НАЦІОНАЛЬНЕ АГЕНТСТВО ІЗ ЗАБЕЗПЕЧЕННЯ ЯКОСТІ ВИЩОЇ ОСВІТИ

ВІДОМОСТІ
про самооцінювання освітньої програми

Заклад вищої освіти	**Національний університет "Чернігівська політехніка"**
Освітня програма	**35717 Кібербезпека**
Рівень вищої освіти	**Магістр**
Спеціальність	**125 Кібербезпека**

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

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

Використані скорочення:

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

Загальні відомості

1. Інформація про ЗВО (ВСП ЗВО)

Реєстраційний номер ЗВО у ЄДЕБО	**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	**35717**
Назва ОП	**Кібербезпека**
Галузь знань	**12 Інформаційні технології**
Спеціальність	**125 Кібербезпека**
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; кафедра іноземних мов професійного спрямування; кафедра інформаційних та комп'ютерних систем**
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	**Завідувач кафедри**
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
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. 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, доктора педагогічних наук, доцента та членів проектної групи Шелеста Михайла Євгеновича, доктора технічних наук, професора, Гур'єва Володимира Івановича, кандидата технічних наук, доцента.
Рецензентами ОПП виступили провідні фахівці сфери захисту інформації, а саме: Смірнов Олексій Анатолійович, доктор технічних наук, 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.
Відгуки рецензентів позитивні.
ОПП затверджено Вченою радою Чернігівського національного технологічного університету (протокол від 27.08.2019 № 7) та введено в дію з 01.09.2019 наказом ректора від 27.08.2019 № 94. У 2020 р. до ОПП внесено зміни (затверджено Вченою радою Національного університету «Чернігівська політехніка», протокол від 24.02.2020 № 2).
Спеціальність 125 Кібербезпека за другим (магістерським) рівнем
у 2019 р. пройшла ліцензування (наказ МОН України від 06.03.2019 № 1753-л.) з
ліцензованим обсягом – 60 осіб з урахуванням строків навчання.

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

Рік навчання	Навчальний рік, у якому відбувся набір здобувачів відповідного року навчання	Обсяг набору на ОП у відповідному навчальному році	Контингент студентів на відповідному році навчання станом на 1 жовтня поточного навчального року	У тому числі іноземців
			ОД	*ОД*
1 курс	2020 - 2021	14	22	0
2 курс	2019 - 2020	8	8	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	**4023 Кібербезпека**
другий (магістерський) рівень	**35717 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	83628	38679
Власні приміщення ЗВО (на праві власності, господарського відання або оперативного управління)	83580	38632
Приміщення, які використовуються на іншому праві, аніж право власності, господарського відання або оперативного управління (оренда, безоплатне користування тощо)	47	47
Приміщення, здані в оренду	6430	1725

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

8. Документи щодо ОП

Документ	Назва файла	Хеш файла
Освітня програма	*ОПП 125 Кібербезпека магістр 2019 зміни 2020.pdf*	iXUtICs1HftCWxpLvlUVLU5GkeS2KpZr0UfFe7a0jkc=
Освітня програма	*ОПП 125 Кібербезпека магістр 2019 .pdf*	DQuzI9C/Z41y83loXCjCgFOyqTbP3YfIqKLkgPgtLXo=
Навчальний план за ОП	*НП 125 Кібербезпека магістр 2020 А.pdf*	G81XmBSXRStFz+GA1qkV3WtVTsTloJGX9aRdLu25yWE=
Навчальний план за ОП	*НП 125 Кібербезпека магістр 2019 А.pdf*	JcHcYW7/VhTDphxLrKodsoEAYk6rvqb6jZSWyWNhaTg=
Рецензії та відгуки роботодавців	*Рецензії магістр ОПП Кібербезпека 2020.pdf*	g52b3IZXzRtWNT6FCp+dVokiMlXbHMHo5o7VSEDxExI=
Рецензії та відгуки роботодавців	*РЕЦЕНЗІЯ ОПП Лисиця.pdf*	f9gDq04SleqjYhP+oevZAPQMOA710m1fA8oocHPOcRY=

1. Проектування та цілі освітньої програми

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

Мета ОПП - забезпечити студентам фундаментальну підготовку у вигляді поглиблених теоретичних і практичних знань, умінь та навичок за спеціальністю 125 Кібербезпека, достатніх для ефективного виконання завдань інноваційного характеру відповідного рівня професійної діяльності в галузях телекомунікацій та інформаційних технологій, захищеності інформаційного і кіберпросторів держави в цілому або окремих суб'єктів їх інфраструктури від ризику стороннього кібернетичного впливу.
Особливістю ОПП є те, що при її розробці, проектною групою було враховано Стратегію розвитку Національного університету «Чернігівська політехніка» (на 2015-2020 роки), а також досвід розробки аналогічних програм як вітчизняних (Київський університет імені Бориса Грінченка, Національний авіаційний університет, Національного університету "Львівська політехніка" тощо) так і закордонних, наприклад, Техніко-гуманітарна академія Бельсько-Бяли (Польща).
Унікальність ОПП полягає в широкому спектрі працевлаштування випускників ОПП, як в ІТ індустрії, за сприяння ІТ-кластер, так і в державних органах (Служба безпеки України, кіберполіція, Управління державного спеціального зв'язку в Чернігівській області тощо).
Навчання на ОПП дає можливість отримати високоякісну фахову освіту, яка ґрунтується на технологіях активного навчання й сучасній матеріально-технічній базі, та у поєднанні з можливостями розвитку соціальних навичок є достатньою для ефективного виконання завдань інноваційного характеру в галузі ІТ та інформаційної безпеки.

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

Місією НУ «Чернігівська політехніка» є розвиток суспільства через освіту та наукові дослідження задля формування лідерства та вирішення глобальних проблем світу, що змінюється
Шляхи реалізації своєї місії Університет вбачає у досягненні таких стратегічних цілей https://www.stu.cn.ua/staticpages/misiya/.
Цілі освітньої програми цілком відповідають місії та стратегії Національного університету «Чернігівська політехніка», оскільки ОПП спрямована на підготовку висококваліфікованих фахівців, які володіють широкими фундаментальними знаннями
та практичними знаннями й навичками, здатних працювати у команді та адаптуватись до змінних вимог ринку праці й технологій, що швидко розвиваються.
Також ОПП передбачає налагодження зв'язків із закордонними ЗВО з метою отримання студентами подвійних дипломів: програма спільний диплом Техніко-гуманітарна академія у Бельсько-Бялій (Польща), ухвала Сенату УББ

№1551/07/VI/2020 від 14.07.2020р. та рішення вченої ради ЧНТУ №5 від 30.06.2020р. Разом з тим, у студентів-магістрів ЗВО є можливість проходження паралельного навчання у інших закордонних закладах освіти (магістри першого року навчання), з отриманням подвійного диплому українського та польського https://stu.cn.ua/announcement/310/.
Отже, ОПП є органічною складовою стратегії НУ «Чернігівська політехніка», що реалізує ключові пріоритети імплементації стратегічного бачення розвитку університету як сучасного університету міжнародного рівня.

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

При розробці ОПП було враховано пропозиції випускників спеціальності 125 «Кібербезпека» бакалаврського рівня. Проект освітньої програми обговорювався із випускним курсом (ІБ-151, протокол №2 від 04.10.18р.) спеціальності 125 «Кібербезпека» з метою встановлення їх бачення та очікувань щодо магістерської програми спеціальності. За їх пропозицією до ПРН включено: проводити та планувати навчання персоналу компанії, користувачів з інформаційних технологій організації у відповідності до сучасних норм, вимог, внутрішніх правил безпечного застосування інформаційних технологій, а також у відповідність вітчизняним і світовим стандартам галузі інформаційної та\або кібербезпеки.
Члени проектної групи при формуванні цілей та визначенні програмних результатів навчання (ПРН) враховували напрацювання в даному напрямку інших ЗВО, а саме Національного авіаційного університету та Національного університету «Львівська Політехніка», де магістерська програма з інформаційної безпеки впроваджувалась вже протягом багатьох років.
Під час перегляду ОПП задля врахування думки стейкхолдерів та узгодженості освітніх програм підготовки з міжнародними колегами (протокол № 10 від 28.01.2020р.) було проведено усне опитування магістрів з кібербезпеки 1 курсу щодо їх враження від ОПП та бакалаврів з кібербезпеки 4 курсу щодо їх очікувань від магістратури, також були проведені спільні зустрічі із стейкхолдерами (протокол №7, 29.11.2019, №10 від 28.01.2020 р. (https://mmi.stu.cn.ua/novyny/spetsialnist-kiberbezpeka-yakoyu-yiyi-bachat-robotodavtsi/).

- роботодавці

Для розробки ОПП “Кібербезпека” запрошувались
директор ІТ-кластеру, представники кіберполіції, директор ТОВ «Інформаційна безпека» (протокол засідання кафедри від 04.10.2018 р.№2).
Так, наприклад, директор ІТ-кластеру внесла пропозицію добавити освітні компоненти, пов’язані із налагодженням системи мережевої безпеки на рівні операційної системи та звернути увагу на технології програмування. Крім того, запропонувала розширити перелік баз практик, зокрема здійснювати практичну підготовку здобувачів вищої освіти, які навчаються за ОПП на підприємствах ІТ-кластеру.
Представник ТОВ «Інформаційна безпека» вніс пропозицію щодо необхідності вивчення питань, пов’язаних із нормативно-правовим забезпеченням профільної галузі.
Вище згадані пропозиції були враховані в розробці ОПП та навчального плану 2019-2020н.р.
Під час перегляду ОПП, представники роботодавців, зауважили, що здобувач вищої освіти повинен мати глибокі теоретичні та практичні знання в галузі інформаційних технологій та інформаційної безпеки, вміти застосовувати набуті знання в практичній діяльності. Тому, директор ІТ-кластеру Лисиця І. зазначила, що питання аудиту інцидентів інформаційної безпеки сьогодні виходить на перший план, а тому мають бути обов’язковими для вивчення. Представник кіберполіції Коган М. зазначив, що можливо студентів зацікавлять освітні компоненти, пов’язані із криміналістикою. Дані пропозиції роботодавців були враховані під час перегляду ОПП.

- академічна спільнота

Інтереси та пропозиції академічної спільноти були враховані при формулюванні цілей, компетентностей, ПРН ОПП. Обговорення відбувалося на засіданнях проектної та робочої груп. Зокрема, були враховані пропозиції фахівців, які працюють у сфері захисту інформації Національного авіаційного університету та НУ «Львівська політехніка». Один із рецензентів від академічної спільноти Смірнов Олексій Анатолійович, доктор технічних наук, професор, завідувач кафедри кібербезпеки та програмного забезпечення Центральноукраїнського національного технічного університету. Представники робочої групи й НПП кафедри кібербезпеки та математичного моделювання брали участь у всеукраїнських та міжнародних конференціях, зокрема, на базі НУ «Чернігівська політехніка» у квітні 2020 року у І Міжнародній науково-практичній конференції «Безпека ресурсів інформаційних систем», в ході яких науковці галузі інформаційної безпеки визначали сучасні тенденції розвитку відповідної галузі, завдання, які перед нею постають, та можливі шляхи їх розв’язання, що знайшло відображення в ОПП. За результатами співпраці із провідними фахівцями-практиками та науковцями галузі формулювались програмні результати ОПП.

- інші стейкхолдери

Іншими стейкхолдерами є територіальна громада Чернігова, успішність якої залежить від розвитку місцевої економіки та людського капіталу, чому в більшій мірі сприяє Університет. Згідно з місією та поставленими цілями Університет відіграє важливу роль у житті міста, покращуючи освітню, наукову сфери міста та його кадровий потенціал. Наразі реалізація ОПП "Кібербезпека" сприяє збільшенню висококваліфікованих фахівців, які працевлаштовуються в тому числі і в місцевих фірмах ІТ галузі, примножуючи та розвиваючи тим самим економіку міста.

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

Ринок праці вимагає висококваліфікованих фахівців, які матимуть теоретичну і практичну базу з питань забезпечення інформаційної безпеки (кібербезпеки). Сьогодні за інформацією Національного інституту стратегічних досліджень в Україні спостерігається дефіцит фахівців у сфері кібербезпеки (https://niss.gov.ua/doslidzhennya/informaciyni-strategii/kiberbezpeka-v-umovakh-rozgortannya-chetvertoi-promislovoi).

Сучасний розвиток інформаційних технологій та інформаційної безпеки відбувається в багатьох напрямках, зокрема, криптозахист інформації, технічний та програмний захист інформації, організаційний тощо. Всі ці тенденції базуються на знаннях ключових засад безпеки з кожного напрямку і враховані в програмних результатах навчання ОПП за ОК "Методи побудови та аналізу криптосистем", "Проектування технічних систем захисту інформації" та ін.

Підтвердженням цьому є також структурно-логічна схема навчання, що реалізується в навчальному плані ОПП та конкретизується в робочих програмах навчальних дисциплін.

Тісна співпраця університету із роботодавцями дозволила студентам спеціальності 125 Кібербезпека проходити у різних профільних підприємствах, установах та організаціях переддипломну, що сприятиме працевлаштуванню випускників ОПП.

Крім того, специфіка сучасного ринку праці вимагає від здобувачів розвинутих соціальних навичок (Soft Skills), що також враховано в ОПП.

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

Під час формулювання цілей та ПРН програми було враховано галузевий контекст у плані визначення загальних пріоритетів сфери ІТ технологій та інформаційної безпеки, бачення процесу підготовки та подальшої діяльності фахівців із захисту ІТ систем та мереж. Галузевий контекст навчання за ОПП відображається повною мірою у практичній підготовці фахівців з кібербезпеки, результати навчання яких є релевантними реальним умовам їх подальшої праці. Регіональний контекст був врахований за пропозиціями ІТ компаній регіону (через ІТ кластер), котрі зацікавлені у фахівцях, які володіють наступними результатами навчання: проектувати, впроваджувати та супроводжувати ІКС, забезпечувати захист інформаційних ресурсів мереж установи на базі сучасних моделей, методів і засобів передачі даних в комутативних, тощо. Обов'язкові компоненти, що забезпечують дані результати: «Управління мережевою безпекою», «Аудит та управління інцидентами ІБ», «Стандартизації, сертифікація засобів та комплексів захисту інформації». Силові структури регіону також зацікавлені у фахівцях, які здатні розробляти, впроваджувати та організовувати реалізацію процесів з використанням методів та засобів криптографічного та технічного захисту інформації на об'єктах інформаційної діяльності згідно з визначеною політикою інформаційної безпеки та/або кібербезпеки і стратегії організації, що забезпечують освітні компоненти «Проектування технічних систем захисту інформації», «Методи побудови та аналізу криптосистем».

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

Було проведено аналіз ОПП за спеціальністю 125 Кібербезпека ЗВО України, які знаходяться у відкритому доступі. Такими ОПП є: «Безпека інформаційних і комунікаційних систем» Київський університет імені Бориса Грінченка, «Адміністративний менеджмент в сфері захисту інформації» Національний авіаційний університету, «Кібербезпека» ТНТУ імені Івана Пулюя, «Кібербезпека» КНУ імені Тараса Шевченка; «Системи технічного захисту інформації» НТУ України «КПІ імені Ігоря Сікорського» тощо.

Вивчення проводилось шляхом порівняння цілей, компетентностей і програмних результатів навчання зазначених ОПП.

Подібні програми існують і в закордонних університетах, зокрема в Техніко-гуманітарній академії у Бельсько-Бяла (Польща).

Зміст ОПП ураховує також зміст професійних програм сертифікації на платформах Cisco (https://www.netacad.com/courses/security), Prometheus (https://courses.prometheus.org.ua/courses/KPI/IS101/2014_T1/info).

Аналіз зазначених програм виявив, що кожна з програм має свою специфіку, яка відповідає спеціальності, а також регіональному контексту.

У результаті аналізу зазначених вище освітніх програм та враховуючи регіональний контент в ОПП було включено актуальні освітні компоненти, наприклад, «Технології IoT та блокчейн», «Безпека в хмарних технологіях» та інші.

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

Стандарт вищої освіти за спеціальністю 125 Кібербезпека галузі знань 12 Інформаційні технології для другого (магістерського) рівня вищої освіти відсутній.

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?

Другий (магістерський) рівень вищої освіти згідно із Національною рамкою кваліфікацій відповідає сьомому кваліфікаційному рівню, згідно з яким студент має набути: спеціалізовані уміння/навички розв'язання проблем,

необхідні для проведення досліджень та/або провадження інноваційної діяльності з метою розвитку нових знань та процедур; здатність інтегрувати знання та розв'язувати складні задачі у широких або мультидисциплінарних контекстах; здатність розв'язувати проблеми у нових або незнайомих середовищах за наявності неповної або обмеженої інформації з урахуванням аспектів соціальної та етичної відповідальності .
Відповідно до запропонованої ОПП у студентів буде сформовано інтегральну компетентність «Здатність розв'язувати складні спеціалізовані задачі та практичні проблеми у галузі забезпечення інформаційної безпеки і\або кібербезпеки, що характеризується комплексністю та неповною визначеністю умов»
Сформована інтегральна компетентність повністю відповідає НРК.
Отже, програма спрямована на розв'язання складних завдань в умовах невизначеності, креативність та генерацію нових ідей здобувачами ВО (інноваційність), що
повністю відповідає сьомому (магістерському) рівню національної рамки кваліфікацій.

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)?

0

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 ОП відповідає предметній області заявленої для неї спеціальності. Це демонструється через об'єкти, цілі, інструменти та обладнання ОПП, а також через інші компоненти ОПП.
Так, об'єктами професійної діяльності випускників згідно з ОПП є: об'єкти інформатизації, включаючи комп'ютерні, автоматизовані, телекомунікаційні, інформаційні, інформаційно-аналітичні, інформаційно-телекомунікаційні системи, інформаційні ресурси і технології; технології забезпечення інформаційної безпеки; процеси управління інформаційною та/або кібербезпекою об'єктів, що підлягають захисту.
Цілями навчання є: забезпечити здобувачам вищої освіти (ЗВО) фундаментальну підготовку у вигляді поглиблених теоретичних і практичних знань, умінь та навичок за спеціальністю 125 Кібербезпека, достатніх для ефективного виконання завдань інноваційного характеру відповідного рівня професійної діяльності в галузях телекомунікацій та інформаційних технологій, захищеності інформаційного і кіберпросторів держави в цілому або окремих суб'єктів їх інфраструктури від ризику стороннього кібернетичного впливу.
Інструменти та обладнання: системи забезпечення моніторингу та контролю процесів інформаційної та/ або кібербезпеки; сучасне програмно-апаратне забезпечення інформаційно-комунікаційних технологій.
Знання студент отримує шляхом оволодіння методами, методиками та технологіями забезпечення кібербезпеки, використовуючи системи розробки, забезпечення, моніторингу та контролю кібербезпеки, а також програмно-апаратне забезпечення кібербезпеки, розташоване у навчальних лабораторіях НУ «Чернігівська політехніка».
Напрямки захисту інформації такі як криптозахист, мережевий, технічний захист інформації, безпекові технології програмування, особливості стандартизації, сертифікації засобів та комплексів захисту інформації, а також аудит та управління інцидентами інформаційної безпеки представлені обов'язковими дисциплінами навчального плану за ОПП.

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

Здобувачі вищої освіти мають можливість формувати індивідуальну освітню траєкторію навчання відповідно до «Порядку запису студентів на вивчення вибіркових навчальних дисциплін в Чернігівському національному технологічному університеті» (https://www.stu.cn.ua/media/files/pdf/p-vibdis.pdf) і і університет має всі необхідні інструменти для цього. Вибіркові дисципліни розміщені у варіативній частині навчального плану та становлять 24 (ОПП 2020)/23(ОП 2019) кредитів ЄКТС, що становить не менш як 25 відсотків загальної кількості кредитів ЄКТС, передбачених для даного рівня вищої освіти. На гарантів освітніх програм, завідувачів випускових кафедр, керівників/заступників інституту ННІ ЕІТ покладено надання кваліфікованих консультацій щодо формування індивідуальної освітньої траєкторії.

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

Процедуру вибору вибіркових дисциплін регламентує «Порядок запису студентів на вивчення вибіркових навчальних дисциплін в Чернігівському національному технологічному університеті», що затверджений наказом

ректора ЧНТУ від 30.11.2015 року №197 https://www.stu.cn.ua/media/files/pdf/p-vibdis.pdf .
Порядок запису студентів на вивчення вибіркових навчальних дисциплін передбачає надання до інститутів робочих навчальних планів та коротких анотацій дисциплін (силабусів), які згідно з ОП є вибірковими. Інститути ознайомлюють студентів із порядком запису на вивчення вибіркових дисциплін та із переліком вибіркових дисциплін. Свій вибір дисциплін здобувач здійснюється шляхом подачі письмової заяви на ім'я директора інституту. За результатами (поданими заявами) розпорядженням по інституту формуються списки студентів академічних груп за обраними дисциплінами.
Мінімальна кількість студентів 15 осіб.
Магістр, який з поважних причин (хвороба, академічна мобільність тощо) не записався на вибіркові дисципліни, має право зробити такий запис протягом першого робочого тижня після того, як він з'явився на навчання.
Якщо вивчення вибіркової дисциплін розпочинається в другому семестрі, то процедура проведення запису на курс здійснюється до 01 листопада поточного навчального року.
Інформація про вибіркові дисципліни заноситься до індивідуального плану здобувача вищої освіти.
З метою врахування останніх нововведень у законодавстві, удосконалення механізму формування індивідуальної освітньої траєкторії у 2020-2021 н.р. введено в дію оновлений «Порядок запису здобувачів вищої освіти на вивчення вибіркових навчальних дисциплін у Національному університеті «Чернігівська політехніка», затверджений наказом ректора від 31.08.20 р. № 26 https://www.stu.cn.ua/media/files/pdf/nzop/p-vib-dis.pdf Даний порядок передбачає, що здобувачі вищої освіти будуть здійснювати свій вибір шляхом самостійного обрання зі списку запропонованих їм для вивчення дисциплін у системі дистанційного навчання Moodle Університету.

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

До ОПП «Кібербезпека» магістерського рівня входить освітня компонента «Практика переддипломна», що проводиться в 3 семестрі, обсягом 11 кредитів. Переддипломна практика проводиться у відповідності до «Положення про проведення практики здобувачів вищої освіти Національного університету «Чернігівська політехніка» (https://www.stu.cn.ua/media/files/pdf/nzop/p-prakt.pdf). Переддипломна практика формує компетентності відповідно до ОПП. Угоди з підприємствами-базами практики укладаються або на час практики, або можуть бути довготривалими – на строк до 5 років. Список баз практики для магістерської ОПП можна знайти на сайті https://robota-chntu.stu.cn.ua/practice/, наприклад ТОВ «ІНТРОБОТС», ПАТ Чернігів обленерго та ін.
Здобувачі ВО мають можливість самостійно обирати базу проходження переддипломної практик, враховуючи прагнення щодо майбутнього працевлаштування, особисті професійні нахили та уподобання, так укладено договори на проходження практики з ТОВ «Інформаційна безпека», Відділ протидії кіберзлочинам в Чернігівські області Департаменту кіберполіції НП України, Чернігівська обласна державна адміністрація тощо. Основними підсумками переддипломної практики є те, шо студенти закріплюють та поглиблюють на практиці теоретичні знання у сфері захисту інформації, формують професійні уміння та навички, що сприятимуть прийняттю самостійних рішень у реальних виробничих умовах, шляхом виконання окремих завдань і функцій, властивих майбутній професії; набувають досвід самостійної науково-дослідної роботи та ін.

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

Наповнення освітньо-професійної програми відповідними освітніми компонентами
дозволяє здобувачам оволодіти комплексом соціальних/універсальних (soft skills) навичок, притаманних сучасному фахівцю. Серед soft skills, що формуються за ОПП, є оволодіння здібностями креативного мислення, управління інформацією, уміння формувати власну думку та приймати рішення, а також уміннями працювати в команді тощо. Формуванню soft skills сприяють такі освітні компоненти ОПП, як переддипломна практика, іноземна мова професійного спрямування, методологія та організація наукових досліджень, аудит та управління інцидентами інформаційної безпеки та ін., у ході вивчення яких студенти навчаються аналізувати, верифікувати, оцінювати повноту та достовірність інформації, за необхідності її доповнювати й синтезувати відсутню, продукувати нові ідеї, формувати власну думку та приймати рішення.
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.

Яким чином зміст ОП ураховує вимоги відповідного професійного стандарту?

Професійний стандарт за спеціальністю 125 Кібербезпека галузі знань 12 Інформаційні технології для другого (магістерського) рівня вищої освіти відсутній. Професійна кваліфікація не надається.

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

Фактичне навантаження здобувачів вищої освіти становить 90 кредитів (2700 годин), та містить 15 освітніх компонентів. Обсяг годин аудиторного навантаження за різними видами складає 1/3, обсяг годин самостійної роботи здобувачів
вищої освіти – 2/3 від загальної кількості годин теоретичного навчання з кожної дисципліни, хоча можлива корекція обсягу годин пропорційно кількості тижнів теоретичного навчання.
Зміст самостійної роботи здобувача вищої освіти над конкретною навчальною дисципліною визначається робочою

програмою дисципліни, методичними
матеріалами, завданнями та вказівками викладача.

Опитування студентів 2-го курсу на предмет чи вистачає їм часу на самостійну роботу показало, що 50% студентів вважають так, що фактичне навантаження цілком співвідноситься із обсягом освітніх компонентів, решта оцінила свою задоволеність фактичним навантаженням (включно із самостійною роботою) за десятибальною шкалою на 7 - 25%, 8-13%, 9-13 %. Що дає нам підстави стверджувати, що обсяг навантаження є незавищеним, а час, виділений на самостійну роботу, є оптимальним.

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

Дуальна форма освіти за ОПП «Кібербезпека» не передбачена. Проте, роботодавці активно беруть участь у реалізації ОПП, в тому числі і через проведення гостьових лекцій («Положення про організацію та проведення гостьових лекцій у Національному університеті «Чернігівська політехніка»» https://www.stu.cn.ua/media/files/pdf/nzop/p-gostl.pdf).

3. Доступ до освітньої програми та визнання результатів навчання

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

https://stu.cn.ua/staticpages/pravilapriem/

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

Згідно з правилами прийому до НУ "Чернігівська політехніка" https://stu.cn.ua/media/files/pdf/pp-cntu2020-6.pdf, якими визначаються строки всіх етапів вступної компанії та порядок розгляду апеляцій на результати вступних випробувань. Вступ на магістерську ОПП "Кібербезпека" відбувається на основі здобутої вищої освіти рівня бакалавр або магістр (ОКР спеціаліста) за конкурсом.
Зарахування за ОПП «Кібербезпека» другого (магістерського) рівня здійснюється на основі ступеня бакалавра, магістра та освітньо-кваліфікаційного рівня спеціаліста, здобутого за вказаною спеціальністю (напрямом підготовки) або за іншими, за умови успішного проходження вступних випробувань (ЄВІ або іноземна мова та фахове вступне випробування) з урахуванням середнього бала відповідного додатка до диплома.Програма вступного випробування за даною ОПП розроблена кафедрою кібербезпеки та математичного моделювання та доступна https://stu.cn.ua/media/files/fvv/125-mag-1.pdf. Відомості про результати вступних випробувань та інших конкурсних показників вносяться до запису про вступника в ЄДЕБО.

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

Визнання результатів навчання в інших ЗВО регламентується в НУ "Чернігівська політехніка" «ПОРЯДОКОМ визначення академічної різниці та перезарахування навчальних дисциплін у Національному університеті «Чернігівська політехніка» https://www.stu.cn.ua/media/files/pdf/nzop/p-akad-rizn.pdf , «ПОЛОЖЕННЯМ про організацію освітнього процесу в Національному університеті «Чернігівська політехніка» https://www.stu.cn.ua/media/files/pdf/nzop/p-org-osp.pdf та «ПОЛОЖЕННЯМ про академічну мобільність учасників освітнього процесу Національного університету «Чернігівська політехніка» https://www.stu.cn.ua/media/files/pdf/nzop/p-akad-mob.pdf .
В останньому зазначаються організаційне забезпечення, мета та цілі, а також процедура визнання та перезарахування результатів навчання студентів у виші-партнері.
Положенням про організацію освітнього процесу в НУ "Чернігівська політехніка" передбачається, що загальний обсяг додаткових кредитів, які здобувач вищої освіти може отримати за навчальний рік, не може перевищувати 20 кредитів за рік.
У «Порядку визначення академічної різниці та перезарахування навчальних дисциплін у Національному університеті «Чернігівська політехніка» прописані поняття академічної різниці, підстави та порядок перезарахування навчальних дисциплін, яке можливе у
випадку, якщо назви навчальних дисциплін ідентичні, а кількість кредитів, навчальної дисципліни відрізняється менше, ніж на 25%, або назви мають незначну стилістичну відмінність, а обсяги та змістова частина не відрізняються.

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

За час реалізації ОПП випадків визнання результатів навчання, отриманих в інших ЗВО, не було.

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

процесу?

Університетом можуть бути визнані результати навчання, здобуті шляхом неформальної освіти.
Процедуру визнання результатів навчання отриманих у неформальній освіті регулює «ПОРЯДОК визначення академічної різниці та перезарахування навчальних дисциплін у Національному університеті «Чернігівська політехніка»» (https://www.stu.cn.ua/media/files/pdf/nzop/p-akad-rizn.pdf). Згідно з яким здобувач вищої освіти, який пройшов таке навчання, має звернутися до директора інституту із відповідною заявою про перезарахування отриманих кредитів. Позитивне рішення про перезарахування може бути прийняте на підставі наданих здобувачем вищої освіти документів про проходження літньої школи, семінару, тренінгу, тощо та за умови відповідності останніх освітній програмі й компетентностям передбаченим ООП.

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

За ОПП «Кібербезпека» другого (магістерського) рівня вищої освіти конкретних прикладів застосування процедури визнання результатів навчання, отриманих у неформальній освіті, не було.
Однак, слід відмітити, що на ОПП здобувачі ВО під менторством Базилевича В.М. в 2019-2020 навчальному році проходили курс на платформі https://www.coursera.org/learn/cloud-security-basics/, результати якого були зараховані замість виконання лабораторного практикуму з курсу “Безпека в хмарних технологіях”.

4. Навчання і викладання за освітньою програмою

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

Організаційні форми освітнього процесу та основні види навчальних занять в НУ “Чернігівська політехніка” регламентуються «ПОЛОЖЕННЯМ про організацію освітнього процесу в Національному університеті «Чернігівська політехніка» https://www.stu.cn.ua/media/files/pdf/nzop/p-org-osp.pdf та ОПП https://op.stu.cn.ua/files/op/%D0%9E%D0%9F%D0%9F%20%20125%20%D0%9A%D1%96%D0%B1%D0%B5%D1%80%D0%B1%D0%B5%D0%B7%D0%BF%D0%B5%D0%BA%D0%B0%20%D0%BC%D0%B0%D0%B3%D1%96%D1%81%D1%82%D1%80%202019%20%D0%B7%D0%BC%D1%96%D0%BD%D0%B8%202020.pdf
На ОПП застосовуються як традиційна система методів і прийомів, так і інтерактивні методики викладання. Їх відповідність програмним результатам навчання по кожному освітньому компоненту представлена в робочих програмах навчальних дисциплін, оприлюднених на сайті https://mmi.stu.cn.ua/predmety/.
За Положенням основними видами навчальних занять в Університеті є: лекція; лабораторне, практичне, семінарське, індивідуальне заняття; консультація.
Всі робочі програми також розміщені в порталі дистанційного навчання НУ “Чернігівська політехніка” https://eln.stu.cn.ua/login/index.php.
Форми і види навчальних занять, а також методи навчання та викладання, що добираються викладачем, корелюються із програмними результатами навчання.
Таким чином, форми та методи навчання і викладання на ОП сприяють досягненню програмних результатів навчання.

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

Студентоцентрований підхід є одним з основних принципів освітньої діяльності Університету, що зазначено у ПОЛОЖЕННІ про організацію освітнього процесу в Національному університеті «Чернігівська політехніка» https://www.stu.cn.ua/media/files/pdf/nzop/p-org-osp.pdf
Даний підхід проявляється у регулярних опитуваннях студентів з метою встановлення зворотного зв’язку щодо рівня задоволеності та якості. Так, серед магістрів другого курсу за результатами першого року навчання було проведено анкетування, серед питань якого розглядався рівень задоволеності методами навчання та викладання. За результатами опитування було встановлено, що магістри цілком задоволені обраними викладачами підходами до навчання, незадоволених методами навчання та викладання студентів немає.
Зазначимо, що по закінченню першого року навчання у системі дистанційного навчання Moodle https://eln.stu.cn.ua/ гарантом проводилось багатоаспектне опитування здобувачів даної ОП. Результати опитування розглядались на засіданні кафедри (Протокол №1 від 27.08.20).

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

Поняття академічна свобода тлумачиться у Положенні про організацію освітнього процесу в Національному університеті «Чернігівська політехніка» https://www.stu.cn.ua/media/files/pdf/nzop/p-org-osp.pdf . Принципів академічної свободи на ОПП «Кібербезпека» дотримуються як з боку закладу освіти, так і з боку викладачів. Зокрема, викладачі можуть обирати форми та методи навчання з відповідних дисциплін, які найкраще відповідатимуть досягненню програмних результатів навчання. За необхідності можуть винести на розгляд засідання кафедри питання щодо перерозподілу обсягів між видами аудиторних занять, або ж – щодо зміни обсягу дисципліни. Магістри ОПП можуть: реалізовувати академічну мобільність; здобувати неформальну освіту;

поєднувати навчання, дослідження, професійну діяльність; за власними науковими інтересами обирати тему випускної кваліфікаційної роботи, керівника ВКР; у ході взаємодії з викладачами визначати оптимальні методи і технології навчання. Таким чином, на ОПП у повній мірі реалізуються принципи академічної свободи, оскільки передбачається максимальна варіативність методів навчання та викладання з урахуванням свободи слова й творчості.

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 *

Загальна інформація про особливості освітньої діяльності за ОПП надається магістрам на організаційних зборах перед початком навчання. Інформація щодо змісту, структури, мети вивчення дисципліни, очікуваних результатів навчання,
порядку та критеріїв оцінювання надається магістрам на першому занятті з кожної
дисципліни, а також на настановчих зборах з практики.
Ще один спосіб інформування студентів це створення груп в різних месенджерах
з окремих дисциплін, де викладач в будь-який момент може надати
консультацію здобувачу ВО, зокрема, і щодо зазначених питань.
Такі форми інформування дозволяють здобувачам вищої освіти отримати повну інформацію щодо цілей, змісту та очікуваних результатів навчання, порядку та критеріїв оцінювання у межах окремих освітніх компонентів ОПП.

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

Поєднання навчання і досліджень під час реалізації ОПП базується на принципах наукової творчості, відкритості, рівності прав, добровільності, академічної доброчесності. Головною характеристикою такого навчання є зорієнтованість освітнього середовища на формування у здобувачів здатності застосовувати знання для вирішення науково-дослідних, практичних завдань.
Студенти, що навчаються на ОПП, долучаються до наукових досліджень,
що проводять викладачі кафедри (номер реєстрації 0117U003187 “Методи та засоби забезпечення безпеки ресурсів інформаційних систем”). Вони є співавторами наукових публікацій, наприклад, студенти гр. МКБп-191 Бригинець А. та Біленький Г. у співавторстві опублікували статті у фахових виданнях.
Два магістри взяли участь у І Міжнародній науково-практичній конференції «БЕЗПЕКА РЕСУРСІВ ІНФОРМАЦІЙНИХ СИСТЕМ» (квітень, 2020, Чернігів, НУ «Чернігівська політехніка»), організованій випусковою кафедрою за ОПП. Значна частина магістрів взяла участь у щорічній Всеукраїнській науково-практичній конференції молодих науковців, аспірантів «Новітні технології у науковій діяльності і навчальному процесі».
При викладанні переважної більшості фахових дисциплін оволодінню навчальним матеріалом сприяє використання форм і методів навчання, заснованих на дослідженнях.

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

Згідно з «ПОЛОЖЕННЯМ про організацію освітнього процесу в Національному університеті «Чернігівська політехніка» обов’язковим є оновлення робочої програми дисципліни один раз на рік. Оскільки зміни у галузі Інформаційних технологій відбуваються дуже швидко, то викладачі, які задіяні у реалізації ОПП, систематично оновлюють навчально-методичні матеріали дисциплін.
Зміст окремих освітніх компонентів коригується на основі сучасних наукових досягнень в галузі (основним інструментом для цього є досвід участі НПП в міжнародних та всеукраїнських наукових конференціях, круглих столах, семінарах, на яких обговорюються сучасні практики та наукові досягнення в галузі), а також на основі імплементації зарубіжного досвіду (за результатами стажування НПП освітньої програми).
Отриманий НПП досвід у вищезазначених заходах дозволяє вносити корективи до змісту освітніх компонентів ОНП та навчальних занять на основі кращих сучасних практик.
Крім того, гарантом програми та викладачами постійно здійснюється системний аналіз публікацій, які висвітлюють наукові питання галузі. Ця інформація аналізується, систематизується, що дозволяє виробити рекомендації щодо оновлення
змісту освітніх компонентів ОНП.
Відповідальним за контроль щодо оновлення змісту навчальних програм є гарант ОПП, який узгоджує робочі програми з дисциплін ОПП, розроблені викладачами.

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

В Університеті чітко окреслена Стратегія інтернаціоналізації Національного університету «Чернігівська політехніка» на 2021-2027 роки https://www.stu.cn.ua/media/files/pdf/nzop/strategia-inter.pdf .
Інтернаціоналізації освітньої програми сприяє можливість проходження магістрами лабораторного циклу курсу «Безпека в хмарних технологіях» на основі он-лайн платформи Cursera англійською мовою з зарахуванням результатів https://www.coursera.org/learn/cloud-security-basics/
В університеті створені всі умови для проходження стажування у закордонних університетах, що сприятиме ознайомленню здобувачів вищої освіти з світовими здобутками. Наприклад, гарант ОПП Ткач Ю.М., проходила закордонне науково-педагогічне стажування на базі Техніко-гуманітарній академії м. Бельсько-Бяла (Польща) з 10 листопада до 08 грудня 2018 року.
В Університеті діє відділ міжнародного співробітництва, який повідомляє НПП та студентів про відкриті можливості

академічної мобільності (Положення про академічну мобільність учасників освітнього процесу Національного університету «Чернігівська політехніка» https://www.stu.cn.ua/media/files/pdf/nzop/p-akad-mob.pdf).
За час реалізації ОПП прикладів академічної мобільності ще не було, проте кафедра активно працює у цьому напрямку. Наразі узгоджено програму подвійних дипломів за ОПП між Університетом та Техніко-гуманітрною академією у Бельсько-Бялій, ухвала Сенату УББ №1551/07/VI/2020 від 14.07.2020р. та рішення вченої ради Університету №5 від 30.06.2020 р.

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

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

Основними нормативними документами, які регламентують перевірку досягнень програмних результатів навчання є Положення про організацію освітнього процесу (https://www.stu.cn.ua/media/files/pdf/nzop/p-org-osp.pdf), Положення про поточне та підсумкове оцінювання знань студентів (https://www.stu.cn.ua/media/files/pdf/nzop/p-pprocin.pdf). З метою всебічного оцінювання ПРН магістрів застосовується усний (індивідуальне, фронтальне опитування, співбесіда, презентація, виступ ін.) та письмовий контроль або їх комбінація (тестування; виконання індивідуальних
завдань, творчої роботи, аналітичного дослідження для перевірки сформованості інтегральної компетентності), комп'ютерний контроль, у т .ч. тестове опитування, що використовується для об'єктивізації оцінювання, самоконтроль – для розвитку у здобувачів уміння оцінювати свої досягнення.
Основними видами контролю є проміжний і підсумковий. Проміжний проводиться на всіх видах аудиторних занять та під час виконання самостійної роботи. Підсумковий контроль - іспит чи залік; з практики – звітування, з курсової роботи/проекту, випускної кваліфікаційної роботи - захист.
Семестровий контроль проводиться за обсягом, визначеним робочою програмою навчальної дисципліни, у формі екзамену, заліку, відповідно до навчального плану у терміни, передбачені графіком освітнього процесу і оцінюється за національною шкалою та шкалою ЄКТС.
Зазначені форми контрольних заходів у межах навчальних дисциплін ОПП дозволяють перевірити досягнення програмних результатів навчання.

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

Критерії оцінювання навчальних досягнень висвітлені в робочих програмах, які розміщуються на порталі дистанційної освіти Університету https://eln.stu.cn.ua/,
вони є заздалегідь оприлюдненими для здобувачів та доступними в будь-який момент часу та з будь-якого місця.
Чіткість та зрозумілість форм контрольних заходів та критеріїв оцінювання навчальних досягнень здобувачів вищої освіти забезпечуються ґрунтовним підходом кафедри до їх планування і формулювання; своєчасним висвітленням необхідної інформації; установчими зборами перед практиками; проведенням поточних консультацій.

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

Основними документами, що регламентують форми контрольних заходів та критерії оцінювання є «Положенні про поточне та підсумкове оцінювання знань здобувачів вищої освіти НУ «Чернігівська політехніка» https://www.stu.cn.ua/media/files/pdf/nzop/p-pprocin.pdf та «Положенні про організацію освітнього процесу в Національному університеті «Чернігівська політехніка» https://www.stu.cn.ua/media/files/pdf/nzop/p-org-osp.pdf .
На початку навчального року на сайті Університету розміщується графік освітнього процесу (https://stu.cn.ua/staticpages/grafik/) із зазначенням атестаційних тижнів, розклад навчальних занять та проведення контрольних заходів (https://schedule.stu.cn.ua/view/schedule.php), який доводиться до здобувачів вищої освіти не пізніше, ніж за місяць до початку екзамену та за тиждень до початку залікового тижня. Робочі програми навчальних дисциплін з переліком форм контрольних заходів і критеріїв оцінювання доступні здобувачам вищої освіти на дистанційній платформі Moodle. Також кожен викладач вже на першому занятті ознайомлює із формами контрольних заходів та критеріями оцінювання за дисципліною. Опитування магістрів вказало, що всі здобувач ВО задоволені рівнем інформаційної підтримки. Зручним та ефективним інформування стосовно різних аспектів навчання вважають 63% опитаних студентів (10 балів), 25% поставили по 9 балів, 13% - по 8 балів.

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

Стандарт вищої освіти за спеціальністю 125 Кібербезпека галузі знань 12 Інформаційні технології для другого (магістерського) рівня вищої освіти відсутній. В ОПП «Кібербезпека» другого (магістерського) рівня формою атестації є захист випускної кваліфікаційної роботи.
Випусковою кафедрою розроблено методичні вказівки з випускної кваліфікаційної роботи для ОПП «Кібербезпека», в яких розкрито всі основні питання щодо процедури написання, оформлення, подачі на кафедру та захисту випускної кваліфікаційної роботи.

Яким документом ЗВО регулюється процедура проведення контрольних заходів? Яким чином

забезпечується його доступність для учасників освітнього процесу?

Процедура проведення контрольних заходів регламентується «Положенням про поточне та підсумкове оцінювання знань здобувачів вищої освіти НУ «Чернігівська політехніка» https://www.stu.cn.ua/media/files/pdf/nzop/p-pprocin.pdf
Доступність для учасників освітнього процесу забезпечується через вільний доступ до вищезгаданого документу на веб-сайті університету.
Конкретні процедури проведення екзаменів, заліків, захисту індивідуальних завдань, тощо наводяться у відповідних робочих програмах дисциплін в розділі «Методи контролю».
Робочі програми з кожної дисципліни, у яких в розділі "Методи контролю" визначені процедури проведення різних видів контролю, розміщені на порталі дистанційної освіти Університету https://eln.stu.cn.ua/, що робить їх доступними для студентів.

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

Об'єктивність екзаменаторів забезпечується чітко виписаними процедурами проведення контрольних заходів та критеріями оцінювання ПРН. У разі виникнення питань щодо об'єктивності екзаменаторів та конфлікту інтересів здобувач вищої освіти може звернутися із письмовою заявою (апеляцією) на ім'я директора, після чого створюється комісія з трьох НПП для приймання екзамену, до складу якої включаються завідувач відповідної кафедри, науково-педагогічні працівники за фахом дисципліни та представники органів студентського самоврядування задля забезпечення об'єктивності екзаменаторів. Відповідна процедура прописана у «Положенні про поточне та підсумкове оцінювання знань здобувачів вищої освіти НУ «Чернігівська політехніка». З метою забезпечення зворотнього зв'язку із здобувачами вищої освіти щодо об'єктивності оцінювання в НУ "Чернігівська політехніка" працює «гаряча лінія», «скриньки довіри», розміщені в різних корпусах Університету, та електронна пошта dovira_chntu@ukr.net, куди здобувачі ВО можуть подати свої анонімні зауваження про необ'єктивність під час складання контрольних заходів, порушення академічної доброчесності, тощо.
За період навчання магістрів за програмою, що акредитується, конфлікту інтересів не виникало. Скарг студентів на упередженість та необ'єктивність екзаменаторів не було.

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

Повторне проходження контрольних заходів здійснюється згідно з «Положенням про поточне та підсумкове оцінювання знань здобувачів вищої освіти НУ «Чернігівська політехніка». У цьому положенні вводяться основні поняття та описуються процедури щодо перескладання контрольних заходів. Здобувачам вищої освіти, які під час семестрового контролю одержали незадовільні оцінки (в тому числі й враховуючи неявку на екзамен (залік) без поважних причин) з дисциплін, сумарний обсяг яких не перевищує 20 кредитів, дозволяється ліквідувати академічну заборгованість. Для ліквідації академзаборгованості складається розклад ліквідаційної сесії та доводиться студентам через різні інформаційні ресурси, зокрема сайт університету, дистанційну платформу Moodle, а також через соціальні мережі, месенджери, наприклад повідомлення в загальних групах студентів або групах з дисциплін.
Скарг студентів на упередженість та необ'єктивність екзаменаторів не було.

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

У "Положенні про поточне та підсумкове оцінювання знань здобувачів вищої освіти НУ «Чернігівська політехніка» прописано процедуру подання та розгляду апеляцій на результати проведення контрольних заходів.
Згідно з цим положенням, для оскарження подається заява на ім'я директора, Розпорядженням по інституту створюється комісія у складі трьох осіб: завідувач кафедри, науково-педагогічні працівники за фахом дисципліни та представники органів студентського самоврядування. Головою АК призначається директор. Апеляція подається особисто здобувачем ВО не пізніше наступного робочого дня після оголошення оцінки. Результати роботи комісії оформлюються протоколом, який підписують всі члени та здобувач, що подав апеляцію.
За період навчання магістрів за програмою, що акредитується, оскарження процедури та результатів проведення контрольних заходів не було. Конфлікту інтересів не виникало. Скарг студентів на упередженість та необ'єктивність екзаменаторів не було.

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

В Університеті розроблена і дотримується нормативна база щодо політики, стандартів і процедур забезпечення академічної доброчесності. Політика, стандарти і процедури дотримання академічної доброчесності регламентуються «Кодексом академічної доброчесності Національного університету «Чернігівська політехніка»» https://stu.cn.ua/media/files/pdf/nzop/p-yakist-kodex.pdf та «Порядком проведення перевірки кваліфікаційних робіт здобувачів вищої освіти на
плагіат в НУ «Чернігівська політехніка»» https://www.stu.cn.ua/media/files/pdf/nzop/p-plagiat.pdf. Розроблено та затверджено «Положення про комісію з питань академічної доброчесності НУ «Чернігівська Політехніка»» https://www.stu.cn.ua/media/files/pdf/nzop/p-yakist-komis.pdf. Наказом ректора Університету (https://www.stu.cn.ua/media/files/pdf/akd-n3.pdf) щороку затверджується склад комісії з питань академічної доброчесності НУ «Чернігівська політехніка». Також на сторінці університету в Нормативній базі

(https://www.stu.cn.ua/staticpages/pi-yakist/) знаходиться ціла низка допоміжних документів щодо дотримання питання академічної доброчесності.

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

До інструментів протидії порушенню академічної доброчесності на ОПП можна віднести: попереднє експертне оцінювання та самооцінювання; технічна перевірка щодо наявності ознак академічного плагіату у текстах, підготовлених до друку із використанням як безкоштовного програмного забезпечення (наприклад, «eTXT Антиплагіат» та «Advego plagiatus») https://stu.cn.ua/staticpages/akadem-dobrochesnist/ та спеціалізованого програмного забезпечення для виявлення плагіату(UniCheck); використання для проведення контрольних заходів аудиторій, обладнання відеокамерами (частина аудиторій навчального корпусу №1, в якому ведеться підготовка здобувачів за ОПП, була обладнана відеокамерами, що унеможливлює списування при проведенні письмових іспитів).
З метою запобігання порушень академічної доброчесності у наукових публікаціях (статтях, дисертаціях, монографіях тощо) бібліотекою НУ "Чернігівська політехніка" здійснюється перевірка за допомогою спеціалізованого програмного засобу Unichek, що використовується в Університеті на умовах договору, та надається експертна оцінка щодо відсутності/наявності академічного плагіату.

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

З метою дотримання принципів академічної доброчесності та запобігання проявам їх порушення в НУ "Чернігівська політехніка" розроблено комплекс профілактичних заходів, який також використовується на ОПП, що акредитується, а саме, обов'язкове інформування/пропагування учасників освітнього процесу про необхідність дотримання принципів та норм академічної чесності шляхом проведення циклу тренінгів з основ академічного письма, етики та доброчесності, із захисту прав
інтелектуальної власності та трансферу технологій, з проектно-орієнтованої діяльності в науковій та підприємницькій діяльності; розповсюдження методичних пропагандних матеріалів; ознайомлення всіх учасників освітнього процесу із нормами Кодексу академічної доброчесності Національного університету «Чернігівська політехніка» (https://www.stu.cn.ua/media/files/pdf/nzop/p-yakist-kodex.pdf).
Крім того, до ОПП включено дисципліну "Методологія та організація наукових досліджень", одним із завдань якої є вивчення методологічних основ проведення наукових досліджень, а дотримання принципів академічної доброчесність є одним з ключових моментів наукового дослідження.
Також керівники під час підготовки випускної кваліфікаційної роботи магістра ознайомлюють ЗВО із принципами дотримання академічної доброчесності, положеннями та процедурами.

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

Кодексом академічної доброчесності Національного університету «Чернігівська політехніка» (https://www.stu.cn.ua/media/files/pdf/nzop/p-yakist-kodex.pdf)передбачено адміністративну та дисциплінарну відповідальність за недоброчесну поведінку у вигляді повторного проходження оцінювання (контрольна робота, екзамен, залік тощо), відповідного освітнього компонента освітньої програми, відрахування з Університету, позбавлення академічної стипендії.
За ОПП «Кібербезпека» випадків порушення академічної доброчесності не було.

6. Людські ресурси

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

Одним з провідних чинників якості надання освітніх послуг університетом є професіоналізм науково-педагогічного персоналу. Відповідно, рівень професіоналізму викладачів є головним критерієм проходження ними конкурсного добору, який регламентується ПОРЯДКОМ ПРОВЕДЕННЯ КОНКУРСНОГО ВІДБОРУ ПРИ ЗАМІЩЕННІ ВАКАНТНИХ ПОСАД НАУКОВО-ПЕДАГОГІЧНИХ ПРАЦІВНИКІВ У НАЦІОНАЛЬНОМУ УНІВЕРСИТЕТІ «ЧЕРНІГІВСЬКА ПОЛІТЕХНІКА» https://www.stu.cn.ua/media/files/pdf/nzop/p-kv-vakant.pdf . Згідно із зазначеним вище документом у конкурсі на заміщення вакантних посад НПП можуть брати участь особи, які здобули повну вищу освіту і за своїми професійно-кваліфікаційними якостями відповідають вимогам, викладеним у Порядку. До всіх посад також висуваються такі додаткові вимоги, як володіння англійською мовою на рівні не нижче В1, вміння користуватися комп'ютерною технікою, мати опубліковані наукові праці, індекс Гірша на рівні не менше одиниці за даними Google Scholar; мати повний пакет навчально-методичних документів, в т.ч. для дистанційної форми навчання (Moodle – система управління курсами).
Претенденту можуть запропонувати провести пробну лекцію або практичне (лабораторне, семінарське) заняття. На цьому занятті мають бути присутні члени призначеної методичної комісії Університету, що дасть можливість довести
необхідний рівень професіоналізму претендента.

Опишіть, із посиланням на конкретні приклади, яким чином ЗВО залучає роботодавців до

організації та реалізації освітнього процесу

Кафедра, що забезпечує реалізацію ОПП, залучає до аудиторних занять професіоналів-практиків, представників роботодавців, запрошуючи їх для проведення лекційних і практичних занять та тренінгів.
Так, ІТ кластером тільки протягом 2019-2020 років організовано та проведено більше 20-ти івентів та дві олімпіади з програмування (https://www.facebook.com/Chernihiv.IT/events/?ref=page_internal)
Щороку восени відбувається кафедральний Meetup «Актуальні питання кібербезпеки» до міжнародного дня захисту інформації та навесні Всеукраїнська науково-практична конференція молодих науковців, аспірантів «Новітні технології у науковій діяльності і навчальному процесі» до проведення яких залучаються представники роботодавців. Зокрема на них запрошуються представники ІТ кластеру, представники відділу протидії кіберзлочинам в Чернігівській області Департаменту кіберполіції НП України та ін. Так у 2020 році семінар відвідав HR однієї з більших ІТ компаній Чернігова Jevera (https://mmi.stu.cn.ua/novyny/chernihiv-it-conference-manage-it/).
Факти проведення даних заходів висвітлені в ФБ (https://www.facebook.com/cnut.cybersec/posts/1316086225242508) та на сайті кафедри https://mmi.stu.cn.ua/novyny/chernihiv-it-conference-manage-it/
Перелік установ, з якими укладено угоди про співпрацю (https://robota-chntu.stu.cn.ua/practice/).

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

Зазначимо, що частина викладачів, які задіяні на ОПП мають досвід практичної роботи за фахом. Зокрема, Шелест М.Є., професор кафедри, генерал-лейтенант, заслужений діяч науки і техніки України, Лауреат державної премії України в галузі науки та техніки, повний кавалер ордену "За заслуги", д.т.н., професор, протягом багатьох років проходив службу у Службі зовнішньої розвідки України, Петренко Т.А., к.т.н., доцент кафедри, більш ніж 5 років займав посаду інженера-програміста.
До проведення аудиторних занять на ОП залучені професіонали-практики. Так, у 2019-2020 н.р. дисципліну "Проектування технічних засобів захисту інформації" викладав д.т.н., доцент, директор ТОВ «Інформаційна безпека» Зайцев С.В. У 2020-2021 н.р. він буде долучений до освітнього процесу із гостьовими лекціями.
Представники роботодавців часто погоджуються проводити одиничні гостьові лекції та семінари для здобувачів ОПП, які йдуть поза межами навчального плану. У 2019 року була проведена відкрита лекція з протидії загрозам інформаційним загрозам держави
(https://www.facebook.com/cnut.cybersec/videos/vb.417165525134587/890988204650662/?type=2&theater) та чотириденний курс навчання, організований Чернігівським ІТ кластером (https://mmi.stu.cn.ua/novyny/uchast-v-programi-prosvita/).

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

В Університеті діє ПОЛОЖЕННЯ про підвищення кваліфікації та стажування педагогічних і науково-педагогічних працівників НУ "Чернігівська політехніка" https://www.stu.cn.ua/media/files/pdf/nzop/p-pidv-kval.pdf . У цьому положенні запропоновано цілісну систему підвищення кваліфікації та стажування. Навчання працівників здійснюється за такими видами: довгострокове підвищення кваліфікації; короткострокове підвищення кваліфікації (семінари, семінари-практикуми, семінари-наради, семінари-тренінги, тренінги, вебінари, «круглі столи» тощо).Отже, НУ "Чернігівська політехніка" постійно дбає про професійний розвиток викладачів. Свідченням цьому є те, що науково-дослідною частиною та міжнародним відділом університету здійснюються регулярні розсилки анонсів конференцій, грантів, в яких пропонується приймати участь викладачам ОПП. Таким чином, викладачі ОП мають можливість проходити наукові стажування за кордоном, і якщо тривалість стажування не перевищує три місяці, їм виплачується середня заробітна плата та
зберігається посада на строк до 1 року.
Слід відзначити, що гарант ОПП пройшла стажування за кордоном на базі Техніко-гуманітарній академії м. Бельсько-Бяла (Польща) з 10 листопада до 08 грудня 2018 року.
Також, в університеті проводяться різноманітні тренінги та семінари для викладачів (зокрема, з підготовки грантових заявок, з написання та подачі наукових статей до наукометричних баз даних Scopus, Web of Science тощо), що сприяє розвитку викладачів.

Продемонструйте, що ЗВО стимулює розвиток викладацької майстерності

ЗВО стимулює розвиток викладацької майстерності через систему заохочення викладачів за досягнення. Зокрема, в НУ "Чернігівська політехніка" діє «Положення про преміювання співробітників за результатами наукових досліджень
» (https://www.stu.cn.ua/media/files/pdf/nzop/p-premnau.pdf
Згідно з «Положенням про щорічне оцінювання науково-педагогічних працівників і кафедр Національного університету «Чернігівська політехніка»» https://www.stu.cn.ua/media/files/pdf/p-ocinnpp3.pdf щорічно оцінюються наукові, навчальні та інші здобутки викладачів. За результатами цього оцінювання десять кращих НПП отримують зменшене на 10% навчальне навантаження на наступний навчальний рік при збереженні рівня заробітної плати. Також за результатами щорічного оцінювання відбувається нагородження дипломами, грамотами, іншими відзнаками.
Відповідно до цього ж положення науково-педагогічних працівників, які у звітному році стали авторами опублікованих наукових праць у періодичних виданнях, включених до Scopus або Web of Science, отримують премії.

7. Освітнє середовище та матеріальні ресурси

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

Освітня діяльність з підготовки здобувачів вищої освіти забезпечується матеріально-технічною базою Університету, яка відповідає ліцензійним вимогам та вимогам провадження освітньої діяльності. В Університеті проводиться постійна робота над поліпшенням матеріально-технічної бази. У навчальному корпусі, де здійснюється підготовка за ОПП, є достатня кількість аудиторій та комп'ютерних класів. Значна частина лекційних аудиторій обладнана мультимедійними проекторами, лабораторні роботи з фахових дисциплін проводяться в лабораторіях з залученням комп'ютерної техніки, а також спеціалізованого лабораторного обладнання, наприклад генератор шуму для силової мережі "Базальт 2ГС", багатофункціональний пошуковий пристрій Andre Advanced тощо.
Університет забезпечує студентів та НПП вільним доступом до інтернету, до фондів та електронних каталогів наукової бібліотеки Університету. Кафедра кібербезпеки та математичного моделювання має свій веб-сайт (https://mmi.stu.cn.ua/). Все необхідне для реалізації ОПП навчально-методичне забезпечення розміщено на сервері дистанційного навчання MoodleЧНТУ (https://eln.stu.cn.ua/). Навчально-методичне забезпечення ОПП дає можливість досягати визначених програмою цілей та програмних результатів навчання завдяки його максимальній змістовій насиченості та постійному оновленню.

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

Освітнє середовище, створене в Університеті, дозволяє задовольнити потреби та інтереси здобувачів вищої освіти, що навчаються за ОПП. Це відбувається завдяки збалансованості матеріальних умов і сприйняття здобувачів як рівноправних партнерів. З метою виявлення та врахування потреб та інтересів здобувачів вищої освіти, які навчаються за ОПП, проводились бесіди із магістрами, консультації з представниками студентського самоврядування. Гарантом ОПП проведено опитування студентів, які навчаються за ОПП «Кібербезпека», щодо важливості/якості роботи бібліотеки, їдальні, місць для самостійної роботи, розкладу, роботи студради, куратора, порталу дистанційного навчання.
Результати анкетування показали: абсолютно задоволені рівнем (на 10 за дестибальною шкалою) консультативної підтримки (на кафедрі, у деканаті, бібліотеці) - 63%, рівнем соціальної підтримки (проживання, харчування, стипендії, соціальна допомога та ін.) - 50%, цілком незадоволених освітнім середовищем не виявлено.

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

ЗВО забезпечує безпечність освітнього середовища для життя та здоров'я здобувачів вищої освіти через суворе дотриманням норм техніки безпеки, постійним інструктуванням НПП та здобувачів вищої освіти, проведенням заходів, які стосуються здорового способу життя тощо. Усі приміщення та будівлі (навчально-лабораторні корпуси, культурно-освітній центр, майстерні, гуртожитки, гаражі, їдальні, спортивні площі - спортивно-оздоровчий комплекс, фізкультурно-оздоровчий комплекс, обладнаний ігровим залом, басейном та двома саунами, спортивно-оздоровчу базу та пансіонат вихідного дня) знаходяться у задовільному санітарно-технічному стані, стан інженерно-технічних комунікацій і систем забезпечення будівель відповідає нормам, про що свідчать Висновки державної сан-
епідеміологічної експертизи, експертний висновок № 114/1 щодо протипожежного стану об'єкта (один висновок на всі адреси), Акт перевірки суб'єкта господарювання тощо. Питаннями захисту психологічного здоров'я і соціального благополуччя займається Психологічна служба (https://www.stu.cn.ua/staticpages/vospitanie-pxihosluzba/), яка проводить тренінги для студентів. Інструктажі для здобувачів ВО проводяться регулярно як з безпеки праці перед початком лабораторних практикумів так і з безпеки життєдіяльності під час канікул, виїздів на конференції та олімпіади, тощо.
Студенти ОП, що акредитується, оцінили на 9,4 з 10 рівень безпечності навчання для свого життя та здоров'я.
За час реалізації ОП звернень щодо проблем психологічного здоров'я не було.

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

Задля унормування механізмів освітньої, організаційної, інформаційної, консультативної та соціальної підтримки здобувачів вищої освіти в Університеті створена документаційна база, яка загальнодоступна у будь-який час на сайті Університету - портал «Нормативна база» https://www.stu.cn.ua/staticpages/public-info/
Освітня підтримка (формування індивідуальної траєкторії, поточні питання навчання, тощо) здійснюється в першу чергу через деканати інститутів. Для зручності та швидкості інформування та консультування студентів в Навчально-науковому інституті електронних та інформаційних технологій використовується телеграм чат-бот, який дає відповіді на найбільш типові запитання здобувачів, дозволяє відправити запит на отримання довідок, тощо.
Для вирішення більшості організаційних питань, за кожною групою закріплено куратора, який консультує здобувачів. Куратори також моніторять ситуацію в групі, надають соціальну підтримку, за потреби, періодично відвідують студентів, що проживають в гуртожитку, дають життєві поради студентам, рекомендують місця практики

та працевлаштування, тощо. Разом з тим, консультативну допомогу студенти можуть отримати безпосередньо в деканаті інституту, а також в адмінчастині Університету (бухгалтерії, військово-обліковому відділі, відділі з питань працевлаштування, практики та зв'язків з громадськістю тощо).
Соціальну та психологічну підтримку здобувачів здійснює Психологічна служба.
Зазначимо, що задля підвищення життєвого рівня та заохочення за успіхи у навчанні, участь у громадській, спортивній і науковій діяльності Університет може надавати матеріальну допомогу та заохочення студентам, які навчаються за кошти юридичних або фізичних осіб за денною формою навчання (з відривом від виробництва) відповідно до Порядок використання коштів, передбачених для надання матеріальної допомоги та заохочення студентів, аспірантів та докторантів денної форми навчання https://www.stu.cn.ua/media/files/pdf/nzop/p-matdop.pdf.
За результатами опитування студенти цілком задоволені освітньою, організаційною, інформаційною, соціальною та консультативною підтримкою під час навчання з боку ЗВО. Так, на запитання "Я задоволений рівнем освітньої підтримки (індивідуальна взаємодія з викладачем, якість роботи деканату та інше)" - студенти, що навчаються на ОПП, поставили 9,2 бали з 10; " Я задоволений рівнем інформаційної підтримки (зручне та ефективне інформування стосовно різних аспектів навчання)" - 9,5; "Я задоволений рівнем консультативної підтримки (на кафедрі, у деканаті, бібліотеці)" - 9,2; "Я задоволений рівнем соціальної підтримки (проживання, харчування, стипендії, соціальна допомога та ін.) - 8,9; "Я задоволений рівнем психологічної підтримки (від куратора, інших викладачів, директора ННІ, фахівців)" - 9,1.
Наступне опитування щодо рівня задоволеності здобувачів освіти щодо зазначених видів підтримки заплановане на грудень 2020 року.

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)

Особливості зарахування на навчання осіб з інвалідністю передбачені у Правилах прийому https://www.stu.cn.ua/staticpages/pravilapriem/. Перелік можливостей доступу до здобуття вищої освіти осіб з особливими потребами включає, зокрема, можливість заочної (дистанційної) форми навчання, академвідпустки, вільного відвідування занять (для здобувачів денної форми, які поєднують навчання з роботою за фахом, мають дітей віком до 3-х років, вагітним та в інших передбачених випадках). Щодо останнього, то в університеті розроблено та затверджено Порядок надання дозволу на вільне відвідування занять здобувачам вищої освіти НУ «Чернігівська політехніка» https://www.stu.cn.ua/media/files/pdf/nzop/p-vilne-vid.pdf
Навчальні корпуси, де зокрема відбувається освітній процес і за ОПП, що акредитується, облаштовано пандусами.
Також розроблено ПОРЯДОК супроводу (надання допомоги) осіб з інвалідністю та інших маломобільних груп населення у НУ «Чернігівська політехніка» https://www.stu.cn.ua/media/files/pdf/nzop/p-invalid.pdf
Передбачено в університеті і супровід впродовж навчання осіб з особливими освітніми потребами. Його здійснює Психологічна служба
https://www.stu.cn.ua/media/files/pdf/pologen-psluzh.pdf
Для координації роботи в напрямку освіти осіб з особливими потребами створено Центр інклюзивної освіти (https://www.stu.cn.ua/media/files/pdf/nzop/p-inkluzo.pdf). Серед здобувачів вищої освіти на ОПП, що акредитується, особи з особливими потребами не навчаються.

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

Документи, які регулюють політику та процедури врегулювання конфліктних ситуацій (включаючи пов'язаних із сексуальними домаганнями,
дискримінацією та корупцією) розміщено на сайту університету в закладці "Нормативні документи". Зокрема, «Положення щодо протидії булінгу (цькуванню) у НУ «Чернігівська політехніка»»
(https://stu.cn.ua/media/files/pdf/pol-bull-1.pdf),
Положення про порядок роботи зі зверненням громадян (https://www.stu.cn.ua/media/files/pdf/nzop/p-zvernennya.pdf), «Антикорупційна програма Національного університету «Чернігівська політехніка»»
(https://www.stu.cn.ua/media/files/pdf/nzop/antikor-programa.pdf).
Передбачається, що у випадку виникнення конфліктної ситуації (булінгу, домагань
сексуального характеру, корупцією, або скаргою іншого характеру) подається заява до загального відділу Університету на ім'я ректора. Ректор направляє заяву для розгляду комісією, якою вона розглядається у триденний термін від дати надходження скарги. За кожним фактом звернення проводиться ретельна перевірка, результати якої надаються ректору/проректорам. Громадянину, що подав звернення, надається письмова (або усна – за згодою) відповідь. Рішення керівництва Університету щодо розгляду скарги у разі незгоди з ним громадянина, може бути оскаржене в суді у терміни, у відповідності до законодавства України. За будь-якого рішення комісії, учасникам цього процесу заклад забезпечує психологічну підтримку усім учасникам конфлікту через Психологічну службу.
Результати опитування студентів показали, що з правилами та процедурами вирішення конфліктних ситуацій в Університеті обізнані на 7,6 з 10 балів; з правилами та процедурами надання пропозицій та розгляду скарг від студентів - 7,4; з своїми правами та обов'язками - 9,6.
Слід відзначити, що під час реалізації ОПП 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 в мережі Інтернет

Положення про внутрішню систему забезпечення якості вищої освіти в Національному університеті «Чернігівська політехніка» https://www.stu.cn.ua/media/files/pdf/nzop/p-yakist-vnutrsist.pdf
Порядок розробки, затвердження, моніторингу та закриття освітніх програм у Національному університеті «Чернігівська політехніка» https://www.stu.cn.ua/media/files/pdf/nzop/p-rozr-op.pdf.

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

Важливою складовою системи внутрішнього забезпечення якості вищої освіти Університету є моніторинг освітніх програм. Процедури, пов'язані із розробленням,
затвердженням, моніторингом та переглядом ОП, прописані в Положенні про внутрішню систему забезпечення якості освітньої діяльності та Порядку розробки, затвердження, моніторингу та закриття освітніх програм в Університеті.
Ініціаторами розробки нової освітньої програми можуть виступати як керівництво університету, навчально-наукового інституту, факультету так і ініціативні групи науково-педагогічних працівників. До відділу методичної роботи, акредитації та ліцензування подаються від ініціаторів пропозиції щодо складу проектної групи, який має відповідати Ліцензійним умовам. Склад проєктної групи формується та
затверджується наказом ректора університету окремо за кожною освітньою програмою на період її розроблення.
Перегляд освітньої програми може здійснюється з ініціативи стейкхолдерів, керівника проєктної групи (гаранта освітньої програми), групи забезпечення відповідної спеціальності та керівництва університету. При внесенні змін враховуються: прийняття чи коригування стандарту вищої освіти; висновки акредитаційної експертизи; відгуки стейкхолдерів; перегляд місії та стратегії університету; результати наукових досліджень у відповідній галузі; результати вступної кампанії та інше.
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, в 2020 році була переглянута. Підстава - у зв'язку з підписанням договору про подвійні дипломи з Техніко-гуманітарною академією м. Бельсько-Бяла (Польща), враховуванням рекомендації роботодавців (ІТ кластер, кіберполіція), а також думки здобувачів вищої освіти.
Зміни, що були внесені: окремі дисципліни були перенесені з вибіркових у нормативні, уточнена назва дисциплін, введено нові дисципліни.
Розширений перелік баз практик. Кількість кредитів вибіркових компонент
збільшена порівняно з ОП 2019 року.
Внесені зміни затверджені в установленому в Університеті порядку.

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

Гарант в кінці семестру, проводить усне (письмове) опитування здобувачів ВО щодо якості навчання за кожною дисципліною, крім того пропозиції студентів збираються безпосередньо під час освітнього процесу шляхом спілкування з гарантом програми, НПП випускової кафедри та адміністрацією. Протягом 2019-2020 н.р. проводились спільні зустрічі магістрів першого року навчання, роботодавців (зокрема, кіберполіція, ІТ кластер) та гаранта з приводу обговорення змісту ОПП та необхідності внесення змін. На сайті кафедри представлені фото з цих зустрічей https://mmi.stu.cn.ua/novyny/zustrich-z-kiberpolitsiyeyu/. Задля отримання зворотного зв'язку від здобувачів вищої освіти щодо якості ОПП «Кібербезпека» 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 (з 2020 р. буде 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 (в 1 семестрі 2020-2021 н.р. (закуплено трьохдіапазонний індикатор поля iProtect 1207, обнаружувач сприхованих камер Wega і, тепловізор Wintact WT3320). Всі пропозиції студентів аналізуються та обговорюються на всіх рівнях в Університеті (від кафедри і до керівництва як на першому.

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

Відповідно до Закону України «Про вищу освіту» здобувачі вищої освіти входять до
складу вченої ради Університету, на засіданнях якої обговорюють та затверджують всі зміни до освітніх програм. Крім цього, здобувачі ВО входять до органів студентського самоврядування Університету: Студентської ради та первинної профспілкової організації студентів, які також проводять такі опитування для всіх студентів університету. Здобувачі ВО можуть подавати свої пропозиції щодо необхідності внесення змін (наприклад, до змісту ОПП або щодо організаційних питань) або через органи студентського самоврядування, або безпосередньо самі.

Студентське самоврядування бере участь у процедурах внутрішнього забезпечення якості ОПП, в тому числі і ОПП, що акредитується, відповідно до Положення про студентське самоврядування (https://www.stu.cn.ua/media/files/pdf/nzop/p-stud-samovr.pdf).
Під час перегляду ОПП представники студентського самоврядування (зокрема, Попов Антон, студент Кб 181) були присутні на зустрічах щодо обговорення необхідності внесення змін до ОПП (Протокол засідання кафедри №10 від 28.01.20).

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

Університет до організації та реалізації освітнього процесу активно залучає роботодавців.
Одним із прикладів є участь роботодавців у роботі Екзаменаційних комісій, що регламентується відповідним положенням.
Університетом підписані угоди з: компанією Soft Industry Alliance, Porta One та громадською організацією «IT кластер», ТОВ "Інформаційна безпека" та ін.
Співпрацю з вищезазначеними організаціями забезпечує випускова кафедра та особисто гарант програми. Під час проходження студентами практик, проводиться опитування керівників від баз практик щодо змісту ОПП.
Обговорення ОПП та змісту її окремих освітніх компонентів відбувається на наукових конференціях і семінарах, зокрема в ході щорічного кафедрального Meetup «Актуальні питання кібербезпеки» до міжнародного дня захисту інформації та щорічній Всеукраїнської науково-практичної конференції молодих науковців, аспірантів «Новітні технології у науковій діяльності і навчальному процесі»
Результати обговорень ОПП із роботодавцями взяті до уваги, що відображено у протоколах засідань кафедри кібербезпеки та математичного моделювання. Останнє проведено в 2020 р.(Протокол №10 від 28.01.20.). Необхідно відмітити той факт, що роботодавці систематично запрошуються на кафедру.

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

Наразі відсутня інформація про траєкторію працевлаштування випускників, оскільки на ОПП «Кібербезпека» ще не було випусків. Проте, гарант ОПП вже здійснює моніторинг серед студентів, які вже працюють під час навчання на ОПП.
До структури НУ "Чернігівська політехніка" входить відділ з питань працевлаштування, практики та зв'язків з громадськістю, у функції якого входить сприяння працевлаштуванню здобувачів ВО (у тому числі під час навчання - у вільний від занять час, а також випускників – після завершення навчання), співпраця з роботодавцями в частині зазначених питань, збір інформації щодо кар'єрного шляху випускників і відгуків із баз практики на практикантів з подальшим їх аналізом задля покращення освітнього процесу.

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

У ході здійснення процедур внутрішнього забезпечення якості під час реалізації ОПП суттєвих недоліків не виявлено.
Проте, були надані загальні рекомендації задля покращення освітнього процесу на ОПП: бажано організувати роботу з документами кафедри в хмарному середовищі; систематично оновлювати та доповнювати навчально-методичні матеріали, що розміщені в системі Moodle, продовжувати активну участь НПП кафедри у наукових заходах, зокрема науково-практичних конференціях.
Підсумки реалізації ОПП будуть підведені після першого випуску здобувачів вищої освіти. Виявлені моменти, які потребуватимуть усунення, будуть враховані у подальшій роботі зі здобувачами та розглянуті на засіданні випускової кафедри із залученням усіх зацікавлених сторін.

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

ОПП спеціальності 125 Кібербезпека другого (магістерського) проходить первинну акредитацію.
У 2019 році успішно відбулась акредитація за напрямом підготовки 6.170103 "Управління інформаційною безпекою" галузі знань 1701 "Інформаційна безпека" у Чернігівському національному технологічному університеті за освітнім ступенем «бакалавр». Разом з тим експерти рекомендували: звернути увагу на необхідність дооснащення лабораторної бази спеціалізованими програмними засобами; розробити план підвищення кваліфікації працівників кафедри у відповідності до зазначеного напряму підготовки; поповнити бібліотечний фонд університету новими навчальними підручниками та посібниками провідних навчальних закладів з грифом МОН України та періодичними науковими виданнями відповідного профілю.
За 2019-2020 рік відкрито лабораторію з кібербезпеки (наказ №175 від 26.12.2018р.) та закуплено сучасне спеціалізоване обладнання (остання закупка 2019 року - багатофункціональний пошуковий пристрій Andre Advanced, у 2020 р. - трьохдіапазонний індикатор поля iProtect 1207, пристрій, який виявляє приховані камери Wega і, тепловізор Wintact WT3320).
В Університеті існує графік підвищення кваліфікації НПП, згідно з яким викладачі підвищують свій фаховий рівень

за відповідним напрямом (наприклад, у 2020 році Петренко Т.А. захистив кандидатську дисертацію за спеціальністю 05.13.21 - системи захисту інформації).
Науково-педагогічними працівниками випускової кафедри протягом 2019-2020 н.р. було опубліковано 4 роботи, що внесені до НМБ Scopus, опубліковано 4 навчальних посібника, підготовлено підручник, завершено створення кафедрою навчально-методичних комплексів з навчальних дисциплін у відповідності до навчального плану та забезпечено можливість вільного до них доступу через дистанційну платформу Moodle.
В Університеті активно ведеться робота з накопичення електронного бібліотечного фонду сучасними науковими вітчизняними виданнями відповідно до освітньо-професійної програми.
Крім того, для вдосконалення освітнього процесу на ОПП, також приймалися до розгляду результати акредитацій інших напрямів підготовки та спеціальностей, що проводилися в Університеті.

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

Учасники академічної спільноти (науковці, НПП, адміністрація ЗВО) залучені до процедур внутрішнього забезпечення якості вищої освіти у різний спосіб, зокрема вони: беруть участь в обговоренні питань забезпечення якості освіти і процедури їх реалізації (на засіданнях кафедр та вчених рад); забезпечують викладання навчальних дисциплін на високому науково-теоретичному і методичному рівнях; підвищують власний професійний рівень, педагогічну майстерність та/або наукову кваліфікацію через участь у численних науково-практичних та науково-методичних конференціях, підвищення кваліфікації та стажування; дотримуються норм академічної доброчесності, педагогічної етики і моралі, тощо.
Провадиться робота щодо ознайомлення учасників академічної спільноти з новими тенденціями через різноманітні заходи, наприклад наукові конференції (І Міжнародна науково-практична конференція “Безпека ресурсів інформаційних систем, квітень, 2020р.).
Студенти систематично проходять анкетування щодо якості освітнього процесу та важливості/якості складових освітнього середовища, результати якого використовуються для покращення відповідних освітніх компонент.
Адміністрація університету здійснює регулярний моніторинг здобутків НПП за допомогою щорічного оцінювання (https://npp.stu.cn.ua/) та навчальних досягнень студентів через регулярні ректорські контролі.

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

Процедури внутрішнього забезпечення якості освіти в Університеті мають дворівневу систему.
На першому рівні процеси та процедури забезпечення якості освіти здійснюють члени проектної групи (що відповідають за розроблення, перегляд
та оновлення змісту ОНП) та члени групи забезпечення ОПП (які особисто беруть участь в реалізації освітнього процесу) під керівництвом гаранта ОПП, який безпосередньо відповідає за здійснення процесів і процедур внутрішнього забезпечення якості освіти.
На другому рівні здійснюється загальне керівництво, контроль внутрішнього забезпечення якості освіти з боку університету через відповідні структурні підрозділи. Обов’язки щодо здійснення процесів і процедур внутрішнього забезпечення якості освіти розподілені між сектором систем менеджменту якості освіти (https://www.stu.cn.ua/media/files/pdf/nzop/p-yakist-sektmen.pdf) і відділом методичної роботи, акредитації та ліцензування (https://www.stu.cn.ua/media/files/pdf/p-pidrozdil/v-metod.pdf).
Участь студентів (органів студентського самоврядування) та роботодавців передбачена на обох рівнях.

9. Прозорість і публічність

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

Основними документами, які регулюють права та обов’язки усіх учасників освітнього процесу в НУ “Чернігівська політехніка” є Статут (https://stu.cn.ua/media/files/pdf/statut2.pdf), Правила внутрішнього розпорядку Національного університету «Чернігівська політехніка» (https://www.stu.cn.ua/media/files/pdf/nzop/pravila-vn-rozp.pdf),
Положення про організацію освітнього процесу в Національному університеті «Чернігівська політехніка» (https://www.stu.cn.ua/media/files/pdf/nzop/p-org-osp.pdf).
В університеті розроблені, погоджені, затверджені у встановленому порядку й викладені для загального доступу на сайті університету в розділі «Нормативна база» інші нормативні документи, які регламентують всі аспекти освітнього процесу. А саме, Положення про проведення практики здобувачів вищої освіти національного університету «Чернігівська політехніка» https://www.stu.cn.ua/media/files/pdf/nzop/p-ppocin.pdf), Положення про академічну мобільність учасників освітнього процесу Національного університету «Чернігівська політехніка» (https://www.stu.cn.ua/media/files/pdf/nzop/p-akad-mob.pdf), Положення про внутрішню систему забезпечення якості вищої освіти в Національному університеті «Чернігівська політехніка» https://www.stu.cn.ua/media/files/pdf/nzop/p-yakist-vnutrsist.pdf, та інші. Куратори на перших зустрічах інформують здобувачів вищої освіти про ці документи та місце їх розміщення. НПП дізнаються про ці документи під час прийому на роботу.

Наведіть посилання на веб-сторінку, яка містить інформацію про оприлюднення на офіційному веб-

сайті ЗВО відповідного проекту з метою отримання зауважень та пропозиції заінтересованих сторін (стейкхолдерів). Адреса веб-сторінки

https://mmi.stu.cn.ua/navchannja/

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

https://op.stu.cn.ua/files/op/%D0%9E%D0%9F%D0%9F%20%20125%20%D0%9A%D1%96%D0%B1%D0%B5%D1%80%D0%B1%D0%B5%D0%B7%D0%BF%D0%B5%D0%BA%D0%B0%20%D0%BC%D0%B0%D0%B3%D1%96%D1%81%D1%82%D1%80%202019%20%D0%B7%D0%BC%D1%96%D0%BD%D0%B8%202020.pdf

11. Перспективи подальшого розвитку ОП

Якими загалом є сильні та слабкі сторони ОП?

Сильні сторони ОНП:
- відповідає тенденціям розвитку спеціальності;
- має чітко сформульовані цілі, що відповідають місії та стратегії ЗВО;
- правила прийому є чіткими;
- висока академічна і професійна кваліфікація викладачів ОПП;
- належна матеріально-технічна база для забезпечення ОНП;
- чіткість і зрозумілість політик та практик дотримання академічної доброчесності;
- дотримання правил і процедур, що регулюють права та обов'язки всіх учасників освітнього процесу;
- сильні соціальні навички, що формуються у випускників;
- залучення роботодавців до освітнього процесу;
- використання дистанційної платформі Moodle.

Водночас, поруч із зазначеними сильними сторонами ОПП, існує низка аспектів, реалізація яких сприятиме покращенню освітньої програми, зокрема, введення викладання частини курсів англійською мовою, активізація участі здобувачів та викладачів у програмах міжнародної академічної мобільності, міжнародних наукових проектах, у т.ч. грантових.

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

Перспективи розвитку чинної ОПП впродовж найближчих років вбачаються у розвитку освітньої програми відповідно до вимог сучасного наукового простору; покращення матеріально-технічної частини навчальних лабораторій; стажування в європейських країнах НПП кафедри; участі у міжнародних проектах, грантових програмах; впровадження англомовних курсів для вивчення на ОПП.

Реалізація цих заходів щодо вдосконалення ОПП сприятиме покращенню освітнього процесу за ОПП.

Разом з тим, у випадку прийняття упродовж найближчих років стандарту за спеціальністю 125 Кібербезпека другого (магістерського) рівня вищої освіти, ОПП буде вимагати перегляду та приведення її у відповідність до стандарту.

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: 07.10.2020 р.

Таблиця 1. Інформація про обов'язкові освітні компоненти ОП

Назва освітнього компонента	Вид компонента	Силабус або інші навчально-методичні матеріали		Якщо освітній компонент потребує спеціального матеріально-технічного та/або інформаційного забезпечення, наведіть відомості щодо нього*
		Назва файла	Хеш файла	
Цивільний захист та охорона праці в галузі	навчальна дисципліна	*ОК 1. Силабус Цивільний захист.pdf*	+wJiBuHYjpDnD+/4HWTITcxu5ZsBkgrrpWQL/9sXQ30=	*Лабораторія 1-419. Наочний матеріал - 7 лабораторних стендів: по електробезпеці; дослідницькі стенди параметрів мікроклімату, стану повітря, рівня шуму та вібрації, штучної та природної вентиляції, еелектромагнітних полів та випромінювання, оцінки радіохімічного стану та протипоженої безпеки; стенд пожежної автоматики. Індивидуальні засоби захисту – 20 комплектів. Мультимедійне обладнання – 1 од.*
Іноземна мова (за професійним спрямуванням)	навчальна дисципліна	*ОК 2. СИЛАБУС Іноземна мова.pdf*	g9G5riUeZlZNM/FsYpoRqhrxu7q/dI8qy3QaUA8pm1U=	*Фонолабораторія кафедри іноземних мов 1-202. Мультимедійне обладнання: Мультимедійний проектор – 1 од. (2010); Екран – 1 од. (2001); роздатковий матеріал; аудіообладнання – 12 од.*
Аудит та управління інцидентами інформаційної безпеки	навчальна дисципліна	*ОК_3_СИЛАБУС_Аудит_та_управління_інцидентами_інформаційної_безпеки.pdf*	saeUtXX+Q27Mfo03VjxjFVaKhsEdfvPjAnTvHA/6Y7A=	*Лабораторія кібербезпеки 1- 111, Персональні комп'ютери GateWay DT55 – 12 од., Шафа телекомукаційна CSV Lite Plus 42U – 1 од., Джерело безперебійного живлення APC Smart-UPS C1000 – 1 од., Комутатор D-Link DES-1024D – 1 од., Бездротовий маршрутизатор Mikrotik hAP ac lite tower - 1 од., Багатофункціональний пошуковий прилад ANDRE № 0000521317, Мультимедійний проектор – 1 од., ПЗ ОС Windows 7 Professional (SP1, 12 ліцензій), ПЗ OpenOffice (v. 4.1.7, 12 ліцензій GNU)*
Методологія та організація наукових досліджень	навчальна дисципліна	*ОК_4_СИЛАБУС_Методологія_та_організація_наукових_досліджень_2020.pdf*	7uTQNBvz1MFZG1YRDraG1poSV3k607ck1s8OH9zaYHU=	*Лабораторія кібербезпеки 1- 111, Персональні комп'ютери GateWay DT55 – 12 од., Мультимедійний проектор – 1 од., Шафа телекомукаційна CSV Lite Plus 42U – 1 од., Джерело безперебійного живлення APC Smart-UPS C1000 – 1 од., Комутатор D-Link DES-1024D – 1 од., ПЗ ОС Windows 7 Professional (SP1, 12 ліцензій), ПЗ OpenOffice (v. 4.1.7, 12 ліцензій GNU)*
Стандартизація, сертифікація засобів та комплексів захисту інформації	навчальна дисципліна	*ОК_5_СИЛАБУС_Стандартизація_2020_2021.pdf*	Ar+9Oj7MslF2qG3asas3AtxlRvp4pq8yhHS/pVBu/5k=	*Лабораторія кібербезпеки 1- 111, Персональні комп'ютери GateWay DT55 – 12 од., Системний блок HP Compaq dc7800 – 3 од., Шафа телекомукаційна CSV Lite Plus 42U – 1 од., Джерело безперебійного живлення APC Smart-UPS C1000 – 1 од., Комутатор D-Link DES-1024D – 1 од., Бездротовий маршрутизатор Mikrotik hAP ac lite tower - 1 од., Багатофункціональний пошуковий прилад ANDRE № 0000521317, Прилад радіочастотного шуму стаціонарний PIAC-1Г№ 0469, Прилад радіочастотного шуму мобільний PIAC-1Г'М № 0164, Генератор шуму для силової мережі Базальт-2Г№ 0414 – 1 од., Випромінювач акустичний PIAC-2BA. № 0517 – 1 од., Вібровипромінювач п'єзоелектричний PIAC-2ВП №№ 0630, 0653 – 2 од., Прилад захисту інформації в аналогових телефонних лініях PIAC-2C/T № 0019 – 1 од., Прилад універсальний напівавтоматичний Бумеранг-2Г – 2 од., Аналізатор спектру С4-77 – 1 од., Інтерферометр INCO NLMZ-4/50 № 1175/81 – 1 од., Селективний мікровольтметр RFT STV 401 № 07045 – 1 од., Мультимедійний проектор – 1 од., ПЗ ОС Windows 7 Professional (SP1, 12 ліцензій), ПЗ OpenOffice (v. 4.1.7, 12 ліцензій GNU), ПЗ ОС Kubuntu (18.04.3-desktop-amd64, 12 ліцензій GNU), ПЗ ОС Kali-Linux (2019.3-amd64, 12 ліцензій GNU), ПЗ VirtualBox (v. 6.0.12, 12 ліцензій GNU), ПЗ ОС BBOS (13 ліцензій)*
Проектування технічних систем захисту інформації	навчальна дисципліна	*ОК_6_СИЛАБУС_Проектування_технічних_систем_захисту_інформації_2020.pdf*	b05VnlzupaPYpJNnMfs8Okl3d5dD1n5MhsdUBrIk2ws=	*Лабораторія кібербезпеки 1- 111, Персональні комп'ютери GateWay DT55 – 12 од., Системний блок HP Compaq dc7800 – 3 од., Шафа телекомукаційна CSV Lite Plus 42U – 1 од., Джерело безперебійного живлення APC Smart-UPS C1000 – 1 од., Комутатор D-Link DES-1024D – 1 од., Маршрутизатор Mikrotik RB3011UiAS-RM – 3 од., Маршрутизатор MikroTik hEX (RB750Gr3) – 4 од., Бездротовий маршрутизатор Mikrotik hAP ac lite tower - 1 од., Багатофункціональний пошуковий прилад ANDRE № 0000521317, Прилад радіочастотного шуму стаціонарний PIAC-1Г№ 0469, Прилад радіочастотного шуму мобільний PIAC-1Г'М № 0164, Генератор шуму для силової мережі Базальт-2Г№ 0414 – 1 од., Випромінювач акустичний PIAC-2BA. № 0517 – 1 од., Вібровипромінювач п'єзоелектричний PIAC-2ВП №№ 0630, 0653 – 2 од., Прилад захисту інформації в аналогових телефонних лініях PIAC-2C/T № 0019 – 1 од., Прилад універсальний напівавтоматичний Бумеранг-2Г – 2 од., Аналізатор спектру С4-77 – 1 од., Інтерферометр INCO NLMZ-4/50 № 1175/81 – 1 од., Селективний мікровольтметр RFT STV 401 № 07045 – 1 од., Мультимедійний проектор – 1 од., ПЗ ОС Windows 7 Professional (SP1, 12 ліцензій), ПЗ OpenOffice (v. 4.1.7, 12 ліцензій GNU), ПЗ ОС Kubuntu (18.04.3-desktop-amd64, 12 ліцензій GNU), ПЗ ОС Kali-Linux (2019.3-amd64, 12 ліцензій GNU), ПЗ VirtualBox (v. 6.0.12, 12 ліцензій GNU), ПЗ ОС BBOS (13 ліцензій)*
Безпекові технології програмування	навчальна дисципліна	*ОК_7_СИЛАБУС_Безпекові_технології_прогр.pdf*	6JaA6cqIXxcS64QhPszT3gtH2mRFSrlGEvXcXPnArqk=	*Аудиторія 4-95.Персональні комп'ютери – 8 од.Навчально-відлагоджувальні стенди "PLD Emulator" власної розробки – 4 од. Пристрій первинної обробки інформації та спряження з ЕОМ власної розробки – 3 од.Генератор синусоїдального сигналу "Генератор сигналов низкочастотный Г3-109"–3 од. Jсцилографи "С1-114/1"–3 од. Керовані джерела постійного струму Б5-46/47 – 3 од. Навчально-відлагоджувальний стенд "EK-TM4C1294XL Launchpad" від компанії Texas Instruments, в основі якого знаходиться мікроконтролер TM4C1294NCPDT із ядром ARM Cortex-M4 – 5 од. Комплект допоміжного навчального обладнання у вигляді портативної елементної бази(давачі, індикатори, ключі, перетворювачі та ін.)–5 од. Допоміжне навчальне обладнання у вигляді шести друкованих плат розширення, що містять набір периферійних пристроїв – 6 од.*
Методи побудови та аналізу криптосистем	навчальна дисципліна	*ОК_8_СИЛАБУС_Методи_побудови_та_аналізу_криптосистем_2020.pdf*	dVRBX1ZbfbnBEMk64y3wScgoQrxmA8Y6r73ZPZ240R8=	*Лабораторія кібербезпеки 1-110, Персональні комп'ютери DELL Optiplex 780 – 12 од., Мультимедійний проектор – 1 од., Шафа телекомукаційна CSV Lite Plus 42U – 1 од., Джерело безперебійного живлення APC Smart-UPS C1000 – 1 од., Комутатор D-Link DES-1024D – 1 од., ПЗ ОС Windows 7 Professional (SP1, 12 ліцензій), ПЗ OpenOffice (v. 4.1.7, 12 ліцензій GNU)*
Управління мережевою безпекою	навчальна дисципліна	*ОК9_СИЛАБУС_Управління_мережевою_безпекою_2020.pdf*	RX74WBBQdyrA5vIK3hXqrseZoPLLw1iB/PKM2uNQazc=	*Аудиторія 4-73. Персональні комп'ютери – 16 од. Комплект обладнання VOIP:сервер PBX – 1 шт. IP-телефони — 10 шт. Мультимедійний проектор(переносний) – 1 од.; Екран(переносний) – 1 од.*

Переддипломна практика	практика	*СИЛАБУС_Переддипломна практика.pdf*	68Y8i1FXCDzv8JUzheyLk2Cpbxb2NyWlopIHoQoiiV4=	*Аудиторія 1-407. Мультимедійне обладнання: Мультимедійний проектор – 1 од.; Екран – 1 од.; роздатковий матеріал*
Підготовка до кваліфікаційної роботи	підсумкова атестація	*Силабус_ВКР.pdf*	JIx8iHe8voFmJD4QY19Gq1yR2cMnP9ms9pDHV4tFQrc=	*Аудиторія 1-407. Мультимедійне обладнання: Мультимедійний проектор – 1 од.; Екран – 1 од.; роздатковий матеріал*

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

Таблиця 2. Зведена інформація про викладачів ОП

ID викладача	ПІБ	Посада	Структурний підрозділ	Кваліфікація викладача	Стаж	Навчальні дисципліни, що їх викладає викладач на ОП	Обґрунтування
229875	Ткач Юлія Миколаївна	Завідувач кафедри, 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 закінчення: 2017, спеціальність: 8.18010014 управління фінансово-економічною безпекою, Диплом доктора наук DD 007402, виданий 16.05.2018, Диплом кандидата наук ДК 059130, виданий 26.05.2010, Атестат доцента 12ДЦ 030905, виданий 17.02.2012	19	Методологія та організація наукових досліджень	Доктор педагогічних наук 13.00.04 «Теорія і методика професійної освіти» Кандидат педагогічних наук. 13.00.02- теорія та методика навчання (математика) Доцент кафедри математичного моделювання та інформатики Навчально-науковий інститут інформаційно-діагностичних систем Національного авіаційного університету, кафедра безпеки інформаційних технологій, з 24.09.2018 по 22.03.2019 року, довідка №03.02/826 від 29.03.2019р. – підвищення кваліфіації Відповідає П 1-3, 7, 8, 13, 15, 16, 18, має значну кількість наукових та навчально-методичних публікацій в напрямку спеціальності 1) 1. Development of adaptive expert system of information security using a procedure of clustering the attributes of anomalies and cyber attacks / Petrenko, T., Lakhno, V.,Tkach, Y., Zaitsev, S.,Bazylevych, V. // Eastern European Journal of Enterprise Technologies, 6/9 (84), 2016.- P. 32-44. https://www.scopus.com/authid/detail.uri?authorId=57193026076 2. Lakhno V., Zaitsev S., Tkach Y., Petrenko T. (2019) Adaptive Expert Systems Development for Cyber Attacks Recognition in In-formation Educational Systems on the Basis of Signs' Clustering. In: Hu Z., Petoukhov S., Dychka I., He M. (eds) Advances in Computer Science for Engineering and Education. ICCSEEA 2019. Advances in Intelligent Systems and Computing, vol 754. Springer, Cham. pp 673-682. https://www.scopus.com/authid/detail.uri?authorId=57193026076 3. 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 4. Oleksandr Milov, Serhii Yevseiev, Andrii Vlasov, Sergey Herasimov, Oleh Dmitriiev, Maksym Kasianenko, Hennady Pievtsov, Yevhen Peleshok, Yuliia Tkach, Serhii Faraon (2019) DEVELOPMENT OF SCENARIO MODELING OF CONFLICT TOOLS IN A SECURITY SYSTEM BASED ON FORMAL GRAMMARS / Східноєвропейський журнал передових технологій Український державний університет залізничного транспорту, ПП «Технологічний центр» Vol 6, No 9 (102) (2019), С. 53-64 http://journals.uran.ua/eejet/article/view/188568 5. 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 2) 1. Аналіз загроз інформаційної безпеки в мережах стандарту ieee 802.11 / Базилевич В.М., Ткач Ю.М., Мехед Д.Б., Петренко Т.А.. // Захист інформації. – 2015. –Том 17, №4.– С. 285–291. 2. Застосування методу експертних оцінок до оцінювання інформаційних ризиків вищого навчального закладу / Ю. М.Ткач, С. В. Казмірчук, Д. Б. Мехед, Д. Б. Базилевич. // Захист інформації. Київ:Національний Авіаційний Університе-тет. – 2017. – №2. – С. 137–142. 3. Аналіз вразливостей корпоративних інформаційних систем / Д.Б. Мехед, Ю.М. Ткач, В.М. Базилевич, В.І. Гур'єв, Я.Ю. Усов // Захист інформації Ukrainian Information Security Research Journal. – 2018. – №1. – С. 61–66. 4. Мехед Д.Б. Дослідження технологій впливу та методів протидії

							фішингу / Мехед Д.Б., Ткач Ю.М., Базилевич В.М. // Захист інформації Ukrainian Information Security Research Journal. – 2019. – №4 (Том 21). – С. 246-251. 5. Ткач Ю.М. Формування готовності до запобігання кіберзагрозам у майбутніх менеджерів організації як елементу ін-форматичної компетентності / Ткач Ю.М. // Актуальні питання природничо-математичної освіти. – Збірник наукових праць. Випуск 1 (13). – Суми: СумДПУ. – 2019. – С. 145-152. 6. 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 7. 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 8. 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. 9. 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 10. 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 11. 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 12. 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 3) Навчальні посібники: 1. Моделювання та аналіз безпеки розподілених інформаційних систем : навч. посіб. [для студ. спец. 121 «Інженерія програмного забезпечення»]/ В.В.Литвинов, В.В.Казимир, І.В.Стеценко та ін. – Чернігів : Чернігів. нац. технол. ун-т, 2016. – 254 с. 2. Інформаційна безпека держави: навч. посіб. для студ. спец. 6.170103 «Управління інформаційною безпекою», 125 «Кібербезпека»/ В.І. Гур'єв, Д.Б. Мехед, Ю.М. Ткач, І.В. Фірсова. – Ніжин: ФОП Лук'яненко В.В. ТПК «Орхідея», 2018. – 166 с. 3. Базилевич В.М. Комп'ютерні мережі. Протоколи, технології, обладнання навч. посіб. для студ. спец. 125 «Кібербезпека» / В. М. Базилевич, Д. Б. Мехед, Ю. М. Ткач. – Ніжин: ФОП Лук'яненко В.В. ТПК «Орхідея», 2018. – 108 с. 4. Мехед Д.Б. Спеціальні глави математики. навч. посіб. для студ. спец. 125 «Кібербезпека» / Д. Б. Мехед, Ю. М. Ткач, В. М. Базилевич. – Ніжин: ФОП Лук'яненкоВ.В. ТПК «Орхідея», 2018. – 124 с. : іл. 5. Менеджмент інформаційної безпеки: навч.посібник для студентів спеціальності 125 «Кібербезпека»/ О.Г. Корченко, М.Є. Шелест, С.В. Казмірчук, Ю.М. Ткач, Є.В. Іванченко.-Ніжин:ФОП Лук'яненко В.В. ТПК «Орхідея», 2019.-408 с. 6. Проектування, введення в дію та супроводження КСЗІ: навчальний посібник / В.Д. Козюра, В.О. Хорошко, М.Є. Шелест, Ю.М. Ткач, С.В. Зайцев. – Ніжин: ФОП Лук'яненко В.В. ТПК «Орхідея», 2019. – 240 с. 7. Комплексні системи захисту інформації в інформаційно-телекоммунікаційних системах: Навч. посіб. / В.Д. Козюра, В.О. Хорошко, Ю.М. М.Є. Шелест, Ю.М. Ткач, Я.Ю. Усов. – Ніжин: ФОП Лук'яненко В.В. ТПК «Орхідея», 2019. – 145 с. 7) Член Акредитаційної комісії МОН: Наказ МОН №336А (від 03.03.2017 р.) про проведення чергової

							акредитаційної експертизи підготовки бакалаврів з напряму підготовки 6.170103 «Управління інформаційною безпекою» у Національному авіаційному університеті. Участь у роботі експертної комісії з метою проведення первинної акредитаційної експертизи ОПП Системи технічногго захисту інформації, автоматизація їх обробки зі спеціальності 125 Кібербезпека за другим (магістерським) рівнем вищої освіти в НАУ. Наказ МОН від 10.09.2018р №1452-л Участь у роботі експертної комісії з метою проведення первинної акредитаційної експертизи програми Комп'ютерне моделювання та обчислювальні методи зі спец. 113 Прикладна математика за другим (магістерським) рівнем вищої освіти у Дніпровському національному універ. ім. О.Гончара. НАКаз МОН від 13.12.18р. №3034-л Участьв роботі експертних груп від НАЗЯВО у якості голови експертної групи та члена групи, 5 разів протягом 2019-2020 р 8) Керівник наукової теми: Методи та засоби забезпечення безпеки ресурсів інформаційних систем. Номер 0117U003187. Терміни виконання 04.17-04.22 13) 1. Базилевич В.М. Інженерна та комп'ютерна графіка. Методичні вказівки до виконання розрахунково-графічної роботи для студентів напряму підготовки (спеціальності) 6.170103 Управління інформаційною безпекою», 125 «Кібербезпека» денної фор-ми навчання / укл. Базилевич В.М., Ткач Ю.М. – Чернігів: ЧНТУ, 2019. – 38 с. 2. Мехед Д. Б. Вища математика. Методичні вказівки до виконання розрахунково-графічних робіт для студентів напряму підготовки (спеціальності) 6.170103 «Управління інформаційною безпекою», 125 «Кібербезпека» денної форми навчання / Укл.: Мехед Д.Б., Ткач Ю.М. – Чернігів: ЧНТУ, 2019. – 51 с. 3. Методичні вказівки до виконання випускної кваліфікаційної роботи здобувачів вищої освіти освітнього ступеню «бакалавр» спеціальності 125 - «Кібербезпека»// Укл.: Т.А. Петренко, Ю.М. Ткач, Д.Б. Мехед - Чернігів: ЧНТУ, 2020. – 34с. 15) 1. Ткач Ю.М. Якісна оцінка ризиків інформаційної безпеки державних вищих навчальних закладів / Ю.М.Ткач // Стан та удосконалення безпеки інформаційно-телекомунікаційнх систем (SITS'2015): збірник тез доповідей науково-практичної конференції (м.Коблево, 9-12 червня 2015 р.). – Коблево : Миколаїв-Коблево, 2015. – С.55-59. 2. Ткач Ю.М. До питання розвитку криптографічних алгоритмів/ Ю.М. Ткач, К. Ветошкіна// Новітні технології у науковій діяльності і навчальному процесі : Всеукраїнська науково-практична конференція студентів, аспірантів та молодих учених (м. Чернігів, 18 - 19 травня 2016 р.) : збірник тез доповідей. - Чернігів : Черніг. нац. технол. ун-т.- 2016. – С. 100-101 . 3. Ткач Ю.М. Threat analysis of computer file-server using experts' evaluation method/ Ю.М. Ткач, Ф.Храмушин// Новітні технології у науковій діяльності і навчальному процесі : Всеукраїнська науково-практична конференція студентів, аспірантів та молодих учених (м. Чернігів, 18 - 19 травня 2016 р.) : збірник тез доповідей. - Чернігів : Черніг. нац. технол. ун-т.- 2016. – С.107-109 4. Ткач Ю.М. Застосування статистичного інструментарію у процесі оцінювання інформаційних ризиків / Ю.М. Ткач, С.В. Казмирчук. // Стан та удосконалення безпеки інформаційно-телекомунікаційнх систем (SITS'2016): збірник тез доповідей 8-ої Всеукраїнської науково-практичної конференції (м.Коблево, 9-12 червня 2016 р.). – Коблево : Миколаїв-Коблево.- 2016. – С.67-70 5. Аналіз загроз інформаційної безпеки в WI-FI мережах / Ю.М. Ткач, Д.Б. Мехед, В.М. Базилевич, Т.А. Петренко. // «Актуальні питання забезпечення кібербезпеки та захисту інформації»: тези доповідей учасників II Міжнародної науково-практичної конференції. – К.: Видавництво Європейського університету.- 2016. – С.151-155. 6. Сучасні засоби оцінювання ризиків інформаційної безпеки/ О.Г. Корченко, С.В. Казмирчук, Ю.М. Ткач, Д.Б. Мехед // Стан та удосконалення безпеки інформаційно-телекомунікцаійних систем (SITS'2017). - Миколаїв: МТУ "Миколаївська політехніка", 2017. - 45-48. 7. Ткач Ю.М. Загрози інформаційній безпеці вищого навчального закладу / Ю.М. Ткач// Комплексне забезпечення якості технологічних

							процесів та систем (КЗЯТПС – 2017) : матеріали тез доповідей VII міжнародної науково-практичної конференції (м. Чернігів , 24–27 квіт. 2017 р.) : у 2-х т. / Чернігівський національний технологічний університет [та ін.]; відп. за вип.: Єрошенко Андрій Михайлович [та ін.]. – Чернігів : ЧНТУ, 2017. – Т. 2. – С.96-97. 8. Ткач Ю.М. Кібератаки в Україні 2014-2019 рр. / Ю.М. Ткач, В.С. Марченко// Новітні технології у науковій діяльності і навчальному процесі : Всеукраїнська науково-практична конференція студентів, аспірантів та молодих учених: збірник тез доповідей. - Чернігів : Черніг. нац. технол. ун-т.- 2019. – С. 124-125 . 9. Ткач Ю. Психологічний вплив на підсвідомість образотворчими засобами / Ю. Ткач, К. Бойко. // Новітні технології у науковій діяльності і навчальному процесі : Всеукраїнська науково-практична конференція студентів, аспірантів та молодих учених: збірник тез доповідей. – 2017. – С. 57–58. 10. Карпінський М. Захищене інформаційне середовище / Карпінський М., Ткач Ю., Усов Я. // ITSec: Безпека інформа-ційних технологій: IX міжнародна науково-технічна конференція, 22-27 березня 2019 р. – К.: НАУ, 2019. – С. 45-46. 11. 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. 12. Ткач Ю.Н. О РАЗВИТИИ КИБЕРПРОСТРАНСТВА И ЕГО ЗАЩИЩЕННОСТИ / 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 13. 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. Чер-нігів 16-17 квітня 2020 р.). – Чернігів : НУЧП, 2020. – С.106-110 14. 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 15. 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. 16) Участь у професійних об'єднаннях за спеціальністю: ГО «Асоціація працівників кібербезпеки». 18) Наукове консультування установ, підприємств, організацій протягом не менше двох років. ТОВ «Інформаційна безпека»
229875	Ткач Юлія Миколаївна	Завідувач кафедри, 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 закінчення: 2017, спеціальність: 8.18010014 управління фінансово-економічною безпекою, Диплом доктора наук DD 007402, виданий 16.05.2018, Диплом кандидата наук ДК 059130, виданий 26.05.2010, Атестат доцента 12ДЦ 030905, виданий 17.02.2012	19	Аудит та управління інцидентами інформаційної безпеки	Доктор педагогічних наук 13.00.04 «Теорія і методика професійної освіти» Кандидат педагогічних наук. 13.00.02- теорія та методика навчання (математика) Доцент кафедри математичного моделювання та інформатики Навчально-науковий інститут інформаційно-діагностичних систем Національного авіаційного університету, кафедра безпеки інформацій-них технологій, з 24.09.2018 по 22.03.2019 року, довідка №03.02/826 від 29.03.2019р. – підвищення кваліфіації Відповідає П 1-3, 7, 8, 13, 15, 16, 18, має значну кількість наукових та навчально-методичних публікацій в напрямку спеціальності 1) 1. Development of adaptive expert system of information security using a procedure of clustering the attributes of anomalies and cyber attacks / Petrenko, T., Lakhno, V.,Tkach, Y., Zaitsev, S.,Bazylevych, V. // Eastern European Journal of Enterprise Technologies, 6/9 (84), 2016.- P. 32-44. https://www.scopus.com/authid/detail.uri?authorId=57193026076 2. Lakhno V., Zaitsev S., Tkach Y., Petrenko T. (2019) Adaptive Expert Systems Development for Cyber Attacks Recognition in In-formation Educational Systems on the Basis of Signs' Clustering. In: Hu Z., Petoukhov S., Dychka I., He M. (eds) Advances in Computer Science for Engineering and

							Education. ICCSEEA 2019. Advances in Intelligent Systems and Computing, vol 754. Springer, Cham. pp 673-682. https://www.scopus.com/authid/detail.uri?authorId=57193026076 3. 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 4. Oleksandr Milov, Serhii Yevseiev, Andrii Vlasov, Sergey Herasimov, Oleh Dmitriiev, Maksym Kasianenko, Hennady Pievtsov, Yevhen Peleshok, Yuliia Tkach, Serhii Faraon (2019) DEVELOPMENT OF SCENARIO MODELING OF CONFLICT TOOLS IN A SECURITY SYSTEM BASED ON FORMAL GRAMMARS / Східноєвропейський журнал передових технологій Український державний університет залізничного транспорту, ПП «Технологічний центр» Vol 6, No 9 (102) (2019), С. 53-64 http://journals.uran.ua/eejet/article/view/188568 5. 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 2) 1. Аналіз загроз інформаційної безпеки в мережах стандарту ieee 802.11 / Базилевич В.М., Ткач Ю.М., Мехед Д.Б., Петренко Т.А.. // Захист інформації. – 2015. –Том 17, №4.– С. 285–291. 2. Застосування методу експертних оцінок до оцінювання інформаційних ризиків вищого навчального закладу / Ю. М.Ткач, С. В. Казмірчук, Д. Б. Мехед, Д. Б. Базилевич. // Захист інформації. Київ:Національний Авіаційний Університет. – 2017. – №2. – С. 137–142. 3. Аналіз вразливостей корпоративних інформаційних систем / Д.Б. Мехед, Ю.М. Ткач, В.М. Базилевич, В.І. Гур'єв, Я.Ю. Усов // Захист інформації Ukrainian Information Security Research Journal. – 2018. – №1. – С. 61–66. 4. Мехед Д.Б. Дослідження технологій впливу та методів протидії фішингу / Мехед Д.Б., Ткач Ю.М., Базилевич В.М. // Захист інформації Ukrainian Information Security Research Journal. – 2019. – №4 (Том 21). – С. 246-251. 5. Ткач Ю.М. Формування готовності до запобігання кіберзагрозам у майбутніх менеджерів організації як елементу ін-форматичної компетентності / Ткач Ю.М. // Актуальні питання природничо-математичної освіти. – Збірник наукових праць. Випуск 1 (13). – Суми: СумДПУ. – 2019. – С. 145-152. 6. 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 7. 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 8. 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. 9. 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 10. 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 11. 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 12. 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 3) Навчальні посібники: 1. Моделювання та аналіз безпеки розподілених інформаційних систем : навч. посіб. [для студ. спец. 121 «Інженерія програмного забезпечення»]/ В.В.Литвинов, В.В.Казимир, І.В.Стеценко та ін. – Чернігів : Чернігів. нац. технол. ун-т, 2016. – 254 с. 2. Інформаційна безпека держави: навч. посіб. для студ. спец. 6.170103 «Управління інформаційною безпекою», 125 «Кібербезпека»/ В.І. Гур'єв, Д.Б. Мехед, Ю.М. Ткач, І.В. Фірсова. – Ніжин: ФОП Лук'яненко В.В. ТПК «Орхідея», 2018. – 166 с. 3. Базилевич В.М. Комп'ютерні мережі. Протоколи, технології, обладнання навч. посіб. для студ. спец. 125 «Кібербезпека» / В. М. Базилевич, Д. Б. Мехед, Ю. М. Ткач. – Ніжин: ФОП Лук'яненко В.В. ТПК «Орхідея», 2018. – 108 с. 4. Мехед Д.Б. Спеціальні глави математики. навч. посіб. для студ. спец. 125 «Кібербезпека» / Д. Б. Мехед, Ю. М. Ткач, В. М. Базилевич. – Ніжин: ФОП Лук'яненкоВ.В. ТПК «Орхідея», 2018. – 124 с. : іл. 5. Менеджмент інформаційної безпеки: навч.посібник для студентів спеціальності 125 «Кібербезпека»/ О.Г. Корченко, М.Є. Шелест, С.В. Казмірчук, Ю.М. Ткач, Є.В. Іванченко.-Ніжин:ФОП Лук'яненко В.В. ТПК «Орхідея», 2019.-408 с. 6. Проектування, введення в дію та супроводження КСЗІ: навчальний посібник / В.Д. Козюра, В.О. Хорошко, М.Є. Шелест, Ю.М. Ткач, С.В. Зайцев. – Ніжин: ФОП Лук'яненко В.В. ТПК «Орхідея», 2019. – 240 с. 7. Комплексні системи захисту інформації в інформаційно-телекоммунікаційних системах: Навч. посіб. / В.Д. Козюра, В.О. Хорошко, Ю.М. М.Є. Шелест, Ю.М. Ткач, Я.Ю. Усов. – Ніжин: ФОП Лук'яненко В.В. ТПК «Орхідея», 2019. – 145 с. 7) Член Акредитаційної комісії МОН: Наказ МОН №336А (від 03.03.2017 р.) про проведення чергової акредитаційної експертизи підготовки бакалаврів з напряму підготовки 6.170103 «Управління інформаційною безпекою» у Національному авіаційному університеті. Участь у роботі експертної комісії з метою проведення первинної акредитаційної експертизи ОПП Системи технічнотго захисту інформації, автоматизація їїх обробки зі спеціальності 125 Кібербезпека за другим (магістерським) рівнем вищої освіти в НАУ. Наказ МОН від 10.09.2018р №1452-л Участь у роботі експертної комісії з метою проведення первинної акредитаційної експертизи програми Комп'ютерне моделювання та обчислювальні методи зі спец. 113 Прикладна математика за другим (магістерським) рівнем вищої освіти у Дніпровському національному універ. ім. О.Гончара. НАКаз МОН від 13.12.18р. №3034-л Участьв роботі експертних груп від НАЗЯВО у якості голови експертної групи та члена групи, 5 разів протягом 2019-2020 р 8) Керівник наукової теми: Методи та засоби забезпечення безпеки ресурсів інформаційних систем. Номер 0117U003187. Терміни виконання 04.17-04.22 13) 1. Базилевич В.М. Інженерна та комп'ютерна графіка. Методичні вказівки до виконання розрахунково-графічної роботи для студентів напряму підготовки (спеціальності) 6.170103 Управління інформаційною безпекою», 125 «Кібербезпека» денної фор-ми навчання / укл. Базилевич В.М., Ткач Ю.М. – Чернігів: ЧНТУ, 2019. – 38 с. 2. Мехед Д. Б. Вища математика. Методичні вказівки до виконання розрахунково-графічних робіт для студентів напряму підготовки (спеціальності) 6.170103 «Управління інформаційною безпекою», 125 «Кібербезпека» денної форми навчання / Укл.: Мехед Д.Б., Ткач Ю.М. – Чернігів: ЧНТУ, 2019. – 51 с. 3. Методичні вказівки до виконання випускної кваліфікаційної роботи здобувачів вищої освіти освітнього ступеню «бакалавр» спеціальності 125 - «Кібербезпека»// Укл.: Т.А.

							Петренко, Ю.М. Ткач, Д.Б. Мехед - Чернігів: ЧНТУ, 2020. – 34с. 15) 1. Ткач Ю.М. Якісна оцінка ризиків інформаційної безпеки державних вищих навчальних закладів / Ю.М.Ткач // Стан та удосконалення безпеки інформаційно-телекомунікаційнх систем (SITS'2015): збірник тез доповідей науково-практичної конференції (м.Коблево, 9-12 червня 2015 р.). – Коблево : Миколаїв-Коблево, 2015. – С.55-59. 2. Ткач Ю.М. До питання розвитку криптографічних алгоритмів/ Ю.М. Ткач, К. Ветошкіна// Новітні технології у науковій діяльності і навчальному процесі : Всеукраїнська науково-практична конференція студентів, аспірантів та молодих учених (м. Чернігів, 18 - 19 травня 2016 р.) : збірник тез доповідей. - Чернігів : Черніг. нац. технол. ун-т.- 2016. – С. 100-101 . 3. Ткач Ю.М. Threat analysis of computer file-server using experts' evaluation method/ Ю.М. Ткач, Ф.Храмушин// Новітні технології у науковій діяльності і навчальному процесі : Всеукраїнська науково-практична конференція студентів, аспірантів та молодих учених (м. Чернігів, 18 - 19 травня 2016 р.) : збірник тез доповідей. - Чернігів : Черніг. нац. технол. ун-т.- 2016. – С.107-109 4. Ткач Ю.М. Застосування статистичного інструментарію у процесі оцінювання інформаційних ризиків / Ю.М. Ткач, С.В. Казмирчук. // Стан та удосконалення безпеки інформаційно-телекомунікаційнх систем (SITS'2016): збірник тез доповідей 8-ої Всеукраїнської науково-практичної конференції (м.Коблево, 9-12 червня 2016 р.). – Коблево : Миколаїв-Коблево.- 2016. – С.67-70 5. Аналіз загроз інформаційної безпеки в WI-FI мережах / Ю.М. Ткач, Д.Б. Мехед, В.М. Базилевич, Т.А. Петренко. // «Актуальні питання забезпечення кібербезпеки та захисту інформації»: тези доповідей учасників II Міжнародної науково-практичної конференції. – К.: Видавництво Європейського університету.- 2016. – С.151-155. 6. Сучасні засоби оцінювання ризиків інформаційної безпеки/ О.Г. Корченко, С.В. Казмирчук, Ю.М. Ткач, Д.Б. Мехед // Стан та удосконалення безпеки інформаційно-телекомунікцаійних систем (SITS'2017). - Миколаїв: МТУ "Миколаївська політехніка", 2017. - 45-48. 7. Ткач Ю.М. Загрози інформаційній безпеці вищого навчального закладу / Ю.М. Ткач// Комплексне забезпечення якості технологічних процесів та систем (КЗЯТПС – 2017) : матеріали тез доповідей VII міжнародної науково-практичної конференції (м. Чернігів , 24–27 квіт. 2017 р.) : у 2-х т. / Чернігівський національний технологічний університет [та ін.]; відп. за вип.: Єрошенко Андрій Михайлович [та ін.]. – Чернігів : ЧНТУ, 2017. – Т. 2. – С.96-97. 8. Ткач Ю.М. Кібератаки в Україні 2014-2019 рр. / Ю.М. Ткач, В.С. Марченко// Новітні технології у науковій діяльності і навчальному процесі : Всеукраїнська науково-практична конференція студентів, аспірантів та молодих учених: збірник тез доповідей. - Чернігів : Черніг. нац. технол. ун-т.- 2019. – С. 124-125 . 9. Ткач Ю. Психологічний вплив на підсвідомість образотворчими засобами / Ю. Ткач, К. Бойко. // Новітні технології у науковій діяльності і навчальному процесі : Всеукраїнська науково-практична конференція студентів, аспірантів та молодих учених: збірник тез доповідей. – 2017. – С. 57–58. 10. Карпінський М. Захищене інформаційне середовище / Карпінський М., Ткач Ю., Усов Я. // ITSec: Безпека інформа-ційних технологій: IX міжнародна науково-технічна конференція, 22-27 березня 2019 р. – К.: НАУ, 2019. – С. 45-46. 11. 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. 12. Ткач Ю.Н. О РАЗВИТИИ КИБЕРПРОСТРАНСТВА И ЕГО ЗАЩИЩЕННОСТИ / 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 13. 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. Чер-нігів 16-17 квітня 2020 р.). – Чернігів : НУЧП, 2020. – С.106-110 14. 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 15. 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. 16) Участь у професійних об'єднаннях за спеціальністю: ГО «Асоціація працівників кібербезпеки». 18) Наукове консультування установ, підприємств, організацій протягом не менше двох років. ТОВ «Інформаційна безпека»
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	14	Управління мережевою безпекою	Кандидат технічних наук, 05.13.21 – Системи захисту інформації, Захист кандидатської дисертації (підвищення кваліфікації) 14.05.2020р. рішення атестаційної колегії № ДК 056619 Відповідає П 1, 2, 10, 13, 15, 16, 17, 18 має значну кі-лькість науко-вих та навчаль-но-методичних публікацій в напрямку спе-ціальності 1) 1. Development of adaptive expert system of information security using a procedure of clustering the attributes of anomalies and cyber attacks / Lakhno, V.,Tkach, Y.,Petrenko, T.,Zaitsev, S.,Bazylevych, V. // Eastern European Journal of Enterprise Technologies, 6/9 (84), 2016.- P. 32-44. Scopus (Особистий внесок: структурна схема адаптивної експертної системи, категорійна модель для визначення інформаційного критерію функціональної результативності навчання експертної системи). 2. V. Lakhno, S. Zaitsev, Y. Tkach, T. Petrenko, “Adaptive expert systems development for cyber attacks recognition in information educational systems on the basis of signs’ clustering”, Advances in Intelligent Systems and Computing, v. 754. pp. 673–682, 2018. (Особистий внесок: модель адаптивної системи розпізнавання, модифікована інформаційна умова функціональної результа-тивності навчання експертної системи). 2) 1. Д.Б. Мехед, Ю.М. Ткач Ю.М., В.М. Базилевич і Т.А. Петренко, “Аналіз загроз інформаційної безпеки в мережах стандарту IEEE 802.11”, Захист інформації, т. 17, №4. с. 285–291, 2015. 2. В.А. Лахно, Т.А Петренко і М.В. Пирог, “Моделювання роботи адаптивної системи розпізнавання кібератак в умовах неод-норідних потоків запитів в модулях e-business”, Безпека інформації, т. 22, № 2, с. 135–142, 2016. 3. В.А. Лахно, А.М. Терещук и Т.А. Петренко, “Совершенствование киберзащиты информационных систем за счет адаптив-ных технологий распознавания кибератак”, Захист інформації, т.18, № 2, с. 99–106, 2016. 4. В.М. Базилевич, М.В.. Мальцева, Т.А. Петренко, Л.Г. Черниш "Захищена система розумного будинку з використанням Internet of Things", Технічні науки та технології : науковий журнал / Чернігів. нац. технол. ун-т. – Чернігів : ЧНТУ, 2020. – № 2 (20). – С. 218-228. 5. Є.В. Риндич, Т.А. Петренко, Л.Г. Черниш, С.М. Семендяй, Г.С. Біленький "Навчальний стенд для вивчення дисциплін із забезпечення мережевого захисту інформації" / Чернігів. нац. технол. ун-т. – Чернігів : ЧНТУ, 2020. – № 2 (20). – С. 229-236. 10) Заступник завідувача кафедри кібербезпеки та математичного моделювання Національного університету Чернігівська полі-техніка 13) 1. Програма навчальної практики з управління інформаційною безпекою [Текст] / Петренко Т.А.. – Чернігів: Чернігівський національний технологічний університет, 2017. – 32 с. 2. Операційні системи: метод. вказівки до виконання розрах.-граф. роботи для студентів за напрямом підгот. (спец.) 6.170103 «Управління інформаційною безпекою», 125 «Кібербезпека» ден. форми навчання / уклад. Т. А. Петренко. – Чернігів : ЧНТУ, 2019. – 26 с. 3. Системи штучного інтелекту: метод. вказівки до виконання розрах.-граф. роботи для студентів за напрямом підгот. (спец.) 6.170103

							«Управління інформаційною безпекою», 125 «Кібербезпека» ден. форми навчання / уклад. Т. А. Петренко. – Черні-гів: ЧНТУ, 2019. – 24 с. 3. Методичні вказівки до виконання випускної кваліфікаційної роботи здобувачів вищої освіти освітнього ступеню «бака-лавр» спеціальності 125 - «Кібербезпека»// Укл.: Т.А. Петренко, Ю.М. Ткач, Д.Б. Мехед - Чернігів: ЧНТУ, 2019. – 34с. 4. Кібербезпека. Методичні вказівки до виробничої практики [Текст] / розробник: Петренко Т.А. – Чернігів: Чернігівський національний технологічний університет, 2020. – 36 с. 15) 1. Система интеллектуальной поддержки принятия решений в слабо формализуемых задачах обеспечения кибербезопасности / Петренко Т.А., Лахно В.А.// Всеукраїнська науково-практична конференція студентів, аспірантів та молодих вчених «Нові-тні технології у науковій діяльності і навчальному процесі» м. Чернігів, ЧНТУ, 2017. 2. Метод та моделі адаптивних експертних систем розпізнавання кібератак на основі кластеризації ознак / Петренко Т.А., Ла-хно В.А // VII міжнародна науково-технічна конференція «ITSEC», м. Київ, НАУ, 16-18 травня, 2017р. 3. Петренко Т.А, Коротка Г.М., Задача розпізнавання образів в інтелектуальних системах виявлення кібератак // Всеукраїнсь-ка науково-практична конференція студентів, аспірантів та молодих вчених «Новітні технології у науковій діяльності і нав-чальному процесі» м. Чернігів, ЧНТУ, 2019. 4. Петренко Т.А, Коротка Г.М., Аналіз складових інформаційної безпеки систем електронного документообігу // Всеукраїн-ська науково-практична конференція студентів, аспірантів та молодих вчених «Новітні технології у науковій діяльності і на-вчальному процесі» м. Чернігів, ЧНТУ, 2020. 5. Петренко Т.А. Особливості управління доступом в сучасних операційних системах / Т.А. Петренко // Безпека ресурсів ін-формаційних систем : збірник тез І Міжнародної науково-практичної конференції (м. Чернігів 16-17 квітня 2020 р.). – Черні-гів : НУЧП, 2020. 16). Участь у професійних об'єднаннях за спеціальністю; ГО "Асоціація працівників кібербезпеки" 17). Досвід практичної роботи за спеціальністю не менше п'яти років; Інженер-програміст Чернігівського державного інституту права, соціальних технологій та праці (2005-2011) 18). Наукове консультування установ, підприємств, організацій протягом не менше двох років. ТОВ «Інформаційна безпека»
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	14	Проектування технічних систем захисту інформації	Кандидат технічних наук, 05.13.21 – Системи захисту інформації, Захист кандидатської дисертації (підвищення кваліфікації) 14.05.2020р. рішення атестаційної колегії № ДК 056619 Пункти 1,2,3,8, 10,13, 15,16, 17,18,19 Відповідає П 1, 2, 10, 13, 15, 16, 17, 18 має значну кі-лькість науко-вих та навчаль-но-методичних публікацій в напрямку спе-ціальності 1) 1. Development of adaptive expert system of information security using a procedure of clustering the attributes of anomalies and cyber attacks / Lakhno, V.,Tkach, Y.,Petrenko, T.,Zaitsev, S.,Bazylevych, V. // Eastern European Journal of Enterprise Technologies, 6/9 (84), 2016.- P. 32-44. Scopus (Особистий внесок: структурна схема адаптивної експертної системи, категорійна модель для визначення інформаційного критерію функціональної результативності навчання експертної системи). 2. V. Lakhno, S. Zaitsev, Y. Tkach, T. Petrenko, “Adaptive expert systems development for cyber attacks recognition in information educational systems on the basis of signs’ clustering”, Advances in Intelligent Systems and Computing, v. 754. pp. 673–682, 2018. (Особистий внесок: модель адаптивної системи розпізнавання, модифікована інформаційна умова функціональної результа-тивності навчання експертної системи). 2) 1. Д.Б. Мехед, Ю.М. Ткач Ю.М., В.М. Базилевич і Т.А. Петренко, “Аналіз загроз інформаційної безпеки в мережах стандарту IEEE 802.11”, Захист інформації, т. 17, №4. с. 285–291, 2015. 2. В.А. Лахно, Т.А Петренко і М.В. Пирог, “Моделювання роботи адаптивної системи розпізнавання кібератак в умовах неод-норідних потоків запитів в модулях e-business”, Безпека інформації, т. 22, № 2, с. 135–142, 2016. 3. В.А. Лахно, А.М. Терещук и Т.А.

							Петренко, “Совершенствование киберзащиты информационных систем за счет адаптив-ных технологий распознавания кибератак”, Захист інформації, т.18, № 2, с. 99–106, 2016. 4. В.М. Базилевич, М.В.. Мальцева, Т.А. Петренко, Л.Г. Черниш "Захищена система розумного будинку з використанням Internet of Things", Технічні науки та технології : науковий журнал / Чернігів. нац. технол. ун-т. – Чернігів : ЧНТУ, 2020. – № 2 (20). – С. 218-228. 5. Є.В. Риндич, Т.А. Петренко, Л.Г. Черниш, С.М. Семендяй, Г.С. Біленький "Навчальний стенд для вивчення дисциплін із забезпечення мережевого захисту інформації" / Чернігів. нац. технол. ун-т. – Чернігів : ЧНТУ, 2020. – № 2 (20). – С. 229-236. 10) Заступник завідувача кафедри кібербезпеки та математичного моделювання Національного університету Чернігівська полі-техніка 13) 1. Програма навчальної практики з управління інформаційною безпекою [Текст] / Петренко Т.А.. – Чернігів: Чернігівський національний технологічний університет, 2017. – 32 с. 2. Операційні системи: метод. вказівки до виконання розрах.-граф. роботи для студентів за напрямом підгот. (спец.) 6.170103 «Управління інформаційною безпекою», 125 «Кібербезпека» ден. форми навчання / уклад. Т. А. Петренко. – Чернігів : ЧНТУ, 2019. – 26 с. 3. Системи штучного інтелекту: метод. вказівки до виконання розрах.-граф. роботи для студентів за напрямом підгот. (спец.) 6.170103 «Управління інформаційною безпекою», 125 «Кібербезпека» ден. форми навчання / уклад. Т. А. Петренко. – Черні-гів: ЧНТУ, 2019. – 24 с. 3. Методичні вказівки до виконання випускної кваліфікаційної роботи здобувачів вищої освіти освітнього ступеню «бака-лавр» спеціальності 125 - «Кібербезпека»// Укл.: Т.А. Петренко, Ю.М. Ткач, Д.Б. Мехед - Чернігів: ЧНТУ, 2019. – 34с. 4. Кібербезпека. Методичні вказівки до виробничої практики [Текст] / розробник: Петренко Т.А. – Чернігів: Чернігівський національний технологічний університет, 2020. – 36 с. 15) 1. Система интеллектуальной поддержки принятия решений в слабо формализуемых задачах обеспечения кибербезопасности / Петренко Т.А., Лахно В.А.// Всеукраїнська науково-практична конференція студентів, аспірантів та молодих вчених «Нові-тні технології у науковій діяльності і навчальному процесі» м. Чернігів, ЧНТУ, 2017. 2. Метод та моделі адаптивних експертних систем розпізнавання кібератак на основі кластеризації ознак / Петренко Т.А., Ла-хно В.А // VII міжнародна науково-технічна конференція «ITSEC», м. Київ, НАУ, 16-18 травня, 2017р. 3. Петренко Т.А, Коротка Г.М., Задача розпізнавання образів в інтелектуальних системах виявлення кібератак // Всеукраїнсь-ка науково-практична конференція студентів, аспірантів та молодих вчених «Новітні технології у науковій діяльності і нав-чальному процесі» м. Чернігів, ЧНТУ, 2019. 4. Петренко Т.А, Коротка Г.М., Аналіз складових інформаційної безпеки систем електронного документообігу // Всеукраїн-ська науково-практична конференція студентів, аспірантів та молодих вчених «Новітні технології у науковій діяльності і на-вчальному процесі» м. Чернігів, ЧНТУ, 2020. 5. Петренко Т.А. Особливості управління доступом в сучасних операційних системах / Т.А. Петренко // Безпека ресурсів ін-формаційних систем : збірник тез І Міжнародної науково-практичної конференції (м. Чернігів 16-17 квітня 2020 р.). – Черні-гів : НУЧП, 2020. 16). Участь у професійних об’єднаннях за спеціальністю; ГО "Асоціація працівників кібербезпеки" 17). Досвід практичної роботи за спеціальністю не менше п’яти років; Інженер-програміст Чернігівського державного інституту права, соціальних технологій та праці (2005-2011) 18). Наукове консультування установ, підприємств, організацій протягом не менше двох років. ТОВ «Інформаційна безпека»
293250	Шелест Михайло Євгенович	Професор, Основне місце роботи	ННІ Електронних та інформаційних технологій	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	39	Методи побудови та аналізу криптосистем	Доктор технічних наук, спеціальність 05.13.21 - системи захисту інформації. Професор кафедри систем захисту інформації. Навчально-науковий інститут інформ-ційно-діагностичних систем Національного авіаційного університету, кафедра безпеки інформацій-них технологій, з 24.09.2018 по 22.03.2019 року. -

				03.07.2008			підвищення кваліфікації Довідка №03-02/825 від 29.03.2019р. Пункти 1,2,3,8,11,16,17, 18 1) Andrushchenko R., Zaitsev S., Druzhynin O., Shelest M. (2019) Method of Encoding Structured Messages by Using State Vectors. Selected Papers of 14th International Scientific-Practical Conference, MODS, 2019 June 24-26, Chernihiv, Ukraine. – 2019. – P. 144 – 153. 2) 1. Хорошко В.О., Хохлачова Ю.С., Шелест М.Є. Оцінка часу прийняття рішень в системах підтримки прийняття рішень // Ін-форматика та математичні методи в моделюванні, №3(т.8). - Одеса: Одеський НПУ, 2018. – С.209-223. 2. Гришук Р.В., Скачек Л.Н., Хорошко В.А., Шелест М.Е. Информационное противоборство: конфликты и противостояние // Інформаційна безпека. - Северодонецьк, 2018. - #4(32) - С.108-118. 3. Козюра В.Д., Хорошко В.О., Шелест М.Є. Аналіз кібернетичної безпеки інформаційного суспільства // Інформаційна безпека, №1(21). - К.: НА СБУ, 2017- С.163-170. 4. Шелест М.Є., Гнатюк С.О., Жмурко Т.О., Кінзерявий В.М., Юбузова Х.І. Експерементальне дослідження методу генерування тритових псевдовипадкових послідовностей для криптографічних застосувань // Захист інформації, №1, т.19. - К.:НАУ, 2017. – С.67-79. 5. Шелест М.Є., Рибальський В.О., Орєхова І.І. Методологічне забезпечення системи підготовки спеціалістів з інформаційної безпеки // Сучасна спеціальна техніка, №4. - К.:НА МВС, 2013. – С. 23-29. 6. 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 7. 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 8. 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 9. 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 3) 1)Хорошко В.А., Шелест М.Е. Информационно-аналитическое обеспечение безопасности: монография . – К.: ВПВ ""Задруга"", 2016 – 183 с. 2) Менеджмент інформаційної безпеки: навч.посібник для студентів спеціальності 125 «Кібербезпека»/ О.Г. Корченко, М.Є. Шелест, С.В. Казмірчук, Ю.М. Ткач, Є.В. Іванченко.-Ніжин:ФОП Лук'яненко В.В. ТПК «Орхідея», 2019.-408 с. 3) Проектування, введення в дію та супроводження КСЗІ: навчальний посібник / В.Д. Козюра, В.О. Хорошко, М.Є. Шелест, Ю.М. Ткач, С.В. Зайцев. – Ніжин: ФОП Лук'яненко В.В. ТПК «Орхідея», 2019. – 240 с. 4) Комплексні системи захисту інформації в інформаційно-телекоммунікаційних системах: Навч. посіб. / В.Д. Козюра, В.О. Хорошко, Ю.М. М.Є. Шелест, Ю.М. Ткач, Я.Ю. Усов. – Ніжин: ФОП Лук'яненко В.В. ТПК «Орхідея», 2019. – 145 с. 5) 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. 7) Робота в експертній раді з питань проведення експертизи дисертацій МОН з питань безпеки, оборони та спеціальних проблем оборono-промислового комплексу (до 2014 року включно). 8) 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; - ""Державна безпека України"", науково-практичний збірник Національної академії наук і Служби

							безпеки України (до 2014 року включно). 11) 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; - член спеціалізованої вченої ради СРД 26.706.02 Національної академії СБ України за спеціальністю 21.07.02-розвідувальна діяльність органів державної безпеки (до 2014 року включно). 16) Участь у професійних об'єднаннях за спеціальністю: ГО «Асоціація працівників кібербезпеки». 17) Більше 20 років в Службі зовнішньої розвідки 18) "Наукове консультування установ, підприємств, організацій протягом не менше двох років. ~~ТОВ «Інформаційна безпека»~~
293250	Шелест Михайло Євгенович	Професор, Основне місце роботи	ННІ Електронних та інформаційних технологій	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	39	Стандартизація, сертифікація засобів та комплексів захисту інформації	Доктор технічних наук, спеціальність 05.13.21 - системи захисту інформації. Професор кафедри систем захисту інформації. Навчально-науковий інститут інформ-ційно-діагностичних систем Національного авіаційного університету, кафедра безпеки інформацій-них технологій, з 24.09.2018 по 22.03.2019 року. - підвищення кваліфікації Довідка №03-02/825 від 29.03.2019р. Пункти 1,2,3,8,11,16,17, 18 1) Andrushchenko R., Zaitsev S., Druzhynin O., Shelest M. (2019) Method of Encoding Structured Messages by Using State Vectors. Selected Papers of 14th International Scientific-Practical Conference, MODS, 2019 June 24-26, Chernihiv, Ukraine. – 2019. – P. 144 – 153. 2) 1. Хорошко В.О., Хохлачова Ю.С., Шелест М.Є. Оцінка часу прийняття рішень в системах підтримки прийняття рішень // Ін-форматика та математичні методи в моделюванні, №3(т.8). - Одеса: Одеський НПУ, 2018. – С.209-223. 2. Гришук Р.В., Скачек Л.Н., Хорошко В.А., Шелест М.Е. Информационное противоборство: конфликты и противостояние // Інформаційна безпека. - Северодонецьк, 2018. - #4(32) - С.108-118. 3. Козюра В.Д., Хорошко В.О., Шелест М.Є. Аналіз кібернетичної безпеки інформаційного суспільства // Інформаційна безпека, №1(21). - К.: НА СБУ, 2017- С.163-170. 4. Шелест М.Є., Гнатюк С.О., Жмурко Т.О., Кінзерявий В.М., Юбузова Х.І. Експеременталь ное дослідження методу генерування тритових псевдовипадкових послідовностей для криптографічних застосувань // Захист інформації, №1, т.19. - К.:НАУ, 2017. – С.67-79. 5. Шелест М.Є., Рибальський В.О., Орєхова І.І. Методологічне забезпечення системи підготовки спеціалістів з інформаційної безпеки // Сучасна спеціальна техніка, №4. - К.:НА МВС, 2013. – С. 23-29. 6. 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 7. 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 8. 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 9. 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 3) 1)Хорошко В.А., Шелест М.Е. Информационно-аналитическое обеспечение безопасности: монография . – К.: ВПВ ""Задруга"", 2016 – 183 с. 2) Менеджмент інформаційної безпеки: навч.посібник для студентів спеціальності 125 «Кібербезпека»/ О.Г. Корченко, М.Є. Шелест, С.В. Казмірчук, Ю.М. Ткач, Є.В. Іванченко.-Ніжин:ФОП Лук'яненко В.В. ТПК «Орхідея», 2019.-408 с. 3) Проектування, введення в дію та супроводження КСЗІ: навчальний посібник / В.Д. Козюра, В.О. Хорошко, М.Є. Шелест, Ю.М. Ткач, С.В. Зайцев. – Ніжин: ФОП Лук'яненко В.В. ТПК «Орхідея», 2019.

							– 240 с. 4) Комплексні системи захисту інформації в інформаційно-телекоммунікаційних системах: Навч. посіб. / В.Д. Козюра, В.О. Хорошко, Ю.М. М.Є. Шелест, Ю.М. Ткач, Я.Ю. Усов. – Ніжин: ФОП Лук'яненко В.В. ТПК «Орхідея», 2019. – 145 с. 5) 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. 7) Робота в експертній раді з питань проведення експертизи дисертацій МОН з питань безпеки, оборони та спеціальних проблем оборонно-промислового комплексу (до 2014 року включно). 8) 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; - ""Державна безпека України"", науково-практичний збірник Національної академії наук і Служби безпеки України (до 2014 року включно). 11) 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; - член спеціалізованої вченої ради СРД 26.706.02 Національної академії СБ України за спеціальністю 21.07.02-розвідувальна діяльність органів державної безпеки (до 2014 року включно). 16) Участь у професійних об'єднаннях за спеціальністю: ГО «Асоціація працівників кібербезпеки». 17) Більше 20 років в Службі зовнішньої розвідки 18) "Наукове консультування установ, підприємств, організацій протягом не менше двох років. ТОВ «Інформаційна безпека»
331674	Базилевич Володимир Маркович	Завідувач кафедри, Основне місце роботи	ННІ Електронних та інформаційних технологій	Диплом спеціаліста, Чернігівський державний технологічний університет, рік закінчення: 2012, спеціальність: 091501 Комп'ютерні системи та мережі, Диплом магістра, Чернігівський національний технологічний університет, рік закінчення: 2017, спеціальність: 8.18010017 економіка довкілля і природних ресурсів, Диплом магістра, Чернігівський національний технологічний університет, рік закінчення: 2017, спеціальність: 8.18010017 економіка довкілля і природних ресурсів, Диплом кандидата наук ДК 033985, виданий 25.02.2016, Атестат доцента АД 000512, виданий 12.12.2017	7	Безпекові технології програмування	Кандидат економічних наук, 08.00.03 – економіка та управління національним господарством, тема дисертації: «Управління економічною безпекою АПК України», доцент кафедри кібербезпеки та математичного моделювання Навчально-науковий інститут інформаційно-діагностичних систем Національного авіаційного університету, кафедра безпеки информа-ційних технологій, з 25.09.2017 по 23.03.2018 року, Довідка №03.02/777 від 31.03.2018; Teacher`s internship program EPAM Systems, Червень-Серпень 2020 р. (Certificate №218) Пункти 1-3, 5-6,8-10, 13, 15, 18 1) 1. Development of adaptive expert system of information security using a procedure of clustering the attributes of anomalies and cyber attacks / Petrenko, T., Lakhno, V.,Tkach, Y., Zaitsev, S.,Bazylevych, V. // Eastern European Journal of Enterprise Technologies, 6/9 (84), 2016.- P. 32-44. https://www.scopus.com/authid/detail.uri?authorId=57193026076 2) 2. Аналіз загроз інформаційної безпеки в мережах стандарту IEEE 802.11 / Базилевич В.М., Ткач Ю.М., Мехед Д.Б., Петренко Т.А.. // Захист інформації. – 2015. –Том 17, №4.– С. 285–291. 3. Застосування методу експертних оцінок до оцінювання інформаційних ризиків вищого навчального закладу / Ю. М.Ткач, С. В. Казмірчук, Д. Б. Мехед, Д. Б. Базилевич. // Захист інформації. Київ:Національний Авіаційний Університет. – 2017. – №2. – С. 137–142. 4. Базилевич В.М. Аналіз методів захисту від кіберзагроз в бездротових мережах стандарту IEEE 802.11 / В. М. Базилевич. // Захист інформації Ukrainian Information Security Research Journal. – 2017. – №3. – С. 222–227 5. Застосування методу експертних оцінок до оцінювання інформаційних ризиків вищого навчального закладу / Ю. М.Ткач, С. В. Казмірчук, Д. Б. Мехед, Д. Б. Базилевич. // Захист інформації. Київ:Національний Авіаційний Університет. – 2017. – №2. – С. 137–142. 6. Bazylevych V. Development of criteria of protection from cyber threats at social enterprise / Bazylevych V., Mekhed D., Guryev V. // Technical sciences and technologies: scientific journal / Chernihiv National University of Technology. – Chernihiv : Chernihiv National University of Technology,

							2018. – № 3 (13). – P. 167-172. 7. Аналіз вразливостей корпоративних інформаційних систем / Д.Б. Мехед, Ю.М. Ткач, В.М. Базилевич, В.І. Гур'єв, Я.Ю. Усов // Захист інформації Ukrainian Information Security Research Journal. – 2018. – №1. – С. 61–66. 8. Мехед Д.Б. Дослідження технологій впливу та методів протидії фішингу / Мехед Д.Б., Ткач Ю.М., Базилевич В.М. // Захист інформації Ukrainian Information Security Research Journal. – 2019. – №4 (Том 21). – С. 246-251. 9. Базилевич В.М. Захищена система розумного будинку з використанням Internet of Things / Базилевич В., Мальцева М., Петренко Т., Черниш Л. // Технічні науки та технології : науковий журнал / Чернігів. нац. технол. ун-т. – Чернігів : ЧНТУ, 2020. – № 2 (20). – С. 218-229 3) 1. Базилевич В.М. Комп'ютерні мережі. Протоколи, технології, обладнання навч. посіб. для студ. спец. 125 «Кібербезпека» / В. М. Базилевич, Д. Б. Мехед, Ю. М. Ткач. – Ніжин: ФОП Лук'яненко В.В. ТПК «Орхідея», 2018. – 108 с. 2. Мехед Д.Б. Спеціальні глави математики. навч. посіб. для студ. спец. 125 «Кібербезпека» / Д. Б. Мехед, Ю. М. Ткач, В. М. Базилевич. – Ніжин: ФОП Лук'яненкоВ.В. ТПК «Орхідея», 2018. – 124 с. : іл. 3. Сучасні інформаційно-комунікаційні технології у навчанні математики в закладах вищої освіти / Ткач Ю.М., Трунова О.В., Мехед Д.Б., Базилевич В.М., Мурашковська В.П., Петрен-ко Т.А., Гур'єв В.І., Фірсова І.В. Монографія. – Чернігів: – 2016. - 360 с. 4. Екологічні аспекти сталого розвитку: монографія / [та інш.]; під заг. ред. д.е.н. проф. Ж.В. Дерій. – К.: Кондор-Видавництво, 2017. – 127 с. Базилевич В.М. Необхідність удосконалення методики оцінки рівня економічної безпеки агропромислового комплексу – С. 5-18. 5). 1. Учасник проекту (веб-розробник) THEOREMES-Dnipro «Підвищення ефективності інтегрованого управління транскордонними водними ресурсами річки Дніпро». 2. Учасник проекту (викладач) NUPASS «Норвегія-Україна. Професійна адаптація. Інтеграція в державну систему» 6) 3. Викладання англійською мовою дисциплін: Organization of databases, Statistical basics of computer engineering, Design and technological practice. 8) Відповідальний виконавець: 1. Методи та засоби забезпечення безпеки ресурсів інформаційних систем. Номер 0117U003187. Терміни виконання 04.17-04.22 9) 1. Член журі ІІІ етапу конкурсу"Мала академія наук України", 2020. 10) Завідувач кафедри інформаційних та комп'ютерних систем 13) 1. Бази даних і знань. Методичні вказівки до виконання курсової роботи / укл. Базилевич В.М., Мехед Д.Б. – Чернігів : ЧНТУ, 2016 – 28 с. 2. Комп'ютерні системи та мережі. Методичні вказівки до виконання курсового проекту для студентів спеціальності 125 «Кібербезпека» / укл. Базилевич В.М., Мехед Д.Б. – Чернігів: ЧНТУ, 2017. – 45 с. 3. Базилевич В.М. Інженерна та комп'ютерна графіка. Методичні вказівки до виконання розрахунково-графічної роботи для студентів напряму підготовки (спеціальності) 6.170103 Управління інформаційною безпекою», 125 «Кібербезпека» денної форми навчання / укл. Базилевич В.М., Ткач Ю.М. – Чернігів: ЧНТУ, 2019. – 38 с. 4. Інтернет-технології : метод. вказівки до виконання розрах.-граф. роботи для студентів напряму підгот. (спец.) 6.170103 «Управління інформаційною безпекою»,125 «Кібербезпека» ден. форми навчання / уклад.: В. М. Базилевич, Д. Б. Мехед. – Чернігів : ЧНТУ, 2019. – 12 с. 5. Імітаційне моделювання : метод. вказівки до виконання розрах. -граф. робіт для студентів напряму підгот. (спец.) 6.170103 «Управління інформаційною безпекою»,125 «Кібербезпека» ден. форми навчання / уклад.: Д. Б. Мехед, В. М. Базилевич. - Чернігів : ЧНТУ, 2019. - 12 с. 15) 1. Базилевич В. М. Оцінка ризиків інформаційної безпеки на підприємстві / Мехед Д. Б., Базилевич В. М., Петренко Т. А. // Стан та удосконалення безпеки інформаційно-телекомунікаційних систем: матеріали VII Всеукраїнської науково-практичної конференці (15-

							16 вересня 2015 р., м. Ізмаїл). – Миколаїв – Коблево: ТОВ «Ділова Інформація», 2015. – С.59-61 (0, 2 друк. арк.). Особистий внесок: класифікація ризиків інформаційній безпеці в рамках управління економічною безпекою національної економіки, 0,15 друк. арк. 2. Базилевич В.М. особливості захисту комп'ютерних систем при використанні їх дітьми / Біленький Г.С., Базилевич В.М. // Новітні технології у науковій діяльності і навчальному процесі : Всеукраїнська науково-практична конференція студентів, аспірантів та молодих учених (м. Чернігів, 18 - 19 травня 2016 р.) : збірник тез доповідей. - Чернігів : Черніг. нац. технол. ун-т, 2016. – С. 95-96 3. Базилевич В.М. Недоліки анонімних інтернет–сервісів на прикладі мережі TOR / Бригинець А.А., Базилевич В.М. // Новітні технології у науковій діяльності і навчальному процесі : Всеукраїнська науково-практична конференція студентів, аспірантів та молодих учених (м. Чернігів, 18 - 19 травня 2016 р.) : збірник тез доповідей. - Чернігів : Черніг. нац. технол. ун-т, 2016. – С. 96-98 4. Базилевич В.М. Формування стратегічних цілей сталого розвитку міста Чернігова на основі SWOT – аналізу / Базилевич В.М., Максьом К.В., Рубан О.А. // «Інноваційний розвиток інформаційного суспільства: економіко-управлінські, правові та соціокультурні аспекти»: збірник матеріалів V Міжнародної науково-практичної інтернет-конференції студентів, аспірантів і молодих учених (м. Чернігів, 23 грудня 2016 р.) / Черніг. нац. технол. ун-т. – Чернігів : Черніг. нац. технол. ун-т, 2016. – С. 16-20 5. V. Bazylevych Development of criteria of protection from cyber threats for social enterprises by analyzing the features of their functioning / Bazylevych V.M. //52nd Summit Conversations on Emerging Issues in Social Entrepreneurship – Lørenskog – Norway, 2017 6. Базилевич В.М. Шляхи діагностики деформації особистості службовців силових структур / Андрієнко О.В., Базилевич В.М. // Математичне та імітаційне моделювання систем. МОДС 2017: тези доповідей Дванадцятої міжнародної науково-практичної конференції (Чернігів, 26-29 червня 2017 р.) / М-во освіти і науки України, Нац. акад. наук України, Академія технологічних наук України, Інженерна академія України та ін. – Чернігів: ЧНТУ, 2017. – С. 58-61 7. Бойко К. В., Базилевич В. М. Використання VPN як спосіб захисту інформації Новітні технології у науковій діяльності і навчальному процесі : Всеукраїнська науково-практична конференція студентів, аспірантів та молодих учених (м. Чернігів, 11 -12 квітня 2018 р.) : збірник тез доповідей. - Чернігів : Черніг. нац. технол. ун-т, 2018. – С. 80-81 8. Васильєва С. П., Базилевич В. М. Аналіз технологій шифрування протоколу SSH. Новітні технології у науковій діяльності і навчальному процесі : Всеукраїнська науково-практична конференція студентів, аспірантів та молодих учених (м. Чернігів, 11 -12 квітня 2018 р.) : збірник тез доповідей. - Чернігів : Черніг. нац. технол. ун-т, 2018. – С. 86-87 9. Коротка Г.М., Базилевич В.М. Аналіз способів атаки мережевих екранів та методів їх захисту. Новітні технології у науковій діяльності і навчальному процесі : Всеукраїнська науково-практична конференція студентів, аспірантів та молодих учених (м. Чернігів, 11 -12 квітня 2018 р.) : збірник тез доповідей. - Чернігів : Черніг. нац. технол. ун-т, 2018. – С. 95-96 10. Мальцева М. М., Базилевич В. М. Аналіз методів соціальної інженерії як загроз кібербезпеки . Новітні технології у науковій діяльності і навчальному процесі : Всеукраїнська науково-практична конференція студентів, аспірантів та молодих учених (м. Чернігів, 11 -12 квітня 2018 р.) : збірник тез доповідей. - Чернігів : Черніг. нац. технол. ун-т, 2018. – С. 96-98 18) Здійснював наукове консультування установ, підприємств, організацій протягом не менше двох років, зокрема ТОВ «Інформаційна безпека» (довідка)
328320	Литвин Світлана Володимирівна	Завідувач кафедри, Основне місце роботи	ННІ Економіки	Диплом кандидата наук ДК 014822, виданий 12.06.2002, Атестат доцента 02ДЦ 011813, виданий 16.02.2006	27	Іноземна мова (за професійним спрямуванням)	Кандидат педагогічних наук – 12.06.2002; 13.00.02 „Теорія і методика навчання германсь-ким мовам”; „Навчання учнів старшої загально-освітньої школи писем-ного спілкування анг-лійською мовою”; до-цент – 16.02.2006 за ка-федрою іноземних мов, протокол № 1/55-Д The Interdisciplinary Professional Develop-men Program in the

framework of the Fourth International Scientific and Practice Conference “Ukraine – EU. Modern Technolo-gy, Business and Law” April 24-28 ,2018 (Slo-vak Republic-Czech Republic), Certificate №2018-4/25 of Advanced Training Dated: 28/04/2018 - підвищення кваліфікації
П.1, 2, 3, 5, 6, 8, 9, 10, 11, 13
1) S. V. Lytvyn, V. A. Perminova, A. I. Sikaliuk Vocational training of future economists as the potential of the development of the country: problems, solutions // Науковий вісник Полісся [Текст]. – Чернігів : ЧНТУ, 2016. – № 2 (6). - С. 45-50.
С. В. Литвин, В. А. Пермінова, А. І. Сікалюк Етика. сучасного менеджменту: соціально-етичні цінності майбутнього управління // Науковий вісник Полісся [Текст]. – Чернігів : ЧНТУ, 2016. – № 3 (7). - С. 277-281.
S. V. Lytvyn, V. A. Perminova, A. I. Sikaliuk Open educational environment as an integral part of innovative education // Науковий вісник Полісся [Текст]. – Чернігів : ЧНТУ, 2017. – № 1 (9). - С. 86-90.
Burmaka I., Stoianov N., Lytvynov V., Dorosh M., Lytvyn S. (2021) Proof of Stake for Blockchain Based Distributed Intrusion Detecting System. In: Shkarlet S., Morozov A., Palagin A. (eds) Mathematical Modeling and Simulation of Systems (MODS'2020). MODS 2020. Advances in Intelligent Systems and Computing, vol 1265. Springer, Cham. https://doi.org/10.1007/978-3-030-58124-4_23
Yakymenko, I., Kazymyr, V., Lytvyn, S. Webometrics ranking analysis and possible ways to improve the position of the university // Proceedings - 2020 IEEE 11th International Conference on Dependable Systems, Services and Technologies, DESSERT 2020, 9124999, с. 422-426

2) S. V. Lytvyn, V. A. Perminova Creative activity as an essential component of vocational training of students // Збірник наукових праць [Херсонського державного університету] : Педагогічні науки / Херсон. держ. ун-т. – Херсон: [б. в.], 2016. – Херсон. : Видавничий дім " “Міленіум” – 2017. – Вип. 76, Том. 2. - Виходить щоквартально. - ISSN 2413-1865
Svitlana Lytvyn Artem Tarasenko, Svitlana Lytvyn, Petro Dubyna Theoretical Aspects of Functioning and Development of Factoring / Проблеми і перспективи економіки та управління: науковий журнал / Чернігів. нац. технол. ун-т. – Чернігів : ЧНТУ, 2017. - №3 (11). – С. 135-144
S. V. Lytvyn, A. I. Sikaliuk CLIL technology in the process of teaching foreign language // Zprávy vědecké ideje – 2018: materiály XIV mezinárodní vědecko – praktická conference. – Volume 5. – Praha : Education and Science, 2018. – P. 76-78.
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 (pp. 99-109), 2020, No 1
Литвин С.В., Дивнич Г.А., Шевченко Ю.В. Оцінювання усного мовлення на заняттях з англійської мови за професійним спрямуванням у нелінгвістичних закладах вищої освіти. Вісник Луганського національного університету імені Тараса Шевченка. Серія: філологічні науки. №7 (330). Вид-во ДЗ «Луганський національний університет імені Тараса Шевченка», 2019. С. 138-146.
Лось О. В., Гаґіна Н. В., Литвин С. В. Навчання іноземної мови професійного спрямування в площині сучасної концепції підготовки фахівців. Вісник Національного університету «Чернігівський колегіум» імені Т. Г. Шевченка. Педагогічні науки. Чернігів, 2019. Вип. 5 (161). С. 115–120.
Ivan Burmaka, Stanislav Zlobin, Svitlana Lytvyn, Valentin Nekhai Detecting Flood Attacks and Abnormal System Usage with Artificial Immune System. Mathematical Modeling and Simulation of Systems Selected Papers of 14th International Scientific-Practical Conference, MODS, 2019 June 24-26, Chernihiv, Ukraine. – P. 131-143

3) Tool-Based Support of University-Industry Cooperation in IT-Engineering / V.V.Lytvynov, V.S.Kharchenko, S.V.Lytvyn, M.V.Saveliev, E.V.Trunova, I.S.Skiter Monograph – Chernihiv: Chernihiv National University of Technology, 2015. – 108 p.
Kazymyr V.V., Sklyar V.V., Lytvyn S.V., LytvynovV.V. Personal Communications Management for Academia-Industry Cooperation in IT-Engineering. training /Kharchenko V.S. – Ministry of Education and Science of Ukraine, Chernihiv National University of Technology, National Aerospace University “KhAI”. 2015. – 133p
Online Learning: Technologies and

							Practices / Kazymyr V.V., Verovko M.V., Drozde O.P., Lytvyn S.V. Monograph - Chernihiv: Publishing “Desna Poligraf”, 2016. – 223 p. S.V.Lytvyn, L.K Svetenok English for Scientific Communication: tutorial for students of the areas 8.05010201 „Computer Systems and Networks”, 8.05010202 “System Programming”, 8.05010301 “System Software”, 8.05010203 “Specialized Computer Systems” - Chernihiv: CNUT, 2016. – 176p. 5) 1.Участь у міжнародному проекті за сприяння Британської Ради “Англійська для університетів” (2014р.-2017р.) 2.Участь у проекті EU TEMPUS project 530319-TEMPUS-1-2012-1-DE-TEMPUS-JPHES “Innovation hybrid strategy of IT-outsourcing partnership with enterprises” (24.06.15-03.07.15), Technische Hochschule Wildau, Germany. 3. Участь у проекті TEMPUS CABRIOLET “Model-Oriented Approach and Intelligent Knowlendge-Based System for Evolvable Academia-Industry Cooperation in Electronic and Computer Engineering” (544497-TEMPUS-1-2013-1-UK-TEMPUS-JPHES). 4. Participation as a lecturer in February – May, 2019 in “Ukraine – Norway” Project “Retraining and social adaptation of military personnel and their family members in Ukraine”. Certificate of participant № 198. 6) Проведені навчальні занятя з дисципліни „Групова динаміка та комунікації” для напряму підготовки 6.050103 „Програмна інженерія” (64 год.) 8) Відповідальна за НДР Сучасні тенденції професійно зорієнтованого навчання іноземних мов у нелінгвістичних закладах вищої освіти. Держ. реєстр. № 0118U007002, 09.2018-03.2022 10) Завідуюча кафедри іноземних мом професійного спрямування 11) Офіційний опонент по дисертації Корнєєвої Ірини Олександрівни поданої на здобуття наукового ступеня кандидата педагогічних наук за спеціальністю 13.00.02 – теорія і методика навчання: германські мови. Запрошення Спеціалізованої вченої ради Д 26.054.01 від 09.09.2019 №1399/12-1 13) ENGLISH FOR LAWYERS. Методичні вказівки з англійської мови за професійним спрямуванням для самостійної роботи для студентів спеціальності 081 “Право”/Укл.: к.п.н. С.В. Литвин, к.п.н. Н.В. Гагіна, к. філ.н. О.В. Лось – Чернігів: ЧНТУ, 2018. – 50с. «Англійська мова в електроенергетичній та електротехнічній галузях. Методичні вказівки до практичних занять для студентів денної форми навчання напряму підготовки 141 «Електроенергетика, електротехніка та електромеханіка» / Укл. Литвин С.В., Сікалюк А.І., Пермінова В.А. – Чернігів : ЧНТУ, 2018. – 58 с. Англійська мова в будівництві та цивільній інженерії. Методичні вказівки для самостійної роботи студентів денної форми навчання спеціальності 192 „Будівництво та цивільна інженерія” І частина / Укл. Пермінова В.А., Сікалюк А.І., Литвин С.В. – Чернігів: ЧНТУ, 2019. – 80 с. FOR ACCOUNTING Методичні вказівки до практичних занять та самостійної роботи для студентів спеціальності "Облік і оподаткування" всіх форм навчання / Укладачі: Юсухно С.І., Литвин С.В. – Чернігів: ЧНТУ, 2019. – 99 с. Англійська мова в будівництві та цивільній інженерії. Методичні вказівки для самостійної роботи студентів денної форми навчання спеціальності 192 «Будівництво та цивільна інженерія». Частина ІІ. / Укл. Пермінова В.А., Сікалюк А.І., Литвин С.В. – Чернігів : ЧНТУ, 2020. – 86 с.
328102	Денисова Наталія Миколаївна	Доцент, Основне місце роботи	ННІ Менеджменту, харчових технологій та торгівлі	Диплом спеціаліста, Таврійська державна агротехнічна академія, рік закінчення: 1999, спеціальність: 091901 Енергетика сільськогосподарського виробництва, 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	19	Цивільний захист та охорона праці в галузі	Кандидат технічних наук, 05.26.01 – охорона праці. Тема дисертації «Зниження забрудненості повітря робочої зони при формуванні поліамідних ниток», доцент кафедри харчових технологій, хімії та БЖД Міжнародна академія безпеки життєдіяльності, м. Київ, академік Міжнародної академії безпеки життєдіяльності, диплом від 11.11.2016р. (протокол №59/16) – підвищення кваліфікації Пункти 1,2,3,13,15,16 1) 1.Gorodny A., Dymerets A., Kuts Ye., Denisov Yu., Denisova N. “Generalized Method of Commutation Processes Calculation in High-Frequency Switched-mode Power Converters”, Mathematical Modeling and Simulation of Systems, pp. 71-80. 2) 1. Буяльська Н., Купчик О., Денисова Н. Використання сорбентів для зниження концентрації важких металів у молочній сировині //Технічні науки та технології : науковий журнал / Чернігів. нац. технол. ун-т. – Чернігів : ЧНТУ, 2019.

							– № 1 (15). – С. 181-189 2. Денисова Н., Гаркава А., Буяльська Н. Використання зброджeного яблучного соку в технології виробництва житньо-пшеничного хліба / Технічні науки та технології : науковий журнал / Чернігів. нац. технол. ун-т. – Чернігів : ЧНТУ, 2019. – № 2 (16). – С. 129-137 3. Буяльська Н., Воєдило В., Денисова Н. Використання йодовмісних добавок у виробництві хлібобулочних виробів оздоровчого призначення // Технічні науки та технології : науковий журнал / Чернігів. нац. технол. ун-т. – Чернігів : ЧНТУ, 2019. – № 2 (16). – С. 137-145 4. Буяльська Н., Литвиненко О., Денисова Н. Використання продуктів переробки амаранту у виробництві хлібобулочних виробів //Технічні науки та технології : науковий журнал / Чернігів. нац. технол. ун-т. – Чернігів : ЧНТУ, 2019. – № 3 (17). – С. 226-234 5. Денисова Н., Зінюк М., Буяльська Н. Використання добавок безглютенового борошна в технології виробництва хлібобулочних виробів // Технічні науки та технології : науковий журнал / Чернігів. нац. технол. ун-т. – Чернігів : ЧНТУ, 2019. – № 3 (17). –. С. 234-241 3) Підвищення харчової цінності хлібобулочних і борошняних кондитерських виробів/ Буяльська Н.П., Гуменюк О.Л, Денисова Н.М., Челябієва В.М.: монографія. - Чернігів: ЧНТУ, 2020 – 122 с. 2. Нальотова Н.І., Дрогомерецька Г.В., Білаш Т.А., Цибуля С.Д., Денисова Н.М. Технологічні операції з ПММ: Навчальний посібник. – Кременчук: КЛК ХНУВС, 2019.- 101 с. 13) 1. 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. 2. Охорона праці в галузі. Методичні вказівки до виконання лабораторних робіт для студентів галузі знань 13 – Механічна інженерія Спеціальність 131 Прикладна механіка (Освітня професійна програма"Технології та устаткування зварювання")/ Укл.: Денисова Н.М., Буяльська Н.П. – Чернігів: ЧНТУ, 2020. –79 с. 3.Санітарія і гігієна підприємств харчової промисловості. Методичні вказівки до виконання лабораторних робіт для студентів напряму підготовки 181-харчові технології/ Укл.: Денисова Н.М., Буяльська Н.П. – Чернігів: ЧНТУ, 2018. –106 с. 4. Промислова екологія харчових виробництв : метод. вказівки до виконання індивід. роботи для студентів спец. 181 "Харчові технології" / уклад.: Н. П. Буяльська, Н. М. Денисова. – Чернігів : ЧНТУ, 2019. – 48 с.(англ) 5. Industrial Ecology. Course of lectures for students of the specialty 181 - Food Technologies // N.P.Buialska, N.M. Denisova. – Chernihiv: CNTU, 2018. – 82 p. 15) 1. Дослідження вмісту важких металів у харчоконцентратах/ Ющенко Н.Ф., Буяльська Н.П., Денисова Н.М., доц. // Новітні технології у науковій діяльності і навчальному процесі: Всеукраїнська науково-практична конференція студентів, аспірантів та молодих учених (м. Чернігів, 8 - 9 квітня 2020 р.) : збірник тез доповідей. - Чернігів :Черніг. нац. технол. ун-т, 2020. – С. 437-438. 2. Денисова Н.М., Карцан В.Д. Оцінка рівня якості плодово-ягідного морозива з удосконаленим білково-вуглеводним складом Національний університет «Чернігівська політехніка», м. Чернігів// Комплексне забезпечення якості технологічних процесів та систем (КЗЯТПС – 2020): матеріали тез доповідей X Міжнародної науково-практичної конференції (м. Чернігів , 29–30 квітня 2020 р.): у 2-х т. – Чернігів : ЧНТУ, 2020. – Т. 1. – С. 256-258. 3. Гаркава А. В., Денисова Н.М. Розробка технології приготування житньо-пшеничного хлібу на заквасках з використанням яблучного сидру/ Новітні технології у науковій діяльності і навчальному процесі : Всеукраїнська науково-практична конференція студентів, аспірантів та молодих учених (м. Чернігів, 10 -11 квітня 2019 р.) : збірник тез доповідей. - Чернігів : Черніг. нац. технол. ун-т, 2019. – С.275-276 4. Зінюк М.О., Денисова Н.М. Розробка технології приготування хлібобулочних виробів з використанням рисового, гречаного та кукурудзяного борошна/ Новітні технології у науковій діяльності і навчальному процесі : Всеукраїнська науково-практична конференція студентів, аспірантів та молодих учених (м. Чернігів, 10 -11 квітня 2019 р.) : збірник тез доповідей. - Чернігів : Черніг. нац. технол. ун-т, 2019. – С.277-278.

							5. Застосування цукрозамінників під час виробництва бісквітів із зниженим показником глікемічності //Денисова Н.М..,Корзаченко А.Г..// Новітні технології сучасного суспільства (НТСС -2018): науково-практична конференція (м.Чернігів, 12 грудня 2018 р.):тези доповідей. – Чернігів: ЧНТУ, 2018.- с.53 16) 1. Міжнародна академія безпеки життєдіяльності. 2. Європейське співтовариство з охорони праці (ESOSH)

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

Програмні результати навчання ОП	ПРН відповідає результату навчання, визначеному стандартом вищої освіти (або охоплює його)	Обов'язкові освітні компоненти, що забезпечують ПРН	Методи навчання	Форми та методи оцінювання
ПРН 5. - реалізовувати процеси постійної самоосвіти і професійної сертифікації, критично осмислювати основні теорії, принципи, методи і поняття у навчанні та професійній діяльності;	☐	Безпекові технології програмування	Лекційні та лабораторні заняття, самостійна аудиторна та поза аудиторна робота здобувачів вищої освіти, консультації	Підсумкові усні опитування здобувачів вищої освіти, виконання розрахунково-графічної роботи, поточний контроль та залік
		Переддипломна практика	Спостереження, впровадження, демонстрація, проектування.	Представлення та захист звіту з практики
		Підготовка до кваліфікаційної роботи	Консультації	Публічний захист випускної кваліфікаційної роботи, презентація
		Проектування технічних систем захисту інформації	Лекційні та лабораторні заняття, самостійна аудиторна та поза аудиторна робота здобувачів вищої освіти, консультації	Підсумкові усні опитування та письмові здобувачів вищої освіти, виконання курсового проекту, поточний та екзаменаційний контроль
		Методологія та організація наукових досліджень	Лекційні та практичні заняття, самостійна аудиторна та поза аудиторна робота здобувачів вищої освіти, консультації	Підсумкові усні опитування здобувачів вищої освіти, виконання контрольної роботи, поточний контроль та залік
		Цивільний захист та охорона праці в галузі	Лекційні та практичні заняття, самостійна аудиторна та поза аудиторна робота здобувачів вищої освіти, консультації	Підсумкові усні опитування здобувачів вищої освіти, поточний контроль та залік
ПРН 8. - проектувати, впроваджувати, супроводжувати системи та комплекси (програмні, програмно-апаратні) захисту додатків (веб - додатків) з метою забезпечення якісного функціонування інформаційно-комунікаційних систем, згідно встановленої політики інформаційної безпеки та/або кібербезпеки і стратегії організації;	☐	Проектування технічних систем захисту інформації	Лекційні та лабораторні заняття, самостійна аудиторна та поза аудиторна робота здобувачів вищої освіти, консультації	Підсумкові усні опитування та письмові здобувачів вищої освіти, виконання курсового проекту, поточний та екзаменаційний контроль
		Управління мережевою безпекою	Лекційні та лабораторні заняття, самостійна аудиторна та поза аудиторна робота здобувачів вищої освіти, консультації	Підсумкові усні опитування та письмові опитування здобувачів вищої освіти, виконання розрахунково-графічної роботи, поточний контроль та залік
		Безпекові технології програмування	Лекційні та лабораторні заняття, самостійна аудиторна та поза аудиторна робота здобувачів вищої освіти, консультації	Підсумкові усні опитування здобувачів вищої освіти, виконання розрахунково-графічної роботи, поточний контроль та залік
ПРН 9. - розробляти, впроваджувати та аналізувати заходи, щодо резервування інформаційних ресурсів, розробки планів відновлення штатного функціонування інфраструктури організації в цілому, які викликані реалізацією різного класу кібератак, виявленням і реєстрацією інцидентів та нештатних ситуацій;	☐	Аудит та управління інцидентами інформаційної безпеки	Лекційні та практичні заняття, самостійна аудиторна та поза аудиторна робота здобувачів вищої освіти, консультації	Підсумкові усні опитування та письмові опитування здобувачів вищої освіти, виконання розрахунково-графічної роботи (РГР), поточний та екзаменаційний контроль
		Стандартизація, сертифікація засобів та комплексів захисту інформації	Лекційні та лабораторні заняття, самостійна аудиторна та поза аудиторна робота здобувачів вищої освіти, консультації	Підсумкові усні опитування здобувачів вищої освіти, виконання розрахунково-графічної роботи, поточний та екзаменаційний контроль
ПРН 1. - постійно вдосконалювати та застосовувати знання державної та іноземних мов з метою забезпечення ефективності професійної комунікації	☐	Іноземна мова (за професійним спрямуванням)	Практичні заняття, самостійна аудиторна та поза аудиторна робота здобувачів вищої освіти, консультації	Підсумкові усні опитування та письмові опитування здобувачів вищої освіти, поточний контроль та залік
		Методологія та організація наукових досліджень	Лекційні та практичні заняття, самостійна аудиторна та поза аудиторна робота здобувачів вищої освіти, консультації	Підсумкові усні опитування здобувачів вищої освіти, виконання контрольної роботи, поточний контроль та залік
		Проектування технічних систем захисту інформації	Лекційні та лабораторні заняття, самостійна аудиторна та поза аудиторна робота здобувачів вищої освіти, консультації	Підсумкові усні опитування та письмові здобувачів вищої освіти, виконання курсового проекту, поточний та екзаменаційний контроль
ПРН 10. - розробляти, планувати, аналізувати та впроваджувати систему доступу до інформаційних ресурсів, інформаційно-комунікаційних систем (вузлів доступу до глобальних мереж, програмно - апаратних комплексів, підсистем, програмного забезпечення, тощо), згідно встановленої політики інформаційної безпеки та/або кібербезпеки і стратегії організації;	☐	Аудит та управління інцидентами інформаційної безпеки	Лекційні та практичні заняття, самостійна аудиторна та поза аудиторна робота здобувачів вищої освіти, консультації	Підсумкові усні опитування та письмові опитування здобувачів вищої освіти, виконання розрахунково-графічної роботи (РГР), поточний та екзаменаційний контроль
		Управління мережевою безпекою	Лекційні та лабораторні заняття, самостійна аудиторна та поза аудиторна робота здобувачів вищої освіти, консультації	Підсумкові усні опитування та письмові опитування здобувачів вищої освіти, виконання розрахунково-графічної роботи, поточний контроль та залік
ПРН 11. - розробляти, впроваджувати, супроводжувати системи аудиту та моніторингу (контролю) якості бізнес/операційних процесів функціонування організації та системи управління інформаційною безпекою та/або кібербезпекою за вітчизняними і світовими нормами та стандартами;	☐	Аудит та управління інцидентами інформаційної безпеки	Лекційні та практичні заняття, самостійна аудиторна та поза аудиторна робота здобувачів вищої освіти, консультації	Підсумкові усні опитування та письмові опитування здобувачів вищої освіти, виконання розрахунково-графічної роботи (РГР), поточний та екзаменаційний контроль
		Безпекові технології програмування	Лекційні та лабораторні заняття, самостійна аудиторна та поза аудиторна робота здобувачів вищої освіти, консультації	Підсумкові усні опитування здобувачів вищої освіти, виконання розрахунково-графічної роботи, поточний контроль та залік
ПРН 14. - розробляти, впроваджувати, та організовувати реалізацію процесів з використанням методів та засобів криптографічного та технічного захисту інформації на об'єктах інформаційної діяльності, згідно встановленої	☐	Методи побудови та аналізу криптосистем	Лекційні та лабораторні заняття, самостійна аудиторна та поза аудиторна робота здобувачів вищої освіти, консультації	Підсумкові усні опитування та письмові опитування здобувачів вищої освіти, виконання розрахунково-графічної роботи, поточний та екзаменаційний контроль
		Проектування технічних систем захисту інформації	Лекційні та лабораторні заняття, самостійна аудиторна та поза аудиторна робота здобувачів вищої освіти, консультації	Підсумкові усні опитування та письмові здобувачів вищої освіти, виконання курсового проекту, поточний та екзаменаційний контроль

політики інформаційної безпеки та/або кібербезпеки і стратегії організації;				
ПРН 7. - проектувати, впроваджувати, та супроводжувати інформаційно-комунікаційні системи, а також забезпечувати захист інформаційних ресурсів мереж (мережева безпека) та всієї інфраструктури установи на базі сучасних моделей, методів і засобів передачі даних в комутативних або без комутативних каналах зв'язку, хмарного простору, протоколів обміну даними, мережного устаткування, тощо;	☐	Аудит та управління інцидентами інформаційної безпеки	Лекційні та практичні заняття, самостійна аудиторна та поза аудиторна робота здобувачів вищої освіти, консультації	Підсумкові усні опитування та письмові опитування здобувачів вищої освіти, виконання розрахунково-графічної роботи (РГР), поточний та екзаменаційний контроль
		Стандартизація, сертифікація засобів та комплексів захисту інформації	Лекційні та лабораторні заняття, самостійна аудиторна та поза аудиторна робота здобувачів вищої освіти, консультації	Підсумкові усні опитування здобувачів вищої освіти, виконання розрахунково-графічної роботи, поточний та екзаменаційний контроль
		Управління мережевою безпекою	Лекційні та лабораторні заняття, самостійна аудиторна та поза аудиторна робота здобувачів вищої освіти, консультації	Підсумкові усні опитування та письмові опитування здобувачів вищої освіти, виконання розрахунково-графічної роботи, поточний контроль та залік
ПРН 2. - планувати та організовувати власну професійну діяльність, обирати оптимальні методи та способи розв'язування складних спеціалізованих задач та практичних проблем у професійній діяльності, оцінювати їхню ефективність;	☐	Методологія та організація наукових досліджень	Лекційні та практичні заняття, самостійна аудиторна та поза аудиторна робота здобувачів вищої освіти, консультації	Підсумкові усні опитування здобувачів вищої освіти, виконання контрольної роботи, поточний контроль та залік
		Проектування технічних систем захисту інформації	Лекційні та лабораторні заняття, самостійна аудиторна та поза аудиторна робота здобувачів вищої освіти, консультації	Підсумкові усні опитування та письмові здобувачів вищої освіти, виконання курсового проекту, поточний та екзаменаційний контроль
		Безпекові технології програмування	Лекційні та лабораторні заняття, самостійна аудиторна та поза аудиторна робота здобувачів вищої освіти, консультації	Підсумкові усні опитування здобувачів вищої освіти, виконання розрахунково-графічної роботи, поточний контроль та залік
		Управління мережевою безпекою	Лекційні та лабораторні заняття, самостійна аудиторна та поза аудиторна робота здобувачів вищої освіти, консультації	Підсумкові усні опитування та письмові опитування здобувачів вищої освіти, виконання розрахунково-графічної роботи, поточний контроль та залік
		Переддипломна практика	Спостереження, впровадження, демонстрація, проектування.	Представлення та захист звіту з практики
		Підготовка до кваліфікаційної роботи	Консультації	Публічний захист випускної кваліфікаційної роботи, презентація
		Аудит та управління інцидентами інформаційної безпеки	Лекційні та практичні заняття, самостійна аудиторна та поза аудиторна робота здобувачів вищої освіти, консультації	Підсумкові усні опитування та письмові опитування здобувачів вищої освіти, виконання розрахунково-графічної роботи (РГР), поточний та екзаменаційний контроль
ПРН 12. - розробляти, впроваджувати та супроводжувати процеси належного функціонування системи моніторингу інформаційних ресурсів і бізнес процесів в інфраструктурі організації	☐	Аудит та управління інцидентами інформаційної безпеки	Лекційні та практичні заняття, самостійна аудиторна та поза аудиторна робота здобувачів вищої освіти, консультації	Підсумкові усні опитування та письмові опитування здобувачів вищої освіти, виконання розрахунково-графічної роботи (РГР), поточний та екзаменаційний контроль
		Безпекові технології програмування	Лекційні та лабораторні заняття, самостійна аудиторна та поза аудиторна робота здобувачів вищої освіти, консультації	Підсумкові усні опитування здобувачів вищої освіти, виконання розрахунково-графічної роботи, поточний контроль та залік
		Управління мережевою безпекою	Лекційні та лабораторні заняття, самостійна аудиторна та поза аудиторна робота здобувачів вищої освіти, консультації	Підсумкові усні опитування та письмові опитування здобувачів вищої освіти, виконання розрахунково-графічної роботи, поточний контроль та залік
ПРН 3. - використовувати результати самостійного пошуку, аналізу та синтезу інформації з різних джерел для ефективного рішення спеціалізованих задач професійної діяльності	☐	Стандартизація, сертифікація засобів та комплексів захисту інформації	Лекційні та лабораторні заняття, самостійна аудиторна та поза аудиторна робота здобувачів вищої освіти, консультації	Підсумкові усні опитування здобувачів вищої освіти, виконання розрахунково-графічної роботи, поточний та екзаменаційний контроль
		Переддипломна практика	Спостереження, впровадження, демонстрація, проектування.	Спостереження, впровадження, демонстрація, проектування.
		Підготовка до кваліфікаційної роботи	Консультації	Консультації
		Іноземна мова (за професійним спрямуванням)	Практичні заняття, самостійна аудиторна та поза аудиторна робота здобувачів вищої освіти, консультації	Підсумкові усні опитування та письмові опитування здобувачів вищої освіти, поточний контроль та залік
		Аудит та управління інцидентами інформаційної безпеки	Лекційні та практичні заняття, самостійна аудиторна та поза аудиторна робота здобувачів вищої освіти, консультації	Підсумкові усні опитування та письмові опитування здобувачів вищої освіти, виконання розрахунково-графічної роботи (РГР), поточний та екзаменаційний контроль
		Методологія та організація наукових досліджень	Лекційні та практичні заняття, самостійна аудиторна та поза аудиторна робота здобувачів вищої освіти, консультації	Підсумкові усні опитування здобувачів вищої освіти, виконання контрольної роботи, поточний контроль та залік
		Проектування технічних систем захисту інформації	Лекційні та лабораторні заняття, самостійна аудиторна та поза аудиторна робота здобувачів вищої освіти, консультації	Підсумкові усні опитування та письмові здобувачів вищої освіти, виконання курсового проекту, поточний та екзаменаційний контроль
		Безпекові технології програмування	Лекційні та лабораторні заняття, самостійна аудиторна та поза аудиторна робота здобувачів вищої освіти, консультації	Підсумкові усні опитування здобувачів вищої освіти, виконання розрахунково-графічної роботи, поточний контроль та залік
		Методи побудови та аналізу криптосистем	Лекційні та лабораторні заняття, самостійна аудиторна та поза аудиторна робота здобувачів вищої освіти, консультації	Підсумкові усні опитування та письмові опитування здобувачів вищої освіти, виконання розрахунково-графічної роботи, поточний та екзаменаційний контроль
		Управління мережевою безпекою	Лекційні та лабораторні заняття, самостійна аудиторна та поза аудиторна робота здобувачів вищої освіти, консультації	Підсумкові усні опитування та письмові опитування здобувачів вищої освіти, виконання розрахунково-графічної роботи, поточний контроль та залік
ПРН 4. - аналізувати, аргументувати, приймати рішення при розв'язанні складних спеціалізованих задач та практичних проблем у професійній діяльності, які характеризуються комплексністю та неповною визначеністю умов, відповідати за прийняті рішення;	☐	Безпекові технології програмування	Лекційні та лабораторні заняття, самостійна аудиторна та поза аудиторна робота здобувачів вищої освіти, консультації	Підсумкові усні опитування здобувачів вищої освіти, виконання розрахунково-графічної роботи, поточний контроль та залік
		Методи побудови та аналізу криптосистем	Лекційні та лабораторні заняття, самостійна аудиторна та поза аудиторна робота здобувачів вищої освіти, консультації	Підсумкові усні опитування та письмові опитування здобувачів вищої освіти, виконання розрахунково-графічної роботи, поточний та екзаменаційний контроль
		Переддипломна практика	Спостереження, впровадження, демонстрація, проектування.	Представлення та захист звіту з практики
		Проектування технічних систем захисту інформації	Лекційні та лабораторні заняття, самостійна аудиторна та поза аудиторна робота здобувачів вищої освіти, консультації	Підсумкові усні опитування та письмові здобувачів вищої освіти, виконання курсового проекту, поточний та екзаменаційний контроль
		Стандартизація, сертифікація засобів та комплексів захисту інформації	Лекційні та лабораторні заняття, самостійна аудиторна та поза аудиторна робота здобувачів вищої освіти, консультації	Підсумкові усні опитування здобувачів вищої освіти, виконання розрахунково-графічної роботи, поточний та екзаменаційний контроль
		Підготовка до кваліфікаційної роботи	Консультації	Публічний захист випускної кваліфікаційної роботи, презентація
		Аудит та управління інцидентами	Лекційні та практичні заняття, самостійна	Підсумкові усні опитування та письмові

		інформаційної безпеки	аудиторна та поза аудиторна робота здобувачів вищої освіти, консультації	опитування здобувачів вищої освіти, виконання розрахунково-графічної роботи (РГР), поточний та екзаменаційний контроль
ПРН 6. - діяти на основі законодавчої та нормативно-правової бази України та вимог відповідних стандартів, у тому числі у напрямах найкращих практик, технічних вимог та рекомендацій з управління інформаційною безпекою та /або кібербезпекою;	☐	Цивільний захист та охорона праці в галузі	Лекційні та практичні заняття, самостійна аудиторна та поза аудиторна робота здобувачів вищої освіти, консультації	Підсумкові усні опитування здобувачів вищої освіти, поточний контроль та залік
		Аудит та управління інцидентами інформаційної безпеки	Лекційні та практичні заняття, самостійна аудиторна та поза аудиторна робота здобувачів вищої освіти, консультації	Підсумкові усні опитування та письмові опитування здобувачів вищої освіти, виконання розрахунково-графічної роботи (РГР), поточний та екзаменаційний контроль
		Стандартизація, сертифікація засобів та комплексів захисту інформації	Лекційні та лабораторні заняття, самостійна аудиторна та поза аудиторна робота здобувачів вищої освіти, консультації	Підсумкові усні опитування здобувачів вищої освіти, виконання розрахунково-графічної роботи, поточний та екзаменаційний контроль
		Методи побудови та аналізу криптосистем	Лекційні та лабораторні заняття, самостійна аудиторна та поза аудиторна робота здобувачів вищої освіти, консультації	Підсумкові усні опитування та письмові опитування здобувачів вищої освіти, виконання розрахунково-графічної роботи, поточний та екзаменаційний контроль
		Управління мережевою безпекою	Лекційні та лабораторні заняття, самостійна аудиторна та поза аудиторна робота здобувачів вищої освіти, консультації	Підсумкові усні опитування та письмові опитування здобувачів вищої освіти, виконання розрахунково-графічної роботи, поточний контроль та залік
ПРН 13. - проводити та планувати навчання персоналу компанії, користувачів з інформаційних технологій організації у відповідності до сучасних норм, вимог, внутрішніх правил безпечного застосування інформаційних технологій, а також у відповідність вітчизняним і світовим стандартам галузі інформаційної та\або кібербезпеки;	☐	Цивільний захист та охорона праці в галузі	Лекційні та практичні заняття, самостійна аудиторна та поза аудиторна робота здобувачів вищої освіти, консультації	Підсумкові усні опитування здобувачів вищої освіти, поточний контроль та залік
		Безпекові технології програмування	Лекційні та лабораторні заняття, самостійна аудиторна та поза аудиторна робота здобувачів вищої освіти, консультації	Підсумкові усні опитування здобувачів вищої освіти, виконання розрахунково-графічної роботи, поточний контроль та залік