта та науковий ступінь відповідають тематиці дисципліни, наукова робота пов'язана з тематикою дисципліни. Навчальні посібники та підручники: 1. Захист систем електронних комунікацій: навч.посіб./ В.О. Хорошко, О.В. Криворучко, М.М. Браіловський та ін. – Київ: Київ. нац. торг.-екон. ун-т, 2019. – 164 с. 2. Браіловський М.М. Технології захисту

							інформації: підручник / М.М. Браіловський, С.В. Зибін, І.В. Пискун, В.О. Хорошко, Ю.Є. Хохлачова. –К.: ЦП «Компринт», 2021. – 296 с. Монографії: 1. Толюпа С.В., Наконечний В.С., Браіловський М.М. Методика виявлення та протидії кібернетичним атакам на інформаційні системи. / Наукоємні технології в інфокомунікаціях: обробка, захист та передача інформації. Монографія Під заг. Радакцією В.М. Безрука, В.В. Баранніка. – Х.: ХНУРЕ., 2018. – с. 310-327 . 2. Лукова-Чуйко Н.В. Системи виявлення вторгнень та функціональна стійкість розподілених інформаційних систем до кібернетичних загроз. // Н.В. Лукова-Чуйко, В.С. Наконечний, Толюпа С.В., М.М. Браіловський // Монографія К.: Формат, 2021. – 407 с. Публікації за тематикою дисципліни: 1. Mykola Brailovskyi, Volodymyr Khoroshko, Volodymyr Artemov, Yulia Khokhlachova, Tyna Pirtskhalava Methods of preparing and conducting modern hybrid wars // Scientific & practical cyber security journal (SPCSJ) VOL 6. №3. [Electronic journal]. https://journal.scsa.ge/wp-content/uploads/2022/10/fulljournalseptember2022.pdf 2. Brailovskyi, M., Saiko, V., Narytnyk, T., Nakonechnyi, V. Radiating telecommunication system of the sub-THz-band to protect objects from unauthorized access. 2019 IEEE International Scientific-Practical Conference: Problems of Infocommunications Science and Technology, PIC S and T 2019 - Proceedingsthis link is disabled, 2019, стр. 698–702, 9061483 3. Brailovskyi M,

Khoroshko V. Models of interaction of a potentially dangerous terrorist group and the security service on a protected object// Scientific & practical cyber security journal (SPCSJ) №3. [Electronic journal]. URL: https://scsa.ge/en/2018/09/30/spcsj-%E2%84%96-3-02-september-2018/
4. Nikolay Brailovskyi, Valeri Kozura, Svetlana Kondakova, Volodymyr Khoroshko Analysis of the cybersecurity status of the information space // Scientific & practical cyber security journal (SPCSJ) №4. [Electronic journal]. URL: https://journal.scsa.ge/issue /december-2018/
5. N. Brailovskyi, V. Khoroshko DEVELOPMENT OF AN AUTOMATED SYSTEM INTRUDER MODEL // Scientific & practical cyber security journal (SPCSJ) VOL 3. №1. [Electronic journal]. URL: https://journal.scsa.ge/ru/papers/development-of-an-automated-system-intruder-model-3/
6. N. Brailovskyi, V. Khoroshko, V. Kozura MATHEMATICAL MODEL OF COUNTER-TERRORIST ACTIVITY // Scientific & practical cyber security journal (SPCSJ) VOL 3. №2. [Electronic journal] https://journal.scsa.ge/ru/papers/matematicheskaja-model-kontrterroristicheskoj-dejatelnosti/.
7. N. Brailovskyi, V. Khoroshko, Y. Khokhlachova, Ayasrah Ahmad Rasmi Ali. Evaluation of the Level of Cyber Security of Information // Scientific & practical cyber security journal (SPCSJ) VOL 3. №3. [Electronic journal]. https://journal.scsa.ge/wp-content/uploads/2019/10/sept_2019_full_issue_.pdf
8. М.М. Браіловський., І. С. Іванченко, І. Р. Опірський, В. О. Хорошко Інформаційно-психологічне протиборство в

							Україні Безпека інформації. Том 25, № 3 (2019) С.144-149. Фахове видання 9. M. Brailovskyi, V. Khoroshko, V. Artemov, I. Ivanchenko Geopolitics and information warfare // Scientific & practical cyber security journal (SPCSJ) VOL 4. №1. [Electronic journal].https://journal.scsa.ge/ru/papers/geopolitics-and-information-warfare-3/ 10. Nikolay Brailovskyi, Volodymyr Khoroshko, Volodymyr Artemov, Ivan Opirskyi, Ihor Ivanchenko Information war in Ukraine// Scientific & practical cyber security journal (SPCSJ) VOL 4. №4. [Electronic journal]. https://journal.scsa.ge/ru/papers/information-war-in-ukraine-2/ 11. Браіловський М.М. Хорошко В.О. Використання теорії ігор при аналізі гібрідних війн // Informatics and Mathematical Methods in Simulation. Vol. 10 (2020), No. 3-4, pp. 222-229. 12. Nikolay Brailovskyi, Volodymyr Khoroshko, Serhii Zybin, Yuliia Khokhlachova Conflict situations and interactions of the parties// Scientific & practical cyber security journal (SPCSJ) VOL 5. №1. [Electronic journal]. https://journal.scsa.ge/ru/papers/conflict-situations-and-interactions-of-the-parties-3/ 13. Mykola Brailovskyi, Volodymyr Khoroshko, Volodymyr Artemov, Oleksandr Lytvynenko Information war in modern conditions. Part 1 // Scientific & practical cyber security journal (SPCSJ) VOL 5. №2. [Electronic journal]. https://journal.scsa.ge/ru/papers/information-war-in-modern-conditions-part-1-3/ 14. Браіловський М.М., Хорошко В. О. Управління конфліктами та інцидентами інформаційної безпеки в мережі Internet // Informatics and Mathematical

							Methods in Simulation. Vol. 11 (2021), No. 1-2, pp. 5-15. 15. Mykola Brailovskyi, Volodymyr Khoroshko, Volodymyr Artemov, Oleksandr Lytvynenko Information war in modern conditions. Part 2 // Scientific & practical cyber security journal (SPCSJ) VOL 5. №3. [Electronic journal]. https://journal.scsa.ge/ru/papers/information-war-in-modern-conditions-part-2-3/ Відомості про підвищення кваліфікації: 1. Стажування в ТОВ «ДЕПС СОЛЮШЕНЗ» з 01.10.2020 по 31.12.2020 р. Обсяг 6 кредитів ECTS / 180 академ. годин. Сертифікат DP № 000133 від 31.12.2020 р. 2. ТОВ "М.Е.Док". Обсяг 180 академ. годин. Сертифікат ITE041 від 26.05.2021 р. 3. Certificate of completion Audit and Risk Management within the 2021 Cybersecuriti Summer Training Program under the USAID Project. 14 june - 23 july. 4. Навчання на курсах "Web security" within the 2022 Cybersecurity Summer Instructor Training Program under the USAID Cybersecurity for Critical Infrastructure in Ukraine Activity. 11 July – 31 August 2022.
337194	Мирутенко Лариса Вікторівна	доцент, Основне місце роботи	Факультет інформаційних технологій	Диплом спеціаліста, Сумський державний педагогісний інститут імені А.С. Макаренка, рік закінчення: 1999, спеціальність: , Диплом кандидата наук ДК 043333, виданий 26.06.2017, Атестат доцента АД 006549, виданий 07.12.2020	17	Кіберпростір та протидія кіберзлочинності	Освіта та науковий ступінь відповідають тематиці дисципліни. Відомості про підвищення кваліфікації: 1. Стажування на кафедрі комп'ютеризованих систем захисту інформації Навчально-наукового інституту комп'ютерних інформаційних технологій Національного авіаційного університету, довідка від 20.12.2018 № 0302/4075. 2. Certificate of completion Cyber-Physical System Security within the

							2021 Cybersecuriti Summer Training Program under the USAID Project. 14 june - 23 july 2021. Публікації за тематикою дисципліни: 1. Model of Information Security Critical Incident Risk Assessment Palko, D., Myrutenko, L., Babenko, T., Bigdan, A. 2020 IEEE International Conference on Problems of Infocommunications Science and Technology, PIC S and T 2020 - Proceedings, 2021, стр. 157–161, 9468107 2. Detection of sql injection attack using neural networks Hubskyi, O., Babenko, T., Myrutenko, L., Oksiiuk, O. Advances in Intelligent Systems and Computing, 2021, 1265 AISC, стр. 277–286 3. Lakhno, V. A., Kravchuk, P. U., Malyukov, V. P., Domrachev, V. N., Myrutenko, L. V., & Piven, O. S. (2017). Developing of the cyber security system based on clustering and formation of control deviation signs. Journal of Theoretical and Applied Information Technology, 95(21), 5778–5786. 4. Kovalova, Y., Babenko, T., Oksiiuk, O., & Myrutenko, L. (2020). OPTIMIZATION OF LIFETIME IN WIRELESS MONITORING NETWORKS. International Journal of Computing, 19(2), 267-272. https://doi.org/10.47839/ijc.19.2.1770 5. Grechko, V., Babenko, T., Myrutenko, L. Secure software developing recommendations / 2019 IEEE International Scientific-Practical Conference: Problems of Infocommunications Science and Technology, PIC S and T 2019 - Proceedingsthis link is disabled, 2019, стр. 45–50.
402045	Михальчук	асистент,	Факультет	Диплом	19	Основи	Освіта та науковий

	Інна Іванівна	Основне місце роботи	інформаційних технологій	спеціаліста, Київський міжнародний університет цивільної авіації, рік закінчення: 2000, спеціальність: 090702 Радіоелектронні пристрої, системи та комплекси, Диплом кандидата наук ДК 062594, виданий 27.09.2021		алгоритмізації та програмування	ступінь відповідають тематиці дисципліни. Відомості про підвищення кваліфікації: 1. Навчання на курсах "Advanced Malware" within the 2022 Cybersecurity Summer Instructor Training Program under the USAID Cybersecurity for Critical Infrastructure in Ukraine Activity. 11 July – 31 August 2022. 2. Підвищення кваліфікації в ТОВ "Хуавей Україна". Тема: Сучасні методики розрахунку мобільних мереж (оптимізація, протоколи). 30.04.2018 р. Публікації за тематикою дисципліни: 1. Лаптєв О.А., Бучик С.С., Савченко В.А., Наконечний В.С. , Михальчук І.І, Шестак Я.В. Виявлення та блокування повільних ddos-атак за допомогою прогнозування поведінки користувача. Наукоємні технології. Інформаційні технології, кібербезпека. К.: НАУ, 2022. – № 3. – .С 184-192. 2. Павлов В. Г., Щербак Л.М., Михальчук І.І. Захист програмного забезпечення. Методичні вказівки для студентів та слухачів спеціальності 7.160105 «Захист інформації в комп`ютерних системах та мережах».– К.: НАУ, 2005. 3. Павлов В.Г., Габрусенко Е.І., Михальчук І.І. Запобігання витоку інформації у бездротових мережах. Безпека інформації: зб.наук. пр. – К.: НАУ, 2014. –Том 20 №1 (2014). –С. 21-24.
302809	Вишивана Ірина Григорівна	асистент, Основне місце роботи	Навчально-науковий інститут високих технологій	Диплом спеціаліста, Київський національний університет імені Тараса Шевченка, рік закінчення: 2000, спеціальність:	11	Науковий образ світу	Освіта та науковий ступінь відповідають тематиці дисципліни, наукова робота пов'язана з тематикою дисципліни. Публікації за тематикою дисципліни: 1. Stanislav Repetsky,

				070102 Фізика твердого тіла, Диплом кандидата наук ДК 045441, виданий 12.03.2008			Iryna Vyshyvana, Yasuhiro Nakazawa, Sergei Kruchinin, Stefano Bellucci. Electron Transport in Carbon Nanotubes with Adsorbed Chromium Impurities. Materials. 12(3), 524,2019 https://doi.org/10.3390/ma12030524 2. S. P. Repetsky, I.G. Vyshyvana, S. P. Kruchinin & Stefano Bellucci. Influence of the ordering of impurities on the appearance of an energy gap and on the electrical conductance of graphene // Scientific Reports volume 8, Article number: 9123 (2018). https://www.nature.com/articles/s41598-018-26925-0 3. S. P. Repetsky, I. G. Vyshyvana, E. Ya. Kuznetsova, S. P. Kruchinin. Energy spectrum of graphene with adsorbed potassium atoms. International Journal of Modern Physics B Vol. 32 1840030, 2018. 4. В. Б. Молодкін, В. В. Лізунов, Г.І. Низкова, Є.М. Кисловський, А. О. Білоцька, Я. В. Василик, С. В. Дмітрієв, Т. П. Владімірова, О. В. Решетник, С. В. Лизунова, І.Е. Голентус, В. В. Молодкін, С. П. Репецький, І. Г.Вишивана, Спосіб визначення структурної досконалості монокристала, Патент України № a2018 04811 від 02.05. 2018.
334866	Сінгаєвський Євген Миколайович	асистент, Основне місце роботи	ННЦ "Інститут біології та медицини"	Диплом спеціаліста, Київський національний університет імені Тараса Шевченка, рік закінчення: 2006, спеціальність: 070405 Зоологія, Диплом кандидата наук ДК 025576, виданий 22.12.2014	22	Основи екології	Освіта та науковий ступінь відповідають тематиці дисципліни. Публікації за тематикою дисципліни: Балан П.Г., Лукашов Д.В., Трохимець В.М., Сінгаєвський Є.М. Практикум із зоології безхребетних: для студентів біологічних факультетів вищих навчальних закладів. Київ: Фітосоціоцентр, 2018. – 154 с. Публікації за тематикою дисципліни: 1) В. Януль., Сінгаєвський Є.М. Попередні відомості про фауну павуків (Arachnida, Aranei)

							Фастівського району (Київська область) // Вісник Київського національного університету імені Тараса Шевченка: серія Біологія. – 2021. – Т.85, Вип., 2. – С. 51–56. 2). Гриник Є.О., Сінгаєвський Є.М. Павуки (Arachnida, Aranei) ландшафтного заказника "Яхнівський" (Київська область) // Вісник Київського національного університету імені Тараса Шевченка: серія Біологія. – 2020. – Т.83, Вип., 4. – С. 33–37.
337194	Мирутенко Лариса Вікторівна	доцент, Основне місце роботи	Факультет інформаційних технологій	Диплом спеціаліста, Сумський державний педагогісний інститут імені А.С. Макаренка, рік закінчення: 1999, спеціальність: , Диплом кандидата наук ДК 043333, виданий 26.06.2017, Атестат доцента АД 006549, виданий 07.12.2020	17	Вступ до кібернетичної безпеки	Освіта та науковий ступінь відповідають тематиці дисципліни. Відомості про підвищення кваліфікації: 1. Повний курс навчання по роботі з обладнанням для модернізації Комплексу прийому та обробки інформації з телефонних мереж зв'язку «Курс-6», ТОВ Криптон-М, сертифікат №54-2018, 31 жовтня 2018 р. 2. Стажування на кафедрі комп'ютеризованих систем захисту інформації Навчально-наукового інституту комп'ютерних інформаційних технологій Національного авіаційного університету, довідка від 20.12.2018 № 0302/4075. 3. Certificate of completion Cyber-Physical System Security within the 2021 Cybersecuriti Summer Training Program under the USAID Project. 14 june - 23 july 2021. Публікації за тематикою дисципліни: 1. Oleksandr, O., Myrutenko, L., Shestak, Y., & Viktoria, G. (2019). Formation of the Method of Branched its Power Distribution by Activities and Specifics of Work. In 2018 International Scientific-Practical Conference on Problems of

Infocommunications Science and Technology, PICS and T 2018 - Proceedings (pp. 95–98). Institute of Electrical and Electronics Engineers Inc. https://doi.org/10.1109/INFOCOMMST.2018.8632025
2. Lakhno, V. A., Kravchuk, P. U., Malyukov, V. P., Domrachev, V. N., Myrutenko, L. V., & Piven, O. S. (2017). Developing of the cyber security system based on clustering and formation of control deviation signs. Journal of Theoretical and Applied Information Technology, 95(21), 5778–5786.
3. Lakhno, V., Kazmirchuk, S., Kovalenko, Y., Myrutenko, L., & Zhmurko, T. (2016). Design of adaptive system of detection of cyber-attacks, based on the model of logical procedures and the coverage matrices of features. Eastern-European Journal of Enterprise Technologies, 3(9), 30–38. https://doi.org/10.15587/1729-4061.2016.71769; 1. Удосконалений метод побудови опорного сегменту мережі LTE / Р. С.Одарченко, С. Ю. Даков, Л. В. Мирутенко, Л. О. Харлай. // Наукоємні технології. – 2018. – С. 18–27.
4. Мирутенко Л. В. Модель формування системи показників та критеріїв оцінювання якості комплексу програмного забезпечення системи дистанційного навчання / Лариса Вікторівна Мирутенко// Системи обробки інформації: збірник наукових праць. – Х.: Харківський університет Повітряних Сил імені Івана Кожедуба, 2016. – Вип. 6 (140). – С. 196 – 200.
5. Мирутенко Л.В. Модель оптимального вибору системи дистанційного навчання / Лариса Вікторівна Мирутенко. //

							Системи управління, навігації та зв'язку: збірник наукових праць. – П.: Полтавський національний технічний університет імені Юрія Кондратюка, 2015.– № 4(36). – С. 79-84. 6. Grechko, V., Babenko, T., Myrutenko, L. Secure software developing recommendations / 2019 IEEE International Scientific-Practical Conference: Problems of Infocommunications Science and Technology, PIC S and T 2019 - Proceedingsthis link is disabled, 2019, стр. 45–50. 7. Kovalova, Y., Babenko, T., Oksiiuk, O., & Myrutenko, L. (2020). OPTIMIZATION OF LIFETIME IN WIRELESS MONITORING NETWORKS. International Journal of Computing, 19(2), 267-272. https://doi.org/10.47839/ijc.19.2.1770
185330	Пархоменко Іван Іванович	доцент, Основне місце роботи	Факультет інформаційних технологій	Диплом кандидата наук ДК 015285, виданий 03.07.2002, Атестат доцента 12ДЦ 017184, виданий 21.06.2007	24	Операційні системи та їх захист	Освіта та науковий ступінь відповідають тематиці дисципліни. Публікації за тематикою дисципліни: 1. S., Druzhynin V., Parkhomenko I. «Signature and statistical analyzers in the cyber attack detection system», Scientific and Practical Cyber Security Journal (SPCSJ) 2(3): 01-07 ISSN 2587-4667 Scientific Cyber Security Association (SCSA), С. 47-53. 2. Serhii Toliupa, Mykola Brailovskyi, Ivan Parkhomenko «Building intrusion detection systems based on the basis of methods of intellectual analysis of data». "Informatyka, Automatyka, Pomiary w Gospodarce i Ochronie Środowiska" – IAPGOS Vol 8 No 4 (2018) pp. 28-31 2018; 8 (4): 28-31. (Іноземне видання) 3. Т. В. Бабенко, І.І. Пархоменко, Р.В. Зюбіна, Д.В. Палко «Захист інформації та

							передачі даних в корпоративних мережах з використанням програмно-апаратних засобів», Вісник інженерної академії України випуск №3 – 2018, с. 68 – 72 (Фахове видання) 4. Толюпа С. В., Пархоменко І. І., Кириленко А. І., Вадис К. А. «Захист корпоративної інформації на мобільних пристроях.», Збірник наукових праць «Моделювання та інформаційні системи в економіці», КНЕУ, 2020. №99 — С. 151 – 161 (Фахове видання) 5. Толюпа С. В., Одарченко Р. С., Пархоменко І. І., Даков С.Ю. «Виявлення атак в корпоративній мережі за допомогою правил нечіткої логіки», Наукоємні технології. – К.:НАУ, 2020. – № 4 (48). – С 470-477 (Фахове видання) 6. Толюпа С.В., Плющ О.Г., Пархоменко І.І. «Побудова систем виявлення вторгнень в інформаційно-телекомунікаційну мережу на основі методів інтелектуального розподілу даних», Збірник наукових праць «Військового інституту Київського національного університету імені Тараса Шевченка.», К.: ВІКНУ, 2020. № 68., -- С. 80-90. (Фахове видання) 7. Роман Сергійович Одарченко, Толюпа Сергій Васильович, Пархоменко Іван Іванович, Даков Сергій Юрійович Виявлення атак в корпоративній мережі за допомогою правил нечіткої логіки, «Наукоємні технології», Том 48, №4 (2020), с. 470-476 8. Serhii Toliupa, Oleksandr Pliushch, Ivan Parkhomenko «Побудова систем виявлення атак в інформаційних мережах на нейромережевих структурах», електронне фахове наукове видання "Кібербезпека: освіта, наука, техніка" том 2

							№10. 2020. С. 169-183. (Електронне фахове наукове видання) 9.Сергій Толюпа, Іван Пархоменко, Людмила Терейковська, Володимир Квасніков Побудова систем виявлення кібератак за допомогою прихованої марківської моделі. Науковий журнал НУ "Чернігівська політехніка" Технічні науки та технології , 2021. №1(23) – с. 89-96. (Фахове видання) 10. С.Толюпа, І. Пархоменко, С. Штаненко. Модель системи протидії вторгненням в інформаційних системах. Інфокомунікаційні технології та електронна інженерія. №1. 2021. С. 86-95. 11. Toliupa S., Parkhomenko I., Antoniuk V. Method for Identification of Critical Information Infrastructure Objects of the State. CEUR Workshop Proceedingsthis link is disabled, 2021, 3179, pp. 262–271 12. Toliupa, S., Buchyk, S., Nakonechnyi, V., Parkhomenko, I., Lukova-Chuiko, N. Building an Intrusion Detection System in Critically Important Information Networks with Application of Data Mining Methods. Proceedings - 16th International Conference on Advanced Trends in Radioelectronics, Telecommunications and Computer Engineering, TCSET 2022, 2022, pp. 128–133 13. Serhii Toliupa, Ivan Parkhomenko, Ruslana Ziubina, Olga Veselska, Stanislaw Rajba, Kornel Warwas Detection of abnormal traffic and network intrusions based on multiple fuzzy rules. Knowledge-Based and Intelligent Information & Engineering Systems: Proceedings of the 26th International Conference KES2022 Procedia Computer Science Volume 207, 2022, Pages 44-53 Відомості про підвищення

							кваліфікації: 1. Стажування в навчально-науковому інституті комп'ютерних інформаційних технологій Національного авіаційного університету з 20.09.2017-20.12.2017 Довідка № 03.02/2724 від 20.12.2017 2. Стажування в ТОВ «ДЕПС СОЛЮШЕНЗ» з 01.10.2020 по 31.12.2020 Сертифікат Серія DP №000132. 3. Certificate of completion Audit and Risk Management within the 2021 Cybersecuriti Summer Training Program under the USAID Project. 14 june - 23 july. 4. Certificate of completion Cloud Cybersecurity within the 2022 Cybersecurity Summer Instructor Training Program under the USAID Cybersecurity for Critical Infrastructure in Ukraine Activity. 11 July – 31 August 2022
340471	Бучик Сергій Степанович	професор, Основне місце роботи	Факультет інформаційних технологій	Диплом доктора наук ДД 006141, виданий 13.12.2016, Диплом кандидата наук ДК 025900, виданий 13.10.2004, Атестат доцента 12ДЦ 019379, виданий 03.07.2008, Атестат професора АП 002394, виданий 09.02.2021	21	Технології програмування захищених систем	Освіта та науковий ступінь відповідають тематиці дисципліни, наукова робота пов'язана з тематикою дисципліни. Автор понад 150 наукових публікацій за профілем кафедри (з них: 65 у періодичних наукових фахових виданнях, 12 публікацій включені до наукометричної бази Scopus: h-індекс в Scopus 5), 4 монографії. Відомості про підвищення кваліфікації: 1. Slovakia, Academic society of Michal Baludansky, 10.11.2019 - 15.11.2019, №23/05-2019, 15.11.2019 (120 hours or 3,6 credits ECTS) 2. Перші Київські державні курси іноземних мов, 09.07.2019 - 30.10.2019, свідоцтво про позашкільну освіту №25390 від 31.10.2019 3. Київський національний університет імені Тараса Шевченка, 09.02.2021, атестат професора АПN№002394 від 09.02.2021

							4. Академії EC-Council, Велікобританія, Security EXPERT GROUP, CND | Certified Network Defender v2, 18.04.2021 - 15.10.2021, Сертифікат від 15.10.2021 (180 год. / 4 кредити ЄКТС) 5. USAID Project "Cybersecurity for Critical Infrastructure in Ukraine", Malware Analysis, 14 June – 23 July 2021, Сертифікат після закінчення курсів, 2021 6. Академії EC-Council, Велікобританія, Security EXPERT GROUP, CEH | Certified Ethical Hacker v11, 16.05.2022 - 17.06.2022, Сертифікат від 17.06.2022 (180 год. / 4 кредити ЄКТС) 7. USAID Project "Cybersecurity for Critical Infrastructure in Ukraine", "Оцінювач результатів навчання здобувачів професійної кваліфікації у сфері інформаційних технологій та кібербезпеки", 20.06.2022 - 25.06.2022, Сертифікат після закінчення курсів, 2022 (60 год. / 2 2 кредити ЄКТС) 8. USAID Project "Cybersecurity for Critical Infrastructure in Ukraine", Pentration Testing, 11 July – 31 August 2022, Сертифікат після закінчення курсів, 2022, (180 год. / 4 кредити ЄКТС) Публікації за тематикою дисципліни: 1. Buchyk S., Yudin O., Ziubina R., Bondarenko I., Suprun O. (2021). Devising a method of protection against zero-day attacks based on an analytical model of changing the state of the network sandbox. Eastern-European Journal of Enterprise Technologies, 1/9 (109), 50–57. doi: http://journals.uran.ua/eejet/article/view/225646. 2. Buchyk S., Lukova-Chuiko N, Tolyupa S., Piatyhor V., Buchyk O. (2021) Diceware Password Generation

							Algorithm Modification based on Pseudo-Random Sequences. Cybersecurity Providing in Information and Telecommunication Systems II 2021, October 26, 2021, Kyiv, Ukraine, pp. 167–176. URL: http://ceur-ws.org/Vol-3188/paper15.pdf. 3. Buchyk S., Tolyupa S., Symonychenko Y., Symonychenko A., Platonenko A. (2021) Improvement of Steganographic Methods based on the Analysis of Image Color Models. Cybersecurity Providing in Information and Telecommunication Systems, January 28, 2021, Kyiv, Ukraine, pp. 117 –124. URL: http://ceur-ws.org/Vol-2923/paper13.pdf. 4. С. Бучик, С. Толюпа, О. Бучик, Д. Мовчан. Інструменти віртуальної лабораторії тестування співробітників для визначення готовності протидії фішинговим атакам. Інфокомунікаційні технології та електронна інженерія, Вип. 2, № 1, 2022. – С. 44–51. DOI: https://doi.org/10.23939/ictee2022.01.044 5. Бучик С. С. Програмування. Основи програмування в середовищі Microsoft Visual C++ : конспект лекцій / С. С. Бучик, Р. В. Нетребко. - Житомир : ЖВІ, 2016. - 204 с. 6. Бучик С.С. Програмування. Основи візуального програмування в середовищі Microsoft Visual C++: [конспект лекцій] / С.С. Бучик, І.О. Канкін, Р.В. Нетребко - Житомир: ЖВІ ДУТ, 2014. - 136с. 7. Державні інформаційні ресурси. Методологія побудови та захисту українського сегмента дерева ідентифікаторів : монографія / О. К. Юдін, С. С. Бучик. – К. : НАУ, 2018. – 319 с. 8. Бучик С. С. Захист інформації в інформаційно-телекомунікаційних системах : конспект

							лекцій / С. С. Бучик, Р. В. Нетребко. – Житомир : ЖВІ, 2018. – 196 с. 9. Толюпа С.В., Бучик С.С., Лукова-Чуйко Н.В., Фесенко А.О. Системи технічного захисту інформації. Навчальний посібник. – Житомир: ФОП Кирилюк І.В., ПП «Рута», 2022. – 364 с. 10. А. с. 74344 Україна. Комп'ютерна програма. Інформаційна система визначення функціонального профілю захищеності та рівня гарантій автоматизованої системи від несанкціонованого доступу (ОФПАС 2.0) / Бучик С.С., Нетребко Р.В. (Україна). – №75070; заявл. 22.08.17; опубл. 26.01.18, Бюл. № 47. – С. 142 - 143.
398995	Торошанко Олександр Станіславович	Асистент, Основне місце роботи	Факультет інформаційних технологій	Диплом магістра, Одеська національна академія зв'язку ім. О.С. Попова, рік закінчення: 2012, спеціальність: 092402 Інформаційні мережі зв'язку, Диплом кандидата наук DK 059383, виданий 09.02.2021	5	Сигнали та процеси в системах технічного захисту інформації	Освіта та науковий ступінь відповідають тематиці дисципліни. Наявність одного патенту на винахід або п'яти деклараційних патентів на винахід чи корисну модель, включаючи секретні, або наявність не менше п'яти свідоцтв про реєстрацію авторського права на твір. Торошанко О.С.,Толубко В.Б., Бугаєнко В.В., Ткаченко О.М., Холявкіна Т.В. Лічильник імпульсів з дискретно-плавним регулюванням коефіцієнта лічби. Опубл. 26.01.2022. – Бюл. № 4. С. 3.43. Торошанко О.С., Толубко В.Б., Бугаєнко В.В., Ткаченко О.М., Черевик В.М. Генератор низьких та інфранизьких частот. Опубл. 21.09.2022. – Бюл. № 38. С. 3.65. Торошанко О.С., Толубко В.Б., Бугаєнко В.В., Ткаченко О.М., Черевик В.М. Світловий сигналізатор стану електромережі. Опубл. 9.02.2022. – Бюл. № 6. С. 3.172 Публікації за тематикою дисципліни: 1. Торошанко О.С., Щебланін Ю.М.,

							Порівняльний аналіз ефективності схем виявлення перевантаження телекомунікаційної мережі, Безпека інформаційних інформаційних систем і технологій №2(6)2022, Київ 2022, С. 64-77 2. Торошанко О.С., Лемешко А. В., Торошанко А.І. Adaptive control of self similar traffic in multiservice telecommunication networks // Інфокомунікаційні та комп'ютерні технології. – 2022. – №2(04). – С. 3. Гладких В.М. Ієрархічна маршрутизація з балансуванням навантаження в сенсорних мережах / В.М. Гладких, О.С. Торошанко // Вісник Національного університету «Львівська політехніка»: Радіоелектроніка та телекомунікації. – 2017. – № 885. – С. 68-75. 4. Заруцкий В.А. энергосберегающая технология передачи данных в сети радиодатчиков с мобильными агентами / В.А. Заруцкий, Е.В. Толстикова, А.С. Торошанко // Збірник наукових праць Військового інституту Київського національного університету імені Тараса Шевченка». – 2017. – №58. – С. 13-19. 5. Торошанко О.С. Метод вимірювань у безпроводових сенсорних мережах датчиками з повільним дрейфом параметрів / О.С. Торошанко // Наукові праці ОНАЗ ім. О.С. Попова. – 2018. – №1. – С. 142-151. 6. Гладких В.М. Дослідження продуктивності сенсорної мережі: основні та додаткові показники ефективності / В.М. Гладких, О.С. Торошанко // Вісник Університету «Україна». Серія: Інформатика, обчислювальна

техніка та кібернетика. – 2019. – 1(22). – С. 240-246.
7. Vinogradov N. Development of the method to control telecommunication network congestion based on a neural model / N. Vinogradov, M. Stepanov, Ya. Toroshanko, V. Cherevyk, A. Savchenko, V. Hladkykh, O. Toroshanko, T. Uvarova // Восточно-Европейский журнал передовых технологий. – 2019. – № 2(9). – С. 67-73.
8. Торошанко О.С. Багатокрокова модель прогнозування та виявлення перевантаження телекомунікаційної мережі / О.С. Торошанко // Телекомунікаційні та інформаційні технології. – 2019. – № 2(63). – С. 35-43.
9. Торошанко О.С. система управління характеристиками безпроводової комунікаційної мережі/ О.С. Торошанко, А.Г. Захаржевський / Телекомунікаційні та інформаційні технології. – 2020.– №1(66). – С.33-44.
10. Заруцький В.О. Комбінований метод управління мережею радіодатчиків з мобільними агентами / В.О. Заруцький, О.В. Толстикова, О.С. Торошанко // Науково-технічна конференція молодих учених «Актуальні проблеми інформаційних технологій – АРІТ», Київський національний університет імені Тараса Шевченка, 8-10 листопада 2017 р. – С. 56-57.
11. Торошанко О.С. Корекція результатів вимірювань датчиків в безпроводових сенсорних мережах // XXXI Международная научная конференция «Актуальные научные исследования в современном мире». Секция: Технические науки. Переяслав-Хмельницкий государственный педагогический университет имени

Григория Сковороды, 26-27 ноября 2017 г. – Вип. 11(31), часть 10. – С. 57-62.
12. Торошанко О.С. Корекція дрейфу і калібрування датчиків в безпроводових сенсорних мережах / О.С. Торошанко, В.О.Заруцький // Науково-технічна конференція «Актуальні проблеми інформаційних технологій», 20-21 листопада 2018 р.. – Київський національний університет імені Тараса Шевченка. – С. 21-22.
13. Торошанко О.С. Зважений алгоритм кластеризації сенсорних мереж / О.С. Торошанко // XII міжнародна науково-технічна конференція «Проблеми інформатизації», 12-13 грудня 2018 р. – Київ: Державний університет телекомунікацій. – С. 51-52.
14. Заруцький В.О., Торошанко О.С. Самоконфігурована сенсорна мережа на основі технології мобільних агентів / В.О. Заруцький, О.С. Торошанко // XII міжнародна науково-технічна конференція «Проблеми інформатизації», 12-13 грудня 2018 р. – Київ: Державний університет телекомунікацій. – С. 52-53.
15. Vinohradov N. Eliminate Application Redundancy Using Local Processing Using Directional Diffusion with Mobile Agents / Nikolay Vinohradov, Mikhailo Stepanov, Valerii Hladkykh, Oleksandr Toroshanko, Andrii Skrypnychenko. // 2019 3rd International Conference on Advanced Information and Communications Technologies (AICT)", Lviv, Ukraine. – 2-6 July, 2019. – P. 360-364."
16. Торошанко О.С. Підвищення точності вимірювань в безпроводових сенсорних мережах з повільним дрейфом параметрів датчиків / О.С. Торошанко // IX

							Міжнародна науково-практична конференція «Інфокомунікації – сучасність та майбутнє», 12-15 листопада 2019 р., ОНАЗ ім. О.С. Попова. – С. 371-375. 17. Торошанко О.С. Управління потоками в сенсорних мережах на основі механізму спрямованої дифузії О.С. Торошанко // IX науково-технічна конференція «Сучасні інфокомунікаційні технології». – Київ, ДУТ. – 5 грудня 2019 р. – С. 238-239. 18. Торошанко О.С. Діагностика та ідентифікація несправностей в телекомунікаційних мережах з розпізнаванням типу відмови // Телекомунікаційні та інформаційні технології. – 2018.– №4(61). – С.62-70. Відомості про підвищення кваліфікації^: Навчання на курсах "Foundations of Computer and Network Security" within the 2022 Cybersecurity Summer Instructor Training Program under the USAID Cybersecurity for Critical Infrastructure in Ukraine Activity. 11 July – 31 August 2022.
398995	Торошанко Олександр Станіславович	Асистент, Основне місце роботи	Факультет інформаційних технологій	Диплом магістра, Одеська національна академія зв'язку ім. О.С. Попова, рік закінчення: 2012, спеціальність: 092402 Інформаційні мережі зв'язку, Диплом кандидата наук DK 059383, виданий 09.02.2021	5	Електроніка та мікросхемотехніка	Освіта та науковий ступінь відповідають тематиці дисципліни. Наявність одного патенту на винахід або п’яти деклараційних патентів на винахід чи корисну модель, включаючи секретні, або наявність не менше п’яти свідоцтв про реєстрацію авторського права на твір. Торошанко О.С.,Толубко В.Б., Бугаєнко В.В., Ткаченко О.М., Холявкіна Т.В. Лічильник імпульсів з дискретно-плавним регулюванням коефіцієнта лічби. Опубл. 26.01.2022. – Бюл. № 4. С. 3.43. Торошанко О.С., Толубко В.Б., Бугаєнко В.В., Ткаченко О.М., Черевик В.М.

							Генератор низьких та інфранизьких частот. Опубл. 21.09.2022. – Бюл. № 38. С. 3.65. Торошанко О.С., Толубко В.Б., Бугаєнко В.В., Ткаченко О.М., Черевик В.М. Світловий сигналізатор стану електромережі. Опубл. 9.02.2022. – Бюл. № 6. С. 3.172 Публікації за тематикою дисципліни: 1. Торошанко О.С., Щебланін Ю.М., Порівняльний аналіз ефективності схем виявлення перевантаження телекомунікаційної мережі, Безпека інформаційних інформаційних систем і технологій №2(6)2022, Київ 2022, С. 64-77 2. Торошанко О.С., Лемешко А. В., Торошанко А.І. Adaptive control of self similar traffic in multiservice telecommunication networks // Інфокомунікаційні та комп'ютерні технології. – 2022. – №2(04). – С. 3. Гладких В.М. Ієрархічна маршрутизація з балансуванням навантаження в сенсорних мережах / В.М. Гладких, О.С. Торошанко // Вісник Національного університету «Львівська політехніка»: Радіоелектроніка та телекомунікації. – 2017. – № 885. – С. 68-75. 4. Заруцкий В.А. энергосберегающая технология передачи данных в сети радиодатчиков с мобильными агентами / В.А. Заруцкий, Е.В. Толстикова, А.С. Торошанко // Збірник наукових праць Військового інституту Київського національного університету імені Тараса Шевченка». – 2017. – №58. – С. 13-19. 5. Торошанко О.С. Метод вимірювань у безпроводових сенсорних мережах датчиками з

повільним дрейфом параметрів / О.С. Торошанко // Наукові праці ОНАЗ ім. О.С. Попова. – 2018. – №1. – С. 142-151.
6. Гладких В.М. Дослідження продуктивності сенсорної мережі: основні та додаткові показники ефективності / В.М. Гладких, О.С. Торошанко // Вісник Університету «Україна». Серія: Інформатика, обчислювальна техніка та кібернетика. – 2019. – 1(22). – С. 240-246.
7. Vinogradov N. Development of the method to control telecommunication network congestion based on a neural model / N. Vinogradov, M. Stepanov, Ya. Toroshanko, V. Cherevyk, A. Savchenko, V. Hladkykh, O. Toroshanko, T. Uvarova // Восточно-Европейский журнал передовых технологий. – 2019. – № 2(9). – С. 67-73.
8. Торошанко О.С. Багатокрокова модель прогнозування та виявлення перевантаження телекомунікаційної мережі / О.С. Торошанко // Телекомунікаційні та інформаційні технології. – 2019. – № 2(63). – С. 35-43.
9. Торошанко О.С. система управління характеристиками безпроводової комунікаційної мережі/ О.С. Торошанко, А.Г. Захаржевський / Телекомунікаційні та інформаційні технології. – 2020.– №1(66). – С.33-44.
10. Заруцький В.О. Комбінований метод управління мережею радіодатчиків з мобільними агентами / В.О. Заруцький, О.В. Толстикова, О.С. Торошанко // Науково-технічна конференція молодих учених «Актуальні проблеми інформаційних технологій – АРІТ», Київський національний університет імені

Тараса Шевченка, 8-10 листопада 2017 р. – С. 56-57.
11. Торошанко О.С. Корекція результатів вимірювань датчиків в безпроводових сенсорних мережах // XXXI Международная научная конференция «Актуальные научные исследования в современном мире». Секция: Технические науки. Переяслав-Хмельницкий государственный педагогический университет имени Григория Сковороды, 26-27 ноября 2017 г. – Вип. 11(31), часть 10. – С. 57-62.
12. Торошанко О.С. Корекція дрейфу і калібрування датчиків в безпроводових сенсорних мережах / О.С. Торошанко, В.О.Заруцький // Науково-технічна конференція «Актуальні проблеми інформаційних технологій», 20-21 листопада 2018 р.. – Київський національний університет імені Тараса Шевченка. – С. 21-22.
13. Торошанко О.С. Зважений алгоритм кластеризації сенсорних мереж / О.С. Торошанко // XII міжнародна науково-технічна конференція «Проблеми інформатизації», 12-13 грудня 2018 р. – Київ: Державний університет телекомунікацій. – С. 51-52.
14. Заруцький В.О., Торошанко О.С. Самоконфігурована сенсорна мережа на основі технології мобільних агентів / В.О. Заруцький, О.С. Торошанко // XII міжнародна науково-технічна конференція «Проблеми інформатизації», 12-13 грудня 2018 р. – Київ: Державний університет телекомунікацій. – С. 52-53.
15. Vinohradov N. Eliminate Application Redundancy Using Local Processing Using Directional Diffusion with Mobile Agents / Nikolay Vinohradov, Mikhailo Stepanov, Valerii Hladkykh,

							Oleksandr Toroshanko, Andrii Skrypnychenko. // 2019 3rd International Conference on Advanced Information and Communications Technologies (AICT)", Lviv, Ukraine. – 2-6 July, 2019. – P. 360-364." 16. Торошанко О.С. Підвищення точності вимірювань в безпроводових сенсорних мережах з повільним дрейфом параметрів датчиків / О.С. Торошанко // IX Міжнародна науково-практична конференція «Інфокомунікації – сучасність та майбутнє», 12-15 листопада 2019 р., ОНАЗ ім. О.С. Попова. – С. 371-375. 17. Торошанко О.С. Управління потоками в сенсорних мережах на основі механізму спрямованої дифузії О.С. Торошанко // IX науково-технічна конференція «Сучасні інфокомунікаційні технології». – Київ, ДУТ. – 5 грудня 2019 р. – С. 238-239. 18. Торошанко О.С. Діагностика та ідентифікація несправностей в телекомунікаційних мережах з розпізнаванням типу відмови // Телекомунікаційні та інформаційні технології. – 2018.– №4(61). – С.62-70. Відомості про підвищення кваліфікації^: Навчання на курсах "Foundations of Computer and Network Security" within the 2022 Cybersecurity Summer Instructor Training Program under the USAID Cybersecurity for Critical Infrastructure in Ukraine Activity. 11 July – 31 August 2022
185330	Пархоменко Іван Іванович	доцент, Основне місце роботи	Факультет інформаційних технологій	Диплом кандидата наук ДК 015285, виданий 03.07.2002, Атестат доцента 12ДЦ 017184, виданий 21.06.2007	24	Архітектура комп'ютерних систем	Освіта та науковий ступінь відповідають тематиці дисципліни. Публікації за тематикою дисципліни: 1. Наконечний В.С., Толюпа С.В., Дружинін В.А., Лукова-Чуйко Н.В., Пархоменко І.І. «Методи та засоби

							підвищення ефективності функціонування радіотехнічних систем розпізнавання багатопозиційного базування» : монографія - К.: 2019. – 237 с. 2. S., Druzhynin V., Parkhomenko I. «Signature and statistical analyzers in the cyber attack detection system», Scientific and Practical Cyber Security Journal (SPCSJ) 2(3): 01-07 ISSN 2587-4667 Scientific Cyber Security Association (SCSA), C. 47-53. 3. Пархоменко І.І., Сторіжко А.С., Іващенко М.С. «Способи захисту інформації у об'єктах інтернету речей від загроз інформаційної безпеки», Вісник інженерної академії України випуск №1 – 2018. – С. 88- 91 (Фахове видання) 4. Serhii Toliupa, Mykola Brailovskyi, Ivan Parkhomenko «Building intrusion detection systems based on the basis of methods of intellectual analysis of data». "Informatyka, Automatyka, Pomiary w Gospodarce i Ochronie Środowiska" – IAPGOS Vol 8 No 4 (2018) pp. 28-31 2018; 8 (4): 28-31. (Іноземне видання) 5. Т. В. Бабенко, І.І. Пархоменко, Р.В. Зюбіна, Д.В. Палко «Захист інформації та передачі даних в корпоративних мережах з використанням програмно-апаратних засобів», Вісник інженерної академії України випуск №3 – 2018, с. 68 – 72 (Фахове видання) 6. Толюпа С. В., Пархоменко І. І., Кириленко А. І., Вадис К. А. «Захист корпоративної інформації на мобільних пристроях.», Збірник наукових праць «Моделювання та інформаційні системи в економіці», КНЕУ, 2020. №99 — С. 151 – 161 (Фахове видання) 7. Толюпа С. В., Одарченко Р. С., Пархоменко І. І., Даков С.Ю.

							«Виявлення атак в корпоративній мережі за допомогою правил нечіткої логіки», Наукоємні технології. – К.:НАУ, 2020. – № 4 (48). – С 470-477 (Фахове видання) 8. Толюпа С.В., Плющ О.Г., Пархоменко І.І. «Побудова систем виявлення вторгнень в інформаційно-телекомунікаційну мережу на основі методів інтелектуального розподілу даних», Збірник наукових праць «Військового інституту Київського національного університету імені Тараса Шевченка.», К.: ВІКНУ, 2020. № 68., -- С. 80-90. (Фахове видання) 9. Роман Сергійович Одарченко, Толюпа Сергій Васильович, Пархоменко Іван Іванович, Даков Сергій Юрійович Виявлення атак в корпоративній мережі за допомогою правил нечіткої логіки, «Наукоємні технології», Том 48, №4 (2020), с. 470-476 10. Serhii Toliupa, Oleksandr Pliushch, Ivan Parkhomenko «Побудова систем виявлення атак в інформаційних мережах на нейромережевих структурах», електронне фахове наукове видання "Кібербезпека: освіта, наука, техніка" том 2 №10. 2020. С. 169-183. (Електронне фахове наукове видання) 11. Toliupa S., Parkhomenko I., Antoniuk V. Method for Identification of Critical Information Infrastructure Objects of the State. CEUR Workshop Proceedingsthis link is disabled, 2021, 3179, pp. 262–271 12. С.Толюпа, І. Пархоменко, С. Штаненко. Модель системи протидії вторгненням в інформаційних системах. Інфокомунікаційні технології та електронна інженерія. №1. 2021. С. 86-95. 13. Serhii Toliupa, Ivan Parkhomenko, Ruslana Ziubina, Olga Veselska,

							Stanislaw Rajba, Kornel Warwas Detection of abnormal traffic and network intrusions based on multiple fuzzy rules. Knowledge-Based and Intelligent Information & Engineering Systems: Proceedings of the 26th International Conference KES2022 Procedia Computer Science Volume 207, 2022, Pages 44-53 14. Toliupa, S., Buchyk, S., Nakonechnyi, V., Parkhomenko, I., Lukova-Chuiko, N. Building an Intrusion Detection System in Critically Important Information Networks with Application of Data Mining Methods. Proceedings - 16th International Conference on Advanced Trends in Radioelectronics, Telecommunications and Computer Engineering, TCSET 2022, 2022, pp. 128–133 Відомості про підвищення кваліфікації: 1. Стажування в навчально-науковому інституті комп'ютерних інформаційних технологій Національного авіаційного університету з 20.09.2017-20.12.2017 Довідка № 03.02/2724 від 20.12.2017 2. Стажування в ТОВ «ДЕПС СОЛЮШЕНЗ» з 01.10.2020 по 31.12.2020 Сертифікат Серія DP №000132. 3. Certificate of completion Audit and Risk Management within the 2021 Cybersecuriti Summer Training Program under the USAID Project. 14 june - 23 july. 4. Certificate of completion Cloud Cybersecurity within the 2022 Cybersecurity Summer Instructor Training Program under the USAID Cybersecurity for Critical Infrastructure in Ukraine Activity. 11 July – 31 August 2022
352533	Ващіліна Олена Валеріївна	Доцент, Основне місце роботи	Факультет інформаційних технологій	Диплом спеціаліста, Київський університет ім. Тараса	18	Математичні основи в інформаційній та кібербезпеці	Освіта та науковий ступінь відповідають тематиці дисципліни, наукова робота пов'язана з тематикою

				Шевченка, рік закінчення: 1995, спеціальність: Прикладна математика, Диплом кандидата наук ДК 009881, виданий 14.03.2001, Атестат доцента 12ДЦ 019995, виданий 30.10.2008			дисципліни. Modelling Emergency Situations in the Drilling of Deep Boreholes/ V. Gulyayev, S. Glazunov, O. Glushakova, E. Vashchilina and etc. Cambridge Scholars Publisher, 2019. 512 p. (монографія). 1. Ващіліна О.В. Робоча програма навчальної дисципліни «Лінійна алгебра та аналітична геометрія» . КНУ, 2021. 2. Ващіліна О.В. Робоча програма навчальної дисципліни «Чисельні методи» . КНУ, 2021. 3. Ващіліна О.В. Робоча програма навчальної дисципліни «Дослідження операцій» . КНУ, 2021 4. Методичні рекомендації до виконання випускної кваліфікаційної роботи на здобуття ступеня вищої освіти «бакалавр» для студентів денної форми навчання зі спеціальності «Комп'ютерні науки» за освітньою програмою «Прикладне програмування» / В.Л. Плескач, О.В. Ващіліна, І.І. Гарко – електронне видання; Київський національний університет імені Тараса Шевченка. Київ, 2019. 64 с. 5. Методичні рекомендації до виконання курсової роботи для студентів денної форми навчання першого (бакалаврського) рівня освіти зі спеціальності 122 «Комп'ютерні науки» за освітньою програмою «Прикладне програмування» / В.Л. Плескач, О.В. Ващіліна, І.І. Гарко – електронне видання; Київський національний університет імені Тараса Шевчнка. Київ, 2019. 43 с. 6. Робоча програма та методичні вказівки до вивчення дисципліни "Теорія ймовірності та математична статистика" для студентів заочної

							форми навчання з напряму підготовки: 6.070101 «Транспортні технології (автомобільний транспорт)» / В.Г. Дегтярь, О.В. Ващіліна, Ю.О. Заєць, Л.В. Шевчук; Національний транспортний університет. Київ, 2018. 62 с. Публікації за тематикою дисципліни: 1. VM Yashchuk, MZ Galunov, IV Lebedyeva, OA Tarasenko, OM Navozenko, EV Vashchilina, AV Krech, M Yu Losytskyy, MA Dotsenko. Some peculiarities of triplet excitations dynamics in organic macromolecules and crystals. Molecular Crystals and Liquid Crystals, 27 Apr. 2022., P.1-11 (Index: Scopus) 2. Kostyantyn Grytsenko, Yurii Kolomzarov, Peter Lytvyn, Iryna Lebedyeva, Elena Vashchilina. Variations of morphology of fluoropolymer thin films versus deposition conditions. Surface Topography: Metrology and Properties, 2021. Vol. 9, No. 4, 045006 (Index: Index: Scopus та Web of Science) 3. M. Dekhtyaruk, M. Shao, S. Yang, Z. Kontrobayeva, E. Vashchilina. Automated system of freight traffic optimisation in the interaction of various modes of transport. Periodicals of Engineering and Natural Sciences. 2021. Vol. 9, No. 3, September 2021, P.844-857 (Index: Scopus) 4. Yaremenko L., Hevchuk A., Vuzh T., Vashchilina E., Yermolaieva M. Information Technologies of Accounting and Analysis in Modern Companies. International Journal of Computer Science and Network Security. 2021. Vol. 21, No. 5. P. 151-159. (Index:Web of Science) 5. Ващіліна О.В., Лебедєва І.В. Деякі особливості руху елементів бурильних установок. Вісник

							Київського національного університету імені Тараса Шевченка. Серія: фізико-математичні науки. 2020, № 1-2, С. 57-60. (фахове видання) 6. Ващіліна О.В., Лебедєва І.В., Білобрицька О.І. Моделювання та чисельне дослідження явища самозбурення коливань кружляння бурильного долота. Вісник Київського національного університету імені Тараса Шевченка. Серія: фізико-математичні науки. 2019, №1, С. 28-33. (фахове видання) 7. Шевчук Л. В., Ващіліна О. В., Лебедєва І.В., Баран С.А. Скінченно-елементний моніторинг напружено-деформованого стану дорожнього покриття з розшаруванням. Вісник Київського національного університету імені Тараса Шевченка. Серія: фізико-математичні науки. 2018, №3. С. 57 – 60. (фахове видання). Відомості про підвищення кваліфікації: 1. «Аудит процесів розробки, впровадження та супроводу інформаційних систем на відповідність міжнародному стандарту якості ISO 9001:2015», 180 годин, компанія «IQusion». 2. Свідоцтво про стажування № 265/10-20 від 16.03.2020 р. 3. «KNU Teach Week», 1 кредит ЄКТС, Київський національний університет імені Тараса Шевченка. 4. Сертифікат про підвищення кваліфікації від 01.03.2021 р. 5. «Digital Skills Pro», 1 кредит ЄКТС, Київський національний університет імені Тараса Шевченка. 6. Сертифікат про підвищення кваліфікації від 22.03.2021 р. 7. «Teachers Internship program», EPAM

							Systems, January – February 2022, 180 hours, сертифікат №750. 8. Наукове стажування у Каунаському технологічному університеті (Литовська Республіка) за програмою академічної мобільності з 16.03.2022 по 30.06.2022. Довідка про проходження стажування від 30.06.2022 р.
402045	Михальчук Інна Іванівна	асистент, Основне місце роботи	Факультет інформаційних технологій	Диплом спеціаліста, Київський міжнародний університет цивільної авіації, рік закінчення: 2000, спеціальність: 090702 Радіоелектронні пристрої, системи та комплекси, Диплом кандидата наук ДК 062594, виданий 27.09.2021	19	Комп'ютерна графіка та мультимедійні технології	Освіта та науковий ступінь відповідають тематиці дисципліни. Відомості про підвищення кваліфікації: 1. Національна академія педагогічних наук України. ДЗВО "Університет менеджменту освіти". Центральний інститут післядипломної освіти. Свідоцтво про підвищення кваліфікації СП 35830447/0980-21. Технології створення освітнього аудіовізуального контенту навчальних фільмів, кліпів, роликів тощо. Тема: Дистанційне тестування як форма контролю якості знань, умінь і навичок здобувачів освіти дистанційної форми навчання з дисципліни "Алгоритми та структури даних". 180 годин/6 кредитів. 18.06.2021 р. 2. Навчання на курсах "Advanced Malware" within the 2022 Cybersecurity Summer Instructor Training Program under the USAID Cybersecurity for Critical Infrastructure in Ukraine Activity. 11 July – 31 August 2022. Публікації за тематикою дисципліни: 1. Павлов В.Г. Михальчук І.І. Структурна організація та архітектура комп`ютерних систем. Конспект лекцій. – К.: Вид-во Нац. авіац. ун-ту «НАУ-друк», 2010. 2. Павлов В.Г. Михальчук І.І. Структурна

							організація та архітектура комп`ютерних систем. Лабораторний практикум. – К.: Вид-во Нац. авіац. ун-ту «НАУ-друк», 2010. С 3. Душеба В.В., Давидеко А.М., Фролова Н.Є.,Михальчук І.І., Кочурков А.А. Апаратні засоби персональних комп`ютерів (частина 1) Методичні вказівки до лаб. роб. для студентів спеціальностей: 7.160105 "Захист інформації в комп`ютерних системах та мережах", 7.160102 "Захист інформації з обмеженим доступом та автоматизація її обробки", 6.170101 "Безпека інформаційних і комунікаційних систем", 6.170103 "Управління інформаційною безпекою". –К.: Укрметтестстандарт, 2009. – 118. 4. Фролова Н. «Захист публічних точок доступу WI-FI» / Михальчук І, Тищенко О.; Нац. ун-т «Чернігівська політехніка». – Ч.: Редакційно-видавничий відділ Нац. ун-ту «Чернігівська політехніка», 2022. – с.123-134. ISSN 2411-5363 (print) ISSN 2519-4569 (online) 5. L.Y. Ilnitskyi “Forming Electromagnetic Field For Antenna Testing” L.V. Sibruk, I. I. Mykhalchuk, A.P. Slobodian; Telecommunications and Radio Engineering – 2022. – T.81, №2. – P. 13-24, Издатель Begel House Inc. Scopus. 6. Ilnitskyi L. Y., Sibruk L. V., Mykhalchuk I. I. Radio monitoring antenna for directional finding. Telecommunications and Radio Engineering. 2019. Vol. 78, № 8. P. 651–662. 7. Ільницкий Л.Я., Михальчук І.І., Щербина О.А. Моделирование поля излучения спиральной антенны. Электронное

							моделирование. - 2010. – Т.32. – №4. – С.61-73.

Таблиця 3. Матриця відповідності програмних результатів навчання, освітніх компонентів, методів навчання та оцінювання

Програмні результати навчання ОП	**ПРН відповідає результату навчання, визначеному стандартом вищої освіти (або охоплює його)**	**Обов'язкові освітні компоненти, що забезпечують ПРН**	**Методи навчання**	**Форми та методи оцінювання**
ПРН 39. - проводити атестацію (спираючись на облік та обстеження) режимних територій (зон), приміщень тощо в умовах додержання режиму секретності із фіксуванням результатів у відповідних документах	☒	Проектно-технологічна практика	консультації з керівником, вивчення документації, самостійна робота, виконання індивідуального завдання, підготовка звіту з практики	поточне оцінювання керівником, захист практики
		Комплексні системи захисту інформації	лекції, практичні та лабораторні заняття, самостійна робота	контрольні роботи, захист звітів з лабораторних та практичних робіт, іспит
		Науково-дослідна практика	консультації з керівником, вивчення документації, самостійна робота, виконання індивідуального завдання, підготовка звіту з практики	поточне оцінювання керівником, захист практики
		Кваліфікаційна робота бакалавра	самостійна робота, консультації з керівником	захист кваліфікаційної роботи
ПРН 38. - інтерпретувати результати проведення спеціальних вимірювань з використанням технічних засобів, контролю характеристик інформаційно-телекомунікаційних систем відповідно до вимог нормативних документів системи технічного захисту інформації	☒	Кваліфікаційна робота бакалавра	самостійна робота, консультації з керівником	захист кваліфікаційної роботи
		Науково-дослідна практика	консультації з керівником, вивчення документації, самостійна робота, виконання індивідуального завдання, підготовка звіту з практики	поточне оцінювання керівником, захист практики
		Проектно-технологічна практика	консультації з керівником, вивчення документації, самостійна робота, виконання індивідуального завдання, підготовка звіту з практики	поточне оцінювання керівником, захист практики
		Сигнали та процеси в системах технічного захисту інформації	лекції, практичні та лабораторні заняття, самостійна робота	контрольні роботи, захист звітів з лабораторних та практичних робіт, іспит
ПРН 37. - вимірювати параметри небезпечних та завадових сигналів під час інструментального контролю процесів захисту інформації та визначати ефективність захисту інформації від витоку	☒	Кваліфікаційна робота бакалавра	самостійна робота, консультації з керівником	захист кваліфікаційної роботи
		Науково-дослідна практика	консультації з керівником, вивчення документації, самостійна робота, виконання індивідуального завдання, підготовка звіту з практики	поточне оцінювання керівником, захист практики
		Проектно-технологічна практика	консультації з керівником, вивчення документації, самостійна робота, виконання індивідуального	поточне оцінювання керівником, захист практики

технічними каналами відповідно до вимог нормативних документів системи технічного захисту інформації			завдання, підготовка звіту з практики	
		Сигнали та процеси в системах технічного захисту інформації	лекції, практичні та лабораторні заняття, самостійна робота	контрольні роботи, захист звітів з лабораторних та практичних робіт, іспит
		Фізика	лекції, практичні та лабораторні заняття, самостійна робота	контрольні роботи, тести, захист звітів з лабораторних та практичних робіт, залік
ПРН 36. - виявляти небезпечні сигнали технічних засобів	☒	Сигнали та процеси в системах технічного захисту інформації	лекції, практичні та лабораторні заняття, самостійна робота	контрольні роботи, захист звітів з лабораторних та практичних робіт, іспит
		Кваліфікаційна робота бакалавра	самостійна робота, консультації з керівником	захист кваліфікаційної роботи
		Науково-дослідна практика	консультації з керівником, вивчення документації, самостійна робота, виконання індивідуального завдання, підготовка звіту з практики	поточне оцінювання керівником, захист практики
		Проектно-технологічна практика	консультації з керівником, вивчення документації, самостійна робота, виконання індивідуального завдання, підготовка звіту з практики	поточне оцінювання керівником, захист практики
		Комплексні системи захисту інформації	лекції, практичні та лабораторні заняття, самостійна робота	контрольні роботи, захист звітів з лабораторних та практичних робіт, іспит
ПРН 35. - вирішувати задачі забезпечення та супроводу комплексних систем захисту інформації, а також протидії несанкціонованому доступу до інформаційних ресурсів і процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах згідно встановленої політики інформаційної і\або кібербезпеки	☒	Комплексні системи захисту інформації	лекції, практичні та лабораторні заняття, самостійна робота	контрольні роботи, захист звітів з лабораторних та практичних робіт, іспит
		Проектно-технологічна практика	консультації з керівником, вивчення документації, самостійна робота, виконання індивідуального завдання, підготовка звіту з практики	поточне оцінювання керівником, захист практики
		Науково-дослідна практика	консультації з керівником, вивчення документації, самостійна робота, виконання індивідуального завдання, підготовка звіту з практики	поточне оцінювання керівником, захист практики
		Кваліфікаційна робота бакалавра	самостійна робота, консультації з керівником	захист кваліфікаційної роботи
ПРН 33. - вирішувати задачі забезпечення безперервності бізнес процесів організації на основі теорії ризиків	☒	Кваліфікаційна робота бакалавра	самостійна робота, консультації з керівником	захист кваліфікаційної роботи
		Управління інформаційною безпекою	лекції, практичні та лабораторні заняття, самостійна робота	контрольні роботи, тести, захист звітів з лабораторних та практичних робіт, іспит
		Проектно-технологічна практика	консультації з керівником, вивчення документації, самостійна робота, виконання індивідуального завдання, підготовка звіту з практики	поточне оцінювання керівником, захист практики
		Науково-дослідна практика	консультації з керівником, вивчення документації, самостійна робота, виконання індивідуального завдання, підготовка звіту з	поточне оцінювання керівником, захист практики

			практики	
ПРН 40. - інтерпретувати результати проведення спеціальних вимірювань з використанням технічних засобів, контролю характеристик ІТС відповідно до вимог нормативних документів системи технічного захисту інформації	☒	Проектно-технологічна практика	консультації з керівником, вивчення документації, самостійна робота, виконання індивідуального завдання, підготовка звіту з практики	поточне оцінювання керівником, захист практики
		Комплексні системи захисту інформації	лекції, практичні та лабораторні заняття, самостійна робота	контрольні роботи, захист звітів з лабораторних та практичних робіт, іспит
		Кваліфікаційна робота бакалавра	самостійна робота, консультації з керівником	захист кваліфікаційної роботи
		Науково-дослідна практика	консультації з керівником, вивчення документації, самостійна робота, виконання індивідуального завдання, підготовка звіту з практики	поточне оцінювання керівником, захист практики
ПРН 32. - вирішувати задачі управління процесами відновлення штатного функціонування інформаційно-телекомунікаційних систем з використанням процедур резервування згідно встановленої політики безпеки	☒	Кваліфікаційна робота бакалавра	самостійна робота, консультації з керівником	захист кваліфікаційної роботи
		Науково-дослідна практика	консультації з керівником, вивчення документації, самостійна робота, виконання індивідуального завдання, підготовка звіту з практики	поточне оцінювання керівником, захист практики
		Проектно-технологічна практика	консультації з керівником, вивчення документації, самостійна робота, виконання індивідуального завдання, підготовка звіту з практики	поточне оцінювання керівником, захист практики
		Інформаційні системи та мережі	лекції, практичні та лабораторні заняття, самостійна робота	контрольні роботи, тести, захист звітів з лабораторних та практичних робіт, іспит
		Архітектура комп'ютерних систем	лекції, практичні та лабораторні заняття, самостійна робота	контрольні роботи, тести, захист звітів з лабораторних та практичних робіт, залік
ПРН 31. - застосовувати теорії та методи захисту для забезпечення безпеки елементів інформаційно-телекомунікаційних систем	☒	Кваліфікаційна робота бакалавра	самостійна робота, консультації з керівником	захист кваліфікаційної роботи
		Науково-дослідна практика	консультації з керівником, вивчення документації, самостійна робота, виконання індивідуального завдання, підготовка звіту з практики	поточне оцінювання керівником, захист практики
		Сигнали та процеси в системах технічного захисту інформації	лекції, практичні та лабораторні заняття, самостійна робота	контрольні роботи, захист звітів з лабораторних та практичних робіт, іспит
		Проектно-технологічна практика	консультації з керівником, вивчення документації, самостійна робота, виконання індивідуального завдання, підготовка звіту з практики	поточне оцінювання керівником, захист практики
ПРН 30. - здійснювати оцінювання можливості несанкціонованого доступу до елементів інформаційно-телекомунікаційних систем	☒	Кваліфікаційна робота бакалавра	самостійна робота, консультації з керівником	захист кваліфікаційної роботи
		Науково-дослідна практика	консультації з керівником, вивчення документації, самостійна робота, виконання	поточне оцінювання керівником, захист практики
		Проектно-технологічна практика	консультації з керівником, вивчення документації,	поточне оцінювання керівником, захист

			самостійна робота, виконання індивідуального завдання, підготовка звіту з практики	практики
		Математичні основи в інформаційній та кібербезпеці	лекції, практичні та лабораторні заняття, самостійна робота	контрольні роботи, тести, захист звітів з лабораторних та практичних робіт, іспит
		Управління інформаційною безпекою	лекції, практичні та лабораторні заняття, самостійна робота	контрольні роботи, тести, захист звітів з лабораторних та практичних робіт, іспит
		Спеціальні математичні методи в інформаційній та кібербезпеці	лекції, практичні заняття, самостійна робота	контрольні роботи, захист звітів з практичних робіт, залік, іспит
ПРН 29. - здійснювати оцінювання можливості реалізації потенційних загроз інформації, що обробляється в інформаційно-телекомунікаційни х системах та ефективності використання комплексів засобів захисту в умовах реалізації загроз різних класів	☒	Кваліфікаційна робота бакалавра	самостійна робота, консультації з керівником	захист кваліфікаційної роботи
		Науково-дослідна практика	консультації з керівником, вивчення документації, самостійна робота, виконання індивідуального завдання, підготовка звіту з практики	поточне оцінювання керівником, захист практики
		Проектно-технологічна практика	консультації з керівником, вивчення документації, самостійна робота, виконання індивідуального завдання, підготовка звіту з практики	поточне оцінювання керівником, захист практики
		Математичні основи в інформаційній та кібербезпеці	лекції, практичні та лабораторні заняття, самостійна робота	контрольні роботи, тести, захист звітів з лабораторних та практичних робіт, іспит
		Теорія інформації та кодування	лекції, практичні заняття, самостійна робота	контрольна робота, захист звітів з практичних робіт, залік
		Спеціальні математичні методи в інформаційній та кібербезпеці	лекції, практичні заняття, самостійна робота	контрольні роботи, захист звітів з практичних робіт, залік, іспит
ПРН 34. - приймати участь у розробці та впровадженні стратегії інформаційної безпеки та кібербезпеки відповідно до цілей і завдань організації	☒	Кваліфікаційна робота бакалавра	самостійна робота, консультації з керівником	захист кваліфікаційної роботи
		Науково-дослідна практика	консультації з керівником, вивчення документації, самостійна робота, виконання індивідуального завдання, підготовка звіту з практики	поточне оцінювання керівником, захист практики
		Проектно-технологічна практика	консультації з керівником, вивчення документації, самостійна робота, виконання індивідуального завдання, підготовка звіту з практики	поточне оцінювання керівником, захист практики
		Вступ до кібернетичної безпеки	лекції, практичні заняття, самостійна робота	контрольні роботи, тести, захист звітів з практичних робіт, залік
		Управління інформаційною безпекою	лекції, практичні та лабораторні заняття, самостійна робота	контрольні роботи, тести, захист звітів з лабораторних та практичних робіт, іспит
ПРН 41. - забезпечувати неперервність	☒	Кваліфікаційна робота бакалавра	самостійна робота, консультації з керівником	захист кваліфікаційної роботи

процесу ведення журналів реєстрації подій та інцидентів на основі автоматизованих процедур		Науково-дослідна практика	консультації з керівником, вивчення документації, самостійна робота, виконання індивідуального завдання, підготовка звіту з практики	поточне оцінювання керівником, захист практики
		Проектно-технологічна практика	консультації з керівником, вивчення документації, самостійна робота, виконання індивідуального завдання, підготовка звіту з практики	поточне оцінювання керівником, захист практики
		Управління інформаційною безпекою	лекції, практичні та лабораторні заняття, самостійна робота	контрольні роботи, тести, захист звітів з лабораторних та практичних робіт, іспит
		Операційні системи та їх захист	лекції, лабораторні заняття, самостійна робота	контрольні роботи, захист звітів з лабораторних робіт, іспит
ПРН 44. - вирішувати задачі забезпечення безперервності бізнес-процесів організації на основі теорії ризиків та встановленої системи управління інформаційною безпекою, згідно з вітчизняними та міжнародними вимогами та стандартами	☒	Управління інформаційною безпекою	лекції, практичні та лабораторні заняття, самостійна робота	контрольні роботи, тести, захист звітів з лабораторних та практичних робіт, іспит
		Науково-дослідна практика	консультації з керівником, вивчення документації, самостійна робота, виконання індивідуального завдання, підготовка звіту з практики	поточне оцінювання керівником, захист практики
		Вибрані розділи трудового права і основ підприємницької діяльності	лекції, практичні заняття, самостійна робота	контрольні роботи, тести, захист звітів з практичних робіт, залік
		Кваліфікаційна робота бакалавра	самостійна робота, консультації з керівником	захист кваліфікаційної роботи
		Проектно-технологічна практика	консультації з керівником, вивчення документації, самостійна робота, виконання індивідуального завдання, підготовка звіту з практики	поточне оцінювання керівником, захист практики
ПРН 43. - застосовувати національні та міжнародні регулюючі акти в сфері інформаційної безпеки та/ або кібербезпеки для розслідування інцидентів	☒	Науково-дослідна практика	консультації з керівником, вивчення документації, самостійна робота, виконання індивідуального завдання, підготовка звіту з практики	поточне оцінювання керівником, захист практики
		Проектно-технологічна практика	консультації з керівником, вивчення документації, самостійна робота, виконання індивідуального завдання, підготовка звіту з практики	поточне оцінювання керівником, захист практики
		Кіберпростір та протидія кіберзлочинності	лекції, практичні та лабораторні заняття, самостійна робота	контрольні роботи, захист звітів з лабораторних та практичних робіт, іспит
		Управління інформаційною безпекою	лекції, практичні та лабораторні заняття, самостійна робота	контрольні роботи, тести, захист звітів з лабораторних та практичних робіт, іспит
		Кваліфікаційна робота бакалавра	самостійна робота, консультації з керівником	захист кваліфікаційної роботи
ПРН 45. - застосовувати різні класи політик інформаційної	☒	Кваліфікаційна робота бакалавра	самостійна робота, консультації з керівником	захист кваліфікаційної роботи
		Науково-дослідна	консультації з керівником,	поточне оцінювання

безпеки та/ або кібербезпеки, що базуються на ризик-орієнтованому контролі доступу до інформаційних активів		практика	вивчення документації, самостійна робота, виконання індивідуального завдання, підготовка звіту з практики	керівником, захист практики
		Проектно-технологічна практика	консультації з керівником, вивчення документації, самостійна робота, виконання індивідуального завдання, підготовка звіту з практики	поточне оцінювання керівником, захист практики
		Управління інформаційною безпекою	лекції, практичні та лабораторні заняття, самостійна робота	контрольні роботи, тести, захист звітів з лабораторних та практичних робіт, іспит
ПРН 46. - здійснювати аналіз та мінімізацію ризиків обробки інформації в інформаційно-телекомунікаційних системах	☒	Кваліфікаційна робота бакалавра	самостійна робота, консультації з керівником	захист кваліфікаційної роботи
		Науково-дослідна практика	консультації з керівником, вивчення документації, самостійна робота, виконання індивідуального завдання, підготовка звіту з практики	поточне оцінювання керівником, захист практики
		Проектно-технологічна практика	консультації з керівником, вивчення документації, самостійна робота, виконання індивідуального завдання, підготовка звіту з практики	поточне оцінювання керівником, захист практики
		Захист інформації в інформаційних системах та мережах	лекції, практичні та лабораторні заняття, самостійна робота	контрольні роботи, захист звітів з лабораторних та практичних робіт, іспит
ПРН 47. - вирішувати задачі захисту інформації, що обробляється в інформаційно-телекомунікаційних системах з використанням сучасних методів та засобів криптографічного захисту інформації	☒	Науково-дослідна практика	консультації з керівником, вивчення документації, самостійна робота, виконання індивідуального завдання, підготовка звіту з практики	поточне оцінювання керівником, захист практики
		Кваліфікаційна робота бакалавра	самостійна робота, консультації з керівником	захист кваліфікаційної роботи
		Проектно-технологічна практика	консультації з керівником, вивчення документації, самостійна робота, виконання індивідуального завдання, підготовка звіту з практики	поточне оцінювання керівником, захист практики
		Захист інформації в інформаційних системах та мережах	лекції, практичні та лабораторні заняття, самостійна робота	контрольні роботи, захист звітів з лабораторних та практичних робіт, іспит
		Криптографічні системи захисту інформації	лекції, практичні та лабораторні заняття, самостійна робота	контрольні роботи, захист звітів з лабораторних та практичних робіт, іспит
		Теорія інформації та кодування	лекції, практичні заняття, самостійна робота	контрольна робота, захист звітів з практичних робіт, залік
		Технології програмування захищених систем	лекції, лабораторні заняття, самостійна робота	контрольні роботи, захист звітів з лабораторних робіт, іспит
ПРН 48. - виконувати впровадження та підтримку систем виявлення вторгнень та використовувати компоненти	☒	Кваліфікаційна робота бакалавра	самостійна робота, консультації з керівником	захист кваліфікаційної роботи
		Науково-дослідна практика	консультації з керівником, вивчення документації, самостійна робота, виконання індивідуального завдання, підготовка звіту з	поточне оцінювання керівником, захист практики

криптографічного захисту для забезпечення необхідного рівня захищеності інформації в інформаційно-телекомунікаційни х системах		~~практики~~		
		Проектно-технологічна практика	консультації з керівником, вивчення документації, самостійна робота, виконання індивідуального завдання, підготовка звіту з практики	поточне оцінювання керівником, захист практики
		Криптографічні системи захисту інформації	лекції, практичні та лабораторні заняття, самостійна робота	контрольні роботи, захист звітів з лабораторних та практичних робіт, іспит
		Теорія інформації та кодування	лекції, практичні заняття, самостійна робота	контрольна робота, захист звітів з практичних робіт, залік
ПРН 49. - забезпечувати належне функціонування системи моніторингу інформаційних ресурсів і процесів в інформаційно-телекомунікаційни х системах	☒	Кваліфікаційна робота бакалавра	самостійна робота, консультації з керівником	захист кваліфікаційної роботи
		Науково-дослідна практика	консультації з керівником, вивчення документації, самостійна робота, виконання індивідуального завдання, підготовка звіту з практики	поточне оцінювання керівником, захист практики
		Проектно-технологічна практика	консультації з керівником, вивчення документації, самостійна робота, виконання індивідуального завдання, підготовка звіту з практики	поточне оцінювання керівником, захист практики
		Операційні системи та їх захист	лекції, лабораторні заняття, самостійна робота	контрольні роботи, захист звітів з лабораторних робіт, іспит
ПРН 50. - забезпечувати функціонування програмних та програмно-апаратних комплексів виявлення вторгнень різних рівнів та класів (статистичних, сигнатурних, статистично-сигнатурних)	☒	Кваліфікаційна робота бакалавра	самостійна робота, консультації з керівником	захист кваліфікаційної роботи
		Науково-дослідна практика	консультації з керівником, вивчення документації, самостійна робота, виконання індивідуального завдання, підготовка звіту з практики	поточне оцінювання керівником, захист практики
		Проектно-технологічна практика	консультації з керівником, вивчення документації, самостійна робота, виконання індивідуального завдання, підготовка звіту з практики	поточне оцінювання керівником, захист практики
		Технології програмування захищених систем	лекції, лабораторні заняття, самостійна робота	контрольні роботи, захист звітів з лабораторних робіт, іспит
ПРН 51. - підтримувати працездатність та забезпечувати конфігурування систем виявлення вторгнень в інформаційно-телекомунікаційни х системах	☒	Науково-дослідна практика	консультації з керівником, вивчення документації, самостійна робота, виконання індивідуального завдання, підготовка звіту з практики	поточне оцінювання керівником, захист практики
		Проектно-технологічна практика	поточне оцінювання керівником, захист практики	консультації з керівником, вивчення документації, самостійна робота, виконання індивідуального завдання, підготовка звіту з практики
		Захист інформації в інформаційних системах та мережах	лекції, практичні та лабораторні заняття, самостійна робота	контрольні роботи, захист звітів з лабораторних та практичних робіт, іспит
		Управління інформаційною безпекою	лекції, практичні та лабораторні заняття, самостійна робота	контрольні роботи, тести, захист звітів з лабораторних та

				практичних робіт, іспит
		Кваліфікаційна робота бакалавра	самостійна робота, консультації з керівником	захист кваліфікаційної роботи
ПРН 52. - використовувати інструментарій для моніторингу процесів в інформаційно-телекомунікаційних системах	☒	Сигнали та процеси в системах технічного захисту інформації	лекції, практичні та лабораторні заняття, самостійна робота	контрольні роботи, захист звітів з лабораторних та практичних робіт, іспит
		Проектно-технологічна практика	консультації з керівником, вивчення документації, самостійна робота, виконання індивідуального завдання, підготовка звіту з практики	поточне оцінювання керівником, захист практики
		Кваліфікаційна робота бакалавра	самостійна робота, консультації з керівником	захист кваліфікаційної роботи
		Науково-дослідна практика	консультації з керівником, вивчення документації, самостійна робота, виконання індивідуального завдання, підготовка звіту з практики	поточне оцінювання керівником, захист практики
		Захист інформації в інформаційних системах та мережах	лекції, практичні та лабораторні заняття, самостійна робота	контрольні роботи, захист звітів з лабораторних та практичних робіт, іспит
ПРН 53. - вирішувати задачі аналізу програмного коду на наявність можливих загроз	☒	Кваліфікаційна робота бакалавра	самостійна робота, консультації з керівником	захист кваліфікаційної роботи
		Науково-дослідна практика	консультації з керівником, вивчення документації, самостійна робота, виконання індивідуального завдання, підготовка звіту з практики	поточне оцінювання керівником, захист практики
		Проектно-технологічна практика	консультації з керівником, вивчення документації, самостійна робота, виконання індивідуального завдання, підготовка звіту з практики	поточне оцінювання керівником, захист практики
		Технології програмування захищених систем	лекції, лабораторні заняття, самостійна робота	контрольні роботи, захист звітів з лабораторних робіт, іспит
ПРН 54. - усвідомлювати цінності громадянського (вільного демократичного) суспільства та необхідність його сталого розвитку, верховенства права, прав і свобод людини і громадянина в Україні	☒	Кваліфікаційна робота бакалавра	самостійна робота, консультації з керівником	захист кваліфікаційної роботи
		Науково-дослідна практика	консультації з керівником, вивчення документації, самостійна робота, виконання індивідуального завдання, підготовка звіту з практики	поточне оцінювання керівником, захист практики
		Вступ до кібернетичної безпеки	лекції, практичні заняття, самостійна робота	контрольні роботи, тести, захист звітів з практичних робіт, залік
		Національна та інформаційна безпека держави	лекції, семінарські та практичні заняття, самостійна робота	контрольні роботи, тести, захист звітів з практичних робіт, іспит
		Філософія	лекції, семінарські заняття, самостійна робота	контрольні роботи, іспит
		Українська та зарубіжна культура	лекції, семінарські заняття, самостійна робота	контрольна робота, тести, залік
		Вступ до університетських студій	лекції, самостійна робота	тест, залік
ПРН 8. - готувати	☒	Науково-дослідна	консультації з керівником,	поточне оцінювання

пропозиції до нормативних актів щодо забезпечення інформаційної та /або кібербезпеки захист кваліфікаційної роботи		практика	вивчення документації, самостійна робота, виконання індивідуального завдання, підготовка звіту з практики	керівником, захист практики
		Проектно-технологічна практика	консультації з керівником, вивчення документації, самостійна робота, виконання індивідуального завдання, підготовка звіту з практики	поточне оцінювання керівником, захист практики
		Кваліфікаційна робота бакалавра	самостійна робота, консультації з керівником	захист кваліфікаційної роботи
		Вибрані розділи трудового права і основ підприємницької діяльності	лекції, практичні заняття, самостійна робота	контрольні роботи, тести, захист звітів з практичних робіт, залік
ПРН 42. - впроваджувати процеси виявлення, ідентифікації, аналізу та реагування на інциденти інформаційної і/або кібербезпеки	☒	Кваліфікаційна робота бакалавра	самостійна робота, консультації з керівником	захист кваліфікаційної роботи
		Науково-дослідна практика	консультації з керівником, вивчення документації, самостійна робота, виконання індивідуального завдання, підготовка звіту з практики	поточне оцінювання керівником, захист практики
		Проектно-технологічна практика	консультації з керівником, вивчення документації, самостійна робота, виконання індивідуального завдання, підготовка звіту з практики	поточне оцінювання керівником, захист практики
		Управління інформаційною безпекою	лекції, практичні та лабораторні заняття, самостійна робота	контрольні роботи, тести, захист звітів з лабораторних та практичних робіт, іспит
ПРН 28. - аналізувати та проводити оцінку ефективності та рівня захищеності ресурсів різних класів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах в ході проведення випробувань згідно встановленої політики інформаційної та\або кібербезпеки	☒	Захист інформації в інформаційних системах та мережах	лекції, практичні та лабораторні заняття, самостійна робота	контрольні роботи, захист звітів з лабораторних та практичних робіт, іспит
		Кваліфікаційна робота бакалавра	самостійна робота, консультації з керівником	захист кваліфікаційної роботи
		Науково-дослідна практика	консультації з керівником, вивчення документації, самостійна робота, виконання індивідуального завдання, підготовка звіту з практики	поточне оцінювання керівником, захист практики
		Проектно-технологічна практика	консультації з керівником, вивчення документації, самостійна робота, виконання індивідуального завдання, підготовка звіту з практики	поточне оцінювання керівником, захист практики
ПРН 25. - забезпечувати введення підзвітності системи управління доступом до електронних інформаційних ресурсів і процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих	☒	Кваліфікаційна робота бакалавра	консультації з керівником, вивчення документації, самостійна робота, виконання індивідуального завдання, підготовка звіту з практики	поточне оцінювання керівником, захист практики
		Науково-дослідна практика	консультації з керівником, вивчення документації, самостійна робота, виконання індивідуального завдання, підготовка звіту з практики	поточне оцінювання керівником, захист практики
		Проектно-	консультації з керівником,	поточне оцінювання

) системах з використанням журналів реєстрації подій, їх аналізу та встановлених процедур захисту		технологічна практика	вивчення документації, самостійна робота, виконання індивідуального завдання, підготовка звіту з практики	керівником, захист практики
		Технології програмування захищених систем	лекції, лабораторні заняття, самостійна робота	контрольні роботи, захист звітів з лабораторних робіт, іспит
		Операційні системи та їх захист	лекції, лабораторні заняття, самостійна робота	контрольні роботи, захист звітів з лабораторних робіт, іспит
ПРН 26. - впроваджувати заходи та забезпечувати реалізацію процесів попередження отриманню несанкціонованого доступу і захисту інформаційних, інформаційно-телекомунікаційних (автоматизованих) систем на основі еталонної моделі взаємодії відкритих систем	☒	Кваліфікаційна робота бакалавра	самостійна робота, консультації з керівником	захист кваліфікаційної роботи
		Науково-дослідна практика	консультації з керівником, вивчення документації, самостійна робота, виконання індивідуального завдання, підготовка звіту з практики	поточне оцінювання керівником, захист практики
		Проектно-технологічна практика	консультації з керівником, вивчення документації, самостійна робота, виконання індивідуального завдання, підготовка звіту з практики	поточне оцінювання керівником, захист практики
		Захист інформації в інформаційних системах та мережах	лекції, практичні та лабораторні заняття, самостійна робота	контрольні роботи, захист звітів з лабораторних та практичних робіт, іспит
ПРН 27. - вирішувати задачі захисту потоків даних в інформаційних, інформаційно-телекомунікаційних (автоматизованих) системах	☒	Комплексні системи захисту інформації	лекції, практичні та лабораторні заняття, самостійна робота	контрольні роботи, захист звітів з лабораторних та практичних робіт, іспит
		Криптографічні системи захисту інформації	лекції, практичні та лабораторні заняття, самостійна робота	контрольні роботи, захист звітів з лабораторних та практичних робіт, іспит
		Теорія інформації та кодування	лекції, практичні заняття, самостійна робота	контрольна робота, захист звітів з практичних робіт, залік
		Проектно-технологічна практика	консультації з керівником, вивчення документації, самостійна робота, виконання індивідуального завдання, підготовка звіту з практики	поточне оцінювання керівником, захист практики
		Науково-дослідна практика	консультації з керівником, вивчення документації, самостійна робота, виконання індивідуального завдання, підготовка звіту з практики	поточне оцінювання керівником, захист практики
		Кваліфікаційна робота бакалавра	самостійна робота, консультації з керівником	захист кваліфікаційної роботи
ПРН 1. - застосовувати знання державної та іноземних мов з метою забезпечення ефективності професійної комунікації	☒	Кваліфікаційна робота бакалавра	самостійна робота, консультації з курівником	захист кваліфікаційної роботи
		Науково-дослідна практика	консультації з керівником, вивчення документації, самостійна робота, виконання індивідуального завдання, підготовка звіту з практики	поточне оцінювання керівником, захист практики
		Соціально-політичні студії	лекції, семінарські заняття, самостійна робота	тест, залік
		Вступ до кібернетичної безпеки	лекції, практичні заняття, самостійна робота	контрольні роботи, тести, захист звітів з практичних робіт, залік

		Іноземна мова	практичні заняття, самостійна робота	контрольні роботи, тести, захист звітів з практичних робіт, іспит
		Кіберпростір та протидія кіберзлочинності	лекції, практичні та лабораторні заняття, самостійна робота	контрольні роботи, захист звітів з лабораторних та практичних робіт, іспит
		Комплексні системи захисту інформації	лекції, практичні та лабораторні заняття, самостійна робота	контрольні роботи, захист звітів з лабораторних та практичних робіт, іспит
		Криптографічні системи захисту інформації	лекції, практичні та лабораторні заняття, самостійна робота	контрольні роботи, захист звітів з лабораторних та практичних робіт, іспит
		Теорія інформації та кодування	лекції, практичні заняття, самостійна робота	контрольні роботи, захист звітів з практичних робіт, залік
		Українська та зарубіжна культура	лекції, семінарські заняття, самостійна робота	контрольна робота, тести, залік
		Вступ до університетських студій	лекції, самостійна робота	тест, залік
ПРН 2. - організовувати власну професійну діяльність, обирати оптимальні методи та способи розв'язування складних спеціалізованих задач та практичних проблем у професійній діяльності, оцінювати їхню ефективність	☒	Науковий образ світу	лекції, самостійна робота	тест, залік
		Математичні основи в інформаційній та кібербезпеці	лекції, практичні та лабораторні заняття, самостійна робота	контрольні роботи, тести, захист звітів з лабораторних та практичних робіт, іспит
		Сигнали та процеси в системах технічного захисту інформації	лекції, практичні та лабораторні заняття, самостійна робота	контрольні роботи, захист звітів з лабораторних та практичних робіт, іспит
		Спеціальні математичні методи в інформаційній та кібербезпеці	лекції, практичні заняття, самостійна робота	контрольні роботи, захист звітів з практичних робіт, залік, іспит
		Проектно-технологічна практика	консультації з керівником, вивчення документації, самостійна робота, виконання індивідуального завдання, підготовка звіту з практики	поточне оцінювання керівником, захист практики
		Науково-дослідна практика	консультації з керівником, вивчення документації, самостійна робота, виконання індивідуального завдання, підготовка звіту з практики	поточне оцінювання керівником, захист практики
		Вибрані розділи трудового права і основ підприємницької діяльності	лекції, практичні заняття, самостійна робота	контрольні роботи, тести, захист звітів з практичних робіт, залік
		Кваліфікаційна робота бакалавра	самостійна робота, консультації з курівником	захист кваліфікаційної роботи
ПРН 3. - використовувати результати самостійного пошуку, аналізу та синтезу інформації з різних джерел для ефективного рішення спеціалізованих задач професійної діяльності	☒	Кваліфікаційна робота бакалавра	самостійна робота, консультації з курівником	захист кваліфікаційної роботи
		Науково-дослідна практика	консультації з керівником, вивчення документації, самостійна робота, виконання індивідуального завдання, підготовка звіту з практики	поточне оцінювання керівником, захист практики
		Вступ до кібернетичної безпеки	лекції, практичні заняття, самостійна робота	контрольні роботи, тести, захист звітів з практичних робіт, залік

		Науковий образ світу	лекції, самостійна робота	тест, залік
		Математичні основи в інформаційній та кібербезпеці	лекції, практичні та лабораторні заняття, самостійна робота	контрольні роботи, тести, захист звітів з лабораторних та практичних робіт, іспит
		Кіберпростір та протидія кіберзлочинності	лекції, практичні та лабораторні заняття, самостійна робота	контрольні роботи, захист звітів з лабораторних та практичних робіт, іспит
		Криптографічні системи захисту інформації	лекції, практичні та лабораторні заняття, самостійна робота	контрольні роботи, захист звітів з лабораторних та практичних робіт, іспит
		Теорія інформації та кодування	лекції, практичні заняття, самостійна робота	контрольна робота, захист звітів з практичних робіт, залік
		Сигнали та процеси в системах технічного захисту інформації	лекції, практичні та лабораторні заняття, самостійна робота	контрольні роботи, захист звітів з лабораторних та практичних робіт, іспит
		Технології програмування захищених систем	лекції, лабораторні заняття, самостійна робота	контрольні роботи, захист звітів з лабораторних робіт, іспит
		Національна та інформаційна безпека держави	лекції, семінарські та практичні заняття, самостійна робота	контрольні роботи, тести, захист звітів з практичних робіт, іспит
		Фізика	лекції, практичні та лабораторні заняття, самостійна робота	контрольні роботи, тести, захист звітів з лабораторних та практичних робіт, залік
ПРН 4. - аналізувати, аргументувати, приймати рішення при розв'язанні складних спеціалізованих задач та практичних проблем у професійній діяльності, які характеризуються комплексністю та неповною визначеністю умов, відповідати за прийняті рішення	☒	Кваліфікаційна робота бакалавра	самостійна робота, консультації з курівником	захист кваліфікаційної роботи
		Науково-дослідна практика	консультації з керівником, вивчення документації, самостійна робота, виконання індивідуального завдання, підготовка звіту з практики	поточне оцінювання керівником, захист практики
		Математичні основи в інформаційній та кібербезпеці	лекції, практичні та лабораторні заняття, самостійна робота	контрольні роботи, тести, захист звітів з лабораторних та практичних робіт, іспит
		Науковий образ світу	лекції, самостійна робота	тест, залік
		Національна та інформаційна безпека держави	лекції, семінарські та практичні заняття, самостійна робота	контрольні роботи, тести, захист звітів з практичних робіт, іспит
		Спеціальні математичні методи в інформаційній та кібербезпеці	лекції, практичні заняття, самостійна робота	контрольні роботи, захист звітів з практичних робіт, залік, іспит
		Філософія	лекції, семінарські заняття, самостійна робота	контрольні роботи, іспит
ПРН 5. - адаптуватися в умовах частої зміни технологій професійної діяльності, прогнозувати кінцевий результат	☒	Кваліфікаційна робота бакалавра	самостійна робота, консультації з курівником	захист кваліфікаційної роботи
		Науково-дослідна практика	консультації з керівником, вивчення документації, самостійна робота, виконання індивідуального завдання, підготовка звіту з практики	поточне оцінювання керівником, захист практики
		Основи екології	лекції, практичні заняття, самостійна робота	контрольні роботи, тести, захист звітів з практичних робіт, залік
		Науковий образ світу	лекції, самостійна робота	тест, залік

		Комплексні системи захисту інформації	лекції, практичні та лабораторні заняття, самостійна робота	контрольні роботи, захист звітів з лабораторних та практичних робіт, іспит
		Криптографічні системи захисту інформації	лекції, практичні та лабораторні заняття, самостійна робота	контрольні роботи, захист звітів з лабораторних та практичних робіт, іспит
ПРН 7. - діяти на основі законодавчої та нормативно-правової бази України та вимог відповідних стандартів, у тому числі міжнародних в галузі інформаційної та /або кібербезпеки	☒	Національна та інформаційна безпека держави	лекції, семінарські та практичні заняття, самостійна робота	контрольні роботи, тести, захист звітів з практичних робіт, іспит
		Криптографічні системи захисту інформації	лекції, практичні та лабораторні заняття, самостійна робота	контрольні роботи, захист звітів з лабораторних та практичних робіт, іспит
		Комплексні системи захисту інформації	лекції, практичні та лабораторні заняття, самостійна робота	контрольні роботи, захист звітів з лабораторних та практичних робіт, іспит
		Кіберпростір та протидія кіберзлочинності	лекції, практичні та лабораторні заняття, самостійна робота	контрольні роботи, захист звітів з лабораторних та практичних робіт, іспит
		Вибрані розділи трудового права і основ підприємницької діяльності	лекції, практичні заняття, самостійна робота	контрольні роботи, тести, захист звітів з практичних робіт, залік
		Кваліфікаційна робота бакалавра	самостійна робота, консультації з курівником	захист кваліфікаційної роботи
		Науково-дослідна практика	консультації з керівником, вивчення документації, самостійна робота, виконання індивідуального завдання, підготовка звіту з практики	поточне оцінювання керівником, захист практики
		Проектно-технологічна практика	консультації з керівником, вивчення документації, самостійна робота, виконання індивідуального завдання, підготовка звіту з практики	поточне оцінювання керівником, захист практики
		Управління інформаційною безпекою	лекції, практичні та лабораторні заняття, самостійна робота	контрольні роботи, тести, захист звітів з лабораторних та практичних робіт, іспит
ПРН 9. - впроваджувати процеси, що базуються на національних та міжнародних стандартах, виявлення, ідентифікації, аналізу та реагування на інциденти інформаційної та кібербезпеки	☒	Кваліфікаційна робота бакалавра	самостійна робота, консультації з керівником	захист кваліфікаційної роботи
		Науково-дослідна практика	консультації з керівником, вивчення документації, самостійна робота, виконання індивідуального завдання, підготовка звіту з практики	поточне оцінювання керівником, захист практики
		Проектно-технологічна практика	консультації з керівником, вивчення документації, самостійна робота, виконання індивідуального завдання, підготовка звіту з практики	поточне оцінювання керівником, захист практики
		Управління інформаційною безпекою	лекції, практичні та лабораторні заняття, самостійна робота	контрольні роботи, тести, захист звітів з лабораторних та практичних робіт, іспит
		Національна та інформаційна безпека держави	лекції, семінарські та практичні заняття, самостійна робота	контрольні роботи, тести, захист звітів з практичних робіт, іспит
ПРН 10. -	☒	Кваліфікаційна робота	самостійна робота,	захист кваліфікаційної

виконувати аналіз та декомпозицію інформаційно-телекомунікаційних систем		бакалавра	консультації з керівником	роботи
		Науково-дослідна практика	консультації з керівником, вивчення документації, самостійна робота, виконання індивідуального завдання, підготовка звіту з практики	поточне оцінювання керівником, захист практики
		Проектно-технологічна практика	консультації з керівником, вивчення документації, самостійна робота, виконання індивідуального завдання, підготовка звіту з практики	поточне оцінювання керівником, захист практики
		Технології програмування захищених систем	лекції, лабораторні заняття, самостійна робота	контрольні роботи, захист звітів з лабораторних робіт, іспит
		Інформаційні технології в кіберпросторі	лекції, практичні та лабораторні заняття, самостійна робота	контрольні роботи, тести, захист звітів з лабораторних та практичних робіт, іспит
ПРН 11. - виконувати аналіз зв'язків між інформаційними процесами на віддалених обчислювальних системах	☒	Інформаційні системи та мережі	лекції, практичні та лабораторні заняття, самостійна робота	контрольні роботи, тести, захист звітів з лабораторних та практичних робіт, іспит
		Проектно-технологічна практика	консультації з керівником, вивчення документації, самостійна робота, виконання індивідуального завдання, підготовка звіту з практики	поточне оцінювання керівником, захист практики
		Науково-дослідна практика	консультації з керівником, вивчення документації, самостійна робота, виконання індивідуального завдання, підготовка звіту з практики	поточне оцінювання керівником, захист практики
		Кваліфікаційна робота бакалавра	самостійна робота, консультації з керівником	захист кваліфікаційної роботи
ПРН 12. - розробляти моделі загроз та порушника	☒	Національна та інформаційна безпека держави	лекції, семінарські та практичні заняття, самостійна робота	контрольні роботи, тести, захист звітів з практичних робіт, іспит
		Кваліфікаційна робота бакалавра	самостійна робота, консультації з керівником	захист кваліфікаційної роботи
		Науково-дослідна практика	консультації з керівником, вивчення документації, самостійна робота, виконання індивідуального завдання, підготовка звіту з практики	поточне оцінювання керівником, захист практики
		Проектно-технологічна практика	консультації з керівником, вивчення документації, самостійна робота, виконання індивідуального завдання, підготовка звіту з практики	поточне оцінювання керівником, захист практики
		Управління інформаційною безпекою	лекції, практичні та лабораторні заняття, самостійна робота	контрольні роботи, тести, захист звітів з лабораторних та практичних робіт, іспит
ПРН 6. - критично осмислювати основні теорії, принципи, методи і поняття у навчанні та професійній	☒	Кваліфікаційна робота бакалавра	самостійна робота, консультації з керівником	захист кваліфікаційної роботи
		Науково-дослідна практика	консультації з керівником, вивчення документації, самостійна робота, виконання індивідуального	поточне оцінювання керівником, захист практики

діяльності			завдання, підготовка звіту з практики	
		Науковий образ світу	лекції, самостійна робота	тест, залік
		Криптографічні системи захисту інформації	лекції, практичні та лабораторні заняття, самостійна робота	контрольні роботи, захист звітів з лабораторних та практичних робіт, іспит
		Теорія інформації та кодування	лекції, практичні заняття, самостійна робота	контрольна робота, захист звітів з практичних робіт, залік
		Сигнали та процеси в системах технічного захисту інформації	лекції, практичні та лабораторні заняття, самостійна робота	контрольні роботи, захист звітів з лабораторних та практичних робіт, іспит
		Спеціальні математичні методи в інформаційній та кібербезпеці	лекції, практичні заняття, самостійна робота	контрольні роботи, захист звітів з практичних робіт, залік, іспит
		Філософія	лекції, семінарські заняття, самостійна робота	контрольні роботи, іспит
ПРН 14. - вирішувати завдання захисту програм та інформації, що обробляється в інформаційно-телекомунікаційних системах програмно-апаратними засобами та давати оцінку результативності якості прийнятих рішень	☒	Науково-дослідна практика	консультації з керівником, вивчення документації, самостійна робота, виконання індивідуального завдання, підготовка звіту з практики	поточне оцінювання керівником, захист практики
		Проектно-технологічна практика	консультації з керівником, вивчення документації, самостійна робота, виконання індивідуального завдання, підготовка звіту з практики	поточне оцінювання керівником, захист практики
		Основи алгоритмізації та програмування	лекції, практичні та лабораторні заняття, самостійна робота	контрольні роботи, тести, захист звітів з лабораторних та практичних робіт, іспит
		Захист інформації в інформаційних системах та мережах	лекції, практичні та лабораторні заняття, самостійна робота	контрольні роботи, захист звітів з лабораторних та практичних робіт, іспит
		Комплексні системи захисту інформації	лекції, практичні та лабораторні заняття, самостійна робота	контрольні роботи, захист звітів з лабораторних та практичних робіт, іспит
		Технології програмування захищених систем	лекції, лабораторні заняття, самостійна робота	контрольні роботи, захист звітів з лабораторних робіт, іспит
		Інформаційні технології в кіберпросторі	лекції, практичні та лабораторні заняття, самостійна робота	контрольні роботи, тести, захист звітів з лабораторних та практичних робіт, іспит
		Кваліфікаційна робота бакалавра	самостійна робота, консультації з керівником	захист кваліфікаційної роботи
ПРН 24. - вирішувати задачі управління доступом до інформаційних ресурсів та процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах на основі моделей управління доступом	☒	Кваліфікаційна робота бакалавра	самостійна робота, консультації з керівником	захист кваліфікаційної роботи
		Науково-дослідна практика	консультації з керівником, вивчення документації, самостійна робота, виконання індивідуального завдання, підготовка звіту з практики	поточне оцінювання керівником, захист практики
		Проектно-технологічна практика	консультації з керівником, вивчення документації, самостійна робота, виконання індивідуального завдання, підготовка звіту з практики	поточне оцінювання керівником, захист практики

(мандатних, дискреційних, рольових)		Управління інформаційною безпекою	лекції, практичні та лабораторні заняття, самостійна робота	контрольні роботи, тести, захист звітів з лабораторних та практичних робіт, іспит
		Технології програмування захищених систем	лекції, лабораторні заняття, самостійна робота	контрольні роботи, захист звітів з лабораторних робіт, іспит
		Операційні системи та їх захист	лекції, лабораторні заняття, самостійна робота	контрольні роботи, захист звітів з лабораторних робіт, іспит
ПРН 23. - реалізовувати заходи з протидії отриманню несанкціонованого доступу до інформаційних ресурсів і процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах	☒	Кваліфікаційна робота бакалавра	самостійна робота, консультації з керівником	захист кваліфікаційної роботи
		Науково-дослідна практика	консультації з керівником, вивчення документації, самостійна робота, виконання індивідуального завдання, підготовка звіту з практики	поточне оцінювання керівником, захист практики
		Проектно-технологічна практика	консультації з керівником, вивчення документації, самостійна робота, виконання індивідуального завдання, підготовка звіту з практики	поточне оцінювання керівником, захист практики
		Комплексні системи захисту інформації	лекції, практичні та лабораторні заняття, самостійна робота	контрольні роботи, захист звітів з лабораторних та практичних робіт, іспит
		Інформаційні системи та мережі	лекції, практичні та лабораторні заняття, самостійна робота	контрольні роботи, тести, захист звітів з лабораторних та практичних робіт, іспит
		Архітектура комп'ютерних систем	лекції, практичні та лабораторні заняття, самостійна робота	контрольні роботи, тести, захист звітів з лабораторних та практичних робіт, залік
		Технології програмування захищених систем	лекції, лабораторні заняття, самостійна робота	контрольні роботи, захист звітів з лабораторних робіт, іспит
		Операційні системи та їх захист	лекції, лабораторні заняття, самостійна робота	контрольні роботи, захист звітів з лабораторних робіт, іспит
ПРН 22. - вирішувати задачі управління процедурами ідентифікації, автентифікації, авторизації процесів і користувачів в інформаційно-телекомунікаційних системах згідно встановленої політики інформаційної і\або кібербезпеки	☒	Кваліфікаційна робота бакалавра	самостійна робота, консультації з керівником	захист кваліфікаційної роботи
		Науково-дослідна практика	консультації з керівником, вивчення документації, самостійна робота, виконання індивідуального завдання, підготовка звіту з практики	поточне оцінювання керівником, захист практики
		Проектно-технологічна практика	консультації з керівником, вивчення документації, самостійна робота, виконання індивідуального завдання, підготовка звіту з практики	поточне оцінювання керівником, захист практики
		Кіберпростір та протидія кіберзлочинності	лекції, практичні та лабораторні заняття, самостійна робота	контрольні роботи, захист звітів з лабораторних та практичних робіт, іспит
		Захист інформації в інформаційних системах та мережах	лекції, практичні та лабораторні заняття, самостійна робота	контрольні роботи, захист звітів з лабораторних та практичних робіт, іспит
		Комплексні системи захисту інформації	лекції, практичні та лабораторні заняття,	контрольні роботи, захист звітів з лабораторних та

			~~самостійна робота~~	~~практичних робіт, іспит~~
		Технології програмування захищених систем	лекції, лабораторні заняття, самостійна робота	контрольні роботи, захист звітів з лабораторних робіт, іспит
		Операційні системи та їх захист	лекції, лабораторні заняття, самостійна робота	контрольні роботи, захист звітів з лабораторних робіт, іспит
ПРН 21. - вирішувати задачі забезпечення та супроводу (в.т. числі: огляд, тестування, підзвітність) системи управління доступом згідно встановленої політики безпеки в інформаційних та інформаційно-телекомунікаційни х (автоматизованих) системах	☒	Управління інформаційною безпекою	лекції, практичні та лабораторні заняття, самостійна робота	контрольні роботи, тести, захист звітів з лабораторних та практичних робіт, іспит
		Захист інформації в інформаційних системах та мережах	лекції, практичні та лабораторні заняття, самостійна робота	контрольні роботи, захист звітів з лабораторних та практичних робіт, іспит
		Проектно-технологічна практика	консультації з керівником, вивчення документації, самостійна робота, виконання індивідуального завдання, підготовка звіту з практики	поточне оцінювання керівником, захист практики
		Кваліфікаційна робота бакалавра	самостійна робота, консультації з керівником	захист кваліфікаційної роботи
		Науково-дослідна практика	консультації з керівником, вивчення документації, самостійна робота, виконання індивідуального завдання, підготовка звіту з практики	поточне оцінювання керівником, захист практики
ПРН 20. - забезпечувати функціонування спеціального програмного забезпечення, щодо захисту інформації від руйнуючих програмних впливів, руйнуючих кодів в інформаційно-телекомунікаційни х системах	☒	Кваліфікаційна робота бакалавра	самостійна робота, консультації з керівником	захист кваліфікаційної роботи
		Науково-дослідна практика	консультації з керівником, вивчення документації, самостійна робота, виконання індивідуального завдання, підготовка звіту з практики	поточне оцінювання керівником, захист практики
		Проектно-технологічна практика	консультації з керівником, вивчення документації, самостійна робота, виконання індивідуального завдання, підготовка звіту з практики	поточне оцінювання керівником, захист практики
		Захист інформації в інформаційних системах та мережах	лекції, практичні та лабораторні заняття, самостійна робота	контрольні роботи, захист звітів з лабораторних та практичних робіт, іспит
ПРН 13. - аналізувати проекти інформаційно-телекомунікаційни х систем базуючись на стандартизованих технологіях та протоколах передачі даних	☒	Кваліфікаційна робота бакалавра	самостійна робота, консультації з керівником	захист кваліфікаційної роботи
		Науково-дослідна практика	консультації з керівником, вивчення документації, самостійна робота, виконання індивідуального завдання, підготовка звіту з практики	поточне оцінювання керівником, захист практики
		Проектно-технологічна практика	консультації з керівником, вивчення документації, самостійна робота, виконання індивідуального завдання, підготовка звіту з практики	поточне оцінювання керівником, захист практики
		Інформаційні системи та мережі	лекції, практичні та лабораторні заняття, самостійна робота	контрольні роботи, тести, захист звітів з лабораторних та практичних робіт, іспит
ПРН 18. -	☒	Кваліфікаційна робота	самостійна робота,	захист кваліфікаційної

використовувати програмні та програмно-апаратні комплекси захисту інформаційних ресурсів		~~бакалавра~~	~~консультації з керівником~~	~~роботи~~
		Науково-дослідна практика	консультації з керівником, вивчення документації, самостійна робота, виконання індивідуального завдання, підготовка звіту з практики	поточне оцінювання керівником, захист практики
		Проектно-технологічна практика	консультації з керівником, вивчення документації, самостійна робота, виконання індивідуального завдання, підготовка звіту з практики	поточне оцінювання керівником, захист практики
		Захист інформації в інформаційних системах та мережах	лекції, практичні та лабораторні заняття, самостійна робота	контрольні роботи, захист звітів з лабораторних та практичних робіт, іспит
		Комплексні системи захисту інформації	лекції, практичні та лабораторні заняття, самостійна робота	контрольні роботи, захист звітів з лабораторних та практичних робіт, іспит
		Операційні системи та їх захист	лекції, лабораторні заняття, самостійна робота	контрольні роботи, захист звітів з лабораторних робіт, іспит
		Інформаційні технології в кіберпросторі	лекції, практичні та лабораторні заняття, самостійна робота	контрольні роботи, тести, захист звітів з лабораторних та практичних робіт, іспит
ПРН 17. - забезпечувати процеси захисту та функціонування інформаційно-телекомунікаційних (автоматизованих) систем на основі практик, навичок та знань, щодо структурних (структурно-логічних) схем, топології мережі, сучасних архітектур та моделей захисту електронних інформаційних ресурсів з відображенням взаємозв'язків та інформаційних потоків, процесів для внутрішніх і віддалених компонент	☒	Кваліфікаційна робота бакалавра	самостійна робота, консультації з керівником	захист кваліфікаційної роботи
		Науково-дослідна практика	консультації з керівником, вивчення документації, самостійна робота, виконання індивідуального завдання, підготовка звіту з практики	поточне оцінювання керівником, захист практики
		Проектно-технологічна практика	консультації з керівником, вивчення документації, самостійна робота, виконання індивідуального завдання, підготовка звіту з практики	поточне оцінювання керівником, захист практики
		Захист інформації в інформаційних системах та мережах	лекції, практичні та лабораторні заняття, самостійна робота	контрольні роботи, захист звітів з лабораторних та практичних робіт, іспит
		Комплексні системи захисту інформації	лекції, практичні та лабораторні заняття, самостійна робота	контрольні роботи, захист звітів з лабораторних та практичних робіт, іспит
		Інформаційні системи та мережі	лекції, практичні та лабораторні заняття, самостійна робота	контрольні роботи, тести, захист звітів з лабораторних та практичних робіт, іспит
ПРН 16. - реалізовувати комплексні системи захисту інформації в автоматизованих системах (АС) організації (підприємства) відповідно до вимог нормативно-правових документів	☒	Кваліфікаційна робота бакалавра	самостійна робота, консультації з керівником	захист кваліфікаційної роботи
		Науково-дослідна практика	консультації з керівником, вивчення документації, самостійна робота, виконання індивідуального завдання, підготовка звіту з практики	поточне оцінювання керівником, захист практики
		Проектно-технологічна практика	консультації з керівником, вивчення документації, самостійна робота, виконання індивідуального завдання, підготовка звіту з практики	поточне оцінювання керівником, захист практики

		Комплексні системи захисту інформації	лекції, практичні та лабораторні заняття, самостійна робота	контрольні роботи, захист звітів з лабораторних та практичних робіт, іспит
ПРН 19. - застосовувати теорії та методи захисту для забезпечення безпеки інформації в інформаційно-телекомунікаційних системах	☒	Кваліфікаційна робота бакалавра	самостійна робота, консультації з керівником	захист кваліфікаційної роботи
		Науково-дослідна практика	консультації з керівником, вивчення документації, самостійна робота, виконання індивідуального завдання, підготовка звіту з практики	поточне оцінювання керівником, захист практики
		Проектно-технологічна практика	консультації з керівником, вивчення документації, самостійна робота, виконання індивідуального завдання, підготовка звіту з практики	поточне оцінювання керівником, захист практики
		Комплексні системи захисту інформації	лекції, практичні та лабораторні заняття, самостійна робота	контрольні роботи, захист звітів з лабораторних та практичних робіт, іспит
		Теорія інформації та кодування	лекції, практичні заняття, самостійна робота	контрольна робота, захист звітів з практичних робіт, залік
		Технології програмування захищених систем	лекції, лабораторні заняття, самостійна робота	контрольні роботи, захист звітів з лабораторних робіт, іспит
ПРН 15. - використовувати сучасне програмно-апаратне забезпечення інформаційно-комунікаційних технологій	☒	Інформаційні технології в кіберпросторі	лекції, практичні та лабораторні заняття, самостійна робота	контрольні роботи, тести, захист звітів з лабораторних та практичних робіт, іспит
		Технології програмування захищених систем	лекції, лабораторні заняття, самостійна робота	контрольні роботи, захист звітів з лабораторних робіт, іспит
		Кваліфікаційна робота бакалавра	самостійна робота, консультації з керівником	захист кваліфікаційної роботи
		Науково-дослідна практика	консультації з керівником, вивчення документації, самостійна робота, виконання індивідуального завдання, підготовка звіту з практики	поточне оцінювання керівником, захист практики
		Проектно-технологічна практика	консультації з керівником, вивчення документації, самостійна робота, виконання індивідуального завдання, підготовка звіту з практики	поточне оцінювання керівником, захист практики
		Основи алгоритмізації та програмування	лекції, практичні та лабораторні заняття, самостійна робота	контрольні роботи, тести, захист звітів з лабораторних та практичних робіт, іспит
		Інформаційні системи та мережі	лекції, практичні та лабораторні заняття, самостійна робота	контрольні роботи, тести, захист звітів з лабораторних та практичних робіт, іспит
		Архітектура комп'ютерних систем	лекції, практичні та лабораторні заняття, самостійна робота	контрольні роботи, тести, захист звітів з лабораторних та практичних робіт, залік
		Операційні системи та їх захист	лекції, лабораторні заняття, самостійна робота	контрольні роботи, захист звітів з лабораторних робіт, іспит