НАЦІОНАЛЬНЕ АГЕНТСТВО ІЗ ЗАБЕЗПЕЧЕННЯ ЯКОСТІ ВИЩОЇ ОСВІТИ

ВІДОМОСТІ
про самооцінювання освітньої програми

Заклад вищої освіти	**Київський національний університет імені Тараса Шевченка**
Освітня програма	**20271 Кібербезпека**
Рівень вищої освіти	**Магістр**
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	**20271**
Назва ОП	**Кібербезпека**
Галузь знань	**12 Інформаційні технології**
Спеціальність	**125 Кібербезпека**
Спеціалізація (за наявності)	*відсутня*
Рівень вищої освіти	**Магістр**
Тип освітньої програми	**Освітньо-наукова**
Вступ на освітню програму здійснюється на основі ступеня (рівня)	**Бакалавр, Магістр (ОКР «спеціаліст»)**
Структурний підрозділ (кафедра або інший підрозділ), відповідальний за реалізацію ОП	**кафедра кібербезпеки та захисту інформації**
Інші навчальні структурні підрозділи (кафедра або інші підрозділи), залучені до реалізації ОП	**кафедра іноземних мов, кафедра етики, естетики та культурології, кафедра філософії та методології науки, кафедра інтелектуальної власності та інформаційного права**
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	**101846**
ПІБ гаранта ОП	**Бабенко Тетяна Василівна**
Посада гаранта ОП	**професор**
Корпоративна електронна адреса гаранта ОП	**tetiana.babenko@knu.ua**
Контактний телефон гаранта ОП	**+38(067)-308-92-18**
Додатковий телефон гаранта ОП	*відсутній*

Форми здобуття освіти на ОП	Термін навчання
очна денна	1 р. 9 міс.

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

Для забезпечення потреб ринку України у висококваліфікованих фахівцях з інформаційної та 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 факультет інформаційних технологій та кафедру кібербезпеки та захисту інформації...
У 2017 році Університет отримав ліцензію на підготовку здобувачів вищої освіти другого рівня в "магістр" за спеціальністю "Кібербезпека". Освітньо-наукова програма "Кібербезпека" другого рівня вищої освіти (далі ОП) розроблена на підставі Закону "Про вищу освіту" проектною групою науково-методичної комісії спеціальності 125 "Кібербезпека" у складі: проф. Бабенко Т.В.,проф. Оксіюк О.Г., проф. Толюпа С.В., проф. Наконечный В.С, доц. Лукова-Чуйко Н.В.
Розглянуто та затверджено на засіданні Вченої ради Київського національного університету науки України 25.06.2017 р. № 12. З метою врахування вимог часу (Концепції вивчення іноземних мов студентами імені Тараса Шевченка Концепція-вивчення-іноземних-мов-студентами-неспеціальних-факультетів....pdf (univ.kiev.ua). На підставі рекомендацій представників ІБ та ІТ кластерів (Хай-ТЕК бюро, "Українські спеціальні системи", ДССЗЗІ, випускників кафедри, які працюють за фахом в державних структурах та приватних компаніях, а також інших зацікавлених осіб, включаючи наукові організації), у 2022 та 2023 роках були оновлені та затверджені актуальні редакції ОП (введено в дію наказами ректора № 160-52 від 23.03.22 та № 584-3 від 27.07.2023 р)

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	2023 - 2024	39	39	1
2 курс	2022 - 2023	39	36	0

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)** **49755 Кібербезпека (на основі ОПС фахового молодшого бакалавра)** **20270 Кібербезпека** **1074 Безпека інформаційних і комунікаційних систем** **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	*125_ОНП_маг_Кібербезпека_2021_КБ_!.pdf*	tEfTEAwifoAtsHWWKld8vvCfKbfYNyFoqviJolkzG/w=
Освітня програма	*125_ОНП_маг_Кібербезпека_2023_КБтаЗІ_!.pdf*	P7u1ivWgcQbdBmzAt0ozDex8/xYPoGnFoiIzV1s32e8=
Навчальний план за ОП	*NP_125_КБ_2023_Кб_та_ЗІ.pdf*	KzTs1fVbE8+tllc9/0t3MnBExXX7KG7rM/9Y/pZRSy0=
Навчальний план за ОП	*NP_125_КБ_2022_Кб.pdf*	yoe7rdcWtnXc5ev+Fgyh7d8D1yacdVEi8XUFxtrn18k=
Рецензії та відгуки роботодавців	*Відгуки.pdf*	r13ms3cdUkCs7o3GVknSZR2VQpV0ERdP4ircKzOP0Dk=
Рецензії та відгуки роботодавців	*ДСЗЗІ_відгук.pdf*	k3RyaCTZGnUD+G/GxGW3QIF/U9NH6+5US917xNd3n4s=

1. Проектування та цілі освітньої програми

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

Мета ОП "Кібербезпека" полягає в підготовці фахівців, здатних використовувати та впроваджувати новітні технології та методи досліджень, виконувати науково-дослідну та інноваційну діяльність у галузі захисту інформації та кібернетичної безпеки.
Особливістю ОП, яка акредитується, є те, що вона орієнтована на найновіші та найбільш актуальні аспекти кібербезпеки, враховуючи сучасні тенденції та виклики в цій галузі. ОП надає студентам глибокі теоретичні знання в області кібербезпеки, охоплюючи мережеву безпеку, управління ризиками, управління інцидентами інформаційної безпеки, реверс інженіринг, безпеку критичної інформаційної інфраструктури, форензік аналіз, системи управління інформаційною безпекою та інші ключові аспекти. Також ОП передбачає можливість приєднатися до наукових груп, лабораторій кафедри, факультету інформаційних технологій, де студенти можуть брати участь у проведенні досліджень з актуальних проблем кібербезпеки. Особливу увагу при розробці ОП приділено досвіду розробки аналогічних програм вітчизняними та закордонними ЗВО, такими як НТУ України "КПІ" імені Ігоря Сікорського, Національний авіаційний університет, ОП університетів США, Європи, Ізраїлю, НАТО та ін, Про унікальність ОП свідчить широкий спектр місць працевлаштування випускників - індустрія ІБ та ІТ, силові структури, банківські установи, аналітичні центри, SOC та CERT.

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

Стратегічний план розвитку КНУ імені Тараса Шевченка до 2025 р. (https://knu.ua/pdfs/official/Development-strategic-plan-22-12-12.pdf). Проводиться профорієнтаційна робота для формування контингенту студентів, які мають необхідні здібності та мотивацію до здобуття вищої освіти в Університеті, створення середовища, забезпечення різнобічного розвитку здобувачів освіти, (Працевлаштування КНУ (univ.kiev.ua)), Загальноуніверситетський кар'єрний онлайн-фестиваль (Telegram: Contact @job_expo_careers). Актуальні позиції від компаній зі сфер EdTech, Customer Support (Telegram: Contact @globalcareerday). ОП активно сприяє підвищенню рівня кібербезпеки країни через проведення наукових досліджень, навчальних заходів та консультацій з державними органами. Навчальні плани ОП адаптовані до потреб ринку праці у сфері кібербезпеки, що забезпечується через активну співпрацю з індустрією та проведення консультацій з експертами для визначення актуальних тематик та навичок, необхідних для успішної кар'єри в цій галузі.
Ця ОП відіграє важливу роль у підготовці кваліфікованих фахівців з кібербезпеки, які є учасниками в забезпеченні кібербезпеки країни.

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

При розробці ОП було враховано пропозиції випускників магістерського рівня спеціальності “Кібербезпека”. Проєкт ОП і її редакцій формувався на основі аналізу результатів опитування здобувачів вищої освіти, щодо наповненості освітніх компонент та рівня досягнення очікуваних програмних результатів (https://kbzi.knu.ua/surveys_of_masters/), та аналізу результатів обговорення наповнення освітніх компонент та досягнутих програмних результатів з випускним курсом спеціальності “Кібербезпека”. (https://kbzi.knu.ua/surveys_of_masters/)

- роботодавці

Для обговорення та врахування думки роботодавців у процесі розробки ОП було здійснено активне залучення фахівців провідних компаній з інформаційної безпеки та інформаційних технологій в місті Києві. Особливий акцент робився на науково-дослідній складовій програми. Пропозиції роботодавців, спрямовані на поглиблення теоретичних знань та розвиток наукових компетентностей студентів, були враховані в процесі формулювання освітніх компонентів програми (https://kbzi.knu.ua/surveys_of_masters/).

- академічна спільнота

Думки та пропозиції академічної спільноти були враховані при формулюванні цілей, компетентностей та програмних результатів навчання всіх редакцій ОП. Обговорення відбувалися на засіданнях проєктної групи та засідання кафедри кібербезпеки та захисту інформації. НПП кафедри разом зі здобувачами вищої освіти організовують та беруть активну участь у щорічних міжнародних науково-практичних конференціях «Проблеми кібербезпеки інформаційно-телекомунікаційних систем» (PCSITS) і «Інформаційні технології та впровадження» (IT&I) (https://kbzi.knu.ua/conference/), 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 науково-метричних 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+ модуль Жан Моне «Інтеграція рамок та політик кібербезпеки ЄС в Україні» тощо. (https://kbzi.knu.ua/surveys_of_masters/)

- інші стейкхолдери

Іншими зацікавленими сторонами є територіальна громада м. Київ та інших регіонів України, чий економічний розвиток, в тому числі, залежить від кваліфікації людського капіталу. Київський національний університет імені Тараса Шевченка значною мірою сприяє цьому процесу. Реалізація освітньої програми "Кібербезпека" сприяє зміцненню економіки та обороноздатності країни в кіберпросторі завдяки збільшенню кількості висококваліфікованих фахівців, які можуть ефективно вирішувати складні завдання в умовах військового часу . (https://kbzi.knu.ua/surveys_of_masters/)

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. При цьому 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 Програмні результати охоплюють ключові аспекти сучасної кібербезпеки, забезпечуючи студентів необхідними навичками для розв'язання складних завдань. тісна взаємодія з роботодавцями та участь у міжнародних програмах дозволяють адаптувати навчання до вимог ринку праці. Використання передових платформ, таких як Rangeforce та hack the box, сприяє практичній підготовці студентів та відповідності їхніх навичок потребам сучасної індустрії кібербезпеки. Кореляція між розвитком спеціальності, програмними результатами даної ОП та ринком праці також досягається завдяки тісній співпраці з роботодавцями, ефективній участі у міжнародних програмах (зокрема, програмах USAID) та систематичній роботі над вдосконаленням ОП

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

При розробці освітньої програми враховано галузевий та регіональний контекст через детальний аналіз пропозицій роботодавців, зокрема ІТ та ІБ компаній міста та регіону. Роботодавці висловили зацікавленість у випускниках з високим рівнем кваліфікації, які мають необхідні компетентності для роботи в SOC (Security Operations Center) або CERT (Computer Emergency Response Team), включаючи моніторинг та аналіз кіберзагроз, виявлення та відповідь на інциденти безпеки, використання сучасних засобів аналізу та виявлення загроз, розробку та впровадження стратегій захисту інформації, реверс-інжиніринг, ефективне взаємодія з іншими членами команди та вирішення завдань у реальному часі. Аналіз та обговорення пропозицій на засіданнях проєктної групи та кафедри стали основою для формування обов'язкових компонентів освітньої програми з метою досягнення визначених результатів навчання

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

Цілі та результати навчання ОП "Кібербезпека" враховують досвід вітчизняних та іноземних програм, зокрема ОП

НТУУ "КПІ" ім. Ігоря Сікорського, Національного авіаційного університету, Київського університету ім. Бориса Грінченка, Харківського національного університету ім. В.Н. Каразіна, а також ОП університетів США, Європи, Ізраїлю та НАТО (https://cutt.ly/iR6YucC). Врахування цього досвіду сприяє адаптації найкращих практик та відповідності вимогам глобальної кібербезпекової спільноти. Кожна ОП має свою унікальність, визначену науковими школами університетів, де реалізовані ці програми. Вони також мають спільні характеристики, що відображають сучасні досягнення в галузі кібербезпеки, такі як безпека управління ризиками, управління інцидентами кібербезпеки, реверс інженіринг, системи управління інформаційною безпекою тощо. Після аналізу цих освітніх програм та програм курсів, які викладачі кафедри вивчали в рамках USAID, і врахування регіональної специфіки, в освітні програми включені актуальні компоненти, такі як "Управління безпекою мереж", "Форензік аналіз" (https://kbzi.knu.ua/quality/)

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 другого (магістерського) рівня вищої освіти затверджено і введено в дію наказом Міністерства освіти і науки України від «18» березня 2021 р. № 332. ОП «Кібербезпека» спрямована на досягнення визначених стандартом результатів навчання. Вона враховує всі вимоги та компетентності, необхідні для магістра зі спеціальності "Кібербезпека" відповідно до стандарту вищої освіти. Кожен елемент програми допомагає студентам здобувати необхідні знання та навички, що відповідають вимогам стандарту (https://kbzi.knu.ua/onp_magistr_2021/, ОНП Магістр 2023 – Кафедра кібербезпеки та захисту інформації (knu.ua)). ОП «Кібербезпека» націлена на створення наукового ембієнту, де студенти мають можливість не лише освоїти передові технології та методи в галузі кібербезпеки, але й активно сприяти розвитку цієї науки. Лабораторні роботи, наукові семінари та співпраця з провідними науковцями створюють інтенсивне наукове середовище, сприяючи розвитку критичного мислення та дослідницьких вмінь у студентів. ОП «Кібербезпека» ефективно сприяє розвитку наукових навичок студентів, створюючи їм можливості для участі у дослідницьких проектах та оприлюднення отриманих наукових результатів на відповідних наукових заходах («Проблеми кібербезпеки інформаційно-телекомунікаційних систем» (PCSITS) (https://pcsits.knu.ua/) і «Інформаційні технології та впровадження» (IT&I), (https://kbzi.knu.ua/i_t_and_i/) різноманітних конкурсах наукових робіт, наукових семінарах кафедри). Цей аспект також відповідає вимогам стандарту вищої освіти. («Кібербезпека критично важливої інфраструктури України» – Кафедра кібербезпеки та захисту інформації (knu.ua)). Таким чином, програма "Кібербезпека" в повній мірі відповідає стандарту вищої освіти за спеціальністю 125, забезпечуючи студентам високоякісну освіту та науковий розвиток, відповідно до вимог стандарту.

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 другого (магістерського) рівня вищої освіти галузі знань 12 «Інформаційні технології» спеціальності 125 «Кібербезпека» затверджений та введений в дію наказом Міністерства освіти і науки України від України від «18» березня 2021 р. № 332 (Затверджені стандарти вищої освіти | Міністерство освіти і науки України (mon.gov.ua)).

2. Структура та зміст освітньої програми

Яким є обсяг ОП (у кредитах ЄКТС)?

120

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)?

90

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

30

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

Зміст ОП відповідає предметній області спеціальності 125 "Кібербезпека" і включає в себе широкий спектр освітніх компонентів, що належать до спеціальності 125 «Кібербезпека». Програма ретельно структурована і логічно впорядкована. Освітні компоненти(https://kbzi.knu.ua/onp_magistr_2021/, https://kbzi.knu.ua/onp_magistr_2023/) програми охоплюють ключові області, такі як об'єкти критичної інформаційної інфраструктури, комп'ютерні та інформаційні ресурси, технології та системи управління інформаційною безпекою, управління ризиками кібербезпеки та інцидентами, реверс інжиніринг. Акцент ОП робиться на науковій складовій підготовки, що відображається у вивченні методології та організації наукових досліджень, можливостях участі студентів у

дослідницьких проектах, публікаціях результатів наукових досліджень та активній участі у наукових заходах («Проблеми кібербезпеки інформаційно-телекомунікаційних систем» (PCSITS) і «Інформаційні технології та впровадження» (IT&I), USAID «Кібербезпека критично важливої інфраструктури України» та ін.
Такий підхід відповідає вимогам стандарту вищої освіти та сприяє розвитку висококваліфікованих фахівців у галузі кібербезпеки, здатних ефективно вирішувати завдання, пов'язані з захистом інформації та кіберпростору.

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

На ОП забезпечено можливість формування індивідуальної освітньої траєкторії для здобувачів вищої освіти. Здобувачі другого рівня вищої освіти мають можливість індивідуально вибирати дисципліни в обсязі, передбаченому Стандартом вищої освіти України для другого (магістерського) рівня спеціальності 125 "Кібербезпека та захист інформації". Процедура вибору індивідуальної освітньої траєкторії регламентується положенням про організацію освітнього процесу в Київському національному університеті імені Тараса Шевченка (див. http://nmc.univ.kiev.ua/docs/Polozhennia-pro-organizatsiyu-osvitniogo-procesu-11_04_2022.pdf) та Положенням про систему забезпечення якості освіти та освітнього процесу в КНУ ім. Тараса Шевченка https://knu.ua/pdfs/official/Quality-assurance-system-of-education-and-educational-process.pdf . Можливість формування індивідуальної освітньої траєкторії відображається в індивідуальних навчальних планах студентів, які затверджуються деканом Факультету інформаційних технологій. Студенти можуть вибирати навчальні дисципліни в межах обсягу не менше 25% від загальної кількості кредитів ЄТКС. При цьому дотримується послідовність вивчення вибраних дисциплін відповідно до структурно-логічної схеми підготовки фахівця. Таким чином, індивідуальна освітня траєкторія також забезпечується правом обирати тему кваліфікаційної роботи, наукового керівника та місця виробничої практики. Гарант ОП та НПП ознайомлюють здобувачів освіти з можливостями внутрішньої мобільності (https://mobility.univ.kiev.ua/?page_id=804&lang=uk.).

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

Право на вибір навчальних дисциплін студенти можуть реалізувати відповідно до процедури 3.7 Положення про систему забезпечення якості освіти та освітнього процесу в КНУ ім. Тараса Шевченка https://knu.ua/pdfs/official/Quality-assurance-system-of-education-and-educational- process.pdf. Вибір навчальних дисциплін студент здійснює в процесі формування свого індивідуального плану навчання у межах, що передбачені ОП та РНП з дотриманням послідовності їх вивчення відповідно до структурно-логічної схеми підготовки фахівця. Здобувач вищої освіти має право ознайомитись із РНП, включених до навчального плану, а також навчальними планами підготовки фахівців інших ОП або інших навчальних закладів при реалізації свого права на академічну мобільність (https://mobility.univ.kiev.ua/?page_id=804&lang=uk.). Вибіркові навчальні дисципліни індивідуального плану студента формуються з вибіркового блоку навчальних дисциплін, а також 2-х дисциплін із запропонованих переліків. Крім того, здобувач має право обрати навчальні дисципліни з інших ОП обов'язкових та вибіркових частин навчальних планів інших спеціальностей того самого рівня, а за умови погодження із деканом факультету – з програм іншого рівня.
Блоки вибіркових компонент, зазначені в ОНП включають фахові дисципліни, що визначають поглиблену спеціалізовану підготовку здобувачів в межах ОНП, і спрямовані на поліпшення здатності до працевлаштування. Якщо студент обрав певний блок вибіркових компонент, то він має прослухати всі дисципліни, що включені до цього блоку. Вибіркові навчальні дисципліни, 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 КНУ імені Тараса Шевченка регламентується "Положенням про проведення практики студентів" (http://surl.li/bjvpv). Практична підготовка здобувачів вищої освіти за ОП передбачає формування фахових компетентностей зі спеціальності, що є необхідними для професійної діяльності випускників. Зокрема ОП передбачено два види практики: виробнича та науково-дослідна. Метою цих практик є набуття студентами професійних навичок за ОП, поглиблення, закріплення та систематизація знань, в тому числі з дослідницької діяльності у сфері ІТ та ІБ. Здобувачам забезпечується вільний вибір місця проходження практики. Університет підтримує зв'язки з підприємствами та організаціями, що є потенційними базами практик та створюють умови для реалізації змісту практик, Практики здійснюється на основі провідних підприємств та організацій, таких як "ЕРАМ", "ДССЗЗІ", "B2B-рішення", ТОВ "Софтпром Солюшнз", ТОВ "МТІ", ТОВ "Ел-Консалтинг", KPMG та ін,.
У щоденнику проходження практики фіксується оцінка роботи здобувача вищої освіти. Також підприємство на якому проходить практику здобувач вищої освіти 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

До обов'язкових компонент ОП, що безпосередньо пов'язані з набуттям соціальних навичок, належать дисципліни «Професійна та корпоративна етика», «Методологія та організація наукових досліджень з основами інтелектуальної власності», «Іноземна мова для академічних цілей», «Виробнича практика» «Науково-дослідна практика».
Компетентності ОП, що відповідають за набуття soft skills:

Здатність спілкуватися з представниками інших професійних груп різного рівня (з експертами з інших галузей знань / видів економічної діяльності).
Програмні результати навчання зазначені в програмі, що стосуються набуття soft skills є наступними: ПРН1, ПРН15, ПРН18, та ПРН23. Підготовка та захист звітів з лабораторних робіт і виробничої та науково-дослідної практики та кваліфікаційної роботи сприяють розвитку умінь аргументувати та відстоювати прийняті рішення, аналізувати їх та вміти нести за них відповідальність, зумовлюють співпрацю з працедавцями, розвивають розуміння важливості виконання завдань в визначений термін, здатність розуміти позицію опонента, вишукувати в ній реальні недоліки та змінювати його ставлення до проблеми або рішення. Процес навчання дозволяє здобувачеві набутити soft skills, що зумовлені цілями ОП, зокрема подальшою професійною діяльністю випускника програми, що підтверджується відгуками працедавців, працевлаштуванням випускників.

Яким чином зміст ОП ураховує вимоги відповідного професійного стандарту?

На час розробки редакції ОП професійний стандарт відсутній.

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 КНУ імені Тараса Шевченка організація освітнього процесу регламентується “Положенням про організацію освітнього процесу”(http://www.nmc.univ.kiev.ua/docs/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 поза аудиторного навантаження, що визначається у відсотках становить структуру кредиту.
Розподіл часу між заняттями і самостійною роботою здійснюється з урахуванням норм «Положення про організацію освітнього процесу», п.5.2.5. де встановлено що для здобувачів ступеня вищої освіти – магістр частка самостійної роботи може становити 67-75% загального обсягу навчального часу дисципліни в свою чергу обсяг самостійної (позааудиторної) роботи з кожної дисципліни визначено в навчальному плані ОП, 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 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, http://fit.univ.kiev.ua/masters_programmes

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 другого (магістерського) рівня вищої освіти МОН України. Умови вступу та перелік необхідних для вступу документів розміщені на офіційному сайті університету у розділі “Вступна кампанія у магістратуру” за посиланням https://vstup.knu.ua/#Section211. Правила прийому на навчання для здобуття ступеня магістра за ОП “Кібербезпека” враховує особливості ОП, зокрема Детальніше https://vstup.knu.ua/images/2022/NMT_ZNO_vstup.pdf .
Згідно з правилами прийому на навчання для здобуття освітнього ступеня магістра за ОП передбачається, що здобувач, повинен мати диплом за першим (бакалаврським) рівнем вищої освіти та скласти іспити з фахових дисциплін для підтвердження його готовності до засвоєння ОНП магістерського рівня. Програма вступних випробувань за ОНП формується кафедрою кібербезпеки та захисту інформації (до дор 1и березня ипоточного навчального року). Вимоги до вступників враховують особливості ОП, оскільки побудовані на програмних результатах навчання ОП бакалаврського рівня та передбачає вивчення іноземної мови.

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 такими документами, які у вільному доступі розміщені на інформаційних ресурсах Університету:
Положення про організацію освітнього процесу у Київському національному університеті імені Тараса Шевченка введене в дію Наказом Ректора від 11.04.2022 р. за №170-32 (зокрема Розділ 7 та Розділ 11):
http://nmc.univ.kiev.ua/docs/Polozhennia-pro-organizatsiyu-osvitniogo-procesu-11_04_2022.pdf

Положення про порядок реалізації права на академічну мобільність Київського національного університету імені Тараса Шевченка від 10.05.2023 р.
https://mobility.univ.kiev.ua/?page_id=804&lang=uk
ПОРЯДОК поновлення та переведення здобувачів вищої освіти (студентів, слухачів, курсантів) у КНУ 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
Положення про порядок перезарахування результатів навчання у КНУ імені Тараса Шевченка:
http://mobility.univ.kiev.ua/?page_id=798&lang=uk

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

Практики застосування вказаних правил на ОП не було

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» в Університеті було розроблено і введено в дію наказом ректора №86-32 від 07.02.2023 Положення про валідацію і визнання результатів навчання здобутих у процесі неформальної та/або інформальної освіти у програмах вищої та фахової передвищої освіти КНУ імені Тараса Шевченка
http://senate.univ.kiev.ua/?p=2271
Здобувачам ОП, починаючи з 2.06.20 була надана можливість зарахування результатів навчання, підтверджених сертифікатами платформи Coursera for Campus (http://www.univ.kiev.ua/news/10974). Питання визнання результатів навчання за наданим студентом сертифікатом могло прийматися викладачем відповідної дисципліни, обговорюватися та затверджуватися на засіданні кафедри. Можливість зарахування сертифікатів, які були отримані в результаті проходження курсів від Coursera та інших академій, і кількість відповідних балів за них було відображено в робочих програмах дисциплін.
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 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

Досягнення ПР навчання на ОП досягається за рахунок поєднання таких форм навчання, як лекційні заняття, практичні роботи, лабораторні заняття, семінарські заняття, самостійної роботи, проходження практик на ОІД. Викладання здійснюється з широким використанням мультимедійних засобів, спеціалізованого програмного забезпечення та світових навчальних платформ (Hack the box, Tryhackme, академії CISCO, RangeForce). Здобувачам вищої освіти надається доступ до інформаційних та методичних матеріалів кожної освітньої компоненти, а саме доступна інформація про автора курсу, робоча програма навчальної дисципліни, перелік рекомендованої літератури, система оцінювання знань, глосарій, лекційні, методичні матеріали, тестові завдання для самоконтролю тощо.
Інформація про методи навчання і викладання, що застосовуються на ОП для кожної ОК деталізовано в таблиці 3.
Посилання на відповідні документи (https://kbzi.knu.ua/magistr/)

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 та викладання на ОП "Кібербезпека" спроектовані з урахуванням студентоцентрованого підходу, в якому акцент зроблений на потребах та індивідуальних можливостях кожного студента. Відповідно до "Положення про організацію освітнього процесу" (http://nmc.univ.kiev.ua/docs/Polozhennia-pro-organizatsiyu-osvitniogo-procesu-11_04_2022.pdf), методи навчання включають різноманітні форми, такі як лекції, лабораторні роботи, практичні заняття, семінари, індивідуальні консультації та самостійна робота.

Кожен студент має можливість вибирати дисципліни вільного вибору, обирати місце проходження практик, визначати тематику індивідуальних завдань та підходити до вивчення матеріалу із урахуванням своїх особистих інтересів та потреб. Це дозволяє студентам активно співпрацювати у власному освітньому процесі і адаптувати його до своїх навчальних цілей.
Для оцінки якості методів навчання і викладання проводяться регулярні анонімні опитування. На підставі їх результатів виділяється високий рівень задоволення студентів, особливо враховуючи наукові і практичні аспекти, а також можливості застосування здобутих знань у реальних сценаріях в галузі кібербезпеки. Результати опитувань доступні для ознайомлення на офіційному веб-сайті випускової кафедри (https://kbzi.knu.ua/surveys_of_masters/)

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

Забезпечення академічних свобод на ОП "Кібербезпека" в КНУ імені Тараса Шевченка визначається Статутом Університету https://knu.ua/pdfs/statut/statut-22-11-28.pdf "Положенням про організацію освітнього процесу (Polozhennia-pro-organizatsiyu-osvitniogo-procesu-11_04_2022.pdf)" та «Етичним кодексом університетської спільноти КНУ імені Тараса Шевченка» (http://www.univ.kiev.ua/pdfs/official/ethical-code/Ethical-code-of-the-university-community.pdf), що базується на студентоцентрованому підході. Одним із важливих аспектів академічних свобод є можливість студентів обирати тематику своїх наукових робіт. Це відкриває перед студентами широкий простір для самореалізації та поглибленого вивчення конкретних аспектів кібербезпеки, що відповідає їхнім особистим інтересам та кар'єрним амбіціям. У взаємодії з викладачами студенти мають можливість обговорення ідей, отримання консультацій та взаємодії на різних етапах навчання. Також на ОП «Кібербезпека» забезпечено свободу висловлення думки, що сприяє розвитку критичного мислення та обміну ідеями в академічному середовищі. Також на ОП «Кібербезпека» забезпечено свободу висловлення думки, що сприяє розвитку критичного мислення та обміну ідеями в академічному середовищі.

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 *

Згідно з "Положенням про організацію навчального процесу" (https://www.knu.ua/pdfs/official/Polozhennia-pro-organizatsiyu-osvitniogo-procesu-11_04_2022.pdf), для кожної навчальної дисципліни, що входить до ОП «Кібербезпека», розроблена робоча навчальна програма. У програмі викладено зміст навчальної дисципліни, послідовність вивчення, форми поточного та семестрового контролю, результати навчання, а також основні і додаткові літературні джерела. Здобувач має можливість ознайомитися з РНП на офіційному веб-сайті кафедри (https://kbzi.knu.ua/magistr/). Інформація оновлюється щорічно перед початком вступної кампанії і є доступною потенційним абітурієнтам і здобувачам вищої освіти при формуванні їхньої індивідуальної освітньої траєкторії. Крім того, на початку кожного семестру лектор та викладачі-асистенти, при проведенні лабораторних, практичних та семінарських занять, надають детальні пояснення здобувачам освіти щодо порядку та критеріїв оцінювання запланованих видів робіт та форм контролю. Перед початком кожного навчального року на сайті факультету виконується оприлюднення грфіку навчального процесу (http://fit.univ.kiev.ua/wp-content/uploads/2014/11/%D0%B3%D1%80%D0%B0%D1%84%D1%96%D0%BA_%D0%9D_%D0%9F%D1%80_%D0%9C%D0%B0%D0%B3%D1%96%D1%81%D1%82%D1%80_1%D0%B8%CC%86_%D0%BA%D1%83%D1%80%D1%81_1_%D1%81%D0%B5%D0%BC_2023_2024.pdf).

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) Nakonechnyi V., Toliupa, S., Kotov, M., Solodovnyk V. RF signals encryption with AES in WDID. CEUR Workshop Proceedings, 2021, 2845, p.p. 96–105. SCOPUS;
2) Nakonechnyi V., Saiko, V., Toliupa, S., Kotov, M., Astapenya, V. Method of determining the angular orientation of small satellites in orbit. Proceedingsthis link is disabled, 2021, 2923, p.p. 224–233. SCOPUS
3) 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;
4) 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 навсеукраїнському 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 ОНП “Кібербезпека” систематично беруть участь в роботі щорічної конференції «Проблеми кібербезпеки інформаційно-телекомунікаційних систем» (PCSITS). Детальніше за посиланням (https://pcsits.knu.ua/).

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 одного разу на рік відповідно до вимог "Положення про організацію освітнього процесу" від 11 квітня 2022 року (http://nmc.univ.kiev.ua/docs/Polozhennia-pro-organizatsiyu-osvitniogo-procesu-11_04_2022.pdf). Моніторинг включає оцінювання відповідності ОП та її освітніх компонентів актуальним науковим досягненням у галузі кібербезпеки, урахування тенденцій розвитку економіки та суспільства, змін у потребах роботодавців, студентів і стейкхолдерів. Наприклад, за рекомендацією ДССЗІ України та на основі курсів, прослуханих викладачами кафедри в рамках проекту USAID “Кібербезпека об'єктів критичної інфраструктури України”, викладачі ОП оновили та розробили РНП з дисциплін: "Управління інцидентами інформаційної безпеки", "Аудит інформаційних систем", "Реверс-інжиніринг", "Безпека критичної інформаційної інфраструктури".

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

Навчання, викладання та наукові дослідження в межах ОП "Кібербезпека" у Київському національному університеті імені Тараса Шевченка мають значущий інтернаціональний компонент, який включає в себе ряд конкретних ініціатив. Науково-педагогічний склад ОП активно впроваджує міжнародні практики через участь у наукових проектах та стажуваннях за кордоном. Професійне стажування за кордоном для викладачів і студентів стає важливим етапом їхньої освітньої та наукової кар'єри, так, наприклад: професор Т. Бабенко професор С. Бучик, професор В. Наконечний, доценти А. Фесенко, Л. Мирутенко та асистент С. Даков (https://kbzi.knu.ua/quality/) успішно пройшли наукові стажування в провідних університетах світу, отримуючи новітні знання у галузі кібербезпеки. Студенти мають можливість брати участь у обміні студентами та викладачами з партнерськими університетами з метою обміну досвідом та вивчення сучасних тенденцій у сфері кібербезпеки. Впровадження концепції вивчення іноземних мов для неспеціальних факультетів КНУ імені Тараса Шевченка, допомагає збільшити міжнародну мобільність студентів та викладачів, сприяючи подальшій інтернаціоналізації нашого освітнього середовища.

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?

Форми контрольних заходів, які можуть бути застосовані в межах навчальних дисциплін ОП, детально описані у Положенні про організацію освітнього процесу в КНУ імені Тараса Шевченка Це положення визначає принципи об'єктивності, систематичності, системності, плановості, єдності вимог, відкритості, прозорості, економічності, доступності та зрозумілості методики оцінювання. 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 РПН (робочою навчальною програмою). Формами поточного контролю можуть бути підготовка доповідей та коротких повідомлень на дискусійні теми, вирішення ситуативних задач, виконання і захист лабораторних та практичних робіт, виконання та захист індивідуальних завдань, експрес-тестування, контрольні роботи, модульні контрольні роботи тощо. Форми поточного контролю, їх оцінка в балах та критерії оцінювання визначаються у відповідності зі специфікою дисципліни та фіксуються у РПН. Підсумковий контроль, представлений іспитами та заліками, оцінює глибину зрозуміння та відповідність програмним результатам. Вибір форми контрольних заходів відбувається на етапі підготовки навчального плану: освітні компоненти, результати яких передбачають практичне наповнення, завершуються заліком, освітні компоненти теоретичного або теоретико-практичного наповнення - іспитом. Для оцінювання рівня сформованості запланованих результатів навчання після проходження виробничих практик (2 практики за період навчання) встановлено форму оцінювання диференційований залік, який виставляється здобувачу освіти за результатами поточної роботи, презентації її результатів та захисту звіту перед комісією. Мінімальний пороговий рівень оцінки за кожним запланованим для освітнього компонента результатом навчання визначається відповідною РПН. Мінімальний пороговий рівень оцінки ОК ОП 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 тих результатів навчання, які не можуть бути оцінені під час підсумкового контролю, або набрав кількість балів, що є недостатньою для отримання позитивної оцінки навіть у випадку досягнення ним на підсумковому контролі максимально можливого результату.
Наведені форми контролю та підхід до оцінювання спрямовані на систематичну та комплексну досягнень студентів у навчанні та їх відповідність програмним результатам ОП «Кібербезпека»

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

У положенні про організацію навчального процесу в КНУ імені Тараса Шевченка визначені принципи та підходи у розділі 7 «ОЦІНЮВАННЯ РЕЗУЛЬТАТІВ НАВЧАННЯ». Детальна інформація щодо організації оцінювання здобувачів освіти, включаючи форми контрольних заходів, критерії оцінювання та процедури, подана відповідно до визначених принципів у відповідних робочих навчальних програмах (РНП) освітніх компонентів. Крім того, конкретні вказівки щодо проведення контрольних заходів, вимог до їх організації та оцінювання, а також визначення умов допуску до них регламентуються відповідними розділами робочих навчальних програм. Доступ до

цих документів забезпечується шляхом їхньої публікації на офіційних ресурсах кафедри кібербезпеки та захисту інформації та надається через інші засоби комунікації студентам. (https://kbzi.knu.ua/magistr/). Дані РНП є частиною організаційно-методичної документації і забезпечують чіткість та зрозумілість оцінювальних процедур для студентів. Для додаткового роз'яснення форм та процедури контрольних заходів здобувачі освіти можуть звернутися безпосередньо до викладача, який проводить заняття, куратора або ж завідувача кафедри, як особисто, так і через засоби комунікації (електронна пошта, телефон, месенджер), контакти надаються на першому занятті. Отже, узгоджене застосування положення та відповідних робочих навчальних програм забезпечує системність, прозорість та ефективність процесу оцінювання, а також сприяє досягненню програмних результатів навчання студентів

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 доводиться до здобувачів вищої освіти кількома способами. Робочі навчальні програми, опис освітньої програми та навчальний план знаходяться на сайті кафедри Кібербезпеки та захисту інформації (https://kbzi.knu.ua/), де їх можна знайти протягом тижня після затвердження. Крім того, згідно з Положенням про порядок оцінювання в Київському національному університеті імені Тараса Шевченка (http://www.nmc.univ.kiev.ua/docs/POLOJENNIA-2010-1.doc), викладач на першому занятті інформує студентів про форми контрольних заходів та терміни їх проведення. Графік навчального процесу з розкладом сесії, проведення практики, та інші важливі події публікуються на сайті факультету (http://fit.univ.kiev.ua/for-students/session-schedule) перед початком навчального року. Додатково, інформація про терміни проведення іспитів, заліків, захисту практик і звітів з практики надходить до викладачів та студентів за місяць до початку екзаменаційної сесії (http://fit.univ.kiev.ua/schedule-session). Графіки перескладань також доступні на сайті факультету (https://cutt.ly/HX8S4e6)

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

Відповідно до Стандарту вищої освіти ОС "магістр" за спеціальністю 125 "Кібербезпека та захист інформації" підсумкова атестація здійснюється у формі захисту випускної кваліфікаційної роботи. На ОП "Кібербезпека" втілено передбачену стандартом форму атестації здобувачів освіти - публічний захист кваліфікаційної роботи магістра. Тематика випускних робіт обговорюється та затверджується на засіданні кафедри кібербезпеки та захисту інформації.
Рекомендації щодо вибору теми, структури роботи, змістовного наповнення розділів та правил оформлення викладені у методичних рекомендаціях до виконання випускної кваліфікаційної роботи для отримання освітнього ступеня «магістр» за спеціальністю 125 «Кібербезпека» (https://kbzi.knu.ua/diplom_mag/)
Регламент виконання випускних кваліфікаційних робіт доводиться до відома студентів перед початком дипломного проєктування. Анотації кваліфікаційних робіт розміщено на сайті кафедри (https://kbzi.knu.ua/annotations_to_masters_theses/), всі роботи долучаються до репозиторію робіт https://ir.library.knu.ua/collections/accd3d48-3ac9-450c-b38a-55d995bb4609(). Атестація здобувачів вищої освіти ОП відбувається шляхом публічного захисту кваліфікаційної роботи. У зв'язку з воєнним станом публічний захист кваліфікаційних робіт проводиться в онлайн режимі за допомогою платформи Zoom.

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

Процедура проведення контрольних заходів регулюється «Положенням про організацію освітнього процесу у КНУ імені Тараса Шевченка» (розділи 4, 7 та інше) (http://nmc.univ.kiev.ua/docs/Polozhennia-pro-organizatsiyu-osvitniogo-procesu-11_04_2022.pdf), а також, в частині, яка не суперечить цьому положенню. («Положення про порядок оцінювання знань студентів при кредитно-модульній системі організації навчального процесу в Київського Національного університету імені Тараса Шевченка» від 2010 року (http://nmc.univ.kiev.ua/docs/POLOJENNIA-2010-1.doc)).
Також застосовуються наступні документи:
1) «Положення про порядок створення та організацію роботи Екзаменаційної комісії в КНУ імені Тараса Шевченка» від 3 листопада 2014 року (http://nmc.univ.kiev.ua/docs/Polojennya%20pro%20DEK.doc);
2) «Положення про систему забезпечення якості освіти та освітнього процесу в Київського Національного університету імені Тараса Шевченка» (http://www.univ.kiev.ua/pdfs/official/Quality-assurance-system-of-education-and-educational-process.pdf);
3) в умовах воєнного стану також діє Тимчасовий порядок проведення заліково-екзаменаційної сесії та підсумкової атестації з використанням технологій дистанційного навчання у КНУ імені Тараса Шевченка (http://nmc.univ.kiev.ua/docs/Poryadok%20zal_ekz%20sesii%20dyst_techn.pdf).
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 ОП "Кібербезпека" гарантується відповідно до "Положення про порядок створення та організацію роботи Екзаменаційної комісії в КНУ імені Тараса Шевченка" (http://nmc.univ.kiev.ua/docs/Polojennya%20pro%20DEK.doc). Оцінювання проводиться комісією, що включає мінімум двох викладачів, один з яких не викладав дану дисципліну. Оцінювачі можуть відмовитися від участі в

оцінюванні при виникненні конфлікту інтересів. Результати зберігаються протягом року, а відеофіксація процедури оцінювання дозволяє перевірити об'єктивність. Критерії та форми оцінювання оприлюднюються заздалегідь. Процедури запобігання та врегулювання конфлікту інтересів регламентуються "Положенням про систему забезпечення якості освіти та освітнього процесу в КНУ імені Тараса Шевченка", а порядок вирішення конфліктних ситуацій представлений у "Порядку вирішення конфліктних ситуацій у КНУ імені Тараса Шевченка". На ОП "Кібербезпека" конфліктних ситуацій під час оцінювання не зафіксовано

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» (http://nmc.univ.kiev.ua/docs/Polozhennia-pro-organizatsiyu-osvitniogo-procesu-11_04_2022.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 "Кібербезпека" всі випадки повторного проходження контрольних заходів здійснюються відповідно до нормативних документів Київського Національного університету імені Тараса Шевченка

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): http://nmc.univ.kiev.ua/docs/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 не було.

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

Поняття академічної доброчесності на ОП регламентується «Етичним кодексом університетської спільноти» (http://www.univ.kiev.ua/pdfs/official/ethical-code/Ethical-code-of-the-university-community.pdf), введено у п.1. «Положення про організацію освітнього процесу у КНУ імені Тараса Шевченка» (http://nmc.univ.kiev.ua/docs/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 КНУ імені Тараса Шевченка (http://www.univ.kiev.ua/pdfs/official/Quality-assurance-system-of-education-and-educational-process.pdf), «Положенням про систему виявлення та запобігання академічному плагіату у Київському національному університеті імені Тараса Шевченка» (http://senate.univ.kiev.ua/?p=1352), «Положенням про забезпечення дотримання академічної доброчесності у КНУ 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 Київського Національного університету 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 КНУ 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. Перевірені та готові до захисту роботи передаються в репозиторій кваліфікаційних робіт.
Також для 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 кібербезпеки та захисту інформації активно підтримується високий ступінь відданості етичним принципам та нормам, визначеним в Етичному кодексі університетської спільноти. Куратори груп та викладачі регулярно проводять зі студентами бесіди та обговорення, спрямовані на усвідомлення різних видів порушення академічної доброчесності, а також встановлення та підтримання норм та принципів її дотримання.
На сайті кафедри створено сторінку (https://kbzi.knu.ua/academic_integrity/), де розміщуються роз'яснювальні матеріали та відповідні нормативні документи.
Університет є учасником проєкту «Ініціатива академічної доброчесності та якості освіти» (Academic Integrity and Quality Initiative – Academic IQ) від Американських Рад з міжнародної освіти, який має на меті об'єднати професійну спільноту освітян середньої та вищої освіти для обміну досвідом та співпраці задля підтримки академічної доброчесності та якості освіти й сприяння розвитку культури академічної доброчесності.
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 КНУ імені Тараса Шевченка» та «Положенням про організацію освітнього процесу у КНУ імені Тараса Шевченка». Види реагування зазначені у п. 9.8.3 «Положення про організацію освітнього процесу у КНУ імені Тараса Шевченка», а саме: повторне проходження оцінювання; повторне проходження відповідного освітнього компонента ОП; 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 КНУ 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?

Порядок обрання за відкритим конкурсом осіб на вакантні посади науково-педагогічних працівників Університету визначають Закон України «Про вищу освіту», Статут КНУ імені Тараса Шевченка (https://www.univ.kiev.ua/pdfs/statut/statut-22-11-28.pdf), Порядок конкурсного відбору на посади науково-педагогічних працівників у Київському національному університеті імені Тараса Шевченка (http://senate.univ.kiev.ua/?p=1863). Вся інформація розміщена на сайті Вченої ради Університету за посиланням http://senate.univ.kiev.ua/. Забезпечення необхідного рівня професіоналізму викладачів здійснюється шляхом дотримання чітко визначеної прозорої процедури конкурсного добору. 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 (посилання); проходження курсів підвищення кваліфікації (посилання на підвищення кваліфікації). Необхідний рівень професіоналізму викладачів забезпечується відповідністю викладачів ОП кваліфікаційним вимогам, визначеними Ліцензійними умовами провадження освітньої діяльності (посилання на таблицю Ліцензійних умов). Наразі кваліфікація НПП, залучених на ОП, забезпечує досягнення визначених ОП ПРН та відповідає вимогам щодо забезпечення провадження освітньої діяльності у сфері вищої освіти

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). ЗВО активно залучає роботодавців до організації та реалізації освітнього процесу, створюючи партнерські зв'язки та програми співпраці.. Завдяки договору співпраці з ДССЗЗІ України викладачі та здобувачі кафедри мають можливість приймати участь в програмі проведення кібернавчань у сфері кібербезпеки та кіберзахисту, які приводяться під егідою ДССЗЗІ та отримати практичні навички. Викладачі кафедри КБЗІ є членами Scientific Cyber Security Association, що є хабом, який поєднує роботодавців у сфері кібербезпеки та академічну спільноту, оскільки членами асоціації є науковці та науково-педагогічні працівники з провідних ЗВО України. Також університет організовує кар'єрні ярмарки та події, де студенти можуть спілкуватися з представниками компаній, дізнаватися про вакансії та можливості працевлаштування. Такі заходи створюють можливості для студентів знайти роботу або здобути практику ще під час навчання. На жаль пандемія Covid2019 та повномасштабне вторгнення в Україну значно ускладнили організацію взаємодії з роботодавцями.

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. Активно впроваджується практика залучення фахівців кібербезпеки до проведення наукових конференцій зі здобувачами вищої освіти (https://kbzi.knu.ua/pcsits/), круглих столів, проведення тренінгів з виконавцями проєкту програми Erasmus+ «dComFra» (https://kbzi.knu.ua/2020/07/20/dcomfra-online-training-activities/), загальноєвропейських ініціатив Girls in ICT, AllDigitalWeek, CodeWeek (https://kbzi.knu.ua/2020/03/26/aweek_p590/, https://kbzi.knu.ua/2022/10/20/codeweek-2022/, https://kbzi.knu.ua/2022/04/28/girls-_n_ict_2022/) тощо. На ОП «Кібербезпека» залучаються провідні науковці, як приклад можна привести відкриту лекцію «Форензік аналіз» д.т.н. професора Гнатюка С.О. для студентів. Кафедра КБЗІ періодично запрошує іноземних професорів до читання відкритих лекцій для здобувачів (https://kbzi.knu.ua/2023/03/04/lecture_ist-2/, https://kbzi.knu.ua/2023/03/04/image_processing_and_analysis/).

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

Підвищегння кваліфікації в унівіерситеті регламентуться "Положенням про підвищення кваліфікації педагогічних та науково-педагогічних
працівників КНУ імені Тараса Шевченко" (http://senate.univ.kiev.ua/?p=1997) 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 та USAID/RangeForce (https://kbzi.knu.ua/cisco/, keycloak.rangeforce.com) 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 (Ukraine Higher Education Teaching Excellence Programme) 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. Університет вдосконалив «Положення про підвищення кваліфікації НПП», передбачивши в ньому можливості різних траєкторій професійного зростання викладачів.
Стимулюванню викладацької майстерності сприяє Наказ Ректора № 71-32 від 31.01.2014 р. «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 й засвоєння нових засобів навчання в Університеті проводяться тренінги для співробітників. Зокрема, у 2023 р. відбувся тренінг з цифрової трансформації для викладачів кафедри та факультету від виконавців проєкту програми Erasmus+ КА2 «dComFra» (https://kbzi.knu.ua/c_d_k/). У 2020 р. в рамках проєкту програми «dComFra» на факультеті створено Центр цифрових компетентностей та розпочався процес його міжнародної акредитації ICDL. В майбутньому при Центрі планується щорічна міжнародна сертифікація викладацького складу

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?

Матеріально-технічна база (МТБ) на факультеті інформаційних технологій відповідає сучасним стандартам і грає ключову роль у досягненні цілей та програмних результатів освітньої програми. Кафедра приймала активну участь в проекті USAID «Кібербезпека критично важливої інфраструктури України» від якого отримала повний комплект обладнання для створення лабороторій та обладнання серверної. За результатами цих проєкту викладачі, які забезпечують ОП, мають сертифікати про закінчення курсів по проекту USIAD (посилання). Лекційні аудиторії обладнані мультимедійними проєкторами, а лабораторії оснащені сучасною комп'ютерною технікою та підключенням до Інтернету. Крім того, наукова бібліотека ім. М. Максимовича надає відкритий доступ до електронних ресурсів (https://goo.su/IHR), https://goo.su/A8j, що сприяє збільшенню обсягу інформації, доступної для студентів та викладачів. Це стимулює їхнє активне вивчення та дослідницьку діяльність.
Описи освітніх програм та робочі програми дисциплін регулярно оновлюються та публікуються на сайті кафедри (https://kbzi.knu.ua/rnp_magistr/) , що забезпечує стабільний доступ студентів до актуальної інформації.
Впровадження освітніх платформ, таких як Microsoft Teams та Moodle, сприяє зручній взаємодії студентів із викладачами та активному використанню сучасних технологій у навчальному процесі

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?

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 (https://knu.ua/pdfs/official/Development-strategic-plan-22-12-12.pdf). Також Університет забезпечує дотримання Правил внутрішнього розпорядку Київського Національного університету імені Тараса Шевченка (https://bit.ly/3S5BMo7), правил внутрішнього розпорядку в студентських гуртожитках університету (https://studmisto.knu.ua/documents/regulation-documents/257-pravyla-vnutrishnoho-rozporiadku). Освітнє середовище Університету є безпечним для життя і здоров'я здобувачів вищої освіти, що забезпечується діяльністю відповідних підрозділів. Також в Університеті проводять заходи, які спрямовані на забезпечення комфортних умов проживання, проведення інструктажів з техніки безпеки на лабораторних заняттях, на канікулах та на час карантину. У разі потреби є можливість звернутись до Інституту психіатрії Університету, що спеціалізується, зокрема, на наданні високоспеціалізованої медичної допомоги особам з вадами психічного здоров'я. На кафедрі створені групи у соціальних мережах Facebook, телеграм-канал, які регулярно інформують про проведення заходів розвитку здорового способу життя (https://www.facebook.com/kbzi.knu.ua).

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

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. Організаційна підтримка студентів здійснюється через центр по роботі зі студентами, відділ академічної мобільності та відділ сприяння працевлаштуванню та роботі з випускниками (http://jobs.knu.ua),. Студенти можуть скористатися послугами спорткомплексу, Молодіжного центру культурно-естетичного виховання (https://goo.su/HzH), Центру комунікацій (https://goo.su/bez), Наукового товариства студентів та аспірантів (http://ntsa.univ.kiev.ua/),, а також Навчальної лабораторії соціологічних та освітніх досліджень. Університет також надає консультації та допомогу з питань здоров'я через власну клініку та психологічну службу. Вирішення організаційних питань на факультеті покладено на деканат, завідувачів та фахівців кафедр, кураторів груп. Інструментами інформаційної підтримки є сайти http://www.univ.kiev.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 Скарг та нарікань від здобувачів щодо усіх видів підтримки не надходило.

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?

Для забезпечення права на якісну вищу освіту осіб з особливими освітніми потребами в Університеті у рамках проєкту «Університет рівних можливостей» було розроблено Концепцію розвитку інклюзивної освіти (https://www.univ.kiev.ua/pdfs/equal-opportunities/Concept-of-inclusive-education-development.pdf). Університет забезпечує доступність і якість освітніх послуг усім суб'єктам освітнього процесу, у тому числі й особам з особливими освітніми потребами, з урахуванням здібностей, можливостей та інтересів кожного шляхом запровадження інклюзивної освіти. В Університеті прийнято Порядок супроводу (надання допомоги) осіб з інвалідністю (https://www.knu.ua/pdfs/equal-opportunities/Poryadok-suprovodu-osib-z-invalidnistyu.pdf) та Пам'ятка про правила комунікації із людьми з інвалідністю (https://www.knu.ua/pdfs/equal-opportunities/Pamyatka-pro-pravyla-komunikaciyi-iz-lyudmy-z-invalidnistyu.pdf), а також план облаштування доступності корпусів факультетів та університетської території, що включає в себе: встановлення мнемосхем та тактильних стрічок для осіб з порушенням зору, облаштування паркувальних місць, облаштування відповідних місць в аудиторіях та приміщень пандусами тощо

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)

Для забезпечення права на якісну вищу освіту осіб з особливими освітніми потребами в Університеті у рамках проєкту «Університет рівних можливостей» було розроблено Концепцію розвитку інклюзивної освіти (https://www.univ.kiev.ua/pdfs/equal-opportunities/Concept-of-inclusive-education-development.pdf). Університет забезпечує доступність і якість освітніх послуг усім суб'єктам освітнього процесу, у тому числі й особам з особливими освітніми потребами, з урахуванням здібностей, можливостей та інтересів кожного шляхом запровадження інклюзивної освіти. В Університеті прийнято Порядок супроводу (надання допомоги) осіб з інвалідністю (https://www.knu.ua/pdfs/equal-opportunities/Poryadok-suprovodu-osib-z-invalidnistyu.pdf) та Пам'ятка про правила комунікації із людьми з інвалідністю (https://www.knu.ua/pdfs/equal-opportunities/Pamyatka-pro-pravyla-komunikaciyi-iz-lyudmy-z-invalidnistyu.pdf), а також план облаштування доступності корпусів факультетів та університетської території, що включає в себе: встановлення мнемосхем та тактильних стрічок для осіб з порушенням зору, облаштування паркувальних місць, облаштування відповідних місць в аудиторіях та приміщень пандусами тощо

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?

Для врегулювання конфліктних ситуацій в Університеті діє Постійна комісія Вченої ради з питань етики, а університетська спільнота керується такими документами та заходами: Положення про організацію освітнього процесу у КНУ імені Тараса Шевченка https://www.knu.ua/pdfs/official/Polozhennia-pro-organizatsiyu-osvitniogo-procesu-11_04_2022.pdf, Порядок вирішення конфліктних ситуацій у КНУ імені Тараса Шевченка https://www.knu.ua/pdfs/official/Procedure-for-resolving-conflict-situations-in-University.pdf, Заходи щодо запобігання та протидії корупції (затверджена Антикорупційна програма https://www.knu.ua/pdfs/official/preventing-corruption/antykoruptsiyna_prohrama.pdf, Етичний кодекс університетської спільноти https://www.knu.ua/pdfs/official/ethical-code/Ethical-code-of-the-university-community.pdf, Порядок запобігання та протидії дискримінації, булінгу, гендерно- обумовленому насильству в КНУ ім. Тараса Шевченка, введений в дію наказом ректора від 08.02.2022 № 79-32 https://www.knu.ua/pdfs/official/Procedure-for-preventing-discrimination-bullying-gender-based-violence-in-University.pdf, Пам'ятка норм етичної поведінки для учасників освітнього процесу КНУ імені Тараса Шевченка, введено в дію наказом ректора від 10.11.2021 № 897-32 https://www.knu.ua/pdfs/official/Memo-of-norms-of-ethical-behavior-in-University.pdf. Здобувачі вищої освіти або співробітники кафедри можуть повідомити про факти корупції анонімно на «скриньку довіри», що розміщена біля викладацької аудиторії кафедри (м. Київ, вул. Б. Гаврилишина, 24, ауд. 407) або надіслати анонімне звернення на сайті кафедри. Випадків конфліктних ситуацій пов'язаних із сексуальними домаганнями, корупцією або дискримінацією на ОП 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) регулюються наступними документами:
1. Положення про організацію освітнього процесу у Київському національному університеті імені Тараса Шевченка (http://nmc.univ.kiev.ua/docs/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. Розділи II.9 та II.10 Положення про систему забезпечення якості освіти та освітнього процесу в Київському національному університеті імені Тараса Шевченка затверджене наказом ректора від 08 липня 2019 за №603-32 (http://nmc.univ.kiev.ua/docs/Polojennya%20QAS%202019.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 проводиться не менше ніж раз на рік. Для обговорення та врахування думки роботодавців, академічної спільноти у процесі розробки ОП залучаються фахівці провідних компаній з інформаційної безпеки та інформаційних технологій. Особливий акцент робиться на науково-дослідній складовій ОП. Пропозиції роботодавців, спрямовані на поглиблення теоретичних знань та розвиток наукових компетентностей здобувачів. (https://kbzi.knu.ua/surveys_of_masters/). 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+ модуль Жан Моне «Інтеграція рамок та політик кібербезпеки ЄС в Україні» тощо. (https://kbzi.knu.ua/surveys_of_masters/). В результатами останнього перегляду ОП було введено цілу низку нових ОК, а саме: «Управління інцедентами інформаційної безпеки», «Реверс-інжиніринг», «Управління безпекою мереж», «Безпека критичної інформаційної інфраструктури», «Форензік аналіз», «Управління ризиками кібербезпеки» та ін.

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 КНУ імені Тараса Шевченка https://www.knu.ua/pdfs/official/Quality-assurance-system-of-education-and-educational-process.pdfз вернення здобувачів освіти або результати опитування здобувачів освіти, які навчаються за освітньою програмою на факультеті, є підставою для ініціювання пропозицій щодо внесення змін до затверджених описів ОП. Кафедрою та факультетом інформаційних технологій проводяться щорічні опитування студентів щодо якості організації освітнього процесу за ОП Кібербезпека, студенти та випускники можуть подавати також свої пропозиції щодо внесення змін до опису ОП, до робочих програм освітніх компонентів, форм та методів навчання, викладання, оцінювання тощо безпосередньо науково-педагогічному працівнику, що залучені до викладання на освітній програмі, гаранту освітньої програми, завідувачу кафедри або надсилати свої пропозиції через сайт кафедри (https://kbzi.knu.ua/location/, e-mail: kbziknu@gmail.com). Отримані пропозиції розглядаються та обговорюються на засіданні кафедри, за рішенням кафедри виносяться до розгляду до науково-методичної комісії факультету та вченої ради факультету тощо 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 Положенням про систему забезпечення якості освіти та освітнього процесу в КНУТШ https://www.knu.ua/pdfs/official/Quality-assurance-system-of-education-and-educational-process.pdf. 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 чинних освітніх програм відповідно є врахування результатів аналізу ринку праці з метою забезпечення потреб ринку висококваліфікованими кадрами. Кафедрою кібербезпеки та захисту інформації та гарантом ОП проводяться постійні консультації з представниками роботодавців з метою визначення актуальни х тенденцій на ринку праці (ТОВ «Акссонсофт», ТОВ «ОМЕГА СОЛЮШИНС», «Sigma Software Group», «SoftServe», «Genesis», ТОВ «Іноваційні ІТ-рішення», «Softengi», ТОВ «BioSol» та з представниками ГО «Українська асоціація ІТ професіоналів»), з представниками наукових установ та академічної спільноти з метою насичення освітнього контенту ОП сучасними науковими досягненнями в області мережевих та інтернет технологій

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 Дня 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 студентських телеграм-каналах 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 процедури, що визначена у Положенні про систему забезпечення якості освіти та освітнього процесу в КНУТШ https://www.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.
В 2019 р. було затверджено нову редакцію ОП, в якій було усунуто певні недоліки, які були виявлені в процесі провадження ОП: було переглянуто концепцію вивчення фундаментальних математичних дисциплін з метою наближення/адаптації змісту дисциплін до сучасних потреб на ринку праці в ІБ, було збільшено обсяги годин (особливо годин для набуття здобувачами освіти практичних навичок). Було перенесені деякі дисципліни у блок обов'язкових.
Після внесення відповідних змін суттєвих недоліків в ОП виявлено не було, але з урахуванням сучасних тенденцій в освітній галузі, в галузі ІТ, виходом 6 професійних стандартів робочою групою при кафедрі кібербезпеки та захисту інформації була підготовлена нова редакція освітньої програми (https://kbzi.knu.ua/onp_magistr_2023/). В новій редакції враховано введення в Україні низькі професійних стандартів, а також запропоновані зміни до організації вільного вибору студентів, впровадження Концепції вивчення іноземних мов Київського Національного університету імені Тараса Шевченка (https://cutt.ly/HC1zE0S), що відповідає Концепції розвитку англійської мови у сфері вищої освіти МОН

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?

На засіданнях кафедри кібербезпеки та захисту інформації проводяться обговорення результатів проведення акредитації освітніх програм Університету ОС "бакалавр" за спорідненими спеціальностями галузі 12 "Інформаційні технології" (https://knu.ua/ua/official/accreditation/master-degree/), а також взяті до уваги аналізи результатів акредитацій освітніх програм КНУТШ у 2019/2020 н.р. http://senate.univ.kiev.ua/?p=1650, у 2020/2021 н.р. http://senate.univ.kiev.ua/?p=1894, та у 2021/2022 н.р. http://senate.univ.kiev.ua/?p=2123 та у 2022/2023 н.р. https://senate.univ.kiev.ua/?p=2445, які розглядались на засіданнях Вченої ради і розсилалися на факультети/інститути.

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 на етапах розроблення, затвердження, моніторингу та періодичного перегляду ОП, 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 (Національний технічний університет України «Київський політехнічний інститут 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 Київського Національного університету імені Тараса Шевченка (https://knu.ua/pdfs/official/Quality-assurance-system-of-education-and-educational-process.pdf) 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 та моніторинг пов'язаних з інформаційним супроводом здобувачів освіти, їх академічною та неакадемічною підтримкою. 2 рівень - кафедри, гаранти програм, проєктні групи, НПП, роботодавці, що відповідають за реалізацію ОП, її моніторинг, ініціювання змін ОП. 3 рівень - структурні підрозділи, які здійснюють освітню діяльність: факультети, їх керівники та 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 та 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, (https://www.facebook.com/department.quality).

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 наступними документами, що знаходяться у

вільному доступі на офіційних сторінках Університету та його структурних підрозділів:
Статут КНУ ім. Тараса Шевченка (Затверджено наказом МОН України від 22.02.2017 р. за №280 (https://www.univ.kiev.ua/pdfs/statut/statut-22-11-28.pdf).
Положення про організацію освітнього процесу у КНУ ім. Тараса Шевченка (http://nmc.univ.kiev.ua/docs/Polozhennia-pro-organizatsiyu-osvitniogo-procesu-11_04_2022.pdf).
Положення про систему забезпечення якості освіти та освітнього процесу в КНУ ім. Тараса Шевченка (https://knu.ua/pdfs/official/Quality-assurance-system-of-education-and-educational-process.pdf).
Положенні про порядок реалізації права на академічну мобільність в КНУ ім. Тараса Шевченка (http://mobility.univ.kiev.ua/?page_id=804&lang=uk)
Етичний кодекс університетської спільноти (https://www.knu.ua/pdfs/official/ethical-code/Ethical-code-of-the-university-community.pdf).
Порядок вирішення конфліктних ситуацій у КНУ ім. Тараса Шевченка https://www.knu.ua/pdfs/official/Procedure-for-resolving-conflict-situations-in-University.pdf Положення про гаранта освітньої програми в КНУ ім. Тараса Шевченка http://senate.univ.kiev.ua/?p=1678.
Правила внутрішнього розпорядку у студентських гуртожитках http://studprof.phys.univ.kiev.ua/?p=41

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

Проєкт (https://kbzi.knu.ua/onp_np_rp_sreak/) поле для зауважень стейкхолдерів розміщується в нижньому правому куті на головній сторінці кафедри, а для для листування email:kbziknu@gmail.com

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
Магістр, ОНП «Кібербезпека»: https://kbzi.knu.ua/magistr/
ОНП (2021) – (https://kbzi.knu.ua/onp_magistr_2021/).
ОНП (2023) – (https://kbzi.knu.ua/onp_magistr_2023/).
Робочі програми навчальних дисциплін (2023) – (https://kbzi.knu.ua/rnp_magistr/).
Навчальний план (2021) – (https://kbzi.knu.ua/np_mag_2021).
Навчальний план (2023) – (https://kbzi.knu.ua/np_mag_2023/).

11. Перспективи подальшого розвитку ОП

Якими загалом є сильні та слабкі сторони ОП?

Сильні сторони:
1. ОП «Кібербезпека» відповідає сучасним викликам у галузі кібербезпеки, що забезпечує її актуальність у контексті швидко змінюючогося кіберландшафту, що швидко змінюється.
2. ОП об'єднує фундаментальні знання з інформаційних технологій, комп'ютерних наук і програмування з глибоким вивченням напрямків досліджень у сфері захисту інформації та кібербезпеки.
3. Високий попит на програму серед абітурієнтів свідчить про її привабливість та репутацію.
4. На ОП забезпечено співпрацю з провідними компаніями та організаціями у сфері кібербезпеки, що дозволяє студентам отримувати практичний досвід та знаходити робочі місця.
5. ОП відповідає світовим стандартам і включає можливості для міжнародного досвіду та обміну знаннями через програми академічної мобільності та партнерства з іноземними університетами.
6. Студентам надаються не лише теоретичні знання, але й практичні навички, необхідні для успішної кар'єри в галузі кібербезпеки. Наприклад, вони мають можливість отримати практичний досвід у провідних компаніях та організаціях, таких як "ДССЗЗІ", "B2B-рішення", "EPAM", ТОВ "Софтпром Солюшнз", ТОВ "МТІ", ТОВ "Ел-Консалтинг", KPMG, CERT та інші. Такі співпраця із відомими гравцями на ринку дозволяє студентам отримати цінний практичний досвід та ознайомитися з сучасними практиками та технологіями у сфері кібербезпеки.
7. На ОП ведеться постійний моніторинг та адаптація програми з урахуванням новітніх наукових тенденцій та вимог ринку та створюються всі можливості для участі студентів у наукових дослідженнях та проектах, що сприяють їх професійному зростанню.
Слабкі сторони:
1. Недостатня активна участь представників відомих компаній та викладачів з міжнародного рівня у навчальному процесі на ОП.
2. Недостатня мотивація студентів до здійснення науково-дослідної роботи.
3. Обмежений доступ до сучасного обладнання та інфраструктури, необхідного для проведення наукових досліджень та практичних занять.

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

Проектування перспектив розвитку ОП наступних трьох років вимагає комплексного підходу та урахування широкого спектру факторів. Ось деякі конкретні заходи, які будуть здійснені на ОП для реалізації цих перспектив

1. Розширення мережі партнерів: укладання нових партнерських угод з відомими компаніями та міжнародними університетами для залучення викладачів та експертів для викладання, а також для організації стажувань та міжнародних обмінів для студентів.
2. Запровадження нових методик навчання: впровадження інноваційних методик навчання, які активно залучатимуть студентів до науково-дослідницької діяльності та сприятимуть їх активній участі у навчальному процес
3. Підвищення мотивації студентів: розробка та впровадження стимулюючих програм для мотивації студентів до науково-дослідницької роботи та участі в наукових конференціях та конкурсах.
4. Підписання угод з провідними компаніями для організації спільних проектів, стажувань та практичних занять для студентів, що дозволить їм отримати практичний досвід у реальних умовах роботи.
5. Аналіз та оптимізація навчального процесу з метою підвищення ефективності навчання та забезпечення високої якості освіти
6. Забезпечення постійного обміну інформацією між успішними випускниками та студентами ОП "Кібербезпека" для сприяння зростанню мережі професійних контактів та передачі цінного досвіду.
7. Створення єдиної навчальної онлайн-платформи

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: Бугров Володимир Анатолійович

Дата: 20.02.2024 р.

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	
Методологія та організація наукових досліджень з основами інтелектуальної власності	навчальна дисципліна	*РНПр МНД за ОНПр 2023р.pdf*	H4eANFebqUWoqKaP6FEEXQvb6sasEisdNKcxzuoKQ8Q=	*Спеціального МТЗ не потребує*
Професійна та корпоративна етика	навчальна дисципліна	*1сем_Маг_ПКЕ_обов_зал_Наконечний_В_С.pdf*	/bW1KwmBD9IZX1dTmsti0q4dPf+2kq7t/rNu6wSS3lM=	*Спеціального МТЗ не потребує*
Реверс-інжиніринг	навчальна дисципліна	*1сем_маг_РЕ_обов_екз.pdf*	ZLVMv4Hb5ysbQWauxKqE93hb/11fnYMLA+fmqpx5vsA=	*ауд. 204, 205 – ПК/Intel x86. Дизасемблери, відладчики, програми для аналізу змін в реєстрі, hex-редактор.*
Управління безпекою мереж	навчальна дисципліна	*1сем_маг_УБМ_обов_екз.pdf*	NdCZ72DJjC35WFggNR1wgbD1l7fv7WI5myCEWJqnoHo=	*SNORT, Surucata, Network Miner, WireShark, Zeek* *Системи виявлення та запобігання вторгненню, аналізатори трафіка, сканери мереж*
Іноземна мова для академічних цілей	навчальна дисципліна	*Іноземна_мова_для_академічних_цілей_КБм.pdf*	KaJThVbMlttpKrRrteoIKT1QM7MHNBzZEIVdo5AVZiM=	*Спеціального МТЗ не потребує*
Аудит інформаційних систем	навчальна дисципліна	*2сем_маг_АІС_обов_екз.pdf*	1SDv4ZApRUYNO6w1G5RTO7k1RQfuehGYKy/rWnNldvo=	*Системи моніторингу, системи тестування на захищеність, сканери інформаційних ресурсів.*
Управління інцидентами інформаційної безпеки	навчальна дисципліна	*РНП УІБ 1к КБм 2023.pdf*	x8mHR5u0+ZH8OM873LBhftgBJ4UOqb+yKJbMXTA2Ywc=	*Не потребую спеціального МТЗ*
Системи управління інформаційною безпекою	навчальна дисципліна	*2сем_маг_СУІБ_обов_зал_.pdf*	7jXr0/sGh6YunEzUxwYQknLgzBFjmWTC5mxp7Pa98EI=	*Не потребує спеціального МТЗ*
Науково-дослідна практика	практика	*4сем_маг_Н_Д_ПРАК.pdf*	MGTcD9VnIo+xJ/aiLVksWdgzLp+vysuOX/mLeACd+gU=	*Спеціального МТЗ не потребує*
Виконання та захист кваліфікаційної роботи	підсумкова атестація	*МДР_магістр.pdf*	Mu7QE6Dey6SCAvfAtai38KzyzXP+CMCehPu3Q2qVUio=	*Спеціального МТЗ не потребує*
Виробнича практика	практика	*2сем_маг_ВИР_ПРАК_обов_диф-зал.pdf*	kB5lhT0HnVm04VFk7BGQsVeQ02mN1kxomUinCwVZSy4=	*Спеціального МТЗ не потребує*
Безпека критичної інформаційної інфраструктури	навчальна дисципліна	*1сем_Маг_БКІІ_обов_зал_.pdf*	2XyHcINrTrttS+VP3pJWEdiawL7TvaTM+CVRMkocXzE=	*Спеціального МТЗ не потребує*
Управління ризиками кібербезпеки	навчальна дисципліна	*2сем_Маг_УРК_обов_зал.pdf*	ejwa4bbWBM9HyU6jJ5pjqtRhxIVmB6oueHIzJCAaRog=	*Спеціального МТЗ не потребує*
Форензік аналіз	навчальна дисципліна	*1сем_маг_ФА_обов_е.pdf*	ij/qTRJCBgS7TtlpKKzvBGozNsxbw5M6Qio0UKbvQXxs=	*Не потребує спеціального МТЗ*

* 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
357801	Зеліковська Олена Олександрівна	доцент, Основне місце роботи	Навчально-науковий інститут філології	Диплом спеціаліста, Український інститут лінгвістики і менеджменту у формі товариства з обмеженою відповідальністю, рік закінчення: 2002, спеціальність: 030505 Прикладна лінгвістика, Диплом кандидата наук ДК 064882, виданий 23.02.2011, Атестат доцента 12ДЦ 038342, виданий 03.04.2014	20	Іноземна мова для академічних цілей	Освіта та науковий ступінь відповідають тематиці дисципліни, наукова робота пов'язана з тематикою дисципліни. 1. ENGLISH FOR IT STUDENTS: Методичні рекомендації для самостійної роботи студентів математичних факультетів Зеліковська О.О. – К., 2020. – 50 с. 2.English for Independent Practice: англійська мова для самостійної роботи студентів: навчальний посібник / Зеліковська О., Соловей Н., Летуновська І. – К.: Редакційно-видавничий центр НУБіП України, 2019. – 150 с. (4,52 д.а. – по 1,5 на кожного співавтора) 3. Авторське право на дослідницьку статтю «Досвід використання smart-технологій у післядипломній освіті лікарів профілактичної ланки». Міністерство економічного розвитку і торгівлі. № 85801. Дата реєстрації 14.02.2019 Публікації за тематикою дисципліни: 1. Virtualization and Programmability in Modern Networks in the Context of SDN Concept. 2022 IEEE 4th International Conference on Advanced Trends in Information Theory (ATIT) 15–17 Dec. 2022. 300-303. DOI: 10.1109/ATIT49449.2019.9030484 A. SCOPUS 2. Development of finance students' professional culture in Ukrainian colleges. Journal of Educational Culture and Society, 2022, Vol.13, №2, 417–430. https://doi.org/10.1550

							3/jecs2022.2.417.430 Web of Science Core collection 3. Специфіка корпоративної освіти в контексті розвитку людських ресурсів корпорації у США «Перспективи та інновації науки (Серія «Педагогіка»)», 2 (7), 2022, 431–443. https://doi.org/10.52058/2786-4952-2022-2(7)-431-443. Index Copernicus; ВАК, В 4. Відкрита освіта: сучасні тренди і нові концепції. Вісник післядипломної освіти. Випуск 21(50) Серія «Педагогічні науки», 2022, 206-218. Міжнародне фахове видання Index Copernicus; ВАК, В https://doi.org/10.32405/2218-7650-2022-21(50)-206-218 5. Information security management system in distributed information systems. 2019 IEEE International Conference on Advanced Trends in Information Theory (ATIT) 18-20 Dec. 2019. 300-303. DOI: 10.1109/ATIT49449.2019.9030484 Міжнародне фахове видання A. SCOPUS 6. Leveraging crowd-based technologies for education in IT-students professional training. Information Technologies and Learning Tools, 2020, 76(2), 213-235. DOI: 10.33407/itlt.v76i2.3378 Міжнародне фахове видання A. Web of Science Core collection 7. The method of improving the signal detection quality by accounting for interference. 2020 IEEE International Conference on Advanced Trends in Information Theory (ATIT) 20-27.11.2020, Kyiv, 172-175. DOI: 10.1109/ATIT50783.2020.9349259 A. SCOPUS Відомості про підвищення кваліфікації: 1. 03.2021 «Віртуальні дошки у навчальному процесі: можливості та перспективи» - 15 год. / 0.5 кредита. 2. 06.2020 «Філологічні й педагогічні студії у вітчизняній та зарубіжній науці XXI

							сторіччя» , КНУ імені Тараса Шевченка, Сертифікат – 60 годин / 2 кредити. 3. .02-.03.2020; «Мобільні технології у навчанні Сертифікат» – 16 годин / 0,53 кредити 4. 09.12.2022 “Erasmus Plus and Micro Credentials Guidelines”, European Training Foundation (a European Union agency). – 2 год. 5. 01.11.2022 “Admin, Faculty and Student Perspectives on Digital Learning in Fall 2022”. Inside Higher Ed. Cengage. – 2 год. 6. 06-07.2022 KNU Educator’s Week – 30 год. Сертифікат 7. 06.2022 “International Trends in Education”. Buda University, Hungary. – 12 год. Сертифікат 8. 05.2022 “Research Smarter: Огляд літератури на відмінно”. Clarivate – 1 год. 9. 05.2022 “Web of Science Core Collection для ефективної наукової діяльності”. Clarivate – 1 год. 10. 02.2022 Курс підвищення кваліфікації та розвитку педагогічних компетентностей викладача. KNU Teach Week 3. – 15 год. Сертифікат № 90-22. 11. 16.11.2022 – 21.12.2022 «Педагогічна освіта та освіта дорослих: національний і європейський вимір». «Центр неперервної освіти» спільно з Інститутом педагогічної освіти і освіти дорослих імені Івана Зязюна НАПН України та Кафедри ЮНЕСКО «Неперервна професійна освіта XXI століття» при ІПООД імені Івана Зязюна НАПН України. – 180 год. (6 кредитів) Сертифікат 16112112/31 від 22.12.2022.
340471	Бучик Сергій Степанович	професор, Основне місце роботи	Факультет інформаційних технологій	Диплом спеціаліста, Житомирське вище военне учілище, рік закінчення: 1993, спеціальність: Радіотехнічні	23	Реверс-інжиніринг	Освіта та науковий ступінь відповідають тематиці дисципліни, наукова робота пов'язана з тематикою дисципліни. Автор понад 160 наукових публікацій за профілем кафедри

				средства, Диплом магістра, Національна академія оборони України, рік закінчення: 2009, спеціальність: Організація бойового та оперативного забезпечення військ, 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			(з них: 67 у періодичних наукових фахових виданнях, 15 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 АП№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. Buchyk S., Shutenko

							D., Toliupa S., (2022) Phishing Attacks Detection. IX International Scientific Conference “Information Technology and Implementation" (IT&I-2022), Workshop Proceedings, Kyiv, Ukraine, November 30 - December 02, 2022., Kyiv, Ukraine, pp. 193–201. URL: https://ceur-ws.org/Vol-3384/Short_7.pdf 6. Toliupa S., Shevchenko A., Buchyk S., Pampukha I., Kulko A. (2023) Managing the Security of the Critical Infrastructure Information Network. Cybersecurity Providing in Information and Telecommunication Systems (CPITS-II 2023), October 26, 2023, Kyiv, Ukraine, pp. 131–142. URL: https://ceur-ws.org/Vol-3550/paper11.pdf 7. 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. 8. Бучик С.С., Толюпа С.В., Шестак Я.В. Прикладні технології програмування в інформаційній безпеці. Лабораторний практикум. – Житомир: ФОП Кирилюк І.В., ПП «Рута», 2023. – 50 с.
37474	Толюпа Сергій Васильович	професор, Основне місце роботи	Факультет інформаційних технологій	Диплом спеціаліста, Київське вище інженерне радіотехнічне училище ППО, рік закінчення: 1986, спеціальність: Автоматизовані системи управління, 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,	31	Управління інцидентами інформаційної безпеки	Освіта та науковий ступінь відповідають тематиці дисципліни, наукова робота пов'язана з тематикою дисципліни. Автор більше 250 наукових публікацій за профілем кафедри. 6 колективних монографій, 61 публікація включені до наукометричної бази Scopus: h-індекс в Scopus - 7, 16 науково-методичних матеріалів (підручники, посібники, лабораторні практикуми). Відомості про підвищення кваліфікації: 1. ТОВ «ДЕПС СЕЛЮШЕНЗ». Сертифікат про

				Атестат професора 12ПР 008351, виданий 25.01.2013			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 Навчально-методичні матеріали, 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., Політанський Р.Л., Лісінський В.В. Управління інформаційною безпекою. Навчальний посібник. За заг. ред. Толюпи С.В. – Чернівці. ЧНУ імені Юрія Федьковича. 2021р. – с. 486. 3. 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. 4. Толюпа С.В., Бучик С.С., Шестак Я.В. Прикладні технології програмування в інформаційній безпеці. Лабораторний практикум. – Житомир: ФОП Кирилюк І.В., ПП «Рута», 2023. – с. 50. 5. Толюпа С.В., Оксіюк О.Г, Вялкова В.І.

							Захист об’єктів інформаційної діяльності. . Навчальний посібник. – К.: “МП Леся”, 2018. – 312с. 6. 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. 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. 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. 3. 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. 4. 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. 5. 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) 6. С.Толюпа, І. Пархоменко, С. Штаненко. Модель системи протидії вторгненням в інформаційних системах. Інфокомунікаційні технології та електронна інженерія. №1. 2021. С. 86-95. (Фахове видання). 7. Самохвалов Юрій, Толюпа Сергій, Штаненко Сергій. Забезпечення кібербезпеки АСУ ТП шляхом застосування ПЛІС технології. Безпека інформаційних систем і технологій. №1. 2021. С. 45-54. 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. 9. 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. 10. 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. 11. Штаненко С.С., Самохвалов Ю.Я., Толюпа С.В. Підхід до виявлення помилок та відновлення правильного функціонування програмних засобів сучасних систем управління, реалізованих за принципом «система на кристалі». Наукоємні технології. – К.: НАУ, 2023. – № 2 (58). – с. 376-384. 12. Сергій Толюпа, Юрій Самохвалов, Павло Хусаінов Сергій, Штаненко. Самодіагностування як спосіб підвищення кіберстійкості термінальних компонентів технологічної системи. Том 2 № 22 (2023): Кібербезпека: освіта, наука, техніка. С. 134-147. 13. Toliupa, S., Shevchenko, A., Buchyk, S., Pampukha, I., Kulko, A. Managing the Security of the Critical Infrastructure Information Network. CEUR Workshop Proceedings, 2023, 3550, страницы 131–142. Scopus. 14. Shestak, Y., Toliupa, S., Shevchenko, A., Torchylo, A., Onyigwang, O.J. Data Pro-cessing Centre's Cyberattack Protection Directions on the Base of Neural Network Algorithms. CEUR Workshop Proceedings, 2023, 3347, pp. 212–221. Scopus. 15. Shtanenko, S., Samokhvalov, Y., Toliupa, S., Silko, O. (2023). The Approach to Assessment of Technical Condition of Microprocessor Systems that Are Implemented on Integrated Circuits with a Programmable Structure. Emerging Networking in the Digital Transformation Age. Lecture Notes in Electrical Engineering, vol 965. Springer, Cham. 16. Buchyk, S., Toliupa, S., Lukova-Chuiko, N., Khomenko, O., Serpinskyi, Y. (2023). Applied Steganographic System for Hiding Textual Information on Audio Files. Emerging

							Networking in the Digital Transformation Age. Lecture Notes in Electrical Engineering, vol 965. Springer, Cham. Scopus.
101846	Бабенко Тетяна Василівна	професор, Основне місце роботи	Факультет інформаційних технологій	Диплом спеціаліста, Дніпропетровський хіміко-технологічний інститут, рік закінчення: 1992, спеціальність: , 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	Аудит інформаційних 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: 67 у періодичних наукових фахових виданнях, 22 публікації включені до наукометричної бази Scopus: h-індекс в Scopus - 6. Публікації за тематикою дисципліни: 1. Palko, D., Babenko, T., Bigdan, A., Gorbovy, O., Borusiewicz, A. Cyber Security Risk Modeling in Distributed Information Systems 2. Applied Sciences (Switzerland), 2023, 13(4), 2393 (SCOPUS) 3. 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) 4. 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) 5. 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 6. 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) 7. 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. 8. 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. 9. Determining key risks for modern distributed information systems Palko, D., Hnatienko, H., Babenko, T., Bigdan, A. CEUR Workshop Proceedings, 2021, 3018, стр. 81–100. 10. 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. 11. 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. 12. 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. 13. 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 14. 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. 15. 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. 16. 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 17. 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. 18. 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. 19. 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. 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). 3. Certificate of completion Cyber-Physical System Security within the 2021 Cybersecuriti Summer Training Program under the USAID Project. 14 june - 23 july 2021.
185330	Пархоменко Іван Іванович	доцент, Основне місце роботи	Факультет інформаційних технологій	Диплом спеціаліста, Український державний університет харчових технологій, рік закінчення: 1996, спеціальність: Автоматизація технологічних процесів у виробництві, Диплом кандидата наук ДК 015285, виданий	25	Управління безпекою мереж	Освіта та науковий ступінь відповідають тематиці дисципліни, наукова робота пов'язана з тематикою дисципліни. Автор понад 100 наукових публікацій за профілем кафедри (з них 75 наукових і 8 навчально-методичних, зокрема 1 колективні монографії, 67 статтей, з яких 28 у вітчизняних фахових виданнях, 17 у закордонних

				03.07.2002, Атестат доцента 12ДЦ 017184, виданий 21.06.2007			виданнях, 9 публікацій включені до наукометричної бази Scopus, h-індекс - 3). Публікації за тематикою дисципліни: 1. Toliupa S, Parkhomenko I, Shvedova H «Security and regulatory aspects of the critical infrastructure objects functioning and cyberpower level assesment» / 2019 3rd International Conference on Advanced Information and Communications Technologies, AICT 2019 - Proceedings (2019) - paper 463 – 469 (https://www.scopus.com/authid/detail.uri?authorId=57194039632) 2. 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 3. 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. 4. 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. 5. 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) 6. Сергій Толюпа, Людмила Терейковська, Іван Пархоменко, 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. 7. Toliupa S., Parkhomenko I., Antoniuk V. Method for Identification of Critical Information Infrastructure Objects of the State. CEUR Workshop Proceedingsthis link is disabled, 2021, 3179,58) 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. 9. pp. 262–271 10. С. Толюпа, І. Пархоменко, С. Штаненко. Модель системи протидії вторгненням в інформаційних системах. Інфокомунікаційні технології та електронна інженерія. №1. 2021. 11. Лукова-Чуйко Наталія, Толюпа Сергій, Пархоменко Іван, Методи виявлення вторгнень в сучасних системах IDS, Науковий журнал “Безпека інформаційних систем і технологій”, 2021 3-4, с.63 12. Лаптєв Олександр, Савченко Віталій, Пономаренко Віталій, Пархоменко Іван. Удосконалення методу підвищення

							завадостійкості систем виявлення сигналів засобів негласного здобуття інформації. Захист інформації. Том 24 № 3 (2022): Захист інформації. с.128-136. 13. Даков С.Ю., Дакова Л.В., Блаженний Н.В., Стадник Д.О., Пархоменко І.І., Механізми безпеки в хмарному середовищі на базі міжнародних стандартів. Зв'язок, № 4 (2022), Державний університет телекомунікацій. с. 37-43. 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 15. 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 16. Дослідження мобільного широкосмугового зв'язку із застосуванням штучного інтелекту Руденко Н. В., Дакова Л. В., Даков С. Ю., Пархоменко І. І., Блаженний Н. В. Зв'язок, № 2 (162) (2023), Державний університет телекомунікацій. 17. Laptiev, O., Makarchuk, A., Parkhomenko, I., Musienko, A., Shapovalov, D. Weierstrass Method of Analogue Signal Approximation, IEEE 4th KhPI Week on

							Advanced Technology, KhPI Week 2023 - Conference Proceedings, 2023 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 Cyber-Physical System Security within the 2021 Cybersecuriti Summer Training Program under the USAID Project. 14 june - 23 july 2021. 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 спеціаліста, Житомирське вище военне учілище, рік закінчення: 1993, спеціальність: Радіотехнічні средства, Диплом магістра, Національна академія оборони України, рік закінчення: 2009, спеціальність: Організація бойового та оперативного забезпечення військ, Диплом доктора наук ДД 006141, виданий 13.12.2016, Диплом кандидата наук ДК 025900, виданий 13.10.2004, Атестат доцента 12ДЦ 019379,	23	Форензік аналіз	Освіта та науковий ступінь відповідають тематиці дисципліни, наукова робота пов'язана з тематикою дисципліни. Автор понад 160 наукових публікацій за профілем кафедри (з них: 67 у періодичних наукових фахових виданнях, 15 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.

				виданий 03.07.2008, Атестат професора АП 002394, виданий 09.02.2021			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. Buchyk S., Shutenko D., Toliupa S., (2022) Phishing Attacks Detection. IX International Scientific Conference “Information Technology and Implementation" (IT&I-2022), Workshop Proceedings, Kyiv, Ukraine, November 30 - December 02, 2022., Kyiv, Ukraine, pp. 193–201. URL: https://ceur-ws.org/Vol-3384/Short_7.pdf
6. Toliupa S., Shevchenko A., Buchyk S., Pampukha I., Kulko A. (2023) Managing the Security of the Critical Infrastructure Information Network. Cybersecurity Providing in Information and

							Telecommunication Systems (CPITS-II 2023), October 26, 2023, Kyiv, Ukraine, pp. 131–142. URL: https://ceur-ws.org/Vol-3550/paper11.pdf 7. 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. 8. Бучик С.С., Толюпа С.В., Шестак Я.В. Прикладні технології програмування в інформаційній безпеці. Лабораторний практикум. – Житомир: ФОП Кирилюк І.В., ПП «Рута», 2023. – 50 с.
37474	Толюпа Сергій Васильович	професор, Основне місце роботи	Факультет інформаційних технологій	Диплом спеціаліста, Київське вище інженерне радіотехнічне училище ППО, рік закінчення: 1986, спеціальність: Автоматизовані системи управління, 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	31	Системи управління інформаційною безпекою	Освіта та науковий ступінь відповідають тематиці дисципліни, наукова робота пов'язана з тематикою дисципліни. Автор більше 250 наукових публікацій за профілем кафедри. 6 колективних монографій, 61 публікація включені до наукометричної бази Scopus: h-індекс в Scopus 7, 16 науково-методичних матеріалів (підручники, посібники, лабораторні практикуми). 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 Навчально-методичні матеріали, 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., Політанський Р.Л., Лісінський В.В. Управління інформаційною безпекою. Навчальний посібник. За заг. ред. Толюпи С.В. – Чернівці. ЧНУ імені Юрія Федьковича. 2021р. – с. 486. 3. 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. 4. 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. 5. Толюпа С.В., Бучик С.С., Шестак Я.В. Прикладні технології програмування в інформаційній безпеці. Лабораторний практикум. – Житомир: ФОП Кирилюк І.В., ПП «Рута», 2023. – с. 50. 6. Толюпа С.В., Оксіюк О.Г, Вялкова В.І. Захист об’єктів інформаційної діяльності. . Навчальний посібник. – К.: “МП Леся”, 2018. – 312с. 7. 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. 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. 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. 3. 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. 4. 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. 5. 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) 6. С.Толюпа, І. Пархоменко, С. Штаненко. Модель системи протидії вторгненням в інформаційних системах. Інфокомунікаційні технології та електронна інженерія. №1. 2021. С. 86-95. (Фахове видання). 7. Самохвалов Юрій, Толюпа Сергій, Штаненко Сергій. Забезпечення кібербезпеки АСУ ТП шляхом застосування ПЛІС технології. Безпека інформаційних систем і технологій. №1. 2021. С. 45-54. 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. 9. 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. 10. 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. 11. Штаненко С.С., Самохвалов Ю.Я., Толюпа С.В. Підхід до виявлення помилок та відновлення правильного

							функціонування програмних засобів сучасних систем управління, реалізованих за принципом «система на кристалі». Наукоємні технології. – К.: НАУ, 2023. – № 2 (58). – с. 376-384. 12. Сергій Толюпа, Юрій Самохвалов, Павло Хусаінов Сергій, Штаненко. Самодіагностування як спосіб підвищення кіберстійкості термінальних компонентів технологічної системи. Том 2 № 22 (2023): Кібербезпека: освіта, наука, техніка. С. 134-147. 13. Toliupa, S., Shevchenko, A., Buchyk, S., Pampukha, I., Kulko, A. Managing the Security of the Critical Infrastructure Information Network. CEUR Workshop Proceedings, 2023, 3550, страницы 131–142. Scopus. 14. Shestak, Y., Toliupa, S., Shevchenko, A., Torchylo, A., Onyigwang, O.J. Data Pro-cessing Centre's Cyberattack Protection Directions on the Base of Neural Network Algorithms. CEUR Workshop Proceedings, 2023, 3347, pp. 212–221. Scopus. 15. Shtanenko, S., Samokhvalov, Y., Toliupa, S., Silko, O. (2023). The Approach to Assessment of Technical Condition of Microprocessor Systems that Are Implemented on Integrated Circuits with a Programmable Structure. Emerging Networking in the Digital Transformation Age. Lecture Notes in Electrical Engineering, vol 965. Springer, Cham. 16. Buchyk, S., Toliupa, S., Lukova-Chuiko, N., Khomenko, O., Serpinskyi, Y. (2023). Applied Steganographic System for Hiding Textual Information on Audio Files. Emerging Networking in the Digital Transformation Age. Lecture Notes in Electrical Engineering, vol 965. Springer, Cham. (Scopus)
333375	Наконечний	професор,	Факультет	Диплом	27	Безпека	Освіта та науковий

	Володимир Сергійович	Основне місце роботи	інформаційних технологій	спеціаліста, Київським вищим цінженерно радіотехнічним училищем ПВО, рік закінчення: 1986, спеціальність: , Диплом доктора наук ДД 004837, виданий 29.09.2015, Диплом кандидата наук ДК 005905, виданий 09.02.2000, Атестат професора АП 002910, виданий 29.06.2021, Атестат старшого наукового співробітника (старшого дослідника) АС 006504, виданий 09.04.2008		критичної інформаційної інфраструктури	ступінь відповідають тематиці дисципліни, наукова робота пов'язана з тематикою дисципліни. Автор понад 170 наукових публікацій за профілем кафедри (з них 87 наукових і 3 навчально-методичних, зокрема 4 колективні монографії, 21 стаття з яких 3 у вітчизняних фахових виданнях, 6 у закордонних виданнях,, 29 публікацій включені до наукометричної бази Scopus: h-індекс в Scopus - 5). Відомості про підвищення кваліфікації: Стажування Варшава, Республіка Польща, від 09 листопада - 18 грудня 2020 р. сертифікат NR164/2020 (180 год) . 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. Перші Київські державні курси іноземних мов, 04.02.2019 - 20.06.2019, свідоцтво про позашкільну освіту №25365 від 21.06.2019 р. Публікації за тематикою дисципліни: 1. Nakonechnyi V. Signature and statistical analyzers in the cyberattack detection system. // V. Nakonechnyi, S. Toliupa, O. Uspenskyi. Information Technology and Security. – January-June 2019. – Vol. 7, Iss. 1(12). – pp. 69–79. 2. Nakonechnyi V. Quality Assurance of Data Transmission in Queuing Networks. / V. S. Nakonechnyi, Komarova L.A., Saiko V. G., Toliupa S.V. // International Journal of Engineering and Advanced Technology (IJEAT) Volume-9 Issue-2, December, 2019. pp. 4019-4024 3. Toliupa S. The Increase of The Energy

Efficiency of the Radio Equipment Based on the Use of Modulation by Orthogonal Harmonic Carriers. / S. Toliupa, V. Nakonechnyi, A. Trush // Informatyka, Automatyka, Pomiary W Gospodarce I Ochronie Środowiska, Vol 10 No 1 (2020). pp. 24-27.
4. Kucherov D. Assessing the Operator's Readiness to Perform Tasks of Controlling by the Unmanned Aerial Platforms./ D. Kucherov, V/ Nakonechnyi, O. Sushchenko, A. Kozub // Advances in Science, Technology and Engineering Systems Journal Vol. 5, No. 4, 2020. pp. 457-462.
5. Nakonechnyi V., Steshenko G.M., Buchyk S.S., Kresina I.O. The mechanics of the blockchain technology. International Journal of Advanced Trends in Computer Science and Engineering. Volume 9(2), pp. 1978-1980. March-April – 2020. SCOPUS
6. Nakonechnyi V., Bichkov O.S., Lukova-Chuiko N.V., Panayotova G.S. Measuring the effectiveness of a radio-identification system. Journal of Communications, 2020 Volume 15(9), pp. 669-675. SCOPUS
7. Толюпа С.В., Наконечний В.С., Штаненко С.С. Алгоритм протидії кібератакам на основі стеганографічних методів технології SOFT TEMPEST. Збірник наукових праць Військового інституту телекомунікацій та інформатизації імені Героїв Крут Випуск № 1. 2020р. с. 56-66.
8. Толюпа С.В., Наконечний В.С. Проблеми захисту критично важливих об'єктів інфраструктури. Безпека інформаційних систем і технологій. Том 1 № 2 (2020). с. 57-65.
9. Толюпа Сергій, Наконечний Володимир, Лукова-Чуйко Наталія,

							Кулініч Олег. Формування стратегії управління режимами роботи систем захисту на основі моделі ігрового управління. Науковий журнал «Безпека інформаційних систем і технологій» 2020. №3. – с. 78-86. 10. Kucherov D., Nakonechnyi V., Sushchenko O., Kozub A. Assessing the operator's readiness to perform tasks of controlling by the unmanned aerial platforms. Advances in Science, Technology and Engineering Systems, 2020, 5(4), pp. 457-462. SCOPUS. 11. Model of Increase of Spectral Efficiency of Use of Frequency Resource of Low-Orbit System with Architecture of the Distributed Satellite Saiko, V., Toliupa, S., Nakonechnyi, V., Brailovskyi, M., Domrachev, V. Lecture Notes in Electrical Engineeringthis link is disabled, 2022, 831, pp. 410–423. Book Chapter 12. Oleksandr Laptiev, Serhiy Buchyk, Vitalii Savchenko, Volodymyr Nakonechny, Inna Mykhalchuk, Yanina Shestak DETECTION AND BLOCKING SLOW DDOS ATTACKS BASED ON PREDICTING USER BEHAVIOR Vol. 55 No. 3 (2022) Published: 2022-11-02 p.p. 184-192. 13. Nakonechnyi V., Saiko, V., Tolupa, S., Andreeva, K. Realization of LEO-systems with architecture of distributed satellites for 5G/IOT. CMiGIN 2019 Conflict Management in Global Information Networks Proceedings of the International Workshop on Conflict Management in Global Information Networks (CMiGIN 2019) colocated with 1st International Conference on Cyber Hygiene and Conflict Management in Global Information Networks (CyberConf 2019) Lviv, Ukraine, November 29, 2019. pp. 604-613. SCOPUS 14. Наконечний В.С. Застосування методів

							теорії ігор для вирішення задач управління інформаційною безпекою. / В.С. Наконечний, В.А. Дружинін, С.В. Толюпа // “Наукоємні технології в інфокомунікація НІСТ’2019”. Матер. III Міжнародної науково-практичної конференції 23-25 травня 2019 р. Харків-Кам’янець-Подільськ 15. Nakonechnyi V., Slipachuk, L., Toliupa, S. The Process of the Critical Infrastructure Cyber Security Management using the Integrated System of the National Cyber Security Sector Management in Ukraine. 2019 3rd International Conference on Advanced Information and Communications Technologies, AICT 2019, Proceedings, 2-6 July 2019, Lviv, Ukraine pp. 451-454. SCOPUS 16. Nakonechnyi V., Toliupa, S., Tereikovska, L., Tereikovskyi, I. One-periodic template marks model of normal behavior of the safety parameters of information systems networking resources.2019 IEEE International Scientific-Practical Conference: Problems of Infocommunications Science and Technology, PIC S and T 2019 - Proceedings, 2019, October 8-11, 2019 Kyiv , Ukraine, pp. 764-768. SCOPUS. 17. Nakonechnyi V., Saiko V., Narytnyk T., Brailovskyi M. Radiating telecommunication system of the sub-THz-band to protect objects from unauthorized access. 2019 IEEE Interna-tional Scientific-Practical Conference: Problems of Infocommunications Science and Tech-nology, PIC S and T 2019 - Proceedings. 2019 October 8-11, 2019 Kyiv, Ukraine, pp. 698-702. SCOPUS 18. Tereikovskyi, I., Subach, I., Tereikovskyi, O., Tereikovska, L., Toliupa, S., &

							Nakonechnyi, V. (2020). Parameter Definition for Multilayer Perceptron Intended for Speaker Identifica-tion (pp. 227–231). Institute of Electrical and Electronics Engineers (IEEE). Scopus. https://doi.org/10.1109/atit49449.2019.9030504 19. Nakonechnyi V., Snitsarenko P., Mikhieiev Y. The Approach to Automated Internet Moni-toring System Creation. 2019 IEEE International Conference on Advanced Trends in Infor-mation Theory, ATIT 2019 – Proceedings, 2019, 18-20 Dec. 2019. Kyiv, Ukraine pp. 257-261. SCOPUS 20. Slipachuk L., Nakonechnyi V. Typology of the Model of Integrated Sectoral Information System of the National Cyber Security Management. 2019 IEEE International Conference on Advanced Trends in Information Theory, ATIT 2019 – Proceedings, 2019, 18-20 Dec. 2019, Kyiv, Ukraine pp. 271-276. SCOPUS 21. Nakonechnyi V. Model of the process of optimal planning of the modular structure of an information security system. / V. Nakonechnyi, S. Toliupa, V. Druzhinin, M. Kotov // Інформаційні технології та взаємодії (IT&I 2019)". Матеріали доповідей VI Міжнародної науково-практичної конференції. 20 грудня 2019 р. К.: Київ. КНУ ім. Тараса Шевченка 2019. - 418 с. С. 267-270. 22. Наконечний В.С. Алгоритм обробки сигналів багатопозиційної системи, що використовує принцип просторово-розподіленого випромінювання. / В.С. Наконечний, В.Г. Сайко, Т.М. Наритник, Н.М. Сивкова // The 3rd International scientific and practical conference "Eurasian

							scientific congress" (March 22-24, 2020) Barca Academy Publishing, Barcelona, Spain. 2020. 475 p. pp. 155-160. 23. Наконечний В.С., Сайко В.Г., Сивкова Н.М. «Модель оцінки методу завадостійкого прийому сигналів, які випромінюються просторово - рознесеними передавачами»: тези доп. Abstracts of XII International Scientific and Practical Conference «IMPACT OF MODERNITY ON SCIENCE AND PRACTICE» Edmonton, Canada 13-14 April 2020р. - с.582-586. 24. Наконечний В.С., Сайко В.Г., Сивкова Н.М. «Модель обробки сигналів від просторово-рознесених передавачів терагерцового діапазону»: тези доп. The 17 th International scientific and practical conference «SCIENCE, TRENDS AND PERSPECTIVES» - Tokyo, Japan 18-19 May, 2020р. – с.336-340. 25. Наконечний В.С., Сайко В.Г., Сивкова Н.М. «Динамічна модель оцінки дальності зв'язку багатопозиційної системи на основі просторово-рознесених пристроїв»: тези доп. The 18 th International scientific and practical conference «MODERN SCIENCE, PRACTICE, SOCIETY» (25-26 May 2020). Boston, USA 2020, - с.410-414. 26. Nakonechnyi V., Toliupa S., Tereikovskyi I., Kulakov Y. Keyboard Dynamic Analysis by Alexnet Type Neural Network. 2020 IEEE 15th International Conference on Advanced Trends in Radioelectronics, Telecommunications and Computer Engineering (TCSET) 25 - 29 February, 2020. pp. 416-420. SCOPUS 27. Nakonechnyi V., Saiko V., Brailovskyi M., Lukova-Chuiko N. Terahertz Range Interconnecting Line for LEO-System. 2020 IEEE 15th International

							Conference on Advanced Trends in Radioelectronics, Telecommunications and Computer Engineering (TCSET) 25 - 29 February, 2020. pp. 425-429. SCOPUS 28. Nakonechnyi V., Saiko V., Brailovskyi M., Toliupa S. Increasing Noise Immunity between LEO Satellite Radio Channels. 2020 IEEE 15th International Conference on Advanced Trends in Radioelectronics, Telecommunications and Computer Engineering (TCSET) 25 - 29 February, 2020. pp. 442-446. SCOPUS 29. Saiko, V., Toliupa, S., Nakonechnyi, V., Brailovskyi, M. Models of Improving the Efficiency of Radio Communication Systems Using the Terrahert Range (2021) 2020 IEEE International Conference on Problems of Infocommunications Science and Technology, PIC S and T 2020 - Proceedings, art. no. 9468022, pp. 192-196. Conference Paper EID: 2- s2.0-85114389274 DOI: 10.1109/PICST51311.2020.9468022 CiteScore 2020 = n/a 2020 IEEE International Conference on Problems of Infocommunications Science and Technology, PIC S and T 2020 Kharkiv, Ukraine 6 October 2020 through 9 October 2020 30. Nakonechnyi V., Toliupa, S., Kotov, M., Solodovnyk V. RF signals encryption with AES in WDID. CEUR Workshop Proceedings, 2021, 2845, p.p. 96–105. SCOPUS 46. Nakonechnyi V., Saiko, V., Toliupa, S., Kotov, M., Astapenya, V. Method of determining the angular orientation of small satellites in orbit. Proceedingsthis link is disabled, 2021, 2923, p.p. 224–233. SCOPUS 31. Building an Intrusion Detection System in Critically Important Information Networks with Application of Data

							Mining Methods Toliupa, S., Buchyk, S., Nakonechnyi, V., ...Parkhomenko, I., Lukova-Chuiko, N. Proceedings - 16th International Conference on Advanced Trends in Radioelectronics, Telecommunications and Computer Engineering, TCSET 2022, 2022, стр. 128–133. SCOPUS 32. Наконечний В.С. Новітні біометричні технології в системах контролю управління доступом / В.С. Наконечний, Г. Кулеша // Проблеми кібербезпеки інформаційно-телекомунікаційних систем: Збірник матеріалів доповідей та тез; м. Київ, 27-28 жовтня 2022 року; Київський національний університет імені Тараса Шевченка / Редкол.: В.В. Ільченко. (голова) та ін. –К.: ВПЦ "Київський університет", 2022. – С.9-10. 33. Valentyn Sobchuk, Serhii Laptiev, Andrii Sobchuk, Iryna Zamrii, Volodymyr Nakonechnyi, Yurii Shcheblanin. Estimates for Harmonic Operators in Modeling Application Processes/2022 IEEE Third International Conference on SYSTEM ANALYSIS & INTELLIGENT COMPUTING (SAIC), 04-07 Oktober, Kyiv, Ukraine. p. 148-153 https://ieeexplore.ieee.org/xpl/conhome/9922952/proceeding SCOPUS 34. Oleksandr Laptiev, Igor Polovinkin, Andrii Sobchuk,Sergii Kopytko, Volodymyr Nakonechnyi, Serhii Buchyk. The method of detection of signals using differential transformation. “Modern information, measurement and control systems: problems, applications and perspectives’2022” (MIMCS’2022). November 4-5, 2022, Antalya, Turkey. 35. Vitalii Savchenko, Oleksandr Laptiev, Vitalii Ponomarenko, Taras Dzyuba, Yuriy Shcheblanin , Valeriia

							Savchenko. The method of localization of signals of radio transmitting devices. “Modern information, measurement and control systems: problems, applications and perspectives’2022” (MIMCS’2022). November 4-5, 2022, Antalya, Turkey. 36. Vladyslav LUTSENKO, Volodymyr NAKONECHNYI, Serhii TOLUPA, Volodymyr SAIKO BLOCKCHAIN TECHNOLOGY USAGE IN THE BANKING INDUSTRY / The 2st International Conference on Emerging Technology Trends on the Smart Industry and the Internet of Things January 24-25th 2023. pp. 61 – 66. 37. Золотарьов К. Нейронні мережі як засіб для виявлення аномалій трафіку / К. Золотарьов, В. Наконечний // Проблеми кібербезпеки інформаційно-телекомунікаційних систем: Збірник матеріалів доповідей та тез; м. Київ, 27 квітня 2023 року; Київський національний університет імені Тараса Шевченка / Редкол.: В.В. Ільченко, д.ф-м.н., проф., (голова); та ін. – К.: ВПЦ "Київський університет", 2023. – 166 с. (с.17-18) 38. Maksym Kotov, Serhii Toliupa, Volodymyr Nakonechnyi / Node.js Package Management And Security // Проблеми кібербезпеки інформаційно-телекомунікаційних систем: Збірник матеріалів доповідей та тез; м. Київ, 27 квітня 2023 року; Київський національний університет імені Тараса Шевченка / Редкол.: В.В. Ільченко, д.ф-м.н., проф., (голова); та ін. – К.: ВПЦ "Київський університет", 2023. – 166 с. (с.36-37) 39. Андрейчук О. Удосконалення процесу забезпечення інформаційної

							безпеки за рахунок комбінації методів її оцінки / О. Андрейчук, В. Наконечний // Проблеми кібербезпеки інформаційно-телекомунікаційних систем: Збірник матеріалів доповідей та тез; м. Київ, 27 квітня 2023 року; Київський національний університет імені Тараса Шевченка / Редкол.: В.В. Ільченко, д.ф-м.н., проф., (голова); та ін. – К.: ВПЦ "Київський університет", 2023. – 166 с. (с.83-85) 40. Conference Paper. Smart Home Network based on Cisco Equipment Kolbasova, K., Zhurakovskyi, B., Poltorak, V., Nakonechnyi, V., Kyrychok, R. CEUR Workshop ProceedingsThis link is disabled., 2023, 3550, pp. 70–80. SCOPUS Монографії 1. 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. 2. Сайко В.Г. Мережі мобільного зв'язку нового покоління 4G/5G/6G // Сайко В.Г., Одарченко Р.С., Абакумова А.О., Наритник Т.М., Наконечний В.С., Домрачев В.М., Толюпа С.В., Заблоцький В.Ю., Баховський П.Ф.: Монографія. – К.: ТОВ «Про формат», 2021. – 200 с.
333375	Наконечний Володимир Сергійович	професор, Основне місце роботи	Факультет інформаційних технологій	Диплом спеціаліста, Київським вищим цінженерно радіотехнічним училищем ПВО, рік закінчення: 1986, спеціальність: , Диплом доктора наук ДД 004837, виданий	27	Професійна та корпоративна етика	Освіта та науковий ступінь відповідають тематиці дисципліни, наукова робота пов'язана з тематикою дисципліни. Автор понад 170 наукових публікацій за профілем кафедри (з них 87 наукових і 3 навчально-методичних, зокрема 4 колективні монографії, 21 стаття з яких 3 у вітчизняних

				29.09.2015, Диплом кандидата наук ДК 005905, виданий 09.02.2000, Атестат професора АП 002910, виданий 29.06.2021, Атестат старшого наукового співробітника (старшого дослідника) АС 006504, виданий 09.04.2008			фахових виданнях, 6 у закордонних виданнях,, 29 публікацій включені до наукометричної бази Scopus, h-індекс в Scopus - 5). Відомості про підвищення кваліфікації: 1. Стажування Варшава, Республіка Польща, від 09 листопада - 18 грудня 2020 р. сертифікат NR164/2020 (180 год) . 2. 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. 3. Перші Київські державні курси іноземних мов, 04.02.2019 - 20.06.2019, свідоцтво про позашкільну освіту №25365 від 21.06.2019 р. Публікації за тематикою дисципліни: 1. Наконечний В.С. Особливості підготовки фахівців з кібербезпеки. / В.С. Наконечний // Scientific and pedagogic internship «Modern process of technical education reforming in Ukraine and EU countries»: Internship proceedings, November 19-30, 2018. Stalowa Wola. 60 pp. 12-18. 2. Наконечний В.С. Застосування методів теорії ігор для вирішення задач управління інформаційною безпекою. / В.С. Наконечний, В.А. Дружинін, С.В. Толюпа // “Наукоємні технології в інфокомунікація НІСТ’2019”. Матер. III Міжнародної науково-практичної конференції 23-25 травня 2019 р. Харків-Кам’янець-Подільськ. 3. Nakonechnyi V., Steshenko G.M., Buchyk S.S., Kresina I.O. The mechanics of the blockchain technology. International Journal of

							Advanced Trends in Computer Science and Engineering. Volume 9(2), pp. 1978-1980. March-April – 2020. (SCOPUS) 4. Толюпа С.В., Наконечний В.С., Штаненко С.С. Алгоритм протидії кібератакам на основі стеганографічних методів технології SOFT TEMPEST. Збірник наукових праць Військового інституту телекомунікацій та інформатизації імені Героїв Крут Випуск № 1. 2020р. с. 56-66. 5. Володимир Наконечний, Олександр Лаптєв, Сергій Погасій, Сергій Лазаренко, Ганна Мартинюк. Відбір джерел з неправдивою інформацію методом бджолиної колонії. Наукоємні технології. Інформаційні технології, кібербезпека. Том 52 № 4 (2021) стр.330-337. DOI: https://doi.org/10.18372/2310-5461.52.16379. 6. Наконечний В.С. Підготовка фахівців ІТ-технологій і сфери безпеки – пріоритетне завдання нашого сьогодення. / В.С. Наконечний, І.І. Пархоменко, С.В. Толюпа // “Прикладні системи та технології в інформаційному суспільстві”. Зб. тез доповідей і наук. повідомл. учасників ІІІ Міжнародної науково-практичної конференції Київ, 30 вересня 2019 р. – К.: КНУ ім. Тараса Шевченка, 2019. – 213 с. С. 179-182. 7. Tereikovskyi, I., Subach, I., Tereikovskyi, O., Tereikovska, L., Toliupa, S., & Nakonechnyi, V. (2020). Parameter Definition for Multilayer Perceptron Intended for Speaker Identification (pp. 227–231). Institute of Electrical and Electronics Engineers (IEEE). Scopus. https://doi.org/10.1109/atit49449.2019.9030504 8. Slipachuk L., Nakonechnyi V. Typology of the Model

							of Integrated Sectoral Information System of the National Cyber Security Management. 2019 IEEE International Conference on Advanced Trends in Information Theory, ATIT 2019 – Proceedings, 2019, 18-20 Dec. 2019, Kyiv, Ukraine pp. 271-276. (SCOPUS) 9. Nakonechnyi V. Model of the process of optimal planning of the modular structure of an information security system. / V. Nakonechnyi, S. Toliupa, V. Druzhinin, M. Kotov // Інформаційні технології та взаємодії (IT&I 2019)". Матеріали доповідей VI Міжнародної науково-практичної конференції. 20 грудня 2019 р. К.: Київ. КНУ ім. Тараса Шевченка 2019. - 418 с. С. 267-270. 10. Nakonechnyi V., Toliupa S., Tereikovskyi I., Kulakov Y. Keyboard Dynamic Analysis by Alexnet Type Neural Network. 2020 IEEE 15th International Conference on Advanced Trends in Radioelectronics, Telecommunications and Computer Engineering (TCSET) 25 - 29 February, 2020. pp. 416-420. SCOPUS 11. Наконечний В.С. Способи копіювання носіїв інформації в комп'ютерній криміналістиці. / В.С. Наконечний, С.В. Толюпа, А.А. Побережний // Матеріали X всеукраїнської науково-практичної конференції "Актуальні питання забезпечення службово-бойової діяльності військових формувань та правоохоронних органів" Національна Академія національної гвардії України Науково-дослідний центр службово-бойової діяльності Національної гвардії України. Науково-дослідна лабораторія забезпечення службово-бойової діяльності Національної гвардії

							України” – 345 с. 29 жовтня 2021 р. Харків 12. Building an Intrusion Detection System in Critically Important Information Networks with Application of Data Mining Methods Toliupa, S., Buchyk, S., Nakonechnyi, V., ...Parkhomenko, I., Lukova-Chuiko, N. Proceedings - 16th International Conference on Advanced Trends in Radioelectronics, Telecommunications and Computer Engineering, TCSET 2022, 2022, стр. 128–133. SCOPUS 13. Наконечний В.С. Машинне навчання як засіб захисту інформаційних ресурсів у корпоративних мережах. / В.С. Наконечний, В.Г. Сайко, Л. Кравченко // Прикладні системи та технології в інформаційному суспільстві: зб. тез доповідей і наук. повідомл. учасників VI Міжнародної науково-практичної конференції (Київ, 30 вересня 2022 р.) С.148-152. / за заг. ред. В. Плескач, В. Зосімов, М. Пирог – К.: Київський нац. ун-т ім. Тараса Шевченка, 2022. – 276 с 14. Наконечний В.С. Використання машинного навчання для запобігання витоку інформації в корпоративних мережах / В.С. Наконечний, Л. Кравченко // Проблеми кібербезпеки інформаційно-телекомунікаційних систем: Збірник матеріалів доповідей та тез; м. Київ, 27-28 жовтня 2022 року; Київський національний університет імені Тараса Шевченка / Редкол.: В.В. Ільченко. (голова) та ін. – К.: ВПЦ "Київський університет", 2022. – С.7-8 15. Наконечний В.С. Новітні біометричні технології в системах контролю управління доступом / В.С.

							Наконечний, Г. Кулеша // Проблеми кібербезпеки інформаційно-телекомунікаційних систем: Збірник матеріалів доповідей та тез; м. Київ, 27-28 жовтня 2022 року; Київський національний університет імені Тараса Шевченка / Редкол.: В.В. Ільченко. (голова) та ін. –К.: ВПЦ "Київський університет", 2022. – С.9-10. 16. Valentyn Sobchuk, Serhii Laptiev, Andrii Sobchuk, Iryna Zamrii, Volodymyr Nakonechnyi, Yurii Shcheblanin. Estimates for Harmonic Operators in Modeling Application Processes/2022 IEEE Third International Conference on SYSTEM ANALYSIS & INTELLIGENT COMPUTING (SAIC), 04-07 Oktober, Kyiv, Ukraine. p. 148-153 https://ieeexplore.ieee.org/xpl/conhome/9922952/proceeding (SCOPUS) 17. Vladyslav LUTSENKO, Volodymyr NAKONECHNYI, Serhii TOLUPA, Volodymyr SAIKO BLOCKCHAIN TECHNOLOGY USAGE IN THE BANKING INDUSTRY / The 2st International Conference on Emerging Technology Trends on the Smart Industry and the Internet of Things January 24-25th 2023. pp. 61 – 66. 18. Корнецький Д. Розвідка на основі відкритих джерел та її вплив на кібербезпеку / Д. Корнецький, В. Наконечний // Проблеми кібербезпеки інформаційно-телекомунікаційних систем: Збірник матеріалів доповідей та тез; м. Київ, 27 квітня 2023 року; Київський національний університет імені Тараса Шевченка / Редкол.: В.В. Ільченко, д.ф-м.н., проф., (голова); та ін. – К.: ВПЦ "Київський університет", 2023. – 166 с. (с.21-22) 19. Андрейчук О.

							Удосконалення процесу забезпечення інформаційної безпеки за рахунок комбінації методів її оцінки / О. Андрейчук, В. Наконечний // Проблеми кібербезпеки інформаційно-телекомунікаційних систем: Збірник матеріалів доповідей та тез; м. Київ, 27 квітня 2023 року; Київський національний університет імені Тараса Шевченка / Редкол.: В.В. Ільченко, д.ф-м.н., проф., (голова); та ін. – К.: ВПЦ "Київський університет", 2023. – 166 с. (с.83-85) Монографії 1. 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. 2. Сайко В.Г. Мережі мобільного зв'язку нового покоління 4G/5G/6G // Сайко В.Г., Одарченко Р.С., Абакумова А.О., Наритник Т.М., Наконечний В.С., Домрачев В.М., Толюпа С.В., Заблоцький В.Ю., Баховський П.Ф.: Монографія. – К.: ТОВ «Про формат», 2021. – 200 с.
333375	Наконечний Володимир Сергійович	професор, Основне місце роботи	Факультет інформаційних технологій	Диплом спеціаліста, Київським вищим цінженерно радіотехнічним училищем ПВО, рік закінчення: 1986, спеціальність: , Диплом доктора наук ДД 004837, виданий 29.09.2015, Диплом кандидата наук ДК 005905, виданий 09.02.2000, Атестат професора АП 002910, виданий	27	Управління ризиками кібербезпеки	Освіта та науковий ступінь відповідають тематиці дисципліни, наукова робота пов'язана з тематикою дисципліни. Автор понад 170 наукових публікацій за профілем кафедри (з них 87 наукових і 3 навчально-методичних, зокрема 4 колективні монографії, 21 стаття з яких 3 у вітчизняних фахових виданнях, 6 у закордонних виданнях,, 29 публікацій включені до наукометричної бази Scopus, h-індекс в Scopus - 5). Відомості про підвищення кваліфікації:

				29.06.2021, Атестат старшого наукового співробітника (старшого дослідника) АС 006504, виданий 09.04.2008			1. Стажування Варшава, Республіка Польща, від 09 листопада - 18 грудня 2020 р. сертифікат NR164/2020 (180 год) . 2. 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. 3. Перші Київські державні курси іноземних мов, 04.02.2019 - 20.06.2019, свідоцтво про позашкільну освіту №25365 від 21.06.2019 р. Публікації за тематикою дисципліни: 1. Nakonechnyi V. Signature and statistical analyzers in the cyberattack detection system. // V. Nakonechnyi, S. Toliupa, O. Uspenskyi. Information Technology and Security. – January-June 2019. – Vol. 7, Iss. 1(12). – pp. 69–79. 2. Toliupa S. The Increase of The Energy Efficiency of the Radio Equipment Based on the Use of Modulation by Orthogonal Harmonic Carriers. / S. Toliupa, V. Nakonechnyi, A. Trush // Informatyka, Automatyka, Pomiary W Gospodarce I Ochronie Środowiska, Vol 10 No 1 (2020). pp. 24-27. 3. Kucherov D. Assessing the Operator's Readiness to Perform Tasks of Controlling by the Unmanned Aerial Platforms./ D. Kucherov, V/ Nakonechnyi, O. Sushchenko, A. Kozub // Advances in Science, Technology and Engineering Systems Journal Vol. 5, No. 4, 2020. pp. 457-462. 4. Nakonechnyi V., Steshenko G.M., Buchyk S.S., Kresina I.O. The mechanics of the blockchain technology. International Journal of Advanced Trends in Computer Science and

							Engineering. Volume 9(2), pp. 1978-1980. March-April – 2020. SCOPUS 5. Толюпа С.В., Наконечний В.С., Штаненко С.С. Алгоритм протидії кібератакам на основі стеганографічних методів технології SOFT TEMPEST. Збірник наукових праць Військового інституту телекомунікацій та інформатизації імені Героїв Крут Випуск № 1. 2020р. с. 56-66. 6. S. Toliupa, V. Nakonechnyi A. Trush. To increase the energy efficiency of radio equipment based on the use of modulation by orthogonal harmonic carriers. Automatyka, Pomiary w Gospodarce i Ochronie Środowiska IAPGOŚ 2020; 9 (1): 24-27. Google Scholar. Poland. 7. Толюпа С.В., Наконечний В.С. Проблеми захисту критично важливих об'єктів інфраструктури. Безпека інформаційних систем і технологій. Том 1 № 2 (2020). с. 57-65. 8. Толюпа Сергій, Наконечний Володимир, Лукова-Чуйко Наталія, Кулініч Олег. Формування стратегії управління режимами роботи систем захисту на основі моделі ігрового управління. Науковий журнал «Безпека інформаційних систем і технологій» 2020. №3. – с. 78-86. 9. Dmytro Kucherov, Andrei Berezkin, Volodymyr Nakonechnyi, Olha Sushchenko, Ihor Ogirko, Olha Ogirko, Ruslan Skrykovskyy Investigation of the LoRa Transceiver in Conditions of Multipath Propagation of Radio Signals Advances in Science, Technology and Engineering Systems Journal Vol. 6, No. 1, 1106-1111 (2021) 10. Model of Increase of Spectral Efficiency of Use of Frequency Resource of Low-Orbit System with Architecture of the Distributed Satellite Saiko, V., Toliupa, S.,

							Nakonechnyi, V., Brailovskyi, M., Domrachev, V. Lecture Notes in Electrical Engineeringthis link is disabled, 2022, 831, pp. 410–423. Book Chapter 11. Володимир Наконечний, Олександр Лаптєв, Сергій Погасій, Сергій Лазаренко, Ганна Мартинюк. Відбір джерел з неправдивою інформацію методом бджолиної колонії. Наукоємні технології. Інформаційні технології, кібербезпека. Том 52 № 4 (2021) стр.330-337. DOI: https://doi.org/10.18372/2310-5461.52.16379. 12. Oleksandr Laptiev, Serhiy Buchyk, Vitalii Savchenko, Volodymyr Nakonechny, Inna Mykhalchuk, Yanina Shestak DETECTION AND BLOCKING SLOW DDOS ATTACKS BASED ON PREDICTING USER BEHAVIOR Vol. 55 No. 3 (2022) Published: 2022-11-02 p.p. 184-192. 13. Наконечний В.С. Застосування методів теорії ігор для вирішення задач управління інформаційною безпекою. / В.С. Наконечний, В.А. Дружинін, С.В. Толюпа // “Наукоємні технології в інфокомунікація НІСТ’2019”. Матер. III Міжнародної науково-практичної конференції 23-25 травня 2019 р. Харків-Кам’янець-Подільський. 14. Nakonechnyi V., Slipachuk, L., Toliupa, S. The Process of the Critical Infrastructure Cyber Security Management using the Integrated System of the National Cyber Security Sector Management in Ukraine. 2019 3rd International Conference on Advanced Information and Communications Technologies, AICT 2019, Proceedings, 2-6 July 2019, Lviv, Ukraine pp. 451-454. SCOPUS 15. Nakonechnyi V., Toliupa, S., Tereikovska, L.,

							Tereikovskyi, I. One-periodic template marks model of normal behavior of the safety parameters of information systems networking resources.2019 IEEE International Scientific-Practical Conference: Problems of Infocommunications Science and Technology, PIC S and T 2019 - Proceedings, 2019, October 8-11, 2019 Kyiv , Ukraine, pp. 764-768. (SCOPUS) 16. Tereikovskyi, I., Subach, I., Tereikovskyi, O., Tereikovska, L., Toliupa, S., & Nakonechnyi, V. (2020). Parameter Definition for Multilayer Perceptron Intended for Speaker Identification (pp. 227–231). Institute of Electrical and Electronics Engineers (IEEE). Scopus. https://doi.org/10.1109/atit49449.2019.9030504 17. Nakonechnyi V., Snitsarenko P., Mikhieiev Y. The Approach to Automated Internet Monitoring System Creation. 2019 IEEE International Conference on Advanced Trends in Infor-mation Theory, ATIT 2019 – Proceedings, 2019, 18-20 Dec. 2019. Kyiv, Ukraine pp. 257-261. (SCOPUS) 18. Slipachuk L., Nakonechnyi V. Typology of the Model of Integrated Sectoral Information System of the National Cyber Security Management. 2019 IEEE International Conference on Advanced Trends in Information Theory, ATIT 2019 – Proceedings, 2019, 18-20 Dec. 2019, Kyiv, Ukraine pp. 271-276. (SCOPUS) 19. Nakonechnyi V. Model of the process of optimal planning of the modular structure of an information security system. / V. Nakonechnyi, S. Toliupa, V. Druzhinin, M. Kotov // Інформаційні технології та взаємодії (IT&I 2019)". Матеріали доповідей

							VI Міжнародної науково-практичної конференції. 20 грудня 2019 р. К.: Київ. КНУ ім. Тараса Шевченка 2019. - 418 с. С. 267-270. 20. Nakonechnyi V., Toliupa S., Tereikovskyi I., Kulakov Y. Keyboard Dynamic Analysis by Alexnet Type Neural Network. 2020 IEEE 15th International Conference on Advanced Trends in Radioelectronics, Telecommunications and Computer Engineering (TCSET) 25 - 29 February, 2020. pp. 416-420. SCOPUS 21. Saiko, V., Toliupa, S., Nakonechnyi, V., Brailovskyi, M. Models of Improving the Efficiency of Radio Communication Systems Using the Terrahert Range (2021) 2020 IEEE International Conference on Problems of Infocommunications Science and Technology, PIC S and T 2020 - Proceedings, art. no. 9468022, pp. 192-196. Conference Paper EID: 2- s2.0-85114389274 DOI: 10.1109/PICST51311.2020.9468022 CiteScore 2020 = n/a 2020 IEEE International Conference on Problems of Infocommunications Science and Technology, PIC S and T 2020 Kharkiv, Ukraine 6 October 2020 through 9 October 2020 22. Nakonechnyi V., Toliupa, S., Kotov, M., Solodovnyk V. RF signals encryption with AES in WDID. CEUR Workshop Proceedings, 2021, 2845, pp. 96–105. SCOPUS 23. Nakonechnyi V., Saiko, V., Toliupa, S., Kotov, M., Astapenya, V. Method of determining the angular orientation of small satellites in orbit. Proceedingsthis link is disabled, 2021, 2923, pp. 224–233. SCOPUS 24. Building an Intrusion Detection System in Critically Important Information Networks with Application of Data Mining Methods Toliupa, S., Buchyk, S.,

							Nakonechnyi, V., Parkhomenko, I., Lukova-Chuiko, N. Proceedings - 16th International Conference on Advanced Trends in Radioelectronics, Telecommunications and Computer Engineering, TCSET 2022, 2022, стр. 128–133. SCOPUS 25. Valentyn Sobchuk, Serhii Laptiev, Andrii Sobchuk, Iryna Zamrii, Volodymyr Nakonechnyi, Yurii Shcheblanin. Estimates for Harmonic Operators in Modeling Application Processes/2022 IEEE Third International Conference on SYSTEM ANALYSIS & INTELLIGENT COMPUTING (SAIC), 04-07 Oktober, Kyiv, Ukraine. p. 148-153 https://ieeexplore.ieee.org/xpl/conhome/9922952/proceeding SCOPUS 26. Vladyslav LUTSENKO, Volodymyr NAKONECHNYI, Serhii TOLUPA, Volodymyr SAIKO BLOCKCHAIN TECHNOLOGY USAGE IN THE BANKING INDUSTRY / The 2st International Conference on Emerging Technology Trends on the Smart Industry and the Internet of Things January 24-25th 2023. pp. 61 – 66. 27. Oleksandr Laptiev, Igor Polovinkin, Andrii Sobchuk, Sergii Kopytko, Volodymyr Nakonechnyi, Serhii Buchyk. The method of detection of signals using differential transformation. “Modern information, measurement and control systems: problems, applications and perspectives’2022” (MIMCS’2022). November 4-5, 2022, Antalya, Turkey. 28. Vitalii Savchenko, Oleksandr Laptiev, Vitalii Ponomarenko, Taras Dzyuba, Yuriy Shcheblanin , Valeriia Savchenko. The method of localization of signals of radio transmitting devices. “Modern information, measurement and control systems: problems, applications and perspectives’2022”

							(MIMCS'2022). November 4-5, 2022, Antalya, Turkey. 29. Андрейчук О. Удосконалення процесу забезпечення інформаційної безпеки за рахунок комбінації методів її оцінки / О. Андрейчук, В. Наконечний // Проблеми кібербезпеки інформаційно-телекомунікаційних систем: Збірник матеріалів доповідей та тез; м. Київ, 27 квітня 2023 року; Київський національний університет імені Тараса Шевченка / Редкол.: В.В. Ільченко, д.ф-м.н., проф., (голова); та ін. – К.: ВПЦ "Київський університет", 2023. – 166 с. (с.83-85) 30. Conference Paper. Smart Home Network based on Cisco Equipment Kolbasova, K., Zhurakovskyi, B., Poltorak, V., Nakonechnyi, V., Kyrychok, R. CEUR Workshop ProceedingsThis link is disabled., 2023, 3550, pp. 70–80 (SCOPUS) Монографії 1. 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. 2. Сайко В.Г. Мережі мобільного зв'язку нового покоління 4G/5G/6G // Сайко В.Г., Одарченко Р.С., Абакумова А.О., Наритник Т.М., Наконечний В.С., Домрачев В.М., Толюпа С.В., Заблоцький В.Ю., Баховський П.Ф.: Монографія. – К.: ТОВ «Про формат», 2021. – 200 с.
37474	Толюпа Сергій Васильович	професор, Основне місце роботи	Факультет інформаційних технологій	Диплом спеціаліста, Київське вище інженерне радіотехнічне училище ППО, рік закінчення: 1986,	31	Методологія та організація наукових досліджень з основами інтелектуальної власності	Освіта та науковий ступінь відповідають тематиці дисципліни, наукова робота пов'язана з тематикою дисципліни. Автор більше 250 наукових публікацій

				спеціальність: Автоматизовані системи управління, 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			за профілем кафедри. 6 колективних монографій, 61 публікація включені до наукометричної бази Scopus: h-індекс в Scopus - 7, 16 науково-методичних матеріалів (підручники, посібники, лабораторні практикуми). Має захищених: 1 д.т.н., 4 к.т.н. Керує 3 аспірантами. 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 Навчально-методичні матеріали, 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., Політанський Р.Л., Лісінський В.В. Управління інформаційною безпекою. Навчальний посібник. За заг. ред. Толюпи С.В. – Чернівці. ЧНУ імені Юрія Федьковича. 2021р. – с. 486. 3. 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. 4. Толюпа С.В., Бучик С.С., Шестак Я.В. Прикладні технології програмування в інформаційній безпеці. Лабораторний практикум. – Житомир: ФОП Кирилюк І.В., ПП «Рута», 2023. – с. 50. 5. Бурячок В.Л., Толюпа С.В., Хорошко В.О. «Інтелектуальна власність у сфері інформаційної безпеки» // За редакцією проф. В.О. Хорошко. – К.: ПВП “Задруга”, – 178с. 6. В.Л. Бурячок, С.В. Толюпа, А.О. Аносов “Системний аналіз та прийняття рішень в інформаційній безпеці”. - К. : ДУТ. – с.345. 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. 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. 3. 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. 4. 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. 5. 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) 6. С.Толюпа, І. Пархоменко, С. Штаненко. Модель системи протидії вторгненням в інформаційних системах. Інфокомунікаційні технології та електронна інженерія. №1. 2021. С. 86-95. (Фахове видання). 7. Самохвалов Юрій, Толюпа Сергій, Штаненко Сергій. Забезпечення кібербезпеки АСУ ТП шляхом застосування ПЛІС технології. Безпека інформаційних систем і технологій. №1. 2021. С. 45-54. 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. 9. 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. 10. 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. 11. Штаненко С.С., Самохвалов Ю.Я., Толюпа С.В. Підхід до виявлення помилок та відновлення правильного функціонування програмних засобів сучасних систем управління, реалізованих за принципом «система на кристалі». Наукоємні технології. – К.: НАУ, 2023. – № 2 (58). – с. 376-384. 12. Сергій Толюпа, Юрій Самохвалов, Павло Хусаінов Сергій, Штаненко. Самодіагностування як спосіб підвищення кіберстійкості термінальних компонентів технологічної системи. Том 2 № 22 (2023): Кібербезпека: освіта, наука, техніка. С. 134-147. 13. Toliupa, S., Shevchenko, A., Buchyk, S., Pampukha, I., Kulko, A. Managing the Security of the Critical Infrastructure Information Network. CEUR Workshop Proceedings, 2023, 3550, страницы 131–142. Scopus. 14. Shestak, Y., Toliupa, S., Shevchenko, A., Torchylo, A., Onyigwang, O.J. Data Pro-cessing Centre's Cyberattack Protection Directions on the Base of Neural Network Algorithms. CEUR Workshop Proceedings, 2023, 3347, pp. 212–221. Scopus. 15. Shtanenko, S., Samokhvalov, Y., Toliupa, S., Silko, O. (2023). The Approach to Assessment of Technical Condition of Microprocessor Systems that Are

							Implemented on Integrated Circuits with a Programmable Structure. Emerging Networking in the Digital Transformation Age. Lecture Notes in Electrical Engineering, vol 965. Springer, Cham. 16. Buchyk, S., Toliupa, S., Lukova-Chuiko, N., Khomenko, O., Serpinskyi, Y. (2023). Applied Steganographic System for Hiding Textual Information on Audio Files. Emerging Networking in the Digital Transformation Age. Lecture Notes in Electrical Engineering, vol 965. Springer, Cham. Scopus

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 25 Оцінювати ефективність та практичну цінність результатів наукових і практичних досліджень та інновацій.	☒	Методологія та організація наукових досліджень з основами інтелектуальної власності	лекції, семінарські заняття, самостійна робота	контрольні роботи, тести, залік
		Професійна та корпоративна етика	Професійна та корпоративна етика	контрольні роботи, тести, залік
		Реверс-інжиніринг	лекції, лабораторні заняття, самостійна робота	контрольні роботи, захист звітів з лабораторних робіт, тести, іспит
		Форензік аналіз	лекції, лабораторні заняття, самостійна робота	контрольні роботи, захист звітів з лабораторних робіт, тести, іспит
		Системи управління інформаційною безпекою	лекції, лабораторні заняття, самостійна робота	контрольні роботи, захист звітів з лабораторних робіт, тести, залік
		Безпека критичної інформаційної інфраструктури	лекції, лабораторні заняття, самостійна робота	контрольні роботи, захист звітів з лабораторних робіт, тести, залік
		Виробнича практика	контрольні роботи, захист звітів з лабораторних робіт, тести, залік	поточне оцінювання керівником, захист практики
		Іноземна мова для академічних цілей	лекції, практичні заняття, семінарські заняття, самостійна робота	контрольні роботи, захист звітів з практичних робіт, тести, іспит
		Аудит інформаційних систем	лекції, лабораторні заняття, самостійна робота	Контрольні роботи, захист звітів з лабораторних робіт,

				тести, іспит
		Управління ризиками кібербезпеки	лекції, лабораторні заняття, самостійна робота	контрольні роботи, захист звітів з лабораторних робіт, тести, залік
		Науково-дослідна практика	консультації з керівником, вивчення документації, самостійна робота, виконання індивідуального завдання, підготовка звіту з практики	поточне оцінювання керівником, захист практики
		Виконання та захист кваліфікаційної роботи	самостійна робота, консультації з керівником	захист кваліфікаційної роботи
ПРН 24 Планувати та виконувати наукові та прикладні дослідження у сфері кібербезпеки із застосуванням сучасних технологій, експериментальни х і теоретичних методів і моделей теорії прийняття рішень, системного аналізу, оптимізації процесів, математичної статистики.	☒	Методологія та організація наукових досліджень з основами інтелектуальної власності	лекції, семінарські заняття, самостійна робота	контрольні роботи, тести, залік
		Реверс-інжиніринг	лекції, лабораторні заняття, самостійна робота	Контрольні роботи, захист звітів з лабораторних робіт, тести, іспит
		Форензік аналіз	лекції, лабораторні заняття, самостійна робота	контрольні роботи, захист звітів з лабораторних робіт, тести, іспит
		Іноземна мова для академічних цілей	лекції, практичні заняття, семінарські заняття, самостійна робота	контрольні роботи, захист звітів з практичних робіт, тести, іспит
		Науково-дослідна практика	консультації з керівником, вивчення документації, самостійна робота, виконання індивідуального завдання, підготовка звіту з практики	поточне оцінювання керівником, захист практики
		Виконання та захист кваліфікаційної роботи	самостійна робота, консультації з керівником	захист кваліфікаційної роботи
ПРН 23 - Обґрунтовувати вибір програмного забезпечення, устаткування та інструментів, інженерних технологій і процесів, а також обмежень щодо них в галузі і кібербезпеки на основі сучасних знань у суміжних галузях, наукової, технічної та довідкової літератури та іншої доступної інформації.	☒	Виконання та захист кваліфікаційної роботи	самостійна робота, консультації з керівником	захист кваліфікаційної роботи
		Іноземна мова для академічних цілей	лекції, практичні заняття, семінарські заняття, самостійна робота	Контрольні роботи, захист звітів з практичних робіт, тести, іспит
		Науково-дослідна практика	консультації з керівником, вивчення документації, самостійна робота, виконання індивідуального завдання, підготовка звіту з практики	поточне оцінювання керівником, захист практики
		Реверс-інжиніринг	лекції, лабораторні заняття, самостійна робота	контрольні роботи, захист звітів з лабораторних робіт, тести, іспит
		Методологія та організація наукових досліджень з основами інтелектуальної власності	лекції, семінарські заняття, самостійна робота	контрольні роботи, тести, залік
		Форензік аналіз	лекції, лабораторні заняття, самостійна робота	контрольні роботи, захист звітів з лабораторних робіт, тести, іспит
ПРН 22 - Планувати та виконувати	☒	Методологія та організація наукових досліджень з	лекції, семінарські заняття, самостійна робота	контрольні роботи, тести, залік

експериментальні і теоретичні дослідження, висувати і перевіряти гіпотези, обирати для цього придатні методи та інструменти, здійснювати статистичну обробку даних, оцінювати достовірність результатів досліджень, аргументувати висновки.		основами інтелектуальної власності		
		Реверс-інжиніринг	лекції, лабораторні заняття, самостійна робота	контрольні роботи, захист звітів з лабораторних робіт, тести, іспит
		Управління безпекою мереж	лекції, лабораторні заняття, самостійна робота	контрольні роботи, захист звітів з лабораторних робіт, тести, іспит
		Форензік аналіз	лекції, лабораторні заняття, самостійна робота	контрольні роботи, захист звітів з лабораторних робіт, тести, іспит
		Виробнича практика	консультації з керівником, вивчення документації, самостійна робота, виконання індивідуального завдання, підготовка звіту з практики	поточне оцінювання керівником, захист практики
		Аудит інформаційних систем	лекції, лабораторні заняття, самостійна робота	контрольні роботи, захист звітів з лабораторних робіт, тести, іспит
		Науково-дослідна практика	консультації з керівником, вивчення документації, самостійна робота, виконання індивідуального завдання, підготовка звіту з практики	поточне оцінювання керівником, захист практики
		Виконання та захист кваліфікаційної роботи	самостійна робота, консультації з керівником	захист кваліфікаційної роботи
ПРН 21 Використовувати методи натурного, фізичного і комп'ютерного моделювання для дослідження процесів, які стосуються кібербезпеки.	☒	Методологія та організація наукових досліджень з основами інтелектуальної власності	лекції, семінарські заняття, самостійна робота	контрольні роботи, тести, залік
		Реверс-інжиніринг	лекції, лабораторні заняття, самостійна робота	контрольні роботи, захист звітів з лабораторних робіт, тести, іспит
		Форензік аналіз	лекції, лабораторні заняття, самостійна робота	контрольні роботи, захист звітів з лабораторних робіт, тести, іспит
		Іноземна мова для академічних цілей	лекції, практичні заняття, семінарські заняття, самостійна робота	лекції, практичні заняття, семінарські заняття, самостійна робота
		Виробнича практика	консультації з керівником, вивчення документації, самостійна робота, виконання індивідуального завдання, підготовка звіту з практики	поточне оцінювання керівником, захист практики
		Аудит інформаційних систем	лекції, лабораторні заняття, самостійна робота	контрольні роботи, захист звітів з лабораторних робіт, тести, іспит
		Науково-дослідна практика	консультації з керівником, вивчення документації, самостійна робота, виконання індивідуального завдання, підготовка звіту з практики	поточне оцінювання керівником, захист практики
		Виконання та захист кваліфікаційної роботи	самостійна робота, консультації з керівником	захист кваліфікаційної роботи
ПРН 20 - Ставити	☒	Методологія та	лекції, семінарські заняття,	контрольні роботи, тести,

та вирішувати складні інженерно-прикладні та наукові задачі кібербезпеки з урахуванням вимог вітчизняних та світових стандартів та кращих практик.		організація наукових досліджень з основами інтелектуальної власності	самостійна робота	залік
		Реверс-інжиніринг	лекції, лабораторні заняття, самостійна робота	контрольні роботи, захист звітів з лабораторних робіт, тести, іспит
		Безпека критичної інформаційної інфраструктури	лекції, лабораторні заняття, самостійна робота	контрольні роботи, захист звітів з лабораторних робіт, тести, залік
		Виробнича практика	консультації з керівником, вивчення документації, самостійна робота, виконання індивідуального завдання, підготовка звіту з практики	поточне оцінювання керівником, захист практики
		Управління ризиками кібербезпеки	лекції, лабораторні заняття, самостійна робота	контрольні роботи, захист звітів з лабораторних робіт, тести, іспит
		Управління інцидентами інформаційної безпеки	лекції, лабораторні заняття, самостійна робота	контрольні роботи, захист звітів з лабораторних робіт, тести, іспит
		Науково-дослідна практика	консультації з керівником, вивчення документації, самостійна робота, виконання індивідуального завдання, підготовка звіту з практики	поточне оцінювання керівником, захист практики
		Іноземна мова для академічних цілей	лекції, практичні заняття, семінарські заняття, самостійна робота	контрольні роботи, захист звітів з практичних робіт, тести, іспит
		Виконання та захист кваліфікаційної роботи	самостійна робота, консультації з керівником	захист кваліфікаційної роботи
ПРН 19 - Обирати, аналізувати і розробляти придатні типові аналітичні, розрахункові та експериментальні методи кіберзахисту, розробляти, реалізовувати та супроводжувати проекти з захисту інформації у кіберпросторі, інноваційної діяльності та захисту інтелектуальної власності.	☒	Виробнича практика	консультації з керівником, вивчення документації, самостійна робота, виконання індивідуального завдання, підготовка звіту з практики	поточне оцінювання керівником, захист практики
		Аудит інформаційних систем	лекції, лабораторні заняття, самостійна робота	контрольні роботи, захист звітів з лабораторних робіт, тести, іспит
		Науково-дослідна практика	консультації з керівником, вивчення документації, самостійна робота, виконання індивідуального завдання, підготовка звіту з практики	поточне оцінювання керівником, захист практики
		Виконання та захист кваліфікаційної роботи	самостійна робота, консультації з керівником	захист кваліфікаційної роботи
		Системи управління інформаційною безпекою	лекції, лабораторні заняття, самостійна робота	контрольні роботи, захист звітів з лабораторних робіт, тести, залік
ПРН 18 Планувати навчання, а також супроводжувати та контролювати роботу з персоналом у напряму кібербезпеки.	☒	Методологія та організація наукових досліджень з основами інтелектуальної власності	лекції, семінарські заняття, самостійна робота	контрольні роботи, тести, залік
		Професійна та корпоративна етика	лекції, семінарські заняття, самостійна робота	контрольні роботи, тести, залік

		Системи управління інформаційною безпекою	лекції, лабораторні заняття, самостійна робота	контрольні роботи, захист звітів з лабораторних робіт, тести, залік
		Виробнича практика	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
		Виконання та захист кваліфікаційної роботи	самостійна робота, консультації з керівником	захист кваліфікаційної роботи
ПРН 17 - Мати навички автономного і самостійного навчання у сфері кібербезпеки і дотичних галузей знань, аналізувати власні освітні потреби та об'єктивно оцінювати результати навчання.	☒	Виконання та захист кваліфікаційної роботи	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
		Іноземна мова для академічних цілей	лекції, практичні заняття, семінарські заняття, самостійна робота	контрольні роботи, захист звітів з практичних робіт, тести, іспит
		Виробнича практика	вивчення документації, самостійна робота, виконання індивідуального завдання, підготовка звіту з практики	поточне оцінювання керівником, захист практики
		Професійна та корпоративна етика	лекції, семінарські заняття, самостійна робота	контрольні роботи, тести, залік
		Методологія та організація наукових досліджень з основами інтелектуальної власності	лекції, семінарські заняття, самостійна робота	контрольні роботи, тести, залік
ПРН 16 - Приймати обґрунтовані рішення з організаційно-технічних питань кібербезпеки у складних і непередбачуваних умовах, у тому числі із застосуванням сучасних методів та засобів оптимізації, прогнозування та прийняття рішень.	☒	Методологія та організація наукових досліджень з основами інтелектуальної власності	лекції, семінарські заняття, самостійна робота	контрольні роботи, тести, залік
		Професійна та корпоративна етика	лекції, семінарські заняття, самостійна робота	контрольні роботи, тести, залік
		Реверс-інжиніринг	лекції, семінарські заняття, самостійна робота	контрольні роботи, тести, іспит
		Безпека критичної інформаційної інфраструктури	лекції, семінарські заняття, самостійна робота	контрольні роботи, захист звітів з лабораторних робіт, тести, іспит
		Форензік аналіз	лекції, лабораторні заняття, самостійна робота	контрольні роботи, захист звітів з лабораторних робіт, тести, іспит
		Виробнича практика	консультації з керівником, вивчення документації, самостійна робота, виконання індивідуального завдання, підготовка звіту з практики	поточне оцінювання керівником, захист практики

		Аудит інформаційних систем	лекції, лабораторні заняття, самостійна робота	контрольні роботи, захист звітів з лабораторних робіт, тести, іспит
		Управління інцидентами інформаційної безпеки	лекції, лабораторні заняття, самостійна робота	контрольні роботи, захист звітів з лабораторних робіт, тести, іспит
		Науково-дослідна практика	консультації з керівником, вивчення документації, самостійна робота, виконання індивідуального завдання, підготовка звіту з практики	поточне оцінювання керівником, захист практики
		Виконання та захист кваліфікаційної роботи	самостійна робота, консультації з керівником	захист кваліфікаційної роботи
ПРН 15 - Зрозуміло і недвозначно доносити власні висновки з проблем інформаційної безпеки кібербезпеки, а також знання та пояснення, що їх обґрунтовують до персоналу, партнерів та інших осіб.	☒	Методологія та організація наукових досліджень з основами інтелектуальної власності	лекції, семінарські заняття, самостійна робота	контрольні роботи, тести, залік
		Професійна та корпоративна етика	лекції, семінарські заняття, самостійна робота	контрольні роботи, тести, залік
		Виробнича 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
		Іноземна мова для академічних цілей	лекції, практичні заняття, семінарські заняття, самостійна робота	контрольні роботи, захист звітів з практичних робіт, тести, іспит
		Виконання та захист кваліфікаційної роботи	самостійна робота, консультації з керівником	захист кваліфікаційної роботи
ПРН 14 - Аналізувати, розробляти і супроводжувати систему аудиту та моніторингу ефективності функціонування інформаційних систем і технологій, бізнес\операційних процесів у сфері кібербезпеки в цілому.	☒	Виконання та захист кваліфікаційної роботи	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
		Управління ризиками кібербезпеки	лекції, лабораторні заняття, самостійна робота	контрольні роботи, захист звітів з лабораторних робіт, тести, іспит
		Аудит інформаційних систем	лекції, лабораторні заняття, самостійна робота	контрольні роботи, захист звітів з лабораторних робіт, тести, іспит
		Управління безпекою мереж	лекції, лабораторні заняття, самостійна робота	контрольні роботи, захист звітів з лабораторних робіт, тести, іспит
		Виробнича практика	консультації з керівником, вивчення документації, самостійна робота, виконання індивідуального завдання, підготовка звіту з	консультації з керівником, вивчення документації, самостійна робота, виконання індивідуального завдання, підготовка звіту з

			практики	практики
ПРН 13 - Досліджувати, розробляти, впроваджувати та використовувати методи та засоби криптографічного та технічного захисту інформації бізнес/операційних процесів, а також аналізувати і надавати оцінку ефективності їх використання в інформаційних системах, на об'єктах інформаційної діяльності та критичної інфраструктури.	☒	Реверс-інжиніринг	лекції, лабораторні заняття, самостійна робота	контрольні роботи, захист звітів з лабораторних робіт, тести, іспит
		Системи управління інформаційною безпекою	лекції, лабораторні заняття, самостійна робота	контрольні роботи, захист звітів з лабораторних робіт, тести, іспит
		Виробнича 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
		Виконання та захист кваліфікаційної роботи	самостійна робота, консультації з керівником	захист кваліфікаційної роботи
ПРН 11 - Аналізувати, контролювати та забезпечувати ефективне функціонування системи управління доступом до інформаційних ресурсів відповідно до встановлених стратегії і політики кібербезпеки організації.	☒	Системи управління інформаційною безпекою	лекції, лабораторні заняття, самостійна робота	контрольні роботи, захист звітів з лабораторних робіт, тести, іспит
		Виробнича практика	консультації з керівником, вивчення документації, самостійна робота, виконання індивідуального завдання, підготовка звіту з практики	поточне оцінювання керівником, захист практики
		Управління інцидентами інформаційної безпеки	лекції, лабораторні заняття, самостійна робота	контрольні роботи, захист звітів з лабораторних робіт, тести, іспит
		Науково-дослідна практика	контрольні роботи, захист звітів з лабораторних робіт, тести, іспит	поточне оцінювання керівником, захист практики
		Виконання та захист кваліфікаційної роботи	самостійна робота, консультації з керівником	захист кваліфікаційної роботи
		Управління безпекою мереж	лекції, лабораторні заняття, самостійна робота	контрольні роботи, захист звітів з лабораторних робіт, тести, іспит
		Реверс-інжиніринг	лекції, лабораторні заняття, самостійна робота	контрольні роботи, захист звітів з лабораторних робіт, тести, іспит
ПРН 10 - Забезпечувати безперервність бізнес/операційних процесів, а також виявляти уразливості інформаційних систем та ресурсів, аналізувати та оцінювати ризики кібербезпеки організації	☒	Науково-дослідна практика	консультації з керівником, вивчення документації, самостійна робота, виконання індивідуального завдання, підготовка звіту з практики	поточне оцінювання керівником, захист практики
		Управління безпекою мереж	лекції, лабораторні заняття, самостійна робота	контрольні роботи, захист звітів з лабораторних робіт, тести, іспит
		Системи управління інформаційною безпекою	лекції, лабораторні заняття, самостійна робота	контрольні роботи, захист звітів з лабораторних робіт, тести, іспит
		Управління ризиками кібербезпеки	лекції, лабораторні заняття, самостійна робота	контрольні роботи, захист звітів з лабораторних робіт, тести, іспит
		Виробнича практика	консультації з керівником,	поточне оцінювання

			вивчення документації, самостійна робота, виконання індивідуального завдання, підготовка звіту з практики	керівником, захист практики
		Управління інцидентами інформаційної безпеки	лекції, лабораторні заняття, самостійна робота	контрольні роботи, захист звітів з лабораторних робіт, тести, іспит
		Виконання та захист кваліфікаційної роботи	самостійна робота, консультації з керівником	захист кваліфікаційної роботи
ПРН 12 - Досліджувати, розробляти та впроваджувати методи і заходи протидії кіберінцидентам, здійснювати процедури управління, контролю та розслідування, а також надавати рекомендації щодо попередження та аналізу кіберінцидентів в цілому	☒	Реверс-інжиніринг	лекції, лабораторні заняття, самостійна робота	контрольні роботи, захист звітів з лабораторних робіт, тести, іспит
		Виробнича практика	консультації з керівником, вивчення документації, самостійна робота, виконання індивідуального завдання, підготовка звіту з практики	поточне оцінювання керівником, захист практики
		Управління ризиками кібербезпеки	лекції, лабораторні заняття, самостійна робота	контрольні роботи, захист звітів з лабораторних робіт, тести, іспит
		Науково-дослідна практика	консультації з керівником, вивчення документації, самостійна робота, виконання індивідуального завдання, підготовка звіту з практики	поточне оцінювання керівником, захист прак
		Виконання та захист кваліфікаційної роботи	самостійна робота, консультації з керівником	захист кваліфікаційної роботи
ПРН 1 - Вільно спілкуватись державною та іноземною мовами, усно і письмово для представлення і обговорення результатів досліджень та інновацій, забезпечення бізнес\операційних процесів та питань професійної діяльності в галузі кібербезпеки.	☒	Іноземна мова для академічних цілей	лекції, практичні заняття, семінарські заняття, самостійна робота	контрольні роботи, захист звітів з практичних робіт, тести, іспит
		Виконання та захист кваліфікаційної роботи	самостійна робота, консультації з керівником	захист кваліфікаційної роботи
ПРН 3 - Провадити дослідницьку та інноваційну діяльність в сфері кібербезпеки, а також в сфері технічного та криптографічного захисту інформації у кіберпросторі.	☒	Методологія та організація наукових досліджень з основами інтелектуальної власності	лекції, семінарські заняття, самостійна робота	контрольні роботи, тести, залік
		Реверс-інжиніринг	лекції, лабораторні заняття, самостійна робота	контрольні роботи, захист звітів з лабораторних робіт, тести, іспит
		Форензік аналіз	лекції, лабораторні заняття, самостійна робота	контрольні роботи, захист звітів з лабораторних робіт, тести, іспит
		Науково-дослідна практика	консультації з керівником, вивчення документації, самостійна робота, виконання індивідуального завдання, підготовка звіту з практики	поточне оцінювання керівником, захист практики

		Виконання та захист кваліфікаційної роботи	самостійна робота, консультації з керівником	самостійна робота, консультації з керівником
ПРН 4 - Застосовувати, інтегрувати, розробляти, впроваджувати та удосконалювати сучасні інформаційні технології, фізичні та математичні методи і моделі в сфері кібербезпеки.	☒	Виконання та захист кваліфікаційної роботи	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
		Реверс-інжиніринг	лекції, лабораторні заняття, самостійна робота	контрольні роботи, захист звітів з лабораторних робіт, тести, іспит
		Безпека критичної інформаційної інфраструктури	лекції, лабораторні заняття, самостійна робота	контрольні роботи, захист звітів з лабораторних робіт, тести, іспит
		Виробнича практика	консультації з керівником, вивчення документації, самостійна робота, виконання індивідуального завдання, підготовка звіту з практики	поточне оцінювання керівником, захист практики
		Управління інцидентами інформаційної безпеки	лекції, лабораторні заняття, самостійна робота	контрольні роботи, захист звітів з лабораторних робіт, тести, іспит
		Іноземна мова для академічних цілей	лекції, практичні заняття, семінарські заняття, самостійна робота	контрольні роботи, захист звітів з практичних робіт, тести, іспит
ПРН 2 - Інтегрувати фундаментальні та спеціальні знання для розв'язування складних задач кібербезпеки у мультидисципліна рних контекстах.	☒	Реверс-інжиніринг	лекції, лабораторні заняття, самостійна робота	контрольні роботи, захист звітів з лабораторних робіт, тести, іспит
		Форензік аналіз	лекції, лабораторні заняття, самостійна робота	контрольні роботи, захист звітів з лабораторних робіт, тести, іспит
		Аудит інформаційних систем	лекції, лабораторні заняття, самостійна робота	контрольні роботи, захист звітів з лабораторних робіт, тести, іспит
		Виробнича 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
		Виконання та захист кваліфікаційної роботи	самостійна робота, консультації з керівником	захист кваліфікаційної роботи
ПРН 6 - Аналізувати та оцінювати захищеність систем, комплексів та засобів кіберзахисту, технології створення та використання спеціалізованого	☒	Управління безпекою мереж	лекції, лабораторні заняття, самостійна робота	контрольні роботи, захист звітів з лабораторних робіт, тести, іспит
		Системи управління інформаційною безпекою	лекції, лабораторні заняття, самостійна робота	контрольні роботи, захист звітів з лабораторних робіт, тести, залік
		Управління інцидентами інформаційної	лекції, лабораторні заняття, самостійна робота	контрольні роботи, захист звітів з лабораторних робіт, тести, залік

програмного забезпечення.		безпеки		
		Аудит інформаційних систем	лекції, лабораторні заняття, самостійна робота	контрольні роботи, захист звітів з лабораторних робіт, тести, залік
		Науково-дослідна практика	консультації з керівником, вивчення документації, самостійна робота, виконання індивідуального завдання, підготовка звіту з практики	поточне оцінювання керівником, захист практики
		Виконання та захист кваліфікаційної роботи	самостійна робота, консультації з керівником	захист кваліфікаційної роботи
ПРН 7 - Обґрунтовувати використання, впроваджувати та аналізувати кращі світові стандарти, практики з метою розв'язання складних задач професійної діяльності в галузі кібербезпеки.	☒	Безпека критичної інформаційної інфраструктури	лекції, лабораторні заняття, самостійна робота	контрольні роботи, захист звітів з лабораторних робіт, тести, залік
		Системи управління інформаційною безпекою	лекції, лабораторні заняття, самостійна робота	контрольні роботи, захист звітів з лабораторних робіт, тести, залік
		Виробнича практика	консультації з керівником, вивчення документації, самостійна робота, виконання індивідуального завдання, підготовка звіту з практики	поточне оцінювання керівником, захист практики
		Управління безпекою мереж	лекції, лабораторні заняття, самостійна робота	контрольні роботи, захист звітів з лабораторних робіт, тести, іспит
		Науково-дослідна практика	консультації з керівником, вивчення документації, самостійна робота, виконання індивідуального завдання, підготовка звіту з практики	поточне оцінювання керівником, захист практики
		Виконання та захист кваліфікаційної роботи	самостійна робота, консультації з керівником	захист кваліфікаційної роботи
ПРН 5 – Критично осмислювати проблеми кібербезпеки, у тому числі на міжгалузевому та міждисциплінарному рівні, зокрема на основі розуміння нових результатів інженерних і фізико-математичних наук, а також розвитку технологій створення та використання спеціалізованого програмного забезпечення.	☒	Форензік аналіз	лекції, лабораторні заняття, самостійна робота	контрольні роботи, захист звітів з лабораторних робіт, тести, іспит
		Аудит інформаційних систем	лекції, лабораторні заняття, самостійна робота	контрольні роботи, захист звітів з лабораторних робіт, тести, іспит
		Управління безпекою мереж	лекції, лабораторні заняття, самостійна робота	контрольні роботи, захист звітів з лабораторних робіт, тести, іспит
		Науково-дослідна практика	консультації з керівником, вивчення документації, самостійна робота, виконання індивідуального завдання, підготовка звіту з практики	поточне оцінювання керівником, захист практики
		Виконання та захист кваліфікаційної роботи	самостійна робота, консультації з керівником	захист кваліфікаційної роботи
		Реверс-інжиніринг	лекції, лабораторні заняття, самостійна робота	контрольні роботи, захист звітів з лабораторних робіт, тести, іспит
ПРН 8 – Досліджувати, розробляти і супроводжувати системи та засоби кібербезпеки на об'єктах	☒	Реверс-інжиніринг	лекції, лабораторні заняття, самостійна робота	контрольні роботи, захист звітів з лабораторних робіт, тести, іспит
		Управління безпекою мереж	лекції, лабораторні заняття, самостійна робота	контрольні роботи, захист звітів з лабораторних робіт, тести, іспит

інформаційної діяльності та критичної інфраструктури.		Виробнича практика	консультації з керівником, вивчення документації, самостійна робота, виконання індивідуального завдання, підготовка звіту з практики	поточне оцінювання керівником, захист практики
		Форензік аналіз	лекції, лабораторні заняття, самостійна робота	контрольні роботи, захист звітів з лабораторних робіт, тести, іспит
		Аудит інформаційних систем	лекції, лабораторні заняття, самостійна робота	контрольні роботи, захист звітів з лабораторних робіт, тести, іспит
		Управління інцидентами інформаційної безпеки	лекції, лабораторні заняття, самостійна робота	контрольні роботи, захист звітів з лабораторних робіт, тести, іспит
		Науково-дослідна практика	консультації з керівником, вивчення документації, самостійна робота, виконання індивідуального завдання, підготовка звіту з практики	поточне оцінювання керівником, захист практики
		Безпека критичної інформаційної інфраструктури	лекції, лабораторні заняття, самостійна робота	контрольні роботи, захист звітів з лабораторних робіт, тести, залік
		Виконання та захист кваліфікаційної роботи	самостійна робота, консультації з керівником	захист кваліфікаційної роботи
ПРН 9 – Аналізувати, розробляти і супроводжувати систему управління кібербезпекою організації на базі стратегії і політики інформаційної безпеки.	☒	Системи управління інформаційною безпекою	лекції, лабораторні заняття, самостійна робота	контрольні роботи, захист звітів з лабораторних робіт, тести, залік
		Виробнича практика	консультації з керівником, вивчення документації, самостійна робота, виконання індивідуального завдання, підготовка звіту з практики	поточне оцінювання керівником, захист практики
		Аудит інформаційних систем	лекції, лабораторні заняття, самостійна робота	контрольні роботи, захист звітів з лабораторних робіт, тести, залік
		Управління ризиками кібербезпеки	лекції, лабораторні заняття, самостійна робота	контрольні роботи, захист звітів з лабораторних робіт, тести, залік
		Управління інцидентами інформаційної безпеки	лекції, лабораторні заняття, самостійна робота	контрольні роботи, захист звітів з лабораторних робіт, тести, залік
		Науково-дослідна практика	консультації з керівником, вивчення документації, самостійна робота, виконання індивідуального завдання, підготовка звіту з практики	поточне оцінювання керівником, захист практики
		Виконання та захист кваліфікаційної роботи	самостійна робота, консультації з керівником	захист кваліфікаційної роботи