НАЦІОНАЛЬНЕ АГЕНТСТВО ІЗ ЗАБЕЗПЕЧЕННЯ ЯКОСТІ ВИЩОЇ ОСВІТИ

ВІДОМОСТІ
про самооцінювання освітньої програми

Заклад вищої освіти	**Київський столичний університет імені Бориса Грінченка**
Освітня програма	**62967 Безпека інформаційних і комунікаційних систем**
Рівень вищої освіти	**Магістр**
Спеціальність	**125 Кібербезпека та захист інформації**

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	**6945**
Повна назва ЗВО	**Київський столичний університет імені Бориса Грінченка**
Ідентифікаційний код ЗВО	**45307965**
ПІБ керівника ЗВО	**Турунцев Олександр Петрович**
Посилання на офіційний веб-сайт ЗВО	**https://kubg.edu.ua**

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

https://registry.edbo.gov.ua/university/6945

3. Загальна інформація про ОП, яка подається на акредитацію

ID освітньої програми в ЄДЕБО	**62967**
Назва ОП	**Безпека інформаційних і комунікаційних систем**
Галузь знань	**12 Інформаційні технології**
Спеціальність	**125 Кібербезпека та захист інформації**
Спеціалізація (за наявності)	*відсутня*
Рівень вищої освіти	**Магістр**
Тип освітньої програми	**Освітньо-професійна**
Вступ на освітню програму здійснюється на основі ступеня (рівня)	**Бакалавр**
Структурний підрозділ (кафедра або інший підрозділ), відповідальний за реалізацію ОП	**кафедра інформаційної та кібернетичної безпеки імені професора Володимира Бурячка факультету інформаційних технологій та математики.**
Інші навчальні структурні підрозділи (кафедра або інші підрозділи), залучені до реалізації ОП	**Кафедра германської філології Факультету романо-германської філології**
Місце (адреса) провадження освітньої діяльності за ОП	**м. Київ, вул. Левка Лук'яненка, 13-Б**
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	**468938**
ПІБ гаранта ОП	**Соколов Володимир Юрійович**
Посада гаранта ОП	**Доцент**
Корпоративна електронна адреса гаранта ОП	**v.sokolov@kubg.edu.ua**
Контактний телефон гаранта ОП	**+38(095)-703-22-92**
Додатковий телефон гаранта ОП	**+49(152)-275-59-75**

Форми здобуття освіти на ОП	Термін навчання
очна денна	1 р. 4 міс.

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

Освітньо-професійна програма «Безпека інформаційних і комунікаційних систем» для другого (магістерського) рівня вищої освіти (далі – ОПП) розроблена відповідно до Закону України «Про вищу освіту», проєкту Стандарту з урахуванням рекомендацій «Магістерської програми нового покоління експертів в інформаційній безпеці». Ця програма впроваджувалася у закладах вищої освіти України в рамках угоди 2013-5084/001-001 про співпрацю між Україною та Європейським Союзом за підтримки Європейської комісії: агентства з освіти, культури та аудіовізуальних засобів (Tempus IV) у 2013–2017 роках.
У 2018 році ОПП розробила проєктна група науково-педагогічних працівників (НПП) під керівництвом Бурячка Володимира Леонідовича, доктора технічних наук, професора. До складу групи також увійшли: Бессалов А. В., доктор технічних наук, професор; Толюпа С. В., доктор технічних наук, професор; Абрамов В. О., кандидат технічних наук, доцент. У процесі розроблення ОПП брали участь адміністративний склад університету, представники академічної спільноти та роботодавці за фахом.
Рецензування програми здійснювали провідні експерти у сфері захисту інформації: Смірнов О. А., доктор технічних наук, професор, завідувач кафедри кібербезпеки та програмного забезпечення Центральноукраїнського національного технічного університету (м. Кропивницький), та Татьянін В. В., директор ТОВ «АВТОР» (м. Київ). Відгуки рецензентів були позитивними.
ОПП затверджена Вченою радою Київського університету імені Бориса Грінченка (протокол від 23.11.2017 № 11) і введена в дію з 01.09.2018 наказом ректора від 24.11.2017 № 762.
2021 року робочою групою у складі: к.т.н., доцента Соколова В.Ю. (гарант ОПП), Семка В.В., Бессалова А.В., Цирканюк Д.А. було розроблено нову редакцію ОПП у зв'язку з необхідністю приведення змісту ОПП до затвердженого стандарту вищої освіти за спеціальністю 125 Кібербезпека.
В подальшому оновленою робочою групою у складі гаранта ОПП Соколова В.Ю., Гулака Г.М,, Жданової Ю.Д., представників роботодавців Шевченка В.Л., Єрмошина В.В. та здобувачів Цирканюк Д., Подріза Л. до ОПП було внесено зміни (протокол №6 від 27.08.2024), що були зумовлені необхідністю реагування на сучасні виклики та загрози, а також рекомендації, надані НПП та здобувачами/випускниками під час опитувань та обговорень.

5. Інформація про контингент здобувачів вищої освіти на ОП станом на 1 жовтня поточного навчального року у розрізі форм здобуття освіти та ліцензійний обсяг за ОП

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	2024 - 2025	45	33	0
2 курс	2023 - 2024	35	25	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	**62922 Безпека інформаційних і комунікаційних систем**
другий (магістерський) рівень	**62967 Безпека інформаційних і комунікаційних систем**
третій (освітньо-науковий/освітньо-творчий) рівень	**62987 Інформаційна безпека держави**

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

	Загальна площа	Навчальна площа
Усі приміщення ЗВО	37102	14041
Власні приміщення ЗВО (на праві власності, господарського відання або оперативного управління)	36183	13269

Приміщення, які використовуються на іншому праві, аніж право власності, господарського відання або оперативного управління (оренда, безоплатне користування тощо)	919	772
Приміщення, здані в оренду	474	0

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

8. Документи щодо ОП

Документ	Назва файла	Хеш файла
Освітня програма	*ОПП_125_Кібербезпека_магістри.pdf*	U8n2EY7groboDTUc/H6Q6nfhf8R+/pQhQIljrYEekRE=
Навчальний план за ОП	*НП_125_Кібербезпека_магістри.pdf*	K/HZxCDoEYNhvtQLMwHJjwSQSc82M9IOnzVhnJJjQoQ=
Матеріали від ЗВО: пропозиції та рекомендації від роботодавців, таблиця відповідності публікацій наукових керівників напрямам (тематикам) досліджень аспірантів (для ОП третього рівня освіти)	*Рецензії.pdf*	oUFeKJ7ZaLXOpDrlhi3PKY4jHCb4gop2CNPrwG6vCZs=

1. Проєктування освітньої програми

Чи освітня програма дає можливість досягти результатів навчання, визначених стандартом вищої освіти за відповідною спеціальністю та рівнем вищої освіти? 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?

Освітньо-професійна програма «Безпека інформаційних і комунікаційних систем» (далі – ОП, ОПП) розроблена у відповідності до Стандарту вищої освіти України зі спеціальності 125 Кібербезпека другого (магістерського) рівня, затвердженого наказом Міністерства освіти і науки України від 18.03.2021 р. № 332
Стандарту відповідають загальні компетентності (ЗК1–ЗК7), спеціальні компетентності (ФК1–ФК10) та результати навчання РН1–РН23 ОПП. Унікальність ОПП забезпечується через формування ФУ11– ФУ12 та досягнення РНУ24. Загальні компетентності формуються такими ОК, як ОД.01, ОД.02, ОД.03, та також в рамках практик (ОП.01-03). Спеціальні компетентності формуються всіма обов'язковими ОК. Результати навчання також формуються всіма обов'язковими ОК.
Досягнення специфічного результату навчання РНУ24 забезпечується такими ОК, як ОД.04, ОД.05, ОД.06, ОП.01-03.
Можливість досягти результатів навчання також здійснюється завдяки системі внутрішнього забезпечення якості вищої освіти Університету, що функціонує з урахуванням студентоцентрованого підходу до організації усіх складових освітнього процесу, має на меті підготовку конкурентоспроможного на ринку праці випускника (р. ІІ Положення про організацію освітнього процесу в КСУБГ) (https://cutt.ly/yeWdgZG4).

Чи зміст освітньої програми враховує вимоги відповідних професійних стандартів (за наявності)?

ОП не передбачає присвоєння професійної кваліфікації.
Зміст ОП враховує вимоги Стандарту вищої освіти за спеціальністю 125 Кібербезпека для другого (магістерського) рівня вищої освіти, береться до уваги Національна рамка кваліфікацій, QF-EHEA та EQF for LLL. ОП враховує перелік професій даної галузі згідно Класифікатору професій та відповідає деяким професійним стандартам, які розробили фахівці Держспецзв'язку за підтримки Проєкту USAID «Кібербезпека критично важливої інфраструктури України».
Наявність в ОП ОК «Технології безпеки та управління критичними інфраструктурами», «Технології безпеки безпроводових і мобільних мереж», «Технології безпеки Web-ресурсів», «Технології розслідування інцидентів безпеки критичної інфраструктури» підкреслює причетність ОП до професійного стандарту «Аналітик з безпеки інформаційно-телекомунікаційних систем» та «Фахівець з реагування на інциденти кібербезпеки».

Чи мета освітньої програми та програмні результати навчання визначаються з урахуванням потреб заінтересованих сторін (стейкголдерів)?
- здобувачі вищої освіти та випускники програми

ОП оновлюється з урахуванням рекомендацій здобувачів та випускників. Кафедрою ІКБ проводиться постійний моніторинг у вигляді зворотного зв'язку з випускниками та здобувачами, які навчаються за ОП (анкетування через

гугл-форми, організаційні зібрання на курсах, особисте спілкування). На сайті ФІТМ наявна вебсторінка «Обговорення освітніх програм» (https://tinyurl.com/4d2dvcrb).Обговорення змін до ОП відбувається на Раді випускників ФІТМ (https://tinyurl.com/s6nepej2)
Крім того, у складі робочої групи, відповідальної за оновлення ОПП (редакція 2024) входив здобувач Леонід Подріз та випускниця Діана Цирканюк.
Також обговорення ОП відбувається на засіданнях вчених рад ФІТМ, до складу якої входять здобувачі освітніх програм спеціальності 125 Кібербезпека та захист інформації Шевчук Д.А., Голінська О.В. (https://tinyurl.com/mth98jy3).

- роботодавці

ОП розроблена і оновлюється з урахуванням потреб роботодавців.
У складі робочої групи, відповідальної за розробку та впровадження ОП 2024, був заступник директора з наукової роботи Інституту програмних систем НАН України Віктор Шевченко та начальник Департаменту інформаційної безпеки НЕК УКРЕНЕРГО Валерій Єрмошин, за ініціативою якого при оновленні ОПП та РПНД було враховано необхідність захисту критичної інфраструктури. Також при розроблені та оновленні ОПП активну участь брали члени Ради роботодавців ФІТМ (https://tinyurl.com/4ywjxy2b). Визначення потреб роботодавців відбувається й під час конференцій, круглих столів, гостьових лекцій (https://tinyurl.com/mr3w58pt).

- академічна спільнота

Пропозиції та інтереси академічної спільноти враховуються в результаті обговорення на круглих столах, конференціях, семінарах, залучення до ОП провідних фахівців-практиків та іншої спільної діяльності. Академічна спільнота постійно підтримує інтереси та пропозицій щодо формулювання цілей та РН на ОП. Відбуваються розширені засідання групи забезпечення із запрошеними представниками інших ЗВО.
Також на ОП було одержано позитивні рецензії від Трофимчука О.М., члена-кореспондента НАН України, директора Інституту телекомунікацій та глобального інформаційного простору НАН України, та Лукової-Чуйко Н.В., завідувача кафедри кібербезпеки та захисту інформації Київського національного університету імені Тараса Шевченка. Також обговорення ОП відбулося на засіданнях кафедри, засіданні вченої ради ФІТМ. ОП була розглянута та затверджена на засіданні Вченої ради Університету Грінченка.
Крім того, дискусії щодо ОП здійснювалися в рамках неформальних комунікацій з колегами з інших ЗВО. Кафедрою щорічно проводиться Cybersecurity Providing in Information and Telecommunication Systems (CPITS) Workshop (https://cpits.kubg.edu.ua/), де на постійній основі проводяться дискусії щодо розвитку та перспектив освітньо-наукової складової сфери кібербезпеки.

- інші стейкхолдери

Інші стейкхолдери не залучалися.

Чи мета освітньої програми відповідає місії та стратегії закладу вищої освіти?

Відповідно до Стратегії розвитку Університету (https://cutt.ly/gwm2Iubp) його місією є служіння людині, громаді, суспільству, а стратегічними пріоритетами – «підготовка конкурентоспроможних професіоналів за сучасними освітніми програмами, проведення актуальних наукових досліджень, відповідальне служіння громаді для сприяння післявоєнній розбудові країни на засадах сталого розвитку та європейській інтеграції України».
Формулювання мети ОП – «забезпечити здобувачам фундаментальну підготовку у вигляді поглиблених теоретичних і практичних знань, умінь та навичок за спеціальністю 125 Кібербезпека та захист інформації, достатніх для ефективного виконання завдань інноваційного характеру відповідного рівня професійної діяльності в галузях телекомунікацій та інформаційних технологій» – повністю корелює із зазначеною місією та стратегією Університету Грінченка.

Чи мета освітньої програми та програмні результати навчання визначаються з урахуванням тенденцій розвитку науки і спеціальності?

Військова агресія росії проти України поставила перед фахівцями з кібербезпеки та захисту інформації нові виклики, пов'язані як з необхідністю працювати в умовах воєнного стану, так і бути готовими підтримувати державні стратегічні комунікації.
Тенденції розвитку спеціальності 125 Кібербезпека та захист інформації враховуються кафедрою під час щорічного перегляду ОП з урахуванням думки академічної спільноти, стейкхолдерів, результатів моніторингу вступної кампанії, сайтів з працевлаштування тощо. Всі програмні результати навчання відбивають тенденції розвитку спеціальності та розвитку науки в даному напрямку.
З урахуванням необхідності реагування на виклики сьогодення було уточнено назви ОК «Технології безпеки та управління критичними інфраструктурами» та «Технології розслідування інцидентів безпеки критичної інфраструктури».

Чи мета освітньої програми та програмні результати навчання визначаються з урахуванням тенденцій розвитку ринку праці, галузевого та регіонального контексту?

Зважаючи на те, що Університет Грінченка є ЗВО комунальної форми власності, підготовка студентів за ОПП спеціальності 125 Кібербезпека та захист інформації дозволить суттєво вплинути на вирішення задач захисту

інформації як в м. Києві, так і загалом у Київському регіоні. З цією ж метою Університетом укладено угоди із спеціалізованим комунальним підприємством м. Києва «Київтелесервіс» та Департаментом ІКТ виконавчого органу КМДА. Це дозволило студентами спеціальності 125 Кібербезпека та захист інформації проходити у зазначених та інших профільних підприємствах, установах та організаціях виробничу, науково-дослідну та переддипломну практики, виконувати під керівництвом кваліфікованих співробітників зазначених установ курсові проєкти та/або кваліфікаційні магістерські роботи. Це також сприяє позитивній динаміці працевлаштування випускників ОПП. Актуальна потреба у фахівцях кібербезпеки, здатних ефективно працювати в умовах воєнного стану, а також значним розвитком SMART-технологій у м. Києві, зумовили формулювання результату навчання РНУ24 та фахових компетентностей ФКУ11 та ФКУ12.

Чи мета освітньої програми та програмні результати навчання визначаються з урахуванням досвіду аналогічних вітчизняних освітніх програм?

Робочою групою був розглянутий та взятий до уваги досвід з підготовки фахівців з аналогічної спеціальності в інших ЗВО України, зокрема: КНУ ім. Тараса Шевченка, ХНУРЕ, НТУУ «КПІ» ім. Сікорського, НУ «Львівська політехніка», Державний університет інформаційно-комунікаційних технологій.
В ОП КНУ ім. Тараса Шевченка здійснено аналіз програмних результатів навчання, структури та змісту освітніх компонентів ОП.
В ОП НТУУ «КПІ» ім. Сікорського проаналізовано структуру й зміст ОП, зокрема увагу привернули освітні компоненти вибіркового блоку.
ОП Державного університету інформаційно-комунікаційних технологій проаналізована особливість підготовки за спеціальністю 125, що полягає у можливості профілювати підготовку за трьома практичними лініями підготовки.
Врахування досвіду вітчизняних освітніх програм дозволило забезпечити відповідність освітньої програми сучасним вимогам та тенденціям розвитку галузі, а також посилити її конкурентні переваги. Важливо відзначити, що конкурентною перевагою ОП, порівняно з аналогічними вітчизняними освітніми програмами, є її практична орієнтованість та компетентнісний підхід.
Разом з тим, ОП, що акредитується, має свою унікальність, яка відображена, серед іншого, в акценті на формуванні результату навчання РН(У) 24 «Знати уразливості й методи їх застосування і різних телекомунікаційних технологіях та SMART-інфраструктурі. Вміти проектувати захищені (з урахування загроз) проводові і безпроводові телекомунікаційні, SMART-системи».

Чи мета освітньої програми та програмні результати навчання визначаються з урахуванням досвіду аналогічних іноземних освітніх програм?

При розробці та оновленні ОПП було проаналізовано зміст програм підготовки в галузі кібербезпеки таких іноземних програм, як University of Colorado (США), College of Engineering and Computing (США). Також був врахований досвід «Магістерської програми підготовки нових експертів з кібербезпеки» (проект ENGENSEC TEMPUS IV №544455- TEMPUS-1-2013—1 SE-TEMPUS-JPCR https://engensec.eu/).
Так в основу розробки ОПП та НП було покладено та адаптовано 7 розроблених курсів:
Курси «Adv. Network & Cloud security» та «Malware»було реалізовано в ОК «Технології безпеки та управління критичними інфраструктурами»
Курс «Wireless & Mobile security» реалізовано в ОК «Технології безпеки безпроводових і мобільних мереж»
Курс «Web security» реалізовано в ОК «Технології безпеки Web-ресурів»
Курси «Pentest and ethical hacking», «Digital forensic», Secure software development» реалізовано в ОК «Прикладні аспекти тестування на проникнення та етичного хакінгу», «Технології розслідування інцидентів безпеки критичної інфраструктури»
Враховані міжнародні стандарти: National Science Education Standards, NRC & NAP та K-4 і 9-12 «Наука і дослідження. Розвиток умінь і знань студентів»; рекомендації міжнародної ініціативи CDIO Standard 2.1.

2. Структура та зміст освітньої програми

Яким є обсяг ОП (у кредитах ЄКТС)?

90

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)?

64

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

26

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

ОПП розроблена у повній відповідності зі Стандартом вищої освіти України спеціальності 125 Кібербезпека другого (магістерського) рівня, затвердженого наказом Міністерства освіти і науки України від 18.03.2021 р. № 332.
Відповідність предметній області відображено в меті, об'єкті, методах та компонентах ОП. Метою ОП є забезпечення студентам фундаментальної підготовки у вигляді поглиблених теоретичних і практичних знань, умінь та навичок за спеціальністю 125, достатніх для ефективного виконання завдань інноваційного характеру відповідного рівня професійної діяльності в галузях телекомунікацій та ІТ.
Об'єктами вивчення та діяльності в рамках ОП є сучасні процеси дослідження, аналізу, створення та забезпечення функціонування інформаційних систем і технологій, інших бізнес-операційних процесів на об'єктах інформаційної діяльності та критичних інфраструктур сфери ІБ та/або КБ, інформаційні системи (інформаційно-комунікаційні, інформаційно-телекомунікаційні, автоматизовані) та технології, інфраструктура об'єктів інформаційної діяльності та критичних інфраструктур, системи та комплекси створення, обробки, передачі, зберігання, знищення, захисту та відображення даних (інформаційних потоків), інформаційні ресурси різних класів (в т.ч. державні інформаційні ресурси), програмне та програмно-апаратне забезпечення (засоби) кіберзахисту, системи управління ІБ та/або КБ, технології, методи, моделі та засоби ІБ та/або КБ, об'єкти інформатизації, включаючи комп'ютерні, автоматизовані, телекомунікаційні, інформаційні, інформаційно-аналітичні, інформаційно-телекомунікаційні системи, інформаційні ресурси і технології, технології КБтаЗІ, процеси управління ІБ та/або КБ об'єктів, що підлягають захисту, методи застосування уразливостей в телекомунікаційних технологіях і SMART-інфраструктури та способи боротьби з ними, методи організації захищеної передачі даних у незахищеному SMART-середовищі, засоби спеціального мережевого обладнання для забезпечення безпеки корпоративних мереж, концепції проєктування, побудови та експлуатації захищених проводових і безпроводових телекомунікаційних та SMART-систем. Це цілком корелює з визначеним в Стандарті об'єктам діяльності, уточнюючи їх відповідно до фокусу ОП.
Методи, моделі, методики та технології створення, обробки, передачі, приймання, знищення, відображення, захисту (кіберзахисту) інформаційних ресурсів у кіберпросторі, а також методи та моделі розробки та використання прикладного і СПЗ для вирішення професійних задач в галузі ІБ та/або КБ.
Теоретичні засади наукових технологій, фізичні і математичні фундаментальні знання, теорії ідентифікації та прийняття рішень, системного аналізу, складних систем, моделювання та оптимізації процесів, теорія математичної статистики, криптографічного та технічного захисту інформації, теорії ризиків та інших міждисциплінарних теорій і практик у галузі ІБ та/або КБ.
Відповідність із визначеним у Стандарті описом предметної області реалізується у змісті обов'язкових ОК.

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

Індивідуальна освітня траєкторія (ІОТ) формується здобувачами вищої освіти з урахуванням їх здібностей, інтересів, потреб, мотивації, можливостей і досвіду і забезпечується такими документами ЗВО:
- Стратегією розвитку ЗВО (https://cutt.ly/gwm2Iubp) (Стратегічні напрями, п.6);
- Положенням про організацію освітнього процесу (https://cutt.ly/yeWdgZG4) (п.5.3 Індивідуальний навчальний план; Додаток 1«Порядок визнання та перезарахування результатів навчання в КСУБГ);
- Положенням про порядок та умови здійснення вибору навчальних дисциплін (https://cutt.ly/XeWdkTfW);
- Положенням про порядок реалізації права на акад. мобільність учасників освітнього процесу (https://cutt.ly/veWdl3xg).
Здобувачі мають право на:
- вибір ОК в обсязі, що становить не менше як 25% від заг. кількості кредитів ЄКТС, передбачених ОПП;
- навчання одночасно за декількома ОПП, зокрема в інших ЗВО;
- навчання за інд. графіком та участь у формуванні ІНП;
- акад. мобільність, зокрема міжнародну;
- визнання РН, отриманих в інших ЗВО;
- можливість зарахування кредитів, отриманих шляхом неформальної та інформальної освіти;
- право на акад. відпустку або перерву в навчанні, а також на поновлення на навчання;
- можливість пропонувати бази для проходження практики;
- можливість пропонувати власні теми кваліфікаційних магістерських робіт.

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

Право на вибір навчальних дисциплін в Університеті реалізується відповідно до Положення про порядок та умови здійснення вибору навчальних дисциплін здобувачами освіти (https://cutt.ly/XeWdkTfW).
Вибір освітніх компонентів здійснюється здобувачем або з вибіркового блоку шляхом написання відповідної заяви на ім'я декана щодо бажання опанувати конкретний блок, або з Каталогу вибіркових дисциплін (КВД) із дотриманням розподілу кредитів по семестрах навчального плану ОП.
КВД (https://tinyurl.com/3t3zprhe) оновлюється щорічно. За Положенням визначаються терміни формування КВД, особливості та термін проведення процедури вибору здобувачем навчальних дисциплін. Наказ про формування переліку вибіркових навчальних дисциплін та строки їх вибору здобувачами освіти у відповідному році закріплює визначену процедуру.
На рівні факультету за розпорядженням декана у грудні для формування переліку вибіркових дисциплін затверджується склад робочої групи. До роботи з формування КВД залучаються як НПП, так і представники студентського самоврядування, Наукового товариства студентів, аспірантів, докторантів та молодих вчених факультету. До 15 січня на кафедрі на основі пропозицій викладачів формується перелік вибіркових дисциплін, який

попередньо обговорюється і затверджується на засіданні кафедри. Для другого (магістерського) рівня вищої освіти перелік може бути уточнений кафедрою до 15 травня поточного навч. року.
Затверджені пропозиції розміщуються у системі електронного навчання Університету.
Члени робочої групи та викладачі кафедри проводять зустрічі зі здобувачами вищої освіти, анонсують затверджені пропозиції вибіркових дисциплін, проводять роз'яснювальну та консультативну роботу. В Ун-ті розроблено й запроваджено «Інструкцію здійснення вибору здобувачами дисциплін з Каталогу вибіркових дисциплін» (https://tinyurl.com/yk76f3zh).
Процедура вибору здійснюється здобувачем в особистому електронному кабінеті. Описи запропонованих вибіркових дисципліни містять мету, анотацію, програмні результати навчання, наявність ЕНК та кількість годин. Обрані дисципліни фіксуються відміткою у полі «Мій вибір остаточний». Це вважається фактом подання заяви для вивчення відповідних вибіркових освітніх компонентів із Каталогу.

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

ОП і НП передбачає практичну підготовку здобувачів освіти: практичні заняття, проходження виробничої практики (4,5 кредитів), науково-дослідницької практики (4,5 кредитів) та переддипломної практики (6 кредитів).
Виробнича, науково-дослідна та переддипломна практики передбачені у 3 семестрі. Базами практики є державні установи, департаменти КМДА та підприємства, (https://tinyurl.com/5ytyjh5y). Бази підбираються відповідно до завдань практики і є середовищем формування професійних компетентностей.
В ОП більшість ОК забезпечують набуття практичних компетентностей для професійної діяльності. НПП, які викладають на ОП, були й залишаються учасниками проєктів у сфері кібербезпеки та захисту інформації (Складанний П., Соколов В.), є членами редколегій наукових видань (Соколов В., Складанний П., Козачок В.) та міжнародних конференцій, мають досвід міжнародного стажування й участі в грантових програмах тощо. Свій практичний досвід вони використовують в освітньому процесі.

Продемонструйте, що ОП дозволяє забезпечити набуття здобувачами вищої освіти соціальних навичок (soft skills) упродовж періоду навчання

П передбачає набуття здобувачами соціальних, зокрема комунікативних навичок (soft skills), неспеціалізованих, надпрофесійних, які відповідають за кооперацію у робочому процесі, продуктивність та ефективність (критичне мислення, креативність, емпатія, самоконтроль, здатність до співробітництва, саморефлексії, толерантність, етичність тощо).
ОК передбачають формування і удосконалення здатності до застосуванні знань у практичних ситуаціях, проведенні досліджень, абстрактного мислення, аналізу та синтезу, забезпеченні якості виконуваних робіт, спілкуватися з представниками інших професійних груп, професійного спілкування іноземною мовою.
Формуванню соціальних навичок сприяють інтерактивні, проблемно-пошукові та дослідницькі методи навчання, серед яких дискусії, мозковий штурм, метод проєктів.
Переддипломна практика, виконання кваліфікаційної магістерської роботи, його розроблення та публічний захист впроваджують соціальні навички у професійну діяльність та унаочнюють рівень їх сформованості.
Розвитку соціальних навичок здобувачів поза навчанням сприяють участь у наукових конференціях, круглих столах, форумах, програмах академічної мобільності.

Продемонструйте, що зміст освітньої програми має чітку структуру; освітні компоненти, включені до освітньої програми, становлять логічну взаємопов'язану систему та в сукупності дають можливість досягти заявленої мети та програмних результатів навчання. Продемонструйте, що зміст освітньої програми забезпечує формування загальнокультурних та громадянських компетентностей, досягнення програмних результатів навчання, що передбачають готовність здобувача самостійно здійснювати аналіз та визначати закономірності суспільних процесів

Зміст ОП складають обов'язкові освітні компоненти загальною кількістю 64 кредити і вибіркові (26 кредитів). Освітні компоненти утворюють логічну систему, розподілені послідовно й умотивовано на 3 семестри навчання здобувачів.
Дисципліни обов'язкового й вибіркового компонентів (вибірковий блок 1) працюють на досягнення мети ОП – забезпечити здобувачам фундаментальну підготовку у вигляді поглиблених теоретичних і практичних знань, умінь та навичок за спеціальністю 125 Кібербезпека та захист інформації, достатніх для ефективного виконання завдань інноваційного характеру відповідного рівня професійної діяльності в галузях телекомунікацій та інформаційних технологій. Вивчення теоретичних і практикоорієнтованих дисциплін ОП сприяють досягненню програмних результатів навчання: вміння приймати ефективні рішення, аналізувати та оцінювати вплив технологій на розвиток галузі, оцінювати достовірність інформації та надійність джерел, ефективно використовувати інформацію для наукової та практичної діяльності. Досягненню мети ОП та програмних результатів навчання сприяє й достатня кількість годин практики (15 кредитів), а також підготовка й захист кваліфікаційної магістерської роботи (6 кредитів), яка передбачає розв'язання задачі дослідницького та/або інноваційного характеру у сфері кібербезпеки.

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

Питання співвіднесення обсягу окремих ОК (у кредитах ЄКТС) із фактичним навантаженням здобувачів вищої освіти регламентується Положенням про організацію освітнього процесу (https://cutt.ly/yeWdgZG4).
Відповідно до Положення у навчальному навантаженні зазначається час, потрібний здобувачам вищої освіти для

завершення всіх видів навчальної діяльності (лекції, практичні, семінарські, самостійна робота, екзамени), необхідних для досягнення очікуваних результатів навчання. 60 кредитів відповідають навчальному навантаженню повного року формального навчання (навчального року) й асоційованим результатам навчання. Навантаження студента становить 1800 годин на навчальний рік. Мінімальний обсяг освітньої компоненти складає 4 кредити. Один кредит відповідає 30 годинам. Кількість аудиторних годин на один кредит для магістрів, як правило, становить 8 годин. Для проміжного (модульного) контролю виділяється до 2 годин на один кредит. Решта часу відводиться для самостійної роботи, з яких для підготовки до екзамену та його складання виділяється 30 годин.

Яким чином структура освітньої програми, освітні компоненти забезпечують практикоорієнтованість освітньої програми? Якщо за ОП здійснюється підготовка здобувачів вищої освіти за дуальною формою освіти, опишіть модель та форми її реалізації

Дороговказом при розробленні ОП стала модель практико-орієнтованого навчання, яка є пріоритетною в Університеті Грінченка.
Практикоорієнтованість ОП забезпечується великим обсягом практик (виробнича, науково-дослідницьк та переддипломна, сумарний обсяг 15 кредитів, та акцентом при вивченні дисциплін на практичних заняттях. Практикоорієнтованість ОП реалізується також через використання в освітньому процесі Центрів компетентностей, обладнаних сучасною технікою, в яких проходять частина занять: Кіберполігон (https://tinyurl.com/ywzepjnc), у складі 3 лабораторій: безпеки інформаційних активів, антивірусного захисту інформації, систем технічного та криптографічного захисту інформації, а також центрі живої математики (https://fitm.kubg.edu.ua/?Itemid=2097), лабораторії комп'ютерних мереж (https://tinyurl.com/2u8shem8), лабораторії вбудованих систем і 3D моделювання (https://tinyurl.com/mtecry7m) та центрі моделювання і програмування (https://tinyurl.com/53k4cwu7).
Підготовка здобувачів вищої освіти за дуальною формою не здійснюється.

Яким чином ОП забезпечує набуття здобувачами навичок і компетентностей направлених на досягнення глобальних цілей сталого розвитку до 2030 року, проголошених резолюцією Генеральної Асамблеї Організації Об'єднаних Націй від 25 вересня 2015 року № 70/1, визначених Указом Президента України від 30 вересня 2019 року № 722

гідно зі Стратегією розвитку (https://cutt.ly/gwm2Iubp), Ун-т реалізує пріоритетні для своєї діяльності Цілі сталого розвитку ООН, зокрема: Ціль 4 Якісна освіта; Ціль 11 Сталий розвиток міст та спільнот; Ціль 16 Мир, справедливість і міцні інституції; Ціль 17 Партнерство заради сталого розвитку та ін. (https://tinyurl.com/2n7ykcdj). Університет має Дорожню карту сталого розвитку університету (https://tinyurl.com/4b6c6ybm), бере участь у щорічному рейтингу Times Higher Education Impact Ranking (https://tinyurl.com/7fzx7h48).
ЦСР-4 досягається як системою внутр. забезпечення якості Ун-ту, так і заходами, що організовуються факультетом та кафедрою (https://tinyurl.com/3kn28a5h). Зокрема, це майстер-класи, відкриті лекції, воркшопи за участю фахівців, дотичних до профілю ОП, в яких беруть участь здобувачі та викладачі ОП.
Найбільшою мірою ОП, що природньо випливає з її фокусу, забезпечує досягнення ЦСР-9 промисловість, інновації та інфраструктура. Враховуючи, що Ун-т є комунальним ЗВО, важливою є ЦСР-11, досягнення якої забезпечується взаємодією з місцевими органами влади, проходженням здобувачами практики в структурах КМДА.

3. Доступ до освітньої програми та визнання результатів навчання

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

Сторінка на сайті університету (вступникам): https://kubg.edu.ua/informatsiya/vstupnikam/pravyla-pryiomu.html

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

Згідно з Правилами прийому на навчання для здобуття ступеня бакалавра, магістра Університету у 2024 р. (https://tinyurl.com/53rp6jmn) для вступників на ОП «Безпека інформаційних у комунікаційних систем» другого (магістерського) рівня освіти встановлено, що вступник має пройти конкурсний відбір за результатами єдиного вступного іспиту (ЄВІ, ЄФВВ). Вступники, які отримали ступінь бакалавра зі спеціальності 125 і у 2024 році складали ЄДКІ, використовують його результати замість ЄФВВ. Правилами також передбачені спеціальні умови участі у конкурсному відборі на навчання: співбесіда з іноземної мови замість ЄВІ та/або фахового іспиту замість ЄФВВ, а також визначено коло осіб, які можуть скористатися цими умовами (п. 8.6 Правил). Під час вступної кампанії 2024 року випадків вступу на ОП за спеціальними умовами не було.
Під час вступної кампанії 2024 р. фахові іспити в Університеті проводились дистанційно (Додаток 10 Правил прийому). За зверненням вступника Приймальна комісія надавала підтримку щодо створення умов для проходження фахового іспиту. Для цього були напоготові технічні засоби, наявні в приміщеннях Університету.

Яким документом ЗВО регулюється питання визнання результатів навчання та кваліфікацій, отриманих на інших освітніх програмах? Яким чином забезпечується доступність цієї процедури для учасників освітнього процесу?

Визнання РН та кваліфікацій, отриманих в інших ЗВО, регулюється:
- Правилами прийому на навчання (https://kubg.edu.ua/informatsiya/vstupnikam/pravyla-pryiomu.html);

- Положенням про організацію освітнього процесу в Київському столичному університеті імені Бориса Грінченка (Додаток 1 «Порядок визнання та перезарахування результатів навчання в Київському столичному університеті імені Бориса Грінченка»),
(https://cutt.ly/yeWdgZG4);
- Положенням про порядок реалізації права на академічну мобільність учасників освітнього процесу КСУБГ (пункт 9) (https://cutt.ly/veWdl3xg).

Ці документи розміщені на сайті Університету, що забезпечує їх доступність для учасників освітнього процесу.

Наведіть конкретні приклади та прийняті рішення щодо визнання результатів навчання та кваліфікацій, отриманих на інших освітніх програмах (зокрема під час академічної мобільності)

На ОП таких прикладів не було.

Яким документом ЗВО регулюється питання визнання результатів навчання, отриманих в неформальній та/або інформальній освіті? Яким чином забезпечується доступність цієї процедури для учасників освітнього процесу?

Процедура визнання результатів навчання (далі – РН), здобутих шляхом неформальної/ інформальної освіти визначена в додатку 1 «Порядок визнання та перезарахування результатів навчання…» до Положення про організацією освітнього процесу в КСУБГ (https://cutt.ly/yeWdgZG4).
Здобувач може ініціювати визнання РН, здобутих шляхом неформальної та/або інформальної освіти, подавши на ім'я декана факультету відповідну заяву До заяви додаються підтвердні документи, що містять інформацію про неформальне чи інформальне навчання. У випадку відсутності підтвердних документів чи відсутності в них задекларованої інформації про зміст та РН здобувач заповнює Декларацію про попереднє навчання, здобуті РН та надає додаткові документи, які підтверджують наведену в Декларації інформацію. Заступник декана з науково-методичної та навчальної роботи приймає заяви, надає консультативну підтримку, зокрема щодо заповнення декларації, проводить попередній аналіз достатності поданої інформації для прийняття подальших рішень. Розгляд заяви, документів та прийняття рішення про визнання здійснюється комісією, до складу якої входять: декан факультету, заступник декана, завідувач відповідної кафедри, гарант відповідної ОП. Рішення про зарахування ОК оформлюється розпорядженням декана факультету.

Наведіть конкретні приклади та прийняті рішення щодо визнання результатів навчання отриманих у неформальній та/або інформальній освіті

На ОП таких прикладів не було.
З метою інформування здобувачів про можливості визнання результатів навчання отриманих у неформальній та/або інформальній освіті на вебсайті ФІТМ створено відповідний розділ «Неформальна/інформальна освіта», де розміщена нормативна база та актуальні можливості: https://fitm.kubg.edu.ua/informatsiya/studentam/neformalna-informalna-osvita/mozhlyvosti.html

4. Навчання і викладання за освітньою програмою

Продемонструйте, що освітній процес на освітній програмі відповідає вимогам законодавства (наведіть посилання на відповідні документи). Яким чином методи, засоби та технології навчання і викладання на ОП сприяють досягненню мети та програмних результатів навчання?

Освітній процес на ОП регулюється Положенням про організацію освітнього процесу (https://cutt.ly/yeWdgZG4). Положення є основним нормативним документом, що регулює діяльність структурних підрозділів Університету з надання освітніх послуг для здобуття вищої освіти. Положення розроблено відповідно до Законів України «Про освіту», «Про вищу освіту» та інших нормативно-правових актів.
Всі форми (лекції, практичні, лабораторні, семінарські заняття, консультації, сам. робота, практ. підготовка, контрольні заходи) спрямовані на формування передбачених ЗК, ФК та досягнення РН.
Освітній процес має практико-орієнтований характер, що реалізується, зокрема, на основі потенціалу центрів компетентностей ФІТМ та під час проходження передбачених ОП практик.
Для досягнення РН використовуються: словесні (лекція), наочні (ілюстрація через презентацію), практичні роботи, лабораторні роботи, самостійна робота. Конкретні форми, методи, засоби та технології навчання і викладання добираються викладачем з огляду на мету та РН конкретної дисципліни і є реалізацією принципу академічної свободи.

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

Пріоритетність студентоцентризму в освітньому процесі закріплена в Стратегії розвитку КСУБГ на 2023-2027 рр. (розділ 6, https://cutt.ly/gwm2Iubp) та Положенні про організацію освітнього процесу (https://cutt.ly/yeOi3cBf). Університет сприяє розвитку здобувачів освіти як свідомих і відповідальних громадян, цілісних та культурних особистостей, конкурентоспроможних професіоналів та лідерів. Методи і засоби навчання обираються відповідно до змісту ОК, їх студентоцентрованість полягає у виборі оптимальних практик викладання, максимально спрямованих

на досягнення ПРН. Для всіх ОК створено ЕНК, які є інформ. ресурсами, що дають змогу здобувачам навчатися в асинхронному режимі у зручний для них час. ЕНК наповнені теорет. та практико-орієнтованими матеріалами, що забезпечує студенту вільний вибір методів навчання.
Для оцінки рівня задоволеності здобувачів методами навчання і викладання проводиться загальноуніверситетське анонімне анкетування «Викладач очима студентів».
НПП ОП традиційно мають високі оцінки: у 2024 р. середньоарифметична оцінка склала 4,88 бали за 5-бальною шкалою.

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

Принципи академічної свободи в Університеті відображені в Положенні про організацію освітнього процесу (https://cutt.ly/yeWdgZG4). Різноманітність форм, методів та засобів навчання і викладання дають можливість реалізувати принципи акад.свободи, оскільки викладачі мають право самостійно обирати форми та методи навчання відповідно до власного бачення та творчого потенціалу, з дотриманням принципу толерантного ставлення до альтернативних позицій і підходів.
Усі учасники освітнього процесу мають вільний доступ до інформаційних і бібліотечних ресурсів. Викладачі мають право обирати способи, форми та бази підвищення кваліфікації.
Здобувачі вільно обирають дисципліни вибіркової частини ОП, теми своїх кваліфікаційних робіт. Вони мають можливість брати участь у роботі наукових семінарів та публікувати свій науковий доробок. Крім того, реалізації принципів академічної свободи сприяє участь здобувачів у роботі органів студентського самоврядування, ВР ф-ту, Наукового товариства студентів, аспірантів, докторантів та молодих учених.

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

На початку освітнього процесу, на першій зустрічі здобувачів другого (магістерського) рівня вищої освіти з гарантом ОП, завідувачем кафедри та НПП кафедри надається інформація про ОП, її цілі та зміст, демонструється та роз'яснюється структурна навчального плану, особливості освітнього процесу в Університеті, права та обов'язки здобувачів.
Відповідно до Положення про організацію освітнього процесу (https://cutt.ly/yeWdgZG4), для кожного ОК, згідно з навчальним планом, щороку викладачі укладають/оновлюють РПНД, які розглядаються на засіданні кафедри, погоджуються з гарантом ОП та затверджуються рішенням кафедри. Розроблення РПНД здійснюється відповідно до Методичних рекомендацій з розроблення робочих програм навчальних дисциплін (https://cutt.ly/oeWdhIch).
Актуальні РПНД розміщено в системі електронного навчання Університету, в оболонці ЕНК на платформі Moodle та на вебсторінці кафедри (https://tinyurl.com/565ahpbf). Кожен викладач на першому занятті ознайомлює здобувачів з РПНД, пояснює цілі, зміст та очікувані РН, порядок і критерії оцінювання. Критерії оцінювання деталізуються у програмах іспитів, які розміщені на вебсторінці факультету (https://tinyurl.com/265aw544).

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

Поєднання навчання і досліджень зумовлене багатьма методами та формами роботи здобувачів. Викладання більшості ОК передбачає використання методології, яка безпосередньо стимулює дослідницьку діяльність здобувачів.
Частка самостійної роботи складає близько 50 % загального обсягу годин, виділених, згідно з НП та ОП, на вивчення обов'язкових ОК. Працюючи самостійно над вирішенням завдань, поставлених викладачем, здобувач набуває ЗК та СК шляхом активного дослідницько-орієнтованого навчання.
Тематичний зміст, плани семінарських і практичних занять побудовані таким чином, що під час заняття здобувачі виконують міні-дослідження, самостійно шукають та аналізують інформацію у відкритих або спеціально підготовлених і наданих викладачем джерелах, а потім удосконалюють, допрацьовують отримані результати цих досліджень у ході дискусій, «мозкових штурмів», із застосуванням інших форм і методів роботи, індивідуальної та групової.
У процесі проходження виробничої, науково-дослідної та переддипломної практики кожний здобувач, як правило, виконує низку завдань дослідницького характеру. Переліки та результати цих досліджень, інколи доволі складних, комплексних, тривалих, відображено в індивідуальних звітах здобувачів про проходження практики, відгуках керівників практики.
Підготовка та захист кваліфікаційної (магістерської) роботи є тим ОК, у якому найбільш активно реалізується поєднання з дослідженнями. Результати дослідницької діяльності здобувачів, отримані в ході роботи на семінарських, практичних заняттях, у самостійній роботі, у процесі виробничої та переддипломної практики й безпосередньої підготовки кваліфікаційної роботи проходять апробацію шляхом участі в круглих столах, наукових, науково-практичних конференціях (https://tinyurl.com/mta7x9k4), а також здобувачі публікують результати власних досліджень в електронному фаховому виданні «Кібербезпека: освіта, наука, техніка» (https://www.csecurity.kubg.edu.ua/)

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

Відповідно до Положення про організацію освітнього процесу (Розділ 2) (https://cutt.ly/yeWdgZG4), система внутрішнього забезпечення якості вищої освіти включає в себе постійне оновлення і вдосконалення навчально-методичного забезпечення і реалізується через: щорічне оновлення робочих програм навчальних дисциплін /

програм практик з обов'язковим їх обговоренням на засіданнях кафедр із зазначенням ресурсів наявних у фондах бібліотеки (основної літератури, фахових періодичних видань, електронних, мультимедійних ресурсів тощо); оновлення і розроблення нових засобів діагностики навчальних досягнень (зокрема засобів проміжного і підсумкового контролю, атестації) для досягнення результатів навчання, програмних результатів навчання; обов'язкове забезпечення навчальних дисциплін електронними навчальними курсами.
Напередодні початку 2024-25 н.р. кафедрою були переглянуті та оновлені РПНД обов'язкових дисциплін ОП, які були затверджені в установленому порядку, та ЕНК низки дисциплін. Зокрема, були оновлені списки джерел (в т.ч. за рахунок нових власних публікацій викладачів), зміст лекцій, семінарських та практичних занять тощо.
Зокрема було оновлено РПНД ОК 7 «Технології розслідування інцидентів безпеки критичної інфраструктури» та ОК 4 «Технології безпеки та управління критичними інфраструктурами», в частині інтеграції питань захисту саме критичної інфраструктури.
Також в РПНД було враховано досвід реалізації кафедральної наукової теми «Методи та моделі забезпечення кібербезпеки інформаційних систем переробки інформації та функціональної безпеки програмно-технічних комплексів управління критичної інфраструктури" (реєстраційний номер 0122U200483)

Опишіть, яким чином навчання, викладання та наукові дослідження пов'язані з інтернаціоналізацією діяльності за освітньою програмою та закладу вищої освіти

Стратегією розвитку Університету (https://cutt.ly/gwm2Iubp) інтернаціоналізація визначена пріоритетом в організації діяльності Університету. Так, у Розділі 8 визначено таку стратегічну ціль: «Університет має розгалужену міжнародну партнерську мережу, ефективно співпрацює з іноземними закладами».
Викладачі ОП є активними учасниками міжнародних конференцій (https://tinyurl.com/y3admf9d) та міжнародних грантів (https://tinyurl.com/23a5k3x2)
Здобувачі ОП брали участь у майстер-класах та гостьових лекціях (https://tinyurl.com/4d923vj7)
Для задоволення публікаційних потреб здобувачів та НПП на кафедрі функціонує Workshop on Cybersecurity Providing in Information and Telecommunication Systems (https://cpits.kubg.edu.ua/) та
Workshop on Classic, Quantum, and Post-Quantum Cryptography (https://cqpc.kubg.edu.ua/), матеріали яких індексуються у наукометричній базі Scopus.
НПП ОП мають публікації у зарубіжних наукових виданнях, у т.ч. що входять до наукометричних БД Scopus, WoS.

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

Яким чином форми контрольних заходів та критерії оцінювання здобувачів вищої освіти дають можливість встановити досягнення здобувачем вищої освіти результатів навчання для окремого освітнього компонента та/або освітньої програми в цілому?

Система контролю за рівнем знань здобувачів регламентована «Положенням про організацію освітнього процесу в Університеті» (п. 4.4) (https://cutt.ly/yeWdgZG4).
Форми контролю для кожного ОК визначено в ОП, навчальному плані, РПНД.
Перевірка й оцінювання результатів навчання передбачає проміжний та підсумковий контроль. Проміжний контроль відбувається упродовж семестру під час виконання практичних завдань, самостійної роботи, усного й письмового опитування з метою оперативного отримання об'єктивних даних про рівень знань, умінь і практичних навичок із навчальної дисципліни. У результаті проміжного контролю визначається рівень розуміння та засвоєння знань з певної теми й уміння застосовувати їх на практиці. За результатами опанування певного змістового модулю передбачено здійснення модульного контролю у формі тестування, або контрольних робіт із запитаннями й завданнями.
Підсумковий контроль включає семестровий контроль: заліки, екзамени (тестування або захисти проєктів, перевірка звіту та матеріалів практики) й атестацію (підготовка та захист кваліфікаційної магістерської роботи).
Форми проведення проміжного контролю та критерії оцінювання зазначаються у РПНД. Обов'язково проводяться поточні й екзаменаційні консультації, для чого відводяться години в навчальному навантаженні НПП.
Екзамен як форма семестрового контролю передбачений для обов'язкових дисциплін ОД.03, ОД.04, ОД.06, ОД.08.
Конкретна форма проведення екзамену добираються викладачем з огляду на мету та зміст дисципліни і є реалізацією принципу академічної свободи. В умовах воєнного стану екзамени можуть проводитися у дистанційній формі з використанням платформи Moodle (https://elearning.kubg.edu.ua/) для письмового виконання тестових завдань та Google Meet.
Результати навчання здобувачів вищої освіти щодо опанування навчальної дисципліни оцінюються за 100-бальною шкалою.

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

Чіткість та зрозумілість форм контрольних заходів та критеріїв оцінювання навчальних досягнень здобувачів вищої освіти, а також термінів їх проведення забезпечують: Положення про організацію освітнього процесу (https://cutt.ly/yeWdgZG4); уніфікована Система оцінювання навчальних досягнень студентів Університету (розділ 6 Положення).
Форми поточного контролю, критерії оцінювання за кожний вид навчальної діяльності містяться у РПНД, які розміщені на сторінці кафедри та в ЕНК відповідної дисципліни. У навчально-методичній картці дисципліни зазначається кількість балів, які здобувач може набрати за кожний вид навчальної діяльності.
Кожен електронний курс на платформі Moodle має опцію «Електронний журнал», у якому кожен здобувач

індивідуально може відслідковувати свої бали за навчальну діяльність.
Форма проведення семестрового контролю, зміст і структура екзаменаційного білету, критерії оцінювання визначаються програмою екзамену (оприлюднюються на сторінці факультету – https://tinyurl.com/265aw544).
Форма атестації випускників – публічний захист кваліфікаційної магістерської роботи. Порядок подання роботи до захисту, процедура захисту, порядок оцінювання наведені в методичних рекомендаціях, розроблених кафедрою (https://tinyurl.com/5yjfft62). Для проведення публічного захисту створюється комісія, відповідно до Положення Університету про порядок створення та організацію роботи ЕК (https://cutt.ly/8eWdjJCD).

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

Форми проведення підсумкового контролю зазначені в ОП та НП, які розміщені на сайті Університету в розділі «Вступникам» та на сторінці кафедри (https://tinyurl.com/3b4r8zsw).
Форми контрольного заходу та критерії оцінювання ОК зазначені в РПНД, ЕНК. РПНД оприлюднюються на сторінці кафедри до початку навчального року (https://tinyurl.com/565ahpbf).
Інформування здобувачів освіти щодо форм контрольних заходів та критеріїв оцінювання навчальних досягнень здійснюється таким чином:
– графіки освітнього процесу, переліки навчальних дисциплін, які виносяться на заліково-екзаменаційну сесію, графіки проходження атестацій, програми іспитів оприлюднені на сторінці ФІТМ (https://fitm.kubg.edu.ua/informatsiya/studentam/osvitnii-protses.html);
– на першому занятті з дисципліни викладачі пояснюють здобувачам вищої освіти процедуру і вимоги контрольних заходів, передбачених РПНД, пояснюють/нагадують критерії системи оцінювання навчальних результатів, що визначає чіткість та зрозумілість подальшої взаємодії;
– під час настановної конференції з практики здобувачам пояснюють критерії оцінювання завдань практики відповідно до робочої програми;
– на сторінці кафедри оприлюднені вимоги до підготовки кваліфікаційної магістерської роботи (https://tinyurl.com/5yjfft62).

Яким чином форми атестації здобувачів вищої освіти відповідають вимогам стандарту вищої освіти (за наявності)? Продемонструйте, що результати навчання підтверджуються результатами єдиного державного кваліфікаційного іспиту за спеціальностями, за якими він запроваджений

Відповідно до вимог Стандарту вищої освіти України другого (магістерського) рівня спеціальності 125 Кібербезпека та захист інформації атестація випускників ОПП здійснюється у формі публічного захисту кваліфікаційної роботи.
Згідно з розробленими та затвердженими випусковою кафедрою «Методичними рекомендаціями …» (https://tinyurl.com/5yjfft62) кваліфікаційна робота має продемонструвати уміння здобувача самостійно вести науковий пошук і вирішувати конкретні наукові завдання.
Кваліфікаційна робота магістра спеціальності 125 Кібербезпека та захист інформації – це самостійно виконане закінчене наукове і теоретико-прикладне дослідження з певної актуальної проблеми, пов'язаної з безпекою інформаційних і комунікаційних систем. Основне її призначення – продемонструвати рівень професійної підготовки випускника і його вміння вирішувати конкретні теоретичні та науково-практичні завдання. Захист магістерської роботи здійснюється у ході відкритого публічного захисту перед екзаменаційною комісією, за результатами якого ухвалюється рішення про присудження здобувачеві ступеня вищої освіти магістра.
Етапи підготовки до проведення атестації, порядок створення екзаменаційної комісії, обов'язки голови, членів та секретаря ЕК, організацію і порядок проведення роботи ЕК, підведення підсумків роботи ЕК регламентує Положення про порядок створення та організацію роботи ЕК (https://cutt.ly/8eWdjJCD).
Тестування у формі ЄДКІ для здобувачів ступеня вищої освіти «магістр» за спеціальністю 125.

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

Процедура проведення контрольних заходів за ОП регулюється Положенням про організацію освітнього процесу (https://cutt.ly/yeWdgZG4), яке розміщене на сайті Університету.
Доступність форм контрольних заходів і критеріїв їх оцінювання для учасників освітнього процесу досягається відображенням в РПНД, які розміщені на сторінці кафедри інформаційної та кібернетичної безпеки ім. професора Володимира Бурячка (ІКБ) (https://tinyurl.com/59n7rem8).
На сторінці ФІТМ в рубриці «Студентам» оприлюднюються графік освітнього процесу (https://tinyurl.com/ydy3pyyw), розклад занять (https://fitm.kubg.edu.ua/informatsiya/studentam/rozklad.html).
За місяць до проведення семестрового контролю на сайті Факультету розміщуються програми іспитів із переліком питань, описом форми проведення та критеріїв оцінювання (https://tinyurl.com/265aw544).
Необхідна інформація щодо процедури проведення контрольних заходів є доступною для усіх учасників освітнього процесу.

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

Об'єктивність екзаменаторів при оцінюванні знань здобувачів у процесі підсумкового семестрового контролю забезпечується проведенням тестових електронних екзаменаційних завдань. Перевірка виконання тестових завдань здійснюється автоматично, без участі викладача, що забезпечує його абсолютну об'єктивність. Рішення про проведення екзамену в усній формі (за необхідності) ухвалює Вчена рада факультету. Захист кваліфікаційної

магістерської роботи проходить перед ЕК за обов'язкової присутності її Голови (Положення про порядок створення та організацію роботи Екзаменаційної комісії; https://cutt.ly/8eWdjJCD).
За період навчання здобувачів на ОП конфлікту інтересів не виникало, скарг на упередженість та необ'єктивність екзаменаторів не було.
Здобувач, який вважає, що на екзамені викладач оцінив відповідь не об'єктивно, у день оголошення оцінки може подати до студентського офісу апеляцію на ім'я декана.

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

Порядок повторного проходження контрольних заходів регулюється п.п. 4.4.3, 7.1.5 «Положення про організацію освітнього процесу…» (https://cutt.ly/yeOi3cBf).
У разі, коли здобувач освіти отримав менше ніж 35 балів за результатами проміжного і підсумкового контролю, він має пройти повторний курс з відповідного ОК, виконати всі види робіт, визначені викладачем відповідно до РПНД.
Здобувачі які сумарно за результатами проміжного та підсумкового контролю набрали від 35 до 59 балів мають право на перескладання екзамену або окремих навчальних завдань проміжного контролю за рішенням викладача, відповідно до РПНД.
Дати повторного проходження контрольних заходів встановлюються ЗВО та відображаються у графіку, що розміщується на сайті Факультету. Перескладання з ОК допускається не більше двох разів. Якщо здобувач вищої освіти не з'явився на перескладання (повторне проходження) підсумкового контролю з певного ОК або отримав за результатами перескладання незадовільну оцінку, він вважається таким, що не виконав індивідуального навчального плану.
За період реалізації ОП був випадок повторного вивчення курсу (F): Білан Д. проходив повторне вивчення ОК «Прикладна загальна теорія систем безпеки» (2024-2025 н.р.). Здобувач успішно пройшов повторний курс.

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

П 4.4.4 «Положення про організацію освітнього процесу…» (https://cutt.ly/yeOi3cBf) визначає процедуру апеляції, на яку має право здобувач у разі, якщо вважає, що викладач оцінив його не об'єктивно. Не пізніше наступного робочого дня від оголошення оцінки здобувач може подати в Студентський офіс апеляцію на ім'я декана Факультету, за розпорядженням якого створюється комісія у складі викладача, який приймав підсумкове оцінювання, іншого викладача відповідного профілю, завідувача кафедри, заступника декана з науково-методичної та навчальної роботи та представника Студентського парламенту. Розгляд апеляції проводиться задля визначення об'єктивності виставленої оцінки. Якщо екзамен був письмовий, то розглядається лише письмова робота. Додаткове опитування здобувача не проводиться. Результати екзаменів, проведених з використанням комп'ютерної техніки, мають бути доступні для проведення апеляції в установлені строки.
Засідання апеляційної комісії відбувається, як правило, наступного робочого дня після отримання заяви здобувача вищої освіти. Підсумкова оцінка, виставлена комісією, є остаточною і апеляції та перескладанню не підлягає.
Прикладів оскарження процедури та результатів проведення контрольних заходів на ОП не було.

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

В Університеті Грінченка політика, стандарти та процедури дотримання академічної доброчесності (АД) відображені у таких документах: Стратегії (програмі) розвитку Університету на 2023-2027 рр. (https://cutt.ly/gwm2Iubp); Кодексі корпоративної культури Київського столичного університету імені Бориса Грінченка (https://cutt.ly/awVqGYkv); Положенні про академічну доброчесність науково-педагогічних, наукових, педагогічних працівників та здобувачів освіти Київського столичного університету імені Бориса Грінченка (https://cutt.ly/ReWdQAzT); наказі про затвердження складу Комісії з академічної доброчесності (https://cutt.ly/VeWdWf4r); Положенні про організацію освітнього процесу (https://cutt.ly/yeWdgZG4).

Які технологічні рішення використовуються на ОП як інструменти протидії порушенням академічної доброчесності? Вкажіть посилання на репозиторій ЗВО, що містить кваліфікаційні роботи здобувачів вищої освіти ОП

Інструментами протидії порушенням АД є такі технологічні рішення:
– підписання НПП та здобувачами на початку навчання Декларації про АД, що є свідченням їх обізнаності з цього питання;
– розроблення та впровадження комп'ютерного тестування здобувачів із автоматичним оцінюванням роботи. За умов змішаного навчання під час контрольних заходів здобувач паралельно із виконанням тестів на платформі Moodle заходить з корпоративного акаунту на відеоконференцію в Google Meet і з увімкненою камерою проходить тестування;
– запровадження процедури обов'язкової технічної перевірки на плагіат кваліфікаційних робіт та підготовлених до друку публікацій, яку безкоштовно здійснює Бібліотека Університету;
– використання для проведення контрольних заходів в аудиторіях, обладнаних відеокамерами, розташування яких дозволяє отримати зображення з усіх кутів огляду, що унеможливлює списування (при офлайн навчанні).
Кваліфікаційні роботи здобувачів освіти завантажуються в Базу кваліфікаційних робіт (з автоматичною перевіркою на плагіат) в системі електронного навчання Університету (Цифровий кампус, https://digital.kubg.edu.ua/).

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

Академічна доброчесність є невід'ємною частиною корпоративної культури Університету. В Кодексі корпоративної культури, п. 3.5, зазначено: «Прийняття та неухильне дотримання принципів академічної доброчесності. Невід'ємною частиною дотримання Кодексу корпоративної культури є підписання працівниками та здобувачами вищої, фахової передвищої освіти Університету Декларації про академічну доброчесність» (https://cutt.ly/awVqGYkv).
Учасників освітнього процесу ознайомлюють з основними принципами Положення про академічну доброчесність науково-педагогічних, наукових, педагогічних працівників та здобувачів освіти Київського столичного університету імені Бориса Грінченка (https://cutt.ly/ReWdQAzT).
Популяризація АД серед здобувачів здійснюється через:
– веб портал ФІТМ (https://tinyurl.com/4cv3edv9)
– Методичні рекомендації до підготовки кваліфікаційних магістерських робіт для здобувачів освітньої програми (https://tinyurl.com/5yjfft62);
– проведення заходів для пояснення процедури підготовки кваліфікаційних робот до захисту та їх перевірку на плагіат;
– проведення заходів для здобувачів та працівників ФІТМ (https://tinyurl.com/d532tj3j).
У структурі Наукового товариства Університету діє Школа академічної доброчесності (https://tinyurl.com/5pada4fh), яка має на меті популяризувати ідеї, норми та цінності академічної доброчесності серед здобувачів вищої освіти, аспірантів, докторантів.

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

Положення про академічну доброчесність науково-педагогічних, наукових, педагогічних працівників та здобувачів освіти, розділ V (https://cutt.ly/ReWdQAzT) передбачає такі види відповідальності:
- щодо здобувачів освіти: попередження; повторне проходження оцінювання (проміжного та підсумкового контролю); повторне проходження відповідного освітнього компонента освітньої (освітньо-професійної, освітньо-наукової) програми; відрахування з Університету; відмова у призначенні академічної стипендії; та ін.
- щодо НПП: попередження; відмова у присудженні наукового ступеня чи присвоєнні вченого звання; – позбавлення присудженого наукового ступеня чи присвоєного вченого звання; позбавлення права брати участь у роботі визначених законом органів (зокрема вчених рад факультетів/інституту/Університету; спеціалізованих вчених рад Університету) чи займати визначені законом посади; позбавлення можливості здійснювати наукове керівництво аспірантами / наукове консультування докторантів; позбавлення можливості викладати дисципліни навчального плану підготовки докторів філософії.

6. Людські ресурси

Продемонструйте, що викладачі, залучені до реалізації освітньої програми, з огляду на їх кваліфікацію та/або професійний досвід спроможні забезпечити освітні компоненти, які вони реалізують у межах освітньої програми, з урахуванням вимог щодо викладачів, визначених законодавством

Реалізацію ОП, а саме викладання обов'язкових та вибіркових освітніх компонентів (ОК), забезпечують НПП кафедри інформаційної та кібернетичної безпеки імені професора Володимира Бурячка (ФІМТ) і кафедри англійської мови та комунікації (Ф-т романо-германської філології).
Підбір викладацького складу здійснюється з урахуванням Ліцензійних умов провадження освітньої діяльності (https://tinyurl.com/5n7h39zp).
Викладання обов'язкових ОК забезпечують 7 НПП, всі – доктори наук, кандидати наук/доктори філософії за профілем відповідних ОК. НПП мають публікації у виданнях, включених до баз даних Scopus та WoS, а саме Соколов В.Ю., Складанний, П.М., Козачок В.А., Аносов А.О., Жданова Ю.Д.,
Махачашвілі Р.К. За період провадження ОП всі НПП пройшли відповідні профілю кафедри та ОК підвищення кваліфікації. Соколов В.Ю., Складанний П.М., Аносов А.О. здійснили успішне керівництво здобувачами на здобуття ступеня доктора філософії, є членами ред. колегій фахового видання, беруть участь у роботі разових спеціалізованих вчених рад, а також є виконавцями наукової теми кафедри ІКБ «Методи та моделі забезпечення кібербезпеки інформаційних систем переробки інформації та функціональної безпеки програмно-технічних комплексів управління критичної інфраструктури» (реєстраційний номер 0122U200483, термін виконання: 2022-2027р.) (https://tinyurl.com/2hhp7j3y).
Детальна інформація про кадрове забезпечення освітнього процесу за ОПП висвітлена в таблиці 2 до ВСО.

Продемонструйте, що процедури конкурсного відбору викладачів є прозорими, недискримінаційними, дають можливість забезпечити потрібний рівень їхнього професіоналізму для успішної реалізації освітньої програми та послідовно застосовуються

Проведення конкурсного відбору на заміщення вакантних посад НПП і укладання з ними контрактів відбувається відповідно до Положення про конкурс на заміщення вакантних посад науково-педагогічних, педагогічних і наукових працівників (https://cutt.ly/9eWdWLDq)
Конкурсний відбір проводиться на засадах відкритості, обґрунтованості й об'єктивності ухвалення рішень. Для нових НПП на ФІТМ запроваджена практика проведення відкритих занять, яке відвідують завідувач кафедри та інші НПП, після чого відбувається обговорення на засіданні кафедри. За результатами обговорення складається відгук про проведене заняття. На кожного з претендентів укладається мотивований висновок про його професійні й особистісні

якості. Рішення щодо рекомендації/не рекомендації кандидатур на відповідні посади приймаються кафедрою шляхом таємного голосування.
При ухваленні рішення береться до уваги результат щорічного конкурсу «Лідер року» (https://cutt.ly/4eWdE0B8) та щорічна оцінка діяльності викладача здобувачами освіти, яка визначається в результаті опитування «Викладач очима студентів». НПП ОПП традиційно мають високі оцінки. Мотивований висновок кафедри та відповідні рекомендації передаються на розгляд вченої ради ФІТМ.

Опишіть, із посиланням на конкретні приклади, яким чином заклад вищої освіти залучає роботодавців, їх організації, професіоналів-практиків та експертів галузі до реалізації освітнього процесу

На Факультеті діє Рада роботодавців (https://tinyurl.com/yrd686zk), створена згідно з Положенням про Раду роботодавців Університету (https://cutt.ly/ReWdfzFw), яка в межах своєї діяльності долучається до обговорення ОП. Представники роботодавців обов'язково залучаються до робочих груп, які розробляють ОП. Членом робочої групи, відповідальної за розробку та впровадження цієї ОП був представник роботодавців В. Єрмошин, начальник департаменту інформаційної безпеки НЕК «Укренерго».
Представники роботодавців також обов'язково входять до складу ЕК (п. 2.5 Положення про порядок створення та організацію роботи Екзаменаційної комісії, https://cutt.ly/8eWdjJCD).
Роботодавці залучаються до процесу організації та проведення практики. Зокрема для реалізації ОП заключено договори з такими базами практики: Департамент інформаційно-комунікаційних технологій виконавчого органу Київської міської ради, Департамент кіберполіції Національної поліції України, Національна енергетична компанія «Укренерго».
Професіонали-практики (https://tinyurl.com/35s6av9v) та експерти галузі залучені до реалізації ОП через проведення гостьових лекцій та майстер-класів (https://tinyurl.com/2n4s2k66).

Яким чином ЗВО сприяє професійному розвиткові викладачів ОП? Наведіть конкретні приклади такого сприяння

Підвищення кваліфікації в Ун-ті регулюється Положенням про підвищення кваліфікації НПП (https://cutt.ly/veWdEqxo), згідно з яким система підвищення кваліфікації НПП складається з обов'язкової та варіативної частин.
Обов'язкова частина спрямована на розвиток ключових компетентностей НПП: фахової, дидактичної, дослідницької, лідерської, цифрової. Варіативна частина передбачає удосконалення та/або набуття інших компетентностей.
Фахове стажування НПП проходять в інших ЗВО, наукових установах в Україні та/або закордоном. Зокрема всі викладачі кафедри ІКБ пройшли фахове стажування в інститутах Національної академії наук відповідно до освітніх компонентів.
Систему внутрішнього підвищ. кваліфікації НПП координує ННЦ розвитку персоналу та лідерства (https://tinyurl.com/kubg-esc-lead) (зокрема, забезпечує підвищ. кваліф. за дидакт., дослідн., лідерським та цифровим модулями),
Для НПП відкритий доступ до НМБД Scopus і Web of Science, є можливість публікації статей у фахових виданнях Ун-ту, зокрема, в електронному журналі ФІТМ «Кібербезпека: освіта, наука, техніка» (https://csecurity.kubg.edu.ua/index.php/journal).
Моніторинг проф. рівня відбувається за допомогою щорічного рейтингового оцінювання «Лідер року», яке містить перелік всіх проф. здобутків НПП за рік та знаходиться у відкритому доступі.

Наведіть конкретні приклади заохочення розвитку викладацької майстерності

В Стратегії розвитку Університету (https://cutt.ly/gwm2Iubp) одним із завдань кадрової політики є заохочення працівників до професійного й особистісного розвитку. Система заохочення НПП регламентується Колективним договором (https://cutt.ly/ZeEj3umY), Положенням про щорічне рейтингове оцінювання проф. діяльності НПП, НП «Лідер року» (https://cutt.ly/4eWdE0B8). Рейтингові показники щороку переглядаються, результати рейтингу використовуються для матеріального та морального заохочення викладачів. Інформацію про діяльність викладача містить «Е-портфоліо» (http://eportfolio.kubg.edu.ua/), вільний доступ до якого сприяє прозорості та об'єктивності оцінки. В Університеті діє Положення про преміювання працівників та надання матеріальної допомоги (https://cutt.ly/yeWdFB1u), а також Порядок преміювання працівників за публікації у Scopus та WoS (https://cutt.ly/feWdGZC1).
Є Положення про відзнаки (https://cutt.ly/2eWdFh8R), в якому передбачено заохочення: оголошення подяки, нагородження грамотою, медаллю Бориса Грінченка (різні рівні), нагрудним знаком «За служіння Університету». У випадках та в порядку, передбаченому законодавством України, працівники можуть представлятись до відзначення державними і відомчими нагородами
З 2022 р. кафедра визнається переможцем у конкурсі «Лідер року» (https://eportfolio.kubg.edu.ua/rating-subdepartments), викладачі Складанний П., Соколов В., Коршун Н., Гулак Г. займають призові місця серед усіх НПП Університету (https://eportfolio.kubg.edu.ua/rating).

7. Освітнє середовище та матеріальні ресурси

Продемонструйте, яким чином навчально-методичне забезпечення, фінансові та матеріально-

технічні ресурси (програмне забезпечення, обладнання, бібліотека, інша інфраструктура тощо) ОП забезпечують досягнення визначених ОП мети та програмних результатів навчання

Освітній процес за ОП здійснюється в корпусі № 1 за адресою вул. Левка Лук'яненка, буд. 13-Б). Аудиторії корпусу обладнані мультимедійними комплексами, необхідним ПЗ і доступом до інтернету, проєкторами та мультимедійними дошками, також для здобувачів є комп'ютерні класи. Практичні заняття здобувачів ОП проходять у Центрах компетенцій: Кіберполігон (https://tinyurl.com/ywzepjnc), у складі 3 лабораторій: безпеки інформаційних активів, антивірусного захисту інформації, систем технічного та криптографічного захисту інформації, а також центрі живої математики (https://fitm.kubg.edu.ua/?Itemid=2097), лабораторії комп'ютерних систем (https://tinyurl.com/2u8shem8), лабораторії вбудованих систем і 3D моделювання (https://tinyurl.com/mtecry7m) та центрі моделювання і програмування (https://tinyurl.com/53k4cwu7).
Університет є учасником ініціативи «Wi-Fi в укриттях», яка започаткована МЦТ та МОН України, має сучасне мережеве обладнання (https://cutt.ly/oeEkPKVz); за програмою Громадського бюджету м. Києва (https://cutt.ly/QeEkAbAH) обладнано Цифровий хаб (https://cutt.ly/PeEkDqHQ).
Для досягнення визначених ОП цілей та РН працює бібліотека, фонди й інформаційні сервіси якої доступні всім здобувачам; також є доступ до НМБД Scopus та WoS, ресурсів SpringerRink, Libraria, ScienceDirect. В університеті функціонує система дистанційного навчання Moodle (https://elearning.kubg.edu.ua/) з ЕНК.
Здобувачам доступна інформація щодо навчально-методичних матеріалів (вебсайт кафедри, в ЕНК дисциплін).

Продемонструйте, яким чином заклад вищої освіти забезпечує доступ викладачів і здобувачів вищої освіти до відповідної інфраструктури та інформаційних ресурсів, потрібних для навчання, викладацької та/або наукової діяльності в межах освітньої програми, відповідно до законодавства

Університет забезпечує учасників освітнього процесу доступом до всіх інформаційних ресурсів. Зокрема в ЗВО діє Цифровий кампус (https://digital.kubg.edu.ua/), в якому об'єднано ресурси з цифрової освіти, науки, управління тощо, а саме: електронна система дистанційного навчання (Moodle) (https://elearning.kubg.edu.ua/), електронний репозиторій (https://elibrary.kubg.edu.ua/), Wiki-портал (http://wiki.kubg.edu.ua/), сервіси Google, зокрема, корпоративна пошта на платформі Gmail (https://cutt.ly/qeEkJ8GX), хмарні сервіси Microsoft (https://ms.kubg.edu.ua/), сервіси Бібліотеки (https://library.kubg.edu.ua/) тощо.
До послуг здобувачів і викладачів працюють актова зала, спортивний комплекс (https://cutt.ly/leEkBzYs), творчі студії та гуртки (https://cutt.ly/UeEkNEpg), їдальня, буфет, медпункт; місця для відпочинку та культурного дозвілля здобувачів, гуртожитки (https://cutt.ly/AeEkNotE). Проводяться регулярні зустрічі зі студпарламентом (https://cutt.ly/keEk1hdw); профспілкою (https://cutt.ly/leEk16XC) для виявлення та врахування потреб й інтересів здобувачів.
Здобувачі мають право на публікацію своїх статей у наукових виданнях ЗВО відповідно до Порядку рекомендації до друку (безкоштовного) статей студентів/магістрантів у виданнях Ун-ту (https://tinyurl.com/3sb5sx5w).

Опишіть, яким чином освітнє середовище надає можливість задовольнити потреби та інтереси здобувачів вищої освіти, які навчаються за освітньою програмою, та є безпечним для їх життя, фізичного та ментального здоров'я

Безпеці та інклюзивному середовищу для всіх учасників освітнього процесу присвячений Розд.10 Стратегії розвитку Ун-ту (https://cutt.ly/gwm2Iubp). Безпечне освітнє середовище формується в ун-ті через дотримання норм техніки безпеки, системне інструктування здобувачів та НПП, пропагування здорового способу життя. Згідно Положення (https://tinyurl.com/bezp-osvita) в ун-ті регулярно проводяться навчання та інструктажі з охорони праці та безпеки життєдіяльності. Безпека всіх учасників освітнього процесу забезпечується відповідними нормативними документами Ун-ту: Про роботу найпростіших укриттів Ун-ту під час повітряної тривоги (https://cutt.ly/xeWdZzKX) та ін.(https://cutt.ly/seElyThM).
Корпус №1, в якому здійснюється підготовка здобувачів за ОП, обладнаний контрольно-пропускною системою, системою протипожежної безпеки, відеокамерами, системою зовн. блискавковідводу і заземлення, укриттям. Укриття Ун-ту були додатково обладнані, перевірені (Акт Комісії Оболонської РДА у м. Києві, 08.11.2023 р.).
Кожен учасник освітнього процесу за ОП має можливість звернутися до Соц.-психол. служби Ун-ту (https://cutt.ly/teElisJq), Ресурсного центру підтримки студентів з інвалідністю (https://cutt.ly/wwm2DVqr); звернутися до керівництва, гаранта ОП через корпоративну ел.пошту чи особисто; повідомити про корупцію, дискримінацію, сексуальні домагання тощо через сервіси Цифрового кампусу (https://tinyurl.com/yas6c962); повідомити про проблеми через анонімний сервіс «Кажи як є» (https://cutt.ly/CeEkVmRy).

Опишіть, яким чином заклад вищої освіти забезпечує освітню, організаційну, інформаційну, консультативну та соціальну підтримку, підтримку фізичного та ментального здоров'я здобувачів вищої освіти, які навчаються за освітньою програмою.

В Ун-ті працює єдина система інформування, яка охоплює освітню, організаційну, інформаційну, консультативну та соціальну підтримку здобувачів і працівників. Документи щодо різних видів підтримки здобувачів освіти та працівників доступні в розділі «Реєстр нормативної бази» https://cutt.ly/nwVqSChc. Положення про правила призначення і виплати стипендій (https://cutt.ly/KeWdbxqS); Положення про стипендіальну комісію (https://cutt.ly/oeWdv1he), Перелік показників та балів у рейтингу успішності здобувачів за участь у науковій, науково-технічній, творчій, спортивній діяльності, громадському житті (https://cutt.ly/qeWdnz6Z); Положення про переведення здобувачів на вакантні місця регіонального замовлення (https://cutt.ly/3eWdboJY), Положення про організацію фізичного виховання і масового спорту (https://tinyurl.com/4rebstds).
В університеті створений Цифровий кампус (https://digital.kubg.edu.ua/) для інформаційної підтримки та комунікації НПП і здобувачів ОП. Доступ до цифрового кампусу здійснюється з корпоративного акаунта.
Основними джерелами інформування щодо організації освітнього процесу є Студентський офіс

(https://tinyurl.com/studentskyi-ofis), гарант ОП, керівництво кафедри, факультету. Інформація для здобувачів про організацію та зміст освітнього процесу розміщена у розділі «Студентам».
Упродовж освітнього процесу спілкування зі здобувачами здійснюється очно на зустрічах, онлайн через електронне листування, на платформах Google Meet, Moodle, Zoom тощо.
Здобувачі ОП своєчасно отримують інформацію про конференції, проєкти, стажування, соціально-гуманітарні заходи через сайт Ун-ту, факультету, кафедри.
Різноманітні послуги можна отримати в Бібліотеці Ун-ту: тематичний підбір літератури, редагування списків літератури, електронна доставка документів тощо (https://library.kubg.edu.ua/).
Усі студенти ОП, які потребували поселення, отримали місце в гуртожитках. За погодженням із Департаментом освіти і науки КМДА здобувачі, що належать до пільгових соціальних категорій, можуть бути переведені на навчання за кошти регіонального бюджету та отримувати соціальну або академічну стипендію.
В Ун-ті й на факультеті ведеться робота з працевлаштування здобувачів і випускників: створено рубрики «Випускникам» (https://cutt.ly/reElckiS) та «Працевлаштування для студентів і випускників» (https://tinyurl.com/3n2y2zm6).
Інформування здобувачів здійснюється через вебсайти кафедри, факультету та Ун-ту. Гарант ОП комунікує зі здобувачами через корпоративну пошту або через загальнодоступні месенджери.

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)

Університет приділяє значну увагу реалізації права на освіту особам з особливими освітніми потребами. У корпусі № 1 за адресою вул. Левка Лук'яненка, 13-Б, де навчаються здобувачі ОП, обладнано безбар'єрний простір: пандуси, горизонтальна платформа з похилим підйомом, два ліфти. Сайт Університету та електронна навчальна платформа Moodle також налаштовані для людей з особливими освітніми потребами (з порушенням зору). Ресурсний центр підтримки студентів з інвалідністю (https://cutt.ly/wwm2DVqr) працює на реалізацію права на освіту здобувачів з особливими потребами.
У розділі VIII Правил прийому зафіксовано спеціальні умови зарахування на навчання осіб із інвалідністю (https://tinyurl.com/53rp6jmn). Заступники деканів з науково-методичної та навчальної роботи і науково-педагогічної та соціально-гуманітарної роботи регулярно беруть участь у семінарах, присвячених організації супроводу здобувачів із числа пільгових категорій та осіб з особливими освітніми потребами (https://cutt.ly/5wBiIKr7).
Серед здобувачів вищої освіти ОП, що акредитується, наразі немає осіб із особливими освітніми потребами.

Продемонструйте наявність унормованих антикорупційних політик, процедур реагування на випадки цькування, дискримінації, сексуального домагання, інших конфліктних ситуацій, які є доступними для всіх учасників освітнього процесу та яких послідовно дотримуються під час реалізації освітньої програми

Політика та процедури врегулювання конфліктних ситуацій регулюються Положенням про засади запобігання і протидії дискримінації, сексуальним домаганням, булінгу, мобінгу та іншим проявам неетичної поведінки в Ун-ті https://cutt.ly/HeWdmjJg, яке розроблено з метою забезпечення рівних можливостей щодо реалізації прав і свобод усіх співробітників та здобувачів освіти, підтримання в ЗВО середовища, вільного від дискримінації, сексуальних домагань, булінгу, мобінгу, принижень честі та гідності особи. В зазначеному Положенні описані: обов'язки співробітників і здобувачів освіти; процедура повідомлення про дискримінацію, сексуальні домагання, булінг, мобінг та інші прояви неетичної поведінки; процедура розгляду скарг.
Розгляд відповідних скарг здійснюється Комісією з етики (https://cutt.ly/9eWdmHEt), персональний склад та строк повноважень якої затверджується згідно з наказом ректора. Скарги, які подані здобувачами освіти та стосовно здобувачів освіти, розглядаються розширеним складом Комісії з етики за участю представників з-поміж здобувачів освіти. Доступність політик і процедур щодо врегулювання конфліктних ситуацій (включаючи випадки дискримінації, сексуальних домагань або корупції) забезпечується за рахунок розміщення інформації щодо основних заходів запобігання та способів сповіщення про такі ситуації на сайті ЗВО. Так, на веб-сторінці сайту ЗВО «Протидія дискримінація» є рубрика «Повідомлення про дискримінацію, сексуальні домагання тощо» (https://cutt.ly/rwZZNuVq), яка дозволяє будь-кому з учасників освіт. процесу повідомити про факти дискримінації, сексуальні домагання, булінг та інші прояви неетичної поведінки, надіславши відповідні матеріали на електронну скриньку Комісії з етики.
У питаннях протидії корупції ЗВО керується Законом України «Про запобігання корупції». На сайті Університету (https://cutt.ly/sUvbTQG) розміщена інформація щодо основних заходів, спрямованих на запобігання, виявлення та протидії корупції. До відома співробітників і здобувачів освіти доведена інформація щодо способу повідомлення про прояви корупції в Університеті, затверджено реєстр корупційних ризиків Університету (https://cutt.ly/EwXw0xsz). Повноваження щодо питань запобігання та виявлення корупції покладені на помічника ректора з правових та кадрових питань https://cutt.ly/UeWdQibF). Університет був учасником проєкту «Антикорупційний комплаєнс у вищій освіті: закордонний досвід і національна практика», в рамках якого робоча група Університету, за підтримки експертів, провела оцінювання корупційних ризиків (https://cutt.ly/1wXw2lLl) та розробила антикорупційну програму Університету (https://cutt.ly/HwZZU5pj).
Під час реалізації ОП, що акредитується, скарг, пов'язаних із випадками дискримінації, сексуальних домагань, інших конфліктних ситуацій, корупції, не було.

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 на своєму вебсайті

Порядок розроблення, реалізації, перегляду, оновлення та припинення освітніх програм визначені в Положенні про освітні програми в Київському столичному університеті імені Бориса Грінченка), затвердженому рішенням Вченої ради Університету від 26 грудня 2024 року (протокол №15) та введеному в дію наказом від 26.12.2024 №986 (https://tinyurl.com/5ttey9rk). Положення оприлюднене в рубриці «Ресурси. Реєстр нормативної бази» (https://cutt.ly/nwVqSChc).
До затвердження цього Положення зазначені процедури регулювалися Методичними рекомендаціями з розроблення та оновлення освітніх програм (https://tinyurl.com/kubg-rozrobka-op). Методичні рекомендації розміщені в рубриці «Ресурси. Архів нормативної бази» (https://tinyurl.com/kubg-norm)

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

Моніторинг ОП є важливою складовою системи внутрішнього забезпечення якості вищої освіти Університету. Перегляд ОП, що акредитується, було здійснено у 2021 р. у зв'язку з затвердженням Стандарту вищої освіти України за спеціальністю 125 «Кібербзепека» галузі знань 12 «Інформаційні технології». Ці зміни були також спрямовані на забезпечення результативності формування компетентностей, визначених ОП, більш повне врахування запитів роботодавців і потреб здобувачів вищої освіти. Результатом змін, внесених в ОП, стало прийняття нової редакції (рішення Вченої ради Університету від 17 червня 2021 р., протокол № 6).
Далі відбувався щорічний перегляд ОП, результатом якого було оновлення РПНД, програм практик.
Під час реалізації ОП були отримані відгуки від стейкголдерів. З урахуванням рекомендацій та керуючись Змінами до переліку галузей знань та спеціальностей, за якими здійснюється підготовка здобувачів вищої освіти (затверджені Постановою КМУ від 16.12.2022 № 1392) та за результатами останнього перегляду у 2024 році до ОП було внесено зміни (рішення Вченої ради ФІТМ від 27 серпня 2024 р., протокол №9). Так, в змінах ОП 2024 було уточнено назви ОК «Технології розслідування інцидентів безпеки» на «Технології розслідування інцидентів безпеки критичної інфраструктури» та «Технології безпеки безпроводових і мобільних мереж» на «Технології безпеки та управління критичними інфраструктурами», а також додано загальну компетентність ЗК-11 «Розуміти, виконувати та дотримуватися принципів академічної доброчесності, зокрема, усвідомлювати важливість інтелектуальної чесності у всіх видах навчальної та дослідницької роботи, дотримуватися правил і обмежень, пов'язаних з плагіатом, шахрайством, підробкою даних та іншими формами недопустимої поведінки».

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

При перегляді змісту ОПП беруться до уваги зауваження здобувачів щодо трансформації елементів ОП. Наприкінці навчального року на засіданні кафедри аналізується успішність та інтерес здобувачів до різних дисциплін, встановлюються причини різного рівня мотивації до вивчення окремих предметів, враховуючи рівень викладання, відповідність змісту дисциплін тощо.
Здобувачі можуть висловити свої зауваження та побажання і під час освітнього процесу (на заняттях, звітуючи про проходження виробничої, науково-дослідної та переддипломної практики). На сторінці Факультету є можливість долучитися до обговорення проєктів змін або нових редакцій ОП, розміщених у рубриці «Форма для пропозицій та зауважень до проєктів Освітніх програм» (https://tinyurl.com/4d2dvcrb).
Крім того, в Університеті діє практика залучення здобувачів освіти до участі в робочих групах з розроблення та внесення змін до ОП.
Думка здобувачів щодо якості викладання на усіх ОП університету вивчається шляхом проведення щорічного анонімного електронного анкетування «Викладач очима студентів».

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

Відповідно до статуту Університету (https://cutt.ly/gwVqFbEi), Положення про ФІТМ (https://tinyurl.com/ry2yc3fp), Положення про студентське самоврядування в Ун-ті (https://cutt.ly/GeWdzpNX) представники студентського самоврядування беруть активну участь у обговоренні та вирішенні питань щодо науково-дослідної роботи, удосконаленні якості освітнього процесу, участі у стипендіальних комісіях, долучаються до організації дозвілля, оздоровлення, побуту і харчування; за їх участі вносяться пропозиції щодо змісту навчальних планів і ОП. Представники студентського самоврядування є членами робочих груп, наукових товариств, Вчених рад Університету та факультетів.
Під час розробки та реалізації ОП зауважень із боку студентської спільноти, а також органів студентського самоврядування не було.

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

Для Університету Грінченка зв'язок із роботодавцями, систематичний моніторинг ринку праці є пріоритетним напрямом. Задля забезпечення високої якості підготовки фахівців було розроблено Положення про Ради

роботодавців Київського столичного університету імені Бориса Грінченка (https://cutt.ly/ReWdfzFw).
У складі робочої групи, відповідальної за розробку та впровадження ОП, був представник роботодавців В. Єрмошин, начальник департаменту інформаційної безпеки НЕК «Укренерго». Він також є членом Ради роботодавців ФІТМ (https://fitm.kubg.edu.ua/informatsiya/s/souncil-of-employers/sklad.html).
Зворотний зв'язок від роботодавців підтримується у формі формальних (характеристика, що дається практикантам) та неформальних відгуків керівників баз практик.

Опишіть практику збирання, аналізу та врахування інформації щодо кар'єрного шляху та траєкторій працевлаштування випускників ОП (зазначте в разі проходження акредитації вперше)

МЦ стандартизації та якості освіти (відділ практики і працевлаштування) координує моніторинг інформації щодо працевлаштування випускників: здійснює контроль і підбиття підсумків працевлаштування; готує статистичну інформацію, яка аналізується на засіданнях Вченої ради Ун-ту та фахівцями Департаменту освіти і науки КМДА. На сайті Ун-ту створена рубрика «Випускникам», де, зокрема, розміщені «Анкета для сприяння працевлаштуванню», «Анкета випускника Університету Грінченка», «Вакансії для студентів і випускників» https://kubg.edu.ua/informatsiya/klub-vipusknikiv/oholoshennia.html).
На ФІТМ з метою посилення впливу випускників Ун-ту на якість підготовки фахівців створено Раду випускників, яка є дорадчо-консультативним органом та учасником системи внутрішнього забезпечення якості освітнього процесу в Університеті (https://fitm.kubg.edu.ua/informatsiya/s/souncil-of-employers.html).
На сторінці ФІТМ створена рубрика «Історії успіху випускників», де висвітлено їх досягнення та професійні здобутки (https://fitm.kubg.edu.ua/informatsiya/vipusknikam/istoriji-uspikhu-vipusknikiv.html).

Продемонструйте, що система забезпечення якості закладу вищої освіти забезпечує вчасне реагування на результати моніторингу освітньої програми та/або освітньої діяльності з реалізації освітньої програми, зокрема здійсненого через опитування заінтересованих сторін

З метою реалізації процедур внутрішнього забезпечення якості ОПП було проведено:
– самоаналіз реалізації ОП;
– аналіз успішності та якості знань здобувачів за результатами екзаменаційних сесій;
– анкетування здобувачів «Викладач очима студентів» (щорічно);
– опитування здобувачів ОП ФІТМ щодо задоволеності якістю навчання;
– опитування науково-педагогічних працівників, які викладають на ОП;
– перегляд і оновлення робочих програм навчальних дисциплін і робочих програм практик із обов'язковим їх обговоренням і затвердженням на засіданні кафедри;
– систематичне підвищення кваліфікації НПП, зокрема за останні 5 років співробітниками кафедри було захищено 1 докторську (Гулак Г.) та 4 кандидатські дисертації (Складанний П., Соколов В., Платоненко А., Ворохоб М.);
– оновлення складу НПП, зокрема кафедра поповнилась випускником-практиком Ворохобом М.В., залучено молодих фахівців Костюк Ю та Бебешко Б.
У ході здійснення процедур внутрішнього забезпечення якості освіти за час реалізації ОП суттєвих недоліків не виявлено. Моніторинг різних аспектів освітнього процесу за ОП виявив високий рівень задоволеності здобувачів. Освітній процес на ОП здійснюється на засадах компетентнісного, системного, інтегративного підходів із застосуванням інноваційних, інтерактивних технологій, елементів дистанційного навчання, виконання проєктів, тощо. У зв'язку з карантинними обмеженнями, спричиненими пандемією Covid-19 та воєнним станом була надана можливість здобувачам проходити практику онлайн (підбір баз практик з такою можливістю), адаптовано завдання в програмах практик, а також здійснено відповідне наповнення ЕНК на платформі Moodle

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

Звіти експертних груп та висновки галузевих експертних рад Національного агентства із забезпечення якості вищої освіти (далі – НА) завжди аналізуються та обговорюються на засіданнях відповідних кафедр, ВРФ, ректорату; плануються заходи з врахування зроблених зауважень.
В реалізації цієї ОПП були враховані рекомендації експертів, зроблені за результатами попередньої акредитації, зокрема щодо роз'яснення здобувачам можливостей здобуття освіти у неформальній та інформальній освіті. Створено окрему рубрику на сайті факультету «Неформальна/ інформальна освіта»(https://tinyurl.com/37suywfw), розроблений та затверджений «Порядок визнання та перезарахування результатів навчання в КСУБГ» (Додаток до Положення про організацією освітнього процесу в КСУБГ (https://cutt.ly/yeWdgZG4).
Також проведена значна профорієнтаційна робота щодо залучення до навчання іноземних студентів. У 2021 році освітній ступінь магістра отримав громадянин Єгипту Мохамед Абдельмаксуд. Також на ОП проходив навчання громадянин Китаю Ши Цзінсянь, але через широкомасштабну війну вимушений був залишити навчання.
З метою забезпечення високої якості підготовки здобувачів та системного залучення стейкголдерів до обговорення змісту та різних питань реалізації ОП на кожному факультеті були створені Ради роботодавців та Ради випускників. Врахована рекомендація експертів включати здобувачів освіти до складу робочих груп з розроблення та оновлення ОП. До складу робочої групи з оновлення ОП у 2024 році було включено здобувача освіти Леонід Подріза та випускницю Діану Цирканюк.
ЗВО проводить заходи для підвищення кваліфікації гарантів, які дають можливість гарантам ознайомитись та врахувати рекомендації експертів НА, що були зроблені при акредитації різних ОП Університету. Зокрема: 21.10.2021 – координаційна нарада гарантів ОП всіх рівнів вищої освіти щодо обговорення результатів акредитацій за 2020/2021 н.р.(https://cutt.ly/qUxGRLp); 16.02.2023 - онлайн вебінар для гарантів «Забезпечення якості вищої освіти: погляд експертів Національного агентства із забезпечення якості вищої освіти»

(https://tinyurl.com/ms3t68yy); у лютому 2025 р. – онлайн вебінар «Акредитація ОП: зміни нормативно-правового та організаційного забезпечення» (https://cutt.ly/9rw3VSq4) та навчально-методичні семінари «Акредитація ОП: робота без помилок» (https://cutt.ly/4rw3BcX2 ; https://cutt.ly/Urw3CMJL).

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

Система внутрішнього забезпечення якості вищої освіти відображена у Положенні про організацію освітнього процесу (Розділ ІІ) (https://cutt.ly/yeWdgZG4). Важливим чинником змістовності залучення до внутрішньої системи забезпечення якості усіх учасників академічної спільноти є Кодекс корпоративної культури ЗВО (https://cutt.ly/awVqGYkv).
Учасники академічної спільноти залучені до:
– розроблення та оновлення ОП та навчальних планів;
– оновлення і вдосконалення навчально-методичного забезпечення;
– обговорень дотичних питань на Вченій раді Університету, на вченій раді ФІТМ, на засіданнях кафедр, під час проведення занять, а також у ході неформальних комунікацій;
– систематично підвищують власний проф. рівень, педагог. майстерність та наук кваліфікацію;
– дотримуються норм академічної доброчесності.
Якість ОПП є предметом постійного моніторингу гаранта та групи забезпечення ОПП (засобами: анкетування, усного опитування, бесід з акад. групою), результати якого обговорюються на засіданнях кафедри та враховуються для удосконалення ОПП.

Продемонструйте, що в академічній спільноті закладу вищої освіти формується культура якості освіти

Університет послідовно і системно формує та забезпечує культуру якості освіти, що знайшло своє відображення у візії ЗВО як столичного університету з розвиненою корпоративною культурою, високими стандартами якості освіти та наукових досліджень, простором для самореалізації кожної особистості, діяльність якого спрямована на відповідальне служіння людині, територіальній громаді міста Києва, Україні (https://cutt.ly/gwm2Iubp). Засадничим принципом Стратегії розвитку Університету є спрямованість на світові стандарти якості освіти, а стратегічною ціллю – забезпечення високої якості освіти, що передбачає підготовку фахівців за актуальними, потрібними суспільству програмами, наявність ефективної внутрішньої системи забезпечення якості ВО,
реалізацію ОП із залученням роботодавців та міжнародних партнерів.
Культура якості формується через наскрізні процеси забезпечення якості, включаючи планування, практичні заходи, контроль та реагування на виявлені проблеми.
В університеті функціонує Науково-методичний центр стандартизації та якості освіти (https://tinyurl.com/standartyzacii), метою якого є сприяння організації освітнього процесу та його науково-методичному забезпеченню на факультетах та у коледжі Університету відповідно до вимог законодавства, функціонування системи внутрішнього забезпечення якості вищої освіти.

9. Прозорість і публічність

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

Документи, якими регулюються права та обов'язки усіх учасників освітнього процесу, оприлюднюються на вебсайті Університету в Реєстрі нормативної бази (https://cutt.ly/nwVqSChc).
До таких документів відносяться: Статут Університету (https://cutt.ly/gwVqFbEi), Кодекс корпоративної культури (https://cutt.ly/awVqGYkv), Правила внутрішнього розпорядку (https://cutt.ly/gwVwaQG8), Положення про організацію освітнього процесу (https://cutt.ly/yeWdgZG4), Положення про студентське самоврядування (https://cutt.ly/GeWdzpNX), Положення про академічну доброчесність науково-педагогічних, наукових, педагогічних працівників та здобувачів освіти (https://cutt.ly/ReWdQAzT), Положення про кафедру (https://tinyurl.com/2akh4ksa), Положення про ФІТМ (https://tinyurl.com/ry2yc3fp).

Наведіть посилання на вебсторінку, яка містить інформацію про оприлюднення ЗВО відповідного проєкту освітньої програми для отримання зауважень та пропозицій заінтересованих сторін (стейкголдерів).

https://fitm.kubg.edu.ua/informatsiya/obhovorennia-osvitnikh-prohram/druhyi-mahisterskyi-riven-vyshchoi-osvity.html

Наведіть посилання на оприлюднену у відкритому доступі на своєму вебсайті інформацію про освітню програму (освітню програму у повному обсязі, навчальні плани, робочі програми навчальних дисциплін, можливості формування індивідуальної освітньої траєкторії здобувачів вищої освіти) в обсязі, достатньому для інформування відповідних заінтересованих сторін та суспільства

ОПП, НП, РПНД - https://fitm.kubg.edu.ua/struktura1/kafedry/kafedra-informatsiinoi-ta-kibernetychnoi-bezpeky-im-profesora-volodymyra-buriachka/navchalno-metodychna-robota.html#arkhiv-2

Формування ІОТ - https://elearning.kubg.edu.ua/local/gdo/catalog/

11. Перспективи подальшого розвитку ОП

Якими загалом є сильні та слабкі сторони ОП?

Сильні сторони:
– ОП має чітко сформульовані мету та цілі, які відповідають місії та стратегії Університету;
– структура та зміст ОП відповідають потребам і викликам часу, змінам, що відбуваються в галузі кібербезпеки та захисту інформації;
– фокус ОП є актуальним, зважаючи на нагальність потреби підготовки фахівців, здатних працювати в системі забезпечення кібербезпеки приватного та державного сектору;
– ОП є логічно структурованою і збалансованою, що сприяє формуванню професійних компетентностей сучасного фахівця в сфері кібербезпеки; форми та методи навчання і викладання дають можливість досягти заявлених в ОП цілей та РН;
– забезпечення ОП висококваліфікованими НПП, що мають наукові ступені, вчені звання;
– підвищення кваліфікації НПП шляхом стажування в українських та закордонних ЗВО, апробація наукових досліджень на всеукраїнських та міжнародних конференціях;
– сучасна матеріально-технічна база, що дозволяє підтримувати високу якість освітнього процесу;
– чіткість і зрозумілість політики дотримання академічної доброчесності;
– урахування необхідності досягнення глобальних цілей сталого розвитку.

Серед слабких сторін ОП:
– недостатній рівень академічної мобільності здобувачів, що пов'язано з повномасштабною російсько-українською війною;
– невисока публікаційна активність здобувачів у виданнях, що індексуються у наукометричних базах, що пов'язано з орієнтованістю здобувачів на практичні проєкти.

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

Подальші перспективи розвитку ОП вбачаємо у:
– збільшенні кількості майстер-класів професіоналів практиків (у т.ч. дистанційних, зважаючи на умови воєнного стану);
– оновленні та подальшому збільшенні баз практик із потенційними роботодавцями;
– більш тісна взаємодія з випускниками ОП;
– започаткування переліку навчальних дисциплін професійного спрямування на ОП, що викладаються іноземними мовами;
– підвищенні активності здобувачів у науковій діяльності та підвищенні публікаційної активності НПП у виданнях, що входять до наукометричних баз даних Scopus, Web of Science;
– сприяння у працевлаштуванні випускникам ОП;
– удосконаленні ОП відповідно до рекомендацій отриманих під час акредитації.

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: ТУРУНЦЕВ ОЛЕКСАНДР ПЕТРОВИЧ

Дата: 17.03.2025 р.

Таблиця 1. Інформація про освітні компоненти ОП

Назва освітнього компонента	**Вид освітнього 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**	
Математичні методи криптографії	навчальна дисципліна	*Математичні методи криптографії.pdf*	G+BH7AhyUDBno2It7NXVp3Wlq7ZdIpDUeHu5jPCQwOE=	*Центр дослідження технологій захисту інформаційних ресурсів Лабораторія криптографічного захисту інформації у складі:* *Ноутбук тип#1 Dell Inspiron 15/500 Series IntelCore i5-8250u cpu, 1.8 Ghz, 8 Gb ОЗУ – 3 шт.* *Програмно-апаратний комплекс "Центр сертифікації ключів" (виробництва ТОВ «Інститут інформаційних технологій», м.Харків)* *Апаратний криптомодуль "Гряда-61" – 1 шт.* *Електронні ключі Кристал-1 – 15 шт.* *Застосування спеціалізованого обладнання ТОВ «ІІТ» дозволяє студентам Університету будувати захищені IP і TCP мережі та захищені міжмережеві з'єднання, обслуговувати сертифікати відкритих ключів користувачів, опановувати технології надання користувачам засобів ЕЦП та шифрування даних, а також технології управління засобами генерації та ключами (що робить неможливим доступ до особистих ключів з боку зовнішнього програмно-апаратного середовища) тощо. Застосування апаратного криптомодулю "Гряда-61" дозволяє студентам Університету реалізовувати процедури криптоперетворення у складі PCт, тощо.* *Програмно-апаратний комплекс криптографічного захисту IP трафіку CryptoIP (виробництва ТОВ АВТОР, м.Київ).* *Смарт-карта CryptoCard-337 – 6 шт.* *Електронний USB-ключ SecureToken-337 – 6 шт.* *Електронний ключ SecureToken-337F – 6 шт.* *Застосування ПАК CryptoIP дозволяє студентам Університету будувати системи захисту IP- трафіку за ідеологією IPSec (RFC 2401), а також віртуальні конфіденційні мережі (VPN) поверх будь-яких (але зв'язкових) IPv4-мереж. Це забезпечує конфіденційність і цілісність даних, тощо.* *Усі заняття проводяться в аудиторіях, які обладнані мультимедійним комплексом*

				(проєктор, SMART-дошка, комп'ютер з встановленими Microsoft Office та антивірусною програмою ESET Endpoint Security). Під час вивчення дисципліни використовується електронний навчальний курс на платформі дистанційного навчання (Moodle) із включенням додаткових інформаційних ресурсів у відкритому доступі, а також статистичних баз даних і аналітичних звітів міжнародних організацій. Заняття при дистанційному навчанні проводяться з використанням корпоративного Google Meet (Zoom).
Технології протидії злоякісному програмному коду	навчальна дисципліна	*Технології протидії злоякісному програмному коду.pdf*	J+QiHnXCEXRmiCbwc/u2oDtoPhs4v5y1NNxQ9ICKiB8=	*Центр дослідження технологій захисту інформаційних ресурсів* *Контур забезпечення всебічного захисту корпоративної мережі від компанії ESET Enterprise Inspector* *у складі:* *ESET Security Management Center 7;* *ESET Remote Administrator;* *ESET Enterprise Inspector;* *ESET Endpoint Antivirus 7.0.2100.4;* *ESET Security Agent;* *ESET Targeted Attack Protection;* *ESET Mail Security for Microsoft Exchange Server 7.0.10024.0;* *ESET File Security for Microsoft Windows Server 7.0.12018.0.* *Застосування спеціалізованого програмного забезпечення ESET Enterprise Inspector (EEI) дозволяє студентам Університету в режимі реального часу виявляти інциденти підвищеної складності та управляти ними, здійснювати збір даних, виявляти аномалії та ознаки порушення політики безпеки, виявляти загрози «0-доби», захищатися від від цільових APT-атак та програм-вимагачів тощо.* *Контур захисту інформації в хмарних сховищах даних* *від компанії IBM* *у складі* *Security QRadar SIEM;* *Security AppScan;* *Security Network Intrusion Prevention System* *Застосування спеціалізованого програмного забезпечення IBM дозволяє студентам Університету досліджувати технології захисту інформації в хмарних сховищах даних, а саме управляти подіями та інцидентами безпеки (Security QRadar SIEM), моніторити уразливості додатків (Security AppScan) та створювати системи запобігання вторгнень (Security Network Intrusion Prevention System)* *Усі заняття проводяться в аудиторіях, які обладнані мультимедійним комплексом*

				(проєктор, SMART-дошка, комп'ютер з встановленими Microsoft Office та антивірусною програмою ESET Endpoint Security). Під час вивчення дисципліни використовується електронний навчальний курс на платформі дистанційного навчання (Moodle) із включенням додаткових інформаційних ресурсів у відкритому доступі, а також статистичних баз даних і аналітичних звітів міжнародних організацій. Заняття при дистанційному навчанні проводяться з використанням корпоративного Google Meet (Zoom).
Технології розробки і тестування ПЗ мережевої безпеки	навчальна дисципліна	*Технології розробки і тестування ПЗ мережевої безпеки.pdf*	uGTfmZgUz41yJnkpkfD6nE5GftQe963wZvxT5yA2z3g=	*Центр дослідження технологій захисту інформаційних ресурсів* *Контур забезпечення всебічного захисту корпоративної мережі від компанії ESET Enterprise Inspector* *у складі:* *ESET Security Management Center 7;* *ESET Remote Administrator;* *ESET Enterprise Inspector;* *ESET Endpoint Antivirus 7.0.2100.4;* *ESET Security Agent;* *ESET Targeted Attack Protection;* *ESET Mail Security for Microsoft Exchange Server 7.0.10024.0;* *ESET File Security for Microsoft Windows Server 7.0.12018.0.* *Застосування спеціалізованого програмного забезпечення ESET Enterprise Inspector (EEI) дозволяє студентам Університету в режимі реального часу виявляти інциденти підвищеної складності та управляти ними, здійснювати збір даних, виявляти аномалії та ознаки порушення політики безпеки, виявляти загрози «0-доби», захищатися від від цільових APT-атак та програм-вимагачів тощо.* *Контур захисту інформації в хмарних сховищах даних від компанії IBM* *у складі* *Security QRadar SIEM;* *Security AppScan;* *Security Network Intrusion Prevention System* *Застосування спеціалізованого програмного забезпечення IBM дозволяє студентам Університету досліджувати технології захисту інформації в хмарних сховищах даних, а саме управляти подіями та інцидентами безпеки (Security QRadar SIEM), моніторити уразливості додатків (Security AppScan) та створювати системи запобігання вторгнень (Security Network Intrusion Prevention System)* *Усі заняття проводяться в аудиторіях, які обладнані мультимедійним комплексом*

				(проєктор, SMART-дошка, комп'ютер з встановленими Microsoft Office та антивірусною програмою ESET Endpoint Security). Під час вивчення дисципліни використовується електронний навчальний курс на платформі дистанційного навчання (Moodle) із включенням додаткових інформаційних ресурсів у відкритому доступі, а також статистичних баз даних і аналітичних звітів міжнародних організацій. Заняття при дистанційному навчанні проводяться з використанням корпоративного Google Meet (Zoom).
Моніторинг, аудит та адміністрування захищених IT систем і мереж	навчальна дисципліна	*Моніторинг, аудит та адміністрування захищених IT систем і мереж.pdf*	e+2WbfyNlX3APlVlLbewfwIiFx8Ym4nw+iaU/3U6rYA=	*Лабораторія технічного захисту інформації у складі: Детектор (індикатор) поля PROTECT 1210і – 1 шт. Детектор (індикатор) поля PROTECT 1206і – 1 шт. Скануючий приймач IC-R20 – 1 шт. Багатофункціональний пошуковий прилад ST-033 «Піранія» – 1 шт. Виявник прихованих відеокамер – 1 шт. Антена рамкова жорстка "PIAC-1АЖ" – 1 шт. Генератор акустичного шуму "PIAC-2ГС" – 1 шт. Вібровипромінювач п'єзоелектричний "PIAC-2ВП" – 1 шт. Випромінювач акустичний "PIAC-2ВА" – 1 шт. Квадрокоптер DJI Mavic PRO – 1 шт. Контроллер Matrix-II Net – 1 шт.* *Застосування обладнання лабораторії дозволяє студентам Університету отримувати знання щодо виявлення радіозакладних пристроїв, забезпечення захисту об'єктів інформаційної діяльності від витоку конфіденційної інформації акустичними і віброакустичними каналами, а також забезпечення контролю та управління доступом на об'єктах інформаційної діяльності з використанням ПЗ захисту ІзОД від НСД в АС класу "1" (автономна ПЕОМ) та класу "2" (ЛОМ), а саме системи "Лоза", комплексу засобів захисту (КЗЗ) "Гриф", комплексу засобів захисту (КЗЗ) "Рубіж": Система "Лоза" реалізує всі стандартні функції, необхідні для надійного захисту інформації від НСД та побудови комплексної системи захисту інформації (КСЗІ) в АС класу "1" та класу "2", а також може використовуватись для захисту інформації, що становить*

				державну таємницю. *КЗЗ "Гриф" призначений для захисту ІзОД, у тому числі інформації, що становить державну таємницю, конфіденційної інформації, яка є власністю держави, персональних даних та іншої інформації, вимоги до захисту якої встановлені законодавством, при її обробці в АС класу "1".* *КЗЗ "Рубіж" призначений для забезпечення захищеної технології оброблення інформації різних рівнів обмеження доступу в АС класу 1* *Усі заняття проводяться в аудиторіях, які обладнані мультимедійним комплексом (проєктор, SMART-дошка, комп'ютер з встановленими Microsoft Office та антивірусною програмою ESET Endpoint Security). Під час вивчення дисципліни використовується електронний навчальний курс на платформі дистанційного навчання (Moodle) із включенням додаткових інформаційних ресурсів у відкритому доступі, а також статистичних баз даних і аналітичних звітів міжнародних організацій.* *Заняття при дистанційному навчанні проводяться з використанням корпоративного Google Meet (Zoom).*
Підготовка та захист кваліфікаційної магістерської роботи	підсумкова атестація	*Методичні_рекомендації_2024_КБтаЗІ_магістр.pdf*	67wcZskeHjyp0M6wzBQk+7h7Mi+SVKvFeTe2uNoSkjY=	*Під час написання магістерської роботи здобувачі використовують відповідні методичні рекомендації, розміщені на сайті випускової кафедри (https://tinyurl.com/5yjfft62).* *Здобувачі можуть використовувати бібліотечний фонд та ресурси Київського столичного університету імені Бориса Грінченка (https://library.kubg.edu.ua/), Цифрові бібліотеки (https://cutt.ly/ECGaMhL), Інституційний репозиторій (https://cutt.ly/cCGa7Qx).* *Для роботи з науковою літературою надається доступ до ресурсів бібліотеки, наукометричних реферативних міжнародних баз даних Web of Science компанії Clarivate Analytics та Scopus Elsevier,* *Всі магістерські роботи перевіряються на виявлення збігів/ідентичності/схожості в текстах засобами сервісу перевірки на плагіат Strike Plagiarism.* *Захист магістерської роботи здобувача проводиться в аудиторіях, які обладнані мультимедійними комплексами (проєктор, SMART-дошка або екран, комп'ютер, на який встановлено Microsoft Office, веб-переглядачі: Chrome, Mozilla, Opera, а також антивірусна програма ESET Endpoint Security).* *У період карантину/воєнного стану захист відбувається з*

				використанням сервісів відеотелефонного зв'язку: Google Meet, Zoom.
Переддипломна практика	практика	*Переддипломна практика.pdf*	ZZ5a2wNv7m6yfR3+2cW+9kdCMYFBvPULgCL82ETFrRg=	*Практика здійснюється на базах практик (https://tinyurl.com/5ytyjh5y) згідно з укладеними договорами про співпрацю або на підставі листів-клопотань. Використовується матеріально-технічне бази практики.*
Виробнича практика (технологічна)	практика	*Виробнича (технологічна) практика.pdf*	3rgZtLqDXvXTlnq2GCC18zCDN7K4FKUcJIaDwXnKS58=	*Практика здійснюється на базах практик (https://tinyurl.com/5ytyjh5y) згідно з укладеними договорами про співпрацю або на підставі листів-клопотань. Використовується матеріально-технічне бази практики.*
Методи побудови і аналізу криптосистем	навчальна дисципліна	*Методи побудови і аналізу криптосистем.pdf*	nTfu9RX71czB4roMMRCgMx9cJeM8lfcEtjC3EvUyBIk=	*Лабораторія криптографічного захисту інформації у складі:* *Ноутбук тип#1 Dell Inspiron 15/500 Series IntelCore i5-8250u cpu, 1.8 Ghz, 8 Gb ОЗУ – 3 шт.* *Програмно-апаратний комплекс "Центр сертифікації ключів" (виробництва ТОВ «Інститут інформаційних технологій», м.Харків)* *Апаратний криптомодуль "Гряда-61" – 1 шт.* *Електронні ключі Кристал-1 – 15 шт.* *Застосування спеціалізованого обладнання ТОВ «ІІТ» дозволяє студентам Університету будувати захищені IP і TCP мережі та захищені міжмережеві з'єднання, обслуговувати сертифікати відкритих ключів користувачів, опановувати технології надання користувачам засобів ЕЦП та шифрування даних, а також технології управління засобами генерації та ключами (що робить неможливим доступ до особистих ключів з боку зовнішнього програмно-апаратного середовища) тощо.* *Застосування апаратного криптомодулю "Гряда-61" дозволяє студентам Університету реалізовувати процедури криптоперетворення у складі PCт, тощо.* *Програмно-апаратний комплекс криптографічного захисту IP трафіку CryptoIP (виробництва ТОВ АВТОР, м.Київ).* *Смарт-карта CryptoCard-337 – 6 шт.* *Електронний USB-ключ SecureToken-337 – 6 шт.* *Електронний ключ SecureToken-337F – 6 шт.* *Застосування ПАК CryptoIP дозволяє студентам Університету будувати системи захисту IP- трафіку за ідеологією IPSec (RFC 2401), а*

				також віртуальні конфіденційні мережі (VPN) поверх будь-яких (але зв'язкових) IPv4-мереж. Це забезпечує конфіденційність і цілісність даних, тощо. *Усі заняття проводяться в аудиторіях, які обладнані мультимедійним комплексом (проєктор, SMART-дошка, комп'ютер з встановленими Microsoft Office та антивірусною програмою ESET Endpoint Security). Під час вивчення дисципліни використовується електронний навчальний курс на платформі дистанційного навчання (Moodle) із включенням додаткових інформаційних ресурсів у відкритому доступі, а також статистичних баз даних і аналітичних звітів міжнародних організацій.* *Заняття при дистанційному навчанні проводяться з використанням корпоративного Google Meet (Zoom).*
Науково-дослідницька практика	практика	*Науково-дослідницька практика.pdf*	Yhl4c6eiDdotL+vwYSFtH8/0KrUaDS3GKkr57ku3Fmo=	*Практика здійснюється на базах практик (https://tinyurl.com/5ytyjh5y) згідно з укладеними договорами про співпрацю або на підставі листів-клопотань.* *Використовується матеріально-технічне бази практики.*
Технології розслідування інцидентів безпеки критичної інфраструктури	навчальна дисципліна	*Технології розслідування інцидентів безпеки критичної інфраструктури.pdf*	AQs1WQrJi8a50BA3kPPtMm+xtCFZMJvaGjVJJUwMD4E=	*Лабораторія безпеки інформаційних активів у складі:* *Сервер Dell PE R530 – 1 шт.* *Сервер Dell PE R530 – 2 шт.* *Сервер HP ProLiant – 2 шт.* *KBM-перемикач з підтримкою USB-периферії – 1 шт.* *Міжмережевий екран FG-100E-BDL-EU – 1 шт.* *Комутатор TP-Link T2600G-52TS – 2 шт.* *Комутатор Mikrotik Cloud Smart Switch CSS326-24G-2S+ – 2 шт.* *Маршрутизатор (router) Cisco – 2 шт.* *Точка доступу Cisco – 2 шт.* *Комп'ютер тип#1 Dell OptiPlex 3050 Micro Form Factor – 15 шт.* *Комп'ютер тип#2 Dell Precision Tower 3620 XCTO BASE – 1 шт.* *Дошка магнітна крейдово-маркерна обертова на колесах – 1 шт.* *Точка wi-fi доступу Linksys Cisco SB WAP 121 (WAP 121-E-K9-G5) – 2 шт.* *Екран для проектора настінний Walfix з механізмом п овернення 150" (4:3) 300x225 см – 1 шт.* *Проектор на стелю мережевий NEC P603X – 1 шт.* *БФП HP LaserJet Pro M130nw (G3Q58A) + USB cable – 1 шт.* *Мережева карта Panda Wireless PAU09 N600 Dual – 1 шт.*

				Мережеве сховище Internet Download Manager Synology DS718+ – 1 шт. *Застосування обладнання лабораторії дозволяє студентам Університету на обладнанні компанії Dell, IBM, D-Link, MicroSof, яке підтримує функцію віртуалізації на рівні процесора і дозволяє використовувати середу віртуалізації DOCKER, платформу OpenStack з готовими мережевими рішеннями (бібліотеку з понад 300 утиліт), а також програмний веб-інтерфейс RESELA+, розроблений Технологічним інститутом Блекинге (Швеція), отримувати: 1) базові знання для формування моделей захисту інформації та політик безпеки, організації пошуку і збору інформації; 2) професійні знання та компетентності щодо виявлення кібератак й протидії ним, захисту інформації в хмарних сховищах даних, моделювання процесів підтримки необхідного рівня захищеності інформаційних активів, ліквідації наслідків застосування кіберзброї та відновлення нормальних режимів функціонування мереж управління об'єктами інформаційної і кіберінфраструктури тощо. Усі заняття проводяться в аудиторіях, які обладнані мультимедійним комплексом (проєктор, SMART-дошка, комп'ютер з встановленими Microsoft Office та антивірусною програмою ESET Endpoint Security). Під час вивчення дисципліни використовується електронний навчальний курс на платформі дистанційного навчання (Moodle) із включенням додаткових інформаційних ресурсів у відкритому доступі, а також статистичних баз даних і аналітичних звітів міжнародних організацій. Заняття при дистанційному навчанні проводяться з використанням корпоративного Google Meet (Zoom).*
Технології безпеки Web-ресурсів	навчальна дисципліна	*Технології безпеки Web-ресурсів.pdf*	dk+//yJjYST+hVoO6oZusznKKcEAf23UiiIEuARZhek=	*Лабораторія безпеки інформаційних активів у складі:* *Сервер Dell PE R530 – 1 шт.* *Сервер Dell PE R530 – 2 шт.* *Сервер HP ProLiant – 2 шт.* *KBM-перемикач з підтримкою USB-периферії – 1 шт.* *Міжмережевий екран FG-100E-BDL-EU – 1 шт.* *Комутатор TP-Link T2600G-52TS – 2 шт.* *Комутатор Mikrotik Cloud Smart Switch CSS326-24G-2S+ – 2 шт.* *Маршрутизатор (router) Cisco – 2 шт.* *Точка доступу Cisco – 2 шт.*

					Комп'ютер тип#1 Dell OptiPlex 3050 Micro Form Factor – 15 шт. Комп'ютер тип#2 Dell Precision Tower 3620 XCTO BASE – 1 шт. Дошка магнітна крейдово-маркерна обертова на колесах – 1 шт. Точка wi-fi доступу Linksys Cisco SB WAP 121 (WAP 121-E-K9-G5) – 2 шт. Екран для проектора настінний Walfix з механізмом п овернення 150" (4:3) 300x225 см – 1 шт. Проектор на стелю мережевий NEC P603X – 1 шт. БФП HP LaserJet Pro M130nw (G3Q58A) + USB cable – 1 шт. Мережева карта Panda Wireless PAU09 N600 Dual – 1 шт. Мережеве сховище Internet Download Manager Synology DS718+ – 1 шт. *Застосування обладнання лабораторії дозволяє студентам Університету на обладнанні компанії Dell, IBM, D-Link, MicroSof, яке підтримує функцію віртуалізації на рівні процесора і дозволяє використовувати середу віртуалізації DOCKER, платформу OpenStack з готовими мережевими рішеннями (бібліотеку з понад 300 утиліт), а також програмний веб-інтерфейс RESELA+, розроблений Технологічним інститутом Блекинге (Швеція), отримувати: 1) базові знання для формування моделей захисту інформації та політик безпеки, організації пошуку і збору інформації; 2) професійні знання та компетентності щодо виявлення кібератак й протидії ним, захисту інформації в хмарних сховищах даних, моделювання процесів підтримки необхідного рівня захищеності інформаційних активів, ліквідації наслідків застосування кіберзброї та відновлення нормальних режимів функціонування мереж управління об'єктами інформаційної і кіберінфраструктури тощо. Усі заняття проводяться в аудиторіях, які обладнані мультимедійним комплексом (проектор, SMART-дошка, комп'ютер з встановленими Microsoft Office та антивірусною програмою ESET Endpoint Security). Під час вивчення дисципліни використовується електронний навчальний курс на платформі дистанційного навчання (Moodle) із включенням додаткових інформаційних ресурсів у відкритому доступі, а також статистичних баз даних і аналітичних звітів міжнародних організацій. Заняття при дистанційному навчанні проводяться з використанням корпоративного*

				Google Meet (Zoom).
Технології безпеки безпроводових і мобільних мереж	навчальна дисципліна	*Технології безпеки безпроводових і мобільних мереж.pdf*	WmDJdcmRdRlUc2LDr2vuWr9Lghgm1RHmBRiRpTtBGIA=	*Лабораторія комп'ютерних мереж* *у складі:* *Комп'ютер тип#1 Intel Core i3 3.0GHz, 4GB RAM, 1000GB HDD, 22" LED. Кількість: 12+1 ПК* *Міжмережевий екран ASA5506-K8 – 1 шт.* *Комутатор WS-C2960+24TC-L – 5 шт.* *Роутер Cisco ISR 4321 Sec bundle w/SEC license – 4 шт.* *Інтерфейсна карта Cisco HWIC-2T – 5 шт.* *Комутатори Catalyst 3650 24 Fast 4x1 G – 2 шт.* *Інтерактивна дошка SMART Board – 1 шт.* *Інтерактивна дошка SMART Board – 1 шт.* *Застосування обладнання лабораторії дозволяє студентам Університету на базовому наборі обладнання (Standard Core) та за програмою компанії Cisco Systems, Inc.:* *1) отримувати як базові, так і професійні знання в галузі мережевих технологій та компетентності в технологіях, використовуваних у структурах мережевої безпеки: встановлення і конфігурування комутаторів і маршрутизаторів Cisco в багатопротокольних мережах; пошуку та усунення несправностей у LAN і WAN мережах; підвищення продуктивності та захищеності мереж тощо, а також професійні знання та компетентності щодо організації роботи з мережами середніх розмірів й забезпечення безпеки мережевих програмно-апаратних засобів тощо;* *2) проходити професійну Cisco-сертифікацію за програмами підготовки фахівців з мереж та обладнанню Cisco – CCNA (спеціаліст) та CCNP (професіонал), а також фахівців, які відповідають за мережеву безпеку – CCNAS (спеціаліст з безпеки).* *Усі заняття проводяться в аудиторіях, які обладнані мультимедійним комплексом (проєктор, SMART-дошка, комп'ютер з встановленими Microsoft Office та антивірусною програмою ESET Endpoint Security). Під час вивчення дисципліни використовується електронний навчальний курс на платформі дистанційного навчання (Moodle) із включенням додаткових інформаційних ресурсів у відкритому доступі, а також статистичних баз даних і аналітичних звітів міжнародних організацій. Заняття при дистанційному навчанні проводяться з використанням корпоративного Google Meet (Zoom).*
Технології безпеки та	навчальна	*Технології безпеки*	NWxzcU10PnTNV52	*Лабораторія комп'ютерних*

управління критичними інфраструктурами	дисципліна	*та управління критичними інфраструктурами.pdf*	AxDAwpp2odcA2XzWPIyPGmxaQ4BA=	*мереж* *у складі:* *Комп'ютер тип#1 Intel Core i3 3.0GHz, 4GB RAM, 1000GB HDD, 22" LED. Кількість: 12+1 ПК* *Міжмережевий екран ASA5506-K8 – 1 шт.* *Комутатор WS-C2960+24TC-L – 5 шт.* *Роутер Cisco ISR 4321 Sec bundle w/SEC license – 4 шт.* *Інтерфейсна карта Cisco HWIC-2T – 5 шт.* *Комутатори Catalyst 3650 24 Fast 4x1 G – 2 шт.* *Інтерактивна дошка SMART Board – 1 шт.* *Інтерактивна дошка SMART Board – 1 шт.* *Застосування обладнання лабораторії дозволяє студентам Університету на базовому наборі обладнання (Standard Core) та за програмою компанії Cisco Systems, Inc.:* *1) отримувати як базові, так і професійні знання в галузі мережевих технологій та компетентност в технологіях, використовуваних у структурах мережевої безпеки: встановлення і конфігурування комутаторів і маршрутизаторів Cisco в багатопротокольних мережах; пошуку та усунення несправностей у LAN і WAN мережах; підвищення продуктивності та захищеності мереж тощо, а також професійні знання та компетентності щодо організації роботи з мережами середніх розмірів й забезпечення безпеки мережевих програмно-апаратних засобів тощо;* *2) проходити професійну Cisco-сертифікацію за програмами підготовки фахівців з мереж та обладнанню Cisco – CCNA (спеціаліст) та CCNP (професіонал), а також фахівців, які відповідають за мережеву безпеку – CCNAS (спеціаліст з безпеки).* *Усі заняття проводяться в аудиторіях, які обладнані мультимедійним комплексом (проєктор, SMART-дошка, комп'ютер з встановленими Microsoft Office та антивірусною програмою ESET Endpoint Security). Під час вивчення дисципліни використовується електронний навчальний курс на платформі дистанційного навчання (Moodle) із включенням додаткових інформаційних ресурсів у відкритому доступі, а також статистичних баз даних і аналітичних звітів міжнародних організацій. Заняття при дистанційному навчанні проводяться з використанням корпоративного Google Meet (Zoom).*
Організація науки і наукових досліджень	навчальна дисципліна	*Організація науки і наукових досліджень.pdf*	bflnPxKC1JYvrlILp5sy8ysfttloqf3cDimcPeyEizw=	*Усі заняття проводяться в аудиторіях, які обладнані мультимедійним комплексом (проєктор, SMART-дошка, комп'ютер з встановленими Microsoft Office та антивірусною програмою ESET Endpoint*

				Security). Під час вивчення дисципліни використовується електронний навчальний курс на платформі дистанційного навчання (Moodle) із включенням додаткових інформаційних ресурсів у відкритому доступі, а також статистичних баз даних і аналітичних звітів міжнародних організацій. Заняття при дистанційному навчанні проводяться з використанням корпоративного Google Meet (Zoom).
Прикладна загальна теорія систем безпеки	навчальна дисципліна	*Прикладна загальна теорія систем безпеки.pdf*	u63rRR4hbdmaXRDO7bHAX6XMvc3s2OGKdARskRrlS1Q=	*Лабораторія вбудованих систем та 3-D моделювання* *у складі:* *Комп'ютер тип#1 Сервер на базі NetNavigatorE, E3-1230V, 16 Гб – 1 шт.* *Комп'ютер тип#2 ПК, Intel Core i3 4160, 4 Гб – 7 шт.* *Комп'ютер тип#3 ПК Intel Core 2 Duo, 512 МБ, 230 Гб – 15 шт.* *Спеціальне обладнання ВС:* *Навчальна плата Arduino Mega 2560 R3 – 1 шт.* *Плата розширення Danger-Shield Bausant (Spark Fan) – 1 шт.* *Плата розширення mSD-Shield v2 (Datenlogger Shield) – 1 шт* *Покроковий потенціометр Drehencoder mit Taster PEC12R-4225F-S0024 – 1 шт.* *Плата розширення GLCD-Shield mit Dispay – 1 шт.* *Плата розширення Ethernet-Shield R3 (Arduino) – 1 шт.* *Навчальна плата для програмування Raspberry Pi 2 Modell B –* *ARM Cortex-A7 Quad Core – 1 шт.* *Плата розширення Shield-Bridge (Raspberry Pi Arduino Adapter) – 1 шт* *Навчальна плата STM32F4-Discovery – 1 шт.* *Плата розширення MI0283AV2 Adapter v2 – 1 шт.* *Плата Intel Galileo – 15 шт.* *Плата Altium NanoBoard 3000 – 1 шт.* *Двоколісна демонстраційна модель Formula Flowcode Buggy – 10шт.* *Макет лабіринту (Maze walls) – 1 шт.* *Усі заняття проводяться в аудиторіях, які обладнані мультимедійним комплексом (проєктор, SMART-дошка, комп'ютер з встановленими Microsoft Office та антивірусною програмою ESET Endpoint Security). Під час вивчення дисципліни використовується електронний навчальний курс на*

				платформі дистанційного навчання (Moodle) із включенням додаткових інформаційних ресурсів у відкритому доступі, а також статистичних баз даних і аналітичних звітів міжнародних організацій. Заняття при дистанційному навчанні проводяться з використанням корпоративного Google Meet (Zoom
Іноземна мова професійного спрямування	навчальна дисципліна	*Іноземна мова професійного спрямування.pdf*	OGY6ehn30JtzyXAo33avB2l6qXRa9wGRkEU7aOG3thg=	*Практичні заняття проводяться в аудиторіях, які обладнані мультимедійними комплексами (проєктор, SMARTдошка/екран, комп'ютер з встановленими Microsoft Office та антивірусною програмою ESET Endpoint Security). Для організації роботи в групах використовуються такі цифрові інструменти як віртуальні дошки: Padlet, Google Jamboard та вбудовані інтерактивні додатки в електронному навчальному курсі на платформі дистанційного навчання (на базі Moodle). Заняття при дистанційному навчанні проводяться з використанням корпоративного Google Meet (Zoom).*
Прикладні аспекти тестувань на проникнення та етичного хакінгу	навчальна дисципліна	*Прикладні аспекти тестувань на проникнення та етичного хакінгу.pdf*	kisNQR6qh4RrIi9D8z87Zcswp8Rw5ZDikLJ9t8MCdYs=	*Лабораторія безпеки інформаційних активів у складі:* *Сервер Dell PE R530 – 1 шт.* *Сервер Dell PE R530 – 2 шт.* *Сервер HP ProLiant – 2 шт.* *KBM-перемикач з підтримкою USB-периферії – 1 шт.* *Міжмережевий екран FG-100E-BDL-EU – 1 шт.* *Комутатор TP-Link T2600G-52TS – 2 шт.* *Комутатор Mikrotik Cloud Smart Switch CSS326-24G-2S+ – 2 шт.* *Маршрутизатор (router) Cisco – 2 шт.* *Точка доступу Cisco – 2 шт.* *Комп'ютер тип#1 Dell OptiPlex 3050 Micro Form Factor – 15 шт.* *Комп'ютер тип#2 Dell Precision Tower 3620 XCTO BASE – 1 шт.* *Дошка магнітна крейдово-маркерна обертова на колесах – 1 шт.* *Точка wi-fi доступу Linksys Cisco SB WAP 121 (WAP 121-E-K9-G5) – 2 шт.* *Екран для проектора настінний Walfix з механізмом п овернення 150" (4:3) 300x225 см – 1 шт.* *Проектор на стелю мережевий NEC P603X – 1 шт.* *БФП HP LaserJet Pro M130nw (G3Q58A) + USB cable – 1 шт.* *Мережева карта Panda Wireless PAU09 N600 Dual – 1 шт.* *Мережеве сховище Internet Download Manager Synology*

				DS718+ – 1 шт. *Застосування обладнання лабораторії дозволяє студентам Університету на обладнанні компанії Dell, IBM, D-Link, MicroSof, яке підтримує функцію віртуалізації на рівні процесора і дозволяє використовувати середу віртуалізації DOCKER, платформу OpenStack з готовими мережевими рішеннями (бібліотеку з понад 300 утиліт), а також програмний веб-інтерфейс RESELA+, розроблений Технологічним інститутом Блекинге (Швеція), отримувати: 1) базові знання для формування моделей захисту інформації та політик безпеки, організації пошуку і збору інформації; 2) професійні знання та компетентності щодо виявлення кібератак й протидії ним, захисту інформації в хмарних сховищах даних, моделювання процесів підтримки необхідного рівня захищеності інформаційних активів, ліквідації наслідків застосування кіберзброї та відновлення нормальних режимів функціонування мереж управління об'єктами інформаційної і кіберінфраструктури тощо. Усі заняття проводяться в аудиторіях, які обладнані мультимедійним комплексом (проєктор, SMART-дошка, комп'ютер з встановленими Microsoft Office та антивірусною програмою ESET Endpoint Security). Під час вивчення дисципліни використовується електронний навчальний курс на платформі дистанційного навчання (Moodle) із включенням додаткових інформаційних ресурсів у відкритому доступі, а також статистичних баз даних і аналітичних звітів міжнародних організацій. Заняття при дистанційному навчанні проводяться з використанням корпоративного Google Meet (Zoom).*

* 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 відповідність НПП оствітнім компонентам

ID викладача	ПІБ	Посада	Структурний підрозділ	Кваліфікація викладача	Стаж	Навчальні дисципліни, що їх викладає викладач на ОП	Обґрунтування відповідності освітньому компоненту (кваліфікація, професійний досвід, наукові публікації)
467237	Балабан Олена Олександрівна	Доцент, Сумісництво	Факультет романо-германської філології	Диплом спеціаліста, Горлівський державний	19	Іноземна мова професійного спрямування	Відповідність освіти: 1. Горлівський державний педагогічний інститут

				педагогічний інститут іноземних мов, рік закінчення: 1996, спеціальність: Англійська та французька мови, Диплом кандидата наук ДК 040792, виданий 10.05.2007, Атестат доцента 12ДЦ 027765, виданий 14.04.2011			іноземних мов, 1996 р., спеціальність: англійська та французька мови, кваліфікація: вчитель англійської та французької мов. 2.Приазовський державний технічний університет, аспірантура, 1997-2000 рр., спеціальність: 10.02.15 - Загальне мовознавство. Рік захисту - 2006 р.. 2.Національний педагогічний університет імені М.П. Драгоманова, докторантура, 2016–2018 рр., спеціальність: 035 – Філологія. 1) наявність не менше п’яти публікацій у періодичних наукових виданнях, що включені до переліку фахових видань України, до наукометричних баз, зокрема Scopus, Web of Science Core Collection 1. Balaban O., Aleksakhina T., Davydova T., Goltsova M., Oleksii Tsepkalo O. The Epistemology-Oriented Conceptual Model of Cognitive-Semantic Universals in Related Languages // Multidisciplinary Science Journal. V.6. (Scopus) 2024 https://malque.pub/ojs/index.php/msj/article/view/3077 2. Marieiev D., Chornyi I., Balaban O., Kobets J., Berezovska-Chmil O., Shchur N. Linguistic Means of Expressing the Category of Temporality in Modern Political Discourse // World Journal of English Language. Vol. 13, No. 4; 2023, ISSN 1925-0703 E-ISSN 1925-0711. P.23-28. (Scopus) https://www.sciedupress.com/journal/index.php/wjel/article/view/23582 3. Балабан О.О. Когнітивний механізм як tertium comparationis для встановлення когнітивно-семантичних універсалій // Академічні студії. Серія «Гуманітарні науки», Вип. 4, Видавничий дім

							«Гельветика», 2021. С. 54-67 4. Балабан О.О. Категорія роду як мультикультурний код та когнітивно-семантична універсалія в споріднених мовах (англійська, французька, українська, російська) // Закарпатські філологічні студії. № 14/2020. Т.1. Ужгород, 2020. С. 158-162. ISSN 2524-0390 5. Balaban O. Archetypization and streotyping as universal mechanizms of conceptualization of human conciousness in related languages // KNOWLEDGE • EDUCATION • LAW • MANAGEMENT. № 5 (33) vol. 1 / 2020. P. 39-44. https://kelmczasopisma.com/en/viewpdf/1732 3) наявність виданого підручника чи навчального посібника (включаючи електронні) або монографії (загальним обсягом не менше 5 авторських аркушів), в тому числі видані у співавторстві (обсягом не менше 1,5 авторського аркуша на кожного співавтора) 1. Balaban O. Clipping Conceptual Models as a Kind of Mental-Oriented Model of Secondary Semiosis and Cognitive-Semantic Universals in Related Languages // Innovative pathway for the development of modern philological sciences in Ukraine and EU countries: Scientific monograph. Volume 1. Riga, Latvia : “Baltija Publishing”, 2022. P. 112-134. 7) участь в атестації наукових кадрів як офіційного опонента або члена постійної спеціалізованої вченої ради, або члена не менше трьох разових спеціалізованих вчених рад 1. Член спеціалізованої вченої ради із захисту дисертації Давиденко А.О. Об’єктивація дискурсотвірних концептів TRADITION/ТРАДИЦ

							ІЯ, FAMILY/РОДИНА, HEALTH/ЗДОРОВ'Я, SUCCESS/УСПІХ у англо- та українськомовній комерційній рекламі», подану на здобуття ступеня вищої освіти доктора філософії зі спеціальності 035 Філологія, Національний педагогічний університет імені М.П. Драгоманова ДФ 26.053.047 (Член ради) (2022 р.) 2. Член спеціалізованої вченої ради із захисту дисертації Білогорської Л.В. «Романи О. Гріна як художня єдність: мотивіка, символіка, хронотоп, хронологія характерів», подану на здобуття ступеня вищої освіти доктора філософії зі спеціальності 035 Філологія, НПУ імені М.П. Драгоманова, Спеціалізована вчена рада ДФ 26.053.008 (2021 р.); 3. Член спеціалізованої вченої ради із захисту дисертації Нікітської К.І. «Жанр поеми у творчості М.С. Гумільова», подану на здобуття ступеня вищої освіти доктора філософії зі спеціальності 035 Філологія, НПУ імені М.П. Драгоманова, Спеціалізована вчена рада ДФ 26.053.010 (2021 р.); 4. Член спеціалізованої вченої ради із захисту дисертації Сорочинської І.Р. «Логіко-семіотичне моделювання педагогічних афоризмів в англійській, італійській та українській мовах», подану на здобуття ступеня вищої освіти доктора філософії зі спеціальності 035 Філологія, НПУ імені М.П. Драгоманова, Спеціалізована вчена рада ДФ 26.053.012 (2021 р.), 5. Опонування дисертації Степанова В.В. Лінгвосинергетичний аспект концепту ПОЛІТИКА в сучасному американському

							англомовному дискурс», подану на здобуття ступеня вищої освіти доктора філософії зі спеціальності 035 Філологія, Запорізькій національний університет, Спеціалізована вчена рада ДФ 17.051.028 (2021 р.) 6. Член спеціалізованої вченої ради із захисту дисертації Карлової В.О. «Когнітивно-матричне моделювання запозиченої лексики в давньоанглійській поемі “Беовульф”», подану на здобуття ступеня вищої освіти доктора філософії зі спеціальності 035 Філологія, НПУ імені М.П. Драгоманова, Спеціалізована вчена рада ДФ 26.053.001 (2020 р.) 8) виконання функцій (повноважень, обов’язків) наукового керівника або відповідального виконавця наукової теми (проекту), або головного редактора/члена редакційної колегії/експерта (рецензента) наукового видання, включеного до переліку фахових видань України, або іноземного наукового видання, що індексується в бібліографічних базах Член редколегії міжнародного американо-українського видання «The Trypillian Civilization Journal (www.trypillia.com)» 12) наявність апробаційних та/або науково-популярних, та/або консультаційних (дорадчих), та/або науково-експертних публікацій з наукової або професійної тематики загальною кількістю не менше п’яти публікацій 1. Балабан О.О. Когнітивна сутність семантичних універсалій крізь призму знакової теорії // ПРОГРАМА і матеріали IV Міжнародної науково-практичної

							конференції 30 березня 2023 року “Філософія мови та нові тенденції в перекладознавстві й лінгвістиці” (30 березня 2023 р.). УДУ імені Михайла Драгоманова. Київ. 2023. С. 16-18. 2. Балабан О.О. Симулякризація як універсальний когнітивний механізм концептуалізації людської свідомості // Зб. Матеріалів ІІІ Міжнародної науково-практичної конференції «Філософія мови та нові тенденції у перекладознавстві й лінгвістиці» (2 квітня 2021 р.). К.: НПУ імені М.П. Драгоманова. 2021. С. 23-26. 19) діяльність за спеціальністю у формі участі у професійних та/або громадських об’єднаннях Дійсний член громадської організації «Асоціація викладачів англійської мови «ТІСОЛ – Україна» (TESOL-Ukraine) особовий номер 23826 г (2023, 2024 р.) Відомості про підвищення кваліфікації Пройшла наукове стажування «Академічна доброчесність: виклики сучасності», організованого Польсько-українською Фундацією – Інститут Міжнародної Академічної та Наукової Співпраці спільно з Духовною Академією Університету Кардинала Стефана Вишинського у Варшаві та польською Фундацією ADD з 24 січня по 4 березня 2022 р. (6 кредитів – 180 год.; сертифікат KW – 040322/010 від 04.03.2022
466024	Махачашвілі Русудан Кирилевна	Завідувач кафедри, Основне місце роботи	Факультет романо-германської філології	Диплом магістра, Запорізький державний університет, рік закінчення: 2004, спеціальність: 030502 Мова та література	19	Іноземна мова професійного спрямування	Відповідність освіти: 1.Запорізький державний університет, 2004 р. Спеціальність: Мова та література (англійська), Кваліфікація: Магістр філології, викладач англійської мови та

				(англійська), Диплом доктора наук ДД 003202, виданий 03.04.2014, Диплом кандидата наук ДК 034763, виданий 11.05.2006, Атестат доцента 12ДЦ 022447, виданий 19.02.2009, Атестат професора АП 005531, виданий 25.10.2023			літератури у вищих навчальних закладах, викладач іспанської мови 2. Доктор філологічних наук, 2014 р. 10.02.04 - Германські мови. Тема дисертації: «Динаміка англомовної інноваційної логосфери комп'ютерного буття» 3. Доцент кафедри теорії та практики перекладу англійської мови, 2009 р. 4. Професор кафедри романської філології та порівняльнотипологічного мовознавства, 2023 р. 1) наявність не менше п’яти публікацій у періодичних наукових виданнях, що включені до переліку фахових видань України, до наукометричних баз, зокрема Scopus, Web of Science Core Collection 1. Makhachashvili, Rusudan та Semenist, Ivan (2024) Artificial Intelligence in Transdisciplinary Communication Paradigm for Digital Education Proceedings of the 18th International Multi-Conference on Society, Cybernetics and Informatics, IMSCI, 1. с. 91-98. ISSN 2831-722X (Scopus). 2. Makhachashvili, Rusudan та Semenist, Ivan та Копитіна, Анастасія Сергіївна та Бахтіна, Анна Олегівна та Білик, Катерина Миколаївна (2024) Emotional Intelligence and Implicit Interdisciplinary Skills: Key Components for Effective Digital And AI-Enhanced Learning Proceedings of the International Multi-Conference on Society, Cybernetics and Informatics, IMSCI, 1. с. 99-106. ISSN 2831-722X (Scopus). 3. Makhachashvili, Rusudan та Semenist, Ivan та Prihodko, G. та Prykhodchenko, O. та Rudik, I. та Ter-Grygoryan, M. та Brus, M. (2024) Interdisciplinary, AI-interoperable, and Universal Skills for

							Foreign Languages Education in Emergency Digitization Proceedings of the International Multi-Conference on Society, Cybernetics and Informatics, IMSCI, 1. c. 107-114. ISSN 2831-722X. (Scopus). 4. Makhachashvili, Rusudan та Semenist, Ivan та Vinnikova, Nataliia та Tupakhina, O. (2024) Interdisciplinary and Interoperable Leadership Skills for Digital Educational Communication Proceedings of the International Multi-Conference on Society, Cybernetics and Informatics, IMSCI, 1. c. 115-122. ISSN 2831-722X (Scopus). 5. Morze, Nataliia та Makhachashvili, Rusudan та Zvonar, V. та Ilich, Liydmyla та Gladun, Mariia (2024) Navigating The Digital Frontier: Ukraine's E-Governance Curriculum Amidst Crisis and EU Integration Proceedings of World Multi-Conference on Systemics, Cybernetics and Informatics, WMSCI, 1. c. 4-9. ISSN 2771-0947 (Scopus). 6. Makhachashvili, Rusudan та Semenist, Ivan (2024) Digital Humanities as a Transdisciplinary Communication Paradigm in the Age of AI Proceedings IMCIC - International Multi-Conference on Complexity, Informatics and Cybernetics, 1. c. 286-293. ISSN 2771-5914 (Scopus). 7. Makhachashvili, Rusudan та Semenist, Ivan та Prihodko, G. та Kolegaeva, I. та Prykhodchenko, O. та Tupakhina, O. (2024) Interdisciplinary Digital Skills Development For Educational Communication: Emergency And AI-Enhanced Digitization Proceedings IMCIC - International Multi-Conference on Complexity, Informatics and Cybernetics, 1. c. 281-285. ISSN 2771-5914 (Scopus). 8. Makhachashvili, Rusudan та Semenist, Ivan (2024)

Transformative, Transdisciplinary, Transcendent Digital Education: Synergy, Sustainability and Calamity Proceedings IMCIC - International Multi-Conference on Complexity, Informatics and Cybernetics, 1. c. 273-280. ISSN 2771-5914 (Scopus).
9. Makhachashvili, Rusudan та Semenist, Ivan (2023) Meta-Disciplinarity of Digital Education and Communication Proceedings of the 14th International Multi-Conference on Complexity, Informatics and Cybernetics: IMCIC 2023 (1). c. 209-214. ISSN 2771-5914 (Scopus)
10. Makhachashvili, Rusudan та Semenist, Ivan (2023) Transdisciplinary Communication in the Meta-Framework of Digital Education Proceedings of the 14th International Multi-Conference on Complexity, Informatics and Cybernetics: IMCIC 2023 (1). c. 215-220. ISSN 2771-5914 (Scopus)
11. Makhachashvili, Rusudan та Семеніст, Іван Васильович та Москальов, Дмитро Петрович (2022) Interdisciplinarity of Foreign Languages Education Design and Management in COVID-19 Artificial Intelligence in Education: Emerging Technologies, Models and Applications. Lecture Notes on Data Engineering and Communications Technologies, 104. c. 239-255. ISSN 2367-4512
12. Makhachashvili, Rusudan та Semenist, Ivan V. (2022) Systemic Dynamics of Digital Education in Foreign Languages Programs Proceedings of the 16th International Multi-Conference on Society, Cybernetics and Informatics, 1. c. 5-10. ISSN 2831-722X
13. Makhachashvili, Rusudan та Семеніст, Іван Васильович (2022) Interdisciplinary and

							Universal Digital Competence for Foreign Languages Education 13th International Multi-Conference on Complexity, Informatics and Cybernetics, 1. c. 36-43. ISSN 2771-5914 14. Makhachashvili, Rusudan та Ivan Semenist, Ivan (2021) Digital Distance And Blended Learning Quality Assessment In Oriental And European Languages University Programs: Regions Of Ukraine Survey Study 9th International Conference on Information and Education Technology, ICIET 2021, 1. c. 149-156. (Scopus) 15. Makhachashvili, Rusudan та Semenist, Ivan (2021) Interdisciplinary skills development through final qualification assessment: Survey study for European and Oriental languages programs IMCIC 2021 - 12th International Multi-Conference on Complexity, Informatics and Cybernetics, Proceedings, 1. c. 144151. (Scopus) 16. Makhachashvili, Rusudan та Ivan Semenist, Ivan and Bakhtina, Anna (2021) ICT tools for final qualification assessment survey study for european and oriental languages programs 8th International Conference on Educational Technologies 2021, ICEduTech 2021 and 17th International Conference on Mobile Learning 2021, ML 2021, pp. 107-115. pp. 107-115. (Scopus) 17. Makhachashvili, R., Semenist, I. Covid-19 context for meta assessment of digital learning on european and oriental languages programs. IMCIC 2021 - 12th International Multi-Conference on Complexity, Informatics and Cybernetics, Proceedings, 2021, 2, pp. 129–134. (Scopus) 18. Makhachashvili, R., Morze N. Digital competence in e-governance education:

							A survey study. CEUR Workshop Proceedings, 2021, 2833, pp. 93–102. (Scopus) Публікації у фахових виданнях України (Категорія Б) 1. Makhachashvili, Rusudan та Семеніст, Іван Васильович (2022) Феноменологічна парадигма інноваційного моделювання цифрової логосфери (на основі інновацій китайської мови) Нова філологія (85). с. 173-180. ISSN 2414-1135. 2. Махачашвілі, Русудан Кирилевна та Семеніст, Іван Васильович (2022) Іллокутивне моделювання інноваційної освітньої комунікації в цифровому середовищі (на матеріалі європейських та азійських варіантів англійської мови) Науковий вісник Міжнародного гуманітарного університету. Сер.: Філологія (54). с. 59-64. ISSN 2409-1154 3. Makhachashvili, Rusudan та Semenist, I.V. (2022) Моделювання цифрової інноваційної комунікації (на матеріалі інновацій східних мов) Науковий вісник Міжнародного гуманітарного університету. Сер.: Філологія (55). с. 56-60. ISSN 2409-1154 4. Махачашвілі, Русудан Кирилевна та Бахтіна, Анна Олегівна (2021) HATE EMOJI в лінгвокриміналістичних експертизах: проблеми декодифікації смислу Вісник Житомирського державного університету імені Івана Франка. Філологічні науки (1(94)). с. 79-96. ISSN 2663-7642; 2707-4463 5. Мультилінгвальна формотворююча асиметрія в динаміці мікроструктури інноваційної Логосфери комп'ютерного буття, Нова філологія, 2 (80), 2021, С. 26-34.

							ISSN 2414-1135. 6. Verbal Modelling of Innovative Educational Communication in The Digital Discourse. Вчені записки Таврійського національного університету імені В. І. Вернадського. Серія: Філологія. Журналістика», Том 32 (71) № 4, 2021 7. DIRECTIONS AND MECHANISMS OF GLOBAL INNOVATIVE LOGOSPHERE OF COMPUTER BEING MICROSTRUCTURE DYNAMICS (BASED ON EUROPEAN AND ORIENTAL LANGUAGES). Науковий Вісник МГУ, №49, 2021 8. INNOVATIVE EDUCATIONAL COMMUNICATION IN THE DIGITAL DISCOURSE: MODELS AND TOOLS. «Актуальні питання гуманітарних наук: міжвузівський збірник наукових праць молодих вчених Дрогобицького державного педагогічного університетуімені Івана Франка», № 40, 2021. 9. ЗМІСТОВА АСИМЕТРІЯ ЯК МЕХАНІЗМ ДИНАМІКИ МІКРОСТРУКТУРИ ГЛОБАЛЬНОЇ ІННОВАЦІЙНОЇ ЛОГОСФЕРИ КОМП'ЮТЕРНОГО БУТТЯ (НА МАТЕРІАЛІ ЄВРОПЕЙСЬКИХ ТА СХІДНИХ МОВ). ""Нова філологія"", № 82, 2021. 10. GLOBAL INNOVATIVE LOGOSPHERE OF COMPUTER BEING MACROSTRUCTURE DYNAMICS (BASED ON EUROPEAN AND ORIENTAL LANGUAGES), Науоквий Вісник МГУ, №48, 2021 11. Digital communication and information communication tools for final qualification assessment in oriental languages programs, Вчені записки Таврійського національного університету імені В.І. Вернадського Серія: Філологія. Соціальні

							комунікації, 31(70) (4), 2020, С. 233-240. ISSN 2663- 6069. 12. Phenomenological principles of global innovative logosphere of computer being construction (based on European and oriental languages), Вчені записки ТНУ імені В. І. Вернадського, 32(71) (1), 2020, С. 195-202. ISSN 2710-4664 13. Digital skills development and ICT tools for final qualification assessment: survey study for students and staff of european and oriental philology programs, Відкрите освітнє е-середовище сучасного університету (9), 2020, С. 54-68. ISSN 2414-0325 3) наявність виданого підручника чи навчального посібника (включаючи електронні) або монографії (загальним обсягом не менше 5 авторських аркушів), в тому числі видані у співавторстві (обсягом не менше 1,5 авторського аркуша на кожного співавтора) Монографії (колективні) 1. Makhachashvili, Rusudan та Семеніст, Іван Васильович та Москальов, Дмитро Петрович (2022) Interdisciplinarity of Foreign Languages Education Design and Management in COVID-19 Artificial Intelligence in Education: Emerging Technologies, Models and Applications. Lecture Notes on Data Engineering and Communications Technologies, 104. Springer, с. 239-255. ISSN 2367-4512 2. Makhachashvili, Rusudan and Shtaltovna, Yuliya (2021) Digital Terraformation: Cyberspace Ontology, Anthropology, and Gnosis Колективна (три і більше авторів). AGA Arti Grafiche Alberobello, Italy. С.441-452. 3. Махачашвілі, Русудан Кирилевна (2020) Моделі й цифрові інструменти

							діагностики динаміки інноваційної полілінгвальної логосфери комп'ютерного буття Колективна (три і більше авторів). Італійсько-Українські Контрастивні Студії: Мовознавство, Літературознавство: колективна монографія. Peter Lang GmbH Internationaler Verlag der Wissenschaften, Берлін. С.99-124. 4. Rusudan Makhachashvili, Anna Bakhtina, Svetlana Kovpik. MOTIVE SUBSTRAT PECULIARITIES IN THE NOVEL "FELIX AUSTRIA" BY S. ANDRUKHOVICH: DIALECTICAL MATERIALISM OF A CHARACTER PSYCHOPHYSIOLOGI CAL STATE. THEORETICAL BASES OF PHILOLOGICAL RESEARCH OF MODERN LITERATURE, pp. 68-86, 2020. 5. Makhachashvili, Rusudan та Семеніст, Іван Васильович та Бахтіна, Анна Олегівна (2020) ІКТ інструменти та практики підсумкової кваліфікаційної атестації в умовах карантинних обмежень COVID-19 Колективна (три і більше авторів). Innovative Educational Technologies, Tools and Methods for E-learning Monograph. University of Silesia in Katowice, Poland, Katowice, Poland. С.183-195. Словники, енциклопедії 1. Махачашвілі, Русудан Кирилевна та Бахтіна, Анна Олегівна та Білик, Катерина Миколаївна (2020) Кібермова: багатомовний електронний лексикографічний проект Колективний. Lexonimy, Elexis project (European comission), Ljubljana, Slovenia. Підручники, навчальні посібники (колективні) 1. Modern dimensions of linguistics and communication:

							models of language development in the digital realm. Навчальний посібник. Київ: Київ. ун-т ім. Б. Грінченка, 2022, 250 с. 4) наявність виданих навчально-методичних посібників/посібників для самостійної роботи здобувачів вищої освіти та дистанційного навчання, електронних курсів на освітніх платформах ліцензіатів, конспектів лекцій/практикумів/методичних вказівок/рекомендацій/ робочих програм, інших друкованих навчально-методичних праць загальною кількістю три найменування 1. Електронний навчальний курс «Сучасні аспекти лінгвістики та мовної комунікації», для освітнього ступеня магістра (наказ про сертифікацію № 811 від 06.12.2021. 2. Електронний навчальний курс «ФІлологічні студії», для освітнього ступеня магістра 2021 р. 3. Електронний навчальний курс "Філософія мови і освіти: Філософія мови", для освітнього ступеня магістра 2020 р. 6) наукове керівництво (консультування) здобувача, який одержав документ про присудження наукового ступеня (прізвище, ім'я, по батькові дисертанта, здобутий науковий ступінь, спеціальність, назва дисертації, рік захисту, серія, номер, дата, ким виданий диплом) 1. Бахтіна Анна Олегівна. Науковий ступінь: Доктор філософії за спеціальністю - 035 філологія (03 Гуманітарні науки). Тема: "Полілатеральність emoji в комп'ютерному бутті (на матеріалі сучасних європейських мов)". 2023 р. Диплом: Н23

							№ 001326 від 14.09.2023 р. Київським столичним університетом імені Бориса Грінченка. 2. Білик Катерина Миколаївна. Науковий ступінь: Доктор філософії за спеціальністю - 035 філологія (03 Гуманітарні науки). Тема: "Жанр "надзвичайні новини" у сучасному європейському медіадискурсі". 2023 р. Диплом: Н23 № 001325 від 14.09.2023 р. Київським столичним університетом імені Бориса Грінченка. 3. Семеніст Іван Васильович. Науковий ступінь: Доктор філологічних наук, 10.02.04 – Германські мови. Тема: "Мовна комунікація в цифровому середовищі: моделі, засоби, механізми (на матеріалі інновацій європейських та азійських варіантів англійської мови)". 2021 р. Диплом: ДД 012791 від 01.02.2022 р. МОН України, Запорізьким національним університетом. 4. Копитіна Анастасія Сергіївна. Науковий ступінь: Доктор філософії за спеціальністю - 035 філологія (03 Гуманітарні науки). Тема: "Лінгвокогнітивні та соціолінгвальні параметри лексико-семантичного поля «простір» (на матеріалі англійської, російської, української та французької мов)". 2021 р. Диплом: ДР № 003465 від 24.03.2022 р. МОН України, Київським університетом імені Бориса Грінченка. 7) участь в атестації наукових кадрів як офіційного опонента або члена постійної спеціалізованої вченої ради, або члена не менше трьох разових спеціалізованих вчених рад 1. Член спеціалізованої вченої ради Д 26.133.03 з правом прийняття до розгляду та проведення захистів

							дисертацій на здобуття наукового ступеня доктора (кандидата) філологічних наук за спеціальностями 10.01.01 «Українська література» та 10.01.06 «Теорія літератури» (2017р.-2020 р.) 2. Член спеціалізованої вченої ради К 26.133.08 з правом прийняття до розгляду та проведення захистів дисертацій на здобуття наукового ступеня кандидата філологічних наук за спеціальностями 10.02.04 «Германські мови» та 10.02.15 «Загальне мовознавство» (2017р.-2020 р.) 3. Одноразові ради 035 Філологія Київського університету імені Бориса Грінченка: Голова ради ДФ 26.133.067, Городілова Тетяна Миколаївна (2024 р.) Голова ради ДФ 26.133.068, Сіваєва Ольга Сергіївна (2024 р.) Рецензент ДФ 26.133.076, Рязанов Ігор Геннадійович (2024 р.) Голова ради ДФ 26.133.013, Гусар Ангеліна Вікторівна (2021 р.) Рецензент ДФ 26.133.014, Рожков Юрій Григорович (2021 р.) Рецензент ДФ 26.133.018, Ладоня Катерина Юріївна (2021 р.)
							8) виконання функцій (повноважень, обов'язків) наукового керівника або відповідального виконавця наукової теми (проекту), або головного редактора/члена редакційної колегії/експерта (рецензента) наукового видання, включеного до переліку фахових видань України, або іноземного наукового видання, що індексується в бібліографічних базах Керівник науково-дослідної теми кафедри романської

							філології та порівняльно типологічного мовознавства «Розвиток європейських мов і літератур в контексті міжкультурної комунікації» (2016-2021, код державної реєстрації 0116U006607) Редколегії наукових видань Україна: Заступник головного редактора – «Синопсис: Текст, Контекст, Медіа» (Категорія Б, Erih Plus, Index Copernicus International) Член редколегій: - Open Educational E-environment of Modern University (Категорія Б, Erih Plus) - ""Нова філологія"" (Категорія Б, Erih Plus) Міжнародні наукові видання (член редколегії): - Turkish Online Journal of Qualitative Inquiry (Scopus) - Information and Education Technology, IEEE (Scopus) - New Trends in Languages, Literature and Social Communications, Atlantic Press, Springer Journal of Systemics, Cybernetics and Informatics (DOAJ) - International Journal of Linguistics, Literature and Culture (Web of Science, ICI, Crossref) DIVAi», «DLCC» (Web of Science) - International Journal of Research in E-learning (Index Copernicus, Erih Plus) - Ukrainian Journal of Sinology Studies 10) участь у міжнародних наукових та/або освітніх проектах, залучення до міжнародної експертизи, наявність звання “суддя міжнародної категорії” Експерт з оцінки грантових заявок програми Горизонт 2020: Європейська комісія. Період реалізації: 01.09.2016-31.12.2020 р. Експерт з оцінки грантових заявок програми Горизонт

							Європа: Європейська комісія. Період реалізації: 10.04.2021-до нині. Експерт Мережі міждисциплінарних досліджень Оксфордського університету (Великобританія); Експерт Європейської Асоціації Цифрової Гуманітаристики (2018-2021). Міжнародні науково-дослідні проєкти Координатор проекту: Європейська лексикографічна структура ELEXIS (Горизонт 2020) Інститут Йозефа Стефана (Словенія) наказ № 848. Період реалізації: 21.02.2019-25.05.2022 Координатор проекту: ELEXIS Association (CLARIN) Інститут Йозефа Стефана (Словенія) 2023-2028 Координатор проєкту TERMCOORD: Terminology Without Borders (Європейський Парламент) – 2023-2025. Рамкові міжнародні науково-дослідні проєкти 1. Учасник проєкту: МЗС Естонії. Таллінський технологічний університет (Естонія). Консультування українських університетів щодо розробки навчальних планів магістерської роботи в електронному уряді (2020-2022). 2. Учасник проєкту The International Study of Leadership Development in Higher Education (Канада), Університет Калгарі. (2015-2021). 3. Учасних проєкту Еразмус+ Модуль Жана Моне EDEBUT (2023-2026) 4. Учасник проєкту COST Action UniDive: Universality and Diversity in Language Technology – 2023-2028. 13) проведення навчальних занять із спеціальних дисциплін іноземною мовою (крім дисциплін мовної підготовки) в обсязі не

							менше 50 аудиторних годин на навчальний рік Цифрова філологія – 100 годин 14) керівництво студентом, який зайняв призове місце на І або ІІ етапі Всеукраїнської студентської олімпіади (Всеукраїнського конкурсу студентських наукових робіт), або робота у складі організаційного комітету / журі Всеукраїнської студентської олімпіади (Всеукраїнського конкурсу студентських наукових робіт), або керівництво постійно діючим студентським науковим гуртком / проблемною групою; керівництво студентом, який став призером або лауреатом Міжнародних, Всеукраїнських мистецьких конкурсів, фестивалів та проектів, робота у складі організаційного комітету або у складі журі міжнародних, всеукраїнських мистецьких конкурсів, інших культурно-мистецьких проектів (для забезпечення провадження освітньої діяльності на третьому (освітньо-творчому) рівні); керівництво здобувачем, який став призером або лауреатом міжнародних мистецьких конкурсів, фестивалів, віднесених до Європейської або Всесвітньої (Світової) асоціації мистецьких конкурсів, фестивалів, робота у складі організаційного комітету або у складі журі зазначених мистецьких конкурсів, фестивалів); керівництво студентом, який брав участь в Олімпійських, Паралімпійських іграх, Всесвітній та Всеукраїнській Універсіаді, чемпіонаті світу, Європи, Європейських іграх, етапах Кубка світу та Європи, чемпіонаті України;

							виконання обов'язків тренера, помічника тренера національної збірної команди України з видів спорту; виконання обов'язків головного секретаря, головного судді, судді міжнародних та всеукраїнських змагань; керівництво спортивною делегацією; робота у складі організаційного комітету, суддівського корпусу Кононенко Катерина Ігорівна, Прикладна лінгвістика, 2020 - І місце, І етап Всеукраїнського конкурсу студентських наукових робіт 19) діяльність за спеціальністю у формі участі у професійних та/або громадських об'єднаннях 1. Член Коаліції цифрової трансформації суспільства (з 2019р.) 2. Член European Association of Digital Humanities (з 2020 р.) Відомості про підвищення кваліфікації 1. Tallinn Technological University, Estonia, сертифікат б/н. E-governance and public communication project seminar, (20-22.09.2022). 06.12.2022. 1 кредит ЄКТС (30 годин). 2. Відділ з питань освіти і культури Посольства Китайської Народної республіки в Україні, Інститут Конфуція Київського національного університету імені Тараса Шевченка, Українська асоціація викладачів китайської мови. Сертифікат № 011/021. Стажування за програмою підвищення кваліфікації викладачів китайської мови на тему: «Сучасні технології навчання китайської мови та літератури в закладах вищої освіти України», 13.11.2021 р.; 180 годин/ 6 кредитів ЄКТС
468593	Жданова Юлія	Доцент, Основне	Факультет інформаційних	Диплом спеціаліста,	27	Математичні методи	Відповідність освіти: 1.Ворошиловградськи

	Дмитрівна	місце роботи	технологій та математики	Ворошиловоградський державний інститут ім. Т.Г. Шевченка, рік закінчення: 1981, спеціальність: , Диплом спеціаліста, Державний університет телекомунікацій, рік закінчення: 2017, спеціальність: 7.17010101 безпека інформаційних і комунікаційних систем, Диплом кандидата наук КН 001399, виданий 29.12.1992, Атестат доцента 02ДЦ 015758, виданий 15.12.2005		криптографії	й державний педагогічний інститут імені Т.Г. Шевченка, 1981р., спеціальність – математика, кваліфікація – викладач математики; 2. Державний університет телекомунікацій, 2017р., спеціальність: «Безпека інформаційних і комунікаційних систем», кваліфікація: «Інженер із захисту інформації в інформаційних і комунікаційних системах» 3. Кандидат фізико-математичних наук, 1992р. 01.01.05 - Теорія ймовірностей і математична статистика. Тема дисертації: «Випадкові блукання та випадкові еволюції на скінченних розв'язуваних групах» 4. Доцент кафедри вищої математики, 2005р. Наявність публікацій за профілем дисципліни у періодичних наукових виданнях, що включені до переліку фахових видань України, до наукометричних баз, зокрема Scopus, Web of Science Core Collection: 1. Астапеня, Володимир Михайлович та Жданова, Юлія Дмитрівна та Шевченко, Світлана Миколаївна та Спасітєлєва, Світлана Олексіївна та Криворучко, О.В. (2024) Conflict Model of Radio Engineering Systems under the Threat of Electronic Warfare Proceedings of the Workshop Cybersecurity Providing in Information and Telecommunication Systems (CPITS 2024), 3654. с. 290-300. ISSN 1613-0073 (Scopus). 2. Шевченко, Світлана Миколаївна та Жданова, Юлія Дмитрівна та Астапеня, Володимир Михайлович та Негоденко, О.В. та Спасітєлєва, Світлана Олексіївна (2024) Conflicting Subsystems in the Information Space: A Study at the Software and Hardware

							Levels Proceedings of the Workshop Cybersecurity Providing in Information and Telecommunication Systems 2024, 3654. с. 333-342. ISSN 1613-0073 (Scopus). 3. Shevchenko, Svitlana та Zhdanova, Yuliia та Shevchenko, Halyna та Nehodenko, Olena та Spasiteleva, Svitlana (2023) Information Security Risk Management using Cognitive Modeling Cybersecurity Providing in Information and Telecommunication Systems, 3550. с. 297-305. ISSN 1613-0073 (Scopus). 4. Жданова Ю.Д. Математичні методи в кібербезпеці: теорія катастроф / С.М. Шевченко, Ю.Д. Жданова, С.О. Спасітєлєва // Кібербезпека: освіта, наука, техніка. – 2023, Том 3, № 19. – С. 165-175. 5. Zhdanova Yu. Conflict Analysis in the “Subject-to-Subject” Security System / S. Shevchenko, Y. Zhdanova, H. Shevchenko, O. Nehodenko, and S.Spasiteleva // CEUR Workshop Proceedings. 2023. V. 3421. 56–66. (Scopus). 6. Zhdanova Yu. Protection of Information in Telecommunication Medical Systems based on a Risk-Oriented Approach / S. Shevchenko, Y. Zhdanova, Yu. Dreis, R. Kyrychok, and D.Tsyrkaniuk // CEUR Workshop Proceedings. 2023. V. 3421. 158–167. (Scopus). 7. Жданова Ю.Д. Розробка безпечних контейнерних застосунків з мікросервісною архітектурою / С.О. Спасітєлєва, І.В. Чичкань, Ю.Д. Жданова, С.М. Шевченко // Кібербезпека: освіта, наука, техніка. – 2023, Том 1, № 21. – С. 193-210. 8. Grechaninov, Viktor та Khoshaba, Oleksandr та Hulak, Hennadii та Zhdanova, Yuliia та Melnyk, Iryna (2022) Models and Methods for

							Determining Application Performance Estimates in Distributed Structures Cybersecurity Providing in Information and Telecommunication Systems 2022, 3288 (1). с. 134-141. ISSN 1613-0073 (Scopus). 9. Dreis, Yurii та Ivanichenko, Yevhen та Nesterova, Olena та Zhdanova, Yuliia та Dmytriienko, Kate (2022) Restricted Information Identification Model Cybersecurity Providing in Information and Telecommunication Systems 2022, 3288 (1). с. 89-95. ISSN 1613-007 (Scopus). 10. Жданова Ю.Д. Інсайдери та інсайдерська інформація: суть, загрози, діяльність та правова відповідальність / С.М. Шевченко, Ю.Д. Жданова, П.М. Складанний, С.В. Бойко // Кібербезпека: освіта, наука, техніка. – 2022, Том 3, № 15. – С. 175-185. 11. Жданова Ю.Д. Уразливості шифрування коротких повідомлень в мобільних інформаційно-комунікаційних системах об'єктів критичної інфраструктури / Г.М. Гулак, Ю.Д. Жданова, П.М. Складанний, Є.Г. Гулак, В.А. Корнієць // Кібербезпека: освіта, наука, техніка. – 2022, Том 1, № 17. – С. 145-158. 12. H. Shevchenko, S. Shevchenko, Yu. Zhdanova, S. Spasiteleva, O. Negodenko. Information Security Risk Analysis SWOT. CEUR Workshop Proceedings. 2021. V. 2923. 309–317 (Scopus). 13. Жданова Ю.Д. Міждисциплінарний підхід до формування навичок управління ризиками ІБ на засадах теорії прийняття рішень / В.Л. Бурячок, Ю.Д. Жданова, С.М. Шевченко, П.М. Складанний // Кібербезпека: освіта, наука, техніка. – 2021,

							Том 3, № 11. – С. 155-165. 14. Жданова Ю.Д. Прикладні та методичні аспекти застосування хеш-функцій в інформаційній безпеці / Ю.Д. Жданова, С.О. Спасітєлєва, С.М. Шевченко, К.В. Кравчук // Кібербезпека: освіта, наука, техніка. – 2020, Том 4, № 8. – С.85-96. 15. Жданова Ю.Д. Проведення SWOT-аналізу оцінювання інформаційних ризиків як засіб формування практичних навичок студентів спеціальності 125 Кібербезпека / Ю.Д. Жданова, С.М. Шевченко, С.О. Спасітєлєва, П.М. Складанний // Кібербезпека: освіта, наука, техніка. – 2020, Том 2, № 10. – С. 158-168. Наявність виданого підручника чи навчального посібника (включаючи електронні) або монографії 1. Модель експертної системи для медичного скринінгу на основі методів кластерного аналізу / С.М. Шевченко, Ю.Д. Жданова, О.В. Негоденко, В.А. Куцук // Moderní aspekty vědy: XXVII. Díl mezinárodní kolektivní monografie / Mezinárodní Ekonomický Institut s.r.o. Česká republika: Mezinárodní Ekonomický Institut s.r.o., 2023. str. 495. – 478-494. 2. Теоретико-ймовірнісні та статистичні методи в захисті інформації. Підручник для студентів спеціальності 125 Кібербезпека / В.М. Астапеня, Ю.Д. Жданова, С.М. Шевченко. – К. Київський університет ім. Б.Грінченка. 2023. Наявність виданих навчально-методичних посібників/посібників для самостійної роботи здобувачів вищої освіти та дистанційного

							навчання, електронних курсів на освітніх платформах: 1. Електронний навчальний курс з дисципліни «Прикладна загальна теорія систем безпеки» для магістрів спеціальності 125 Кібербезпека та захист інформації денної форми навчання. 2. Електронний навчальний курс з дисципліни «Прикладна криптологія» для бакалаврів спеціальності 125 Кібербезпека та захист інформації денної форми навчання. 3. Електронний навчальний курс з дисципліни «Прийняття рішень в інформаційній і кібербезпеці» для бакалаврів спеціальності 125 та захист інформації Кібербезпека денної форми навчання. 4. Електронний навчальний курс з дисципліни «Вища математика: Математичний наліз та чисельні методи» для бакалаврів спеціальності 125 Кібербезпека та захист інформації денної форми навчання. 5. Електронний навчальний курс з дисципліни «Вища математика» для бакалаврів спеціальності 123 Комп'ютерна інженерія денної форми навчання. 6. Методичні рекомендації до виконання та захисту кваліфікаційної роботи бакалавра для студентів спеціальності 125 Кібербезпека освітньої програми 125.00.01 Безпека інформаційних і комунікаційних систем / Укладачі: Жданова Ю.Д., Шевченко С.М., Складанний П.М. – Київ: КУБГ. 2023. – 51 с. 7. Методичні рекомендації до виконання та захисту кваліфікаційної роботи магістра для студентів спеціальності 125 Кібербезпека та захист

							інформації освітньої програми 125.00.01 Безпека інформаційних і комунікаційних систем / Укладачі: Жданова Ю. Д., Складанний П. М., Шевченко С. М. – Київ: КУБГ, 2023. –57 с. Наявність апробаційних та/або науково-популярних, та/або консультаційних (дорадчих), та/або науково-експертних публікацій з наукової або професійної тематики: 1. Шевченко, Світлана Миколаївна та Жданова, Юлія Дмитрівна та Шевченко, Галина Володимирівна та Негоденко, Олена Василівна та Спасітєлєва, Світлана Олексіївна (2023) Conflict Analysis in the Information Security System: Subject - Subject CEUR Workshop Proceedings., 3421. с. 56-66. ISSN 1613-0073 2. Шевченко, Світлана Миколаївна та Жданова, Юлія Дмитрівна та Дрейс, Юрій Олександрович та Киричок, Роман Васильович та Цирканюк, Діана Андріївна (2023) Protection of Information in Telecommunication Medical Systems based on a Risk-Oriented Approach CEUR Workshop Proceedings. 2023. (3421). с. 158-167. ISSN 1613-0073 3. Shevchenko, Svitlana та Zhdanova, Yuliia та Shevchenko, Halyna та Nehodenko, Olena та Spasiteleva, Svitlana (2023) Information Security Risk Management using Cognitive Modeling Cybersecurity Providing in Information and Telecommunication Systems, 3550. с. 297-305. ISSN 1613-0073 4. Grechaninov, Viktor та Khoshaba, Oleksandr та Hulak, Hennadii та Zhdanova, Yuliia та Melnyk, Iryna (2022) Models and Methods for Determining Application Performance Estimates in Distributed

							Structures Cybersecurity Providing in Information and Telecommunication Systems 2022, 3288 (1). с. 134-141. ISSN 1613-0073 5. Dreis, Yurii та Ivanichenko, Yevhen та Nesterova, Olena та Zhdanova, Yuliia та Dmytriienko, Kate (2022) Restricted Information Identification Model Cybersecurity Providing in Information and Telecommunication Systems 2022, 3288 (1). с. 89-95. ISSN 1613-0073 6. Жданова Ю.Д., Шевченко С.М. Аналіз шляхів забезпечення кібербезпеки у віртуальному навчальному середовищі. Управління науковими та освітніми проєктами: матеріали всеукраїнського науково-педагогічного підвищення кваліфікації, 24 січня – 6 березня 2022 року. – Одеса: Видавничий дім «Гельветика», 2022. – 328 с. – С.133-136. 7. Жданова Ю.Д., Спасітєлєва С.О., Шевченко С.М. Активні методи навчання у вивченні ризиків інформаційної безпеки. Математика в сучасному технічному університеті : Матеріали IX Міжнар. наук.-практ. конф. «Математика в сучасному технічному університеті», Київ, 28–29 грудня 2020 р. — Вінниця: Видавець ФОП Кушнір Ю. В., 2021. – 330 с.– С.291-294. 8. Жданова Ю.Д., Спасітєлєва С.О., Шевченко С.М. Особливості застосування технологій захисту інформації в корпоративних освітніх мережах. Теоретико-практичні проблеми використання математичних методів і комп'ютерно-орієнтованих технологій в освіті та науці: зб. матеріалів III Всеукраїнської науково-практичної

							конференції, 28 квітня 2021 р., м. Київ / Київ. ун-т ім. Б. Грінченка. – К.: Київ. ун-т ім. Б. Грінченка, 2021. – 203 с. – С. 183-185. Діяльність за спеціальністю у формі участі у професійних та/або громадських об'єднаннях Член "Internet Society (IS): Reston, VA, US" Відомості про підвищення кваліфікації: 1. Підвищення кваліфікації науково-педагогічних працівників Університету за модулем «ІКТ». Київський університет імені Бориса Грінченка, 13.04.2020-25.04.2020. 30 год. (сертифікат № 1299 від 04.05.2020). 2. Підвищення кваліфікації науково-педагогічних працівників Університету за Лідерським модулем. Київський університет імені Бориса Грінченка, 18.02.2021-26.02.2021. 30 год. (сертифікат № 1510/41 від 05.03.2021). 3. Всеукраїнське науково-педагогічне підвищення кваліфікації «Управління науковими та освітніми проєктами» 24.01.2022-06.03.2022. 180 год. (сертифікат №ADV-240170-OLA від 06.03.2022). 4. Інститут телекомунікацій і глобального інформаційного простору НАН України, відділ інформаційної безпеки, овідка про проходження стажування № 161/12.05.2023-4, тема: «Криптографія з багатьма змінними, пов'язана з використанням алгебраїчної комбінаторики», від 10.05.2023 р., 4 кредити ЄКТС (120 годин) 5. Програма підвищення кваліфікації «Цифрові технології в наукових дослідженнях», 01.11 2023-13.12.2023, 60

							год. (сертифікат №20231213/171 від 13.12.2023).
468938	Соколов Володимир Юрійович	Доцент, Основне місце роботи	Факультет інформаційних технологій та математики	Диплом магістра, Національний технічний університет України "Київський політехнічний інститут", рік закінчення: 2005, спеціальність: 090803 Електронні системи, Диплом кандидата наук ДК 055193, виданий 16.12.2019, Атестат доцента АД 009225, виданий 30.11.2021	18	Технології протидії злоякісному програмному коду	Відповідність освіти: 1.Національний технічний університет України «Київський політехнічний інститут», 2005р. Спеціальність: «Електронні системи». Кваліфікація: магістр електроніки. 2.Кандидат технічних наук, 2019р. 05.13.06 – Інформаційні технології. Тема дисертації: «Методи і засоби підвищення інформаційної та функціональної безпеки безпроводових мереж передавання даних» 3.Доцент кафедри інформаційної та кібернетичної безпеки, 2021 р. Наявність публікацій за профілем дисципліни у періодичних наукових виданнях, що включені до переліку фахових видань України, до наукометричних баз, зокрема Scopus, Web of Science Core Collection: 1. Iavich, M. та Kovalchuk, O. та Gnatyuk, S. та Khavikova, Y. та Sokolov, Volodymyr (2024) Classical and post-quantum encryption for GDPR Classic, Quantum, and Post-Quantum Cryptography 2024, 3829. с. 70-78. ISSN 1613-0073 2. Kriuchkova, Larysa та Sokolov, Volodymyr та Skladannyi, Pavlo (2024) Determining the Zone of Successful Interaction in RFID Technologies 2024 IEEE 29th International Seminar/Workshop on Direct and Inverse Problems of Electromagnetic and Acoustic Wave Theory (DIPED). с. 168-171. ISSN 979-8-3315-0608-7 3. Bessalov, Anatoly та Sokolov, V. Y. та Abramov, Serhii (2024) Efficient Commutative PQC Algorithms on Isogenies of Edwards Curves Cryptography, 8 (3). с. 1-17. ISSN 2410-387X 4. Sokolov, Volodymyr

and Skladannyi, Pavlo and Platonenko, Artem (2023) Jump-Stay Jamming Attack on Wi-Fi Systems 2023 IEEE 18th International Conference on Computer Science and Information Technologies (CSIT). pp. 1-5. ISSN 2766-3639
5. Bessalov, Anatoly and Abramov, Serhii and Sokolov, Volodymyr and Skladannyi, Pavlo and Zhyltsov, Oleksii (2023) Multifunctional CRS Encryption Scheme on Isogenies of Non-Supersingular Edwards Curves Workshop on Classic, Quantum, and Post-Quantum Cryptography (CQPC 2023), 3504. pp. 12-25. ISSN 1613-0073
6. Marusenko, R. and Sokolov, V. Y. and Skladannyi, Pavlo (2023) Social Engineering Penetration Testing in Higher Education Institutions In: Lecture Notes on Data Engineering and Communications Technologies. Springer, pp. 1132-1147.
7. Buriachok, Volodymyr and Korshun, Natalia and Zhyltsov, Oleksii and Sokolov, Volodymyr and Skladannyi, Pavlo (2023) Implementation of Active Cybersecurity Education in Ukrainian Higher School Lecture Notes on Data Engineering and Communications Technologies, 178. pp. 533-551. ISSN 2367-4512
8. TajDini, Mahyar and Sokolov, V. Y. and Kuzminykh, Ievgeniia and Ghita, B. (2023) Brainwave-based authentication using features fusion Computers & Security (129). p. 103198. ISSN 0167-4048 9. Sokolov, Volodymyr and Skladannyi, Pavlo and Astapenya, Volodymyr (2023) Bluetooth Low-Energy Beacon Resistance to Jamming Attack 2023 IEEE 13th International Conference on Electronics and Information Technologies (ELIT). pp. 270-274. ISSN 979-8-3503-8309-6

							10. Bessalov, Anatoliy and Abramov, Serhii and Sokolov, Volodymyr and Mazur, Nataliia (2023) CSIKE-ENC Combined Encryption Scheme with Optimized Degrees of Isogeny Distribution Cybersecurity Providing in Information and Telecommunication Systems, 3421. pp. 36-45. ISSN 1613-0073 11. Kipchuk, F. and Sokolov, Volodymyr and Skladannyi, Pavlo and Zhyltsov, Oleksii and Ageyev, D. (2023) Method for Increasing the Various Sources Data Consistency for IoT Sensors IEEE 9th International Conference on Problems of Infocommunications, Science and Technology (PICST). pp. 522-526. ISSN 979-8-3503-9891-5 12. Abramov, Serhii and Bessalov, Anatoly and Sokolov, Volodymyr (2023) Properties of Isogeny Graph of Non-Cyclic Edwards Curves Cybersecurity Providing in Information and Telecommunication Systems, 3550. pp. 234-239. ISSN 1613-0073 13. Anakhov, P. and Zhebka, V. and Popereshnyak, S and Skladannyi, Pavlo and Sokolov, Volodymyr (2023) Protecting Objects of Critical Information Infrastructure from Wartime Cyber Attacks by Decentralizing the Telecommunications Network Cybersecurity Providing in Information and Telecommunication Systems, 3550. pp. 240-245. ISSN 1613-0073 14. Bahatskyi, Oleksii and Bahatskyi, V. and Sokolov, Volodymyr (2023) Smart Home Subsystem for Calculating the Quality of Public Utilities Cybersecurity Providing in Information and Telecommunication Systems, 3421. pp. 168-173. ISSN 1613-0073 Наявність виданого підручника чи навчального посібника (включаючи електронні) або монографії 1. Hu, Z. B. Deduplication Method

							for Ukrainian Last Names, Medicinal Names, and Toponyms Based on Metaphone Phonetic Algorithm / Z. B. Hu, V. Buriachok, V. Sokolov // Advances in Computer Science for Engineering and Education III. — Vol. 1247. — Cham : Springer, 2020. — P. 518–533. [Колективна монографія. Індексується в Scopus.] 2. Marusenko, R. Experimental Evaluation of Phishing Attack on High School Students / R. Marusenko, V. Sokolov, V. Buriachok // Advances in Computer Science for Engineering and Education III. — Vol. 1247. — Cham : Springer, 2020. — P. 668–680. [Колективна монографія. Індексується в Scopus.] 3. Sokolov, V. Development of Low-Budget Spectrum Analyzers for IoT and Sensor Networks / V. Sokolov, A. Platonenko, L. Kuzmenko, V. Buriachok // Projektowanie, badania i eksploatacja. — Bielsku-Białej : NATH, 2020. — P. 331–342. [Колективна монографія.] 4. Бурячок, В. Л. Безпека безпроводових і мобільних мереж : Навчальний посібник / В. Л. Бурячок, В. Ю. Соколов, М. М. Таджділі. — 2 вид., доп. — К. : КУБГ, 2020. — 144 с. [Посібник.] Наявність виданих навчально-методичних посібників/посібників для самостійної роботи здобувачів вищої освіти та дистанційного навчання, електронних курсів на освітніх платформах: 1. Електронний навчальний курс з дисципліни Основи ОС та сучасних Інтернет-технологій (1 курс, 1р ВО, БІКС, очна). Освітньо-професійна програма 125.00.01 Безпека інформаційних та комунікаційних систем (2019, 2023). Бакалавр. (Наказ №

							448 від 30.06.2021; Наказ № 786 від 04.12.2023 (пролонгація 2023/24 н.р.)). 2. Електронний навчальний курс з дисципліни Інформаційне право (2 курс, КІ, денна). Освітньо-професійна програма 123.00.01 Комп'ютерна інженерія (2022). Бакалавр. (Наказ № 420 від 02.05.2024) Участь в атестації наукових кадрів як офіційного опонента або члена постійної спеціалізованої вченої ради, або члена не менше трьох разових спеціалізованих вчених рад 1. Разова спеціалізована вчена рада ДФ 26.133.056 (13.02.2024, Київський столичний університет імені Бориса Грінченка) з правом прийняття до розгляду та проведення захисту дисертації Ворохоба Максима Віталійовича з метою присудження ступеня доктора філософії з галузі знань 12 Інформаційні технології за спеціальністю 125 Кібербезпека та захист інформації — рецензент. 2. Разова спеціалізована вчена рада ДФ 26.002.132 (06.06.2024, Національний технічний університет України «Київський політехнічний інститут імені Ігоря Сікорського») з правом прийняття до розгляду та проведення захисту дисертації Головатенка Іллі Анатолійовича з метою присудження ступеня доктора філософії з галузі знань 12 Інформаційні технології за спеціальністю 126 Інформаційні системи та технології — офіційний опонент. 3. Разова спеціалізована вчена рада ДФ 26.133.062 (12.06.2024, Київський столичний університет імені Бориса Грінченка) з правом прийняття до розгляду та проведення захисту

							дисертації Черненка Романа Миколайовича з метою присудження ступеня доктора філософії з галузі знань 12 Інформаційні технології за спеціальністю 125 Кібербезпека та захист інформації — рецензент. 4. Разова спеціалізована вчена рада ДФ 26.002.160 (27.06.2024, Національний технічний університет України «Київський політехнічний інститут імені Ігоря Сікорського») з правом прийняття до розгляду та проведення захисту дисертації Нікітіна Валерія Андрійовича з метою присудження ступеня доктора філософії з галузі знань 12 Інформаційні технології за спеціальністю 126 Інформаційні системи та технології — офіційний опонент. 5. Разова спеціалізована вчена рада 133 (13.08.2024, Національний університет «Львівська політехніка») з правом прийняття до розгляду та проведення захисту дисертації Курія Євгенія Олеговича з метою присудження ступеня доктора філософії з галузі знань 12 Інформаційні технології за спеціальністю 125 Кібербезпека — офіційний опонент. 6. Разова спеціалізована вчена рада 132 (13.08.2024, Національний університет «Львівська політехніка») з правом прийняття до розгляду та проведення захисту дисертації Журавчака Даниїла Юрійовича з метою присудження ступеня доктора філософії з галузі знань 12 Інформаційні технології за спеціальністю 125 Кібербезпека — офіційний опонент. Виконання функцій (повноважень, обов'язків) наукового керівника або відповідального

							виконавця наукової теми (проекту), або головного редактора/члена редакційної колегії/експерта (рецензента) наукового видання, включеного до переліку фахових видань України, або іноземного наукового видання, що індексується в бібліографічних базах 1. Член редакційної колегії електронного фахового наукового видання «Кібербезпека: освіта, наука, техніка» (електронне видання). 2. Член редакційної колегії електронного міжнародного наукового видання «International Journal of Wireless and Microwave Technologies» (електронне видання). 3. Член організаційного комітету міжнародної конференції «IEEE International Scientific-Practical Conference on Problems of Infocommunications Science and Technology» (індексується в Scopus). 4. Головний редактор міжнародної конференції «Workshop on Cybersecurity Providing in Information and Telecommunication Systems» (індексується в Scopus). 5. Редактор міжнародної конференції «Workshop on Classic, Quantum, and Post-Quantum Cryptography» (індексується в Scopus). 6. Член організаційного комітету міжнародної конференції «International Conference on Computer Science, Engineering and Education Applications» (індексується в Scopus). Участь у міжнародних наукових та/або освітніх проектах, залучення до міжнародної експертизи, наявність звання «суддя

							міжнародної категорії» 1. 01.02.2023–31.05.2023 «Development of DAO-modules for the DAO economic system» (XGROUP GLOBAL PTE Ltd., Сінгапур). 2. 01.08.2023–31.07.2024 «Research of Speech Emotion Recognition» (№89-080123, Ender Turing OÜ, Таллінн, Естонія). Діяльність за спеціальністю у формі участі у професійних та/або громадських об'єднаннях 1. Член «European Microwave Assosiation (EuMA)» (№ AM3734, з 2019 до 2026 р.). 2. Член «International Telecommunication Union (ITU-T)» (№ 1200190674, з 2017 до 2021 р.). Досвід практичної роботи за спеціальністю не менше п'яти років (крім педагогічної, науково-педагогічної, наукової діяльності) 1. Senior System Analyst / Proxy Product Owner (09.2022–07.2023, Pivotal Commware, США). 2. Senior System Analyst (08.2021–02.2022, Raiffeisen Bank, Україна). 3. Business Analyst (03.2020–07.2021, Competo, Азербайджан). Відомості про підвищення кваліфікації: 1.Підвищення кваліфікації науково-педагогічних працівників Університету за Дослідницьким модулем (поглиблений рівень). Київський університет імені Бориса Грінченка, 22.10.2021-30.11.2021. 30 год. (сертифікат № 1766/41 від 03.12.2021). 2. Інститут телекомунікацій та глобального інформаційного простору НАН України. Довідка № 161/24.05.2023-3. Тема: Створення нових LDPC кодів супутникового зв'язку за екстремальними графами. Від 24.05.2023р. 120

							годин (4 кредити ЄКТС). 3. Підвищення кваліфікації науково-педагогічних працівників Університету за Цифровим модулем. Київський університет імені Бориса Грінченка, 30 год. (наказ № 842 від 25.12.2023).
468938	Соколов Володимир Юрійович	Доцент, Основне місце роботи	Факультет інформаційних технологій та математики	Диплом магістра, Національний технічний університет України "Київський політехнічний інститут", рік закінчення: 2005, спеціальність: 090803 Електронні системи, Диплом кандидата наук ДК 055193, виданий 16.12.2019, Атестат доцента АД 009225, виданий 30.11.2021	18	Технології розробки і тестування ПЗ мережевої безпеки	Відповідність освіти: 1.Національний технічний університет України «Київський політехнічний інститут», 2005р. Спеціальність: «Електронні системи». Кваліфікація: магістр електроніки. 2.Кандидат технічних наук, 2019р. 05.13.06 – Інформаційні технології. Тема дисертації: «Методи і засоби підвищення інформаційної та функціональної безпеки безпроводових мереж передавання даних» 3.Доцент кафедри інформаційної та кібернетичної безпеки, 2021 р. Наявність публікацій за профілем дисципліни у періодичних наукових виданнях, що включені до переліку фахових видань України, до наукометричних баз, зокрема Scopus, Web of Science Core Collection: 1. Iavich, M. та Kovalchuk, O. та Gnatyuk, S. та Khavikova, Y. та Sokolov, Volodymyr (2024) Classical and post-quantum encryption for GDPR Classic, Quantum, and Post-Quantum Cryptography 2024, 3829. c. 70-78. ISSN 1613-0073 2. Kriuchkova, Larysa та Sokolov, Volodymyr та Skladannyi, Pavlo (2024) Determining the Zone of Successful Interaction in RFID Technologies 2024 IEEE 29th International Seminar/Workshop on Direct and Inverse Problems of Electromagnetic and Acoustic Wave Theory (DIPED). c. 168-171.

ISSN 979-8-3315-0608-7
3. Bessalov, Anatoly та Sokolov, V. Y. та Abramov, Serhii (2024) Efficient Commutative PQC Algorithms on Isogenies of Edwards Curves Cryptography, 8 (3). с. 1-17. ISSN 2410-387X
4. Sokolov, Volodymyr and Skladannyi, Pavlo and Platonenko, Artem (2023) Jump-Stay Jamming Attack on Wi-Fi Systems 2023 IEEE 18th International Conference on Computer Science and Information Technologies (CSIT). pp. 1-5. ISSN 2766-3639
5. Bessalov, Anatoly and Abramov, Serhii and Sokolov, Volodymyr and Skladannyi, Pavlo and Zhyltsov, Oleksii (2023) Multifunctional CRS Encryption Scheme on Isogenies of Non-Supersingular Edwards Curves Workshop on Classic, Quantum, and Post-Quantum Cryptography (CQPC 2023), 3504. pp. 12-25. ISSN 1613-0073
6. Marusenko, R. and Sokolov, V. Y. and Skladannyi, Pavlo (2023) Social Engineering Penetration Testing in Higher Education Institutions In: Lecture Notes on Data Engineering and Communications Technologies. Springer, pp. 1132-1147.
7. Buriachok, Volodymyr and Korshun, Natalia and Zhyltsov, Oleksii and Sokolov, Volodymyr and Skladannyi, Pavlo (2023) Implementation of Active Cybersecurity Education in Ukrainian Higher School Lecture Notes on Data Engineering and Communications Technologies, 178. pp. 533-551. ISSN 2367-4512
8. TajDini, Mahyar and Sokolov, V. Y. and Kuzminykh, Ievgeniia and Ghita, B. (2023) Brainwave-based authentication using features fusion Computers & Security (129). p. 103198. ISSN 0167-4048 9. Sokolov, Volodymyr and Skladannyi, Pavlo and

Astapenya, Volodymyr (2023) Bluetooth Low-Energy Beacon Resistance to Jamming Attack 2023 IEEE 13th International Conference on Electronics and Information Technologies (ELIT). pp. 270-274. ISSN 979-8-3503-8309-6
10. Bessalov, Anatoliy and Abramov, Serhii and Sokolov, Volodymyr and Mazur, Nataliia (2023) CSIKE-ENC Combined Encryption Scheme with Optimized Degrees of Isogeny Distribution Cybersecurity Providing in Information and Telecommunication Systems, 3421. pp. 36-45. ISSN 1613-0073 11. Kipchuk, F. and Sokolov, Volodymyr and Skladannyi, Pavlo and Zhyltsov, Oleksii and Ageyev, D. (2023) Method for Increasing the Various Sources Data Consistency for IoT Sensors IEEE 9th International Conference on Problems of Infocommunications, Science and Technology (PICST). pp. 522-526. ISSN 979-8-3503-9891-5 12. Abramov, Serhii and Bessalov, Anatoly and Sokolov, Volodymyr (2023) Properties of Isogeny Graph of Non-Cyclic Edwards Curves Cybersecurity Providing in Information and Telecommunication Systems, 3550. pp. 234-239. ISSN 1613-0073
13. Anakhov, P. and Zhebka, V. and Popereshnyak, S and Skladannyi, Pavlo and Sokolov, Volodymyr (2023) Protecting Objects of Critical Information Infrastructure from Wartime Cyber Attacks by Decentralizing the Telecommunications Network Cybersecurity Providing in Information and Telecommunication Systems, 3550. pp. 240-245. ISSN 1613-0073
14. Bahatskyi, Oleksii and Bahatskyi, V. and Sokolov, Volodymyr (2023) Smart Home Subsystem for Calculating the Quality of Public Utilities Cybersecurity Providing in Information and

							Telecommunication Systems, 3421. pp. 168-173. ISSN 1613-0073 Наявність виданого підручника чи навчального посібника (включаючи електронні) або монографії 1. Hu, Z. B. Deduplication Method for Ukrainian Last Names, Medicinal Names, and Toponyms Based on Metaphone Phonetic Algorithm / Z. B. Hu, V. Buriachok, V. Sokolov // Advances in Computer Science for Engineering and Education III. — Vol. 1247. — Cham : Springer, 2020. — P. 518–533. [Колективна монографія. Індексується в Scopus.] 2. Marusenko, R. Experimental Evaluation of Phishing Attack on High School Students / R. Marusenko, V. Sokolov, V. Buriachok // Advances in Computer Science for Engineering and Education III. — Vol. 1247. — Cham : Springer, 2020. — P. 668–680. [Колективна монографія. Індексується в Scopus.] 3. Sokolov, V. Development of Low-Budget Spectrum Analyzers for IoT and Sensor Networks / V. Sokolov, A. Platonenko, L. Kuzmenko, V. Buriachok // Projektowanie, badania i eksploatacja. — Bielsku-Białej : NATH, 2020. — P. 331–342. [Колективна монографія.] 4. Бурячок, В. Л. Безпека безпроводових і мобільних мереж : Навчальний посібник / В. Л. Бурячок, В. Ю. Соколов, М. М. Тадждіні. — 2 вид., доп. — К. : КУБГ, 2020. — 144 с. [Посібник.] Наявність виданих навчально-методичних посібників/посібників для самостійної роботи здобувачів вищої освіти та дистанційного навчання, електронних курсів на освітніх платформах: 1. Електронний

							навчальний курс з дисципліни Основи ОС та сучасних Інтернет-технологій (1 курс, 1р ВО, БІКС, очна). Освітньо-професійна програма 125.00.01 Безпека інформаційних та комунікаційних систем (2019, 2023). Бакалавр. (Наказ № 448 від 30.06.2021; Наказ № 786 від 04.12.2023 (пролонгація 2023/24 н.р.)). 2. Електронний навчальний курс з дисципліни Інформаційне право (2 курс, КІ, денна). Освітньо-професійна програма 123.00.01 Комп'ютерна інженерія (2022). Бакалавр. (Наказ № 420 від 02.05.2024) Участь в атестації наукових кадрів як офіційного опонента або члена постійної спеціалізованої вченої ради, або члена не менше трьох разових спеціалізованих вчених рад 1. Разова спеціалізована вчена рада ДФ 26.133.056 (13.02.2024, Київський столичний університет імені Бориса Грінченка) з правом прийняття до розгляду та проведення захисту дисертації Ворохоба Максима Віталійовича з метою присудження ступеня доктора філософії з галузі знань 12 Інформаційні технології за спеціальністю 125 Кібербезпека та захист інформації — рецензент. 2. Разова спеціалізована вчена рада ДФ 26.002.132 (06.06.2024, Національний технічний університет України «Київський політехнічний інститут імені Ігоря Сікорського») з правом прийняття до розгляду та проведення захисту дисертації Головатенка Іллі Анатолійовича з метою присудження ступеня доктора філософії з галузі знань 12 Інформаційні технології за спеціальністю 126 Інформаційні системи

							та технології — офіційний опонент. 3. Разова спеціалізована вчена рада ДФ 26.133.062 (12.06.2024, Київський столичний університет імені Бориса Грінченка) з правом прийняття до розгляду та проведення захисту дисертації Черненка Романа Миколайовича з метою присудження ступеня доктора філософії з галузі знань 12 Інформаційні технології за спеціальністю 125 Кібербезпека та захист інформації — рецензент. 4. Разова спеціалізована вчена рада ДФ 26.002.160 (27.06.2024, Національний технічний університет України «Київський політехнічний інститут імені Ігоря Сікорського») з правом прийняття до розгляду та проведення захисту дисертації Нікітіна Валерія Андрійовича з метою присудження ступеня доктора філософії з галузі знань 12 Інформаційні технології за спеціальністю 126 Інформаційні системи та технології — офіційний опонент. 5. Разова спеціалізована вчена рада 133 (13.08.2024, Національний університет «Львівська політехніка») з правом прийняття до розгляду та проведення захисту дисертації Курія Євгенія Олеговича з метою присудження ступеня доктора філософії з галузі знань 12 Інформаційні технології за спеціальністю 125 Кібербезпека — офіційний опонент. 6. Разова спеціалізована вчена рада 132 (13.08.2024, Національний університет «Львівська політехніка») з правом прийняття до розгляду та проведення захисту дисертації Журавчака Даниїла Юрійовича з метою присудження

							ступеня доктора філософії з галузі знань 12 Інформаційні технології за спеціальністю 125 Кібербезпека — офіційний опонент. Виконання функцій (повноважень, обов'язків) наукового керівника або відповідального виконавця наукової теми (проекту), або головного редактора/члена редакційної колегії/експерта (рецензента) наукового видання, включеного до переліку фахових видань України, або іноземного наукового видання, що індексується в бібліографічних базах 1. Член редакційної колегії електронного фахового наукового видання «Кібербезпека: освіта, наука, техніка» (електронне видання). 2. Член редакційної колегії електронного міжнародного наукового видання «International Journal of Wireless and Microwave Technologies» (електронне видання). 3. Член організаційного комітету міжнародної конференції «IEEE International Scientific-Practical Conference on Problems of Infocommunications Science and Technology» (індексується в Scopus). 4. Головний редактор міжнародної конференції «Workshop on Cybersecurity Providing in Information and Telecommunication Systems» (індексується в Scopus). 5. Редактор міжнародної конференції «Workshop on Classic, Quantum, and Post-Quantum Cryptography» (індексується в Scopus). 6. Член організаційного комітету міжнародної конференції «International Conference on Computer Science,

							Engineering and Education Applications» (індексується в Scopus). Участь у міжнародних наукових та/або освітніх проектах, залучення до міжнародної експертизи, наявність звання «суддя міжнародної категорії» 1. 01.02.2023–31.05.2023 «Development of DAO-modules for the DAO economic system» (XGROUP GLOBAL PTE Ltd., Сінгапур). 2. 01.08.2023–31.07.2024 «Research of Speech Emotion Recognition» (№89-080123, Ender Turing OÜ, Таллінн, Естонія). Діяльність за спеціальністю у формі участі у професійних та/або громадських об'єднаннях 1. Член «European Microwave Assosiation (EuMA)» (№ AM3734, з 2019 до 2026 р.). 2. Член «International Telecommunication Union (ITU-T)» (№ 1200190674, з 2017 до 2021 р.). Досвід практичної роботи за спеціальністю не менше п'яти років (крім педагогічної, науково-педагогічної, наукової діяльності) 1. Senior System Analyst / Proxy Product Owner (09.2022–07.2023, Pivotal Commware, США). 2. Senior System Analyst (08.2021–02.2022, Raiffeisen Bank, Україна). 3. Business Analyst (03.2020–07.2021, Competo, Азербайджан). Відомості про підвищення кваліфікації: 1.Підвищення кваліфікації науково-педагогічних працівників Університету за Дослідницьким модулем (поглиблений рівень). Київський університет імені Бориса Грінченка, 22.10.2021-30.11.2021. 30 год. (сертифікат № 1766/41 від 03.12.2021). 2. Інститут

							телекомунікацій та глобального інформаційного простору НАН України. Довідка № 161/24.05.2023-3. Тема: Створення нових LDPC кодів супутникового зв'язку за екстремальними графами. Від 24.05.2023р. 120 годин (4 кредити ЄКТС). 3. Підвищення кваліфікації науково-педагогічних працівників Університету за Цифровим модулем. Київський університет імені Бориса Грінченка, 30 год. (наказ № 842 від 25.12.2023).
468580	Аносов Андрій Олександрович	Доцент, Основне місце роботи	Факультет інформаційних технологій та математики	Диплом спеціаліста, Вороніжське вище військове інженерне училище радіоелектроніки, рік закінчення: 1988, спеціальність: Командно-тактична, радіоелектронні засоби, Диплом магістра, Національна академія оборони України, рік закінчення: 1999, спеціальність: Організація бойового та оперативного забезпечення військ (сил), Диплом кандидата наук ДК 029855, виданий 30.06.2005, Атестат доцента 12ДЦ 044758, виданий 15.12.2015	41	Моніторинг, аудит та адміністрування захищених ІТ систем і мереж	Відповідність освіти: 1.Воронізьке вище воєнне інженерне училище радіоелектроніки, 1988р. Спеціальність: «Командно-тактична, радіоелектронні засоби». Кваліфікація: «Радіо-інженер». 1.Національний академія оборони України, 1999р. Спеціальність: «Організація бойового та оперативного забезпечення військ (сил)». Кваліфікація: «Офіцер військового управління оперативно-тактичного рівня». 3.Кандидат військових наук, 2005р. 20.01.12 «Радіоелектронна боротьба, способи та засоби». Тема дисертації: «Методика обґрунтування раціональних способів радіоелектронного подавлення супутникових систем зв'язку». 4.Доцент кафедри інформаційної та кібернетичної безпеки, 2015 р. Наявність публікацій за профілем дисципліни у періодичних наукових виданнях, що включені до переліку фахових видань України, до наукометричних баз, зокрема Scopus, Web of Science Core Collection: 1. Zahynei, A. та Shcheblanin, Y. та Kurchenko, O. та Anosov, Andrii та Kruglyk, V. (2024)

							Method for Calculating the Residual Resource of Fog Node Elements of Distributed Information Systems of Critical Infrastructure Facilities Cybersecurity Providing in Information and Telecommunication Systems 2024, 3654. с. 432-439. ISSN 1613-0073 2. Chernenko, Roman та Anosov, Andrii та Kyrychok, Roman та Brzhevska, Zoreslava та Spasiteleva, Svitlana (2022) Encryption Method for Systems with Limited Computing Resources Cybersecurity Providing in Information and Telecommunication Systems 2022, 3288 (1). с. 142-148. ISSN 1613-0073 3. Brzhevska, Zoreslava та Kyrychok, Roman та Anosov, Andrii та Skladannyi, Pavlo та Vorokhob, Maksym (2021) Analysis of the Process of Information Transfer from the Source-to-User in Terms of Information Impact Cybersecurity Providing in Information and Telecommunication Systems II 2021, 3188 (2). с. 257-264. ISSN 1613-0073 4. Brzhevska, Zoreslava та Haidur, Halyna та Dovzhenko, Nadiia та Anosov, Andrii та Vorokhob, Maksym (2021) Recurrent Estimation of the Information State Vector and the Correlation of Measuring Impact Matrix using a Multi-Agent Model Cybersecurity Providing in Information and Telecommunication Systems 2021, 2963. с. 272-276. ISSN 1613-0073 5. Черненко, Роман Миколайович та Рябчун, Олена Петрівна та Ворохоб, Максим Віталійович та Аносов, Андрій Олександрович та Козачок, Валерій Анатолійович (2021) Підвищення рівня захищеності систем мережі інтернету речей за рахунок шифрування даних на пристроях з обмеженими обчислювальними

							ресурсами Електронне фахове наукове видання "Кібербезпека: освіта, наука, техніка", 3 (11). с. 124-135. ISSN 2663-4023 6. Platonenko, Artem та Sokolov, V. Y. та Skladannyi, Pavlo та Anosov, A та Oleksiienko, H. (2021) Порівняння сучасних технічних засобів аеророзвідки для забезпечення безпеки контрольованої зони Кібербезпека: освіта, наука, техніка (13). с. 170-182. ISSN 2663-4023 Наявність виданих навчально-методичних посібників/посібників для самостійної роботи здобувачів вищої освіти та дистанційного навчання, електронних курсів на освітніх платформах: 1. Електронний навчальний курс з дисципліни «Захист інформації в інформаційно-комунікаційних системах» для бакалаврів спеціальності 125 Кібербезпека та захист інформації денної форми навчання. 2. Електронний навчальний курс з дисципліни : Моніторинг, аудит та адміністрування захищених ІТ систем і мереж (1 курс, 2р ВО, БІКС, очна). Освітньо-професійна програма 125.00.01 Безпека інформаційних і комунікаційних систем (2021, 2024). Магістр. (Наказ № 811 від 06.12.2021; Наказ № 699 від 02.11.2023 (пролонгація 2023/24 н.р.)) 3. Електронний навчальний курс з дисципліни: Технології безпеки мережевої та Smart інфраструктури (1 курс, 2р ВО, БІКС, очна). Освітньо-професійна програма 125.00.01 Безпека інформаційних і комунікаційних систем (2021, 2024). Магістр. (Наказ № 786 від 04.12.2023) Наукове керівництво (консультування) здобувача, який одержав документ про

							присудження наукового ступеня Черненко Роман Миколайович. Ступінь доктора філософії за спеціальності 125 Кібербезпека та захист інформації галузі знань 12 Інформаційні технології. Тема: Моделі та методи забезпечення захисту інформації, що передається відкритими каналами в мережах інтернету речей. 2024 р. Н24 № 002735 від 27.06.2024 Київський столичний університет імені Бориса Грінченка Виконання функцій (повноважень, обов'язків) наукового керівника або відповідального виконавця наукової теми (проекту), або головного редактора/члена редакційної колегії/експерта (рецензента) наукового видання, включеного до переліку фахових видань України, або іноземного наукового видання, що індексується в бібліографічних базах Член редакційної колегії електронного фахового наукового видання Київського столичного університету імені Бориса Грінченка "КІБЕРБЕЗПЕКА: ОСВІТА, НАУКА, ТЕХНІКА". Діяльність за спеціальністю у формі участі у професійних та/або громадських об'єднаннях Член "Internet Society (IS): Reston, VA, US" Відомості про підвищення кваліфікації: 1. Інститут телекомунікацій та глобального інформаційного простору НАН України. Довідка № 161/10.05.2023-1. Тема: «Робота зі шлюзом законного перехоплення для PS core компанії». від 10.05.2023 р. 4 кредити ЄКТС (120 годин). 2. Підвищення кваліфікації науково-педагогічних працівників Університету за

							Лідерським модулем. Київський столичний університет імені Бориса Грінченка, 02.04.2024-09.04.2024. 30 год. (наказ № 397 від 25.04.2024).
468938	Соколов Володимир Юрійович	Доцент, Основне місце роботи	Факультет інформаційних технологій та математики	Диплом магістра, Національний технічний університет України "Київський політехнічний інститут", рік закінчення: 2005, спеціальність: 090803 Електронні системи, Диплом кандидата наук ДК 055193, виданий 16.12.2019, Атестат доцента АД 009225, виданий 30.11.2021	18	Прикладні аспекти тестувань на проникнення та етичного хакінгу	Відповідність освіти: 1.Національний технічний університет України «Київський політехнічний інститут», 2005р. Спеціальність: «Електронні системи». Кваліфікація: магістр електроніки. 2.Кандидат технічних наук, 2019р. 05.13.06 – Інформаційні технології. Тема дисертації: «Методи і засоби підвищення інформаційної та функціональної безпеки безпроводових мереж передавання даних» 3.Доцент кафедри інформаційної та кібернетичної безпеки, 2021 р. Наявність публікацій за профілем дисципліни у періодичних наукових виданнях, що включені до переліку фахових видань України, до наукометричних баз, зокрема Scopus, Web of Science Core Collection: 1. Iavich, M. та Kovalchuk, O. та Gnatyuk, S. та Khavikova, Y. та Sokolov, Volodymyr (2024) Classical and post-quantum encryption for GDPR Classic, Quantum, and Post-Quantum Cryptography 2024, 3829. c. 70-78. ISSN 1613-0073 2. Kriuchkova, Larysa та Sokolov, Volodymyr та Skladannyi, Pavlo (2024) Determining the Zone of Successful Interaction in RFID Technologies 2024 IEEE 29th International Seminar/Workshop on Direct and Inverse Problems of Electromagnetic and Acoustic Wave Theory (DIPED). c. 168-171. ISSN 979-8-3315-0608-7 3. Bessalov, Anatoly та Sokolov, V. Y. та Abramov, Serhii (2024) Efficient Commutative

PQC Algorithms on Isogenies of Edwards Curves Cryptography, 8 (3). c. 1-17. ISSN 2410-387X
4. Sokolov, Volodymyr and Skladannyi, Pavlo and Platonenko, Artem (2023) Jump-Stay Jamming Attack on Wi-Fi Systems 2023 IEEE 18th International Conference on Computer Science and Information Technologies (CSIT). pp. 1-5. ISSN 2766-3639
5. Bessalov, Anatoly and Abramov, Serhii and Sokolov, Volodymyr and Skladannyi, Pavlo and Zhyltsov, Oleksii (2023) Multifunctional CRS Encryption Scheme on Isogenies of Non-Supersingular Edwards Curves Workshop on Classic, Quantum, and Post-Quantum Cryptography (CQPC 2023), 3504. pp. 12-25. ISSN 1613-0073
6. Marusenko, R. and Sokolov, V. Y. and Skladannyi, Pavlo (2023) Social Engineering Penetration Testing in Higher Education Institutions In: Lecture Notes on Data Engineering and Communications Technologies. Springer, pp. 1132-1147.
7. Buriachok, Volodymyr and Korshun, Natalia and Zhyltsov, Oleksii and Sokolov, Volodymyr and Skladannyi, Pavlo (2023) Implementation of Active Cybersecurity Education in Ukrainian Higher School Lecture Notes on Data Engineering and Communications Technologies, 178. pp. 533-551. ISSN 2367-4512
8. TajDini, Mahyar and Sokolov, V. Y. and Kuzminykh, Ievgeniia and Ghita, B. (2023) Brainwave-based authentication using features fusion Computers & Security (129). p. 103198. ISSN 0167-4048 9. Sokolov, Volodymyr and Skladannyi, Pavlo and Astapenya, Volodymyr (2023) Bluetooth Low-Energy Beacon Resistance to Jamming Attack 2023 IEEE 13th International

							Conference on Electronics and Information Technologies (ELIT). pp. 270-274. ISSN 979-8-3503-8309-6 10. Bessalov, Anatoliy and Abramov, Serhii and Sokolov, Volodymyr and Mazur, Nataliia (2023) CSIKE-ENC Combined Encryption Scheme with Optimized Degrees of Isogeny Distribution Cybersecurity Providing in Information and Telecommunication Systems, 3421. pp. 36-45. ISSN 1613-0073 11. Kipchuk, F. and Sokolov, Volodymyr and Skladannyi, Pavlo and Zhyltsov, Oleksii and Ageyev, D. (2023) Method for Increasing the Various Sources Data Consistency for IoT Sensors IEEE 9th International Conference on Problems of Infocommunications, Science and Technology (PICST). pp. 522-526. ISSN 979-8-3503-9891-5 12. Abramov, Serhii and Bessalov, Anatoly and Sokolov, Volodymyr (2023) Properties of Isogeny Graph of Non-Cyclic Edwards Curves Cybersecurity Providing in Information and Telecommunication Systems, 3550. pp. 234-239. ISSN 1613-0073 13. Anakhov, P. and Zhebka, V. and Popereshnyak, S and Skladannyi, Pavlo and Sokolov, Volodymyr (2023) Protecting Objects of Critical Information Infrastructure from Wartime Cyber Attacks by Decentralizing the Telecommunications Network Cybersecurity Providing in Information and Telecommunication Systems, 3550. pp. 240-245. ISSN 1613-0073 14. Bahatskyi, Oleksii and Bahatskyi, V. and Sokolov, Volodymyr (2023) Smart Home Subsystem for Calculating the Quality of Public Utilities Cybersecurity Providing in Information and Telecommunication Systems, 3421. pp. 168-173. ISSN 1613-0073 Наявність виданого підручника чи навчального

							посібника (включаючи електронні) або монографії 1. Hu, Z. B. Deduplication Method for Ukrainian Last Names, Medicinal Names, and Toponyms Based on Metaphone Phonetic Algorithm / Z. B. Hu, V. Buriachok, V. Sokolov // Advances in Computer Science for Engineering and Education III. — Vol. 1247. — Cham : Springer, 2020. — P. 518–533. [Колективна монографія. Індексується в Scopus.] 2. Marusenko, R. Experimental Evaluation of Phishing Attack on High School Students / R. Marusenko, V. Sokolov, V. Buriachok // Advances in Computer Science for Engineering and Education III. — Vol. 1247. — Cham : Springer, 2020. — P. 668–680. [Колективна монографія. Індексується в Scopus.] 3. Sokolov, V. Development of Low-Budget Spectrum Analyzers for IoT and Sensor Networks / V. Sokolov, A. Platonenko, L. Kuzmenko, V. Buriachok // Projektowanie, badania i eksploatacja. — Bielsku-Białej : NATH, 2020. — P. 331–342. [Колективна монографія.] 4. Бурячок, В. Л. Безпека безпроводових і мобільних мереж : Навчальний посібник / В. Л. Бурячок, В. Ю. Соколов, М. М. Таджділні. — 2 вид., доп. — К. : КУБГ, 2020. — 144 с. [Посібник.] Наявність виданих навчально-методичних посібників/посібників для самостійної роботи здобувачів вищої освіти та дистанційного навчання, електронних курсів на освітніх платформах: 1. Електронний навчальний курс з дисципліни Основи ОС та сучасних Інтернет-технологій (1 курс, 1р ВО, БІКС, очна). Освітньо-

							професійна програма 125.00.01 Безпека інформаційних та комунікаційних систем (2019, 2023). Бакалавр. (Наказ № 448 від 30.06.2021; Наказ № 786 від 04.12.2023 (пролонгація 2023/24 н.р.)). 2. Електронний навчальний курс з дисципліни Інформаційне право (2 курс, КІ, денна). Освітньо-професійна програма 123.00.01 Комп'ютерна інженерія (2022). Бакалавр. (Наказ № 420 від 02.05.2024) Участь в атестації наукових кадрів як офіційного опонента або члена постійної спеціалізованої вченої ради, або члена не менше трьох разових спеціалізованих вчених рад 1. Разова спеціалізована вчена рада ДФ 26.133.056 (13.02.2024, Київський столичний університет імені Бориса Грінченка) з правом прийняття до розгляду та проведення захисту дисертації Ворохоба Максима Віталійовича з метою присудження ступеня доктора філософії з галузі знань 12 Інформаційні технології за спеціальністю 125 Кібербезпека та захист інформації — рецензент. 2. Разова спеціалізована вчена рада ДФ 26.002.132 (06.06.2024, Національний технічний університет України «Київський політехнічний інститут імені Ігоря Сікорського») з правом прийняття до розгляду та проведення захисту дисертації Головатенка Іллі Анатолійовича з метою присудження ступеня доктора філософії з галузі знань 12 Інформаційні технології за спеціальністю 126 Інформаційні системи та технології — офіційний опонент. 3. Разова спеціалізована вчена рада ДФ 26.133.062 (12.06.2024,

							Київський столичний університет імені Бориса Грінченка) з правом прийняття до розгляду та проведення захисту дисертації Черненка Романа Миколайовича з метою присудження ступеня доктора філософії з галузі знань 12 Інформаційні технології за спеціальністю 125 Кібербезпека та захист інформації — рецензент. 4. Разова спеціалізована вчена рада ДФ 26.002.160 (27.06.2024, Національний технічний університет України «Київський політехнічний інститут імені Ігоря Сікорського») з правом прийняття до розгляду та проведення захисту дисертації Нікітіна Валерія Андрійовича з метою присудження ступеня доктора філософії з галузі знань 12 Інформаційні технології за спеціальністю 126 Інформаційні системи та технології — офіційний опонент. 5. Разова спеціалізована вчена рада 133 (13.08.2024, Національний університет «Львівська політехніка») з правом прийняття до розгляду та проведення захисту дисертації Курія Євгенія Олеговича з метою присудження ступеня доктора філософії з галузі знань 12 Інформаційні технології за спеціальністю 125 Кібербезпека — офіційний опонент. 6. Разова спеціалізована вчена рада 132 (13.08.2024, Національний університет «Львівська політехніка») з правом прийняття до розгляду та проведення захисту дисертації Журавчака Даниїла Юрійовича з метою присудження ступеня доктора філософії з галузі знань 12 Інформаційні технології за спеціальністю 125 Кібербезпека —

							офіційний опонент. Виконання функцій (повноважень, обов'язків) наукового керівника або відповідального виконавця наукової теми (проекту), або головного редактора/члена редакційної колегії/експерта (рецензента) наукового видання, включеного до переліку фахових видань України, або іноземного наукового видання, що індексується в бібліографічних базах 1. Член редакційної колегії електронного фахового наукового видання «Кібербезпека: освіта, наука, техніка» (електронне видання). 2. Член редакційної колегії електронного міжнародного наукового видання «International Journal of Wireless and Microwave Technologies» (електронне видання). 3. Член організаційного комітету міжнародної конференції «IEEE International Scientific-Practical Conference on Problems of Infocommunications Science and Technology» (індексується в Scopus). 4. Головний редактор міжнародної конференції «Workshop on Cybersecurity Providing in Information and Telecommunication Systems» (індексується в Scopus). 5. Редактор міжнародної конференції «Workshop on Classic, Quantum, and Post-Quantum Cryptography» (індексується в Scopus). 6. Член організаційного комітету міжнародної конференції «International Conference on Computer Science, Engineering and Education Applications» (індексується в Scopus). Участь у міжнародних

							наукових та/або освітніх проектах, залучення до міжнародної експертизи, наявність звання «суддя міжнародної категорії» 1. 01.02.2023–31.05.2023 «Development of DAO-modules for the DAO economic system» (XGROUP GLOBAL PTE Ltd., Сінгапур). 2. 01.08.2023–31.07.2024 «Research of Speech Emotion Recognition» (№89-080123, Ender Turing OÜ, Таллінн, Естонія). Діяльність за спеціальністю у формі участі у професійних та/або громадських об'єднаннях 1. Член «European Microwave Assosiation (EuMA)» (№ AM3734, з 2019 до 2026 р.). 2. Член «International Telecommunication Union (ITU-T)» (№ 1200190674, з 2017 до 2021 р.). Досвід практичної роботи за спеціальністю не менше п'яти років (крім педагогічної, науково-педагогічної, наукової діяльності) 1. Senior System Analyst / Proxy Product Owner (09.2022–07.2023, Pivotal Commware, США). 2. Senior System Analyst (08.2021–02.2022, Raiffeisen Bank, Україна). 3. Business Analyst (03.2020–07.2021, Competo, Азербайджан). Відомості про підвищення кваліфікації: 1.Підвищення кваліфікації науково-педагогічних працівників Університету за Дослідницьким модулем (поглиблений рівень). Київський університет імені Бориса Грінченка, 22.10.2021-30.11.2021. 30 год. (сертифікат № 1766/41 від 03.12.2021). 2. Інститут телекомунікацій та глобального інформаційного простору НАН України. Довідка № 161/24.05.2023-3.

							Тема: Створення нових LDPC кодів супутникового зв'язку за екстремальними графами. Від 24.05.2023р. 120 годин (4 кредити ЄКТС). 3. Підвищення кваліфікації науково-педагогічних працівників Університету за Цифровим модулем. Київський університет імені Бориса Грінченка, 30 год. (наказ № 842 від 25.12.2023).
468547	Гулак Геннадій Миколайович	Професор, Основне місце роботи	Факультет інформаційних технологій та математики	Диплом спеціаліста, Вища школа КДБ СРСР, рік закінчення: 1977, спеціальність: прикладна математика, Диплом доктора наук ДД 011796, виданий 29.06.2021, Диплом кандидата наук ДК 047448, виданий 02.07.2008, Атестат доцента 12ДЦ 030734, виданий 17.05.2012, Атестат професора АП 005030, виданий 27.04.2023	42	Методи побудови і аналізу криптосистем	Відповідність освіти: 1. Вища школа КДБ СРСР, 1977р. 2. Доктор технічних наук, 2021р. 05.13.06 – інформаційні технології. Тема дисертації: «Закрита» 3. Професор кафедри інформаційної та кібернетичної безпеки, 2023р. Наявність публікацій за профілем дисципліни у періодичних наукових виданнях, що включені до переліку фахових видань України, до наукометричних баз, зокрема Scopus, Web of Science Core Collection: 1. Rzaieva, S. та Rzaiev, D. та Kostyuk, Y. та Hulak, Hennadii та Shcheblanin, O. (2024) Methods of Modeling Database System Security Cybersecurity Providing in Information and Telecommunication Systems 2024, 3654. с. 384-390. ISSN 1613-0073 2. Dudykevych, V та Yevseiev, S та Mykytyn, H та Ruda, K та Hulak, Hennadii (2024) Detecting Deepfake Modifications of Biometric Images using Neural Networks Cybersecurity Providing in Information and Telecommunication Systems 2024, 3654. с. 391-397. ISSN 1613-0073 3. Buhas, V. та Ponomarenko, I. та Buhas, N. та Hulak, Hennadii (2024) Cybersecurity Role in AI-Powered Digital Marketing Digital Economy Concepts and Technologies Workshop 2024, 3665. с. 1-11.

							ISSN 1613-0073 4. Popereshnyak, S. та Ovcharenko, V. та Novikov, Y. та Hulak, Hennadii (2024) Detection of intrusions based on text analysis and machine learning methods in the development of information systems Cybersecurity Providing in Information and Telecommunication Systems II 2024, 3826. с. 310-318. ISSN 1613-0073 5. Dudykevych, V та Yevseiev, S та Mykytyn, H та Ruda, K та Hulak, Hennadii (2024) Detecting Deepfake Modifications of Biometric Images using Neural Networks Cybersecurity Providing in Information and Telecommunication Systems 2024, 3654. с. 391-397. ISSN 1613-0073 6. Mykhaylova, O та Fedynyshyn, T та Datsiuk, A та Fihol, B та Hulak, Hennadii (2023) Mobile Application as a Critical Infrastructure Cyberattack Surface Cybersecurity Providing in Information and Telecommunication Systems II 2023, 3050. с. 29-43. ISSN 1613-0073 7. Гулак, Геннадій Миколайович та Жданова, Юлія Дмитрівна та Складанний, Павло Миколайович та Гулак, Євген та Корнієць, Віктор (2022) Уразливості шифрування коротких повідомлень в мобільних інформаційно-комунікаційних системах об'єктів критичної інфраструктури Електронне фахове наукове видання ""Кібербезпека: освіта, наука, техніка"", 1 (17). с. 145-158. ISSN 2663-4023. Наявність виданого підручника чи навчального посібника (включаючи електронні) або монографії Гулак Г. М., Жильцов О. Б., Киричок Р. В., Коршун Н. В., Складанний П. М. Інформаційна та кібернетична безпека

							підприємства : підруч. / Г. М. Гулак, О. Б. Жильцов, Р. В. Киричок, Н. В. Коршун, П. М. Складанний – 2023. – 370 с. Наявність виданих навчально-методичних посібників/посібників для самостійної роботи здобувачів вищої освіти та дистанційного навчання, електронних курсів на освітніх платформах: 1. Електронний навчальний курс з дисципліни: Інфраструктура відкритих ключів (4 курс, 1р ВО, БІКС, очна) Освітньо-професійна програма 125.00.01 Безпека інформаційних та комунікаційних систем (2019, 2023). Бакалавр. (Наказ № 811 від 06.12.2021; Наказ № 786 від 04.12.2023 (пролонгація 2023/24 н.р.)). 2. Електронний навчальний курс з дисципліни: Кібернетичне право (2 курс, 1р ВО, БІКС, очна). Освітньо-професійна програма 125.00.01 Безпека інформаційних та комунікаційних систем (2019, 2023). Бакалавр. (Наказ № 786 від 04.12.2023). 3. Методичні рекомендації до виконання та захисту кваліфікаційної роботи магістра для студентів спеціальності 125 Кібербезпека та захист інформації освітньої програми 125.00.01 Безпека інформаційних і комунікаційних систем / Укладачі: Жданова Ю. Д., Складанний П. М., Шевченко С. М, Гулак Г.М.. – Київ: КУБГ, 2023. –57 с. Захист дисертації на здобуття наукового ступеня У 2021 році рішенням Атестаційної колегії Міністерства освіти і науки України присвоєно науковий ступінь доктора технічних наук за спеціальністю 05.13.06 – Інформаційні технології. Тема

							дисертації: "Спеціальна" Наукове керівництво (консультування) здобувача, який одержав документ про присудження наукового ступеня 1. Складанний Павло Миколайович. Науковий ступінь кандидат технічних наук за спеціальністю 05.13.06 – Інформаційні технології. Тема: Моделі і методи забезпечення імітостійкості та конфіденційності в системах обробки інформації. 2021 р. ДК № 061086 від 29.06.2021 р. Інститут телекомунікацій і глобального інформаційного простору Національної академії наук України. 2. Кузьменко Лідія Володимирівна. Науковий ступінь кандидата технічних наук за спеціальністю 05.13.06 – Інформаційні технології. Тема: Інформаційна технологія для створення перспективних гарантоздатних автоматизованих систем управління об'єктами критичної інфраструктури. 2021 р. ДК № 061085 від 29.06.2021 р. Інститут телекомунікацій і глобального інформаційного простору Національної академії наук України. Участь в атестації наукових кадрів як офіційного опонента або члена постійної спеціалізованої вченої ради, або члена не менше трьох разових спеціалізованих вчених рад 1. Член постійної спеціалізованої вченої ради з захисту дисертацій Д 26.204.01 в ІПММС НАН України. 2. Разова спеціалізована вчена рада ДФ 26.133.056 з правом прийняття до розгляду та проведення захисту дисертації Ворохоба Максима Віталійовича з метою пресудження ступеня доктора філософії з галузі

							знань 12 Інформаційні технології за спеціальністю 125 Кібербезпека та захист інформації - Голова ради (2024 р.) 3. Разова спеціалізована вчена рада ДФ 26.133.062 з правом прийняття до розгляду та проведення захисту дисертації Черненка Романа Миколайовича зметою присудження ступеня доктора філософії в галузі знань 12 Інформаційні технології за спеціальністю 125 Кібербезпека та захист інформації - Рецензент (2024 р.)
							Наявність апробаційних та/або науково-популярних, та/або консультаційних (дорадчих), та/або науково-експертних публікацій з наукової або професійної тематики 1. Tyshyk, I. та Hulak, Hennadii (2024) Testing an organization's information system for unauthorized access Cybersecurity Providing in Information and Telecommunication Systems II 2024, 3826. с. 17-29. ISSN 1613-0073 2. Buhas, V. та Ponomarenko, I. та Buhas, N. та Hulak, Hennadii (2024) Cybersecurity Role in AI-Powered Digital Marketing Digital Economy Concepts and Technologies Workshop 2024, 3665. с. 1-11. ISSN 1613-0073 3. Otto, G. та Otto, K. та Hulak, Hennadii та Astapenya, Volodymyr та Tyshchenko, D. (2023) Parametric Model of a Laser with External Distributed Feedback in the System of Remote Measurement of Nanovibrations Cybersecurity Providing in Information and Telecommunication Systems 2023, 3421. с. 284-292. ISSN 1613-0073 4. Ilyenko, A та Ilyenko, S та Prokopenko, O та Hulak, Hennadii та Melnyk, Iryna (2023) Practical Aspects of Using Fully Homomorphic

Encryption Systems to Protect Cloud Computing Cybersecurity Providing in Information and Telecommunication Systems, 3550. с. 226-233. ISSN 1613-0073
5. Virovets, Denis та Obushnyi, Sergiy та Shtepa, Olena та Hulak, Hennadii та Vlasenko, V. (2023) Ways of Interaction of Autonomous Economic Agents in Decentralized Autonomous Organizations Cybersecurity Providing in Information and Telecommunication Systems 2023, 3421. с. 183-190. ISSN 1613-0073
6. Hulak, Hennadii та Skladannyi, Pavlo та Sokolov, Volodymyr та Hulak, E. та Korniiets, V. (2022) Dynamic model of guarantee capacity and cyber security management in the critical automated systems 2nd International Conference on Conflict Management in Global Information Networks (CMiGiN 2022), 3530. с. 102-111. ISSN 1613-0073
7. Sokolov, V. Y. та Skladannyi, Pavlo та Hulak, Hennadii (2022) Stability Verification of Self-Organized Wireless Networks with Block Encryption Cybersecurity Providing in Information and Telecommunication Systems, 3137. с. 227-237. ISSN 1613-0073
8. Grechaninov, Viktor та Khoshaba, Oleksandr та Hulak, Hennadii та Zhdanova, Yuliia та Melnyk, Iryna (2022) Models and Methods for Determining Application Performance Estimates in Distributed Structures Cybersecurity Providing in Information and Telecommunication Systems 2022, 3288 (1). с. 134-141. ISSN 1613-0073
9. Grechaninov, Viktor та Hulak, Hennadii та Sokolov, V. Y. та Skladannyi, Pavlo та Korshun, Natalia (2022) Formation of Dependability and Cyber Protection Model in Information Systems of Situational Center

							Emerging Technology Trends on the Smart Industry and the Internet of Things 2022, 3149. с. 107-117. ISSN 1613-0073 Діяльність за спеціальністю у формі участі у професійних та/або громадських об'єднаннях Член "Internet Society (IS): Reston, VA, US" Відомості про підвищення кваліфікації: 1. Підвищення кваліфікації науково-педагогічних працівників Університету за Дослідницьким модулем. Київський університет імені Бориса Грінченка, 18.10.2021-26.11.2021. 30 год. (сертифікат № 1792/41 від 30.11.2021). 2. Фаховий модуль: Інститут телекомунікацій та глобального інформаційного простору НАНУ, відділ інформаційної безпеки. Довідка № 161/17.05.23-2. Тема: "Некомутативна криптографія в термінах- теоріях груп та навгруп перетворень афінних пристроїв" від 17.05.2023 р. 4 кредити ЄКТС (120 годин). 3. Підвищення кваліфікації науково-педагогічних працівників Університету за Цифровим модулем. Київський університет імені Бориса Грінченка, 30 год. (наказ № 842 від 25.12.2023). 4. Підвищення кваліфікації науково-педагогічних працівників Університету за Лідерським модулем. Київський столичний університет імені Бориса Грінченка. 02.04.2024-09.04.2024, 30 год. (наказ №397 від 25.04.2024 р.)
468938	Соколов Володимир Юрійович	Доцент, Основне місце роботи	Факультет інформаційних технологій та математики	Диплом магістра, Національний технічний університет України "Київський	18	Технології безпеки Web-ресурсів	Відповідність освіти: 1.Національний технічний університет України «Київський політехнічний інститут», 2005р. Спеціальність:

				політехнічний інститут", рік закінчення: 2005, спеціальність: 090803 Електронні системи, Диплом кандидата наук ДК 055193, виданий 16.12.2019, Атестат доцента АД 009225, виданий 30.11.2021			«Електронні системи». Кваліфікація: магістр електроніки. 2.Кандидат технічних наук, 2019р. 05.13.06 – Інформаційні технології. Тема дисертації: «Методи і засоби підвищення інформаційної та функціональної безпеки безпроводових мереж передавання даних» 3.Доцент кафедри інформаційної та кібернетичної безпеки, 2021 р. Наявність публікацій за профілем дисципліни у періодичних наукових виданнях, що включені до переліку фахових видань України, до наукометричних баз, зокрема Scopus, Web of Science Core Collection: 1. Iavich, M. та Kovalchuk, O. та Gnatyuk, S. та Khavikova, Y. та Sokolov, Volodymyr (2024) Classical and post-quantum encryption for GDPR Classic, Quantum, and Post-Quantum Cryptography 2024, 3829. с. 70-78. ISSN 1613-0073 2. Kriuchkova, Larysa та Sokolov, Volodymyr та Skladannyi, Pavlo (2024) Determining the Zone of Successful Interaction in RFID Technologies 2024 IEEE 29th International Seminar/Workshop on Direct and Inverse Problems of Electromagnetic and Acoustic Wave Theory (DIPED). с. 168-171. ISSN 979-8-3315-0608-7 3. Bessalov, Anatoly та Sokolov, V. Y. та Abramov, Serhii (2024) Efficient Commutative PQC Algorithms on Isogenies of Edwards Curves Cryptography, 8 (3). с. 1-17. ISSN 2410-387X 4. Sokolov, Volodymyr and Skladannyi, Pavlo and Platonenko, Artem (2023) Jump-Stay Jamming Attack on Wi-Fi Systems 2023 IEEE 18th International Conference on Computer Science and Information Technologies (CSIT).

pp. 1-5. ISSN 2766-3639
5. Bessalov, Anatoly and Abramov, Serhii and Sokolov, Volodymyr and Skladannyi, Pavlo and Zhyltsov, Oleksii (2023) Multifunctional CRS Encryption Scheme on Isogenies of Non-Supersingular Edwards Curves Workshop on Classic, Quantum, and Post-Quantum Cryptography (CQPC 2023), 3504. pp. 12-25. ISSN 1613-0073
6. Marusenko, R. and Sokolov, V. Y. and Skladannyi, Pavlo (2023) Social Engineering Penetration Testing in Higher Education Institutions In: Lecture Notes on Data Engineering and Communications Technologies. Springer, pp. 1132-1147.
7. Buriachok, Volodymyr and Korshun, Natalia and Zhyltsov, Oleksii and Sokolov, Volodymyr and Skladannyi, Pavlo (2023) Implementation of Active Cybersecurity Education in Ukrainian Higher School Lecture Notes on Data Engineering and Communications Technologies, 178. pp. 533-551. ISSN 2367-4512
8. TajDini, Mahyar and Sokolov, V. Y. and Kuzminykh, Ievgeniia and Ghita, B. (2023) Brainwave-based authentication using features fusion Computers & Security (129). p. 103198. ISSN 0167-4048 9. Sokolov, Volodymyr and Skladannyi, Pavlo and Astapenya, Volodymyr (2023) Bluetooth Low-Energy Beacon Resistance to Jamming Attack 2023 IEEE 13th International Conference on Electronics and Information Technologies (ELIT). pp. 270-274. ISSN 979-8-3503-8309-6
10. Bessalov, Anatoliy and Abramov, Serhii and Sokolov, Volodymyr and Mazur, Nataliia (2023) CSIKE-ENC Combined Encryption Scheme with Optimized Degrees of Isogeny Distribution Cybersecurity Providing

							in Information and Telecommunication Systems, 3421. pp. 36-45. ISSN 1613-0073 11. Kipchuk, F. and Sokolov, Volodymyr and Skladannyi, Pavlo and Zhyltsov, Oleksii and Ageyev, D. (2023) Method for Increasing the Various Sources Data Consistency for IoT Sensors IEEE 9th International Conference on Problems of Infocommunications, Science and Technology (PICST). pp. 522-526. ISSN 979-8-3503-9891-5 12. Abramov, Serhii and Bessalov, Anatoly and Sokolov, Volodymyr (2023) Properties of Isogeny Graph of Non-Cyclic Edwards Curves Cybersecurity Providing in Information and Telecommunication Systems, 3550. pp. 234-239. ISSN 1613-0073 13. Anakhov, P. and Zhebka, V. and Popereshnyak, S and Skladannyi, Pavlo and Sokolov, Volodymyr (2023) Protecting Objects of Critical Information Infrastructure from Wartime Cyber Attacks by Decentralizing the Telecommunications Network Cybersecurity Providing in Information and Telecommunication Systems, 3550. pp. 240-245. ISSN 1613-0073 14. Bahatskyi, Oleksii and Bahatskyi, V. and Sokolov, Volodymyr (2023) Smart Home Subsystem for Calculating the Quality of Public Utilities Cybersecurity Providing in Information and Telecommunication Systems, 3421. pp. 168-173. ISSN 1613-0073
							Наявність виданого підручника чи навчального посібника (включаючи електронні) або монографії 1. Hu, Z. B. Deduplication Method for Ukrainian Last Names, Medicinal Names, and Toponyms Based on Metaphone Phonetic Algorithm / Z. B. Hu, V. Buriachok, V. Sokolov // Advances in Computer Science for Engineering and Education III. — Vol.

							1247. — Cham : Springer, 2020. — P. 518–533. [Колективна монографія. Індексується в Scopus.] 2. Marusenko, R. Experimental Evaluation of Phishing Attack on High School Students / R. Marusenko, V. Sokolov, V. Buriachok // Advances in Computer Science for Engineering and Education III. — Vol. 1247. — Cham : Springer, 2020. — P. 668–680. [Колективна монографія. Індексується в Scopus.] 3. Sokolov, V. Development of Low-Budget Spectrum Analyzers for IoT and Sensor Networks / V. Sokolov, A. Platonenko, L. Kuzmenko, V. Buriachok // Projektowanie, badania i eksploatacja. — Bielsku-Białej : NATH, 2020. — P. 331–342. [Колективна монографія.] 4. Бурячок, В. Л. Безпека безпроводових і мобільних мереж : Навчальний посібник / В. Л. Бурячок, В. Ю. Соколов, М. М. Таджділні. — 2 вид., доп. — К. : КУБГ, 2020. — 144 с. [Посібник.] Наявність виданих навчально-методичних посібників/посібників для самостійної роботи здобувачів вищої освіти та дистанційного навчання, електронних курсів на освітніх платформах: 1. Електронний навчальний курс з дисципліни Основи ОС та сучасних Інтернет-технологій (1 курс, 1р ВО, БІКС, очна). Освітньо-професійна програма 125.00.01 Безпека інформаційних та комунікаційних систем (2019, 2023). Бакалавр. (Наказ № 448 від 30.06.2021; Наказ № 786 від 04.12.2023 (пролонгація 2023/24 н.р.)). 2. Електронний навчальний курс з дисципліни Інформаційне право (2 курс, КІ, денна).

							Освітньо-професійна програма 123.00.01 Комп'ютерна інженерія (2022). Бакалавр. (Наказ № 420 від 02.05.2024) Участь в атестації наукових кадрів як офіційного опонента або члена постійної спеціалізованої вченої ради, або члена не менше трьох разових спеціалізованих вчених рад 1. Разова спеціалізована вчена рада ДФ 26.133.056 (13.02.2024, Київський столичний університет імені Бориса Грінченка) з правом прийняття до розгляду та проведення захисту дисертації Ворохоба Максима Віталійовича з метою присудження ступеня доктора філософії з галузі знань 12 Інформаційні технології за спеціальністю 125 Кібербезпека та захист інформації — рецензент. 2. Разова спеціалізована вчена рада ДФ 26.002.132 (06.06.2024, Національний технічний університет України «Київський політехнічний інститут імені Ігоря Сікорського») з правом прийняття до розгляду та проведення захисту дисертації Головатенка Іллі Анатолійовича з метою присудження ступеня доктора філософії з галузі знань 12 Інформаційні технології за спеціальністю 126 Інформаційні системи та технології — офіційний опонент. 3. Разова спеціалізована вчена рада ДФ 26.133.062 (12.06.2024, Київський столичний університет імені Бориса Грінченка) з правом прийняття до розгляду та проведення захисту дисертації Черненка Романа Миколайовича з метою присудження ступеня доктора філософії з галузі знань 12 Інформаційні технології за спеціальністю 125 Кібербезпека та захист

							інформації — рецензент. 4. Разова спеціалізована вчена рада ДФ 26.002.160 (27.06.2024, Національний технічний університет України «Київський політехнічний інститут імені Ігоря Сікорського») з правом прийняття до розгляду та проведення захисту дисертації Нікітіна Валерія Андрійовича з метою присудження ступеня доктора філософії з галузі знань 12 Інформаційні технології за спеціальністю 126 Інформаційні системи та технології — офіційний опонент. 5. Разова спеціалізована вчена рада 133 (13.08.2024, Національний університет «Львівська політехніка») з правом прийняття до розгляду та проведення захисту дисертації Курія Євгенія Олеговича з метою присудження ступеня доктора філософії з галузі знань 12 Інформаційні технології за спеціальністю 125 Кібербезпека — офіційний опонент. 6. Разова спеціалізована вчена рада 132 (13.08.2024, Національний університет «Львівська політехніка») з правом прийняття до розгляду та проведення захисту дисертації Журавчака Даниїла Юрійовича з метою присудження ступеня доктора філософії з галузі знань 12 Інформаційні технології за спеціальністю 125 Кібербезпека — офіційний опонент. Виконання функцій (повноважень, обов'язків) наукового керівника або відповідального виконавця наукової теми (проекту), або головного редактора/члена редакційної колегії/експерта (рецензента) наукового видання, включеного до переліку фахових

							видань України, або іноземного наукового видання, що індексується в бібліографічних базах 1. Член редакційної колегії електронного фахового наукового видання «Кібербезпека: освіта, наука, техніка» (електронне видання). 2. Член редакційної колегії електронного міжнародного наукового видання «International Journal of Wireless and Microwave Technologies» (електронне видання). 3. Член організаційного комітету міжнародної конференції «IEEE International Scientific-Practical Conference on Problems of Infocommunications Science and Technology» (індексується в Scopus). 4. Головний редактор міжнародної конференції «Workshop on Cybersecurity Providing in Information and Telecommunication Systems» (індексується в Scopus). 5. Редактор міжнародної конференції «Workshop on Classic, Quantum, and Post-Quantum Cryptography» (індексується в Scopus). 6. Член організаційного комітету міжнародної конференції «International Conference on Computer Science, Engineering and Education Applications» (індексується в Scopus). Участь у міжнародних наукових та/або освітніх проектах, залучення до міжнародної експертизи, наявність звання «суддя міжнародної категорії» 1. 01.02.2023–31.05.2023 «Development of DAO-modules for the DAO economic system» (XGROUP GLOBAL PTE Ltd., Сінгапур). 2. 01.08.2023–

							31.07.2024 «Research of Speech Emotion Recognition» (№89-080123, Ender Turing OÜ, Таллінн, Естонія). Діяльність за спеціальністю у формі участі у професійних та/або громадських об'єднаннях 1. Член «European Microwave Assosiation (EuMA)» (№ AM3734, з 2019 до 2026 р.). 2. Член «International Telecommunication Union (ITU-T)» (№ 1200190674, з 2017 до 2021 р.). Досвід практичної роботи за спеціальністю не менше п'яти років (крім педагогічної, науково-педагогічної, наукової діяльності) 1. Senior System Analyst / Proxy Product Owner (09.2022–07.2023, Pivotal Commware, США). 2. Senior System Analyst (08.2021–02.2022, Raiffeisen Bank, Україна). 3. Business Analyst (03.2020–07.2021, Competo, Азербайджан). Відомості про підвищення кваліфікації: 1.Підвищення кваліфікації науково-педагогічних працівників Університету за Дослідницьким модулем (поглиблений рівень). Київський університет імені Бориса Грінченка, 22.10.2021-30.11.2021. 30 год. (сертифікат № 1766/41 від 03.12.2021). 2. Інститут телекомунікацій та глобального інформаційного простору НАН України. Довідка № 161/24.05.2023-3. Тема: Створення нових LDPC кодів супутникового зв'язку за екстремальними графами. Від 24.05.2023р. 120 годин (4 кредити ЄКТС). 3. Підвищення кваліфікації науково-педагогічних працівників Університету за Цифровим модулем. Київський університет імені Бориса

							Грінченка, 30 год. (наказ № 842 від 25.12.2023).
468938	Соколов Володимир Юрійович	Доцент, Основне місце роботи	Факультет інформаційних технологій та математики	Диплом магістра, Національний технічний університет України "Київський політехнічний інститут", рік закінчення: 2005, спеціальність: 090803 Електронні системи, Диплом кандидата наук ДК 055193, виданий 16.12.2019, Атестат доцента АД 009225, виданий 30.11.2021	18	Технології безпеки безпроводових і мобільних мереж	Відповідність освіти: 1.Національний технічний університет України «Київський політехнічний інститут», 2005р. Спеціальність: «Електронні системи». Кваліфікація: магістр електроніки. 2.Кандидат технічних наук, 2019р. 05.13.06 – Інформаційні технології. Тема дисертації: «Методи і засоби підвищення інформаційної та функціональної безпеки безпроводових мереж передавання даних» 3.Доцент кафедри інформаційної та кібернетичної безпеки, 2021 р. Наявність публікацій за профілем дисципліни у періодичних наукових виданнях, що включені до переліку фахових видань України, до наукометричних баз, зокрема Scopus, Web of Science Core Collection: 1. Iavich, M. та Kovalchuk, O. та Gnatyuk, S. та Khavikova, Y. та Sokolov, Volodymyr (2024) Classical and post-quantum encryption for GDPR Classic, Quantum, and Post-Quantum Cryptography 2024, 3829. с. 70-78. ISSN 1613-0073 2. Kriuchkova, Larysa та Sokolov, Volodymyr та Skladannyi, Pavlo (2024) Determining the Zone of Successful Interaction in RFID Technologies 2024 IEEE 29th International Seminar/Workshop on Direct and Inverse Problems of Electromagnetic and Acoustic Wave Theory (DIPED). с. 168-171. ISSN 979-8-3315-0608-7 3. Bessalov, Anatoly та Sokolov, V. Y. та Abramov, Serhii (2024) Efficient Commutative PQC Algorithms on Isogenies of Edwards Curves Cryptography, 8 (3). с. 1-17. ISSN 2410-387X 4. Sokolov, Volodymyr

and Skladannyi, Pavlo and Platonenko, Artem (2023) Jump-Stay Jamming Attack on Wi-Fi Systems 2023 IEEE 18th International Conference on Computer Science and Information Technologies (CSIT). pp. 1-5. ISSN 2766-3639
5. Bessalov, Anatoly and Abramov, Serhii and Sokolov, Volodymyr and Skladannyi, Pavlo and Zhyltsov, Oleksii (2023) Multifunctional CRS Encryption Scheme on Isogenies of Non-Supersingular Edwards Curves Workshop on Classic, Quantum, and Post-Quantum Cryptography (CQPC 2023), 3504. pp. 12-25. ISSN 1613-0073
6. Marusenko, R. and Sokolov, V. Y. and Skladannyi, Pavlo (2023) Social Engineering Penetration Testing in Higher Education Institutions In: Lecture Notes on Data Engineering and Communications Technologies. Springer, pp. 1132-1147.
7. Buriachok, Volodymyr and Korshun, Natalia and Zhyltsov, Oleksii and Sokolov, Volodymyr and Skladannyi, Pavlo (2023) Implementation of Active Cybersecurity Education in Ukrainian Higher School Lecture Notes on Data Engineering and Communications Technologies, 178. pp. 533-551. ISSN 2367-4512
8. TajDini, Mahyar and Sokolov, V. Y. and Kuzminykh, Ievgeniia and Ghita, B. (2023) Brainwave-based authentication using features fusion Computers & Security (129). p. 103198. ISSN 0167-4048 9. Sokolov, Volodymyr and Skladannyi, Pavlo and Astapenya, Volodymyr (2023) Bluetooth Low-Energy Beacon Resistance to Jamming Attack 2023 IEEE 13th International Conference on Electronics and Information Technologies (ELIT). pp. 270-274. ISSN 979-8-3503-8309-6

							10. Bessalov, Anatoliy and Abramov, Serhii and Sokolov, Volodymyr and Mazur, Nataliia (2023) CSIKE-ENC Combined Encryption Scheme with Optimized Degrees of Isogeny Distribution Cybersecurity Providing in Information and Telecommunication Systems, 3421. pp. 36-45. ISSN 1613-0073 11. Kipchuk, F. and Sokolov, Volodymyr and Skladannyi, Pavlo and Zhyltsov, Oleksii and Ageyev, D. (2023) Method for Increasing the Various Sources Data Consistency for IoT Sensors IEEE 9th International Conference on Problems of Infocommunications, Science and Technology (PICST). pp. 522-526. ISSN 979-8-3503-9891-5 12. Abramov, Serhii and Bessalov, Anatoly and Sokolov, Volodymyr (2023) Properties of Isogeny Graph of Non-Cyclic Edwards Curves Cybersecurity Providing in Information and Telecommunication Systems, 3550. pp. 234-239. ISSN 1613-0073 13. Anakhov, P. and Zhebka, V. and Popereshnyak, S and Skladannyi, Pavlo and Sokolov, Volodymyr (2023) Protecting Objects of Critical Information Infrastructure from Wartime Cyber Attacks by Decentralizing the Telecommunications Network Cybersecurity Providing in Information and Telecommunication Systems, 3550. pp. 240-245. ISSN 1613-0073 14. Bahatskyi, Oleksii and Bahatskyi, V. and Sokolov, Volodymyr (2023) Smart Home Subsystem for Calculating the Quality of Public Utilities Cybersecurity Providing in Information and Telecommunication Systems, 3421. pp. 168-173. ISSN 1613-0073 Наявність виданого підручника чи навчального посібника (включаючи електронні) або монографії 1. Hu, Z. B. Deduplication Method

							for Ukrainian Last Names, Medicinal Names, and Toponyms Based on Metaphone Phonetic Algorithm / Z. B. Hu, V. Buriachok, V. Sokolov // Advances in Computer Science for Engineering and Education III. — Vol. 1247. — Cham : Springer, 2020. — P. 518–533. [Колективна монографія. Індексується в Scopus.] 2. Marusenko, R. Experimental Evaluation of Phishing Attack on High School Students / R. Marusenko, V. Sokolov, V. Buriachok // Advances in Computer Science for Engineering and Education III. — Vol. 1247. — Cham : Springer, 2020. — P. 668–680. [Колективна монографія. Індексується в Scopus.] 3. Sokolov, V. Development of Low-Budget Spectrum Analyzers for IoT and Sensor Networks / V. Sokolov, A. Platonenko, L. Kuzmenko, V. Buriachok // Projektowanie, badania i eksploatacja. — Bielsku-Białej : NATH, 2020. — P. 331–342. [Колективна монографія.] 4. Бурячок, В. Л. Безпека безпроводових і мобільних мереж : Навчальний посібник / В. Л. Бурячок, В. Ю. Соколов, М. М. Таджділі. — 2 вид., доп. — К. : КУБГ, 2020. — 144 с. [Посібник.] Наявність виданих навчально-методичних посібників/посібників для самостійної роботи здобувачів вищої освіти та дистанційного навчання, електронних курсів на освітніх платформах: 1. Електронний навчальний курс з дисципліни Основи ОС та сучасних Інтернет-технологій (1 курс, 1р ВО, БІКС, очна). Освітньо-професійна програма 125.00.01 Безпека інформаційних та комунікаційних систем (2019, 2023). Бакалавр. (Наказ №

							448 від 30.06.2021; Наказ № 786 від 04.12.2023 (пролонгація 2023/24 н.р.)). 2. Електронний навчальний курс з дисципліни Інформаційне право (2 курс, КІ, денна). Освітньо-професійна програма 123.00.01 Комп'ютерна інженерія (2022). Бакалавр. (Наказ № 420 від 02.05.2024) Участь в атестації наукових кадрів як офіційного опонента або члена постійної спеціалізованої вченої ради, або члена не менше трьох разових спеціалізованих вчених рад 1. Разова спеціалізована вчена рада ДФ 26.133.056 (13.02.2024, Київський столичний університет імені Бориса Грінченка) з правом прийняття до розгляду та проведення захисту дисертації Ворохоба Максима Віталійовича з метою присудження ступеня доктора філософії з галузі знань 12 Інформаційні технології за спеціальністю 125 Кібербезпека та захист інформації — рецензент. 2. Разова спеціалізована вчена рада ДФ 26.002.132 (06.06.2024, Національний технічний університет України «Київський політехнічний інститут імені Ігоря Сікорського») з правом прийняття до розгляду та проведення захисту дисертації Головатенка Іллі Анатолійовича з метою присудження ступеня доктора філософії з галузі знань 12 Інформаційні технології за спеціальністю 126 Інформаційні системи та технології — офіційний опонент. 3. Разова спеціалізована вчена рада ДФ 26.133.062 (12.06.2024, Київський столичний університет імені Бориса Грінченка) з правом прийняття до розгляду та проведення захисту

							дисертації Черненка Романа Миколайовича з метою присудження ступеня доктора філософії з галузі знань 12 Інформаційні технології за спеціальністю 125 Кібербезпека та захист інформації — рецензент. 4. Разова спеціалізована вчена рада ДФ 26.002.160 (27.06.2024, Національний технічний університет України «Київський політехнічний інститут імені Ігоря Сікорського») з правом прийняття до розгляду та проведення захисту дисертації Нікітіна Валерія Андрійовича з метою присудження ступеня доктора філософії з галузі знань 12 Інформаційні технології за спеціальністю 126 Інформаційні системи та технології — офіційний опонент. 5. Разова спеціалізована вчена рада 133 (13.08.2024, Національний університет «Львівська політехніка») з правом прийняття до розгляду та проведення захисту дисертації Курія Євгенія Олеговича з метою присудження ступеня доктора філософії з галузі знань 12 Інформаційні технології за спеціальністю 125 Кібербезпека — офіційний опонент. 6. Разова спеціалізована вчена рада 132 (13.08.2024, Національний університет «Львівська політехніка») з правом прийняття до розгляду та проведення захисту дисертації Журавчака Даниїла Юрійовича з метою присудження ступеня доктора філософії з галузі знань 12 Інформаційні технології за спеціальністю 125 Кібербезпека — офіційний опонент. Виконання функцій (повноважень, обов'язків) наукового керівника або відповідального

							виконавця наукової теми (проекту), або головного редактора/члена редакційної колегії/експерта (рецензента) наукового видання, включеного до переліку фахових видань України, або іноземного наукового видання, що індексується в бібліографічних базах 1. Член редакційної колегії електронного фахового наукового видання «Кібербезпека: освіта, наука, техніка» (електронне видання). 2. Член редакційної колегії електронного міжнародного наукового видання «International Journal of Wireless and Microwave Technologies» (електронне видання). 3. Член організаційного комітету міжнародної конференції «IEEE International Scientific-Practical Conference on Problems of Infocommunications Science and Technology» (індексується в Scopus). 4. Головний редактор міжнародної конференції «Workshop on Cybersecurity Providing in Information and Telecommunication Systems» (індексується в Scopus). 5. Редактор міжнародної конференції «Workshop on Classic, Quantum, and Post-Quantum Cryptography» (індексується в Scopus). 6. Член організаційного комітету міжнародної конференції «International Conference on Computer Science, Engineering and Education Applications» (індексується в Scopus). Участь у міжнародних наукових та/або освітніх проектах, залучення до міжнародної експертизи, наявність звання «суддя

							міжнародної категорії» 1. 01.02.2023–31.05.2023 «Development of DAO-modules for the DAO economic system» (XGROUP GLOBAL PTE Ltd., Сінгапур). 2. 01.08.2023–31.07.2024 «Research of Speech Emotion Recognition» (№89-080123, Ender Turing OÜ, Таллінн, Естонія). Діяльність за спеціальністю у формі участі у професійних та/або громадських об'єднаннях 1. Член «European Microwave Assosiation (EuMA)» (№ AM3734, з 2019 до 2026 р.). 2. Член «International Telecommunication Union (ITU-T)» (№ 1200190674, з 2017 до 2021 р.). Досвід практичної роботи за спеціальністю не менше п'яти років (крім педагогічної, науково-педагогічної, наукової діяльності) 1. Senior System Analyst / Proxy Product Owner (09.2022–07.2023, Pivotal Commware, США). 2. Senior System Analyst (08.2021–02.2022, Raiffeisen Bank, Україна). 3. Business Analyst (03.2020–07.2021, Competo, Азербайджан). Відомості про підвищення кваліфікації: 1.Підвищення кваліфікації науково-педагогічних працівників Університету за Дослідницьким модулем (поглиблений рівень). Київський університет імені Бориса Грінченка, 22.10.2021-30.11.2021. 30 год. (сертифікат № 1766/41 від 03.12.2021). 2. Інститут телекомунікацій та глобального інформаційного простору НАН України. Довідка № 161/24.05.2023-3. Тема: Створення нових LDPC кодів супутникового зв'язку за екстремальними графами. Від 24.05.2023р. 120

							годин (4 кредити ЄКТС). 3. Підвищення кваліфікації науково-педагогічних працівників Університету за Цифровим модулем. Київський університет імені Бориса Грінченка, 30 год. (наказ № 842 від 25.12.2023).
468580	Аносов Андрій Олександрович	Доцент, Основне місце роботи	Факультет інформаційних технологій та математики	Диплом спеціаліста, Вороніжське вище військове інженерне училище радіоелектроніки, рік закінчення: 1988, спеціальність: Командно-тактична, радіоелектронні засоби, Диплом магістра, Національна академія оборони України, рік закінчення: 1999, спеціальність: Організація бойового та оперативного забезпечення військ (сил), Диплом кандидата наук ДК 029855, виданий 30.06.2005, Атестат доцента 12ДЦ 044758, виданий 15.12.2015	41	Технології безпеки та управління критичними інфраструктурами	Відповідність освіти: 1.Воронізьке вище воєнне інженерне училище радіоелектроніки, 1988р. Спеціальність: «Командно-тактична, радіоелектронні засоби». Кваліфікація: «Радіо-інженер». 1.Національний академія оборони України, 1999р. Спеціальність: «Організація бойового та оперативного забезпечення військ (сил)». Кваліфікація: «Офіцер військового управління оперативно-тактичного рівня». 3.Кандидат військових наук, 2005р. 20.01.12 «Радіоелектронна боротьба, способи та засоби». Тема дисертації: «Методика обґрунтування раціональних способів радіоелектронного подавлення супутникових систем зв'язку». 4.Доцент кафедри інформаційної та кібернетичної безпеки, 2015 р. Наявність публікацій за профілем дисципліни у періодичних наукових виданнях, що включені до переліку фахових видань України, до наукометричних баз, зокрема Scopus, Web of Science Core Collection: 1. Zahynei, A. та Shcheblanin, Y. та Kurchenko, O. та Anosov, Andrii та Kruglyk, V. (2024) Method for Calculating the Residual Resource of Fog Node Elements of Distributed Information Systems of Critical Infrastructure Facilities Cybersecurity Providing in Information and Telecommunication Systems 2024, 3654. с. 432-439. ISSN 1613-

0073
2. Chernenko, Roman та Anosov, Andrii та Kyrychok, Roman та Brzhevska, Zoreslava та Spasiteleva, Svitlana (2022) Encryption Method for Systems with Limited Computing Resources Cybersecurity Providing in Information and Telecommunication Systems 2022, 3288 (1). с. 142-148. ISSN 1613-0073
3. Brzhevska, Zoreslava та Kyrychok, Roman та Anosov, Andrii та Skladannyi, Pavlo та Vorokhob, Maksym (2021) Analysis of the Process of Information Transfer from the Source-to-User in Terms of Information Impact Cybersecurity Providing in Information and Telecommunication Systems II 2021, 3188 (2). с. 257-264. ISSN 1613-0073
4. Brzhevska, Zoreslava та Haidur, Halyna та Dovzhenko, Nadiia та Anosov, Andrii та Vorokhob, Maksym (2021) Recurrent Estimation of the Information State Vector and the Correlation of Measuring Impact Matrix using a Multi-Agent Model Cybersecurity Providing in Information and Telecommunication Systems 2021, 2963. с. 272-276. ISSN 1613-0073
5. Черненко, Роман Миколайович та Рябчун, Олена Петрівна та Ворохоб, Максим Віталійович та Аносов, Андрій Олександрович та Козачок, Валерій Анатолійович (2021) Підвищення рівня захищеності систем мережі інтернету речей за рахунок шифрування даних на пристроях з обмеженими обчислювальними ресурсами Електронне фахове наукове видання "Кібербезпека: освіта, наука, техніка", 3 (11). с. 124-135. ISSN 2663-4023
6. Platonenko, Artem та Sokolov, V. Y. та Skladannyi, Pavlo та Anosov, A та Oleksiienko, H. (2021)

							Порівняння сучасних технічних засобів аеророзвідки для забезпечення безпеки контрольованої зони Кібербезпека: освіта, наука, техніка (13). с. 170-182. ISSN 2663-4023 Наявність виданих навчально-методичних посібників/посібників для самостійної роботи здобувачів вищої освіти та дистанційного навчання, електронних курсів на освітніх платформах: 1. Електронний навчальний курс з дисципліни «Захист інформації в інформаційно-комунікаційних системах» для бакалаврів спеціальності 125 Кібербезпека та захист інформації денної форми навчання. 2. Електронний навчальний курс з дисципліни : Моніторинг, аудит та адміністрування захищених IT систем і мереж (1 курс, 2р ВО, БІКС, очна). Освітньо-професійна програма 125.00.01 Безпека інформаційних і комунікаційних систем (2021, 2024). Магістр. (Наказ № 811 від 06.12.2021; Наказ № 699 від 02.11.2023 (пролонгація 2023/24 н.р.)) 3. Електронний навчальний курс з дисципліни: Технології безпеки мережевої та Smart інфраструктури (1 курс, 2р ВО, БІКС, очна). Освітньо-професійна програма 125.00.01 Безпека інформаційних і комунікаційних систем (2021, 2024). Магістр. (Наказ № 786 від 04.12.2023) Наукове керівництво (консультування) здобувача, який одержав документ про присудження наукового ступеня Черненко Роман Миколайович. Ступінь доктора філософії за спеціальності 125 Кібербезпека та захист інформації галузі знань 12 Інформаційні технології. Тема: Моделі та методи забезпечення захисту

							інформації, що передається відкритими каналами в мережах інтернету речей. 2024 р. Н24 № 002735 від 27.06.2024 Київський столичний університет імені Бориса Грінченка Виконання функцій (повноважень, обов'язків) наукового керівника або відповідального виконавця наукової теми (проекту), або головного редактора/члена редакційної колегії/експерта (рецензента) наукового видання, включеного до переліку фахових видань України, або іноземного наукового видання, що індексується в бібліографічних базах Член редакційної колегії електронного фахового наукового видання Київського столичного університету імені Бориса Грінченка "КІБЕРБЕЗПЕКА: ОСВІТА, НАУКА, ТЕХНІКА". Діяльність за спеціальністю у формі участі у професійних та/або громадських об'єднаннях Член "Internet Society (IS): Reston, VA, US" Відомості про підвищення кваліфікації: 1. Інститут телекомунікацій та глобального інформаційного простору НАН України. Довідка № 161/10.05.2023-1. Тема: «Робота зі шлюзом законного перехоплення для PS соге компанії». від 10.05.2023 р. 4 кредити ЄКТС (120 годин). 2. Підвищення кваліфікації науково-педагогічних працівників Університету за Лідерським модулем. Київський столичний університет імені Бориса Грінченка, 02.04.2024-09.04.2024. 30 год. (наказ № 397 від 25.04.2024).
468593	Жданова Юлія	Доцент, Основне	Факультет інформаційних	Диплом спеціаліста,	27	Прикладна загальна теорія	Відповідність освіти: 1.Ворошиловградськи

	Дмитрівна	місце роботи	технологій та математики	Ворошиловоградський державний інститут ім. Т.Г. Шевченка, рік закінчення: 1981, спеціальність: , Диплом спеціаліста, Державний університет телекомунікацій, рік закінчення: 2017, спеціальність: 7.17010101 безпека інформаційних і комунікаційних систем, Диплом кандидата наук КН 001399, виданий 29.12.1992, Атестат доцента 02ДЦ 015758, виданий 15.12.2005		систем безпеки	й державний педагогічний інститут імені Т.Г. Шевченка, 1981р., спеціальність – математика, кваліфікація – викладач математики; 2. Державний університет телекомунікацій, 2017р., спеціальність: «Безпека інформаційних і комунікаційних систем», кваліфікація: «Інженер із захисту інформації в інформаційних і комунікаційних системах» 3. Кандидат фізико-математичних наук, 1992р. 01.01.05 - Теорія ймовірностей і математична статистика. Тема дисертації: «Випадкові блукання та випадкові еволюції на скінченних розв'язуваних групах» 4. Доцент кафедри вищої математики, 2005р. Наявність публікацій за профілем дисципліни у періодичних наукових виданнях, що включені до переліку фахових видань України, до наукометричних баз, зокрема Scopus, Web of Science Core Collection: 1. Астапеня, Володимир Михайлович та Жданова, Юлія Дмитрівна та Шевченко, Світлана Миколаївна та Спасітєлєва, Світлана Олексіївна та Криворучко, О.В. (2024) Conflict Model of Radio Engineering Systems under the Threat of Electronic Warfare Proceedings of the Workshop Cybersecurity Providing in Information and Telecommunication Systems (CPITS 2024), 3654. с. 290-300. ISSN 1613-0073 (Scopus). 2. Шевченко, Світлана Миколаївна та Жданова, Юлія Дмитрівна та Астапеня, Володимир Михайлович та Негоденко, О.В. та Спасітєлєва, Світлана Олексіївна (2024) Conflicting Subsystems in the Information Space: A Study at the Software and Hardware

							Levels Proceedings of the Workshop Cybersecurity Providing in Information and Telecommunication Systems 2024, 3654. с. 333-342. ISSN 1613-0073 (Scopus). 3. Shevchenko, Svitlana та Zhdanova, Yuliia та Shevchenko, Halyna та Nehodenko, Olena та Spasiteleva, Svitlana (2023) Information Security Risk Management using Cognitive Modeling Cybersecurity Providing in Information and Telecommunication Systems, 3550. с. 297-305. ISSN 1613-0073 (Scopus). 4. Жданова Ю.Д. Математичні методи в кібербезпеці: теорія катастроф / С.М. Шевченко, Ю.Д. Жданова, С.О. Спасітєлєва // Кібербезпека: освіта, наука, техніка. – 2023, Том 3, № 19. – С. 165-175. 5. Zhdanova Yu. Conflict Analysis in the “Subject-to-Subject” Security System / S. Shevchenko, Y. Zhdanova, H. Shevchenko, O. Nehodenko, and S.Spasiteleva // CEUR Workshop Proceedings. 2023. V. 3421. 56–66. (Scopus). 6. Zhdanova Yu. Protection of Information in Telecommunication Medical Systems based on a Risk-Oriented Approach / S. Shevchenko, Y. Zhdanova, Yu. Dreis, R. Kyrychok, and D.Tsyrkaniuk // CEUR Workshop Proceedings. 2023. V. 3421. 158–167. (Scopus). 7. Жданова Ю.Д. Розробка безпечних контейнерних застосунків з мікросервісною архітектурою / С.О. Спасітєлєва, І.В. Чичкань, Ю.Д. Жданова, С.М. Шевченко // Кібербезпека: освіта, наука, техніка. – 2023, Том 1, № 21. – С. 193-210. 8. Grechaninov, Viktor та Khoshaba, Oleksandr та Hulak, Hennadii та Zhdanova, Yuliia та Melnyk, Iryna (2022) Models and Methods for

							Determining Application Performance Estimates in Distributed Structures Cybersecurity Providing in Information and Telecommunication Systems 2022, 3288 (1). с. 134-141. ISSN 1613-0073 (Scopus). 9. Dreis, Yurii та Ivanichenko, Yevhen та Nesterova, Olena та Zhdanova, Yuliia та Dmytriienko, Kate (2022) Restricted Information Identification Model Cybersecurity Providing in Information and Telecommunication Systems 2022, 3288 (1). с. 89-95. ISSN 1613-007 (Scopus). 10. Жданова Ю.Д. Інсайдери та інсайдерська інформація: суть, загрози, діяльність та правова відповідальність / С.М. Шевченко, Ю.Д. Жданова, П.М. Складанний, С.В. Бойко // Кібербезпека: освіта, наука, техніка. – 2022, Том 3, № 15. – С. 175-185. 11. Жданова Ю.Д. Уразливості шифрування коротких повідомлень в мобільних інформаційно-комунікаційних системах об'єктів критичної інфраструктури / Г.М. Гулак, Ю.Д. Жданова, П.М. Складанний, Є.Г. Гулак, В.А. Корнієць // Кібербезпека: освіта, наука, техніка. – 2022, Том 1, № 17. – С. 145-158. 12. H. Shevchenko, S. Shevchenko, Yu. Zhdanova, S. Spasiteleva, O. Negodenko. Information Security Risk Analysis SWOT. CEUR Workshop Proceedings. 2021. V. 2923. 309–317 (Scopus). 13. Жданова Ю.Д. Міждисциплінарний підхід до формування навичок управління ризиками ІБ на засадах теорії прийняття рішень / В.Л. Бурячок, Ю.Д. Жданова, С.М. Шевченко, П.М. Складанний // Кібербезпека: освіта, наука, техніка. – 2021,

							Том 3, № 11. – С. 155-165. 14. Жданова Ю.Д. Прикладні та методичні аспекти застосування хеш-функцій в інформаційній безпеці / Ю.Д. Жданова, С.О. Спасітєлєва, С.М. Шевченко, К.В. Кравчук // Кібербезпека: освіта, наука, техніка. – 2020, Том 4, № 8. – С.85-96. 15. Жданова Ю.Д. Проведення SWOT-аналізу оцінювання інформаційних ризиків як засіб формування практичних навичок студентів спеціальності 125 Кібербезпека / Ю.Д. Жданова, С.М. Шевченко, С.О. Спасітєлєва, П.М. Складанний // Кібербезпека: освіта, наука, техніка. – 2020, Том 2, № 10. – С. 158-168. Наявність виданого підручника чи навчального посібника (включаючи електронні) або монографії 1. Модель експертної системи для медичного скринінгу на основі методів кластерного аналізу / С.М. Шевченко, Ю.Д. Жданова, О.В. Негоденко, В.А. Куцук // Moderní aspekty vědy: XXVII. Díl mezinárodní kolektivní monografie / Mezinárodní Ekonomický Institut s.r.o. Česká republika: Mezinárodní Ekonomický Institut s.r.o., 2023. str. 495. – 478-494. 2. Теоретико-ймовірнісні та статистичні методи в захисті інформації. Підручник для студентів спеціальності 125 Кібербезпека / В.М. Астапеня, Ю.Д. Жданова, С.М. Шевченко. – К. Київський університет ім. Б.Грінченка. 2023. Наявність виданих навчально-методичних посібників/посібників для самостійної роботи здобувачів вищої освіти та дистанційного

							навчання, електронних курсів на освітніх платформах: 1. Електронний навчальний курс з дисципліни «Прикладна загальна теорія систем безпеки» для магістрів спеціальності 125 Кібербезпека та захист інформації денної форми навчання. 2. Електронний навчальний курс з дисципліни «Прикладна криптологія» для бакалаврів спеціальності 125 Кібербезпека та захист інформації денної форми навчання. 3. Електронний навчальний курс з дисципліни «Прийняття рішень в інформаційній і кібербезпеці» для бакалаврів спеціальності 125 та захист інформації Кібербезпека денної форми навчання. 4. Електронний навчальний курс з дисципліни «Вища математика: Математичний наліз та чисельні методи» для бакалаврів спеціальності 125 Кібербезпека та захист інформації денної форми навчання. 5. Електронний навчальний курс з дисципліни «Вища математика» для бакалаврів спеціальності 123 Комп'ютерна інженерія денної форми навчання. 6. Методичні рекомендації до виконання та захисту кваліфікаційної роботи бакалавра для студентів спеціальності 125 Кібербезпека освітньої програми 125.00.01 Безпека інформаційних і комунікаційних систем / Укладачі: Жданова Ю.Д., Шевченко С.М., Складанний П.М. – Київ: КУБГ. 2023. – 51 с. 7. Методичні рекомендації до виконання та захисту кваліфікаційної роботи магістра для студентів спеціальності 125 Кібербезпека та захист

							інформації освітньої програми 125.00.01 Безпека інформаційних і комунікаційних систем / Укладачі: Жданова Ю. Д., Складанний П. М., Шевченко С. М. – Київ: КУБГ, 2023. –57 с. Наявність апробаційних та/або науково-популярних, та/або консультаційних (дорадчих), та/або науково-експертних публікацій з наукової або професійної тематики: 1. Шевченко, Світлана Миколаївна та Жданова, Юлія Дмитрівна та Шевченко, Галина Володимирівна та Негоденко, Олена Василівна та Спасітєлєва, Світлана Олексіївна (2023) Conflict Analysis in the Information Security System: Subject - Subject CEUR Workshop Proceedings., 3421. с. 56-66. ISSN 1613-0073 2. Шевченко, Світлана Миколаївна та Жданова, Юлія Дмитрівна та Дрейс, Юрій Олександрович та Киричок, Роман Васильович та Цирканюк, Діана Андріївна (2023) Protection of Information in Telecommunication Medical Systems based on a Risk-Oriented Approach CEUR Workshop Proceedings. 2023. (3421). с. 158-167. ISSN 1613-0073 3. Shevchenko, Svitlana та Zhdanova, Yuliia та Shevchenko, Halyna та Nehodenko, Olena та Spasiteleva, Svitlana (2023) Information Security Risk Management using Cognitive Modeling Cybersecurity Providing in Information and Telecommunication Systems, 3550. с. 297-305. ISSN 1613-0073 4. Grechaninov, Viktor та Khoshaba, Oleksandr та Hulak, Hennadii та Zhdanova, Yuliia та Melnyk, Iryna (2022) Models and Methods for Determining Application Performance Estimates in Distributed

							Structures Cybersecurity Providing in Information and Telecommunication Systems 2022, 3288 (1). с. 134-141. ISSN 1613-0073 5. Dreis, Yurii та Ivanichenko, Yevhen та Nesterova, Olena та Zhdanova, Yuliia та Dmytriienko, Kate (2022) Restricted Information Identification Model Cybersecurity Providing in Information and Telecommunication Systems 2022, 3288 (1). с. 89-95. ISSN 1613-0073 6. Жданова Ю.Д., Шевченко С.М. Аналіз шляхів забезпечення кібербезпеки у віртуальному навчальному середовищі. Управління науковими та освітніми проєктами: матеріали всеукраїнського науково-педагогічного підвищення кваліфікації, 24 січня – 6 березня 2022 року. – Одеса: Видавничий дім «Гельветика», 2022. – 328 с. – С.133-136. 7. Жданова Ю.Д., Спасітєлєва С.О., Шевченко С.М. Активні методи навчання у вивченні ризиків інформаційної безпеки. Математика в сучасному технічному університеті : Матеріали IX Міжнар. наук.-практ. конф. «Математика в сучасному технічному університеті», Київ, 28–29 грудня 2020 р. — Вінниця: Видавець ФОП Кушнір Ю. В., 2021. – 330 с.– С.291-294. 8. Жданова Ю.Д., Спасітєлєва С.О., Шевченко С.М. Особливості застосування технологій захисту інформації в корпоративних освітніх мережах. Теоретико-практичні проблеми використання математичних методів і комп'ютерно-орієнтованих технологій в освіті та науці: зб. матеріалів III Всеукраїнської науково-практичної

							конференції, 28 квітня 2021 р., м. Київ / Київ. ун-т ім. Б. Грінченка. – К.: Київ. ун-т ім. Б. Грінченка, 2021. – 203 с. – С. 183-185. Діяльність за спеціальністю у формі участі у професійних та/або громадських об'єднаннях Член "Internet Society (IS): Reston, VA, US" Відомості про підвищення кваліфікації: 1. Підвищення кваліфікації науково-педагогічних працівників Університету за модулем «ІКТ». Київський університет імені Бориса Грінченка, 13.04.2020-25.04.2020. 30 год. (сертифікат № 1299 від 04.05.2020). 2. Підвищення кваліфікації науково-педагогічних працівників Університету за Лідерським модулем. Київський університет імені Бориса Грінченка, 18.02.2021-26.02.2021. 30 год. (сертифікат № 1510/41 від 05.03.2021). 3. Всеукраїнське науково-педагогічне підвищення кваліфікації «Управління науковими та освітніми проєктами» 24.01.2022-06.03.2022. 180 год. (сертифікат №ADV-240170-OLA від 06.03.2022). 4. Інститут телекомунікацій і глобального інформаційного простору НАН України, відділ інформаційної безпеки, овідка про проходження стажування № 161/12.05.2023-4, тема: «Криптографія з багатьма змінними, пов'язана з використанням алгебраїчної комбінаторики», від 10.05.2023 р., 4 кредити ЄКТС (120 годин) 5. Програма підвищення кваліфікації «Цифрові технології в наукових дослідженнях», 01.11 2023-13.12.2023, 60

							год. (сертифікат №20231213/171 від 13.12.2023).
468609	Козачок Валерій Анатолійович	Доцент, Основне місце роботи	Факультет інформаційних технологій та математики	Диплом спеціаліста, Київське вище інженерне радіотехнічне училище ППО, рік закінчення: 1988, спеціальність: радіотехнічні засоби, Диплом магістра, Національна академія оборони України, рік закінчення: 2006, спеціальність: Організація бойового та оперативного забезпечення військ (за видами та родами військ і сил), Диплом кандидата наук КН 014905, виданий 17.06.1997, Атестат доцента 12ДЦ 046343, виданий 25.02.2016	40	Технології розслідування інцидентів безпеки критичної інфраструктури	Відповідність освіти: 1.Київське вище інженерне радіотехнічне училище ППО, 1988р., спеціальність: «Радіотехнічні засоби», кваліфікація: радіоінженер. 2.Національна академія оборони України, 2006р., спеціальність: «Організація бойового та оперативного забезпечення військ (за видами та родами військ і сил)», кваліфікація: магістр військового управління, офіцер військового управління оперативно-тактичного рівня 3.Кандидат технічних наук, 1997р. 20.02.14 – озброєння та військова техніка. Тема дисертації: спеціальна. 4.Доцент кафедри інформаційної та кібернетичної безпеки, 2016р. Наявність публікацій за профілем дисципліни у періодичних наукових виданнях, що включені до переліку фахових видань України, до наукометричних баз, зокрема Scopus, Web of Science Core Collection: 1. Козачок В.А. Автоматизація процесів управління даними в хмарних сховищах / Шаповал, В. та Зубик, Л. та Зубик, Ю. та Курченко, О.// Забезпечення кібербезпеки в інформаційно-телекомунікаційних системах 2024, 3654. с. 410-418. ISSN 1613-073 2. Козачок В.А. Minimization of Bitsliced Representation of 4×4 S-Boxs based on Ternary Logic Instruction Cybersecurity / Sovyn, Y. and Khoma, V. and Opirskyy, I.// Providing in Information and Telecommunication Systems 2023, 3421. стор. 12-24. ISSN 1613-0073 3. Козачок В.А. Дослідження розвитку

							та інновації кіберзахисту на об'єктах критичної інфраструктури /Машталяр, Я.Р. та Бржевська, Зореслава Михайлівна та Богданов, Олександр Михайлович// Кібербезпека: освіта, наука, техніка, 2023, (2(22)). С. 156-167. ISSN 2663-4023 4. Козачок В.А. Аналіз методів виявлення дезінформації в соціальних мережах за допомогою машинного навчання / Марценюк, М.С. та Богданов, Олександр та Бржевська, Зореслава Михайлівна// Кібербезпека: освіта, наука, техніка, 2023, (2(22)). С. 148-155. 5. Козачок В.А. Виявлення відхилень в інформаційних процесах за допомогою мультифрактального аналізу. /Іваніченко, Євген та Дрейс, Юрій та Нестерова, Олена та Дмитрієнко, Кейт// Забезпечення кібербезпеки в інформаційно-телекомунікаційних системах II 2021, 3187 (1). С. 251-259. ISSN 1613-0073 6. Козачок В.А. Підхід до аналізу атак для зменшення пропусків у забезпеченні кібербезпеки. /Зибін, Сергій та Хорошко, Володимир та Хохлачова, Юлія// Управління ризиками в інформаційно-телекомунікаційних системах 2021, 2963. С. 318-328. ISSN 1613-0073 7. Козачок В.А. Метод побудови профілів користувача маркетплейсу і зловмисника / Цирканюк, Діана Андріївна та Соколов, Володимир Юрійович та Мазур, Наталія Петрівна та Астапеня, Володимир Михайлович// Кібербезпека: освіта, наука, техніка, 2021, 2 (14). с. 50-67. ISSN 2663-4023 8. Козачок В.А. Експериментальне визначення оптимальних параметрів роботи телеконференції на мобільних пристроях

							/ Биць, Андрій Віталійович та Соколов, Володимир Юрійович та Мазур, Наталія Петрівна та Бессалов, Анатолій Володимирович// Кібербезпека: освіта, наука, техніка, 2021 (2(14)). с. 68-86. ISSN 2663-4023 9. Козачок В.А. Підвищення рівня захищеності систем мережі Інтернету речей за рахунок шифрування даних на пристроях з обмеженими обчислювальними ресурсами / Р. М. Черненко, О.П. Рябчун, М.В. Ворохоб, А.О. Аносов // Кібербезпека: освіта, наука, техніка", 2021, 3 (11). с. 124-135. ISSN 2663-4023. 10. Козачок В.А. Використання ТРМ-модулів з метою підвищення захищеності інформаційно-телекомунікаційних систем / Козачок В.А// Збірник матеріалів III Всеукраїнської конференції «Теоретико-практичні проблеми використання математичних методів і комп'ютерно-орієнтованих технологій в освіті та науці» — К. : КУБГ, 2021. — С. 185–187. 11. Козачок В.А. Оцінка стану кібербезпеки критичної інформаційної інфраструктури в ході виявлення та відслідкування кризових індикаторів / І.В. Ткаченко, С.О. Гахов, В.Є. Дмітрієв // К., ДУТ, Збірник наукових праць «Сучасний захист інформації», 2020 р., вип. №1 (41). с. 54-57. Наявність виданого підручника чи навчального посібника (включаючи електронні) або монографії Козачок В.А., Коршун Н.В., Мазур Н.П., Платоненко А.В., Складанний П.М. Прикладні аспекти аналізу та синтезу політик безпеки. Навчальний посібник для студентів галузі

							знань 12 Інформаційні технології спеціальності 125 Кібербезпека – Київ: Вид-во КУБГ. 2021. - 160 с. Наявність виданих навчально-методичних посібників/посібників для самостійної роботи здобувачів вищої освіти та дистанційного навчання, електронних курсів на освітніх платформах: 1. Електронний навчальний курс з дисципліни : Прикладні аспекти побудови комплексу технічного захисту інформації (2 курс, 1р ВО, БІКС, очна). Освітньо-професійна програма 125.00.01 Безпека інформаційних та комунікаційних систем (2019, 2023). Бакалавр. (Наказ № 577 від 28.06.2024) 2. Електронний навчальний курс з дисципліни "Програмні комплекси захисту АС від несанкціонованого доступу" для бакалаврів 125 Кібербезпека та захит інформації денної форми навчання 3. Електронний навчальний курс з дисципліни "Технології розслідування інцидентів безпеки" для магістрів 125 Кібербезпека та захит інформації денної форми навчання 4. Електронний навчальний курс з дисципліни "Апаратне та програмне зебезпечення ПК" для бакалаврів 123 Комп'ютерна інженерія денної форми навчання Виконання функцій (повноважень, обов'язків) наукового керівника або відповідального виконавця наукової теми (проекту), або головного редактора/члена редакційної колегії/експерта (рецензента) наукового видання, включеного до переліку фахових видань України, або іноземного наукового видання, що

							індексується в бібліографічних базах Член редакційної колегії електронного фахового наукового видання Київського столичного університету імені Бориса Грінченка "КІБЕРБЕЗПЕКА: ОСВІТА, НАУКА, ТЕХНІКА". Діяльність за спеціальністю у формі участі у професійних та/або громадських об'єднаннях Член "Internet Society (IS): Reston, VA, US" Відомості про підвищення кваліфікації: 1.Підвищення кваліфікації науково-педагогічних працівників Університету за Лідерським модулем. Київський університет імені Бориса Грінченка, 18.02.2021-26.02.21, 30 год. (сертифікат № 1516/41 від 05.03.2021). 2. Підвищення кваліфікації науково-педагогічних працівників Університету за Дослідницьким модулем. Київський університет імені Бориса Грінченка, 18.10.2021-26.11.2021. 30 год. (сертифікат № 1787/41 від 30.11.2021). 3. Інститут телекомунікацій та глобального інформаційного простору НАН України. Довідка № 161/10.05.2023-5. Тема: Криптографія з багатьма змінними, пов'язана з використанням алгебраїчної комбінаторики. Від 10.05.2023р. 4 кредити ЄКТС (120 годин). 4. Підвищення кваліфікації науково-педагогічних працівників Університету за Лідерським модулем. Київський столичний університет імені Бориса Грінченка. 02.04.2024-09.04.2024, 30 год. (наказ №397 від 25.04.2024 р.)
468544	Складанний Павло Миколайови	Завідувач кафедри, Основне	Факультет інформаційних технологій та	Диплом бакалавра, Державний	9	Організація науки і наукових	Відповідність освіти: 1.Державний університет

	ч	місце роботи	математики	університет інформаційно-комунікаційних технологій, рік закінчення: 2013, спеціальність: Безпека інформаційних і комунікаційних систем, Диплом спеціаліста, Державний університет телекомунікацій, рік закінчення: 2015, спеціальність: , Диплом магістра, Державний університет телекомунікацій, рік закінчення: 2014, спеціальність: Безпека інформаційних і комунікаційних систем, Диплом кандидата наук ДК 061086, виданий 29.06.2021, Атестат доцента АД 011358, виданий 10.10.2022		досліджень	телекомунікацій, 2014р. Спеціальність: «Безпека інформаційних і комунікаційних систем».Кваліфікація: «Професіонал із організації інформаційної безпеки» 2.Кандидат технічних наук, 2021р. 05.13.06 – Інформаційні технології. Тема дисертації: «Моделі і методи забезпечення імітостійкості та конфіденційності в системах обробки інформації» 3.Доцент кафедри інформаційної та кібернетичної безпеки, 2022 р. Наявність публікацій за профілем дисципліни у періодичних наукових виданнях, що включені до переліку фахових видань України, до наукометричних баз, зокрема Scopus, Web of Science Core Collection: 1. Шевченко, Світлана Миколаївна та Жданова, Юлія Дмитрівна та Спасітєлєва, Світлана Олексіївна та Мазур, Наталія Петрівна та Складанний, Павло Миколайович та Негоденко, Віталій Петрович (2024) Математичні методи в кібербезпеці: кластерний аналіз та його застосування в інформаційній та кібернетичній безпеці Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка», 23 (3). с. 258-273. ISSN 2663-4023. 2. Костюк, Юлія Володимирівна та Бебешко, Богдан Тарасович та Крючкова, Лариса Петрівна та Литвинов, В.А. та Оксанич, І.М. та Складанний, Павло Миколайович та Хорольська, К.В. (2024) Захист інформації та безпека обміну даними в безпроводових мобільних мережах з автентифікацією і протоколами обміну ключами Кібербезпека: освіта, наука, техніка, 1 (25). с. 229-252. ISSN 2663-4023

							3. Довженко, Надія Михайлівна та Іваніченко, Євген Вікторович та Складанний, Павло Миколайович та Аушева, Н.М. (2024) Інтеграція безпеки та відмовостійкості сенсорних мереж на основі аналізу енергоспоживання та трафіку Кібербезпека: освіта, наука, техніка, 1 (25). с. 390-400. ISSN 2663-4023 4. Bessalov, Anatoly та Abramov, Serhii та Sokolov, Volodymyr та Skladannyi, Pavlo та Zhyltsov, Oleksii (2023) Multifunctional CRS Encryption Scheme on Isogenies of Non-Supersingular Edwards Curves Workshop on Classic, Quantum, and Post-Quantum Cryptography (CQPC 2023), 3504. с. 12-25. ISSN 1613-0073 (Scopus). 5. Marusenko, R. та Sokolov, V. Y. та Skladannyi, Pavlo (2023) Social Engineering Penetration Testing in Higher Education Institutions In: Lecture Notes on Data Engineering and Communications Technologies. Springer, с. 1132-1147. (Scopus). 6. Buriachok, Volodymyr та Korshun, Natalia та Zhyltsov, Oleksii та Sokolov, Volodymyr та Skladannyi, Pavlo (2023) Implementation of Active Cybersecurity Education in Ukrainian Higher School Lecture Notes on Data Engineering and Communications Technologies, 178. с. 533-551. ISSN 2367-4512 (Scopus). 7. Sokolov, Volodymyr та Skladannyi, Pavlo та Astapenya, Volodymyr (2023) Bluetooth Low-Energy Beacon Resistance to Jamming Attack 2023 IEEE 13th International Conference on Electronics and Information Technologies (ELIT). с. 270-274. ISSN 979-8-3503-8309-6 (Scopus). 8. Astafieva, Mariia та Bodnenko, Dmitry та Lytvyn, Oksana та Proshkin, Volodymyr та Skladannyi, Pavlo (2023) Formation of

							High School Students' Resistance to Destructive Information Influences Cybersecurity Providing in Information and Telecommunication Systems 2023, 3421. с. 87-96. ISSN 1613-0073 (Scopus). 9. Anakhov, P. та Zhebka, V. та Kravchenko, V. та Skladannyi, Pavlo та Zhyltsov, Oleksii (2023) Hybrid Study of the Geophysical Situation in the Depressed Zone of Hydroelectric Power Plants Reservoir Cybersecurity Providing in Information and Telecommunication Systems, 3550. с. 269-274. ISSN 1613-0073 (Scopus). 10. Skladannyi, Pavlo та Trofimov, Olexandr та Korniiets, Viktor та Vorokhob, Maksym та Opryshko, Tetiana (2023) Improving the Security Policy of the Distance Learning System based on the Zero Trust Concept CPITS 2023: Workshop on Cybersecurity Providing in Information and Telecommunication Systems. с. 97-106. ISSN 1613-0073 (Scopus). 11. Kipchuk, F. та Sokolov, Volodymyr та Skladannyi, Pavlo та Zhyltsov, Oleksii та Ageyev, D. (2023) Method for Increasing the Various Sources Data Consistency for IoT Sensors IEEE 9th International Conference on Problems of Infocommunications, Science and Technology (PICST). с. 522-526. ISSN 979-8-3503-9891-5 (Scopus). 12. Anakhov, P. та Zhebka, V. та Popereshnyak, S та Skladannyi, Pavlo та Sokolov, Volodymyr (2023) Protecting Objects of Critical Information Infrastructure from Wartime Cyber Attacks by Decentralizing the Telecommunications Network Cybersecurity Providing in Information and Telecommunication Systems, 3550. с. 240-245. ISSN 1613-0073 (Scopus). 13. Соколов,

							Володимир Юрійович та Складанний, Павло Миколайович (2023) Методика оцінки комплексних збитків від інциденту інформаційної безпеки Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка», 1 (21). с. 99-120. ISSN 2663-4023 Наявність виданого підручника чи навчального посібника (включаючи електронні) або монографії 1. Гулак Г. М., Жильцов О. Б., Киричок Р. В., Коршун Н. В., Складанний П. М. Інформаційна та кібернетична безпека підприємства: підруч. / Г. М. Гулак, О. Б. Жильцов, Р. В. иричок, Н. В. Коршун, П. М. Складанний – 2023. – 370 с. 2. Козачок В.А., Коршун Н.В., Мазур Н.П., Платоненко А.В., Складанний П.М. Прикладні аспекти аналізу та синтезу політик безпеки. Навчальний посібник для студентів галузі знань 12 Інформаційні технології спеціальності 125 Кібербезпека – Київ: Вид-во КУБГ. 2021. - 160 с. 3. Астапеня, Володимир Михайлович та Бржевська, Зореслава Михайлівна та Мазур, Наталія Петрівна та Складанний, Павло Миколайович та Тихонов, Юрій Олександрович (2023) Теорія електричних кіл і сигналів в інформаційному та кіберпросторах: Навчальний посібник. Київський університет імені Бориса Грінченка, Україна, Київ. - 209 с. Наявність виданих навчально-методичних посібників/посібників для самостійної роботи здобувачів вищої освіти та дистанційного навчання, електронних курсів на освітніх платформах: 1. Електронний навчальний курс з дисципліни Основи

							інформаційної і кібербезпеки та захисту інформації (1 курс, 1р ВО, БІКС, очна). Освітньо-професійна програма 125.00.01 Безпека інформаційних та комунікаційних систем (2019, 2023). Бакалавр. (Наказ № 385 від 04.06.2021; Наказ № 699 від 02.11.2023 (пролонгація 2023/24 н.р.)). 2. Електронний навчальний курс з дисципліни Системний аналіз та прийняття рішень в інформаційній і кібербезпеці (1 курс, АСП). Освітньо-наукова програма 125. Кібербезпека (2022). Доктор філософії. Освітньо-наукова програма 125. Кібербезпека (2020). Доктор філософії. (Наказ № 856 від 30.12.2021; Наказ № 843 від 25.12.2023 (пролонгація 2023/24 н.р.)). 3. Електронний навчальний курс з дисципліни Організація науки і наукових досліджень (1 курс, 2р ВО, БІКС, очна). Освітньо-професійна програма 125.00.01 Безпека інформаційних і комунікаційних систем (2021, 2024). Магістр. (Наказ № 212 від 02.05.2022; Наказ № 699 від 02.11.2023 (пролонгація 2023/24 н.р.)). 4. Електронний навчальний курс з дисципліни Основи інформаційної безпеки (2 курс, КВД, денна). Освітньо-професійна програма 029.00.02 Інформаційна, бібліотечна та архівна справа (2021). Бакалавр. Освітньо-професійна програма 073.00.01 Менеджмент організацій (2021). Бакалавр. (Наказ № 266 від 03.06.2022; Наказ № 843 від 25.12.2023 (пролонгація 2023/24 н.р.)). 5. Методичні рекомендації до виконання та захисту кваліфікаційної роботи бакалавра для студентів

							спеціальності 125 Кібербезпека освітньої програми 125.00.01 Безпека інформаційних і комунікаційних систем / Укладачі: Жданова Ю.Д., Шевченко С.М., Складанний П.М. – Київ: КУБГ. 2023. – 51 с. 6. Методичні рекомендації до виконання та захисту кваліфікаційної роботи магістра для студентів спеціальності 125 Кібербезпека та захист інформації освітньої програми 125.00.01 Безпека інформаційних і комунікаційних систем / Укладачі: Жданова Ю. Д., Складанний П. М., Шевченко С. М., Гулак Г.М. – Київ: КУБГ, 2023. –57 с. Захист дисертації на здобуття наукового ступеня 26 червня 2021 року рішенням Атестаційної колегії Міністерства освіти і науки України присвоєно науковий ступінь кандидата технічних наук за спеціальністю 05.13.06 – Інформаційні технології. Тема дисертації: "Моделі і методи забезпечення імітостійкості та конфіденційності в системах обробки інформації" Наукове керівництво (консультування) здобувача, який одержав документ про присудження наукового ступеня 1. Ворохоб Максим Віталійович. Ступінь доктора філософії за спеціальності 125 Кібербезпека та захист інформації галузі знань 12 Інформаційні технології. Тема: Моделі і методи вдосконалення політики безпеки підприємства на основі методології Zero Trust. 2024 р. Диплом Н24 № 002138 від 03.04.2024 Київським столичним університетом імені Бориса Грінченка Виконання функцій (повноважень, обов’язків) наукового керівника або відповідального

							виконавця наукової теми (проекту), або головного редактора/члена редакційної колегії/експерта (рецензента) наукового видання, включеного до переліку фахових видань України, або іноземного наукового видання, що індексується в бібліографічних базах Головний редактор електронного фахового наукового видання Київського столичного університету імені Бориса Грінченка "КІБЕРБЕЗПЕКА: ОСВІТА, НАУКА, ТЕХНІКА". Участь у міжнародних наукових та/або освітніх проектах, залучення до міжнародної експертизи, наявність звання «суддя міжнародної категорії» 1. «Research of Speech Emotion Recognition» за грантом №89-080123 від Ender Turing OÜ (Таллін, Естонія) з 01.08.2023 по 31.07.2024. 2. «Development of DAO-modules for the DAO economic system» з 01.02.2023 по 31.05.2023. Наявність апробаційних та/або науково-популярних, та/або консультаційних (дорадчих), та/або науково-експертних публікацій з наукової або професійної тематики загальною кількістю не менше п’яти публікацій 1. Zhebka, V. та Skladannyi, Pavlo та Zhebka, S. та Shlianchak, S. та Bondarchuk, A. (2024) Methodology for Predicting Failures in a Smart Home based on Machine Learning Methods Cybersecurity Providing in Information and Telecommunication Systems 2024, 3654. с. 322-332. ISSN 1613-0073 2. Dudykevych, V. та Mykytyn, G. та Stosyk, T. та Skladannyi, Pavlo (2024) Platform for the Security of Cyber-Physical Systems and the IoT in the

							Intellectualization of Society Cybersecurity Providing in Information and Telecommunication Systems 2024, 3654. с. 449-457. ISSN 1613-0073 3. Kriuchkova, Larysa та Sokolov, Volodymyr та Skladannyi, Pavlo (2024) Determining the Zone of Successful Interaction in RFID Technologies 2024 IEEE 29th International Seminar/Workshop on Direct and Inverse Problems of Electromagnetic and Acoustic Wave Theory (DIPED). с. 168-171. ISSN 979-8-3315-0608-7 4. Hulak, Hennadii та Skladannyi, Pavlo та Sokolov, Volodymyr та Hulak, E. та Korniiets, V. (2022) Dynamic model of guarantee capacity and cyber security management in the critical automated systems 2nd International Conference on Conflict Management in Global Information Networks (CMiGiN 2022), 3530. с. 102-111. ISSN 1613-0073 5. Anakhov, P. та Zhebka, V. та Tushych, A. та Kravchenko, V. та Blazhennyi, N. та Skladannyi, Pavlo та Sokolov, Volodymyr (2022) Evaluation Method of the Physical Compatibility of Equipment in a Hybrid Information Transmission Network Journal of Theoretical and Applied Information Technology, 100 (22). с. 6635-6644. ISSN 1817-3195 6. Astapenya, Volodymyr та Sokolov, Volodymyr та Skladannyi, Pavlo (2022) Problematic Issues of the Accelerating Lens Deployment 2022 IEEE 2nd Ukrainian Microwave Week (UkrMW). с. 337-341. ISSN 979-8-3503-3152-3 7. Romanovskyi, O. та Iosifov, Ievgen та Iosifova, Olena та Sokolov, Volodymyr та Skladannyi, Pavlo та Sukaylo, Igor (2022) Prototyping Methodology of End-to-

							End Speech Analytics Software Modern Machine Learning Technologies and Data Science Workshop, 3312 (1). с. 76-86. ISSN 1613-0073 8. Brzhevska, Zoreslava та Kyrychok, Roman та Anosov, Andrii та Skladannyi, Pavlo та Vorokhob, Maksym (2021) Analysis of the Process of Information Transfer from the Source-to-User in Terms of Information Impact Cybersecurity Providing in Information and Telecommunication Systems II 2021, 3188 (2). с. 257-264. ISSN 1613-0073 Керівництво студентом, який зайняв призове місце на І або ІІ етапі Всеукраїнської студентської олімпіади (Всеукраїнського конкурсу студентських наукових робіт) 1. Репін Владислав Володимирович, переможець І туру Всеураїнського конкурсу студентських наукових робіт зі спеціальності 125 Кібербезпека (2021 рік). 2. Марценюк Максим Станіславович, переможець І туру Всеураїнського конкурсу студентських наукових робіт зі спеціальності 125 Кібербезпека (2022 рік). Діяльність за спеціальністю у формі участі у професійних та/або громадських об'єднаннях Член "Internet Society (IS): Reston, VA, US" Відомості про підвищення кваліфікації: 1. Підвищення кваліфікації науково-педагогічних працівників Університету за Дослідницьким модулем. Київський університет імені Бориса Грінченка, 08.10.2020-26.11.2020. 30 год. (сертифікат № 1453/41 від 01.12.2020). 2. Підвищення кваліфікації науково-педагогічних працівників Університету за

							Лідерським модулем. Київський університет імені Бориса Грінченка, 24.11.2020-30.11.2020. 30 год. (сертифікат № 1477/41 від 04.12.2020). 3. Фаховий модуль (стажування) «Academic innovations and online learning methodology: psychological, technological and ethical aspects», 07.06.2021-11.07.2021, 180 год. (6 ECTS), Europejska Uczelnia Spoleczno-Techniczna, Варшава, Польща (сертифікат № AD 084-210711). 4. Підвищення кваліфікації науково-педагогічних працівників Університету за Дослідницьким модулем (поглиблений рівень). Київський університет імені Бориса Грінченка, 22.10.2021-30.11.2021. 30 год. (сертифікат № 1765/41 від 03.12.2021). 5. Інститут телекомунікацій та глобального інформаційного простору НАНУ, відділ інформаційної безпеки. Довідка № 161/24.05.23-2. Тема: Створення нових LDPC кодів супутникового зв'язку за екстремальними графами. Від 24.05.2023 р. 120 годин (4 кредити ЄКТС). 6. Підвищення кваліфікації науково-педагогічних працівників Університету за Лідерським модулем. Київський столичний університет імені Бориса Грінченка, 31.01.2024-06.02.2024. 30 год. (наказ № 323 від 01.04.2024).

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

Програмні результати навчання ОП	**ПРН відповідає результату навчання, визначеному стандартом вищої**	**Обов'язкові освітні компоненти, що забезпечують ПРН**	**Методи навчання**	**Форми та методи оцінювання**

	освіти (або охоплює його)			