НАЦІОНАЛЬНЕ АГЕНТСТВО ІЗ ЗАБЕЗПЕЧЕННЯ ЯКОСТІ ВИЩОЇ ОСВІТИ

ВІДОМОСТІ
про самооцінювання освітньої програми

Заклад вищої освіти	**Національний університет "Чернігівська політехніка"**
Освітня програма	**59717 Кібербезпека**
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	**140**
Повна назва ЗВО	**Національний університет "Чернігівська політехніка"**
Ідентифікаційний код ЗВО	**05460798**
ПІБ керівника ЗВО	**Новомлинець Олег Олександрович**
Посилання на офіційний веб-сайт ЗВО	**stu.cn.ua**

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

https://registry.edbo.gov.ua/university/140

3. Загальна інформація про ОП, яка подається на акредитацію

ID освітньої програми в ЄДЕБО	**59717**
Назва ОП	**Кібербезпека**
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, Магістр (ОКР «спеціаліст»)**
Структурний підрозділ (кафедра або інший підрозділ), відповідальний за реалізацію ОП	**Кафедра кібербезпеки та математичного моделювання**
Інші навчальні структурні підрозділи (кафедра або інші підрозділи), залучені до реалізації ОП	**Кафедра харчових технологій та екології; кафедра іноземної філології**
Місце (адреса) провадження освітньої діяльності за ОП	**вул.Шевченка, 95, м.Чернігів, 14035**
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	**229875**
ПІБ гаранта ОП	**Ткач Юлія Миколаївна**
Посада гаранта ОП	**Завідувачка кафедри / Професор**
Корпоративна електронна адреса гаранта ОП	**tkachym@stu.cn.ua**
Контактний телефон гаранта ОП	**+38(063)-594-22-94**
Додатковий телефон гаранта ОП	*відсутній*

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

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

Освітньо-професійна програма «Кібербезпека» другого (магістерського) рівня вищої освіти (далі – ОПП) розроблена на підставі Закону України «Про вищу освіту».
Передумовами започаткування даної спеціальності, в тому числі зазначеної ОПП, стало те, що сьогодні відбувається постійне зростання кількості кібератак на інформаційні системи державних та приватних структур, включаючи атаки на об'єкти критичної інфраструктури (енергетика, транспорт, банківський сектор та інші), що в свою чергу спричинили зростання попиту у висококваліфікованих фахівцях за спеціальністю 125 Кібербезпека та захист інформації. Таким чином, високий суспільний запит на фахівців з кібербезпеки та наявність відповідної кадрової та матеріально-технічної бази спонукали до відкриття даної спеціальності в університеті.
ОПП розроблено проєктною групою науково-педагогічних працівників (НПП) у складі керівника групи Ткач Юлії Миколаївни, к.т.н, д.пед.н., професора та членів проектної групи Шелеста Михайла Євгеновича, д.т.н., професора, Петренка тараса Анатолійовича, к.т.н.
Рецензентами ОПП виступили провідні фахівці сфери захисту інформації, а саме: Смірнов Олексій Анатолійович, д. т. н., професор, завідувач кафедри кібербезпеки та програмного забезпечення Центральноукраїнського національного технічного університету (м. Кропивницький); Богдан Дмитро, начальник відділу протидії кіберзлочинам в Чернігівській області Департаменту кіберполіції НП України;
Постернак Юрій Миколайович, начальник Управління Державної служби спеціального зв'язку та захисту інформації України в Чернігівській області;
Лисиця Ірина Миколаївна, директор Chernihiv IT;
Ревунов Павло, начальник Управління Служби безпеки України в Чернігівській області,
Сорока Б.І., IT кластер, Зайцев С.В., директор ТОВ "Інформаційна бехпека", Євсеєв С.П., доктор технічних наук, професор, завідуючий кафедри кібербезпека НТУ «Харківський політехнічний інститут»
Відгуки рецензентів позитивні.
ОПП затверджено Вченою радою Чернігівського національного технологічного університету (протокол від 27.08.2019 No 7) та введено в дію з 01.09.2019 наказом ректора від 27.08.2019 No 94. По теперішній час до ОПП систематично вносяться зміни.

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	*З*	*ОД*	*З*
1 курс	2025 - 2026	0	21	18	0	0
2 курс	2024 - 2025	0	17	11	0	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	**59648 Кібербезпека**
другий (магістерський) рівень	**59717 Кібербезпека**
третій (освітньо-науковий/освітньо-творчий) рівень	*програми відсутні*

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

	Загальна площа	Навчальна площа
Усі приміщення ЗВО	83157	49455

Власні приміщення ЗВО (на праві власності, господарського відання або оперативного управління)	68018	38024
Приміщення, які використовуються на іншому праві, аніж право власності, господарського відання або оперативного управління (оренда, безоплатне користування тощо)	0	0
Приміщення, здані в оренду	15139	11430

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	*OPP_125_Cyber_Security_master_2024_2v_ (1).pdf*	R8QewhnyHFI5XiKREe81LZ9UAOO5TEEOzLF/emggGoQ=
Навчальний план за ОП	*NP_125_Cyber_Security_master_2024_2.pdf*	PCf5PyQFn5V2IGfcBXDAvE2u++U/Hx77bryLdd6I5LA=
Навчальний план за ОП	*NP_125_Cyber_Security_master_2024_z.pdf*	7czMf4Cgx8HS+zyarz1If1Zzy+nGAQ/Mkf5wt+3N+E4=
Матеріали від ЗВО: пропозиції та рекомендації від роботодавців, таблиця відповідності публікацій наукових керівників напрямам (тематикам) досліджень аспірантів (для ОП третього рівня освіти)	*Recenzi_125_Cyber_Security_master_2024.pdf*	WPH280DxeKpXbPAgsE4wzBHS46LJ3gsoG78mbPo/YUU=

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?

ОПП «Кібербезпека» підготовки здобувачів другого (магістерського) рівня вищої освіти затверджена у 2019 році. Розробка відбувалась за відсутності відповідного Стандарту освіти. Після затвердження Стандарту (Наказ МОН від 18.03.2021 №332)ОПП була
приведена у відповідність йому, а саме: уточнено цілі ОП, загальні та фахові компетентності, РН; оновлено перелік обов'язкових дисциплін, які на 100 % забезпечують компетентності та РН освітнього Стандарту, збільшена кількість кредитів на Переддипломну практику (до 15 кредитів). Згідно зі Стандартом вищої освіти в ОПП передбачено можливість вільного вибору дисциплін для реалізації індивідуальної освітньої траєкторії здобувачів вищої освіти. В подальшому ОПП регулярно оновлювалась.

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

ОПП не передбачає присвоєння професійної кваліфікації. Проте підготовка фахівців за освітньо-професійною програмою 'Кібербезпека' другого (магістерського) рівня вищої освіти орієнтована на вимоги Професійного стандарту 'Адміністратор мереж і систем', затвердженого наказом Адміністрації Державної служби спеціального зв'язку та захисту інформації України від 25 листопада 2022 року № 715 (https://qc.csi.cip.gov.ua/uk/pages/professional-qualifications). Програма забезпечує здобувачів необхідними знаннями та навичками для встановлення, підтримки та адміністрування мережевих і системних ресурсів, конфігурування та оновлення апаратного і програмного забезпечення, управління базами даних, резервного копіювання та відновлення, а також реалізації заходів з кібербезпеки в організаціях відповідно до сучасних стандартів та вимог інформаційної безпеки.
З метою орієнтації на один з професійних стандартів гарантом було проаналізовано відповідність навчальних дисциплін вимогам зазначеного вище професійного стандарту('Адміністратор мереж і систем'), за результатом аналізу актуалізовано зміст робочих програм шляхом розширення змістових модулів щодо охоплення ключових компетентностей.

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

Рез-ти моніторингу відгуків та пропозицій зд-чів щодо змісту ОПП пок-ть, що студенти прагнуть розвивати інновацій у навчанні, комунікації та співпраці, поглиблено вивчати передові технології кіберзахисту. Ці проп-ії розглядаються як на зустрічах зі стейкхолдерами, так під час засідань кафедри, щорічного Meetup «Актуальні питання кібербезпеки» та Всеукраїнської науково-практичної конференції молодих науковців, аспірантів "Юність науки". Під час обговорення пропозицій проводиться аналіз їх кореляції з метою та РН ОПП та можуть вноситись зміни як до самої ОПП так і до робочих програми окремих дисциплін.
Випускник Шпитальний Б. (наразі АТ "ЧЕРНІГІВОБЛЕНЕРГО"-фахівець з кібербезпеки) запр-в до вив-ня пит-ня, які пов'язані з УІБ на підприємстві. Такми чином, було повністю сформовано новий модуль робочої програми ОК5 "Стандартизація, сертифікація засобів та комплексів захисту інформації".
Ст-т Дятел І. запропонував додати в навч.дисц-ни теми про сканування мереж за допомогою nmap, виявлення та використання вразливостей у комп'ютерних системах та мережах. В дисципліну «Управління мережевою безпекою» було додано детальний опис архітектури мереж WPA та WPA2 з попередньо розданим ключем (PSK) та ін. Додатково, студентам-магістрам надається можливість пройти навчальний курс "Ethical Hacker" в Академії Cisco НУ "Чернігівська політехніка". За рез-ми опит-ня здобувачі освіти задоволені наповненням ОПП.

- роботодавці

Для розробки ОПП "Кібербезпека" запрошувались представники різних зацікавлених сторін (державних установ, Держспецзв'язку, Департаменту кіберполіції Національної поліції України, представників Чернігівського IT Кластера тощо).
Випусковою кафедрою систематично проводяться зустрічі з роботодавцями та обговорення вимог до фахівця на ринку праці (напр. протокол №3, від 13.03.2025).
В результаті такої взаємодії з урахуванням специфіки ОПП, введенням в дію Професійних стандартів та необхідності орієнтації на один з них, пропозицій роботодавців, зокрема враховано пропозицію представника Держспецзв'язку відносно перенесення з числа вибіркових дисциплін у обов'язкові дисципліну ОК 7 "Технології безпеки бездротових і мобільних мереж".
Аналіз цих зустрічей дозволив зробити висновок, що вимоги роботодавців до потенційних випускників-кандидатів на працевлаштування корелюють з метою, змістом та РН чинної редакції ОПП.
У межах діяльності Екзаменаційної комісії, що проводить атестацію здобувачів освіти, випускова кафедра запрошує до головування представників роботодавців. Висновки та рекомендації, висловлені членами ЕК, використовуються для вдосконалення освітньої програми,наприклад, шляхом коригування змісту робочих програм, переліку дисциплін як обов'язкових, так і вибіркових.

- академічна спільнота

Співпраця з представниками українських та закордонних закладів вищої освіти сприяє врахуванню інтересів академічної спільноти у формуванні мети та програмних результатів освітньо-професійної програми. Це відбувається шляхом обміну досвідом та активного обговорення під час науково-практичних секцій, міжуніверситетських і міжнародних наукових конференцій, семінарів, круглих столів та інших фахових заходів, що дозволяє адаптувати навчальні програми до сучасних викликів у сфері кібербезпеки та інформаційного захисту.
Додатковим чинником підвищення ефективності співпраці є залучення здобувачів освіти та викладачів випускової кафедри до міжнародних освітніх проєктів, які реалізуються за участі українських закладів вищої освіти. Зокрема, гарант освітньої програми Ткач Ю.М. брала участь у міжнародному проєкті Erasmus+, що спрямований на розвиток освіти, підвищення кваліфікації та зміцнення співпраці з європейськими університетами. У межах цього проєкту викладачі пройшли стажування у провідних університетах ЄС, що посприяло оновленню навчальних програм, інтеграції інноваційних методик викладання та обміну досвідом у підготовці майбутніх фахівців із кібербезпеки.
Відповідно до сучасних вимог ринку праці та на основі рекомендацій представників академічної спільноти (рецензентів) – до освітнього процесу було інтегровано додаткові питання, що охоплюють сучасні методи захисту інформаційних систем.

- інші стейкхолдери

Серед інших зацікавлених сторін - територіальна громада м. Чернігова, соціально-економічний розвиток якої безпосередньо залежить від підвищення рівня локальної економіки та ефективного використання людського капіталу, чому значною мірою сприяє діяльність Університету. Відповідно до місії та стратегічних цілей, Університет відіграє фундаментальну роль у розвитку міста, зокрема через удосконалення його освітнього, наукового та інноваційного потенціалу.
Функціонування та реалізація освітньо-професійної програми "Кібербезпека" сприяє підготовці висококваліфікованих фахівців, здатних ефективно інтегруватися у професійне середовище, зокрема у сферах інформаційної безпеки та інформаційних технологій. Випускники програми забезпечують зростання кадрового потенціалу як державних установ, так і комерційного сектору, включаючи місцеві підприємства IT-галузі, що, у свою чергу, сприяє підвищенню рівня цифрової трансформації регіону, стимулюванню інноваційних процесів та економічному зростанню міста.

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

Національний університет «Чернігівська політехніка» визначає свою місію як сприяння розвитку суспільства через освіту та наукові дослідження, що спрямовані на формування лідерства та вирішення актуальних глобальних викликів. Реалізація цієї місії здійснюється шляхом досягнення стратегічних цілей університету, визначених на офіційному вебресурсі: https://stu.cn.ua/universytet/misiya-ta-strategiya/ .
Цілі освітньо-професійної програми повністю узгоджуються з місією та стратегією університету, оскільки програма

спрямована на підготовку висококваліфікованих спеціалістів, які мають глибокі фундаментальні знання, практичні навички, а також здатні ефективно працювати в команді та адаптуватися до динамічних змін ринку праці й стрімкого розвитку технологій.
Що в свою чергу передбачає інноватівність, збалансованість, успіх і реалізується через розвиток системи освіти та наукової діяльності шляхом підготовки високопрофесійних, конкурентоспроможних фахівців, здатних активно діяти в умовах ринкової економіки та соціального партнерства; розвиток наукових пріоритетів, наукових шкіл, інноваційної складової.
Крім того, програма передбачає розширення міжнародної співпраці із закордонними закладами вищої освіти, зокрема через можливість здобуття подвійних дипломів. Одним із прикладів такої співпраці є спільна програма з Техніко-гуманітарною академією в м.Бельсько-Бяла (Польща), яка затверджена ухвалою Сенату Університету Бельсько-Бяла(УББ).

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

Останні роки характеризуються активним впровадженням різноманітних інформаційних і телекомунікаційних технологій, що сприяє цифровій трансформації всіх сфер суспільного життя. Це, своєю чергою, стимулює науково-прикладні дослідження у сфері кібербезпеки, розробку новітніх технологій захисту інформації та їх практичне застосування в державному, військовому та приватному секторах.
Значне поширення кіберзагроз, у тому числі кібератак на критичну інформаційну інфраструктуру, інформаційно-психологічних операцій та зростання кількості випадків кіберзлочинності, зумовлюють підвищений попит на висококваліфікованих фахівців у сфері кібербезпеки. Особливо гостро ця потреба постала у зв'язку з військовими діями в Україні, які супроводжуються масштабними кіберопераціями, зокрема атаками на урядові ресурси, фінансову систему, енергетичний сектор та об'єкти критичної інфраструктури.
Розвиток освітньої програми забезпечується завдяки тісній співпраці з роботодавцями, залученню студентів і викладачів до міжнародних проєктів та грантових ініціатив (зокрема, USAID, CRDF Global тощо), а також систематичному вдосконаленню освітнього процесу відповідно до сучасних вимог спеціальності. Це створює необхідні передумови для узгодження змісту програми з актуальними викликами у сфері кібербезпеки та забезпечення конкурентоспроможності її випускників на ринку праці.

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

Враховуючи швидкий розвиток інф.-ком. технологій, а також актуальний галузевий контекст, змістове наповнення ОПП було сформульовано з урахуванням сучасних викликів та потреб ринку праці.
Компетентності випускників програми відповідають актуальним вимогам у сфері захисту інформаційних ресурсів, критичної інфраструктури, корпоративного сектору та суміжних галузей. Додаткову конкурентну перевагу випускникам надають сертифікати Cisco, отримані студентами під час проходження курсів в розрізі окремих дисциплін ОПП.
На базі кафедри кібербезпеки та математичного моделювання, а також університету загалом, укладено низку договорів про співпрацю з державними установами та комерційними компаніями (https://robota-chntu.stu.cn.ua/practice/#). Ці угоди забезпечують студентам можливості проходження практики та подальшого працевлаштування, що дозволяє їм ефективно інтегруватися в професійне середовище та адаптуватися до реальних вимог ринку праці.
На регіональному рівні розвиток освітньої програми узгоджується з пріоритетами та планами розвитку (Стратегічні, операційні цілі та завдання оновленої Стратегії сталого розвитку Чернігівської області на період до 2027 року (https://cg.gov.ua/index.php?id=28101&tp=1). У цьому контексті випускники програми є затребуваними фахівцями для роботи в державних установах і їх структурних підрозділах, на підприємствах промислового сектору та в IT-компаніях міста Чернігова та України.

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

Було проведено аналіз освітньо-професійних програм (ОПП) за спеціальністю 125 «Кібербезпека», що розміщені у відкритому доступі серед закладів вищої освіти (ЗВО) України. До таких програм належать:
Київський національний університет імені Тараса Шевченка - https://fit.knu.ua/wp-content/uploads/2024/03/125_ОНП_маг_Кібербезпека_2023_КБтаЗІ_-1.pdf
Національний університет «Львівська політехніка» - https://lpnu.ua/sites/default/files/2021/program/15950/administruvannya-sistem-kiberbezpeki_0.PDF
https://lpnu.ua/sites/default/files/2021/program/15951/125-mag-biks-2024.PDF
https://lpnu.ua/sites/default/files/2021/program/15320/sistemi-tekhnichnogo-zakhistu-informacii-avtomatizaciya-ii-obrobki_0.PDF
https://lpnu.ua/sites/default/files/2021/program/15321/upravlinnya-informaciynoyu-bezpekoyu_0.PDF
Національний технічний університет України «КПІ імені Ігоря Сікорського» - https://osvita.kpi.ua/125_OPPM_STZI
Харківський національний університет радіоелектроніки - https://nure.ua/wp-content/uploads/Education_programs/2024/2024_mag_125_opp_biks.pdf
https://nure.ua/wp-content/uploads/Education_programs/2024/2024_mag_125_opp_amszi.pdf
https://nure.ua/wp-content/uploads/Education_programs/2024/2024_mag_125_opp_stzia.pdf
Київський університет імені Бориса Грінченка - https://kubg.edu.ua/images/stories/Departaments/vstupnikam/fitm/OPP_125_KBtaZI_mahistry.pdf
Аналіз здійснювався шляхом порівняння цілей, компетентностей і програмних результатів навчання зазначених

ОПП.
Подібні програми також реалізуються у закордонних закладах вищої освіти, зокрема в Техніко-гуманітарній академії у Бельсько-Бяла (Польща) - договір про подвійні дипломи University of Bielsko-Biala Poland: https://ubb.edu.pl/en/full-studies-admission/programmes-in-english , Університет комісії народної освіти (Краків, Польща) - наразі тривають переговори щодо підписання договору про співпрацю та програму подвійних дипломів https://ii.uken.krakow.pl/plany-i-programy-studiow/ та Університет Томаша Баті у Зліні (Чехія): https://www.utb.cz/vyhledavac-oboru/informacni-technologie-mgr/kyberneticka-bezpecnost-mgr/ , Czech University of Life Sciences Prague - наразі тривають переговори щодо підписання договору про співпрацю та програму подвійних дипломів https://www.pef.czu.cz/en/r-9395-departments.
Зміст ОПП враховує сучасні тенденції кібербезпеки та орієнтується на зміст професійних програм сертифікації, таких як:
Cisco Networking Academy (https://www.netacad.com/courses/introduction-to-cybersecurity?courseLang=en-US),
Prometheus (https://courses.prometheus.org.ua/courses/course-v1:Prometheus+CS50+2022_T1/about),
Coursera (спеціалізації з кібербезпеки від Google, IBM та інших),
Udemy https://ua.udemy.com/ .
Аналіз зазначених освітніх програм дозволив виявити їх специфіку, зумовлену як особливостями навчальних закладів, так і регіональними потребами.
Це дозволяє випускникам отримати актуальні знання та компетентності, що відповідають сучасним викликам у сфері кібербезпеки.

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

У 2020 році, на підставі аналізу освітньої програми Техніко-гуманітарної академії у Бельсько-Бяла (Польща), який грунтувався на порівнянні цілей, компетентностей і програмних результатів навчання, було уточнено перелік обов'язкових дисциплін освітньо-професійної програми та скориговано змістове наповнення робочих програм дисциплін.
Аналіз показав, що кожна з них має власну специфіку, яка відповідає профілю спеціальності та враховує регіональний контекст. В результаті проведеного дослідження та з урахуванням актуальних тенденцій розвитку галузі, до нашої ОПП було включено низку освітніх компонентів, зокрема:
ОК Безпекові технології програмування
ВБ . Риторика
ВБ . Управління фінансово-економічною безпекою
ВБ. Методи та системи підтримки прийняття рішень
ВБ. Управління ризиками інформаційної безпеки
ВБ. Тестування на проникнення та етичний хакінг
ВБ. Цифрова криміналістика

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)?

66

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

24

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

Зміст та ОК ОПП являють собою логічно взаємопов'язану систему та відповідають предметній області спеціальності 125 – Кібербезпека та захист інформації згідно зі Стандартом вищої освіти. Цілі ОПП відповідають Стандарту; програма має прикладне спрямування і орієнтована на підготовку фахівців, здатних не лише реагувати на сучасні кіберзагрози, активно впроваджувати інноваційні рішення у сфері інформаційної безпеки, здійснювати аналіз мереж та систем та ефективно застосовувати засоби протидії кібератакам, а і розв'язувати задачі дослідницького та/або інноваційного характеру у сфері інформаційної та/або кібербезпеки, зокрема, відповідно до проф. стандарту «Адміністратор мереж та систем».
Об'єктами проф. діяльності в ОПП, згідно зі Стандартом, є: сучасні процеси дослідження, аналізу, створення та забезпечення функціонування інформ. систем і технологій, інших бізнес-операційних процесів на об'єктах інформ. діяльності; інформ. системи та технології; системи та комплекси створення, обробки, передачі, зберігання, знищення, захисту та відображення даних (інформ. потоків); тощо. Такі об'єкти вивчаються в межах ОК професійної

підготовки ОП.
Кожний ОК ОП враховує складові теоретичного змісту предметної області, а саме: теоретичні засади наукоємних технологій, фізичні і математичні знання, теорії ідентифікації та прийняття рішень, системного аналізу, складних систем; моделювання та оптимізації процесів, теорія математичної статистики; криптографічного та технічного захисту інформації тощо.
При формуванні ОПП враховані надані в описі предметної області Стандарту методи, методики та технології створення, обробки, передачі, приймання, знищення, відображення, захисту інформ. ресурсів у кіберпросторі, а також методи та моделі розробки та використання прикладного і спеціалізованого програмного забезпечення для вирішення професійних задач в галузі інформ. безпеки та/або кібербезпеки.
Інструменти та обладнання предметної області включають засоби, пристрої, мережне устаткування та середовище, прикладне та спеціалізоване ПЗ; автоматизовані системи та комплекси проектування, моделювання, експлуатації, контролю, моніторингу, обробки, відображення та захисту даних (інформ. потоків).
ОПП містить також практичну складову, спрямовану на закріплення набутих навичок використання інструментів та обладнання предметної області.

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

Формування індивідуальної освітньої траєкторії забезпечується наявністю вибіркових дисциплін загальним обсягом 24 кредити, що становить майже 27 %. Порядок вибору здобувачами вищої освіти вибіркових дисциплін врегульовується Положенням про індивідуальну освітню траєкторію здобувачів вищої освіти Національного університету «Чернігівська політехніка» https://stu.cn.ua/wp-content/stu-media/normobaza/normdoc/norm-osvitproces/polozhennya-pro-indyvidualnu-osvitnyu-trayektoriyu.pdf . Здобувачі вищої освіти можуть реалізувати своє право на індивідуальну траєкторію через свої електронні кабінети, при цьому попередньо ознайомитися із вибірковими дисциплінами вони можуть у відповідному розділі вибіркових дисциплін в «MOODLE». Обрані здобувачами ВК заносяться до їх індивідуальних навчальних планів.
Крім цього формування індивідуальної освітньої траєкторії відбувається і через вибір здобувачами тем індивідуальних робіт, тем для написання тез і кваліфікаційної роботи, а також баз практики. До того ж здобувачі вищої освіти мають права на вільне відвідування згідно Порядку надання дозволу на вільне відвідування занять здобувачам вищої освіти
Національного університету «Чернігівська політехніка» https://stu.cn.ua/normatyvna-baza/normatyvne-zabezpechennya-osvitnogo-proczesu/ .

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

Порядок реалізації індивідуальної освітньої траєкторії здобувачами вищої освіти університету здійснюється відповідно до Положення про індивідуальну освітню траєкторію здобувачів вищої освіти НУ «Чернігівська політехніка» https://stu.cn.ua/wp-content/stu-media/normobaza/normdoc/norm-osvitproces/polozhennya-pro-indyvidualnu-osvitnyu-trayektoriyu.pdf. За ОПП здобувачі вищої освіти можуть обрати 24 кредити ECTS. Оскільки вивчення вибіркових дисциплін на ОПП розпочинається в другому семестрі, то процес формування індивідуальної освітньої траєкторії здійснюється після зарахування до Університету до початку нового навчального року.
При цьому, консультаційну роботу з ознайомлення здобувачів вищої освіти із Положенням щодо формування індивідуальної освітньої траєкторії та процедурою вибору, а також переліком вибіркових дисциплін проводить приймальна комісія разом з директорами (деканами) та завідувачами відповідних кафедр до початку нового навчального року. У виключних випадках (у разі відсутності технічної можливості ознайомлення з переліком та обрання вибіркових дисциплін за допомогою особистого електронного кабінету) здобувач може звернутись на кафедру щодо ознайомлення з переліком та змістом можливих вибіркових дисциплін, а також подати письмову заяву до дирекції/деканату щодо врахування переліку обраних ним вибіркових дисциплін на наступний навчальний рік під час складання його індивідуального навчального плану. За результатами обрання здобувачами вищої освіти вибіркових дисциплін директор навчально-наукового інституту (декан факультету, директор центру) розпорядженням по інституту (факультету, центру) до 1 грудня поточного навчального року формує списки здобувачів вищої освіти академічних груп за обраними дисциплінами за погодженням із завідувачами кафедри або гарантами освітніх програм. Інформація про вибіркові дисципліни заноситься до індивідуального навчального плану здобувача вищої освіти.

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

ОПП та навчальним планом у третьому семестрі передбачено практичну підготовку здобувачів вищої освіти обсягом 16 кредитів. Під час проходження практики здобувачі набувають та закріплюють отримані загальні та спеціальні компетентності.
Практики завершуються захистом на випусковій кафедрі у відповідності до затвердженого порядку. На основі багаторічного досвіду проведення практик визначене
колом підприємств, які здатні організовувати цей вид підготовки фахівців на належному рівні (https://robota-chntu.stu.cn.ua/practice/#). Виходячи з потреб роботодавців і моніторингу ринку праці та розвитку спеціальності, формулюються цілі й завдання практичної діяльності студентів, визначається її зміст, який переглядається щорічно при оновленні робочих програм.
Для сприяння організації практичної підготовки в НУ функціонує Центр розвитку кар'єри https://robota-chntu.stu.cn.ua/ , де зокрема розміщені договори із базами практик.
Основними базами практики є: Відділ протидії кіберзлочинам в Чернігівській області Департаменту кіберполіції НП України, ПАТ "Чернігівобленерго", ТОВ "Інформаційна безпека", ТОВ "Інформаційні системи захисту", Chernihiv

ІТ.

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

ОП забезпечує набуття здобувачем важливих навичок soft skills, необхідних для успішної роботи і кар'єрного зростання, які формують засади комунікативності, роботи в команді, вміння публічно викладати свою думку, особисті лідерські якості, гнучкість і адаптивність відповідно до ситуації.
Мовні навички забезпечуються при вивченні іноземної мови за професійним спрямуванням; креативне мислення – набуває розвитку на семінарах з ОК. Також частина фахових дисципліни передбачають групову форму виконання лабораторних робіт (Методологія та організація наукових досліджень, Методи побудови та аналізу криптосистем та ін.), що також сприяє формуванню soft skills.
Важливе місце у набутті студентами вміння вільно спілкуватись, доносити свою думку колегам чи клієнтам зрозуміло і ввічливо, використовуючи проф. термінологію, займають
консультації, що регулярно проводяться викладачами.
Здобувачі освіти беруть активну участь у діяльності органів студентського самоврядування, де в тому числі розвиваються їх soft skills.
Крім того, під час наукових заходів (зокрема конференцій), у яких студенти беруть участь, вони навчаються аналізувати (явища, ситуації та проблеми), здійснювати інноваційну діяльність, вести міжособистісне спілкування та ін.

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 має чітку структуру, ОК утворюють логічну взаємопов'язану систему, що відображено в структурно-логічній схемі. Це допомагає здобувачеві освіти осягнути зміст і взаємозв'язок ОК та сформувати індивідуальну освітню траєкторію на основі запропонованих вибіркових дисциплін.
Успішне виконання здобувачем освіти передбачених ОП ОК забезпечує досягнення заявленої мети та програмних результатів навчання та слугують передумовою успішного проходження професійної сертифікації.

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

В НУ "Чернігівська політехніка" правовою основою для співвіднесення годин в межах освітніх компонентів є ЗУ «Про вищу освіту», Положення про організацію освітнього процесу в НУ «Чернігівська політехніка», Методичні рекомендації щодо розробки, структури та змісту навчальних планів підготовки здобувачів вищої освіти https://stu.cn.ua/wp-content/stu-media/normobaza/normdoc/norm-osvitproces/metod-rekom-rozr-struktury-ta-zmistu-np-zvo.pdf , положення яких враховані при розробці та реалізації ОП. Зокрема, обсяг одного кредиту ECTS становить 30 академічних годин. Навантаження одного навчального року за денною формою здобуття вищої освіти – 60 кредитів ECTS, обсяг обов'язкових компонентів навчального плану за освітніми програмами не може перевищувати 75% загальної кількості кредитів ECTS, за даною ОП – 73% (66 кредитів), обсяг навчальних дисциплін за вільним вибором здобувача вищої освіти має становити не менш як 25 % обсягу загальної кількості кредитів ECTS, за даною ОП – 27% (24 кредити).
Обсяг годин аудиторного навантаження за видами складає 1/3, а обсяг годин самостійної роботи – 2/3 від загальної кількості годин теоретичного навчання з кожної дисципліни (допускається встановлення обсягу годин пропорційно кількості тижнів теоретичного навчання). За результатом опитування, було встановлено, що студенти в цілому задоволені таким співвідношенням.

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

Відповідно до Стандарту освіти, 16 кредитів ОПП відведено на проходження здобувачами практики (ОК 10), яка може проводитись на підприємствах та на базі держустанов сфери кібербезпеки. Також практична підготовка в рамках ОПП передбачає виконання завдань на практичних та лабораторних заняттях, які мають конкретизований практико орієнтований характер. Зокрема, в дисципліні ОКО6 "Проектування технічних систем захисту інформації" студенти виконують курсовий проект, де зокрема, в ході виконання якого проектують системи захисту інформації від її витоку технічними каналами, системи відеоспостереження, контролю та управління доступом, протипожежні та охоронні системи та ін. з метою захисту інформації з обмеженим доступом на підприємствах, в установах та організаціях.
З метою провадження освітнього процесу за дуальною формою відповідно до Розпорядження Кабінету Міністрів України від 19.09.2018 № 660-р «Про схвалення Концепції підготовки фахівців за дуальною формою здобуття освіти» в НУ "Чернігівська політехніка" прийнято «Положення про дуальну форму здобуття вищої освіти» (https://stu.cn.ua/wp-content/stu-media/normobaza/normdoc/norm-osvitproces/p-pro-dualnu-formu-zdobuttya-vo.pdf).
Підготовка здобувачів за дуальною формою освіти в рамках ОПП «Кібербезпека» не здійснюється, проте запроваджуються заходи щодо подолання розриву між теорією і практикою, освітою й виробництвом, підвищення

якості підготовки з урахуванням вимог роботодавців.

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

Досягнення цілей сталого розвитку задекларовано у Стратегії розвитку Національного Університету «Чернігівська політехніка» на 2021-2027 роки (https://stu.cn.ua/wp-content/uploads/2021/03/strategia-roz.pdf), зокрема, у розділі ІІ - Завдання Університету.
Університет дотримується загальнолюдських та державних цінностей і пропагує це через Стратегію сталого та стійкого розвитку. Цілями сталого розвитку ОП, які спрямовані на набуття ЗО навичок і компетентностей, що сприяють досягненню глобальних цілей сталого розвитку до 2030 року, зокрема, є:
- Якісна освіта. ОПП забезпечує доступ до інноваційної освіти у сфері кібербезпеки та захисту інформації, використовуючи сучасні методи навчання, залучає стейкголдерів тощо.
- Гідна праця та економічне зростання. ОПП спрямована на підготовку висококваліфікованих фахівців для ринку праці, що відповідають потребам цифрової економіки.
- Інновації та інфраструктура. ОПП спрямована на підготовку фахівців, здатних розробляти та впроваджувати інноваційні рішення для забезпечення кібербезпеки.
- Сталий розвиток міст та громад. Навички захисту інформації, здобуті ЗО, сприяють зміцненню кібербезпеки на рівні державних та приватних установ, що є важливим елементом забезпечення стійких інституцій. ОПП інтегрує ці глобальні цілі через освітні компоненти та практичну діяльність здобувачів.

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

Правила прийому до Національного університету «Чернігівська політехніка» на навчання для здобуття вищої освіти в 2025 році (https://stu.cn.ua/wp-content/uploads/2025/07/pravyla-pryjomu-2025-7.pdf).

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

Відповідно до Правил прийому до НУ «Чернігівська політехніка в 2025 році» для здобуття вищої освіти за ОС магістр на ОПП «Кібербезпека» приймаються особи, які здобули ступінь бакалавра, магістра та освітньо-кваліфікаційного рівня спеціаліста, здобутого за іншою спеціальністю (напрямом підготовки), за умови успішного проходження вступних випробувань.
Згідно Положення VII. Конкурсний відбір, його організація та проведення п.4 для вступу на спеціальність галузі знань F «Інформаційні технології» та ін»: ЄВІ 2023, або 2024, або 2025 років та єдиного державного кваліфікаційного іспиту (ЄДКІ) зі спеціальності 125 «Кібербезпека та захист інформації» 2024 або 2025 року (тільки для вступників на спеціальність F5 «Кібербезпека та захист інформації», які складали відповідний ЄДКІ 2024 або 2025 року); ЄВІ 2023, або 2024, або 2025 років та ЄФВВ 2025 року (крім вступників на спеціальність F5 «Кібербезпека та захист інформації», які складали відповідний ЄДКІ 2024 або 2025 року); вступного іспиту для іноземців з дисциплін, визначених Правилами прийому (за потреби).
У передбачених Порядком прийому випадках замість результатів ЄВІ (обох блоків) використовуються результати співбесіди з іноземної мови, замість результатів ЄФВВ – результат фахового іспиту.

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 результатів навчання, отриманих в інших ЗВО, регулює Порядок визначення академічної різниці та визнання результатів попереднього навчання http://surl.li/qlbnqe Перезарахування дисциплін проводиться по заяві на підставі порівняння навчального плану та документів, виданих здобувачу вищої освіти за попереднім місцем навчання. Рішення щодо перезарахування може бути прийнято за умов якщо: назви дисциплін ідентичні або мають незначну відмінність, але обсяги, зміст навчальних програм та результати навчання не відрізняються; кількість кредитів відрізняється менше, ніж на 25%.
Відповідно до Положення про організацію освітнього процесу в Національному університеті «Чернігівська політехніка» http://surl.li/djteja при переведенні та поновленні здобувача академічна різниця не повинна складати більше 20 кредитів ECTS. Визнання результатів навчання здобувача вищої освіти, який брав участь у програмі академічної мобільності http://surl.li/tuunbg та зарахування йому здобутих
кредитів ECTS у закладі-партнері, здійснюється відповідно до договору про навчання та індивідуального навчального плану учасника академічної мобільності. Рішення про визнання приймається директором ННІ (деканом факультету) або науково-педагогічним працівником (завідувачем кафедри) за дорученням директора ННІ (декана факультету) на підставі академічної довідки або іншого документу, виданого учаснику академічної мобільності закладом партнером. Всі зазначені документи розміщені на сайті НУ та є доступними для всіх 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)

За період реалізації ОП практики застосування вказаних правил ще не було.
Проте проводиться робота щодо підготовки і реалізації зазначених можливостей: між НУ та ЗВО України активно розвивається співпраця у напрямку внутрішньої академічної мобільності, укладаються відповідні договори та обговорюються можливі напрямки співпраці.

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?

Питання визнання результатів навчання, отриманих у неформальній освіті, регулює п.8.4. Положення про організацію освітнього процесу https://stu.cn.ua/wp-content/stu-media/normobaza/normdoc/norm-osvitproces/polozhennya-pro-organizacziyu-osvitnogo-proczesu.pdf та ПОРЯДОК визначення академічної різниці та визнання результатів попереднього навчання https://stu.cn.ua/wp-content/stu-media/normobaza/normdoc/norm-osvitproces/poryadok-vyznachennya-akademichnoi-riznyczi-ta-vyznannya-rezultativ-poperednogo-navchannya.pdf .
Відповідно до п. 3.4 та 3.5 Порядку визнання результатів навчання у неформальній та/або інформальній освіті дозволяється для всіх дисциплін та розповсюджується на обов'язкові, вибіркові дисципліни ОПП, а також на окремі змістові модулі (теми) навчальних дисциплін.
У п. 3.6 зазначено, що загальний обсяг освітніх компонентів освітньої програми, що зараховуються здобувачу вищої освіти за підсумками визнання результатів неформального навчання, не може перевищувати 25 відсотків відповідної освітньої програми.
У разі негативного висновку предметної комісії щодо визнання результатів навчання здобувач має право звернутися з апеляцією до ректора Університету у порядку визначеному «Положення про організацію освітнього процесу в Національному університеті «Чернігівська політехніка» https://stu.cn.ua/wp-content/stu-media/normobaza/normdoc/norm-osvitproces/polozhennya-pro-organizacziyu-osvitnogo-proczesu.pdf

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

Випадків зарахування результатів навчання як окремих курсів, отриманих у неформальній освіті, за ОПП «Кібербезпека» не було.

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 ОПП відповідає вимогам законодавства: ЗУ «Про освіту » https://zakon.rada.gov.ua/laws/show/2145-19#Text, ЗУ «Про вищу освіту» https://zakon.rada.gov.ua/laws/show/1556-18#Text, Про забезпечення функціонування української мови як державної https://zakon.rada.gov.ua/laws/show/2704-19#Text, Ліцензійним умовам провадження освітньої діяльностіhttps://zakon.rada.gov.ua/laws/show/1187-2015-%D0%BF#Text та ін.
Під час викладання на ОПП використовуються різноманітні форми та методи навчання, передбачені ЗУ «Про вищу освіту» від 1 липня 2014 року № 1556-VII, а також Положенням про організацію освітнього процесу в Національному університеті «Чернігівська політехніка» від 31 серпня 2020 року https://stu.cn.ua/wp-content/stu-media/normobaza/normdoc/norm-osvitproces/polozhennya-pro-organizacziyu-osvitnogo-proczesu.pdf. Форми та методи навчання з усіх дисциплін ОПП прописані у робочих програмах та силабусах навчальних дисциплін, які систематично оновлюються. Силабуси освітніх компонентів розміщені на дистаційнійній платформі MOODLE у відповідному навчальному курсі http://surl.li/frsnio.
Поєднання різних форм та методів сприяють досягненню всіх програмних результатів навчання за ОПП. НПП, які забезпечують викладання навчальних дисциплін в межах ОПП, постійно удосконалюють свою викладацьку майстерність, про що свідчать відповідні сертифікати проходження курсів та тренінгів.

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?

Студентоцентрований підхід в навчанні та викладанні реалізується за допомогою застосування різних методів і форм відповідно до освітнього компоненту. Лекційний матеріал здобувач вищої освіти може опанувати безпосередньо на занятті, а при неможливості бути присутнім - на дистанційній платформі Moodle, де розміщується навчально-методичне забезпечення відповідного компоненту. Для більш повного опанування матеріалу в ході практичних/лабораторних занять приділяється увага індивідуальній роботі здобувачів вищої освіти, використовується наочний матеріал і лекції-презентації. Здобувачі взаємодіють з викладачами і мають можливість задавати питання, консультуватись, запропонувати кращі способи вирішення завдання, обрати найбільш актуальну для себе тему для дослідження. Система оцінювання, вимоги, види робіт (основні та альтернативні) тощо

зазначаються у робочій програмі та силабусі, що дозволяє здобувачам використовувати різні форми демонстрації своїх знань.
Підтвердженням цього є результати опитування студентів щодо задоволеності та якості викладання дисциплін, які проводяться з метою аналізу якості навчання. Слід відмітити, що за результатами опитувань загальний рівень задоволеності є досить високим, про що свідчать результати опитувань здобувачів .

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

Національний університет «Чернігівська політехніка» підписав меморандум про приєднання до Magna Charta Universitatum 20 вересня 2013 року у м. Болонья (Італія), підтвердивши свою належність до академічної співдружності, яка надає усім громадянам необхідні права і свободи у сфері культури, науки та освіти (http://surl.li/inxak). У відповідності до Положення про організацію освітнього процесу в Національному університеті «Чернігівська політехніка» освітній процес в Університеті базується на принципах, одним із яких є академічна свобода учасників освітнього процесу https://stu.cn.ua/wp-content/stu-media/normobaza/normdoc/norm-osvitproces/polozhennya-pro-organizacziyu-osvitnogo-proczesu.pdf). Методи навчання і викладання на ОПП повною мірою дозволяють реалізуватися принципам академічної свободи, оскільки передбачається їх максимальна варіативність, урахування свободи слова й творчості.
Принципів академічної свободи на ОПП «Кібербезпека» дотримуються всі учасники освітнього процесу. Зокрема, викладачі можуть обирати форми та методи навчання з відповідних дисциплін, які найкраще сприятимуть досягненню програмних результатів навчання. Здобувачі вищої освіти мають можливість обирати теми курсових та випускних кваліфікаційних робіт, напрям і тематику наукових досліджень. Викладачі та ЗВО мають можливість удосконалювати кваліфікацію, ознайомлюватися з досягненнями в науковій діяльності через участь у конференціях, семінарах, круглих столах та тематичних виставках.

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

Інформація про цілі, зміст, очікувані результати, порядок та критерії оцінювання є обов'язковою складовою силабусів та робочих навчальних програм дисциплін, затверджених в Національному університеті «Чернігівська політехніка», які в електронному вигляді розміщуються в системі дистанційного навчання (https://eln.stu.cn.ua/login/index.php) та на сайті кафедри https://mmi.stu.cn.ua. Ці матеріали доступні для ЗВО, ознайомитись з ними можливо в будь-який зручний для себе час. Зокрема,такий доступ до інформації спрощує вибір освітніх компонент.
Під час вивчення дисципліни корисною є інформація про оцінювання окремих її складових, яка надається ЗВО в системі дистанційного навчання. Інформація щодо цілей, змісту та очікуваних результатів навчання, порядку та критеріїв оцінювання у межах окремих освітніх компонентів доводиться до здобувачів освіти викладачами по кожній окремій дисципліні і куратором за програмою в цілому. У випадку, коли ЗВО був відсутній та не отримав інформацію з вищенаведених питань, викладач може ознайомити ЗВО в індивідуальному порядку під час консультацій.
Ще одним способом інформування є комунікація між викладачами та ЗВО через месенджери. У разі виникнення питань зі сторони ЗВО щодо цілей, змісту та очікуваних результатів навчання, порядку та критеріїв оцінювання, викладач може оперативно надати консультацію.

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

В рамках ОПП «Кібербезпека» передбачені різні форми та методи участі магістрів у дослідницькій діяльності. Серед них виконання завдань з науково-дослідною складовою у процесі вивчення фахових дисциплін (курсовий проект з Проектування технічних систем захисту інформації, практичні заняття з ОК «Методологія та організація наукових досліджень» та ін.), а також доповіді за результатами досліджень в рамках тематики дипломного проектування і на наукових конференціях різного рівня, наприклад, на щорічній Міжнародній науково-практичній конференції студентів, аспірантів та молодих учених «Юність науки-2025» .
Під час виконання зазначених завдань здобувачі опановують вміння та навички аналізувати, верифікувати, оцінювати повноту інформації в ході професійної діяльності, при необхідності доповнювати й синтезувати відсутню інформацію та працювати в умовах невизначеності тощо.
Викладачі, які забезпечують освітній процес за ОПП, не обмежуються ознайомленням здобувачів із новітніми технологіями та науково-технічною інформацією в рамках викладу матеріалу навчальних предметів на заняттях, а й залучають студентів до досліджень за науковою тематикою випускової кафедри 0124U004485 "Методологія побудови захищеного кіберпростору", а також держбюджетною темою загального конкурсу проектів фундаментальних наукових досліджень, прикладних наукових досліджень, що виконується на кафедрі.
Здобувачі ОПП успішно беруть участь в олімпіадах, зокрема Міжнародній студентській олімпіаді "ШЛЯХИ ТА МЕХАНІЗМИ ЗАХИСТУ ІНФОРМАЦІЙНОГО ПРОСТОРУ УКРАЇНИ ВІД ШКІДЛИВИХ ІНФОРМАЦІЙНО-ПСИХОЛОГІЧНИХ ВПЛИВІВ". Так, Бакуменко Богдан ставав неодноразовим переможцем цієї олімпіади різних років.
При кафедрі кібербезпеки та математичного моделювання під керівництвом Семендяя С.М. функціонує науковий гурток CyberLab, який сприяє розвитку розвиток науково-дослідної, проектної та виробничої діяльності здобувачів.

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

В НУ «Чернігівська політехніка» впроваджено систему оновлення змісту освітніх компонентів всіх освітніх програм. У відповідності до її норм, обов'язковим є перегляд навчально-методичних матеріалів дисциплін (наприклад, робочі програми дисципліни та силабуси) щорічно.
НПП постійно отримують нові знання, приймаючи участь у міжнародних та всеукраїнських конференціях, вебінарах, тренінгах та проектах, завдяки яким оновлюють навчально-методичне забезпечення дисциплін.
РП навчальних дисциплін ОПП «Кібербезпека» та інше навчально-методичне забезпечення, в якому відображено зміст ОК, затверджуються випусковою кафедрою перед початком нового навчального року. На випусковій кафедрі проводяться зустрічі у форматі MeetUp, регулярно відбуваються обговорення результатів стажування та підвищення кваліфікації професорсько-викладацького складу, аналіз результатів роботи Екзаменаційної комісії по захисту кваліфікаційних робіт/проектів. На основі пропозицій, висловлених під час цих заходів, викладачі, які забезпечують освітні компоненти ОП, формують нові елементи робочих навчальних програм дисциплін та коригують програми практик.
Зокрема, доцентом Ларченко М.О. в результаті обговорення кафедрою результатів підвищення її кваліфікації в межах «Зимової ІТ-школи «Data Engineering and Security 2025» було повністю сформовано новий модуль робочої програми ОК5 "Стандартизація, сертифікація засобів та комплексів захисту інформації": Лекція 6. Системи управління інформаційною безпекою (СУІБ), де обговорюється: 1) концепція та впровадження систем управління; 2) сертифікація СУІБ за стандартами ISO/IEC 27001, а також оновлена відповідна їй лабораторна робота 5 з теми "Розробка комплексної моделі захисту на основі стандартів сертифікації".

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

Інтер-ція д-ті ун-ту передбачає активізацію учасників освітнього процесу в програмах академічної мобільності, міжнародних проєктах, конкурсах, співпраці з іноземними ВНЗ та ін.
В Ун-ті фун-нує Програма підвищення рівня володіння англійською мовою НПП (https://stu.cn.ua/wp-content/stu-media/normobaza/normdoc/norm-osvitproces/programa-pidvyshhennya-rivnya-volodinnya-anglijskoyu-movoyu-npp.pdf). Створений Центр іноземних мов http://surl.li/slawmf , який дає можливість опанувати англ., нім. та франц. мови. Вищеперераховані заходи створюють умови для підвищення академічної мобільності НПП та ЗВО, як одного із пріоритетних напрямків досягнення завдань інтернаціоналізації.
ОПП передбачає ознайомлення здобувачів зі світовими науковими здобутками у сфері інформаційної безпеки. У локальній мережі НУ є доступ до баз даних Web of Science, Scopus та ін.
Викладачі, залучені до реалізації ОПП, проходять міжнародне стажування та беруть участь у програмах академічної мобільності (проф. Ткач Ю.М. (Латвія, програма мобільності Erasmus+ International Week 2023 «Future University, Connecting Regions», де прочитала вікриту лекцію англійської мовою "Personal Safety in Cyberspace")).
Завдяки програмі Європейського Союзу у сфері освіти, професійної підготовки, молоді та спорту Erasmus+ у лютому 2023 року студентки Лук'янець М., Мацнева М. мали можливість пройти двотижневе навчання в університеті на Кіпрі University of Cyprus на інноваційній магістерській програмі «Інтелектуальні системи критичної інфраструктури» .

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?

Для оцінювання здобувачів вищої освіти за ОК ОП використовуються різні контрольні заходи у межах та на підставі нормативних актів НУ: 1) Положення про організацію освітнього процесу в Національному університеті «Чернігівська політехніка» http://surl.li/tgcibq ;
2) Положення про внутрішню систему забезпечення якості вищої освіти в Національному університеті «Чернігівська політехніка» http://surl.li/tpzgon ;
3) Положення про поточне та підсумкове оцінювання знань здобувачів вищої освіти НУ http://surl.li/lpjwkg .
Система оцінювання знань здобувачів вищої освіти у межах ОП включає поточний, проміжний (модульний), а також семестровий контроль. Поточний контроль здійснюється протягом семестру під час проведення лекційних, лабораторних/практичних занять, виконання індивідуальних завдань і оцінюється сумою набраних балів. Для ефективного та всебічного оцінювання на ОП передбачені різноманітні за змістом і формою контрольні заходи, які дозволяють об'єктивно перевірити досягнення програмних результатів навчання здобувачів ВО.
Усне опитування, підбір матеріалів з відповідної тематики та сучасних практик, вирішення задач (практичних ситуацій) є базовими контрольними заходами, які дозволяють з'ясувати рівень засвоєння та можливість використання набутих знань здобувачами ВО.
Контрольні питання (питання для самоперевірки) дають змогу ЗВО провести самооцінку якості засвоєння навчального матеріалу з конкретної теми навчальної дисципліни. Аналітичний огляд наукових статей, тез, наукова робота дозволяють перевірити вміння ЗВО самостійно проводити збір, аналіз та узагальнення матеріалів, здійснювати презентацію свого дослідження тощо.
Письмова контрольна робота/ тестування проводиться наприкінці семестру за результатом вивчення більшості змістових модулів.Проміжний контроль має на меті оцінку результатів знань здобувачів вищої освіти після вивчення матеріалу з логічно завершеної частини дисципліни. Цей вид контролю може бути проведений у формі контрольної роботи (тестів) і оцінюється відповідною сумою балів.
Під час семестрового контролю оцінювання успішності ЗВО здійснюється у формі екзамену або диференційованого заліку з урахуванням результатів поточного та проміжного (модульного) контролю за національною

(чотирибальною) шкалою («відмінно», «добре», «задовільно», «незадовільно» та шкалою ECTS.
Визначені та описані форми контрольних заходів відображаються у силабусах та робочих програмах кожної навчальної дисципліни, методичних вказівках до практичних (лабораторних) занять з обов'язковим розміщенням на сторінці відповідного навчального курсу у системі дистанційного навчання Moodle.

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

Чіткість і зрозумілість контрольних заходів та критеріїв оцінювання забезпечується доступністю загальноуніверситетських нормативних документів, які врегульовують порядок і критерії оцінювання навчальних досягнень здобувачів вищої освіти для всіх учасників навчального процесу через розміщення їх на сайті НУ «Чернігівська політехніка»: розділ «Нормативне забезпечення освітнього процесу» http://surl.li/ftikik , а також силабусів та РП навчальних дисциплін, методичних вказівок через розміщення їх у системі дистанційного навчання Moodle http://surl.li/pfmfmj . Чіткість і зрозумілість контрольних заходів забезпечується також засобами безпосереднього спілкування, зокрема викладачами навчальних дисциплін та куратором групи. Під час першого заняття викладач інформує здобувачів вищої освіти про графік і форми контролю, методи та критерії оцінювання згідно з силабусом та РП навчальної дисципліни. Питання для підсумкового контролю (залікові та екзаменаційні питання) також заздалегідь розміщуються у системі Moodle на сторінці відповідної навчальної дисципліни. Результати опитування здобувачів вищої освіти показали, що контрольні заходи та критерії оцінювання для здобувачів вищої освіти є зрозумілими і чіткими https://mmi.stu.cn.ua/novyny/rezultaty-opytuvannya-zdobuvachiv-vyshhoyi-osvity-spetsialnosti-125-kiberbezpeka-u-2025-rotsi/.

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

Система оцінювання рівня знань ЗВО на ОП формується та діє у відповідності до норм. док. НУ, згадуваних вище. Інформація про форми контрольних заходів та критерії оцінювання відображається у силабусі дисципліни та РП, які розміщується в системі Moodle, чим забезпечується вільний постійний доступ ЗВО до зазначеної інформації. Критерії оцінювання є обов'язковою складовою силабусу та РП. На початку семестру НПП, який викладає дисципліну, знайомить зі змістом, структурою дисципліни, а також із системою критеріїв оцінювання. Терміни та час проведення різних видів навчальної роботи регламентуються розкладами занять, заліково-екзаменаційних сесій, роботи екзаменаційних комісій, графіками консультацій. У розкладах навчальних занять і заліково-екзаменаційних сесій обов'язково вказується назва дисципліни, час, місце проведення (аудиторія), форма проведення (лекція чи лабораторне/практичне заняття), прізвище та ініціали НПП, його посада. Розклади занять оприлюднюються та доводяться до відома НПП і здобувачів вищої освіти не пізніше як за три дні до початку семестру. Розклади заліків, екзаменів оприлюднюється не пізніше як за місяць до початку заліково-екзаменаційної сесії http://surl.li/obgccq. Графіки консультацій НПП складаються на кафедрах і затверджуються. Відповідно до опитування гарантом здобувачів вищої освіти з'ясувалося, що процедури проведення контрольних заходів та оскарження оцінювання знань (подачі апеляції) здобувачам є зрозумілими.

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

Форми атестації здобувачів вищої освіти відповідають вимогам стандарту вищої освіти України другого (магістерського) рівня вищої освіти спеціальності 125 – Кібербезпека атестація випускників.
За ОПП «Кібербезпека» атестація проводиться у формі захисту випускної кваліфікаційної роботи та завершується видачею документу встановленого зразка про присудження здобувачу ступеня магістра із присвоєнням кваліфікації: магістр з кібербезпеки та захисту інформації.
Атестація здійснюється відкрито і публічно. Кваліфікаційна робота не повинна містити академічного плагіату, фабрикації, фальсифікації.
Кваліфікаційна робота розміщується у репозитарії Університету.

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

Процедура проведення контрольних заходів регулюється Положенням про поточне та підсумкове оцінювання знань здобувачів вищої освіти Національного університету «Чернігівська політехніка», затвердженим вченою радою Університету 31 серпня 2020 р. протокол № 6 і введеним в дію наказом ректора від 31 серпня 2020 р. № 26 (https://numl.org/NLV).
Проміжний контроль проводиться в межах вивчення модулів окремих дисциплін, завдання до них розробляються викладачем.
Для проведення іспитів та атестації здобувачів вищої освіти розроблено Положення про порядок створення та організацію роботи екзаменаційних комісій для атестації здобувачів вищої освіти Національного університету «Чернігівська політехніка», затвердженого вченою радою Університету 31 серпня 2020 р. протокол № 6, введеного в дію наказом ректора від 31 серпня 2020 р. № 26 (https://numl.org/NUS).

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

В кожній робочій програмі дисципліни детально розписано критерії оцінювання та мінімальні вимоги до знань здобувачів. У випадку, якщо у здобувача є претензії щодо об'єктивності, то він має право звернутися з апеляцією, процедура якої розписана в розділі 6 та 7 Положення про поточне та підсумкове оцінювання знань здобувачів вищої освіти НУ «Чернігівська політехніка» (https://numl.org/NLV). Апеляція щодо процедури проведення та об'єктивності оцінювання подається особисто здобувачем через загальний відділ Університету на ім'я ректора не пізніше наступного робочого дня після оголошення оцінки. Ректор направляє заяву для розгляду апеляційною комісією відповідного ННІ для вирішення спірних питань, пов'язаних з організацією і проведенням оцінювання здобувача, визнанням результатів навчання. В ННІ розпорядженням директора створюється апеляційна комісія. Головою комісії є директор, який забезпечує належну організацію роботи комісії, своєчасний і об'єктивний розгляд апеляцій ЗВО, ведення справ і збереження документів. Розгляд апеляційних заяв здійснюється комісією в триденний термін від дати надходження заяви. Комісія за результатами розгляду заяви може або задовольнити заяву, або відмовити в задоволенні заяви через недостатність підстав для зміни результату. Результати повторного проведення екзамену (заліку), визнання результатів навчання або атестації не підлягають оскарженню. Конфліктів інтересів між екзаменатором і здобувачем вищої освіти на даній ОПП не було.

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

Процедури порядку повторного проходження контрольних заходів описані в Положенні про організацію освітнього процесу в НУ «Чернігівська політехніка» https://stu.cn.ua/wp-content/stu-media/normobaza/normdoc/norm-osvitproces/polozhennya-pro-organizacziyu-osvitnogo-proczesu.pdf) і в Положенні про поточне та підсумкове оцінювання знань здобувачів вищої освіти (https://numl.org/NLV).
Акад. забор-ть з підсумкового сем. контролю знань ліквідується здобувачами під час додаткових сесій з ліквідації академзаборгованості, її організовує дирекція ННІ згідно з графіком навчального процесу, затвердженим ректором Університету. Повторне складання іспитів (диференційованих заліків) можливе не більше двох разів з кожної дисципліни: один раз викладачу, другий – комісії, яка створюється директором ННІ, до складу якої входять завідувачі кафедр, НПП і представники органів студентського самоврядування. Головою комісії призначається директор інституту. Він забезпечує належну організацію роботи комісії, ведення справ і збереження документів і несе персональну відповідальність за виконання покладених на комісію завдань і здійснення нею своїх функцій. Результати ліквідації академзаборгованості відображаються в ліквідаційній відомості успішності. Здобувач, який одержав незадовільні оцінки з дисциплін, сумарний обсяг яких перевищує 20 кредитів, або отримав незадовільну оцінку з однієї дисципліни після трьох спроб складання екзамену (заліку), підлягає відрахуванню зі складу здобувачів вищої освіти за невиконання індивідуального навчального плану.

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

Порядок оскарження процедури та результатів проведення контрольних заходів регулюється «Положенням про поточне та підсумкове оцінювання знань здобувачів вищої освіти НУ. Для вирішення спірних питань, пов'язаних з організацією та проведенням семестрового контролю, оцінюванням практик та визнання результатів навчання в неформальній та/або інформальній освіті, розпорядженням декана/директора щорічно створюється апеляційна комісія.
Головою апеляційної комісії призначається декан/директор. Апеляція подається особисто здобувачем вищої освіти через загальний відділ Університету на ім'я Ректора не пізніше наступного робочого дня після оголошення оцінки. Ректор направляє заяву для розгляду апеляційною комісією відповідного інституту (факультету), якою вона розглядається у триденний термін від дати надходження апеляційної заяви. У разі задоволення заяви, комісія пропонує скасувати результати контрольного заходу або атестації та призначити його повторне проведення, після чого видається відповідне розпорядження по інституту (для результатів оцінювання знань під час семестрового контролю та оцінювання практик) або відповідний наказ Ректора (для результатів оцінювання атестації).
На ОП, що акредитується, випадків подачі апеляцій здобувачами вищої освіти не було.

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

Питання політики, стандартів і процедури дотримання академічної доброчесності в Університеті регулюються Кодексом академічної доброчесності НУ, Положенням про комісію з питань академічної доброчесності НУ «Чернігівська політехніка», Порядком проведення перевірки кваліфікаційних робіт та індивідуальних завдань здобувачів вищої освіти на плагіат в НУ. Вказані нормативні акти оприлюднені на офіційному сайті Університету в розділі «Академічна доброчесність» http://surl.li/lodmgd. Згідно з Положенням про інформаційний центр запобігання та виявлення плагіату Національного університету «Чернігівська політехніка» http://surl.li/itmjhf в НУ функціонує Центр запобігання та виявлення плагіату (далі – ЦЗВП), який проводить перевірку щодо наявності можливих фактів академічного плагіату з застосуванням програмного забезпечення StrikePlagiarizm.
Наказом Ректора затверджено склад Комісії з питань академічної доброчесності https://stu.cn.ua/wp-content/stu-media/normobaza/normdoc/nakazu/2025/nakaz-07-VC.pdf , яка сприяє дотриманню етичних принципів і стандартів, фундаментальних принципів академічної доброчесності та розв'язанню конфліктів між членами університетської спільноти. Результати опитування здобувачів вищої освіти показали, що вони достатньо ознайомлені із принципами і правилами
академічної доброчесності (протокол № 9 від 30.08.2024 року) http://surl.li/iekxus.

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

Перелік технологічних рішень–інструментів визначається «Кодексом академічної доброчесності (https://numl.org/O5l), а також «Порядком проведення перевірки кваліфікаційних робіт та індивідуальних завдань здобувачів вищої освіти на плагіат (https://numl.org/NUW). Порядок містить типові форми Довідки про відсутність плагіату у КР, Акту перевірки на плагіат КР. Перевірка здійснюється автором та керівником КР на етапах підготовки роботи, а також керівником по закінченню роботи; Центром запобігання та виявлення плагіату НУ (ЦЗВП); комісією з академічної доброчесності НУ в разі подання апеляційної скарги автора на результати попередньої перевірки.
Відповідно до пункту 2.3 Порядку: автор та керівник КР в процесі підготовки КР можуть використовувати будь-які програмно-технічні засоби для визначення відсотку унікальності тексту або плагіату у КР. Рекомендуються до використання програми, які знаходяться у відкритому доступі в мережі Інтернет і програмні засоби ЦЗВП.
Посилання на репозиторій ЗВО, що містить кваліфікаційні роботи здобувачів вищої освіти ОП https://ir.stu.cn.ua/handle/123456789/18291/discover?query=%D0%9A%D1%96%D0%B1%D0%B5%D1%80%D0%B1%D0%B5%D0%B7%D0%BF%D0%B5%D0%BA%D0%B0&filtertype=dateIssued&filter_relational_operator=equals&filter=2024.

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

Академічна доброчесність як позитивна практика популяризується в ЗВО через постійну роз'яснювальну роботу, тренінги щодо інтелектуальної власності та академічної доброчесності, вивчення кращих практик інших ЗВО тощо. На сайті НУ є розділ «Академічна доброчесність» із нормативними та просвітницькими матеріалами про академічну доброчесність, контактами осіб, до яких можна звернутися у разі виникнення питань (https://numl.org/O5n).
Для попередження порушень в освітній та науковій діяльності ЗВО в НУ розроблено наступний комплекс профілактичних заходів: обов'язкове інформування учасників ОП про необхідність дотримання принципів та норм академічної чесності шляхом проведення циклу тренінгів з етики та доброчесності, із захисту прав інтелектуальної власності та трансферу технологій, з проєктноорієнтованої діяльності в науковій та підприємницькій діяльності; розповсюдження методичних пропагандних матеріалів; ознайомлення на зустрічах з гарантом ОП всіх учасників ОП із нормами Положення про академічну доброчесність студентів та науково-педагогічних працівників НУ «Чернігівська політехніка» та про те, що академічна доброчесність – це не лише відсутність плагіату, а і списування, роботи на замовлення, тощо. Крім того, до ОПП «Кібербезпека» входить дисципліна «Методологія та організація наукових досліджень», в якій розглядаються питання дотримання академічної доброчесності під час написання наукових та кваліфікаційних робіт.

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

Відповідно до «Кодексу академічної доброчесності НУ наслідком порушення академічної доброчесності ЗВО може бути: повторне проходження оцінювання (контрольна робота, екзамен, залік тощо); повторне проходження відповідного освітнього компонента освітньої програми; відрахування з НУ; позбавлення академічної стипендії. Якщо внаслідок перевірки на плагіат унікальність роботи менша, ніж передбачений мінімальний показник, здобувач не допускається до захисту твору. Робота повертається на доопрацювання. У разі незгоди з результатами перевірки на плагіат, здобувач вищої освіти має право подати апеляцію, згідно пп 7.1-7.5 Кодексу академічної доброчесності НУ. На ОП постійно ведеться продуктивна робота з підвищення якості академічної доброчесності, зокрема при написанні контрольних робіт студентами, а особливо написанні наукових статей та тез доповідей. На ОП були випадки, коли здобувачі вищої освіти за рекомендацією НПП доопрацьовували тези в частині правильності оформлення посилань та збільшення відсотка унікальності, після чого надсилалися на перевірку і отримували результат, що дозволяв опублікувати тези.

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

Відповідність освітньої та/або проф. кваліф. НПП ОК визначається згідно з законодавством: ЗУ «Про вищу освіту», «Рекоменд. щодо пров. конкурсн. відбору для заміщення вакантних посад НПП та укладання з ними труд. дог. (контрактів)», затверджених наказом МОНУ 05.10.2015, № 1005, Постанови КМУ «Про затвердження Ліцензійних умов провадження освітньої діяльності» від 30.12.2015 № 1187, Проф. Станд. на групу професій «Викладачі закладів вищої освіти», затверджених наказом МОНУ 23.03.2021, № 610. Вимоги вищезазначених НА відображені у Порядку проведення конкурсного відбору при заміщенні вакантних посад НПП у НУ від 31.08.2020 р. https://stu.cn.ua/wp-content/stu-media/normobaza/normdoc/kadrove-zabezpechennya-ta-vakansiyi/poryadok-provedennya-konkursnogo-vidboru-pry-zamishhenni-vakantnyh-posad-npp.pdf . Посади НПП можуть обіймати особи, які мають науковий ступінь та/або вчене звання, ОС магістра або освітньо-кваліфікаційний рівень спеціаліста у галузі знань відповідно до профілю викладання. Необхідними для допуску до роботи на посаді асистента, викладача, старшого викладача є ступінь магістра (спеціаліста) за відповідною спеціальністю; на посаді доцента, професора – науковий ступінь та/або вчене звання за відповідною галуззю знань.

Вимоги щодо стажу НПР до осіб, які претендують на посади НПП: асистент, викладач – не пред'являються; старший викладач – не менше 3-х років; доцент – не менше 3-х років; професор – не менше 6-ти років; завідувач кафедри – не менше 6-ти років. У випадку відсутності відповідного наукового ступеня та/або вченого звання до осіб, які претендують на посаду старшого викладача, може вимагатися стаж роботи у галузі чи виді професійної діяльності, що відповідає профілю викладання, не менше 5 років (п. 6.2 Порядку). До реалізації освітньої програми залучені кваліфіковані НПП, професійний досвід яких дозволяє фахово забезпечити освітні компоненти. Усі НПП освітньої програми мають вищу освіту, окрім цього науковий ступінь доктора технічних наук 05.13.21 системи захисту інформації має Шелест М.Є., д.пед.н., к.т.н. (21.05.01 -інформаційна безпека держави) Ткач Ю.М., к.т.н. (05.13.21 системи захисту інформації) Петренко Т.А., магістерський ступінь з кібербезпеки має Синенко М.А., Ларченко М.О., Мехед Д,Б.

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

Прийняття НПП на роботу відбувається згідно з Порядком https://stu.cn.ua/wp-content/stu-media/normobaza/normdoc/kadrove-zabezpechennya-ta-vakansiyi/poryadok-provedennya-konkursnogo-vidboru-pry-zamishhenni-vakantnyh-posad-npp.pdf .
До додаткових вимог до кандидатів на заміщення вакантних посад НПП НУ (зав. кафедр, проф., доц., старших викл., викл., асистентів) належать: вільне володіння державною мовою, а в окремих випадках знання мови країни, яка входить до ОЕСР; висока цифр. грам.; знання та розуміння предметної області і проф. діяльності; наявність повного пакету навч.-метод. забезп. навч. дисц.; наявність наукових праць (не менше ніж 1 стаття за рік), опубл.у фах.виданнях України категорії Б або В та/або в періодичних виданнях, включених до наукометричних баз Scopus або Web of Science; та ін.
Також передбачено обговорення кандидатур претендентів на заміщення вакант. посад труд. кол. відповідної кафедри в їх присутності на засіданні кафедри. Для оцінки рівня проф. квал. претендента кафедра може запропонувати йому прочитати пробні лекції, провести практичні заняття в присутності НПП НУ. Висновки кафедр про професійні та особистісні якості претендентів затвердж. таємним голос. та разом з витягом з протоколу засідання кафедри передаються на розгляд конкурсної комісії в письмовій формі. У разі незгоди окремих НПП із загальним рішенням щодо заміщення вакантної посади, на розгляд конк. ком. подаються вмотивовані окремі висновки НПП, які викладені в письм. ф. та підписані власноруч.

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

Частина викладачів, задіяних в ОПП, мають значний практичний досвід у сфері кібербезпеки. Зокрема, Шелест М.Є., професор кафедри, заслужений діяч науки і техніки України, лауреат Державної премії України в галузі науки і техніки, повний кавалер ордена «За заслуги», доктор технічних наук, професор, тривалий час (біля 40 років) проходив службу у військовій розвідці, СБУ, Службі зовнішньої розвідки України. Семендяй С.М., ст. викладач, тривалий час проходив військову службу в СБУ та ДССЗЗІ України, обіймав посади пов ′язані із виконанням функцій, що відповідають напрямкам спеціальності «Кібербезпека та захист інформації», а саме: криптографічний, ТЗІ, організаційний захист інформації. Брав участь у створенні телекомунікаційних мереж спеціального призначення, Петернко Т., к.т.н., має досвід роботи інженером-програмістом, Гребенник А.Г. має більше п'яти років досвіду роботи інженером. Ларченко М.А. наразі працює фахівцем відділу оцінки ризиків та методології інформаційної безпеки. Компанія Modus X.
До проведення різних заходів зал-ся фахівці-практики. Виступили Лукінов І., операційний директор, фірма Quantum (квітень 2025), Молодецька К., д.т.н. проф.. Гостьові лекції: Кіберполіція Сучасні кіберзагрози та протидія ним (https://mmi.stu.cn.ua/novyny/zustrich-z-predstavnykamy-kiberpolitsiyi/) та закордонні вчені Andrei Yurchenko (Malaysian Company) "Zero Trust Security Model — the main challenge for future information security and freedom" https://mmi.stu.cn.ua/novyny/gostova-lektsiya-do-mizhnarodnogo-dnya-zahystu-informatsiyi/.

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

Підв. квал. НПП здійсн. на основі Положення про підвищення кваліфікації педагогічних і НПП НУhttps://stu.cn.ua/wp-content/stu-media/normobaza/normdoc/kadrove-zabezpechennya-ta-vakansiyi/polozh-pro-pidvyshhennya-kvalifikacziyi-pedagogichnyh-i-npp.pdf .
Так, за сприяння університету гарант ОПП Ткач Ю.М. пройшла міжнародне стажування (м. Валмієра, Латвія, участь у програмі мобільності Erasmus+ International Week 2023 «Future University, Connecting Regions» у Відземському університеті прикладних наук терміном на 9 днів з 13 травня по 21 травня 2023 року включно).
В НУ проводиться активна робота щодо підвищення професійного розвитку НПП. Так, Відділ міжнародних зв'язків, Центр розвитку кар'єри, Центр проєктної діяльності, Науково-дослідна частина здійснюють розсилки анонсів проведення науково-практичних конференцій, проведення грантових конкурсів, стартапів, стажувань тощо, інформація про які надходить у рішеннях ректорату, а також розміщується на відповідних сторінках сайту НУ. Також в НУ проводяться тренінги для НПП щодо розробки і подання грант. заявок, участі у конкурсах стартапів тощо, які проводяться відповідно до Плану заходів на 2021-2025 р.р. щодо підв. публ. активн. та цитування НПП НУ http://surl.li/jijmyr .

Наведіть конкретні приклади заохочення розвитку викладацької майстерності

З метою стимулювання розвитку і вдосконалення викладацької майстерності науково-педагогічних працівників в НУ «Чернігівська політехніка» передбачено їх рейтингування згідно з «Положенням про щорічне оцінювання науково-педагогічних працівників і кафедр НУ «Чернігівська політехніка» (https://numl.org/O5y). Щорічне рейтингове оцінювання НПП заохочує їх зміцнювати свої позиції за всіма критеріями, створює атмосферу змагання і здорової конкуренції. Нематеріальне заохочення передбачає відзначення викладачів державними нагородами, грамотами та подяками адміністрації Університету, центральних і місцевих органів влади, що позитивно позначається на моральному піднесенні.
Дієвим заохоченням є фінансова підтримка НПП: доплати до посадового окладу, фінансова допомога, преміювання, прописані у відповідних додатках Колективного договору трудового колективу та адміністрації НУ «Чернігівська політехніка» (https://stu.cn.ua/wp-content/stu-media/normobaza/normdoc/kol-dogovir.pdf).
До того ж згідно з Положенням про школу молодого викладача та вдосконалення виклад. майстерн.і створ. умови для вдоск. виклад. майстерн. та надається допомога молодим викладачам в адаптації та набутті педагог. досвіду роботи https://stu.cn.ua/wp-content/stu-media/normobaza/normdoc/kadrove-zabezpechennya-ta-vakansiyi/p-pro-shkolu-molodogo-vykladacha.pdf

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

Навч.-мет. заб-ня з ОП представлене на сайті кафедри mmi.stu.cn.ua та дистанційній платформі Moodle (https://eln.stu.cn.ua/login/index.php?loginredirect=1).
Для підготовки здобувачів за ОПП використовується мат.-тех. база НУ, яка відповідає Ліц. вимогам провадження освітньої діяльності. Для виконання лаб. і практичних робіт створено лабораторію кібербезпеки, яка включає навчальну серверну, та низку спецлабораторій: кабінет технічного захисту інформації (1-105), лабораторія мережевої безпеки (1-110-111), системного адміністрування (1-106).
Освітній процес цифровізований, функціонує система АСУ «ВНЗ», кожен здобувач вищої освіти і НПП мають свої електронні кабінети, що спрощує роботу під час освітнього процесу. Матеріально-технічна база НУ https://stu.cn.ua/wp-content/uploads/2021/04/mtz19-1.pdf аудиторний фонд, спортивний комплекс, гуртожитки https://stu.cn.ua/veb-resursy/gurtozhytky/, їдальня https://stu.cn.ua/veb-resursy/yidalnya/,фонди бібліотеки http://library2.stu.cn.ua/resursi_biblioteki/, система дистанційного навчання https://eln.stu.cn.ua/login/index.php, психологічна служба НУ http://surl.li/xqsomp тощо відповідають Ліцензійним умовам провадження освітньої діяльності і призначена для задоволення потреб та інтересів здобувачів вищої освіти. Інформація про фінансові ресурси НУ розміщена https://stu.cn.ua/normatyvna-baza/finansovo-ekonomichna-diyalnist/.Комфортність освітнього середовища в НУ забезпечується керівництвом спільно з органами студентського самоврядування - Студентською радою.

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

Освітнє середовище, створене в НУ, задовольняє потреби та інтереси здобувачів вищої освіти. Матеріально-технічна база забезпечує реалізацію ОПП. ЗВО мають можливість брати участь у міжнародній академічній мобільності https://stu.cn.ua/mizhnarodna-diyalnist/ , https://stu.cn.ua/nauka-ta-innovatcii/czentr-stvorennya-ta-rozvytku-startapiv/ у розробці стартапів та інноваційних проєктів, у виченні мов https://stu.cn.ua/veb-resursy/czentr-inozemnyh-mov/ . Бібліотека надає широкий спектр послуг, в тому числі і дистанційно http://library2.stu.cn.ua/naukova_diyaljnistj/ , зарубіжні видання з відкритим доступом
http://library2.stu.cn.ua/na_dopomogu_naukovcyu/zarubizhni_vidannya_z_vidkritim_dostupom/ , доступні пошукові системи наукової інформації
http://library2.stu.cn.ua/na_dopomogu_naukovcyu/poshukovi_sistemi_naukovoi_informacii/ та наукометричні бази даних http://library2.stu.cn.ua/na_dopomogu_naukovcyu/naukometrichni_bazi_danih/
Діяльність студентського самоврядування зорієнтована на створення комфортних умов для навчання, дозвілля та реалізації студентами своїх прагнень, потреб та інтересів, задля з'ясування котрих проводяться опитування в межах освітніх компонентів гарантом та централізовано Сектором систем менеджменту забезпечення якості вищої освіти http://surl.li/rmevsa. Рада з якості НУ аналізує результати даних опитувань та вносить пропозиції на Вчену раду НУ з покращення освітнього середовища http://surl.li/nixckw.

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

В НУ безпечність освітнього середовища для життя та здоров'я здобувачів вищої освіти досягається шляхом дотримання норм техніки безпеки, санітарних та гігієнічних норм, постійним інструктажем НПП та здобувачів ВО щодо дій у надзвичайних ситуаціях, цивільного захисту та безпеки життєдіяльності, сприятливої психологічної атмосфери та відсутності проявів насильства. Для безпеки освітнього процесу навчальні корпуси охороняються, вхід можливий лише по перепустках або студентських квитках. Також в НУ дбають про психічне здоров'я здобувачів вищої освіти та інших учасників освітнього процесу. Для запобігання психічним перенавантаженням, булінгу та загальної психологічної підтримки діє Психологічна служба http://surl.li/guosdd, http://surl.li/npcfcw, яка проводить

консультування, тренінги для здобувачів вищої освіти та НПП. Крім того діє Положення про цілісну систему турботи про психічне здоров'я учасників освітнього процесу http://surl.li/ioiajt. Із урахуванням воєнного стану безпечність освітнього середовища для життя та здоров'я здобувачів вищої освіти забезпечується також через інформування щодо алгоритму дій за сигналом «Повітряна тривога» https://stu.cn.ua/wp-content/stu-media/normobaza/normdoc/nakazu/2025/nakaz-01-VC.pdf, функціонуванням укриттів у різних корпусах НУ. Крім того, задля безпечності освітнього процесу практичні/лабораторні заняття, сесія відбувається у змішаному режимі – здобувач обирає форму участі: аудиторно чи дистанційно.

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.

Підтримка здобувачів вищої освіти має системний характер з формальними і неформальними механізмами реалізації, в якій задіяні всі структурні підрозділи НУ з урахуванням студентоцентрованого підходу. Освітня та організаційна підтримка реалізується через деканат – кафедру– гаранта - старост академічних груп – студентську раду. Створено матеріально-технічне та навчально-методичне забезпечення; впроваджуються інноваційні технології та методи навчання, запроваджено електронне супроводження освітньої діяльності. Здобувачі вищої освіти мають можливість реалізувати право на участь у програмах академічної мобільності, формувати індивідуальну освітню траєкторію, навчатися за індивідуальним планом. Інформаційна ж підтримка здійснюється на рівні всіх структурних підрозділів НУ, які мають власні сайти та сторінки в соціальних мережах (Whatsapp, Facebook та Instagram). Основним і важливим джерелом інформаційної підтримки є сайт НУ https://stu.cn.ua/ , де висвітлюється вся необхідна інформація для здобувачів як з освітніх, так і інших питань. Важливим джерелом інформації є бібліотека http://library2.stu.cn.ua, яка забезпечує створення комфортного середовища для використання здобувачами інформації, засобів міжособистісного спілкування й обміну знаннями. Основними напрямками соціальної підтримки є соціальний захист, поліпшення побутових умов у гуртожитках, організація оздоровлення та відпочинку здобувачів. З метою підвищення життєвого рівня та заохочення за успіхи у навчанні, участь у громадській, спортивній і науковій діяльності НУ може надавати матеріальну допомогу та заохочення здобувачам вищої освіти http://surl.li/xyoddt . За рейтингом успішності з урахуванням соціального статусу здійснюється переведення здобувачів на навчання за кошти державного або місцевого бюджету, виключно на конкурсній основі http://surl.li/zxzqey. Соціальну та психологічну підтримку здобувачів здійснює Психологічна служба університету http://surl.li/trmmjl. Консультативна підтримка надається на рівні всіх підрозділів Університету: консультації викладачів, гаранта, деканату, бухгалтерії, військово-облікового відділу, Центру розвитку кар'єри з питань працевлаштування та проходження правки https://robota-chntu.stu.cn.ua. Анкетування здобувачів свідчить, що освітня, організаційна, інформаційна, консультативна та соціальна їх підтримка в НУ і на кафедрі знаходиться на належному рівні.

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)

У НУ створені достатні умови для забезпечення права на освіту особам з особливими освітніми потребами. На сайті НУ в правилах прийому https://stu.cn.ua/wp-content/uploads/2025/07/pravyla-pryjomu-2025-7.pdf , зокрема в частині створення спеціальних умов вступу (наприклад, п. XV) та нормативних документах наведено перелік можливостей для навчання таких осіб, зокрема, можливість заочної (дистанційної) форми навчання, академічної відпустки, вільного відвідування занять – Порядок надання дозволу на вільне відвідування занять http://surl.li/oimyik. Впродовж навчання осіб з особливими освітніми потребами супроводжує Психологічна служба. Для координації роботи в напрямку освіти осіб з особливими потребами в НУ створено Центр інклюзивної освіти http://surl.li/onjutl , який забезпечує сприятливі умови для навчання молоді з особливими освітніми потребами та вдосконалення соціальних стандартів системи вищої освіти.
Навчальні корпуси НУ обладнані пандусами для маломобільних груп населення, передбачено порядок супроводу осіб, що потребують допомоги (через чергових корпусів) – «Порядок супроводу осіб з інвалідністю та інших маломобільних груп населення у НУ http://surl.li/wccqjy. Окрім того, є Технічний звіт щодо доступності будівель для маломобільних категорій населення https://stu.cn.ua/wp-content/uploads/2022/12/zvit-pro-dostupnist-shevchenka-1.pdf. Наразі на ОП не було осіб з 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

Механізм вирішення конфліктних ситуацій урегульовано відповідними нормативними актами, розміщеними на сайті НУ: Кодекс корпоративної культури Національного університету «Чернігівська політехніка» http://surl.li/prwroi, згідно з яким гендерне насильство, у тому числі, сексуальні домагання на робочому місці та в освітньому процес, засуджується та вживаються заходи, спрямовані на протидію цьому явищу; Положення щодо протидії булінгу (цькуванню) http://surl.li/jmfuix, Положення про порядок роботи зі зверненням громадян http://surl.li/hddgei, Антикорупційна програма http://surl.li/loxead, Положення про функціонування телефону довіри, електронної та поштової скриньок довіри з питань запобігання та протидії корупції http://surl.li/sjxhrn . Крім того, на сайті НУ розміщені корисні посилання http://surl.li/khqdsv. Вся необхідна інформація знаходиться у вільному доступі на сайті НУ. Відповідно до зазначених нормативних документів при виникненні конфліктної ситуації, що має характер булінгу, домагання сексуального характеру, дискримінації, корупції або скарга іншого характеру можна: до загального відділу власноруч або на електронну пошту Університету НУ на ім'я ректора

надіслати заяву (скаргу, пропозицію), зазначену на сайті (cstu@stu.cn.ua); викласти свої пропозиції (зауваження, скарги, заяву) на особистому прийомі у посадової особи (ректора, проректорів, директорів інститутів) або скористатися “Телефоном довіри” чи “Скринькою довіри”, зазначеними на сайті НУ http://surl.li/icgubk . Первинний розгляд письмових звернень громадян проводиться ректором НУ або його проректорами відповідно до їх повноважень. За кожним фактом звернення проводиться ретельна перевірка, результати якої надаються ректору/проректорам. Громадянину, що подав звернення, надається письмова (або усна – за згодою) відповідь. Зокрема у разі, якщо буде встановлено факт булінгу, ректор зобов’язаний повідомити уповноважені підрозділи органів Національної поліції України та інші відповідні служби, зокрема, Службу у справах дітей. У разі, якщо комісія не кваліфікує випадок як булінг, а постраждалий не згодний з цим, то він може одразу звернутись до органів Національної поліції України, за будь-якого рішення комісії ректор НУ забезпечує психологічну підтримку усім учасникам випадку http://surl.li/zsnxlm. За час реалізації ОП випадків подібних конфліктних ситуацій (корупційних, дискримінаційних або сексуальних домагань) не виникало.

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

У Національному університеті «Чернігівська політехніка» запроваджено процедури розроблення, затвердження, моніторингу та перегляду ОП, які регламентуються такими документами:
1) Порядок розробки, затвердження, моніторингу та закриття освітніх програм у Національному університеті «Чернігівська політехніка» https://stu.cn.ua/wp-content/stu-media/normobaza/normdoc/norm-osvitproces/poryadok-rozrobky-zatverdzhennya-monitoryngu-ta-zakryttya-osvitnih-program.pdf ;
2) Положення про гаранта освітньої програми в Національному університеті «Чернігівська політехніка» https://stu.cn.ua/wp-content/stu-media/normobaza/normdoc/norm-osvitproces/polozhennya-pro-garanta-osvitnoyi-programy.pdf ;
3) Положення про внутрішню систему забезпечення якості вищої освіти в Національному університеті «Чернігівська політехніка» https://stu.cn.ua/wp-content/stu-media/normobaza/normdoc/norm-yakist/polozh-pro-vnutrishnyu-systemu-zabezpechennya-yakosti-vo.pdf ;
4) Положення про раду із забезпечення якості вищої освіти в Національному університеті «Чернігівська політехніка» https://stu.cn.ua/wp-content/stu-media/normobaza/normdoc/norm-yakist/polozh-pro-radu-iz-zabezpechennya-yakosti-vo.pdf
5) Положення про внутрішню акредитацію освітніх програм у Національному університеті «Чернігівська політехніка» https://stu.cn.ua/wp-content/stu-media/normobaza/normdoc/norm-yakist/polozh-pro-vnutrishnyu-akredytacziyu-op.pdf ;
6) Положення про сектор систем менеджменту якості вищої освіти в Національному університеті «Чернігівська політехніка» https://stu.cn.ua/wp-content/stu-media/normobaza/normdoc/norm-yakist/polozh-pro-sektor-system-menedzhmentu-yakosti-vo.pdf .

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

Важливою складовою системи внутрішнього забезпечення якості вищої освіти Університету є моніторинг освітніх програм. Процедури, пов’язані з розробкою, затвердженням, моніторингом та переглядом ОП, прописані в Порядку розробки, затвердження, моніторингу та закриття освітніх програм у Національному університеті «Чернігівська політехніка» https://numl.org/O4V.
Згідно з п. 15. Порядку: моніторинг та періодичний перегляд освітньої програми здійснюється стейкхолдерами, гарантом освітньої програми та керівництвом Університету шляхом аналізу ефективності її подальшої реалізації в незмінному виді. При цьому враховується: прийняття чи коригування стандарту вищої освіти; висновки акредитаційної експертизи; відгуки стейкхолдерів; перегляд місії та стратегії Університету; результати наукових досліджень; результати вступної кампанії та інше.
У випадку необхідності внесення змін гарант освітньої програми здійснює коригування потрібних елементів освітньої програми, узгоджує її з навчальним та навчально-методичними відділами, виносить на затвердження Вченою радою Університету. Зміни вводяться в дію наказом ректора та мають бути оприлюднені на офіційних веб ресурсах Університету.
Моніторинг освітньої програми проводиться систематично відповідними відділами та відповідно до документів зазначених вище, а періодичний перегляд – один раз на рік (до початку нового навчального року).
ОПП «Кібербезпека», яка була розроблена в 2019 році, систематично оновлювалась, зокрема, на підставі підписання договору про подвійні дипломи з Техніко-гуманітарною академією м. Бельсько-Бяла (Польща), рекомендацій роботодавців (ІТ кластер, кіберполіція) та пропозицій здобувачів вищої освіти.
Зміни, що були внесені: окремі дисципліни були перенесені з вибіркових у нормативні, уточнена назва дисциплін, введено нові дисципліни. Кількість кредитів вибіркових компонент збільшена порівняно з ОП 2019 року.

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

Наявний постійний доступ до змісту та складових ОПП на сайті www.stu.cn.ua.

В Університеті діє система опитування щодо якості НПП та ОПП – https://poll.stu.cn.ua/auth.php , https://stu.cn.ua/yakist-osvity/monitoryng-yakosti/.
Запущено ел.сервіс внесення пропозицій,: https://offers.stu.cn.ua/view/total_view.php. Кафедрою проводяться опитування студентів. Пропозиції здобувачів щодо уд-ня ОПП збир-ся також безпосередньо під час освітнього процесу шляхом спілкування з гарантом програми, НПП випускових кафедр та адміністрацією університету. Протягом навчального року проводяться спільні зустрічі студентів, роботодавців та гаранта з приводу обговорення змісту ОПП щодо необхідності внесення змін.
На сайті кафедри представлені фото з цих зустрічей, напр. https://mmi.stu.cn.ua/novyny/rozshyrene-zasidannya-kafedry-kiberbezpeky-ta-matematychnogo-modelyuvannya/ На платформі Moodle здійснюється моніторинг щодо задоволеності навчанням, при цьому анкета містить варіант відкритої відповіді “Ваші пропозиції із удосконалення освітнього процесу в ННІ ЕІТ”. Окремі пропозиції були наступні: Поглиблення процесів взаємодії з підприємствами, організаціями, установами (було розпочато цикл зустрічей із представниками СБУ в Чернігівській області з питань ознайомлення студентів із технологією OSINT), Поява специфічного апаратного забезпечення для тестів, практики та опрацювання професійних навичок в процесі вивчення (закуплено трьохдіапазонний індикатор поля iProtect 1207, обнаружувач сприхованих камер Wega і, тепловізор Wintact WT3320 тощо).

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

Згідно з Положенням про студентське самоврядування Національного університету «Чернігівська політехніка», затв. Конференцією студентів Національного університету «Чернігівська політехніка» 30 червня 2020 року, https://stu.cn.ua/wp-content/stu-media/normobaza/normdoc/norm-stud-samovryad/polozh-pro-stud-samovryad.pdf в Університеті діють органи студентського самоврядування. Згідно з п. 10 підрозділу 5.6.2 Статуту органи студентського самоврядування вносять пропозиції щодо змісту навчальних планів і ОП https://stu.cn.ua/wpcontent/uploads/2021/04/statut2.pdf
Так, на одній із зустрічі роботодавців, представників кафедри кібербезпеки та математичного моделювання та здобувачів вищої освіти був присутній Дятел І., представник студентського самоврядування (голова студради ННІ ЕІТ), який запропонував додати в навчальні дисципліни теми про сканування мереж за допомогою nmap, виявлення та використання вразливостей у комп ′ ютерних системах та мережах.
В зміст навчальної дисципліни Управління мережевою безпекою було додано детальний опис архітектури мереж WPA та WPA2 з попередньо розданим ключем (PSK) та ін
Також магістрам пропонується дисципліна "Тестування на проникнення та етичний хакінг", де більш детально розглядаються відповідні питання. Додатково ще суденти можуть пройти курс "Ethical Hacker" в Академії Cisco НУ "Чернігівська політехніка".
Пропозицію було обговорено на засіданні кафедри та прийнято відповідні рішення.

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

В НУ діє Положення про організацію опитування стейкхолдерів щодо якості освіти і освітньої діяльності НУ, затв. Вченою радою НУ 31 серпня 2020 р. протокол No6. http://surl.li/ksbckl. Згідно п. 2.1 Положення, опитування стейкхолдерів здійснюється за допомогою системи онлайн опитування на сайті НУ або за допомогою Google-форм з використанням анкет щодо оцінки якості ОПП та вдосконалення ОПП для роботодавців.
Роботодавці також мають можливість брати участь у засіданнях кафедри та вносити пропоз. за допомогою сервісу внесення пропозицій щодо змін до ОП та підвищення якості вищої освіти на сайті НУ https://offers.stu.cn.ua/view/total_view.php.
Так, на засіданнях кафедри був присутній стейкхолдер Зайцев С.В. (директор ТОВ “Інформаційна безпека держави”), Руденок О.А. (директор ТОВ “Інформаційні системи захисту”), які вносили свої пропозиції щодо оновлення змісту робочих програм дисциплін пов’язаних з питаннями технічного захисту інформації.
Також одним із прикладів безпосереднього залучення роботодавців до реалізації ОПП є робота у Екзаменаційних комісій, що регламентується відповідним положенням.
Крім того, під час проходження студентами практик, проводиться опитування керівників від баз практик щодо змісту ОПП.
Систематичне обговорення ОПП та змісту її окремих освітніх компонентів відбувається на наукових конференціях і семінарах, зокрема на Meetup «Актуальні питання кібербезпеки» та щорічних Всеукраїнських конференція. напр "Юність науки”.
Всі пропозиції стейкхолдерів були розглянуті та прийняті на засіданнях кафедри.

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

В структурі НУ «Чернігівська політехніка» діє Центр розвитку кар’єри, який на постійній основі займається працевлаштуванням здобувачів та випускників Університету, організацією їх практичної підготовки та налагодженню стратегічного партнерства з підприємствами, установами та організаціями. Центр розвитку кар’єри має відповідну сторінку на сайті Університету https://robota-chntu.stu.cn.ua/, де публікує вакантні посади, які роботодавці пропонують випускникам, анонсує «ярмарки вакансій» та інші заходи, що організовуються для допомоги у працевлаштуванні. Про відповідні заходи Центр також інформує через різні канали комунікації, в тому числі і соціальні мережі.
Збиранням інформації щодо працевлаштування випускників ОПП займається деканат, який постійно співпрацює зі старостами, а також гарант ОПП.

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

Процедури внутрішнього забезпечення якості освіти в НУ врегульовуються Положенням про внутрішню акредитацію освітніх програм у НУ «Чернігівська політехніка» https://stu.cn.ua/wp-content/stu-media/normobaza/normdoc/norm-yakist/polozh-pro-vnutrishnyu-systemu-zabezpechennya-yakosti-vo.pdf ,
Положенням про внутрішню систему забезпечення якості вищої освіти в НУ «Чернігівська політехніка» https://stu.cn.ua/wp-content/stu-media/normobaza/normdoc/norm-yakist/polozh-pro-vnutrishnyu-systemu-zabezpechennya-yakosti-vo.pdf та іншими.

На основі результатів внутрішніх процедур забезпечення якості, зокрема внутрішніх акредитацій, перевірки дистанційної платформи «Moodle» тощо сектором СМЯВО проводяться відповідні заходи з метою донесення до відома гарантів, НПП та врахування виявлених недоліків: Методичний семінар з актуальних питань акредитації освітніх програм (26.04.2024 року) https://stu.cn.ua/news/metodychnyj-seminar-z-aktualnyh-pytan-akredytacziyi-osvitnih-program/, Рішення Вченої ради НУ про стан методичної роботи кафедри університету https://stu.cn.ua/wp-content/uploads/2024/05/rishennya-metod-robota.pdf (27.05.2024) Семінар щодо особливостей проходження акредитації https://stu.cn.ua/news/seminar-shhodo-osoblyvostej-prohodzhennya-akredytaczij/ (06.06.2024) тощо. Основними рекомендаціями були: систематично оновлювати та доповнювати навчально-методичні матеріали, що розміщені в системі Moodle, завідувачам кафедри перевіряти дисципліни щодо наповненості та актуальності навчально-методичних матеріалів у системі Moodle, що відповідно здійснюється і про що обговорюється на засіданнях кафедри, а також контролювати відповідність компетентностей та програмних результатів навчання, вказаних в силабусах, наведеним у ОПП.

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?

За результатами акредитації 26.10.2020 р. – 28.10.2020 р. ООП Кібербезпека освітнього рівня магістр ЕГ були визначені основні слабкі сторони та надані рекомендації, а саме:
1) Активізувати роботу по залученню студентів до процесів коригування ОПП.
Здобувачі ВО НУ «Чернігівська політехніка» залучені до процедур періодичного перегляду ОПП та інших процедур внутрішнього забезпечення якості освіти шляхом проведення опитувань. В НУ «Чернігівська політехніка» функціонує Система опитування здобувачів вищої освіти щодо якості НПП та ОП, результати опитувань оприлюднюються на офіційному сайті університету (Моніторинг якості: http://surl.li/aoqru). Крім цього, кафедрою щосеместрово проводяться опитування щодо якості освітнього процесу та якості викладання конкретної дисципліни, результати опитувань оприлюднюються на офіційному сайті кафедри (https://mmi.stu.cn.ua/novyny/rezultaty-opytuvannya-zdobuvachiv-vyshhoyi-osvity-spetsialnosti-125-kiberbezpeka-u-2025-rotsi/ , https://mmi.stu.cn.ua/novyny/12436/).
Також здобувачі вищої освіти запрошуються на засідання кафедри з перегляду ОПП, де можуть висловити свої пропозиції щодо удосконалення ОПП. Запроваджено додаткові механізми збору пропозицій від студентів через електронні платформи (https://offers.stu.cn.ua/view/total_view.php) та інтерактивні обговорення.
2) Стимулювати обізнаність студентів щодо освітніх компонентів та принципів студентоцентрованого навчання.
ЗВО забезпечив:
- наявність інформаційних систем для ефективного управління освітнім процесом;
- вибір форм і методів викладання й навчання, що заохочує активну участь здобувачів вищої освіти в освітньому процесі;
- збирання та аналіз інформації зворотного зв'язку від здобувачів вищої освіти щодо методів, засобів та технологій навчання і викладання з освітніх компонентів.
3) Посилити матеріально-технічне забезпечення кафедри в аспекті підготовки фахівців захисту мережевого та кібернетичного простору.
Проведено закупівлю додаткового обладнання, а також отримано обладнання в межах проекту USAID
4) Оптимізувати процедури вибору вибіркових дисциплін шляхом перегляду обмежень на мінімальну чисельність групи студентів.
Формування індивідуальної освітньої траєкторії забезпечується наявністю вибіркових дисциплін загальним обсягом 27 %. Порядок вибору здобувачами вищої освіти вибіркових дисциплін врегульовується Положенням https://stu.cn.ua/wp-content/stu-media/normobaza/normdoc/norm-osvitproces/polozhennya-pro-indyvidualnu-osvitnyu-trayektoriyu.pdf . Здобувачі вищої освіти можуть реалізувати своє право на індивідуальну траєкторію через свої електронні кабінети, при цьому попередньо ознайомитися із вибірковими дисциплінами вони можуть у відповідному розділі вибіркових дисциплін в «MOODLE». Обрані здобувачами ВК заносяться до їх індивідуальних навчальних планів.
Каталог дисциплін https://stu.cn.ua/osvitnij-proczes/katalog-zagalnouniversitetskih-distciplin/
Для удосконалення ОП брався до уваги досвід акредитації інших ОПП у НУ.

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

До процедур внутр. забезп. якості ОПП в НУ задіяні всі учасники академічної спільноти, починаючи від етапу розробки ОПП. Крім робочої групи, в яку входять висококвал. НПП, задіяні також здобувачі вищої освіти, НПП, роботод., а також навч. відділ, навч.-метод. відділ. Під час реалізації ОПП здійснюється ряд процедур, направлених

на з'ясування особливостей реалізації ОПП та покращення освітнього процесу. Сектором СМЯВО проводяться опитування здоб., роботод., про які згадувалося вище, а також НПП http://surl.li/rtxtqk . Результати опитування аналізуються і разом із результатами проходж. попередніх акредитацій, перевірки навч.-метод. заб., н-д, наповнення «Moodle», проводяться відповідні заходи з удоскон. ОПП. Опитув. провод. НПП в межах окремих освітніх компон., результати яких обгов. на засіданні кафедри. Якість пров. навч. занять контрол. згідно з Положенням про оцінювання якості проведення навчальних занять у НУ http://surl.li/pbpkks . Здійснюється оцінка рівня проф. квал. НПП, який претендує на підв. в посаді або на заміщ. вакант. посади; визначання відповідн. науково-методичного рівня викладан. ОК, вимогам до присвоєння вченого звання. Положенням про щорічне оцінювання НПП і кафедр НУ, http://surl.li/tdppxl передбачено звітування НПП за основн. напрям. діяльн. та щорічне оцінювання НПП і кафедр НУ за допом. електрон. системи звітув., що знаход.– http://npp.stu.cn.ua . Центр розвитку кар'єри контролює вчасність підв. квал. НПП.

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

Процедури внутрш. забезп. якості освіти здійснюються згідно з Положенням про внутрішню систему забезп. якості вищої освіти в НУ, затв. Вченою радою НУ 31 серпня 2020 р. протокол No6 http://surl.li/stdzmz. У внутрішн. забезп. якості освіти беруть участь ЗВО, кафедри, гарант ОПП, НПП, які забезп. виклад. дисц. на ОП, стейкхолдери, сектор СМЯВО. За реалізацію ОПП відповідає гарант ОПП. На гаранта ОПП покладається обов'язок внесення змін до діючої освітньої ОПП як на основі самооцінки, так і зовнішнього оцінювання з урахув. опитувань та рекоменд. стейкхолдерів, виклад. та здобувачів ВО. Стейкхолдери, НПП та здобувачі вищої освіти здійснюють оцінку якості освіти шляхом анкетування. На засіданнях кафедри обговорюються питання організації та проведення освітнього процесу з навчальних дисциплін кафедри відповідно до ОП, навчального плану. Сектор СМЯВО здійснює організацію, проведення та аналіз результатів опитувань (анкетувань) стейкхолдерів, викладачів та здобувачів з питань якості організації освітнього процесу в НУ, якості ОПП, якості викладання навчальних дисциплін та рівня підготовленості випускників НУ до професійної діяльності згідно з Положенням про сектор систем менеджменту якості вищої освіти в НУ, затв. Вченою радою НУ 31 серпня 2020 р. протокол No6 http://surl.li/vaarpx . Важливими складовими в системі забезп якості вищої освіти є Рада роботодавців http://surl.li/kyjmwx , Рада із забезпечення якості вищої якості http://surl.li/bskunb , також органи студент. самовр.

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?

Основними документами, які регулюють права та обов'язки усіх учасників освітнього процесу в НУ "Чернігівська політехніка" є Статут (https://stu.cn.ua/wp-content/uploads/2022/05/statut.pdf), Колективний договір (https://stu.cn.ua/wp-content/stu-media/normobaza/normdoc/kol-dogovir.pdf), Правила внутрішнього розпорядку (https://stu.cn.ua/wp-content/stu-media/normobaza/normdoc/pravila-vnutrishnogo-rozporyadku.pdf), Кодекс корпоративної культури (https://stu.cn.ua/wp-content/stu-media/normobaza/normdoc/kodeks-korporatyvnoyi-kultury.pdf), Кодекс академічної доброчесності (https://stu.cn.ua/wp-content/stu-media/normobaza/normdoc/norm-yakist/kodeks-akademichnoyi-dobrochesnosti.pdf), Положення про організацію освітнього процесу в університеті ((https://stu.cn.ua/wp-content/stu-media/normobaza/normdoc/norm-osvitproces/polozhennya-pro-organizacziyu-osvitnogo-proczesu.pdf) та ін.
В університеті розроблені, погоджені, затверджені у встановленому порядку й викладені для загального доступу на сайті університету в розділі «Нормативна база»(https://stu.cn.ua/normatyvna-baza/) інші нормативні документи, які регламентують всі аспекти освітнього процесу.
НПП дізнаються про ці документи під час прийому на роботу.
Знайомство першокурсників з особливостями організації освітнього процесу в Університеті відбувається в «Школі першокурсника» (http://surl.li/lbvzt).
Також оприлюднено у відкритому доступі на веб-сайті університету інформацію про освітню програму https://op.stu.cn.ua/view/total_view.php.

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

https://op.stu.cn.ua/view/total_view.php

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

https://op.stu.cn.ua/files/op/OPP_125_Cyber_Security_master_2024_2v.pdf, mmi.stu.cn.ua.
https://op.stu.cn.ua/files/np/NP_125_Cyber_Security_master_2024_2.pdf
https://op.stu.cn.ua/files/np/NP_125_Cyber_Security_master_2024_z.pdf

https://stu.cn.ua/wp-content/stu-media/normobaza/normdoc/norm-osvitproces/polozhennya-pro-indyvidualnu-osvitnyu-trayektoriyu.pdf.

11. Перспективи подальшого розвитку ОП

Якими загалом є сильні та слабкі сторони ОП?

Сильні сторони ОП:
-впроваджена система забезпечення якості освітнього процесу (використання Moodle, хмарних сервісів, електронного документообігу);
-висока академічна і професійна кваліфікація НПП, наявність фахівців з практичним досвідом у сфері кіберзахисту, залучення експертів ДССЗЗІ, СБУ, кіберполіції, ІТ-бізнесу;
-сучасне матеріально-технічне забезпечення, лабораторії кіберзахисту, мережевого захисту, лабораторія ТЗІ, навчальна серветна тощо;
-практикоорієнтованість навчання;
-активне залучення роботодавців до формування та рецензування ОП;
-гнучкість ОП — наявність вибіркових дисциплін, що відповідають міжнародним трендам (з цифрової криміналістики, пентесту, безпеки хмарних технологій, управління інцидентами);
- створені умови для отримання подвійних дипломів.

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

-розширення лінійки дисциплін, які викладають англійською мовою;
-участь студентів та викладачів у програмах міжнародної академічної мобільності (наприклад, Erasmus+);
-залучення здобувачів до міжнародних науково-дослідних та інноваційних проєктів;
-подальше покращення матеріально-технічної бази навчальних лабораторій.

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: Новомлинець Олег Олександрович

Дата: 23.09.2025 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	
ОК 4. Методологія та організація наукових досліджень	навчальна дисципліна	*ОК04_С_Методологія та організація наукових досліджень.docx.pdf*	iKofDDzWOGXow8D7OPdm79ffH41TsNytoVuefrpZSCw=	*Лабораторія кібербезпеки 1-111* *1. Системний блок Intel Core i3/ RAM 8 GB/ SSD 250 Gb/ HDD 1 Tb/ keybord/ mouse – 12 од.* *Рік введення в експлуатацію: 2021* *2. Монітор Philips 246E 9QPJB/00 – 12 од.* *Рік введення в експлуатацію: 2021* *3. 3. ПЗ Microsoft Windows* *Рік введення в експлуатацію: 2024* *Версія програмного забезпечення та кількість ліцензій: Windows 11 Pro Ukrainian DVD, 12 ліцензій* *4. ПЗ Microsoft Office* *Рік введення в експлуатацію: 2024* *Версія програмного забезпечення та кількість ліцензій: Office Home and Student 2021 ESD,* *12 ліцензій* *5. ПЗ ОС Ubuntu Desktop* *Рік введення в експлуатацію: 2025* *Версія програмного забезпечення та кількість ліцензій: 24.04.2 LTS, ліцензія GNU* *6. ПЗ ОС Kali-Linux* *Рік введення в експлуатацію: 2025* *Версія програмного забезпечення та кількість ліцензій: 2024.4-Kernel 6.11.0, Xfce 4.18.6, ліцензія GNU* *7. ПЗ VirtualBox* *Рік введення в експлуатацію: 2025* *Версія програмного забезпечення та кількість ліцензій: v. 7.1.6, ліцензія GNU* *8. Проектор Optoma x342e – 1 од.* *Рік введення в експлуатацію: 2024* *9. Екран проекційний – 1 од.* *Рік введення в експлуатацію: 2024* *10. Багатофункціональний пошуковий прилад ANDRE – 1 од.* *Рік введення в експлуатацію: 2019* *11. Багатоканальний детектор бездротових протоколів PROTECT 1207i – 1 од.* *Рік введення в експлуатацію: 2020* *12. Детектор прихованих камер WEGAi – 1 од.* *Рік введення в експлуатацію: 2020* *13. Тепловізор Wintact WT3320 – 1 од.* *Рік введення в експлуатацію: 2020* *14. SDR-radio HackRF One PortaPack H2 – 1 компл.* *Рік введення в експлуатацію: 2023* *15. Тестер радіокомунікаційний Rohde&Schwartz CMD55 – 1 од.* *16. Осцилограф цифровий двоканальний FNIRSI-1013D – 1 од.* *Рік введення в експлуатацію: 2024* *17. Блок живлення лабораторний KORAD KD3005D – 1 од.* *Рік введення в експлуатацію: 2024* *18. Паяльна станція BAKU BK852D – 1 од.* *Рік введення в експлуатацію: 2024* *19. Мультиметр UNI-T UT89X – 1 од.* *Рік введення в експлуатацію: 2024* *20. Тестер кабельний – 1 од.* *Рік введення в експлуатацію: 2024* *21. Аналізатор спектра С4-77 – 1 од.* *22. Інтерферометр INCO NLMZ-4/50 № 1175/81 – 1 од.* *23. Селективний мікровольтметр RFT STV 401 № 07045 – 1 од.* *24. Аналізатор спектра С1-55 – 1 од.* *25. Фліпчарт магнітно-маркер. двохсторонній на колесах 1000*700 – 1 од.* *Рік введення в експлуатацію: 2023*
ОК 5. Стандартизація, сертиікація засобів та компллксів захисту інформації	навчальна дисципліна	*ОК05_С_СЗтаКЗІ_2024.docx.pdf*	74m7xbvH4pomAIskq5bOWVPLf/5+LooiIEcDovgI63s=	*Лабораторія кібербезпеки 1-105* *1. Моноблок All in one HP 205G824AiOBU-R3-5425UIDS / VA / 8GB / 256 SSD / W11p64DowngradeW10p64 / 1yw / 125 BLKkbd / 125mouse / No WLAN / Iron Gray with 5MP WebCam ID / Sea and Rail / – 15 од.* *Рік введення в експлуатацію: 2024* *Версія програмного забезпечення та кількість ліцензій: Windows 11 Pro, 15 ліцензій* *2. ПЗ Microsoft Office* *Рік введення в експлуатацію: 2024* *Версія програмного забезпечення та кількість ліцензій: Office Home and Student 2021 ESD,* *15 ліцензій* *3. ПЗ ОС Ubuntu Desktop* *Рік введення в експлуатацію: 2025* *Версія програмного забезпечення та кількість ліцензій: 24.04.2 LTS, ліцензія GNU* *4. ПЗ ОС Kali-Linux* *Рік введення в експлуатацію: 2025* *Версія програмного забезпечення та кількість ліцензій: 2024.4-Kernel 6.11.0, Xfce 4.18.6, ліцензія GNU* *5. ПЗ VirtualBox* *Рік введення в експлуатацію: 2025* *Версія програмного забезпечення та кількість ліцензій: v. 7.1.6, ліцензія GNU* *6. Проектор Optoma x342e – 1 од.* *Рік введення в експлуатацію: 2024* *7. Екран проекційний – 1 од.* *Рік введення в експлуатацію: 2024* *8. Стенд навчальний "Охоронні системи TIRAS" – 1 од.* *Рік введення в експлуатацію: 2023* *9. Програмний продукт система захист. інформації "Лоза-1" версія 4 – 2 од.* *Рік введення в експлуатацію: 2021* *10. Програмний продукт "Zillya Антивірус для Бізнесу" версія 1.1.xxxx. у на 2 об'єкти з правом користування на 5 років – 2 од.* *Рік введення в експлуатацію: 2021* *11. Локатор нелінійний – 1 од.* *12. Прилад акустичного шуму мобільний PIAC-2ГМ № 0110 – 1 од.* *13. Генератор лінійного шуму Базальт-2ГС № 0414 – 1 од.* *14. Випромінювач акустичний PIAC-2ВА. № 0517 – 1 од.* *15. Вібровипромінювач п'єзоелектричний PIAC-2ВП №№ 0630, 0653 – 2 од.* *16. Прилад захисту інформації в аналогових телефонних лініях PIAC-2С/Т № 0019 – 1 од.* *17. Прилад радіочастотного шуму стаціонарний PIAC-1ГС № 0469 – 1 од.* *18. Прилад радіочастотного шуму мобільний PIAC-1ГМ № 0164 – 1 од.*
ОК 6. Проектування технічних систем	навчальна дисципліна	*ОК06_С_ПроектТехСистЗахІнф*	4Z8s6t/DnvC9dLJcKIQThHEQfOZs	*Лабораторія кібербезпеки 1-105*

захисту інформації		*_2024.docx.pdf*	lmm/HFvCCd+hlMc=	*1. Моноблок All in one HP 205G824AiOBU-R3-5425UIDS / VA / 8GB / 256 SSD / W11p64DowngradeW10p64 / 1yw / 125 BLKkbd / 125mouse / No WLAN / Iron Gray with 5MP WebCam ID / Sea and Rail / – 15 од.* *Рік введення в експлуатацію: 2024* *Версія програмного забезпечення та кількість ліцензій: Windows 11 Pro, 15 ліцензій* *2. ПЗ Microsoft Office* *Рік введення в експлуатацію: 2024* *Версія програмного забезпечення та кількість ліцензій: Office Home and Student 2021 ESD,* *15 ліцензій* *3. ПЗ ОС Ubuntu Desktop* *Рік введення в експлуатацію: 2025* *Версія програмного забезпечення та кількість ліцензій: 24.04.2 LTS, ліцензія GNU* *4. ПЗ ОС Kali-Linux* *Рік введення в експлуатацію: 2025* *Версія програмного забезпечення та кількість ліцензій: 2024.4-Kernel 6.11.0, Xfce 4.18.6, ліцензія GNU* *5. ПЗ VirtualBox* *Рік введення в експлуатацію: 2025* *Версія програмного забезпечення та кількість ліцензій: v. 7.1.6, ліцензія GNU* *6. Проектор Optoma x342e – 1 од.* *Рік введення в експлуатацію: 2024* *7. Екран проекційний – 1 од.* *Рік введення в експлуатацію: 2024* *8. Стенд навчальний "Охоронні системи TIRAS" – 1 од.* *Рік введення в експлуатацію: 2023* *9. Програмний продукт система захист. інформації "Лоза-1" версія 4 – 2 од.* *Рік введення в експлуатацію: 2021* *10. Програмний продукт "Zillya Антивірус для Бізнесу" версія 1.1.xxxx. у на 2 об ' єкти з правом користування на 5 років – 2 од.* *Рік введення в експлуатацію: 2021* *11. Локатор нелінійний – 1 од.* *12. Прилад акустичного шуму мобільний PIAC-2ГМ № 0110 – 1 од.* *13. Генератор лінійного шуму Базальт-2ГС № 0414 – 1 од.* *14. Випромінювач акустичний PIAC-2ВА. № 0517 – 1 од.* *15. Вібровипромінювач п'єзоелектричний PIAC-2ВП №№ 0630, 0653 – 2 од.* *16. Прилад захисту інформації в аналогових телефонних лініях PIAC-2С/Т № 0019 – 1 од.* *17. Прилад радіочастотного шуму стаціонарний PIAC-1ГС № 0469 – 1 од.* *18. Прилад радіочастотного шуму мобільний PIAC-1ГМ № 0164 – 1 од.*
ОК 7. Технології безпеки бездротових і мобільних мереж	навчальна дисципліна	*ОК7_Силабус_ Технології безпеки бездротових і мобільних мереж_2024.docx.pdf*	KD4tDHd4+fo366zZEKMHRG8iG MOqa9O4ufkQTtTWVmY=	*Лабораторія кібербезпеки 1-110* *1. Системний блок Intel Core i3 8100/ RAM 8 GB/ SSD 120 Gb/ HDD 1 Tb/ keybord/ mouse – 12 од.* *Рік введення в експлуатацію: 2020* *2. Монітор LG 22MP58VQ – 12 од.* *Рік введення в експлуатацію: 2020* *3. ПЗ Microsoft Windows* *Рік введення в експлуатацію: 2024* *Версія програмного забезпечення та кількість ліцензій: Windows 10 Pro Ukrainian DVD, 12 ліцензій* *4. ПЗ Microsoft Office* *Рік введення в експлуатацію: 2024* *Версія програмного забезпечення та кількість ліцензій: Office Home and Student 2021 ESD,* *12 ліцензій* *5. ПЗ ОС Ubuntu Desktop* *Рік введення в експлуатацію: 2025* *Версія програмного забезпечення та кількість ліцензій: 24.04.2 LTS, ліцензія GNU* *6. ПЗ ОС Ubuntu Server* *Рік введення в експлуатацію: 2025* *Версія програмного забезпечення та кількість ліцензій: 24.04.2 LTS, ліцензія GNU* *7. ПЗ ОС Kali-Linux* *Рік введення в експлуатацію: 2025* *Версія програмного забезпечення та кількість ліцензій: 2024.4-Kernel 6.11.0, Xfce 4.18.6, ліцензія GNU* *8. ПЗ VirtualBox* *Рік введення в експлуатацію: 2025* *Версія програмного забезпечення та кількість ліцензій: v. 7.1.6, ліцензія GNU* *9. Шафа телекомукаційна CSV Lite Plus 42U – 1 од.* *Рік введення в експлуатацію: 2020* *10. Сервер Intel Core i5-650 3.2 HGz/ 4096 Mb * 2/ IP55/ 1000 Gb *2/ 8400 GS/ 500W / keybord/ mouse – 1 од.* *Рік введення в експлуатацію: 2021* *11. Raspberry Pi 4 Model 4 Gb – 3 од.* *Рік введення в експлуатацію: 2023, 2024* *12. Адаптер Wi-Fi ALFA AWUS 036AC– 2 од.* *Рік введення в експлуатацію: 2021* *13. Проектор Optoma x342e – 1 од.* *Рік введення в експлуатацію: 2021* *14. Екран проекційний – 1 од.* *Рік введення в експлуатацію: 2021* *15. Бездротовий маршрутизатор Mikrotik hAP ac lite tower (RB952Ui-5ac2nD) – 1 од.* *Рік введення в експлуатацію: 2020* *16. Маршрутизатор Mikrotik RB3011UiAS-RM – 2 од.* *Рік введення в експлуатацію: 2020* *17. Маршрутизатор MikroTik hEX (RB750Gr3) – 4 од.* *Рік введення в експлуатацію: 2020* *18. Комутатор Cisco catalyst 2960-S – 3 од.* *Рік введення в експлуатацію: 2021* *19. Комутатор D-Link DES-1024D – 1 од.* *Рік введення в експлуатацію: 2020* *20. Джерело безперебійного живлення APC Smart-UPS C1000 – 1 од.* *Рік введення в експлуатацію: 2020*
ОК 8. Методи побудови та аналізу криптосистем	навчальна дисципліна	*ОК8_МПАК_(2024).pdf*	DZgTdn2QHcQ108q6ZNuVbMkl85l Cngj/qYER/0/tQOI=	*Лабораторія кібербезпеки 1-111* *1. Системний блок Intel Core i3/ RAM 8 GB/ SSD 250 Gb/ HDD 1 Tb/ keybord/ mouse – 12 од.* *Рік введення в експлуатацію: 2021* *2. Монітор Philips 246E 9QPJB/00 – 12 од.* *Рік введення в експлуатацію: 2021* *3. 3. ПЗ Microsoft Windows* *Рік введення в експлуатацію: 2024* *Версія програмного забезпечення та кількість ліцензій: Windows 11 Pro Ukrainian DVD, 12 ліцензій* *4. ПЗ Microsoft Office* *Рік введення в експлуатацію: 2024* *Версія програмного забезпечення та кількість ліцензій: Office Home and Student 2021 ESD,* *12 ліцензій* *5. ПЗ ОС Ubuntu Desktop* *Рік введення в експлуатацію: 2025* *Версія програмного забезпечення та кількість ліцензій: 24.04.2 LTS, ліцензія GNU*

				6. ПЗ ОС Kali-Linux *Рік введення в експлуатацію: 2025* *Версія програмного забезпечення та кількість ліцензій: 2024.4-Kernel 6.11.0, Xfce 4.18.6, ліцензія GNU* *7. ПЗ VirtualBox* *Рік введення в експлуатацію: 2025* *Версія програмного забезпечення та кількість ліцензій: v. 7.1.6, ліцензія GNU* *8. Проектор Optoma x342e – 1 од.* *Рік введення в експлуатацію: 2024* *9. Екран проекційний – 1 од.* *Рік введення в експлуатацію: 2024* *10. Багатофункціональний пошуковий прилад ANDRE – 1 од.* *Рік введення в експлуатацію: 2019* *11. Багатоканальний детектор бездротових протоколів PROTECT 1207i – 1 од.* *Рік введення в експлуатацію: 2020* *12. Детектор прихованих камер WEGAi – 1 од.* *Рік введення в експлуатацію: 2020* *13. Тепловізор Wintact WT3320 – 1 од.* *Рік введення в експлуатацію: 2020* *14. SDR-радіо HackRF One PortaPack H2 – 1 компл.* *Рік введення в експлуатацію: 2023* *15. Тестер радіокомунікаційний Rohde&Schwartz CMD55 – 1 од.* *16. Осцилограф цифровий двоканальний FNIRSI-1013D – 1 од.* *Рік введення в експлуатацію: 2024* *17. Блок живлення лабораторний KORAD KD3005D – 1 од.* *Рік введення в експлуатацію: 2024* *18. Паяльна станція BAKU BK852D – 1 од.* *Рік введення в експлуатацію: 2024* *19. Мультиметр UNI-T UT89X – 1 од.* *Рік введення в експлуатацію: 2024* *20. Тестер кабельний – 1 од.* *Рік введення в експлуатацію: 2024* *21. Аналізатор спектра С4-77 – 1 од.* *22. Інтерферометр INCO NLMZ-4/50 № 1175/81 – 1 од.* *23. Селективний мікровольтметр RFT STV 401 № 07045 – 1 од.* *24. Аналізатор спектра С1-55 – 1 од.* *25. Фліпчарт магнітно-маркер. двохсторонній на колесах 1000*700 – 1 од.* *Рік введення в експлуатацію: 2023*
ОК 10. Переддипломна практика	практика	*ОК10_РП_ПередДипПр_2024.docx.pdf*	Ti73/YEHEQ8PcwGv2KAFaNefxjW47yktpxVHJ4Nkx1Q=	*Лабораторія кібербезпеки 1-106, 105* *1. Комп'ютер персональний 2E Integer Intel i5-11400/H510/16/480F/int/FreeDos/2E-S616/400W – 18 од.* *Рік введення в експлуатацію: 2024* *2. Монітор LCD 23.8" DELL SE2422H D-Sub, HDMI, VA – 18 од.* *Рік введення в експлуатацію: 2024* *3. ПЗ Microsoft Windows* *Рік введення в експлуатацію: 2024* *Версія програмного забезпечення та кількість ліцензій: Windows 11 Pro Ukrainian DVD, 18 ліцензій* *4. ПЗ Microsoft Office* *Рік введення в експлуатацію: 2024* *Версія програмного забезпечення та кількість ліцензій: Office Home and Student 2021 ESD,* *18 ліцензій* *5. ПЗ ОС Ubuntu Desktop* *Рік введення в експлуатацію: 2025* *Версія програмного забезпечення та кількість ліцензій: 24.04.2 LTS, ліцензія GNU* *6. ПЗ ОС Kali-Linux* *Рік введення в експлуатацію: 2025* *Версія програмного забезпечення та кількість ліцензій: 2024.4-Kernel 6.11.0, Xfce 4.18.6, ліцензія GNU* *7. ПЗ VirtualBox* *Рік введення в експлуатацію: 2025* *Версія програмного забезпечення та кількість ліцензій: v. 7.1.6, ліцензія GNU* *8. Проектор Optoma x342e – 1 од.* *Рік введення в експлуатацію: 2024* *9. Екран проекційний – 1 од.* *Рік введення в експлуатацію: 2024* *10. Телевізор 50" TCL LED 4K 60Hz Smart, Android, Black – 1 од.* *Рік введення в експлуатацію: 2024* *8. Стенд навчальний "Охоронні системи TIRAS" – 1 од.* *Рік введення в експлуатацію: 2023* *9. Програмний продукт система захист. інформації "Лоза-1" версія 4 – 2 од.* *Рік введення в експлуатацію: 2021* *10. Програмний продукт "Zillya Антивірус для Бізнесу" версія 1.1.xxxx. у на 2 об ' єкти з правом користування на 5 років – 2 од.* *Рік введення в експлуатацію: 2021* *11. Локатор нелінійний – 1 од.* *12. Прилад акустичного шуму мобільний PIAC-2ГМ № 0110 – 1 од.* *13. Генератор лінійного шуму Базальт-2ГС № 0414 – 1 од.* *14. Випромінювач акустичний PIAC-2ВА. № 0517 – 1 од.* *15. Вібровипромінювач п'єзоелектричний PIAC-2ВП №№ 0630, 0653 – 2 од.* *16. Прилад захисту інформації в аналогових телефонних лініях PIAC-2С/Т № 0019 – 1 од.* *17. Прилад радіочастотного шуму стаціонарний PIAC-1ГС № 0469 – 1 од.* *18. Прилад радіочастотного шуму мобільний PIAC-1ГМ № 0164 – 1 од.* *Серверна кімната 1-106а* *1. Сервер HPE DL160 Gen10 – 2 од.* *Рік введення в експлуатацію: 2024* *Версія програмного забезпечення та кількість ліцензій: Примірник програмного забезпечення HP iLO Adv incl 3yr TS U E-LTU, 2 ліцензії* *2. Джерело безперебійного живлення HPE R1500 G5 INTL UPS – 2 од.* *Рік введення в експлуатацію: 2024* *3. Мережеве сховище Synology RS1221+ – 1 од.* *Рік введення в експлуатацію: 2024* *4. Коммутатор HPE Aruba 2930F-24G + 24xGE+4xGE-SFP, L2/L3, LT Warranty – 2 од.* *Рік введення в експлуатацію: 2024* *5. Маршрутизатор* *MikroTik RB 3011– 1 од.* *Рік введення в експлуатацію: 2020* *6. Ноутбук Dell Vostro 3510/Core i3-1115G4/8GB/256GB SSD/15.6" FHD/Intel UHD/Cam & Mic/WLAN + BT/Backlit Kb/3 Cell/W11Pro/ – 10 од.* *Рік введення в експлуатацію: 2024* *Версія програмного забезпечення та кількість ліцензій: Windows 11 Pro, 10 ліцензій* *7. ПЗ Microsoft Windows* *Рік введення в експлуатацію: 2025*

				Версія програмного забезпечення та кількість ліцензій: Windows Server 2025 Datacenter (16 core), 1 ліцензія *8. ПЗ Microsoft Windows* *Рік введення в експлуатацію: 2025* *Версія програмного забезпечення та кількість ліцензій: Windows Server 2025 Remote Desktop Services User connections,* *50 ліцензій* *9. ПЗ Microsoft Office* *Рік введення в експлуатацію: 2024* *Версія програмного забезпечення та кількість ліцензій: Office Home and Student 2021 ESD,* *10 ліцензій* *10. ПЗ ОС Ubuntu Server* *Рік введення в експлуатацію: 2025* *Версія програмного забезпечення та кількість ліцензій: 24.04.2 LTS, ліцензія GNU* *11. ПЗ Захищена ОС ВВОС* *Рік введення в експлуатацію: 2018* *Версія програмного забезпечення та кількість ліцензій: версія для серверів, 1 ліцензія* *12. ПЗ Захищена ОС ВВОС* *Рік введення в експлуатацію: 2018* *Версія програмного забезпечення та кількість ліцензій: версія для робочих станцій, 12 ліцензій*
ОК 11. Підготовка кваліфікаційної роботи	підсумкова атестація	*ОК11_МВ до ВКР_2025.docx.pdf*	EI/oTw1ZJTU1Oe2OYMxb3U2HK1WUvMf44RuKsp7Y6dE=	*Лабораторія кібербезпеки 1-105* *1. Моноблок All in one HP 205G824AiOBU-R3-5425UIDS / VA / 8GB / 256 SSD / W11p64DowngradeW10p64 / 1yw / 125 BLKkbd / 125mouse / No WLAN / Iron Gray with 5MP WebCam ID / Sea and Rail / – 15 од.* *Рік введення в експлуатацію: 2024* *Версія програмного забезпечення та кількість ліцензій: Windows 11 Pro, 15 ліцензій* *2. ПЗ Microsoft Office* *Рік введення в експлуатацію: 2024* *Версія програмного забезпечення та кількість ліцензій: Office Home and Student 2021 ESD,* *15 ліцензій* *3. ПЗ ОС Ubuntu Desktop* *Рік введення в експлуатацію: 2025* *Версія програмного забезпечення та кількість ліцензій: 24.04.2 LTS, ліцензія GNU* *4. ПЗ ОС Kali-Linux* *Рік введення в експлуатацію: 2025* *Версія програмного забезпечення та кількість ліцензій: 2024.4-Kernel 6.11.0, Xfce 4.18.6, ліцензія GNU* *5. ПЗ VirtualBox* *Рік введення в експлуатацію: 2025* *Версія програмного забезпечення та кількість ліцензій: v. 7.1.6, ліцензія GNU* *6. Проектор Optoma x342e – 1 од.* *Рік введення в експлуатацію: 2024* *7. Екран проекційний – 1 од.* *Рік введення в експлуатацію: 2024* *8. Стенд навчальний "Охоронні системи TIRAS" – 1 од.* *Рік введення в експлуатацію: 2023* *9. Програмний продукт система захист. інформації "Лоза-1" версія 4 – 2 од.* *Рік введення в експлуатацію: 2021* *10. Програмний продукт "Zillya Антивірус для Бізнесу" версія 1.1.xxxx. у на 2 об ' єкти з правом користування на 5 років – 2 од.* *Рік введення в експлуатацію: 2021* *11. Локатор нелінійний – 1 од.* *12. Прилад акустичного шуму мобільний PIAC-2ГМ № 0110 – 1 од.* *13. Генератор лінійного шуму Базальт-2ГС № 0414 – 1 од.* *14. Випромінювач акустичний PIAC-2ВА. № 0517 – 1 од.* *15. Вібровипромінювач п'єзоелектричний PIAC-2ВП №№ 0630, 0653 – 2 од.* *16. Прилад захисту інформації в аналогових телефонних лініях PIAC-2С/Т № 0019 – 1 од.* *17. Прилад радіочастотного шуму стаціонарний PIAC-1ГС № 0469 – 1 од.* *18. Прилад радіочастотного шуму мобільний PIAC-1ГМ № 0164 – 1 од.* *Лабораторія кібербезпеки 1-106* *1. Комп'ютер персональний 2E Integer Intel i5-11400/H510/16/480F/int/FreeDos/2E-S616/400W – 18 од.* *Рік введення в експлуатацію: 2024* *2. Монітор LCD 23.8" DELL SE2422H D-Sub, HDMI, VA – 18 од.* *Рік введення в експлуатацію: 2024* *3. ПЗ Microsoft Windows* *Рік введення в експлуатацію: 2024* *Версія програмного забезпечення та кількість ліцензій: Windows 11 Pro Ukrainian DVD, 18 ліцензій* *4. ПЗ Microsoft Office* *Рік введення в експлуатацію: 2024* *Версія програмного забезпечення та кількість ліцензій: Office Home and Student 2021 ESD,* *18 ліцензій* *5. ПЗ ОС Ubuntu Desktop* *Рік введення в експлуатацію: 2025* *Версія програмного забезпечення та кількість ліцензій: 24.04.2 LTS, ліцензія GNU* *6. ПЗ ОС Kali-Linux* *Рік введення в експлуатацію: 2025* *Версія програмного забезпечення та кількість ліцензій: 2024.4-Kernel 6.11.0, Xfce 4.18.6, ліцензія GNU* *7. ПЗ VirtualBox* *Рік введення в експлуатацію: 2025* *Версія програмного забезпечення та кількість ліцензій: v. 7.1.6, ліцензія GNU* *8. Проектор Optoma x342e – 1 од.* *Рік введення в експлуатацію: 2024* *9. Екран проекційний – 1 од.* *Рік введення в експлуатацію: 2024* *10. Телевізор 50" TCL LED 4K 60Hz Smart, Android, Black – 1 од.* *Рік введення в експлуатацію: 2024* *Серверна кімната 1-106а* *1. Сервер HPE DL160 Gen10 – 2 од.* *Рік введення в експлуатацію: 2024* *Версія програмного забезпечення та кількість ліцензій: Примірник програмного забезпечення HP iLO Adv incl 3yr TS U E-LTU, 2 ліцензії* *2. Джерело безперебійного живлення HPE R1500 G5 INTL UPS – 2 од.* *Рік введення в експлуатацію: 2024* *3. Мережеве сховище Synology RS1221+ – 1 од.* *Рік введення в експлуатацію: 2024* *4. Коммутатор HPE Aruba 2930F-24G + 24xGE+4xGE-SFP, L2/L3, LT Warranty – 2 од.* *Рік введення в експлуатацію: 2024*

				5. Маршрутизатор *MikroTik RB 3011– 1 од.* *Рік введення в експлуатацію: 2020* *6. Ноутбук Dell Vostro 3510/Core i3-1115G4/8GB/256GB SSD/15.6" FHD/Intel UHD/Cam & Mic/WLAN + BT/Backlit Kb/3 Cell/W11Pro/ – 10 од.* *Рік введення в експлуатацію: 2024* *Версія програмного забезпечення та кількість ліцензій: Windows 11 Pro, 10 ліцензій* *7. ПЗ Microsoft Windows* *Рік введення в експлуатацію: 2025* *Версія програмного забезпечення та кількість ліцензій: Windows Server 2025 Datacenter (16 core), 1 ліцензія* *8. ПЗ Microsoft Windows* *Рік введення в експлуатацію: 2025* *Версія програмного забезпечення та кількість ліцензій: Windows Server 2025 Remote Desktop Services User connections,* *50 ліцензій* *9. ПЗ Microsoft Office* *Рік введення в експлуатацію: 2024* *Версія програмного забезпечення та кількість ліцензій: Office Home and Student 2021 ESD,* *10 ліцензій* *10. ПЗ ОС Ubuntu Server* *Рік введення в експлуатацію: 2025* *Версія програмного забезпечення та кількість ліцензій: 24.04.2 LTS, ліцензія GNU* *11. ПЗ Захищена ОС BBOS* *Рік введення в експлуатацію: 2018* *Версія програмного забезпечення та кількість ліцензій: версія для серверів, 1 ліцензія* *12. ПЗ Захищена ОС BBOS* *Рік введення в експлуатацію: 2018* *Версія програмного забезпечення та кількість ліцензій: версія для робочих станцій, 12 ліцензій*
ОК 1. Академічна англійська мова	навчальна дисципліна	*ОК1 _Англійська_2024-2025 н.р..docx.pdf*	e8QQrh+yVEnsjZGuIEE33y+ZgfuHRUUUk54jonFz16k=	*Проектор EPSON-W-31 Екран проекційний DRAPER Ноутбук DEL VOSTRO 3510/Core i3-1115G4/8GB/256GB SSD/ 15.6* FHD/ Intel UHD/ Cam & Mic/WLAN+BT/Backlit Kb/3 C (2023). Акустична система JBL 5 Grey*
ОК 9. Управління мережевою безпекою	навчальна дисципліна	*ОК9_УпрМережБезпекою_Силабус_2024.docx.pdf*	PbZeE8iQ6Di1hJsx44p4Ig6g23guKmzmA6k6e7R//qU=	*Лабораторія кібербезпеки 1-106* *1. Комп'ютер персональний 2E Integer Intel i5-11400/H510/16/480F/int/FreeDos/2E-S616/400W – 18 од.* *Рік введення в експлуатацію: 2024* *2. Монітор LCD 23.8" DELL SE2422H D-Sub, HDMI, VA – 18 од.* *Рік введення в експлуатацію: 2024* *3. ПЗ Microsoft Windows* *Рік введення в експлуатацію: 2024* *Версія програмного забезпечення та кількість ліцензій: Windows 11 Pro Ukrainian DVD, 18 ліцензій* *4. ПЗ Microsoft Office* *Рік введення в експлуатацію: 2024* *Версія програмного забезпечення та кількість ліцензій: Office Home and Student 2021 ESD,* *18 ліцензій* *5. ПЗ ОС Ubuntu Desktop* *Рік введення в експлуатацію: 2025* *Версія програмного забезпечення та кількість ліцензій: 24.04.2 LTS, ліцензія GNU* *6. ПЗ ОС Kali-Linux* *Рік введення в експлуатацію: 2025* *Версія програмного забезпечення та кількість ліцензій: 2024.4-Kernel 6.11.0, Xfce 4.18.6, ліцензія GNU* *7. ПЗ VirtualBox* *Рік введення в експлуатацію: 2025* *Версія програмного забезпечення та кількість ліцензій: v. 7.1.6, ліцензія GNU* *8. Проектор Optoma x342e – 1 од.* *Рік введення в експлуатацію: 2024* *9. Екран проекційний – 1 од.* *Рік введення в експлуатацію: 2024* *10. Телевізор 50" TCL LED 4K 60Hz Smart, Android, Black – 1 од.* *Рік введення в експлуатацію: 2024* *Серверна кімната 1-106а* *1. Сервер HPE DL160 Gen10 – 2 од.* *Рік введення в експлуатацію: 2024* *Версія програмного забезпечення та кількість ліцензій: Примірник програмного забезпечення HP iLO Adv incl 3yr TS U E-LTU, 2 ліцензії* *2. Джерело безперебійного живлення HPE R1500 G5 INTL UPS – 2 од.* *Рік введення в експлуатацію: 2024* *3. Мережеве сховище Synology RS1221+ – 1 од.* *Рік введення в експлуатацію: 2024* *4. Коммутатор HPE Aruba 2930F-24G + 24xGE+4xGE-SFP, L2/L3, LT Warranty – 2 од.* *Рік введення в експлуатацію: 2024* *5. Маршрутизатор* *MikroTik RB 3011– 1 од.* *Рік введення в експлуатацію: 2020* *6. Ноутбук Dell Vostro 3510/Core i3-1115G4/8GB/256GB SSD/15.6" FHD/Intel UHD/Cam & Mic/WLAN + BT/Backlit Kb/3 Cell/W11Pro/ – 10 од.* *Рік введення в експлуатацію: 2024* *Версія програмного забезпечення та кількість ліцензій: Windows 11 Pro, 10 ліцензій* *7. ПЗ Microsoft Windows* *Рік введення в експлуатацію: 2025* *Версія програмного забезпечення та кількість ліцензій: Windows Server 2025 Datacenter (16 core), 1 ліцензія* *8. ПЗ Microsoft Windows* *Рік введення в експлуатацію: 2025* *Версія програмного забезпечення та кількість ліцензій: Windows Server 2025 Remote Desktop Services User connections,* *50 ліцензій* *9. ПЗ Microsoft Office* *Рік введення в експлуатацію: 2024* *Версія програмного забезпечення та кількість ліцензій: Office Home and Student 2021 ESD,* *10 ліцензій* *10. ПЗ ОС Ubuntu Server* *Рік введення в експлуатацію: 2025* *Версія програмного забезпечення та кількість ліцензій: 24.04.2 LTS, ліцензія GNU* *11. ПЗ Захищена ОС BBOS* *Рік введення в експлуатацію: 2018* *Версія програмного забезпечення та кількість ліцензій: версія для серверів, 1 ліцензія* *12. ПЗ Захищена ОС BBOS* *Рік введення в експлуатацію: 2018* *Версія програмного забезпечення та кількість ліцензій: версія для робочих станцій, 12 ліцензій*

ОК 3. Аудит та управління інцидентами інформаційної безпеки	навчальна дисципліна	*ОК 3_Силабус(24) Аудит та управління інцидентами інформаційної безпеки.docx.pdf*	CNeBf9w3UfoapQAfeIxet2onNvz2QLerdkSK9OPvQGw=	*Лабораторія кібербезпеки 1-106* *1. Комп'ютер персональний 2E Integer Intel i5-11400/H510/16/480F/int/FreeDos/2E-S616/400W – 18 од.* *Рік введення в експлуатацію: 2024* *2. Монітор LCD 23.8" DELL SE2422H D-Sub, HDMI, VA – 18 од.* *Рік введення в експлуатацію: 2024* *3. ПЗ Microsoft Windows* *Рік введення в експлуатацію: 2024* *Версія програмного забезпечення та кількість ліцензій: Windows 11 Pro Ukrainian DVD, 18 ліцензій* *4. ПЗ Microsoft Office* *Рік введення в експлуатацію: 2024* *Версія програмного забезпечення та кількість ліцензій: Office Home and Student 2021 ESD,* *18 ліцензій* *5. ПЗ ОС Ubuntu Desktop* *Рік введення в експлуатацію: 2025* *Версія програмного забезпечення та кількість ліцензій: 24.04.2 LTS, ліцензія GNU* *6. ПЗ ОС Kali-Linux* *Рік введення в експлуатацію: 2025* *Версія програмного забезпечення та кількість ліцензій: 2024.4-Kernel 6.11.0, Xfce 4.18.6, ліцензія GNU* *7. ПЗ VirtualBox* *Рік введення в експлуатацію: 2025* *Версія програмного забезпечення та кількість ліцензій: v. 7.1.6, ліцензія GNU* *8. Проектор Optoma x342e – 1 од.* *Рік введення в експлуатацію: 2024* *9. Екран проекційний – 1 од.* *Рік введення в експлуатацію: 2024* *10. Телевізор 50" TCL LED 4K 60Hz Smart, Android, Black – 1 од.* *Рік введення в експлуатацію: 2024* *Серверна кімната 1-106а* *1. Сервер HPE DL160 Gen10 – 2 од.* *Рік введення в експлуатацію: 2024* *Версія програмного забезпечення та кількість ліцензій: Примірник програмного забезпечення HP iLO Adv incl 3yr TS U E-LTU, 2 ліцензії* *2. Джерело безперебійного живлення HPE R1500 G5 INTL UPS – 2 од.* *Рік введення в експлуатацію: 2024* *3. Мережеве сховище Synology RS1221+ – 1 од.* *Рік введення в експлуатацію: 2024* *4. Коммутатор HPE Aruba 2930F-24G + 24xGE+4xGE-SFP, L2/L3, LT Warranty – 2 од.* *Рік введення в експлуатацію: 2024* *5. Маршрутизатор* *MikroTik RB 3011– 1 од.* *Рік введення в експлуатацію: 2020* *6. Ноутбук Dell Vostro 3510/Core i3-1115G4/8GB/256GB SSD/15.6" FHD/Intel UHD/Cam & Mic/WLAN + BT/Backlit Kb/3 Cell/W11Pro/ – 10 од.* *Рік введення в експлуатацію: 2024* *Версія програмного забезпечення та кількість ліцензій: Windows 11 Pro, 10 ліцензій* *7. ПЗ Microsoft Windows* *Рік введення в експлуатацію: 2025* *Версія програмного забезпечення та кількість ліцензій: Windows Server 2025 Datacenter (16 core), 1 ліцензія* *8. ПЗ Microsoft Windows* *Рік введення в експлуатацію: 2025* *Версія програмного забезпечення та кількість ліцензій: Windows Server 2025 Remote Desktop Services User connections,* *50 ліцензій* *9. ПЗ Microsoft Office* *Рік введення в експлуатацію: 2024* *Версія програмного забезпечення та кількість ліцензій: Office Home and Student 2021 ESD,* *10 ліцензій* *10. ПЗ ОС Ubuntu Server* *Рік введення в експлуатацію: 2025* *Версія програмного забезпечення та кількість ліцензій: 24.04.2 LTS, ліцензія GNU* *11. ПЗ Захищена ОС BBOS* *Рік введення в експлуатацію: 2018* *Версія програмного забезпечення та кількість ліцензій: версія для серверів, 1 ліцензія* *12. ПЗ Захищена ОС BBOS* *Рік введення в експлуатацію: 2018* *Версія програмного забезпечення та кількість ліцензій: версія для робочих станцій, 12 ліцензій*
ОК 2. Цивільний захист та охорона праців галузі	навчальна дисципліна	*ОК 2 Цив захист-24.docx (1).pdf*	ov2yQmhu+GwvlEspgm3aXB69iQ/ZtYJpyMebtVd3sck=	*Спеціалізований кабінет-лабораторія, І–419. Мультимедійне обладнання: Мультимедійний проектор та екран – 1; IP камера Seven IP 7232P (2019 р.) з безкоштовним ПЗ Shinobi для проведення занять в змішаній та дистанційній формі. Наочний матеріал - 7 лабораторних стендів: по електробезпеці; дослідницькі стенди параметрів мікроклімату, стану повітря, рівня шуму та вібрації, штучної та природної вентиляції, електромагнітних полів та випромінювання, оцінки радіохімічного стану та протипожежної безпеки; стенд пожежної автоматики. Індивідуальні засоби захисту – 20 комплектів.*

* 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 освітнім компонентам

ID викладача	ПІБ	Посада	Структурний підрозділ	Кваліфікація викладача	Стаж	Навчальні дисципліни, що їх викладає викладач на ОП	Обгрунтування відповідності освітньому компоненту (кваліфікація, професійний досвід, наукові публікації)
229875	Ткач Юлія Миколаївна	Завідувачка кафедри / Професор, Основне місце роботи	ННІ Електронних та інформаційних технологій	Диплом спеціаліста, Чернігівський державний педагогічний університет імені Т.Г. Шевченка, рік закінчення: 2001, спеціальність: 010103 Педагогіка і методика середньої освіти. Математика та основи економіки, Диплом магістра, Чернігівський національний технологічний університет, рік	23	ОК 4. Методологія та організація наукових досліджень	Підвищення кваліфікації: Державний університет інформаційно-комунікаційних технологій (31.03.2025 – 16.05.2025), Довідка №26/903 від 20.05.2025. Технічний експерт з питань систем керування інформаційною безпекою вимогам ДСТУ ISO/IEC 27001:2023 (ISO/IEC 27001:2022, IDT) свідоцтво №E35-01/25 Distributed Lab Cryptography: A Modern Approach Інструктор Cisco "CCNA CyberOps, Network Security

				закінчення: 2017, спеціальність: 8.18010014 управління фінансово-економічною безпекою, Диплом магістра, Національний авіаційний університет, рік закінчення: 2020, спеціальність: 125 Кібербезпека, Диплом доктора наук ДД 007402, виданий 16.05.2018, Диплом кандидата наук ДК 059130, виданий 26.05.2010, Атестат доцента 12ДЦ 030905, виданий 17.02.2012, Атестат професора АП 002293, виданий 26.11.2020			П1. Scopus https://www.scopus.com/authid/detail.uri?authorId=57193026076 https://orcid.org/0000-0002-8565-0525 1. Zaitsev Sergei , Vasylenko Vladyslav, Trofymchuk Oleksandr, Tkach Yuliia (2020) Retransmission Request Method for Modern Mobile Networks. In: Palagin A., Anisimov A., Morozov A., Shkarlet S. (eds) Mathematical Modeling and Simulation of Systems. MODS 2019. Advances in Intelligent Systems and Computing, vol 1019. Springer, Cham. pp. 113-121 https://link.springer.com/chapter/10.1007/978-3-030-25741-5_12 2. Akhmetov B., Lakhno V., Tkach Y., Adranova A., Zhilkishbayeva G. (2020) PROBLEMS OF DEVELOPMENT OF A CLOUD-ORIENTED EDUCATIONAL ENVIRONMENT OF THE UNIVERSITY // International Journal of Advanced Trends in Computer Science and Engineering. Volume 9. No.2. March-April 2020 Available Online at http://www.warse.org/IJATCSE/static/pdf/file/ijatcse196922020.pdf https://doi.org/10.30534/ijatcse/2020/196922020 3. Zaitsev, S.V., Sokorinskaya, N.V., Vasylenko, V.M., Trofimchuk, A.N., Tkach, Y.N. Optimization of Turbo Code Encoding/Decoding Processes for Development of 5G Mobile Communication Systems (2021) Radioelectronics and Communications Systems, 64 (8), pp. 440-450. Цитирован(ы) 1 раз. https://www.scopus.com/inward/record.uri?eid=2-s2.0-85117933910&doi=10.3103%2fS0735272721080045&partnerID=40&md 4. Zaitsev, S., Vasylenko, V., Tkach, Y., Posternak, Y., Lytvyn, S. Adaptive Selection of Turbo Code Parameters in Wireless Data Transmission Systems (2022) Lecture Notes in Networks and Systems, 344, pp. 253-262. https://www.scopus.com/inward/record.uri?eid=2-s2.0-85126223107&doi=10.1007%2f978-3-030-89902-8_20&partnerID=40&m 5. Tkach, Y, Sinenko M, Shelest M, Mekhed D, Kosareva D (2023) Construction of the Assessment Model of the Information Security System of the Enterprise. 17th International Conference on Mathematical Modeling and Simulation of Systems, MODS 2022, 14 November 2022 до 16 November 2022. Chernihiv – 2023. - P. 171 – 181. https://www.scopus.com/record/display.uri?eid=2-s2.0-85164030510&origin=resultslist&sort=plf-f&src=s&sid=4e5a0a770893702998b0058673121367&sot=b&sdt=b&s=TITLE-ABS-KEY%28Construction+of+the+Assessment+Model+of+the+Information+Security+System+of+the+Enterprise%29&sl=104&sessionSearchId=4e5a0a770893702998b0058673121367 6. Tkach, Y, Vasylieva O, Shyian A, Diuba I (2023) Method of effective counteraction against negative information-psychological impact on the regional community by using social networks . The 18th International conference Mathematical Modeling and Simulation Systems (MODS2023) November 13-15, 2023. Chernihiv – 2023. 7. Semendiai, S., Tkach, Y., Shelest, M., Ziubina, R., Veselska, O. (2023) Improving the Efficiency of UAV Communication Channels in the Context of Electronic Warfare. International Journal of Electronics and Telecommunications, 2023, 69(4), P. 727–732 https://www.scopus.com/record/display.uri?eid=2-s2.0-85178995614&origin=resultslist 8. Vasylenko, V., Zaitsev, S., Tkach, Y., Ziubina, R., Veselska, O. (2024) Method of assessing the information reliability of in 5G wireless transmission systems. International Journal of Electronics and Telecommunications, 2024, 70(1), P. 205–210 https://www.scopus.com/record/display.uri?eid=2-s2.0-85189459595&origin=resultslist 9. Zaitsev, S., Rohovenko, A., Ryndych, Y., Tkach, Y., Horlynskyi, B., Rudenok, O. (2025). The Method of Multi-vector Routing in Mobile IoT Networks Under the Influence of Strong Interference. In: Dovgyi, S., Siemens, E., Globa, L., Kopiika, O., Stryzhak, O. (eds) Applied Innovations in Information and Communication Technology. ICAIIT 2024. Lecture Notes in Networks and Systems, vol 1338. Springer, Cham. pp. 3-16 https://link.springer.com/chapter/10.1007/978-3-031-89296-7_1 Фахові: 1. Хорошко В.О. БАГАТОКРИТЕРІАЛЬНА ОЦІНКА ЕФЕКТИВНОСТІ ПРОЕКТІВ ІЗ ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ / Хорошко В.О., Шелест М.Є., Ткач Ю.М. // Технічні науки та технології :

							науковий журнал / Чернігів. нац. технол. ун-т. – Чернігів : ЧНТУ, 2020. – № 1 (19). – С. 114-124 2. Ткач Ю.М. TELEGRAM OPEN NETWORK. КОМПЛЕКСНИЙ АНАЛІЗ ІННОВАЦІЙНОГО ПРОЕКТУ ТА ЙОГО СКЛАДОВИХ / Ткач Ю.М., Бригинець А.А. // КІБЕРБЕЗПЕКА: освіта, наука, техніка / Київський університет імені Бориса Гринченка. – Київ, 2020. – № 4 (8). – С. 61-72 https://www.csecurity.kubg.edu.ua/index.php/journal/article/view/157 ISSN: 2663-4023 DOI: https://doi.org/10.28925/2663-4023.2020.8.6172 3. Синенко М.А., Ткач Ю.М. Математична модель методів активного захисту інформації // Технічні науки та технології : науковий журнал / Чернігів. нац. технол. ун-т. – Чернігів : ЧНТУ, 2020. – № 2 (20). – С. 109-115. 4. Ткач Ю., Мехед Д., Мехед К., Черниш Л. Організація наукових досліджень в умовах пандемії та карантину // Технічні науки та технології : науковий журнал / Чернігів. нац. технол. ун-т. – Чернігів : ЧНТУ, 2020. – № 2 (20). – С. 197-203 5. Ткач Ю., Шелест М., Черниш Л., Литвин С., Бригинець А.Аналіз систем підтримки аудиту інформаційної безпеки/ Технічні науки та технології : науковий журнал / Чернігів. нац. технол. ун-т. – Чернігів : ЧНТУ, 2020. – № 2 (20). – С. 203-210 6. Шелест М., Ткач Ю., Семендяй С., Синенко М., Черниш Л. Дослідження стійкості алгоритму автентифікованого шифрування на базі sponge-функції // Технічні науки та технології : науковий журнал / Чернігів. нац. технол. ун-т. – Чернігів : ЧНТУ, 2020. – № 2 (20). – С. 210-218 7. Семендяй С., Шелест М., Ткач Ю., Черниш Л. Етичний хакінг у бізнес-компаніях та виявлення вразливостей в інформаційних системах державних органів України / Технічні науки та технології : науковий журнал / Чернігів. нац. технол. ун-т. – Чернігів : ЧНТУ, 2020. – № 2 (20). – С. 237-241 8. Ткач Ю.М. Тенденції розвитку сучасного кіберпростору та його захищеності в умовах інформаційного протиборства // Безпека інформації. – 2020. – Т. 26 (2). – С. 74–80. 9. Ткач Ю.М. Оптимізація вибору функціонального профілю захищеності інформаційної системи держави // Інформатика та математичні методи в моделюванні. – 2020. – Т.10 (1–2). – С. 68–74. 10. Ткач Ю.М. Концептуальна модель безпеки кіберпростору // Технічні науки та технології : науковий журнал / Національний університет «Чернігівська політехніка». – Чернігів : НУ «Чернігівська політехніка», 2020. – № 4(22). – С. 96–108. 11. Ткач Ю.М. Модель захисту кіберпростору Cybersec // Захист інформації. – 2020. – Т. 22, № 4. – С. 206–210. 12. Ткач Ю.М. Моделі систем захисту інформаційної сфери держави // Сучасна спеціальна техніка. – 2020. – № 2 (61). – С. 59–66. 13. Ткач Ю.М. Кількісно-якісна оцінка та визначення рівня кібербезпеки інформаційних систем держави // Ткач Ю.М., Хорошко В.О., Хохлачова Ю.Є., Пискун І.В. Аясрах Ахмад Расмі Алі, Аль-Даваш Аблуллах Фоуад // Науковий журнал «Безпека інформації», 2020 вип. 26. Т. 3. – С. 131–136. 14. Ткач Ю.М. Математична модель методів активного захисту інформації / Синенко М.А., Ткач Ю.М. // Технічні науки та технології : науковий журнал / Чернігів. нац. технол. ун-т. – Чернігів : ЧНТУ, 2020. – № 2 (20). – С. 109–115. 15. Хорошко В., Виявлення та оцінювання кібератак в інформаційних мережах із випадковим моментом появи. / Шелест М., Ткач Ю. //Технічні науки та технології. 2021. № 1 (23). С. 96–102. 16. Опірський І., Виявлення кібератак в інформаційних мережах / Ткач Ю., Хорошко В. // Інформатика та математичні методи в моделюванні. 2020. Т. 10, № 3-4. С. 177–189. 17. Ткач Ю.М. МЕТОД ВИБОРУ ФУНКЦІОНАЛЬНОГО ПРОФІЛЮ ЗАХИЩЕНОСТІ // Informatics & Mathematical Methods in Simulation. – Vol. 10 (2020), № 1-2, pp. 68–74. 18. Ткач, Ю. ., Шелест, М. ., Синенко, М., & Петренко, Т. (2023). Історія виникнення клептографії та її місце в безпеці інформації. Технічні науки та технології, (3 (33), 150–161. https://doi.org/10.25140/2411-5363-2023-3(33)-150-161 П3. Навчальні посібники: 1. Козюра В.Д. Інформатика та комп'ютерна техніка. Частина І.

							Основи загальноїінформатики: /навчальний посібник / В.Д. Козюра, Ю.М. Ткач, В.О. Хорошко,В.В. Кузовков, С.В. Зайцев, М.Є. Шелест, О.В. Гаркун. Ніжин: ФОП Лук'яненко В.В., ТПК «Орхідея», 2022., 464 с. ISBN 978-617-7609-84-0 2. Інформатика та комп'ютерна техніка: Спеціальна Інформатика: Навчальний посібник., Т. ІІ., Ч. ІІ / В.Д. Козюра, Ю.М. Ткач, В.О. Хорошко, М.Є. Шелест, М.А. Синенко: Ніжин, ТПК «Орхідея», ФОП Лук'яненко В. В,,2022.,352 с. ISBN 978-617-7609-89-5 3. Козюра В.Д. Технології програмування: навч.посібник. Том 1. Основи алгоритмізації та програмування/ В.Д. Козюра, Ю.М. Ткач, В.О. Хорошко,, Ю.Є. Хохлачова, Д.Б. Мехед. Ніжин: ФОП Лук'яненко В.В., ТПК «Орхідея», 2021.,310 с. ISBN 978-617-7609-85-7 4. Козюра В.Д. Технології програмування: навчальний посібник. Том 2. Сучасні технології програмування / Козюра В.Д., Ткач Ю.М., Хорошко В.О., Кузовков В.В., Хохлачова Ю.Є., Семендяй С.М. Ніжин: ФОП Лук'яненко В.В., ТПК «Орхідея», 2022., 300 с. ISBN 978-617-7609-86-4 5. Інформатика та комп'ютерна техніка. Частина ІІ. Спеціальна інформантика. Том 1: навч. посібник / Козюра В. Д., Ткач Ю. М., Хорошко В.О., Шелест М.Є., Петренко Т.А. Ніжин: ФОП Лук'яненко В.В., ТПК «Орхідея», 2022., 288 с. ISBN 978-617-7609-80-2 6. Спеціалізовані програмні засоби наукових досліджень: навчальний посібник / М.М. Браіловський, В.Д. КОЗЮРА, В.В. Кузавков, Ю.В. Пепа, Ю.М. Ткач, В.О. Хорошко, Ю.Є. Хохлачова – К.: ФОП Ямчинський О.В.,2021. – 204 с. 7. Інформатика та комп'ютерна техніка. Частина І. Основи загальної інформатики: /навчальний посібник / В.Д.Козюра, Ю.М. Ткач, В.О. Хорошко, В.В. Кузовков, С.В. Зайцев, М.Є. Шелест, О.В. Гаркун. Ніжин ФОП Лук'яненко В.В., ТПК «Орхідея», 2023. – 464 с. ISBN 978-617-7609-84-0 8. Інформатика та комп'ютерна техніка. Частина ІІ. Спеціальна інформантика. Том 1: навч. посібник / Козюра В. Д., Ткач Ю. М., Хорошко В.О., Шелест М.Є., Петренко Т.А. Ніжин: ФОП Лук'яненко В.В., ТПК «Орхідея», 2023., 288 с. ISBN 978-617-7609-80-2 9. Інформатика та комп'ютерна техніка: Спеціальна інформатика: Навчальний посібник., Т. ІІ., Ч. ІІ / В.Д. Козюра, Ю.М. Ткач, В.О. Хорошко, М.Є. Шелест, М.А. Синенко: Ніжин: ТПК "Орхідея", ФОП Лук'яненко В. В., 2023., 352 с. ISBN 978-617-7609-89-5 10. Козюра В.Д. Технології програмування: навч. посібник. Том 1. Основи алгоритмізації та програмування/ В.Д. Козюра, Ю.М. Ткач, В.О. Хорошко, Ю.Є. Хохлачова, Д.Б. Мехед. Ніжин: ФОП Лук'яненко В. В., ТПК "Орхідея", 2023. – 310 с. ISBN 978-617-7609-85-7 11. Козюра В.Д. Технології програмування: навч. посібник. Том 2. Сучасні технології програмування/ Козюра В.Д., Ткач Ю.М., Хорошко В.О., Кузовков В.В. Хохлачова Ю.Є., Семендяй С.М.. Ніжин: ФОП Лук'яненко В. В., ТПК "Орхідея", 2023. – 300 с. ISBN 978-617-7609-85-4 12. Дискретна математика: Навч. посіб. / Козюра В.Д., Ткач Ю.М., Мехед Д.Б., 2024. – 233 с. 13. Збірник задач з дискретної математики: Практикум / Козюра В.Д., Ткач Ю.М., Синенко М.А. – 2024. – 231 с Підручник: 1. Козюра В.Д., Хорошко В.О., Шелест М.Є., Ткач Ю.М., Балюнов О.О. Захист інформації в комп'ютерних системах : пі-дручник. – Ніжин : ФОП Лук'яненко В.В., ТПК «Орхидея», 2020. – 236 с. Монографія: 1. Захист кіберпростору: монографія / Ю.М. Ткач, М.Є. Шелест, В.О. Хорошко, І.М.Дюба, Д.В.Кальченко, 2024. – 198 с. П4. 1. Кібербезпека. Методичні вказівки до виконання кваліфікаційної роботи здобувачів вищої освіти другого (магістерського) рівня вищої освіти спеціальності 125-Кібербезпека та захист інформації/F5 – Кібербезпека та захист інформації // Укл.: Т.А. Петренко, Ю.М. Ткач, М.Є.Шелест, С.М.Семендяй. - Чернігів: НУ «Чернігівська політехніка», 2025 – 42с. 5. Ліцензування та сертифікація у сфері захисту інформації: Методичні вказівки до виконання лабораторних робіт / М.М. Браіловський, С.О. Клімович, Ю.М. Ткач, В.О. Хорошко, Ю.Є. Хохлачова. К.: ФОП Ямчинський О.В., 2023.70с. 6. Основи криптографічного захисту

							інформації. Методичні вказівки до виконання курсової роботи для здобувачів першого (бакалаврського) рівня вищої освіти освітньо-професійної програми «Кібербезпека» спеціальності 125 Кібербезпека та захист інформації. / уклад.: М.А. Синенко, Ю.М. Ткач, М.Є. Шелест, С.М. Семендяй. – Чернігів: НУ «Чернігівська політехніка», 2024 – 40 с. 7. Кібербезпека та захист інформації. Методичні вказівки з ознайомчої практики для здобувачів першого (бакалаврського) рівня вищої освіти освітньо-професійної програми «Кібербезпека» спеціальності 125 Кібербезпека та захист інформації. / уклад.: Т.А. Петренко, Ю.М. Ткач, М.Є. Шелест, Д.В. Кальченко, І.М. Дюба. – Чернігів: НУ «Чернігівська політехніка», 2024 – 25 с. 8. Кібербезпека та захист інформації. Методичні вказівки з навчальної практики для здобувачів першого (бакалаврського) рівня вищої освіти освітньо-професійної програми «Кібербезпека» спеціальності 125 Кібербезпека та захист інформації. / уклад.: Т.А. Петренко, Ю.М. Ткач, М.Є. Шелест, Д.В. Кальченко, І.М. Дюба. – Чернігів: НУ «Чернігівська політехніка», 2024 – 23 с 9. Кібербезпека та захист інформації. Методичні вказівки з технологічної практики для здобувачів першого (бакалаврського) рівня вищої освіти освітньо-професійної програми «Кібербезпека» спеціальності 125 Кібербезпека та захист інформації. / уклад.: Т.А. Петренко, Ю.М. Ткач, М.Є. Шелест, С.М. Семендяй. – Чернігів: НУ «Чернігівська політехніка», 2024 – 26 с 10. Кібербезпека та захист інформації. Методичні вказівки з виробничої практики для здобувачів першого (бакалаврського) рівня вищої освіти освітньо-професійної програми «Кібербезпека» спеціальності 125 Кібербезпека та захист інформації. / уклад.: Т.А. Петренко, Ю.М. Ткач, М.Є. Шелест, С.М. Семендяй. – Чернігів: НУ «Чернігівська політехніка», 2024 – 25 с 11. Прогнозування та моделювання. Методичні вказівки до виконання лабораторних робіт для здобувачів першого (бакалаврського) рівня вищої освіти освітньо-професійної програми «Кібербезпека» спеціальності 125 Кібербезпека та захист інформації. / уклад.: Ю.М. Ткач, М.А. Синенко, Д.Б. Мехед, С.П. Корнієнко. – Чернігів: НУ «Чернігівська політехніка», 2024 – 93 с. 12. Основи наукового дослідження. Методичні вказівки до виконання розрахунково-графічної роботи для здобувачів першого (бакалаврського) рівня вищої освіти освітньо-професійної програми «Кібербезпека» спеціальності 125 Кібербезпека та захист інформації. / уклад.: С.П. Корнієнко, М.А. Синенко, Ю.М. Ткач, Д.Б. Мехед. – Чернігів: НУ «Чернігівська політехніка», 2024 – 36 с. 13. Організаційне забезпечення захисту інформації. Методичні вказівки до практичних занять для здобувачів першого (бакалаврського) рівня вищої освіти освітньо-професійної програми «Кібербезпека» спеціальності 125 Кібербезпека та захист інформації. / уклад.: С.П. Корнієнко, М.А. Синенко, Ю.М. Ткач, Д.Б. Мехед. – Чернігів: НУ «Чернігівська політехніка», 2024 – 39 с. 14. Комплексні системи захисту інформації. Методичні вказівки до курсового проектування для здобувачів першого (бакалаврського) рівня вищої освіти освітньо-професійної програми «Кібербезпека» спеціальності 125 Кібербезпека та захист інформації. / уклад.: С.М. Семендяй, Ю.М. Ткач, М.Є. Шелест. – Чернігів: НУ «Чернігівська політехніка», 2024 – 100 с 15. Інциденти інформаційної безпеки. Методичні вказівки до виконання лабораторних робіт для здобувачів першого (бакалаврського) рівня вищої освіти освітньо-професійної програми «Кібербезпека» спеціальності 125 Кібербезпека та захист інформації. / уклад.: А.Г. Гребенник, Ю.М. Ткач, С.М. Семендяй. – Чернігів: НУ «Чернігівська політехніка», 2024 – 62 с 16. Математичні основи криптографії. Методичні вказівки до виконання розрахунково-графічної роботи для здобувачів першого (бакалаврського) рівня вищої освіти освітньо-професійної програми «Кібербезпека» спеціальності 125 Кібербезпека та захист інформації. / уклад.: М.А. Синенко, Ю.М. Ткач, Д.Б. Мехед, І.М. Головатенко. – Чернігів: НУ «Чернігівська політехніка», 2024 – 40 с. 17. Комп'ютерна графіка. Методичні вказівки до виконання розрахунково-

							графічної роботи для здобувачів першого (бакалаврського) рівня вищої освіти освітньо-професійної програми «Кібербезпека» спеціальності 125 Кібербезпека та захист інформації. / уклад.: Ю.М. Ткач, Д.Б. Мехед, Б.В. Кальченко, В.О. Нороха. – Чернігів: НУ «Чернігівська політехніка», 2024 – 24 с. 18. Стандартизація, сертифікація засобів та комплексів захисту інформації. Методичні вказівки до виконання лабораторних робіт для здобувачів другого (магістерського) рівня вищої освіти освітньо-професійної програми «Кібербезпека» спеціальності 125 Кібербезпека та захист інформації. / уклад.: В.О. Хорошко, Ю.М. Ткач, М.Є. Шелест. – Чернігів: НУ «Чернігівська політехніка», 2024 – 94 с. 19. Інформаційна безпека держави. Методичні вказівки до практичних занять для здобувачів першого (бакалаврського) рівня вищої освіти освітньо-професійної програми «Кібербезпека» спеціальності 125 Кібербезпека та захист інформації. / уклад.: М.О. Ларченко, Ю.М. Ткач.– Чернігів: НУ «Чернігівська політехніка», 2024 – 40 с. 20. Системи охорони державної таємниці. Методичні вказівки до практичних занять для здобувачів першого (бакалаврського) рівня вищої освіти освітньо-професійної програми «Кібербезпека» спеціальності 125 Кібербезпека та захист інформації. / уклад.: М.О. Ларченко, Ю.М. Ткач. – Чернігів: НУ «Чернігівська політехніка», 2024 – 26 с. 21. Електронний документообіг. Методичні вказівки до практичних занять для здобувачів першого (бакалаврського) рівня вищої освіти освітньо-професійної програми «Кібербезпека» спеціальності 125 Кібербезпека та захист інформації. / уклад.: М.О. Ларченко, Ю.М. Ткач. – Чернігів: НУ «Чернігівська політехніка», 2024 – 58 с. 22. Нормативно-правове забезпечення інформаційної безпеки. Методичні рекомендації до виконання практичних робіт для здобувачів освітнього ступеня «Бакалавр» спеціальності 125 «Кібербезпека та захист інформації». / уклад: Браіловський М.М., Лаптєв О.А., Наконечний В.С., Ткач Ю.М., Хорошко В.О. – Київ: Київський національний університет імені Тараса Шевченка, 2025 – 59 с. П5. Кандидат технічних наук. 21.05.01-Інформаційна безпека держави. Диплом кандидата наук: Національний авіаційний університет – захист дисертації, диплом кандидата наук від 30.11.2021, ДК № 063487 П8. Керівник наукової теми: Методологія побудови захищеного кіберпростору. Номер 0124U004485. Терміни виконання 10.24-10.27 Член редакційної колегії наукового видання «Актуальні питання природничо-математичної освіти». Керівник ДБТ, держфінансування П9. З 2024-2025 н.р. член ГЕР. 12 галузь – Інформаційні технології Участь в роботі експертних груп від НАЗЯВО у якості голови експертної групи та члена групи: 1) Наказ № 1275-Е про призначення експертної групи від 10 вересня 2020 року та наказ про внесення змін до наказів від 12 жовтня 2020 року №1507-Е . Державний університет телекомунікацій за спеціальності «125 Кібербезпека» освітньої програми «Кібербезпека» (ID у ЄДЕБО 36680) за третім рівнем вищої освіти (справа №167/АС-20) з 02.11 по 04.11.2020 року. 2) Наказ про призначення експертної групи від 02 вересня 2020 року № 1172-Е. Київський університет імені Бориса Грінченка для проведення акредитаційної експертизи за спеціальності «011 Науки про освіту» освітньої програми «Освітні, педагогічні науки» (ID у ЄДЕБО 38800) за третім рівнем вищої освіти (справа №834/АС-20) з 21 по 23 вересня 2020 року включно. 3) Наказ про призначення експертної групи від 05 березня 2020 року № 256-Е. Житомирський державний університет імені Івана Франка за спеціальністю 014 «Середня освіта» освітньої програми «Середня освіта (Математика)» (ID у ЄДЕБО 30633) за першим рівнем вищої освіти (справа № 261/АС-20) з 25 березня по 27 березня 2020 року включно. 4) Наказ про призначення експертної групи від 10 березня 2021 року № 516-Е. Державний університет «Житомирська політехніка» за спеціальністю «125 Кібербезпека» освітньої програми «Кібербезпека» (ID у ЄДЕБО 18949) за першим

							рівнем вищої освіти (справа №491/АС-21) у роботі експертної групи з 24 по 26 березня 2021 року включно. 5) Наказ про призначення експертної групи від 13.05.21 №1051-Е. Інститут інформаційних технологій і засобів навчання Національної академії педагогічних наук України 6) наказ про призначення експертної групи від 22 грудня 2021 року № 2253-Е. Харківський національний університет радіоелектроніки 7) наказ про призначення експертної групи від 07 жовтня 2022 року № 521-Е. Національний технічний університет «Дніпровська політехніка» 8) наказ про призначення експертної групи від 15 лютого 2023 року № 272-Е. Національний аерокосмічний університет ім. М.Є. Жуковського «Харківський авіаційний інститут» 9) наказ про призначення експертної групи від 05 квітня 2023 року № 721-Е. Київський національний університет імені Тараса Шевченка 10) наказ про призначення експертної групи від 06 вересня 2023 року №865-Е. Національний Університет «Харківський політехнічний інститут» спеціальність 125 «Кібербезпека» освітньої програми «Кібербезпека» (ID у ЄДЕБО 54114) за другим рівнем вищої освіти (справа №1812/АС-23) 11) наказ про призначення експертної групи від 12 жовтня 2023 року №1249-Е. Вінницький національний технічний університет спеціальність 125 «Кібербезпека» освітньої програми «Кібербезпека інформаційних технологій та систем» (ID у ЄДЕБО 53941) за другим рівнем вищої освіти (справа №2309/АС-23) 12) наказ про призначення експертної групи від 07 березня 2025 року №497-Е. Мелітопольський державний педагогічний університет імені Богдана Хмельницького спеціальність 015 «Професійна освіта» освітньої програми «Професійна освіта. Комп'ютерні технології» (ID у ЄДЕБО 47179) за першим рівнем вищої освіти (справа №677/АС-25) П11. ТОВ «Інформаційна безпека», укладено договір про співпрацю. П12. 1. Бакрі М. РЕАЛІЗАЦІЯ СТАНДАРТУ ШИФРУВАННЯ SES ДЛЯ ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ ЦИФРОВОЇ ІНФРА-СТРУКТУРИ / Бакрі М., Гері Лох Чі Віяй, Юрченко А.В., Ткач Ю.М., Шелест М.Є. //Безпека ресурсів інформаційних систем : збірник тез І Міжнародної науково-практичної конференції (м. Чернігів 16-17 квітня 2020 р.). – Чернігів : НУЧП, 2020. – С.47-50. 2. Лисиця Т.А. SPEAR PHISHING АТАКА: ОСОБЛИВОСТІ ТА СПОСОБИ ЗАХИСТУ/ Лисиця Т.А., Яковлєв О.О., Ткач Ю.М.// Безпека ресурсів інформаційних систем : збірник тез І Міжнародної науково-практичної конференції (м. Чернігів 16-17 квітня 2020 р.). – Чернігів : НУЧП, 2020. – С.106-110 3. Полевод О.М.OPEN SOURCE INTELLIGENCE ЯК ПРОВІДНИЙ НАПРЯМ КОНКУРЕНТНОЇ РОЗВІДКИ/ Полевод О.М., Трощилов М.О., Ткач Ю.М. // Безпека ресурсів інформаційних систем : збірник тез І Міжнародної науково-практичної конференції (м. Чернігів 16-17 квітня 2020 р.). – Чернігів : НУЧП, 2020. – С.133-139 4. Постол Т.Г. ДОСЛІДЖЕННЯ ФУНКЦІОНАЛЬНИХ МОЖЛИВОСТЕЙ АНТИВІРУСНИХ ПРОГРАМ / Постол Т.Г., Ткач Ю.М. // Безпека ресурсів інформаційних систем : збірник тез І Міжнародної науково-практичної конференції (м. Чернігів 16-17 квітня 2020 р.). – Чернігів : НУЧП, 2020. – С.139-146. 5. Ткач Ю. М. KUBERNETES - ОРКЕСТРАЦІЇ КОНТЕЙНЕРІВ, ЩО ЗАБЕЗПЕЧУЄ ВІДМОВОСТІЙКІСТЬ ТА ДОСТУПНІСТЬ ДОДАТКУ / Ткач Ю. М., Клименок В. О. // Новітні технології у науковій діяльності і навчальному процесі : Всеукраїнська науково-практична конференція студентів, аспірантів та молодих учених: збірник тез доповідей (м. Чернігів 18-19 березня 2021 р.). - Чернігів : НУЧП, 2021. – С.176-178 6. Ткач Ю. М. ПЕРЕВІРКА ТА АУТЕНТИФІКАЦІЯ КОРИСТУВАЧІВ ІНФОРМАЦІЙНО-КОМП'ЮТЕРНИХ СИСТЕМ НА ОСНОВІ ТЕХНОЛОГІЇ SINGLE SIGN-ON (SSO) / Ткач Ю. М., Дюба І.М. // Новітні технології у науковій діяльності і навчальному процесі : Всеукраїнська науково-практична конференція студентів, аспірантів та молодих учених: збірник тез доповідей (м. Чернігів 19-20 квітня 2023 р.). - Чернігів : НУЧП, 2023. 7. Ткач Ю. М. ТЕХНОЛОГІЇ OSINT: БАЗОВІ ПОШУКОВІ ІНСТРУМЕНТИ / Дятел І.В., Сурмило Д.О., Ткач Ю.М. // Новітні технології у науковій

							діяльності і навчальному процесі : Всеукраїнська науково-практична конференція студентів, аспірантів та молодих учених: збірник тез доповідей (м. Чернігів 19-20 квітня 2023 р.). - Чернігів : НУЧП, 2023. 8. Ткач Ю. М. АЛГОРИТМИ РЕАГУВАННЯ НА КІБЕРІНЦИДЕНТИ / Лаврів Н.О., Ткач Ю. М.// Новітні технології у науковій діяльності і навчальному процесі : Всеукраїнська науково-практична конференція студентів, аспірантів та молодих учених: збірник тез доповідей (м. Чернігів 19-20 квітня 2023 р.). - Чернігів : НУЧП, 2023. 9. Ткач Ю. М. МОДЕЛЮВАННЯ ПОВЕДІНКИ НАТОВПУ В УМОВАХ ВІЙНИ / Нороха В.О., Ткач Ю. М.// Новітні технології у науковій діяльності і навчальному процесі : Всеукраїнська науково-практична конференція студентів, аспірантів та молодих учених: збірник тез доповідей (м. Чернігів 19-20 квітня 2023 р.). - Чернігів : НУЧП, 2023. 10. Бабічев В.С. АНАЛІЗ МЕТОДІВ ВПЛИВУ ІНФОРМАЦІЙНО-ПСИХОЛОГІЧНИХ ОПЕРАЦІЙ НА МАСОВУ СВІДОМІСТЬ СУСПІЛЬСТВА В СТАНІ ВІЙНИ / Бабічев В.С., Ткач Ю. М.// «ЮНІСТЬ НАУКИ – 2024»: XIV Міжнародна науково-практична конференція студентів, аспірантів та молодих учених: збірник тез доповідей (м. Чернігів 24-26 квітня 2024 р.). П13. Соціальна інженерія, 4 курс, 4 кредити П19. Участь у професійних об'єднаннях за спеціальністю: ГО «Асоціація працівників кібербезпеки». Участь у професійних об'єднаннях за спеціальністю: ГО «Наукова асоціація кібербезпеки України». (SCSA-UA)
293250	Шелест Михайло Євгенович	Професор, Основне місце роботи	ННІ Електронних та інформаційних технологій	Диплом спеціаліста, Львівський політехнічний інститут, рік закінчення: 1976, спеціальність: прикладна математика, Диплом спеціаліста, Академія зв'язку, рік закінчення: 1986, спеціальність: інженерія автоматизованих систем управління, Диплом доктора наук ДД 003791, виданий 16.09.2004, Диплом кандидата наук ДК 001440, виданий 14.10.1998, Атестат доцента ДЦ 006092, виданий 23.12.2002, Атестат професора 12ПР 005627, виданий 03.07.2008	43	ОК 8. Методи побудови та аналізу криптосистем	Підвищення кваліфікації: Державний вищий навчальний заклад «Ужгородський національний університет» Довідка №1636/01-14 від 07.05.2024. 1.Networking Technologies. Course "NT -CSF Cyber Security "16.09.2022 2.r_d.Course "Generation AI Model Development"(27 год) 03.09.2025 3.Distributed Lab.Course "Cryptography: A Modern Approach"11.06.2025 4.Курс "Покоління Python" для просунутих 28.01.2023 5.NEOVERSITY Курс "AI & Cybersecurity" П1. Scopus https://www.scopus.com/authid/detail.uri?authorId=57211429755 https://orcid.org/0000-0001-7110-4876 1. Bezkorovainyi V., Bychkov O., Golub S., Shelest M.(2021) Preface CEUR Workshop Proceedings of 2nd International Conference on Intellectual Systems and Information Technologies, ISIT; 2021 September 13-19; Odesa; Ukraine. – 2021 2. Tkach, Y, Sinenko M, Shelest M, Mekhed D, Kosareva D (2023) Construction of the Assessment Model of the Information Security System of the Enterprise. 7th International Conference on Mathematical Modeling and Simulation of Systems, MODS 2022, 14 November 2022до 16 November 2022. Chernihiv – 2023. - P. 171 – 181. Посилання на статтю 3. Semendiai, S., Tkach, Y., Shelest, M., Ziubina, R., Veselska, O. (2023) Improving the Efficiency of UAV Communication Channels in the Context of Electronic Warfare. International Journal of Electronics and Telecommunications, 2023, 69(4), P. 727–732 4. Andrushchenko, R., Zaitsev, S., Druzhynin, O., Shelest, M. (2020) Method of encoding structured messages by using state vectors. Advances in Intelligent Systems and Computing, 2020, 1019, P. 144–153 Фахові: 1. Хорошко В.О. БАГАТОКРИТЕРІАЛЬНА ОЦІНКА ЕФЕКТИВНОСТІ ПРОЕКТІВ ІЗ ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ / Хорошко В.О., Шелест М.Є., Ткач Ю.М. // Технічні науки та технології : науковий журнал / Чернігів. нац. технол. ун-т. – Чернігів : ЧНТУ, 2020. – № 1 (19). – С. 114-124 2. Ткач Ю., Шелест М., Черниш Л., Литвин С., Бригинець А. Аналіз систем підтримки аудиту інформаційної безпеки/ Технічні науки та технології : науковий журнал / Чернігів. нац. технол. ун-т. – Чернігів : ЧНТУ, 2020. – № 2 (20). – С. 203-210 3. Шелест М., Ткач Ю., Семендяй С., Синенко М., Черниш Л. Дослідження стійкості алгоритму автентифікованого шифрування на базі sponge-функції // Технічні науки та технології : науковий журнал /

							Чернігів. нац. технол. ун-т. – Чернігів : ЧНТУ, 2020. – № 2 (20). – С. 210-218 4. Семендяй С., Шелест М., Ткач Ю., Черниш Л. Етичний хакінг у бізнес-компаніях та виявлення вразливостей в інформаційних системах державних органів України / Технічні науки та технології : науковий журнал / Чернігів. нац. технол. ун-т. – Чернігів : ЧНТУ, 2020. – № 2 (20). – С. 237-241 5. Хорошко В.О., Багатоальтернативне виявлення кібератак в інформаційних мережах / Шелест М.Є., Ткач Ю.М.// Безпека інформації. 2021. Т. 27, № 3. С. 136-141. 6. Хорошко В. Виявлення та оцінювання кібератак в інформаційних мережах з випадковим моментом появи / Хорошко В., Шелест М., Ткач Ю. // Технічні науки та технології. -2021. - № 1(23). - С. 96-102. П2. Патент на винахід «Спосіб лінгвістичної стеганографії» (62434А, 7 G06K9/72, H04L9/28). П3. Навчальні посібники: 1. Інформатика та комп'ютерна техніка. Частина І. Основи загальної інформатики: /навчальний посібник / В.Д.Козюра, Ю.М. Ткач, В.О. Хорошко, В.В. Кузовков, С.В. Зайцев, М.Є. Шелест, О.В. Гаркун. Ніжин ФОП Лук'яненко В.В., ТПК «Орхидея», 2023. – 464 с. ISBN 978-617-7609-84-0 2. Інформатика та комп ' ютерна техніка. Частина ІІ. Спеціальна інформантика. Том 1: навч. посібник / Козюра В. Д., Ткач Ю. М., Хорошко В.О., Шелест М.Є., Петренко Т.А. Ніжин: ФОП Лук ' яненко В.В., ТПК «Орхідея», 2023., 288 с. ISBN 978-617-7609-80-2 3. Інформатика та комп'ютерна техніка: Спеціальна інформатика: Навчальний посібник., Т. ІІ., Ч. ІІ / В.Д. Козюра, Ю.М. Ткач, В.О. Хорошко, М.Є. Шелест, М.А. Синенко: Ніжин: ТПК "Орхідея", ФОП Лук'яненко В. В., 2023., 352 с. ISBN 978-617-7609-89-8) 4. Процеси та технології в інформаційних системах: навч.посібник / Козюра В.Д., Скачек Л.М., Ткач Ю.М., Хорошко В.О., Шелест М.Є., Мехед Д.Б. Ніжин: ФОП Лук'яненко В.В., ТПК «Орхідея», 2020.-278 с. Підручник: 1. Козюра В.Д., Хорошко В.О., Шелест М.Є., Ткач Ю.М., Балюнов О.О. Захист інформації в комп ' ютерних системах : підручник. – Ніжин : ФОП Лук ' яненко В.В., ТПК «Орхидея», 2020. – 236 с. 2. Кібербезпека: підручник / Ю.В. Баланюк, В.В. Козловський, Ю.М. Лисецький, Б.В. Моркляник, В.О. Хорошко, Ю.Є. Хохлачова, М.Є. Шелест. – Київ: Видавець Бихун В.Ю., 2024. – 540 с. Монографія: 1. Захист кіберпростору: монографія / Ю.М. Ткач, М.Є. Шелест, В.О. Хорошко, І.М.Дюба, Д.В.Кальченко, 2024. – 198 с. П4. 1. Основи криптографічного захисту інформації. Методичні вказівки до виконання курсової роботи для здобувачів першого (бакалаврського) рівня вищої освіти освітньо-професійної програми «Кібербезпека» спеціальності 125 Кібербезпека та захист інформації. / уклад.: М.А. Синенко, Ю.М. Ткач, М.Є. Шелест, С.М. Семендяй. – Чернігів: НУ «Чернігівська політехніка», 2024 – 40 с 2. Кібербезпека та захист інформації. Методичні вказівки з ознайомчої практики для здобувачів першого (бакалаврського) рівня вищої освіти освітньо-професійної програми «Кібербезпека» спеціальності 125 Кібербезпека та захист інформації. / уклад.: Т.А. Петренко, Ю.М. Ткач, М.Є. Шелест, Д.В. Кальченко, І.М. Дюба. – Чернігів: НУ «Чернігівська політехніка», 2024 – 25 с. 3. Кібербезпека та захист інформації. Методичні вказівки з навчальної практики для здобувачів першого (бакалаврського) рівня вищої освіти освітньо-професійної програми «Кібербезпека» спеціальності 125 Кібербезпека та захист інформації. / уклад.: Т.А. Петренко, Ю.М. Ткач, М.Є. Шелест, Д.В. Кальченко, І.М. Дюба. – Чернігів: НУ «Чернігівська політехніка», 2024 – 23 с 4. Кібербезпека та захист інформації. Методичні вказівки з технологічної практики для здобувачів першого (бакалаврського) рівня вищої освіти освітньо-професійної програми «Кібербезпека» спеціальності 125 Кібербезпека та захист інформації. / уклад.: Т.А. Петренко, Ю.М. Ткач, М.Є. Шелест, С.М. Семендяй. – Чернігів: НУ «Чернігівська політехніка», 2024 – 26 с

							5. Кібербезпека та захист інформації. Методичні вказівки з виробничої практики для здобувачів першого (бакалаврського) рівня вищої освіти освітньо-професійної програми «Кібербезпека» спеціальності 125 Кібербезпека та захист інформації. / уклад.: Т.А. Петренко, Ю.М. Ткач, М.Є. Шелест, С.М. Семендяй. – Чернігів: НУ «Чернігівська політехніка», 2024 – 25 с 6. Комп'ютерні мережі. Методичні вказівки до курсового проектування для здобувачів першого (бакалаврського) рівня вищої освіти освітньо-професійної програми «Кібербезпека» спеціальності 125 Кібербезпека та захист інформації. / уклад.: С.М. Семендяй, Т.А. Петренко, М.Є. Шелест, А.Г. Гребенник. – Чернігів: НУ «Чернігівська політехніка», 2024 – 40 с. 7. Комплексні системи захисту інформації. Методичні вказівки до курсового проектування для здобувачів першого (бакалаврського) рівня вищої освіти освітньо-професійної програми «Кібербезпека» спеціальності 125 Кібербезпека та захист інформації. / уклад.: С.М. Семендяй, Ю.М. Ткач, М.Є. Шелест. – Чернігів: НУ «Чернігівська політехніка», 2024 – 100 с 8. Стандартизація, сертифікація засобів та комплексів захисту інформації. Методичні вказівки до виконання лабораторних робіт для здобувачів другого (магістерського) рівня вищої освіти освітньо-професійної програми «Кібербезпека» спеціальності 125 Кібербезпека та захист інформації. / уклад.: В.О. Хорошко, Ю.М. Ткач, М.Є. Шелест. – Чернігів: НУ «Чернігівська політехніка», 2024 – 94 с. П6. Ткач Ю.М., 2021р к.т.н., 21.05.01 Інформаційна безпека держави П7. Участь в атестації наукових кадрів: - член та офіційний опонент спеціалізованої вченої ради Д.26.062.17 Національного авіаційного університету за спеціальністю 05.13.21-системи захисту інформації(по теперішній час); - офіційний опонент Аясраха Ахмада Расмі Алі – дисертаційне дослідження представлене на здобуття наукового ступеня доктора філософії за спеціальністю 125 «Кібербезпека», галузь знань 12 «Інформаційні технології» (2023) - офіційний опонент Соколова Артема Вікторовича – дисертація представлена до захисту на здобуття ступеня доктора технічних наук за спеціальністю 05.13.21 Системи захисту інформації (2023) - офіційний опонент Войцеховської Марії Іванівни – дисертація представлена до захисту на здобуття ступеня доктора філософії в галузі знань 12 – «Інформаційні технології» за спеціальністю 122 – «Комп'ютерні науки». (2023) П8. Член редакційної колегії наукових видань: - "Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні" науково-технічний збірник Національного технічного університету "КПІ"; - журнал "Захист інформації", засновник та видавець Національний авіаційний університет; П11. ТОВ «Інформаційна безпека», укладено договір про співпрацю П12. 1.Бакрі М. РЕАЛІЗАЦІЯ СТАНДАРТУ ШИФРУВАННЯ SES ДЛЯ ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ ЦИФРОВОЇ ІНФРА-СТРУКТУРИ / Бакрі М., Гері Лох Чі Віяй, Юрченко А.В., Ткач Ю.М., Шелест М.Є. //Безпека ресурсів інформаційних систем : збірник тез І Міжнародної науково-практичної конференції (м. Чернігів 16-17 квітня 2020 р.). – Чернігів : НУЧП, 2020. – С.47-50. 2. Ткач Ю.Н. Про розвиток кіберпростору та його захищеності / Ткач Ю.Н., Шелест М.Е., Карпинский Н.П. // Безпека ресурсів інформаційних систем : збірник тез І Міжнародної науково-практичної конференції (м. Черні-гів 16-17 квітня 2020 р.). – Чернігів : НУЧП, 2020. – С.173-178 3. Бакуменко Б.С. МЕТОДИ ШИФРУВАННЯ ТА ДЕШИФРУВАННЯ НА ПРИКЛАДІ З CTF / Семендяй С.М., Шелест М.Є. // Новітні технології у науковій діяльності і навчальному процесі : Всеукраїнська науково-практична конференція студентів, аспірантів та молодих учених: збірник тез доповідей (м. Чернігів 19-20 квітня

							2023 р.). - Чернігів : НУЧП, 2023. П19. Участь у професійних об'єднаннях за спеціальністю: ГО «Асоціація працівників кібербезпеки». П20. біля 40 років служби у військовій розвідці, СБУ, Службі зовнішньої розвідки
299888	Петренко Тарас Анатолійович	Доцент, Основне місце роботи	ННІ Електронних та інформаційних технологій	Диплом молодшого спеціаліста, Чернігівський державний інститут права, соціальних технологій та праці, рік закінчення: 2008, спеціальність: 060101 Правознавство, Диплом бакалавра, Чернігівський державний технологічний університет, рік закінчення: 2004, спеціальність: 0915 Комп'ютерна інженерія, Диплом спеціаліста, Чернігівський державний технологічний університет, рік закінчення: 2005, спеціальність: 091502 Системне програмування, Диплом кандидата наук ДК 0586619, виданий 14.05.2020	18	ОК 6. Проектування технічних систем захисту інформації	Підвищення кваліфікації: Державний університет інформаційно-комунікаційних технологій, Довідка №26/907 від 20.05.2025 П1 1. Шелест М., Петренко Т., Семендяй С. Нороха В. Тестова конфігурація об'єкта інформаційної діяльності для відпрацювання навичок із пошуку технічних каналів витоку інформації. Український науковий журнал інформаційної безпеки, 2024, том 30, випуск 1, с.82. doi: 10.18372/2225-5036.30.18608 2. Ткач, Ю. ., Шелест, М. ., Синенко, М., & Петренко, Т. (2023). Історія виникнення клептографії та її місце в безпеці інформації. Технічні науки та технології, (3 (33), 150–161. doi: 10.25140/2411-5363-2023-3(33)-150-161 3. Борода А., Петренко Т.А. (2023). Вплив атак за побічними каналами на інформаційну безпеку. Технічні науки та технології, (4 (34), 91–103. doi:10.25140/2411-5363-2023-4(34)-91-103 4. Риндич, Є. В., Петренко, Т. А., Черниш, Л. Г., Семендяй, С. М., & Біленький, Г. С. (2020). Навчальний стенд для вивчення дисциплін із забезпечення мережевого захисту інформації. Технічні науки та технології, (2(20), 229–236. 5. Базилевич, В. М., Мальцева, М. В., Петренко, Т. А., & Черниш, Л. Г. (2020). Захищена система розумного будинку з використанням Internet of Things. Технічні науки та технології, (2(20), 218–228. П3 1. Інформатика та комп'ютерна техніка: Ч. II Спеціальна інформатика: навч.посібник / В.Д. Козюра, Ю.М. Ткач, В.О. Хорошко, М.Є. Шелест, Т.А. Петренко. 2023. – Т. 1. – 288 с. П4 1. Кібербезпека. Методичні вказівки до виробничої практики [Текст] / розробник: Петренко Т.А. – Чернігів: Чернігівський національний технологічний університет, 2020. – 36 с. 2. Кібербезпека. Методичні вказівки до виконання кваліфікаційної роботи здобувачів вищої освіти другого (магістерського) рівня вищої освіти спеціальності 125-Кібербезпека та захист інформації/F5 – Кібербезпека та захист інформації // Укл.: Т.А. Петренко, Ю.М. Ткач, М.Є.Шелест, С.М.Семендяй. - Чернігів: НУ «Чернігівська політехніка», 2025 – 42с. 3. Кібербезпека. Методичні вказівки до переддипломної практики для здобувачів другого (магістерського) рівня вищої освіти спеціальності 125 - Кібербезпека / укл: Петренко Т.А., Ткач Ю.М. – Чернігів: Національний університет «Чернігівська політехніка», 2020. – 30 с. 4. Проектування технічних систем захисту інформації: методичні вказівки до виконання курсового проекту для здобувачів другого (магістерського) рівня вищої освіти спеціальності 125 - «Кібербезпека» // Укл.: Т.А. Петренко - Чернігів: НУ «Чернігівська політехніка», 2020. – 28с. 5. Бази даних. Методичні вказівки до виконання курсової роботи для здобувачів першого (бакалаврського) рівня вищої освіти освітньо-професійної програми «Кібербезпека» спеціальності 125 Кібербезпека та захист інформації. / уклад.: В.М. Базилевич, Д.Б. Мехед, А.Г. Гребенник, Т.А. Петренко. – Чернігів: НУ «Чернігівська політехніка», 2024 – 26 с. 6. Інформатика. Методичні вказівки до виконання лабораторних робіт для здобувачів першого (бакалаврського) рівня вищої освіти освітньо-професійної програми «Кібербезпека» спеціальності 125 Кібербезпека та захист інформації. / уклад.: А.Г. Гребенник, Т.А. Петренко, І.М. Дюба. – Чернігів: НУ «Чернігівська політехніка», 2024 – 42 с. 7. Кібербезпека та захист інформації. Методичні вказівки з ознайомчої практики для здобувачів першого (бакалаврського) рівня вищої освіти освітньо-професійної програми «Кібербезпека» спеціальності 125 Кібербезпека та захист інформації. / уклад.: Т.А. Петренко, Ю.М. Ткач, М.Є. Шелест, Д.В. Кальченко, І.М. Дюба. – Чернігів: НУ «Чернігівська політехніка», 2024 – 25 с. 8. Кібербезпека та захист інформації. Методичні вказівки з навчальної практики для здобувачів першого

							(бакалаврського) рівня вищої освіти освітньо-професійної програми «Кібербезпека» спеціальності 125 Кібербезпека та захист інформації. / уклад.: Т.А. Петренко, Ю.М. Ткач, М.Є. Шелест, Д.В. Кальченко, І.М. Дюба. – Чернігів: НУ «Чернігівська політехніка», 2024 – 23 с 9. Кібербезпека та захист інформації. Методичні вказівки з технологічної практики для здобувачів першого (бакалаврського) рівня вищої освіти освітньо-професійної програми «Кібербезпека» спеціальності 125 Кібербезпека та захист інформації. / уклад.: Т.А. Петренко, Ю.М. Ткач, М.Є. Шелест, С.М. Семендяй. – Чернігів: НУ «Чернігівська політехніка», 2024 – 26 с 10. Кібербезпека та захист інформації. Методичні вказівки з виробничої практики для здобувачів першого (бакалаврського) рівня вищої освіти освітньо-професійної програми «Кібербезпека» спеціальності 125 Кібербезпека та захист інформації. / уклад.: Т.А. Петренко, Ю.М. Ткач, М.Є. Шелест, С.М. Семендяй. – Чернігів: НУ «Чернігівська політехніка», 2024 – 25 с 11. Адміністрування Unix-подібних систем. Конспект лекцій для здобувачів першого (бакалаврського) рівня вищої освіти освітньо-професійної програми «Кібербезпека» спеціальності 125 Кібербезпека та захист інформації. / уклад.: С.М. Семендяй, Т.А. Петренко, А.Г. Гребенник, Д.В. Кальченко. – Чернігів: НУ «Чернігівська політехніка», 2024 – 170с. 12. Комп'ютерні мережі. Методичні вказівки до курсового проектування для здобувачів першого (бакалаврського) рівня вищої освіти освітньо-професійної програми «Кібербезпека» спеціальності 125 Кібербезпека та захист інформації. / уклад.: С.М. Семендяй, Т.А. Петренко, М.Є. Шелест, А.Г. Гребенник. – Чернігів: НУ «Чернігівська політехніка», 2024 – 40 с. П5. Захист дисертації, Ніціональний авіаційний університет, диплом кандидата наук від 14 травня 2020р. ДК №056619 П7. Опонент на дисертаційну роботу Шабана Максима Радуйовича “Моделі підтримки прийняття рішень для експертиз технічного захисту інформації”, представлену ним на здобуття наукового ступеня кандидата технічних наук за спеціальністю 05.13.21 – “Системи захисту інформації”. Захист відбувся 22 квітня 2021 р. на засіданні спеціалізованої вченої ради Д 26.062.17 при Національному авіаційному університеті. П12. 1. Петренко Т.А, Коротка Г.М., Аналіз складових інформаційної безпеки систем електронного документообігу // Всеукраїнська науково-практична конференція студентів, аспірантів та молодих вчених «Новітні технології у науковій діяльності і навчальному процесі» м. Чернігів, ЧНТУ, 2020. 2. Петренко Т.А. Особливості управління доступом в сучасних операційних системах / Т.А. Петренко // Безпека ресурсів інформаційних систем : збірник тез I Міжнародної науково-практичної конференції (м. Чернігів 16-17 квітня 2020 р.). – Чернігів: НУЧП, 2020. 3. Петренко Т.А, Вильотніков В.В., Методи захисту інформації в бездротових мережах // Всеукраїнська науково-практична конференція студентів, аспірантів та молодих вчених «Новітні технології у науковій діяльності і навчальному процесі» м. Чернігів, НУЧП , 2021. 4 Петренко Т.А, Баглай Ю.О. Analysis of tor and decentralized web systems as censorship resistance tools // Всеукраїнська науково-практична конференція студентів, аспірантів та молодих вчених «Новітні технології у науковій діяльності і навчальному процесі» м. Чернігів, НУЧП , 2023. 5. Петренко Т.А., Горбач Я. Ю. IoT та блокчейн: сучасні можливості та виклики // Всеукраїнська науково-практична конференція студентів, аспірантів та молодих вчених «Новітні технології у науковій діяльності і навчальному процесі» м. Чернігів, НУЧП , 2023. 6. Kuznetsova A.M., Petrenko T.A., Lytvyn S.V. Cyber hygiene in online dating // Всеукраїнська науково-практична конференція студентів, аспірантів та молодих вчених «Новітні технології у науковій діяльності і навчальному процесі» м. Чернігів, НУЧП , 2023. 7. Петренко Т.А., Медведський А.А. Проблеми забезпечення кібербезпеки мобільних пристроїв // Всеукраїнська науково-практична конференція студентів, аспірантів та молодих вчених «Новітні технології у науковій

							діяльності і навчальному процесі» м. Чернігів, НУЧП , 2023. 8. Радченко В.Ю., Петренко Т.А. Devsecops: розробка та тестування програмного забезпечення // Всеукраїнська науково-практична конференція студентів, аспірантів та молодих вчених «Новітні технології у науковій діяльності і навчальному процесі» м. Чернігів, НУЧП , 2023. 9. Сомов В. О., Петренко Т.А., Технології LoRaWAN та Zigbee в «розумних мережах» // Всеукраїнська науково-практична конференція студентів, аспірантів та молодих вчених «Новітні технології у науковій діяльності і навчальному процесі» м. Чернігів, НУЧП , 2023. 10. Петренко Т.А., Шпитальний Б.Н. Проектування захищених робочих місць від витоку інформації з обмеженим доступом каналом побічного-електромагнітного випромінювання шляхом екранування // Міжнародна науково-практична конференція «Юність науки-2024», м. Чернігів, НУ «Чернігівська політехніка» , 2024. 11. Петренко Т.А., Сьомченко Д.В. Використання моделей глибинного навчання трансформерів для виявлення спаму в текстових повідомленнях // Міжнародна науково-практична конференція «Юність науки-2024», м. Чернігів, НУ «Чернігівська політехніка», 2024. 12. Петренко Т.А., Земляков Д.П. Аналіз радіочастотного спектру інформаційного середовища // Міжнародна науково-практична конференція «Юність науки-2024», м. Чернігів, НУ «Чернігівська політехніка» , 2024. 13. Петренко Т.А., Апанасенко В.В. Проблеми забезпечення безпеки інформації в IoT-системах // Міжнародна науково-практична конференція «Юність науки-2024», м. Чернігів, НУ «Чернігівська політехніка» , 2024 П19. ГО "Асоціація працівників кібербезпеки"
343930	Гребенник Алла Григорівна	Старший викладач, Основне місце роботи	ННІ Електронних та інформаційних технологій	Диплом спеціаліста, Чернігівський технологічний інститут, рік закінчення: 1992, спеціальність: обчислювальні машини, комплекси, системи і мережі	18	ОК 3. Аудит та управління інцидентами інформаційної безпеки	Підвищення кваліфікації: Державний вищий навчальний заклад «Ужгородський національний університет», Довідка №1635/01-14 від 07.05.2024 П1. Scopus https://www.scopus.com/authid/detail.uri?authorId=57219054928 1. Vitalii Lytvynov, Alla Hrebennyk, Elena Trunova, Igor Skiter, Yurii Lysetskyi (2020) Principles of Adaptive Corporate Network Security Management. The Model of Information Security Culture Level Estimation of Organization In: Palagin A., Anisimov A., Morozov A., Shkarlet S. (eds) Mathematical Modeling and Simulation of Systems. MODS 2020. Advances in Intelligent Systems and Computing, vol 1265. Springer, Cham. pp. 255-265 2. Hrebennyk A., Trunova E., Kazymyr, V., Tarasov, A. Modelling a Multi-agent Protection System of an Enterprise Network. DIGILIENCE 2020: Digital Transformation, Cyber Security and Resilience. – 2024. - Vol .1790. - P.113–122. Фахові: 1. В.В. Литвинов, Н. Стоянов, І.С. Скітер, О.В. Трунова, А.Г. Гребенник / Аналіз систем та методів виявлення несанкціонова-них вторгнень у комп'ютерні мережі // Математичні машини і системи. – 2018. - №1. – С.31-40. 2. Lytvynov V., Stoianov N., Skiter I., Trunova H., Hrebennyk A. / Corporate networks protection against attacks using content-analysis of global information space // Технічні науки та технології: науковий журнал / Черніг. нац. технол. ун-т. – Чернігів : ЧНТУ, 2018. – № 1 (11). – С.115-128. 3. В.В. Литвинов, Н. Стоянов, І.С. Скітер, О.В. Трунова, А.Г. Гребенник / Використання методів підтримки прийняття рішень при пошуку джерел атак на комп'ютерні мережі в умовах невизначеності // Математичні машини і системи. – 2019. – № 4. – С. 38-51. 4. Гребенник А.Г., Трунова О.В., Казимир В.В., Міщенко М.В. / Виявлення та прогнозування рівня загроз для корпоративної комп'ютерної мережі // Технічні науки та технології: науковий журнал / Черніг. нац. технол. ун-т. – Чернігів : ЧНТУ, 2020. – № 2 (20). – С.175-185. 5. Vitalii Lytvynov, Alla Hrebennyk, Elena Trunova, Igor Skiter and Yurii Lysetskyi / Principles of adaptive corporate network security management // MODS 2020. Advances in Intelligent Systems and Computing. Springer, Cham. P. II. Mathematical Modeling and Simulation of Systems. – 2021. – Vol. 1265. – P.255-265. 6. Design of Industry Centers of Cyber Security of Facilities of Critical Infrastructure / A. Morozov, A. Hrebennyk, E. Trunova, I. Skiter, E. Hulak. – Kyiv: Cybersecurity Providing

							in Information and Telecommunication Systems, 2021. - P.27-37. П.3 Навчальні посібники, монографії 1. Методи аналізу та моделювання безпеки розподілених інформаційних систем: монографія / В.В. Литвинов, В.В. Казимир, І.В. Стеценко, О.В. Трунова, І.С. Скітер, Ю.М. Ткач, А.Г. Гребенник, В.В. Нехай : за заг. ред. проф. С.М. Шкарлета. – Черні-гів: Чернігів. Нац. Технол. Ун-т, 2017. – 206с. 2. Моделювання та аналіз безпеки розподілених інформаційних систем: навч. посіб. [для студ. спец. 121 «Інженерія програм-ного забезпечення] / В.В. Литвинов, В.В. Казимир, І.В. Стеценко, О.В. Трунова, І.С. Скітер, Ю.М. Ткач, А.Г. Гребенник, В.В. Нехай. – Чернігів: Чернігів. Нац. Технол. Ун-т, 2017. – 254 с. 3. Університетськоіндустріальна коопера-ція. Веб-портал. Наста-нова з використання. / Під ред. Кондратенка Ю.П., Харченка В.С. – Міністерство освіти і науки України, Черніговський національний технологічний універси-тет, Національний аероко-смічний універси-тет ім. М.Є. Жуковського «ХАІ». 2017, Т.3. – 180с. 4. Computer nets attacks defense tools based on extended information about environment : monograph / V. Lytvynov, N. Stoianov, I. Stetsenko, I. Skiter, O. Trunova, A. Hrebennyk, V. Nekhai, I. Burmaka. – Chernihiv : Chernihiv Politechnic National University, 2021. –212 с. П.4 1. Бази даних. Методичні вказівки до виконання курсової роботи для здобувачів першого (бакалаврського) рівня вищої освіти освітньо-професійної програми «Кібербезпека» спеціальності 125 Кібербезпека та захист інформації. / уклад.: В.М. Базилевич, Д.Б. Мехед, А.Г. Гребенник, Т.А. Петренко. Чернігів: НУ «Чернігівська політехніка», 2024 – 26с. 2. Інформатика. Методичні вказівки до виконання лабораторних робіт для здобувачів першого (бакалаврського) рівня вищої освіти освітньо-професійної програми «Кібербезпека» спеціальності 125 Кібербезпека та захист інформації. / уклад.: А.Г. Гребенник, Т.А. Петренко, І.М. Дюба. – Чернігів: НУ «Чернігівська політехніка», 2024 – 42с. 3. Технології програмування. Методичні вказівки до виконання лабораторних робіт для здобувачів першого (бакалаврського) рівня вищої освіти освітньо-професійної програми «Кібербезпека» спеціальності 125 Кібербезпека та захист інформації. / уклад.: І.М. Дюба, С.М. Семендяй, А.Г. Гребенник. – Чернігів: НУ «Чернігівська політехніка», 2024 – 42с. 4. Адміністрування Unix-подібних систем. Конспект лекцій для здобувачів першого (бакалаврського) рівня вищої освіти освітньо-професійної програми «Кібербезпека» спеціальності 125 Кібербезпека та захист інформації. / уклад.: С.М. Семендяй, Т.А. Петренко, А.Г. Гребенник, Д.В. Кальченко. – Чернігів: НУ «Чернігівська політехніка», 2024 – 170 с. 5. Комп'ютерні мережі. Методичні вказівки до курсового проектування для здобувачів першого (бакалаврського) рівня вищої освіти освітньо-професійної програми «Кібербезпека» спеціальності 125 Кібербезпека та захист інформації. / уклад.: С.М. Семендяй, Т.А. Петренко, М.Є. Шелест, А.Г. Гребенник. – Чернігів: НУ «Чернігівська політехніка», 2024 – 40с. 6. Інциденти інформаційної безпеки. Методичні вказівки до виконання лабораторних робіт для здобувачів першого (бакалаврського) рівня вищої освіти освітньо-професійної програми «Кібербезпека» спеціальності 125 Кібербезпека та захист інформації. / уклад.: А.Г. Гребенник, Ю.М. Ткач, С.М. Семендяй. – Чернігів: НУ «Чернігівська політехніка», 2024 – 62с. П.10 Відповідальний виконавець у міжнародному науковому проекті «Системи захисту від мережевих атак CyRADARS за грантом NATO SPS, (grant agreement number: G5286)» П.12 1. Литвинов В.В., Трунова О.В., Гребенник А.Г. / Модель адаптивного управління безпекою корпоративної мережі // V міжнародна конференція «Проблеми зняття з експлуатації об'єктів ядерної енергетики та відновлення навколишнього середовища» INUDECO 2020 в режимі онлайн (27–29 квітня 2020 року, м. Славутич). Збірник матеріалів. – Чернігів, ЧНТУ, 2020. –

							С.138-141. 2. Міщенко М.В., Гребенник А.Г., Трунова О.В. / Прогнозування рівня загроз з використанням мереж Байєса // Математичне та імітаційне моделювання систем. МОДС 2020 : тези доповідей П'ятнадцятої міжнародної науково-практичної конференції (Чернігів, 29 червня – 1 липня 2020 р.). – Чернігів: ЧНТУ, 2020. – С. 120-123. 3. Тарасов О.Є., Гребенник А.Г., Трунова О.В. / Використання мультиагентних систем для захисту корпоративних мереж // Математичне та імітаційне моделювання систем. МОДС 2020 : тези доповідей П'ятнадцятої міжнародної науково-практичної конференції (Чернігів, 29 червня – 1 липня 2020 р.). – Чернігів: ЧНТУ, 2020. – С. 186-190. 4. Філон А.А., Гребенник А.Г. / Адаптивне управління захищеністю корпоративної мережі на основі нечіткої логіки // Математичне та імітаційне моделювання систем. МОДС 2020 : тези доповідей П'ятнадцятої міжнародної науково-практичної конференції (Чернігів, 29 червня – 1 липня 2020 р.). – Чернігів: ЧНТУ, 2020. – С. 229-232. 5. Гребенник А.Г. Методи конкурентної розвідки у виявленні джерел загроз мережевому контенту / Юність науки – 2024 : збірник тез доповідей XIV Міжнародної науково-практичної конференції студентів, аспірантів і молодих вчених (м. Чернігів, 24-26 квітня 2024 р.). – Чернігів : НУ «Чернігівська політехніка», 2024. – С.1099-1100. П.20 Досвід практичної роботи за спеціальністю 6 років (1992-1994рр. інженер ЕОМ ОЦ ЧТУ; 1994-1998. інженер ЕОМ лабораторії ОТ ЧДІЕУ)
376336	Семендяй Сергій Матвійович	Старший викладач, Основне місце роботи	ННІ Електронних та інформаційних технологій	Диплом спеціаліста, Національний технічний університет України "Київський політехнічний інститут", рік закінчення: 2008, спеціальність: 090701 Радіотехніка	27	ОК 7. Технології безпеки бездротових і мобільних мереж	Підвищення кваліфікації: Державний університет інформаційно-комунікаційних технологій, Довідка №26/906 від 20.05.2025 Інструктор Академій Cisco.Курси "CCNA SRWE(Основи комутації,маршрутизації та бездротових мереж)", “CCNA CyberOps, Network Security. П.1. Scopus https://orcid.org/0000-0002-7751-5956 1 Serhii Semendiai, Yuliia Tkach, Mykhailo Shelest, Oleksandr Korchenko, Ruslana Ziubina, Olga Veselska (2023) Improving the Efficiency of UAV Communication Channels in the Context of Electronic Warfare // International Journal of Electronics and Telecommunications, 2023, vol. 69, no. 4, pp. 727-732. 2 Семендяй, С. (2023). Використання технології когнітивного радіо для підвищення ефективності безпроводових систем передачі даних в умовах активного застосування засобів радіоелектронної боротьби. Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка», 4(20), 220–229. https://doi.org/10.28925/2663-4023.2023.20.220229. 3 Семендяй С. Підвищення ефективності безпроводових систем передачі даних в умовах застосування засобів радіоелектронної боротьби. Технічні науки та технології. 2023. № 2(32). С. 224-234. 4 Семендяй, С. М., Шелест, М. Є., Ткач, Ю. М., & Черниш, Л. Г. (2020). Етичний хакінг у бізнес-компаніях та виявлення вразливостей в інформаційних системах державних органів України. Технічні науки та технології, (2(20), 237–240. вилучено із http://tst.stu.cn.ua/article/view/215813. 5 Шелест, М. Є., Ткач, Ю. М., Семендяй, С. М., Синенко, М. А., & Черниш, Л. Г. (2020). Дослідження стійкості алгоритму автентифікованого шифрування на базі sponge-функції. Технічні науки та технології, (2(20), 210–217. вилучено із http://tst.stu.cn.ua/article/view/215809. 6 Риндич, Є. В., Петренко, Т. А., Черниш, Л. Г., Семендяй, С. М., & Біленький, Г. С. (2020). Навчальний стенд для вивчення дисциплін із забезпечення мережевого захисту інформації. Технічні науки та технології, (2(20), 229–236. вилучено із http://tst.stu.cn.ua/article/view/215811. 7 Зайцев С.В. Огляд адаптивних методів забезпечення достовірності передачі інформації при використанні завадостійкого кодування у системах бездротового зв'язку / С.В. Зайцев, В.М. Василенко, С.М. Семендяй // Informatics and Mathematical Methods in Simulation Vol. 11 (2021), No. 4, pp. 278-286. 8 Shelest M., Petrenko T., Semendyay S., Norokha V. Test configuration of the object of information activity for practicing skills in finding technical channels of information leakage //

							Ukrainian Scientific Journal of Information Security, 2024, vol. 30, issue 1, pp. 82-87. https://doi.org/10.18372/2225-5036.30.18608. П.3. Технології програмування: навчальний посібник. Том 2. Сучасні технології програмування / Козюра В.Д., Ткач Ю.М., Хорошко В.О., Кузовков В.В., Хохлачова Ю.Є., Семендяй С.М. Ніжин: ФОП Лук'яненко В.В., ТПК "Орхідея", 2022., 300 с. П.4. 1. Інформаційна безпека держави : метод. вказівки до самост. роботи для здобувачів першого (бакалавр.) рівня вищ. освіти спец. 262 "Правоохоронна діяльність" / уклад.: Ю. М.Ткач, С. М. Семендяй. - Чернігів : НУ «Чернігівська політехніка», 2020. – 16 с. 2. Інформаційна безпека держави : метод. вказівки до практ. занять для здобувачів першого (бакалавр.) рівня вищ. освіти спец. 262 "Правоохоронна діяльність" / уклад.: Ю. М. Ткач, С. М. Семендяй. - Чернігів : НУ «Чернігівська політехніка», 2020. – 112 с. 3. Інформаційна безпека держави. Конспект лекцій для здобувачів вищої освіти освітнього ступеню «бакалавр» спеціальності 262 – «Правоохоронна діяльність»// Укл.: Ю.М.Ткач, С.М.Семендяй - Чернігів: НУ «Чернігівська політехніка», 2020. – 126 с. 4. Інформаційна безпека держави : конспект лекцій для здобувачів вищ. освіти освіт. ступеню «бакалавр» спец. 262 «Правоохоронна діяльність» / уклад.: Ю. М. Ткач, С. М. Семендяй. – Чернігів : НУ «Чернігівська політехніка», 2022. – 133 с. 5. Інформаційна безпека держави : метод. вказівки до самост. роботи для здобувачів першого (бакалавр.) рівня вищ. освіти спец. 262 "Правоохоронна діяльність" / уклад.: Ю. М. Ткач, С. М. Семендяй. – Чернігів : НУ «Чернігівська політехніка», 2022. – 19 с. 6. Комплексні системи захисту інформації : метод. вказівки до виконання курс. проєкту / уклад.: Ю. М. Ткач, С. М. Семендяй. – Чернігів : Національний університет «Чернігівська політехніка», 2021. – 132 с. 7. Основи криптографічного захисту інформації. Методичні вказівки до виконання курсової роботи для здобувачів першого (бакалаврського) рівня вищої освіти освітньо-професійної програми «Кібербезпека» спеціальності 125 Кібербезпека та захист інформації. / уклад.: М.А. Синенко, Ю.М. Ткач, М.Є. Шелест, С.М. Семендяй. – Чернігів: НУ «Чернігівська політехніка», 2024 – 40 с. 8. Технології програмування. Методичні вказівки до виконання лабораторних робіт для здобувачів першого (бакалаврського) рівня вищої освіти освітньо-професійної програми «Кібербезпека» спеціальності 125 Кібербезпека та захист інформації. / уклад.: І.М. Дюба, С.М. Семендяй, А.Г. Гребенник. – Чернігів: НУ «Чернігівська політехніка», 2024 – 42 с. 9. Кібербезпека та захист інформації. Методичні вказівки з технологічної практики для здобувачів першого (бакалаврського) рівня вищої освіти освітньо-професійної програми «Кібербезпека» спеціальності 125 Кібербезпека та захист інформації. / уклад.: Т.А. Петренко, Ю.М. Ткач, М.Є. Шелест, С.М. Семендяй. – Чернігів: НУ «Чернігівська політехніка», 2024 – 26 с. 10. Кібербезпека та захист інформації. Методичні вказівки з виробничої практики для здобувачів першого (бакалаврського) рівня вищої освіти освітньо-професійної програми «Кібербезпека» спеціальності 125 Кібербезпека та захист інформації. / уклад.: Т.А. Петренко, Ю.М. Ткач, М.Є. Шелест, С.М. Семендяй. – Чернігів: НУ «Чернігівська політехніка», 2024 – 25 с. 11. Адміністрування Unix-подібних систем. Конспект лекцій для здобувачів першого (бакалаврського) рівня вищої освіти освітньо-професійної програми «Кібербезпека» спеціальності 125 Кібербезпека та захист інформації. / уклад.: С.М. Семендяй, Т.А. Петренко, А.Г. Гребенник, Д.В. Кальченко. – Чернігів: НУ «Чернігівська політехніка», 2024 – 170 с. 12. Комп'ютерні мережі. Методичні вказівки до курсового проектування для здобувачів першого (бакалаврського) рівня вищої освіти освітньо-професійної програми «Кібербезпека» спеціальності 125 Кібербезпека та захист інформації. / уклад.: С.М. Семендяй, Т.А. Петренко, М.Є. Шелест, А.Г. Гребенник. – Чернігів: НУ «Чернігівська політехніка», 2024 – 40 с.

							13. Комплексні системи захисту інформації. Методичні вказівки до курсового проектування для здобувачів першого (бакалаврського) рівня вищої освіти освітньо-професійної програми «Кібербезпека» спеціальності 125 Кібербезпека та захист інформації. / уклад.: С.М. Семендяй, Ю.М. Ткач, М.Є. Шелест. – Чернігів: НУ «Чернігівська політехніка», 2024 – 100 с. 14. Інциденти інформаційної безпеки. Методичні вказівки до виконання лабораторних робіт для здобувачів першого (бакалаврського) рівня вищої освіти освітньо-професійної програми «Кібербезпека» спеціальності 125 Кібербезпека та захист інформації. / уклад.: А.Г. Гребенник, Ю.М. Ткач, С.М. Семендяй. – Чернігів: НУ «Чернігівська політехніка», 2024 – 62 с. П.8. Відповідальний виконавець ДБТ, держфінансування, з 2025 р П.11. Здійснював наукове консультування установ, підприємств, організацій протягом не менше трьох років, зокрема ТОВ «Інформаційна безпека» (довідка). П.12. 1 Семендяй С.М. Співіснування BLUETOOTH з бездротовими мережами 802.11 / С.М. Семендяй // Новітні технології у науковій діяльності і навчальному процесі : Всеукраїнська науково-практична конференція студентів, аспірантів та молодих учених: збірник тез доповідей (м. Чернігів 19-20 квітня 2023 р.). - Чернігів : НУЧП, 2023. 2 Бакуменко Б.С. Методи шифрування та дешифрування на прикладі з CTF / Б.С. Бакуменко, С.М. Семендяй, Шелест М.Є. // Новітні технології у науковій діяльності і навчальному процесі : Всеукраїнська науково-практична конференція студентів, аспірантів та молодих учених: збірник тез доповідей (м. Чернігів 19-20 квітня 2023 р.). - Чернігів : НУЧП, 2023. 3 Семендяй С.М., Зайцев С.В. Метод забезпечення достовірності інформації в безпроводових засобах передачі даних за рахунок структурної адаптації та використання нейронних мереж /Безпека ресурсів інформаційних систем : тези доп. учасників І Міжнар. наук.-практ. конф.(м. Чернігів 16-17 квіт. 2020 р.) - Чернігів: Вид-во ЧНТУ, 2020. – С.182 – 185. 4 Семендяй С. Адаптивний метод вибору каналу зв'язку для застосування в БпЛА. Інформаційні технології у житі студентів та молодих науковців Закарпаття : зб. наук. праць за матеріалами VII регіональної наук.-практ. конф. (м. Ужгород, 30 листопада 2023 р.). Ужгород : УжНУ, 2023. С. 189–192. 5 Дмитренко С.В. Використання програмного забезпечення MATLAB для моделювання бездротових засобів передавання даних/ Дмитренко С.В., Семендяй С. М.// «ЮНІСТЬ НАУКИ – 2024»: XIV Міжнародна науково-практична конференція студентів, аспірантів та молодих учених: збірник тез доповідей (м. Чернігів 24-26 квітня 2024 р.). П.14. Керівництво постійно діючим студентським науковим гуртком "CybersecurityLab" кафедри кібербезпеки та математичного моделювання. П.19. Участь у професійних об'єднаннях за спеціальністю: ГО «Асоціація працівників кібербезпеки». П. 20. Досвід практичної роботи за спеціальністю становить 22 роки.
376336	Семендяй Сергій Матвійович	Старший викладач, Основне місце роботи	ННІ Електронних та інформаційних технологій	Диплом спеціаліста, Національний технічний університет України "Київський політехнічний інститут", рік закінчення: 2008, спеціальність: 090701 Радіотехніка	27	ОК 9. Управління мережевою безпекою	Підвищення кваліфікації: Державний університет інформаційно-комунікаційних технологій, Довідка №26/906 від 20.05.2025 Інструктор Академій Cisco.Курси "CCNA SRWE(Основи комутації,маршрутизації та бездротових мереж)", "CCNA CyberOps, Network Security. П.1. Scopus https://orcid.org/0000-0002-7751-5956 1 Serhii Semendiai, Yuliia Tkach, Mykhailo Shelest, Oleksandr Korchenko, Ruslana Ziubina, Olga Veselska (2023) Improving the Efficiency of UAV Communication Channels in the Context of Electronic Warfare // International Journal of Electronics and Telecommunications, 2023, vol. 69, no. 4, pp. 727-732. 2 Семендяй, С. (2023). Використання технології когнітивного радіо для підвищення ефективності безпроводових систем передачі даних в умовах активного застосування засобів радіоелектронної боротьби. Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка», 4(20), 220–229.

							https://doi.org/10.28925/2663-4023.2023.20.220229. 3 Семендяй С. Підвищення ефективності безпроводових систем передачі даних в умовах застосування засобів радіоелектронної боротьби. Технічні науки та технології. 2023. № 2(32). С. 224-234. 4 Семендяй, С. М., Шелест, М. Є., Ткач, Ю. М., & Черниш, Л. Г. (2020). Етичний хакінг у бізнес-компаніях та виявлення вразливостей в інформаційних системах державних органів України. Технічні науки та технології, (2(20), 237–240. вилучено із http://tst.stu.cn.ua/article/view/215813. 5 Шелест, М. Є., Ткач, Ю. М., Семендяй, С. М., Синенко, М. А., & Черниш, Л. Г. (2020). Дослідження стійкості алгоритму автентифікованого шифрування на базі sponge-функції. Технічні науки та технології, (2(20), 210–217. вилучено із http://tst.stu.cn.ua/article/view/215809. 6 Риндич, Є. В., Петренко, Т. А., Черниш, Л. Г., Семендяй, С. М., & Біленький, Г. С. (2020). Навчальний стенд для вивчення дисциплін із забезпечення мережевого захисту інформації. Технічні науки та технології, (2(20), 229–236. вилучено із http://tst.stu.cn.ua/article/view/215811. 7 Зайцев С.В. Огляд адаптивних методів забезпечення достовірності передачі інформації при використанні завадостійкого кодування у системах бездротового зв'язку / С.В. Зайцев, В.М. Василенко, С.М. Семендяй // Informatics and Mathematical Methods in Simulation Vol. 11 (2021), No. 4, pp. 278-286. 8 Shelest M., Petrenko T., Semendyay S., Norokha V. Test configuration of the object of information activity for practicing skills in finding technical channels of information leakage // Ukrainian Scientific Journal of Information Security, 2024, vol. 30, issue 1, pp. 82-87. https://doi.org/10.18372/2225-5036.30.18608. П.3. Технології програмування: навчальний посібник. Том 2. Сучасні технології програмування / Козюра В.Д., Ткач Ю.М., Хорошко В.О., Кузовков В.В., Хохлачова Ю.Є., Семендяй С.М. Ніжин: ФОП Лук'яненко В.В., ТПК "Орхідея", 2022., 300 с. П.4. 1. Інформаційна безпека держави : метод. вказівки до самост. роботи для здобувачів першого (бакалавр.) рівня вищ. освіти спец. 262 "Правоохоронна діяльність" / уклад.: Ю. М.Ткач, С. М. Семендяй. - Чернігів : НУ «Чернігівська політехніка», 2020. – 16 с. 2. Інформаційна безпека держави : метод. вказівки до практ. занять для здобувачів першого (бакалавр.) рівня вищ. освіти спец. 262 "Правоохоронна діяльність" / уклад.: Ю. М. Ткач, С. М. Семендяй. - Чернігів : НУ «Чернігівська політехніка», 2020. – 112 с. 3. Інформаційна безпека держави. Конспект лекцій для здобувачів вищої освіти освітнього ступеню «бакалавр» спеціальності 262 – «Правоохоронна діяльність»// Укл.: Ю.М.Ткач, С.М.Семендяй - Чернігів: НУ «Чернігівська політехніка», 2020. – 126 с. 4. Інформаційна безпека держави : конспект лекцій для здобувачів вищ. освіти освіт. ступеню «бакалавр» спец. 262 «Правоохоронна діяльність» / уклад.: Ю. М. Ткач, С. М. Семендяй. – Чернігів : НУ «Чернігівська політехніка», 2022. – 133 с. 5. Інформаційна безпека держави : метод. вказівки до самост. роботи для здобувачів першого (бакалавр.) рівня вищ. освіти спец. 262 "Правоохоронна діяльність" / уклад.: Ю. М. Ткач, С. М. Семендяй. – Чернігів : НУ «Чернігівська політехніка», 2022. – 19 с. 6. Комплексні системи захисту інформації : метод. вказівки до виконання курс. проєкту / уклад.: Ю. М. Ткач, С. М. Семендяй. – Чернігів : Національний університет «Чернігівська політехніка», 2021. – 132 с. 7. Основи криптографічного захисту інформації. Методичні вказівки до виконання курсової роботи для здобувачів першого (бакалаврського) рівня вищої освіти освітньо-професійної програми «Кібербезпека» спеціальності 125 Кібербезпека та захист інформації. / уклад.: М.А. Синенко, Ю.М. Ткач, М.Є. Шелест, С.М. Семендяй. – Чернігів: НУ «Чернігівська політехніка», 2024 – 40 с. 8. Технології програмування. Методичні вказівки до виконання лабораторних робіт для здобувачів першого (бакалаврського) рівня

							вищої освіти освітньо-професійної програми «Кібербезпека» спеціальності 125 Кібербезпека та захист інформації. / уклад.: І.М. Дюба, С.М. Семендяй, А.Г. Гребенник. – Чернігів: НУ «Чернігівська політехніка», 2024 – 42 с. 9. Кібербезпека та захист інформації. Методичні вказівки з технологічної практики для здобувачів першого (бакалаврського) рівня вищої освіти освітньо-професійної програми «Кібербезпека» спеціальності 125 Кібербезпека та захист інформації. / уклад.: Т.А. Петренко, Ю.М. Ткач, М.Є. Шелест, С.М. Семендяй. – Чернігів: НУ «Чернігівська політехніка», 2024 – 26 с. 10. Кібербезпека та захист інформації. Методичні вказівки з виробничої практики для здобувачів першого (бакалаврського) рівня вищої освіти освітньо-професійної програми «Кібербезпека» спеціальності 125 Кібербезпека та захист інформації. / уклад.: Т.А. Петренко, Ю.М. Ткач, М.Є. Шелест, С.М. Семендяй. – Чернігів: НУ «Чернігівська політехніка», 2024 – 25 с. 11. Адміністрування Unix-подібних систем. Конспект лекцій для здобувачів першого (бакалаврського) рівня вищої освіти освітньо-професійної програми «Кібербезпека» спеціальності 125 Кібербезпека та захист інформації. / уклад.: С.М. Семендяй, Т.А. Петренко, А.Г. Гребенник, Д.В. Кальченко. – Чернігів: НУ «Чернігівська політехніка», 2024 – 170 с. 12. Комп'ютерні мережі. Методичні вказівки до курсового проектування для здобувачів першого (бакалаврського) рівня вищої освіти освітньо-професійної програми «Кібербезпека» спеціальності 125 Кібербезпека та захист інформації. / уклад.: С.М. Семендяй, Т.А. Петренко, М.Є. Шелест, А.Г. Гребенник. – Чернігів: НУ «Чернігівська політехніка», 2024 – 40 с. 13. Комплексні системи захисту інформації. Методичні вказівки до курсового проектування для здобувачів першого (бакалаврського) рівня вищої освіти освітньо-професійної програми «Кібербезпека» спеціальності 125 Кібербезпека та захист інформації. / уклад.: С.М. Семендяй, Ю.М. Ткач, М.Є. Шелест. – Чернігів: НУ «Чернігівська політехніка», 2024 – 100 с. 14. Інциденти інформаційної безпеки. Методичні вказівки до виконання лабораторних робіт для здобувачів першого (бакалаврського) рівня вищої освіти освітньо-професійної програми «Кібербезпека» спеціальності 125 Кібербезпека та захист інформації. / уклад.: А.Г. Гребенник, Ю.М. Ткач, С.М. Семендяй. – Чернігів: НУ «Чернігівська політехніка», 2024 – 62 с. П.8. Відповідальний виконавець ДБТ, держфінансування, з 2025 р П.11. Здійснював наукове консультування установ, підприємств, організацій протягом не менше трьох років, зокрема ТОВ «Інформаційна безпека» (довідка). П.12. 1 Семендяй С.М. Співіснування BLUETOOTH з бездротовими мережами 802.11 / С.М. Семендяй // Новітні технології у науковій діяльності і навчальному процесі : Всеукраїнська науково-практична конференція студентів, аспірантів та молодих учених: збірник тез доповідей (м. Чернігів 19-20 квітня 2023 р.). - Чернігів : НУЧП, 2023. 2 Бакуменко Б.С. Методи шифрування та дешифрування на прикладі з CTF / Б.С. Бакуменко, С.М. Семендяй, Шелест М.Є. // Новітні технології у науковій діяльності і навчальному процесі : Всеукраїнська науково-практична конференція студентів, аспірантів та молодих учених: збірник тез доповідей (м. Чернігів 19-20 квітня 2023 р.). - Чернігів : НУЧП, 2023. 3 Семендяй С.М., Зайцев С.В. Метод забезпечення достовірності інформації в безпроводових засобах передачі даних за рахунок структурної адаптації та використання нейронних мереж /Безпека ресурсів інформаційних систем : тези доп. учасників І Міжнар. наук.-практ. конф.(м. Чернігів 16-17 квіт. 2020 р.) - Чернігів: Вид-во ЧНТУ, 2020. – С.182 – 185. 4 Семендяй С. Адаптивний метод вибору каналу зв'язку для застосування в БпЛА. Інформаційні технології у житі студентів та молодих науковців Закарпаття : зб. наук. праць за матеріалами VII регіональної наук.-практ. конф. (м. Ужгород, 30 листопада 2023 р.). Ужгород : УжНУ, 2023. С. 189–192. 5 Дмитренко С.В. Використання програмного забезпечення MATLAB для моделювання бездротових

							засобів передавання даних/ Дмитренко С.В., Семендяй С. М.// «ЮНІСТЬ НАУКИ – 2024»: XIV Міжнародна науково-практична конференція студентів, аспірантів та молодих учених: збірник тез доповідей (м. Чернігів 24-26 квітня 2024 р.). П.14. Керівництво постійно діючим студентським науковим гуртком "CybersecurityLab" кафедри кібербезпеки та математичного моделювання. П.19. Участь у професійних об'єднаннях за спеціальністю: ГО «Асоціація працівників кібербезпеки». П. 20. Досвід практичної роботи за спеціальністю становить 22 роки.
328102	Денисова Наталя Миколаївна	Доцент, Основне місце роботи	ННІ Природокористування та гуманітарних наук	Диплом спеціаліста, Таврійська державна агротехнічна академія, рік закінчення: 1999, спеціальність: 091901 Енергетика сільськогосподарського виробництва, Диплом спеціаліста, Таврійська державна агротехнічна академія, рік закінчення: 1999, спеціальність: 091902 Механізація сільського господарства, Диплом магістра, Таврійська державна агротехнічна академія, рік закінчення: 2000, спеціальність: 091902 Механізація сільського господарства, Диплом кандидата наук ДК 064146, виданий 22.12.2010, Атестат доцента 12ДЦ 034858, виданий 28.03.2013	24	ОК 2. Цивільний захист та охорона праців галузі	Підвищення кваліфікації: 1) Онлайн-тренінг «Керування ризиками стресу в системах управління безпекою праці та здоров'я працівників (стандарти BSI PAS 1010, ILO та ін.) сертифікат 3-0242 (4-6 листопада 2020 р.) 2) Науково-практичне стажування «Наука та освіта в умовах інформаційного суспільства: проблеми та перспективи» з 9.11.2020 по 17.11.2020. Свідоцтво 1 СПК 00051 від 20.11.2020 (3 кредити , 90 год.) 3) Навчання викладачів курсу «Охорона праці» в вищих навчальних закладах, Головний навчально-методичний центр Держпраці (4-8 листопада 2021р.), посвідчення №549-21 від 08.10.2021 р. 4) Курси підвищення кваліфікації НІПП за програмою «Сучасна інженерія» 20-31.05.2024, сертифікат № 00493698/ТМ00040-24 (60 год., 2 кред.) 5) Навчання викладачів курсу «Охорона праці» в вищих навчальних закладах, Головний навчально-методичний центр Держпраці (4-8 листопада 2024р.), посвідчення №282-24 від 08.10.2024 р. 6) Навчання педагогічних та науково-педагогічних працівників, які проводять навчання здобувачів фахової предвищої на початковому рівні (короткому циклі), першому (бакалаврському) та другому (магістерському) рівнях вищої освіти діям у НС, Навчально-методичний центр ЦЗ та БЖД Чернігівської області (27-30 травня 2025 р.), посвідчення № 24008743 від 30.05.2025 р. ПП 1, 4, 12, 14, 19 П.1. Буяльська Н. П., Денисова Н. М., Кузін А. О. Зниження впливу шкідливих антропогенних факторів на людину шляхом розробки раціону харчування в умовах забруднення ґрунту відходами війни//Технічнінауки та технології : науковий журнал / Національний університет «Чернігівська політехніка». –Чернігів : НУ «Чернігівська політехніка», 2025. – No 1(39). – С.231-240 П.4. 1) Цивільний захист та охорона праці в галузі : метод. вказівки до практ. занять / уклад.: Н. М. Денисова, Н. П. Буяльська. – Чернігів : НУ «Чернігівська політехніка», 2022. – 143 с. 2) Цивільний захист та охорона праці в галузі. Практикум для здобувачів вищої освіти другого (магістерського) рівня вищої освіти ОПП «Адміністративна та цивільна юстиція» зі спеціальності 081 Право, галузі знань 08 Право/Денисова Н.М. – Чернігів: НУ «Чернігівська політехніка», 2024. – 91 с. 3) Охорона праці в галузі та цивільний захист. Методичні вказівки до виконання лабораторних робіт для студентів галузі знань 18-Харчові технології/ Укл.: Денисова Н.М., Буяльська Н.П. – Чернігів: ЧНТУ, 2020. – 113 с. 4) Пожежна безпека будівель та споруд (Змістовий модуль 1. Сутність процесів горіння, розвитку пожеж і пожежогасіння). Конспект лекцій для ЗВО другого (магістерського) рівня спеціальності 192 – Будівництво і цивільна інженерія, галузі знань – 19 Архітектура і будівництво /Денисова Н.М. – Чернігів: НУ «Чернігівська політехніка», 2024. – 182 с. 5) Пожежна безпека будівель та споруд (Змістовий модуль 2. Системи попередження, обмеження розповсюдження, ліквідації та локалізації пожеж). Конспект лекцій для ЗВО другого (магістерського) рівня спеціальності 192 – Будівництво і цивільна інженерія, галузі знань – 19 Архітектура і будівництво /Денисова Н.М. – Чернігів: НУ «Чернігівська політехніка», 2025. – 164 с. 6) Пожежна безпека будівель та споруд. Лабораторний практикум для здобувачів вищої освіти другого (магістерського) рівня спеціальності 192 – Будівництво і цивільна

							інженерія, галузі знань – 19 Архітектура і будівництво /Денисова Н.М. – Чернігів: НУ «Чернігівська політехніка», 2025. – 67 с. П.12. 1. Шостак О.С., Денисова Н.М. Особливості функціонування системи управління охороною праці під час воєнного стану/ Комплексне забезпечення якості технологічних процесів та систем (КЗЯТПС – 2023) : матеріали тез доповідей XIII Міжнародної науково-практичної конференції (м. Чернігів, 25–26 травня 2023 р.) : у 2 т. / Національний університет «Чернігівська політехніка» [та ін.] ; відп. за вип.: Єрошенко Андрій Михайлович [та ін.]. – Чернігів : НУ «Чернігівська політехніка», 2023. – Т. 2. – С.353-354. 2. Труш М.В., Денисова Н.М. Основні шкідливі та небезпечні фактори на робочих місцях з ПЕОМ/ Комплексне забезпечення якості технологічних процесів та систем (КЗЯТПС – 2023) : матеріали тез доповідей XIII Міжнародної науково-практичної конференції (м. Чернігів, 25–26 травня 2023 р.) : у 2 т. / Національний університет «Чернігівська політехніка» [та ін.] ; відп. за вип.: Єрошенко Андрій Михайлович [та ін.]. – Чернігів : НУ «Чернігівська політехніка», 2023. – Т. 2. – С. 355-356. 3. Геращенко І. В., Денисова Н.М. Розроблення інноваційного методу поліпшення умов праці працівників тепличних господарств// I International Scientific and Practical Conference "Current methods of improving outdated technologies and methods", January 08-10, 2024, Bilbao, Spain - P.441-445. 4. Соколенко Ю.В., Денисова Н.М. Особливості розслідування нещасних випадків, які стались внаслідок військових (бойових) дій/ Актуальні питання економіки, фінансів, обліку та права: теорія і практика: збірник тез доповідей міжнародної науково-практичної конференції (Кременчук, 16 листопада 2023 р.). Кременчук: ЦФЕНД, 2023. - С.72-75 5. Денисова Н.М., Бузюн Д.С. Штучний інтелект у сфері безпеки праці //Meaningful artificial intelligence – 2024 : збірник матеріалів круглого столу, м. Київ, 26 січня 2024 р., ІПМЕ ім. Г.Є. Пухова НАН України. – 2024. – С.28-30. 6. Денисова Н. М., Буяльська Н. П. До проблеми формування раціону лікувально-профілактичного харчування працівників зі шкідливими та небезпечними умовами праці /Проблеми охорони праці, промислової та цивільної безпеки: Збірник матеріалів XXXI Всеукраїнської науково-методичної конференції (з участю студентів), м. Київ, 13 листопада 2024 р. – Електронне видання. – К.: КПІ ім. Ігоря Сікорського, 2024. – С.65-70. 7. Лабенок А. О., Денисова Н. М Пожежний нагляд в умовах воєнного стану/ Проблеми та перспективи реалізації та впровадження міждисциплінарних наукових досягнень: збірник наукових праць з матеріалами VIII Міжнародної наукової конференції, м. Конотоп, 20 грудня, 2024р.//Міжнародний центр наукових досліджень. -Вінниця: ТОВ «УКРЛОГОС Груп», 2024 – С.289-291. П.14 Керівництво студентом, який зайняв призове місце у II етапі Всеукраїнського конкурсу студентських наукових робіт з «Цивільна безпека в умовах воєнного стану, за темою «Формування екологічної свідомості, як елемент концепції «Smart-City» (Денисов Д.Ю., гр.ПЕ-221, диплом 1 ступеня, Національний університет цивільного захисту, м.Харків, 26.04.2024 р.) П.19 1. Міжнародна академія безпеки життєдіяльності, м. Київ, академік Міжнародної академії безпеки життєдіяльності, диплом від 11.11.2016 р. (протокол №59/16) 2. Асоційований член Європейського співтовариства з охорони праці, дата реєстрації 19.09.2019 р.
465921	Ларченко Марина Олександрівна	Доцент, Сумісництво	ННІ Електронних та інформаційних технологій	Диплом спеціаліста, Дніпропетровський державний університет, рік закінчення: 2000, спеціальність: 060101 Правознавство, Диплом магістра, Національний університет "Чернігівська політехніка", рік закінчення: 2022, спеціальність: 125 Кібербезпека, Диплом кандидата наук ДК 056222, виданий 18.11.2009, Атестат доцента 12ДЦ 029397, виданий 23.12.2011	21	ОК 5. Стандартизація, сертикація засобів та комплксів захисту інформації	Підвищення кваліфікації: 1. м. Львів, Міністерство цифрової трансформації України: - успішно завершила winter school "DATA ENGINEERING AND SECURITY 2025" з 20.01.2025 р. по 02.02.2025 р. – 120 год. /4 кредити ECTS/ (Сертифікат N°DES-2025-0628 від 02.02.2025 р.). 2. 12 вер. 2021 завершила Google Cloud Fundamentals: Core Infrastructure факультативний онлайн курс, підготовлений Google Cloud та запропонований освітньою платформою Coursera. Сертифікат Google Cloud від 12 вересня 2021 р. 3. Cisco Networking Academy Сертифікат про закінчення курсу Introduction to IoT від 19 квітня 2022 р.

							4. Python Institute. Statement of Achievement PCAP: Programming Essentials in Python. The graduate of the PCAP: Programming Essentials in Python course, provided by Cisco Networking Academy in collaboration with OpenEDG Python Institute. Certificate від 06.10.2022 р. 5. Навчання в магістратурі Національного університету "Чернігівська політехніка" з 01.09.2021 р. По 31.12.2022 р. Диплом з відзнакою М22 № 097768 від 31.12.2022 р. (90 кредитів ЄКТСЄКТС 6. Національний університет "Києво-Могилянська Академія. Курс "Кіберзахист для організацій" 17.03.25. Сертифікат № L6NyQXl4ya. 7. Cisco Networking Academy Сертифікат про закінчення курсу "Ethical Hacker" offered by Chernihiv National University of Technology through the Cisco Networking Academy program. Certificate 22 Aug 2025. 8. Сертифікат № LDA-2025-1452. Львівська академія дронів та оборонних технологій у Львівському національному університеті імені Івана Франка. 30 годин/1 кредит ECTS. 25.03.2025 - 28.03.2025. 9. Диплом за 3 місце у змаганнях проєктів у складі команди "ForensAI" із проєктом "CyberInsight" в межах DES-2025 П.1 Наукові публікації, проіндексовані в Scopus: 1. Larchenko, M. (2025). Development of a secure storage architecture for digital evidence. Technology Audit and Production Reserves, 3(2(83), 33–43. https://doi.org/10.15587/2706-5448.2025.329386 https://journals.uran.ua/tarp/article/view/329386 Фахові видання (категорія Б): 1. Марина Ларченко. Сучасні проблеми криптографічного захисту баз даних. Технічні науки та технології. Науковий журнал. 2022. № 3(29). С. 76-88. URL: http://tst.stu.cn.ua/article/view/268004/263774. 2. Ларченко, М. О. Моделювання злочинної поведінки методами ланцюгів маркова. Проблеми сучасних трансформацій. Серія: право, публічне управління та адміністрування, (15), 2025. https://doi.org/10.54929/2786-5746-2025-15-01-08 3. Ларченко М.О. Деякі особливості розслідування кіберзлочинів. Науковий вісник Львівського державного університету внутрішніх справ. Серія юридична. № 3 (2024). С. 70-77. URL: http://journals.lvduvs.lviv.ua/index.php/law/issue/view/74 4. Ларченко М.О. Застосування нейромережі Stable Diffusion для візуалізації злочинних сцен та моделювання кримінальних подій. Науковий вісник УжНУ. Серія «Право». Випуск 85(4). 2024. С. 118-124. DOI https://doi.org/10.24144/2307-3322.2024.85.4.16 5. Larchenko Maryna. Administrative and legal regulation of the use of radio frequency resources for UAVs under martial law. Philosophy, Economics and Law Review. Vol. 5, No. 1, 2025. https://doi.org/10.31733/2786-491X-2025-1-124 6. Ларченко М.О. Роль адміністративного права у протидії ворожим БПЛА в тилу: виклики та інституційна спроможність. Науковий вісник УжНУ. Серія «Право». Випуск 89. 2025. DOI: https://doi.org/10.24144/2307-3322.2025.89.3.1 7. Ларченко М.О. Моделювання злочинної поведінки методами ланцюгів Маркова. Проблеми сучасних трансформацій. Серія: право, публічне управління та адміністрування. №15 (2025). https://doi.org/10.54929/2786-5746-2025-15-01-08 8. Ларченко М.О., Ткач О.О. Юридичне оформлення процесу спадкування цифрових активів. Проблеми сучасних трансформацій. Серія: право, публічне управління та адміністрування. №13 (2024). https://doi.org/10.54929/2786-5746-2024-13-01-0 П.3 Монографії: 1. Maryna Larchenko. Modeling and Predicting Criminal Behaviour. World and Ukrainian Experience: LAP LAMBERT Academic Publishing, 2020. 508 p. (монографія, міжнародне видання категорії С). 2. Ларченко М.О. Кримінологічне моделювання та прогнозування злочинної поведінки: монографія. Ніжин: НДУ ім. М. Гоголя, 2019. 357 с. П.4 Навчально-методичні посібники: 1. Інформаційна безпека держави. Методичні вказівки до практичних занять для здобувачів першого (бакалаврського)

							рівня вищої освіти освітньо-професійної програми «Кібербезпека» спеціальності 125 Кібербезпека та захист інформації. / уклад.: М.О. Ларченко, Ю.М. Ткач.– Чернігів: НУ «Чернігівська політехніка», 2024 – 40 с. 2. Системи охорони державної таємниці. Методичні вказівки до практичних занять для здобувачів першого (бакалаврського) рівня вищої освіти освітньо- професійної програми «Кібербезпека» спеціальності 125 Кібербезпека та захист інформації. / уклад.: М.О. Ларченко, Ю.М. Ткач. – Чернігів: НУ «Чернігівська політехніка», 2024 – 26 с. 3. Електронний документообіг. Методичні вказівки до практичних занять для здобувачів першого (бакалаврського) рівня вищої освіти освітньо- професійної програми «Кібербезпека» спеціальності 125 Кібербезпека та захист інформації. / уклад.: М.О. Ларченко, Ю.М. Ткач. – Чернігів: НУ «Чернігівська політехніка», 2024 – 58 с. 4. Менеджмент інформаційної безпеки. Методичні вказівки до виконання розрахунково-графічної роботи для здобувачів першого (бакалаврського) рівня вищої освіти освітньо-професійної програми «Кібербезпека» спеціальності 125 Кібербезпека та захист інформації. / уклад.: Ю.М. Ткач, М.О. Ларченко. – Чернігів: НУ «Чернігівська політехніка», 2024 – 32 с. П. 8 Відповідальний виконавець наукової теми Методологія побудови захищеного кіберпростору 0124U004485 П.12 1. Ларченко М.О. Гармонізація національного законодавства з європейськими стандартами у сфері кібербезпеки. Матеріали V Міжнародної науково- практичної конференції «Кібербезпека в сучасному світі: актуальні виклики» 22 листопада 2024 року м. Одеса. 2. Ларченко М.О., Луняк М.Є. Інтеграція штучного інтелекту в бізнес-процеси для підвищення стійкості українських компаній. Матеріали Конференції «Інноватика в освіті, науці та бізнесі: виклики та можливості». Київський національний університет технологій та дизайну. 15.11.2024 р. 3. Ларченко М.О., Луняк М.Є. Застосування штучного інтелекту для протидії інформаційним атакам у соціальних медіа. Детермінанти відновлення та розвитку України. Збірник матеріалів II Міжнародної науково-практичної конференції (м. Чернігів, 28 червня 2024 року). Чернігів : ГО «Науково-освітній інноваційний центр суспільних трансформацій», 2024. DOI: https://doi.org/10.54929/conf_28_06_2024 4. Марина Ларченко. Застосування генетичного алгоритму у виявленні та аналізі цифрових слідів злочину. Юність науки – 2024 : збірник тез доповідей XIV Міжнародної науково-практичної конференції студентів, аспірантів і молодих вчених (м. Чернігів, 24-26 квітня 2024 р.). – Чернігів : НУ «Чернігівська політехніка», 2024. – 1440 с. С. 1116-1117. URL: https://ir.stu.cn.ua/handle/123456789/30262 5. Ларченко Марина. Правове забезпечення системи охорони державної таємниці. Актуальні дослідження суспільних наук : матеріали X Всеукр. наук. конф. (м. Умань, 28 берез. 2024 р.) / МОН України, Уманський держ. пед. ун-т імені Павла Тичини, Черкаський нац. ун-т імені Богдана Хмельницького [та ін.]; [голов. ред. А. Л. Бержанір ; редкол.: Я. М. Балановський, В. І. Пархета]. – Умань : Візаві, 2024. – 346 с. С. 314-317. 6. Марина Ларченко. Ефективність та проблеми використання кібернавігаційних та кіберпросторових методів у розслідуванні кіберзлочинів. Збірник праць. XIII міжнародна науково-технічна конференція «ITSEC», 9-11 травня 2024 р., Україна, м. Львів, 2024. 7. Ларченко М.О. Парадокси діджиталізації та готовність до цифрової трансформації. Сучасні вектори відновлення та розвитку України на засадах сталості та безпеки. Збірник матеріалів Міжнародної науково-практичної конференції (м. Київ, 21 листопада 2023 року). Чернігів : ГО «Науково-освітній інноваційний центр суспільних трансформацій», 2023. 274 с. DOI:

							https://doi.org/10.54929/conf_21_11_2023. С. 139-142. 8. Ларченко М.О. Прогнозування злочинної поведінки за допомогою штучних нейронних мереж / Матеріали V Міжнародної науково-практичної конференції "Інформаційна безпека та комп'ютерні технології": тези доповідей, 19–20 травня 2022 р. – Кропивницький: ЦНТУ, 2022. – 66 с. С. 16 – 17. 9. Ларченко Марина. Процеси інформаційно-технічного реформування в установах пенітенціарної системи. / Політичні трансформації сучасного суспільства : зб. матеріалів III Всеукр. наук.-практ. конф. (м. Полтава, 24 лютого 2022 р.). Полтава : ПДАУ, 2022. 187 с. С. 180 – 184. 10. Ларченко М.О. Використання комп'ютерних технологій при реформуванні пенітенціарної системи. / Матеріали I Міжнародного пенітенціарного форуму «Пенітенціарна система у глобальному вимірі» (29-30 жовтня 2021 р.) Рівне: Видавничий дім «Гельветика», 2021. - 140 с. С. 38 – 40. 11. Ларченко М.О. Інформаційні війни та правова освіта: формування цифрової гігієни серед студентів-правників. Міжнародній науково-практичній конференції «Вища освіта у період воєнного стану: сучасні виклики та проблемні питання», 2025. 12. Ларченко М.О. Кіберрозвідка і контррозвідка в Україні: правові межі під час воєнного стану. Матеріали VIII Міжнародного правничого форуму «Права людини та публічне врядування» (до 150-річчя заснування Чернівецького національного університету імені Юрія Федьковича) 30 травня 2025 року. 13. Ларченко М.О. Правові проблеми використання програмного забезпечення з відкритим кодом в державних структурах. Збірник XII Всеукраїнської науково-практичної конференції «Розвиток основних напрямів соціогуманітарних наук: проблеми та перспективи» (м. Кам'янське, 15 – 16 травня 2025 р.). 14. Ларченко М.О. Захист оперативної пам'яті як ключовий елемент державних інформаційних систем. VIII Міжнародна науково-практична конференція "Інформаційна безпека та комп'ютерні технології", 2025. 15. Ларченко М.О. Моделювання злочинних схем у кіберпросторі: цифрові докази та їх використання. Юність науки – 2025 : збірник тез доповідей XV Міжнародної науково-практичної конференції студентів, аспірантів і молодих вчених (м. Чернігів, 2025 р.). – Чернігів : НУ «Чернігівська політехніка», 2025. 16. Марина Ларченко. Цифрове профілювання кіберзлочинців на основі криміналістичних артефактів. ITSec: Безпека інформаційних технологій: матеріали XIV Міжнар. наук.-техн. конф., м. Тернопіль, 22-24 трав. 2025 р. Тернопіль-Київ: ЗУНУ-ДУІКТ, 2025. 243с.С. 122-123. П.14 Керівництво постійно діючим студентським науковим гуртком "CybersecurityLab" кафедри кібербезпеки та математичного моделювання. П.19 Участь у професійних об'єднаннях за спеціальністю: ГО «Асоціація працівників кібербезпеки». Участь у професійних об'єднаннях за спеціальністю: ГО «Наукова асоціація кібербезпеки України». (SCSA-UA).
328320	Литвин Світлана Володимирівна	Завідувачка кафедри / Доцент, Основне місце роботи	ННІ Природокористування та гуманітарних наук	Диплом спеціаліста, Ніжинський ордена Трудового Червоного Прапора державний педагогічний інститут ім.М.В.Гоголя, рік закінчення: 1990, спеціальність: англійська, німецька мова, Диплом магістра, Ніжинський державний університет імені Миколи Гоголя, рік закінчення: 2023, спеціальність: 035 Філологія, Диплом кандидата наук ДК 014822, виданий 12.06.2002, Атестат доцента 02ДЦ 011813, виданий 16.02.2006	31	ОК 1. Академічна англійська мова	Відповідає П 1, П 3, П 4, П 7, П 8, П 10, П 12, П 14. Підвищення кваліфікації 1. НУ ЧП Сертифікат в онлайн-школі «Конкурентоспроможність викладача сучасного закладу вищої освіти», 14-16 липня 2020 року 2. Сертифікат НАЗЯВО «Зміцнення викладання та організаційного управління в університетах» від 13.02.2021 3. DINTERNAL сертифікат DE-40-0802202116-3408 Єдиний вступний іспит з англійської мови для абітурієнтів у магістратуру: типи завдань та стратегії підготовки студентів до іспитів (08.02.21) 4. Сертифікат Дніпровська політехніка 1899 Назустріч викликам сьогодення: забезпечення якості мовної освіти в умовах змішаного навчання; № 6/12.03.21 від 12.03.2021 5. CERTIFICATE VI International Scientific and Practical Conference "INTERNATIONAL SCIENTIFIC INNOVATIONS IN HUMAN LIFE" 24 Hours of Participation (0,8 ECTS credits) MANCHESTER 15-17 December 2021 6. Certificate The Johns Hopkins University School of Nursing& The Ukrainian-American Concordia University "Covid-19 & Mental Health: Response and Management" January 27, 2022 7. Certificate № 2ПК05460798/765 "IntelR Skills Innovation" Initiative

							Training Chernihiv Polytechnic University 02-05 august 2022 (30 hours) 8. CERTIFICATE № CUPA12042024 of attendance Cambridge University Press & Assessment Seminar Svitlana Lytvyn studied the topics: Can We Trust AI? (0,03 кредиту ЄКТС) (12.04.24) 9. Сертифікат Британської Ради в Україні від 11.08.2025. Модуль 4. Фінанси, ресурси, проєкти Програми професійного розвитку академічних менеджерів. П 1 1. Юлія Ткач, Михайло Шелест, Леся Черниш, Світлана Литвин, Артур Бригинець Аналіз систем підтримки аудиту інформаційної безпеки / Technical Sciences and Technologies, 2020. №2 (20). - С. 203-209 2. Burmaka, I., Lytvynov, V., Skiter, I., & Lytvyn, S. Evaluating a blockchain-based network performance for the intrusion detection system. ISSN 1028-9763. Математичні машини і системи, 2020, No 19 - P. 99-109 3. Zaitsev S., Vasylenko V., Tkach Y., Posternak Y., Lytvyn S. Adeptive Selection of Turbo Code Paramaters in Wireless Data Trasmission Systems. ISBN: 978-3-030-89902-8. Mathematical Modeling and Simulation of Systems, 2021, № 20 - P.253-262 4. A. I. Sikaliuk, S. V. Lytvyn Educational terminological dictionaries: classification and methods of their composing // Вісник науки та освіти. Серія: «Філологія». - Вип. 5 (11). – К.: ГНО «Всеукраїнська асамблея докторів наук з державного управління», 2023. – С. 27-38 5. Sikaliuk A. I. Preconditions for appearance of computer lexicography / Sikaliuk A. I., Lytvyn S. V., Shevchenko Y. V. // Вісник науки та освіти. Серія: «Філологія». - Вип. 1 (19). – К. : .: ГНО «Всеукраїнська асамблея докторів наук з державного управління», 2024. - С. 79-89 П 3 Sikaliuk A. I., Lytvyn S.V. Modern lexicography: aspects of terminological dictionaries. Modern aspects of science: 34-th volume of the international collective monograph. Česká republika : Mezinárodní Ekonomický Institut, 2023. P. 95-116. (особистий внесок 1,5 друкованих арк.). П 4 1. Литвин С.В. Англійська мова для академічних цілей. Методичні вказівки до практичних занять для студентів всіх спеціальностей денної та заочної форм навчання освітнього ступеня «Магістр» / Укладачі: Литвин С. В., Сікалюк А. І., Пермінова В. А. – Чернігів : НУ «Чернігівська політехніка», 2021. – 44 с. П 7 1. Участь в якості офіційного опоненту у захисті дисертаційного дослідження Тулякової Катерини Робертівни «Методика навчання англомовного професійно орієнтованого монологічного мовлення майбутніх фахівців у сфері медіації та врегулювання конфліктів», поданого на здобуття наукового ступеня кандидата педагогічних наук за спеціальністю 13.00.02 – теорія і методика навчання (германські мови). Засідання спеціалізованої Вченої ради К 26.001.49 в Інституті філології Київського національного університету імені Тараса Шевченка (2020р.) П 8 Виконання функцій наукового керівника наукових тем: «Актуальні питання іншомовної освіти й комунікації: методичний та лінгвістичний аспекти». Державний реєстраційний №: 0122U201599, 11.22 - 05.25. П 10 Участь у програмі професійного розвитку академічних менеджерів у рамках реалізації проєкту світового банку «Удосконалення вищої освіти в Україні заради результатів» (Ukraine Improving Higher Education for Results Project – UIHERP). П 12 1. Khropatyi O.M., Lohinov O.V., Kazymyr V.V., Lytvyn S.V. The choice of hardware component for modified existing distributed simulation modeling system: Юність науки – 2020: соціально-економічні, соціально-економічні та гуманітарні аспекти розвитку суспільства: збірник тез доповідей X Міжнародної науково-практичної конференції студентів, аспірантів і молодих вчених (м. Чернігів, 23-24 квітня 2020 р.) / Національний університет «Чернігівська політехніка». – Чернігів: ЧНТУ, 2020. – С. 835-837 2. Lohinov O. V., PhD student in the department of information and computer systems, Supervisor - Kazymyr V. V., Doctor of Sciences, Professor, Lytvyn S. V., PhD, Associate Professor National University

							“Chernihiv Polytechnics” (Chernihiv, Ukraine). Embedded model system realization: Юність науки – 2021: соціально-економічні, соціально-економічні та гуманітарні аспекти розвитку суспільства: збірник тез доповідей XI Міжнародної науково-практичної конференції студентів, аспірантів і молодих вчених (м. Чернігів, 25-26 березня 2021 р.) / Національний університет «Чернігівська політехніка». – Чернігів, 2021. – С. 401-403 3. Khropatyi O. M., PhD student in the department of information and computer systems, Supervisor - Kazymyr V. V., Doctor of Sciences, Professor, Lytvyn S. V., PhD, Associate Professor Chernihiv Polytechnic National University (Chernihiv, Ukraine). Characteristics and operating principles of the e-net model system: Юність науки – 201: соціально-економічні, соціально-економічні та гуманітарні аспекти розвитку суспільства: збірник тез доповідей XI Міжнародної науково-практичної конференції студентів, аспірантів і молодих вчених (м. Чернігів, 25-26 березня 2021 р.) / Національний університет «Чернігівська політехніка». – Чернігів, 2021. – С. 433-435. 4. Dymerets A. V., PhD student in the department of electronics, automatics, robotics and mechatronics, Supervisors – Gorodny O. M., PhD, Associate Professor, Lytvyn S. V., PhD, Associate Professor National university «Chernihivska Politechnika» (Chernihiv, Ukraine). Quasi-resonant converters in unmanned aerial vehicle power supply systems: Юність науки – 2021: соціально-економічні, соціально-економічні та гуманітарні аспекти розвитку суспільства: збірник тез доповідей XI Міжнародної науково-практичної конференції студентів, аспірантів і молодих вчених (м. Чернігів, 25-26 березня 2021 р.) / Національний університет «Чернігівська політехніка». – Чернігів, 2021. – С. 442-444. 5. Andrii Khyzhniak, Svitlana Lytvyn. AN AUTOMATED SYSTEM FOR GENERATING PERSONALISED PRACTICAL TASKS AND THEIR AUTOMATIC ASSESSMENT IN DISTANCE LEARNING Юність науки – 2024: соціально-економічні та гуманітарні аспекти розвитку суспільства збірник тез доповідей XIV Міжнародної науково-практичної конференції студентів, аспірантів і молодих вчених (24-26 квітня 2024 р.). Чернігів: НУ «Чернігівська політехника», 2024. С. 761-763. 6. Kovalenko Ye. M., Lytvyn S.V. Moral and ethical challenges of digital transformation: balancing innovation and human values. Стратегічні орієнтири сталого розвитку в Україні та світі: збірник тез доповідей IV Міжнародної науково-практичної конференції молодих учених (м. Чернігів, 20 березня 2025 р.). Чернігів : НУ «Чернігівська політехніка», 2025. С. 275-277. П 14 1. Керівництво студентом (Грязнов О., гр. МКІ-232), який зайняв ІІ місце на ІІ етапі Всеукраїнського конкурсу студентських наукових робіт з англійської мови та комп’ютерних наук (1-31 березня 2024 р.) КПІ ім. Ігоря Сікорського (сертифікат НОД/125/24) 2. Керівництво студентом (Скосир А., гр. МКІ-231), який зайняв ІІ місце на ІІ етапі Всеукраїнського конкурсу студентських наукових робіт з англійської мови та комп’ютерних наук (1-31 березня 2024 р.) КПІ ім. Ігоря Сікорського (сертифікат НОД/125/24)

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

Програмні результати навчання ОП	ПРН відповідає результату навчання, визначеному стандартом вищої освіти (або охоплює його)	Обов’язкові освітні компоненти, що забезпечують ПРН	Методи навчання	Форми та методи оцінювання