НАЦІОНАЛЬНЕ АГЕНТСТВО ІЗ ЗАБЕЗПЕЧЕННЯ ЯКОСТІ ВИЩОЇ ОСВІТИ

ВІДОМОСТІ
про самооцінювання освітньої програми

Заклад вищої освіти	**Державний торговельно-економічний університет**
Освітня програма	**55058 Безпека систем електронних комунікацій в економіці**
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

Савченко П. В.

Хаустова О. В.

Загальні відомості

1. Інформація про ЗВО (ВСП ЗВО)

Реєстраційний номер ЗВО у ЄДЕБО	**6594**
Повна назва ЗВО	**Державний торговельно-економічний університет**
Ідентифікаційний код ЗВО	**44470624**
ПІБ керівника ЗВО	**Мазаракі Анатолій Антонович**
Посилання на офіційний веб-сайт ЗВО	

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

https://registry.edbo.gov.ua/university/6594

3. Загальна інформація про ОП, яка подається на акредитацію

ID освітньої програми в ЄДЕБО	**55058**
Назва ОП	**Безпека систем електронних комунікацій в економіці**
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 інженерії програмного забезпечення та кібербезпеки**
Інші навчальні структурні підрозділи (кафедра або інші підрозділи), залучені до реалізації ОП	**Кафедра сучасних європейських мов, кафедра філософії, соціології та політології, кафедра правового забезпечення безпеки бізнесу, кафедра цифрової економіки та системного аналізу, кафедра психології, кафедра адміністративного, фінансового та інформаційного права**
Місце (адреса) провадження освітньої діяльності за ОП	**02156, м. Київ, вул. Кіото, 19**
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	**414197**
ПІБ гаранта ОП	**Савченко Тетяна Віталіївна**
Посада гаранта ОП	**Доцент**
Корпоративна електронна адреса гаранта ОП	**savchenko_tv@knute.edu.ua**
Контактний телефон гаранта ОП	**+38(050)-559-70-29**
Додатковий телефон гаранта ОП	**+38(044)-592-85-70**

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

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

В сучасних умовах, коли Україна захищає свою національну безпеку та цілісність від країни-агресора, кіберпростір – це стратегічно важливий фронт. З початку війни наша країна стала ціллю чисельних кібератак на державні установи, приватні організації та громадян, особливої уваги потребують підприємства, що є частиною критичної інфраструктури та є пріоритетними цілями в період війни. З розвитком цифрової економіки та віртуальної реальності проблема захисту особистої та комерційної інформації є особливо гострою, тому роль фахівців з кібербезпеки зростає й стає ще актуальнішою з розвитком інформатизації суспільства. Незважаючи на велику кількість закладів вищої освіти, що готують фахівців у галузі інформаційних технологій, в Україні та в усьому світі залишається потреба в спеціалістах з кібербезпеки. Для забезпечення зростаючих потреб ринку праці у фахівцях з кібербезпеки та захисту інформації в Київському національному торговельно-економічному університеті на кафедрі програмної інженерії та інформаційних систем була започаткована освітня програма «Безпека інформаційних і комунікаційних систем в економіці». Розробці освітньої програми передував моніторинг ринку праці та запитів роботодавців, аналіз існуючих ОП закладів вищої освіти України зі спеціальності 125 «Кібербезпека» та аналогічних програм провідних університетів світу. Перший набір на освітню програму в кількості 27 осіб було здійснено в 2018 році виключно за кошти фізичних осіб. У 2022 році було проведено успішну акредитацію ОП «Безпека інформаційних і комунікаційних систем в економіці» першого (бакалаврського) рівня (сертифікат про акредитацію №3588 від 23.06.2022). У цьому ж році в Державному торговельно-економічному університеті на кафедрі інженерії програмного забезпечення та кібербезпеки було започатковано освітньо-професійну програму «Безпека систем електронних комунікацій в економіці» на другому (магістерському) рівні вищої освіти. Перший набір на дану освітню програму склав 57 осіб (38 денної та 19 заочної форми навчання).
Отже, на акредитацію подано першу редакцію освітньо-професійної програми «Безпека систем електронних комунікацій в економіці» другого (магістерського) рівня вищої освіти спеціальності 125 «Кібербезпека» 2022 року, що адаптована до нових вимог і потреб регіонального ринку праці, а також враховано рекомендації стейкхолдерів та учасників освітнього процесу (http://surl.li/ktidc). Освітньо-професійна програма була розроблена робочою групою у складі: Пашорін В.І. – професор кафедри інженерії програмного забезпечення та кібербезпеки (керівник робочої групи), к.т.н., професор; Криворучко О.В. – завідувач кафедри інженерії програмного забезпечення та кібербезпеки, д.т.н., професор; Савченко Т.В. – доцент кафедри інженерії програмного забезпечення та кібербезпеки, к.т.н., доцент; Токар В.В. – професор кафедри інженерії програмного забезпечення та кібербезпеки, д.е.н., професор; Харченко О.А. – декан факультету інформаційних технологій, к.т.н., доцент; Сашньова М.В. – доцент кафедри інженерії програмного забезпечення та кібербезпеки, к.т.н., доцент; Десятко А.М. – доцент кафедри інженерії програмного забезпечення та кібербезпеки, PhD; Котенко Н.О. – доцент кафедри інженерії програмного забезпечення та кібербезпеки, к.пед.н.; Жирова Т.О. – доцент кафедри інженерії програмного забезпечення та кібербезпеки, к.пед.н.; Чубаєвський В.І. – доцент кафедри інженерії програмного забезпечення та кібербезпеки, заступник директора Департаменту інформаційно-аналітичної підтримки Національної поліції України, к.політ.н., доцент; Бойко Т.В. – студент факультету інформаційних технологій, 4 курсу, 11 групи, спеціальність «Кібербезпека»; Чудік М.І. – студент факультету інформаційних технологій, 2 курсу, 6м групи, спеціальність «Інженерія програмного забезпечення».
Базовим структурним підрозділом реалізації освітньо-професійної програми «Безпека систем електронних комунікацій в економіці» є кафедра інженерії програмного забезпечення та кібербезпеки (http://surl.li/ccwcq). За наказом № 3071 «Про затвердження складу груп забезпечення спеціальностей» від 22.11.2022 р. керівником групи забезпечення спеціальності та гарантом ОП «Безпека систем електронних комунікацій в економіці» другого (магістерського) рівня вищої освіти призначено доцента кафедри інженерії програмного забезпечення та кібербезпеки ДТЕУ Савченко Тетяну Віталіївну.

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	*З*	*ОД*	*З*
1 курс	2023 - 2024	48	43	5	0	0
2 курс	2022 - 2023	57	39	18	0	0

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

6. Інформація про інші ОП ЗВО за відповідною спеціальністю

Рівень вищої освіти	Інформація про освітні програми
початковий рівень (короткий цикл)	*програми відсутні*
перший (бакалаврський) рівень	**54971 Безпека інформаційних і комунікаційних систем в економіці**
другий (магістерський) рівень	**55058 Безпека систем електронних комунікацій в економіці**
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	112260	28931
Власні приміщення ЗВО (на праві власності, господарського відання або оперативного управління)	112260	28931
Приміщення, які використовуються на іншому праві, аніж право власності, господарського відання або оперативного управління (оренда, безоплатне користування тощо)	0	0
Приміщення, здані в оренду	40	0

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

8. Документи щодо ОП

Документ	Назва файла	Хеш файла
Освітня програма	*2022_ОПП_125_М_Акредитація.pdf*	k92nzEpaYh31agXtsNzs/Reupjyn8lk5Evqp11Mj3Gg=
Освітня програма	*2023_ОПП_125_М_Акредитація.pdf*	CJayKeq34NmkFe+3tpoKLWN8idTvkd+eYvBWSa7ca+E=
Навчальний план за ОП	*125-М-Д-2022_Акредитація.pdf*	NWcqPm+Vda/JlYrC3eXuAXy53+Dp56QKLiZUdXSrqvM=
Навчальний план за ОП	*125-М-Д-2023_Акредитація.pdf*	72gIdpQg5uoZOqDTxxBtBHMs2+N3ct/xnSSswmBEZMo=
Рецензії та відгуки роботодавців	*Рецензії_стейкхолдерів_2022.pdf*	SG4D2+Yb/HJJ8cHeEsOrgzadwJjKy1zoMs575k/xALA=
Рецензії та відгуки роботодавців	*Рецензії_стейкхолдерів_2023.pdf*	g8+NL8pkOvouzmlW3hKrzUBKNJuLTm5CICbborew7nk=

1. Проектування та цілі освітньої програми

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

Метою ОП «Безпека систем електронних комунікацій в економіці» є підготовка магістрів з кібербезпеки та захисту інформації, що здатні вирішувати задачі дослідницького та інноваційного характеру у сфері інформаційної безпеки та кібербезпеки в галузі економіки, моделювати та прогнозувати можливі кібервпливи на суб'єкти господарювання економіки держави та фізичних осіб; проводити аудит систем електронних комунікацій суб'єктів господарювання; застосовувати нормативні документи та стандарти в розробці заходів по захисту систем електронних комунікацій суб'єктів господарювання економіки держави. Програма спрямована на поєднання практики та науки щодо організації, розробки та експлуатації комплексних складових кіберпростору з метою забезпечення інформаційної безпеки суб'єктів господарювання економіки держави з урахуванням можливих зовнішніх кібервпливів, ймовірних загроз і рівня розвитку технологій захисту систем електронних комунікацій. Унікальністю програми є формування фахівця, що здатний розв'язувати професійні задачі, пов'язані з системами електронних комунікацій, зокрема в економіці, враховуючи галузеву спрямованість ЗВО.

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

стратегії ЗВО

Місія ЗВО: «Працюємо для нинішнього та майбутнього поколінь» (елітарна освіта нинішнього та прийдешніх поколінь на засадах прийнятності традицій та інновацій задля забезпечення поступального розвитку України) http://surl.li/jykhd. Стратегічною метою ДТЕУ є побудова моделі європейського інноваційного університету на засадах випереджального розвитку освітньої, наукової діяльності, формування гармонійної особистості, стабільно високої конкурентоспроможності в країні та світі. Візія ДТЕУ в майбутньому – флагман економічної вищої освіти країни, поліфункціональний університет, здатний генерувати сучасні знання та забезпечувати їх трансфер, що відзначено в Стратегії розвитку ДТЕУ: http://surl.li/dajad.
Цілі ОП «Безпека систем електронних комунікацій в економіці» направлені на підготовку фахівців з кібербезпеки та захисту інформації, здатних вирішувати задачі дослідницького та інноваційного характеру у сфері інформаційної безпеки та кібербезпеки в галузі економіки, з метою забезпечення інформаційної безпеки суб'єктів господарювання економіки держави та здатних розв'язувати задачі, пов'язані з системами електронних комунікацій, зокрема в економіці, що повністю відповідає Стратегії ДТЕУ. Отже, ОП має чітко сформульовані цілі, які відповідають місії, візії та стратегічним цілям розвитку ДТЕУ.
Реалізація ОП здійснюється на основі «Положення про розроблення та реалізацію освітніх програм ДТЕУ» http://surl.li/czrpb в межах принципів діяльності ЗВО, при врахуванні автономії вибору технологій і векторів розвитку ОП.

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

Здобувачі вищої освіти завжди входять до робочої групи з розробки ОП «Безпека систем електронних комунікацій в економіці». А саме, в розробці ОП 2022 року брали участь здобувачі вищої освіти: студент 4 курсу 11 групи Бойко Т.В. спеціальності 125 «Кібербезпека» та студент 2 курсу 6м групи Чудік М.І. спеціальності «Інженерія програмного забезпечення». Побажання та зауваження здобувачів вищої освіти враховуються за результатами періодичних опитувань та анкетування. Крім того, здобувачі вищої освіти входять до складу вчених рад ДТЕУ та факультету інформаційних технологій, на яких обговорюються цілі та програмні результати навчання за ОП. Зокрема, при обговоренні проекту освітньої програми 2022 року за пропозиціями здобувачів було змінено послідовність вивчення освітніх компонент (ОК7 «Цифрова криміналістика» перенесена в перший семестр з другого, а ОК5 «Етичний хакінг» навпаки). Також враховується думка здобувачів при розробці РП нових ОК та вдосконаленні існуючих, таким чином, було вдосконалено зміст програми та робочої програми ОК «Англійська мова інформаційних технологій» з урахуванням специфіки спеціальності. Інтереси, пропозиції, запити здобувачів враховуються робочою групою з розробки ОП з метою внутрішнього забезпечення якості освітніх послуг відповідно до Положення про розроблення та реалізацію освітніх програм ДТЕУ http://surl.li/czrpb. Зараз триває процес обговорення проєкту ОП «Безпека систем електронних комунікацій в економіці» на 2024 р., що розміщено у відкритому доступі (http://surl.li/ktrjr).

- роботодавці

Вимоги ринку у сфері кібербезпеки та захисту інформації та експертна думка роботодавців враховуються при оновленні щорічно ОП, формулюванні цілей та програмних результатів навчання. Зокрема, відбувається врахування пропозицій роботодавців шляхом співпраці з компаніями у сферах інформаційних технологій, кібербезпеки та захисту інформації (http://surl.li/jysef).
Зовнішні партнери освітньої програми (Департамент кіберполіції Національної поліції України, Національний координаційний центр кібербезпеки, Громадська спілка «Кіберковчег») беруть участь в освітньому процесі, в засіданнях робочих груп з обговорення ОП, вносять пропозиції щодо актуалізації змісту окремих дисциплін, вдосконалення змісту та структури ОП «Безпека систем електронних комунікацій в економіці». За пропозиціями роботодавців, а саме, Звєрєва В.П., заступника керівника служби з питань інформаційної безпеки та кібербезпеки, керівника управління інформаційної безпеки Апарату РНБО України, було додано унікальні компетентності та програмні результати навчання, які не визначені відповідним СВО, проте забезпечуються обов'язковими освітніми компонентами та задають специфіку освітньої програми, що акредитується (КФ11, РН24).
Крім того, враховуються результати обговорення зустрічей зі стейкхолдерами, їх опитування під час Ярмарок вакансій, Днів кар'єри, онлайн-опитування, що проводяться Центром розвитку кар'єри разом з Центром педагогічних та психологічних досліджень.

- академічна спільнота

Пропозиції та інтереси академічної спільноти враховуються в результаті обговорення на круглих столах (http://surl.li/jyufe), конференціях, семінарах, залучення до освітнього процесу провідних фахівців-практиків (http://surl.li/jyuko) та іншої спільної діяльності відповідно договорів про наукове-співробітництво, зокрема з: Київським національним університетом імені Тараса Шевченка (https://www.univ.kiev.ua/), Національним університетом біоресурсів і природокористування України (https://nubip.edu.ua/), Київським національним університетом будівництва і архітектури (http://surl.li/jyulj), Чернівецьким національним університетом ім. Юрія Федьковича (http://surl.li/jyulx), Київським університетом імені Бориса Грінченка (http://surl.li/jyuhh) тощо.

- інші стейкхолдери

Питання вдосконалення змісту освітньої програми та пропозиції стейкхолдерів регулярно розглядаються на засіданнях робочої групи, кафедри, вченої ради факультету. Зокрема, до освітнього процесу залучаються фахівці-

практики (http://surl.li/jyvap) відповідно договорів про співпрацю з ТОВ «Майкрософт Україна» (http://surl.li/jyuuo), ТОВ «ЕПАМ СИСТЕМЗ» (http://surl.li/jyuwa), компанією «Intela Solutions» (http://surl.li/jyuvm), ТОВ «Айті Бізнес Солюшн» (http://surl.li/jyuwy), ТОВ «Парус-Регіони» (http://surl.li/jyuyb), M.E.Doc (https://medoc.ua/), IBM (https://www.ibm.com/ua-en), MUK (https://muk.ua/), ISACA (www.isaca.org.ua), Google (https://about.google/), Microsoft Azure (https://azure.microsoft.com/en-us/) тощо.

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

Аналіз ринку праці та ситуація в країні показує, що потреба в кваліфікованих кадрах з кібербезпеки та захисту інформації постійно зростає, про що свідчать численні кібератаки, для протидії яких слід залучати нові наукові підходи та фахівців у цій галузі. Тенденції розвитку спеціальності на ринку праці враховуються кафедрою під час щорічного перегляду освітньої програми «Безпека систем електронних комунікацій в економіці» з урахуванням думки академічної спільноти, стейкхолдерів, результатів моніторингу вступної кампанії, сайтів з працевлаштування тощо. Представлені в ОП цілі та ПРН відповідають стандарту вищої освіти та враховують економічну орієнтованість і провідні позиції ДТЕУ на ринку освітніх послуг. Не зважаючи на зростання кількості ЗВО, які здійснюють підготовку фахівців за напрямком «Кібербезпека», що свідчить про тенденції розвитку спеціальності та є особливо актуально в сучасних умовах, враховуючи зростання кіберзагроз, що надходять від агресора, збільшується кількість відділень захисту інформації та кібербезпеки, які потребують висококваліфікованих фахівців. В ОП «Безпека систем електронних комунікацій в економіці» наведений широкий діапазон посад, які здатні обіймати випускники, враховуючи специфіку та унікальність даної спеціальності. Таким чином, можна стверджувати, що всі програмні результати навчання відбивають тенденції розвитку спеціальності на ринку праці, зокрема ПРН24, що додана в ОП 2023 року, відтворює економічну направленість та специфіку ДТЕУ та унікальність освітньої програми.

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

Під час формування цілей та програмних результатів навчання освітньої програми галузевий контекст було враховано при формуванні сучасної системи професійних знань і навичок у сфері кібербезпеки та захисту інформації в системах електронних комунікацій суб'єктів господарювання, зокрема в економіці. Крім того, враховано регіональний контекст, який визначається промисловим розвитком м. Києва та вимагає конкурентоспроможних фахівців ІТ-галузі з відповідними знаннями та практичними навичками у сфері кібербезпеки та захисту інформації, що є одним з пріоритетів у системі національної безпеки України відповідно до Указу президента України №447/221 «Про рішення Ради національної безпеки і оборони від 14 травня 2021 року «Про Стратегію кібербезпеки України»» (http://surl.li/bnpdr).
Галузевий університетський контекст враховано при виборі прикладних задач, що пов'язано з торговельно-економічною діяльністю суб'єктів господарювання, темою дипломних проєктів, а також переліком вибіркових дисциплін економіко-правового напрямку, що дозволяє здобувачам вищої освіти формувати індивідуальну освітню траєкторію та реалізувати свої професійні навички у сфері інформаційних технологій, кібербезпеки та захисту інформації.

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

Під час формулювання цілей та програмних результатів навчання ОП «Безпека систем електронних комунікацій в економіці» було враховано досвід аналогічних вітчизняних ОП, а саме: Київського національного університету імені Тараса Шевченка (http://surl.li/jzrye), Київського університету імені Бориса Грінченка (http://surl.li/jzrnf), Національного авіаційного університету (http://surl.li/jzrvk), Національного технічного університету України «Київський політехнічний інститут імені Ігоря Сікорського» (http://surl.li/jzrus), Національного університету «Львівська політехніка» (http://surl.li/jzroe), Харківського національного економічного університету імені С.Кузнеця (http://surl.li/jzrra), Харківського національного університету радіоелектроніки (http://surl.li/ktses), Чернівецького національного університету ім. Ю.Федьковича (http://surl.li/jzrlg), які сприяли формуванню загальної концепції підготовки фахівця з кібербезпеки.
Також було розглянуто досвід іноземних програм: MSc in Cyber Security, University of Oxford (Велика Британія); Master of Science in Cyber Security, Stanford University (США); Master of Science in Cybersecurity, University of Toronto (Канада). Суттєвий вплив на розвиток освітньої програми та впровадження освітніх компонент мають програми професійних сертифікацій фахівців з кібербезпеки академії Cisco (https://www.cisco.com). Поширення кіберзагроз на всі сфери життєдіяльності та вдосконалення інструментарію їх реалізації зумовлює необхідність зміни стратегії і тактики протидії ним (http://surl.li/bnpdr).

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

Освітня програма «Безпека систем електронних комунікацій в економіці» повністю відповідає та узгоджується з відповідним СВО за спеціальністю 125 «Кібербезпека» для другого (магістерського) рівня вищої освіти, який був затверджений наказом №332 МОН України від 18.03.2021 р. (http://surl.li/katao). Зміст ОП дозволяє повністю досягти результатів навчання, визначених стандартом вищої освіти (http://surl.li/katas), оскільки всі результати навчання, визначені стандартом, включені до освітньої програми «Безпека систем електронних комунікацій в економіці» (http://surl.li/ktidc), а кожному результату навчання відповідає мінімум одна обов'язкова освітня компонента ОП. Відповідність програмних результатів навчання і обов'язкових компонент наведено в матриці 5.1 освітньої програми. Вибіркові компоненти розширюють можливості досягнення програмних результатів навчання

та дозволяють ефективно вибудовувати індивідуальну траєкторію навчання (матриця 5.2). Крім того, ОП 2023 року (http://surl.li/kttpu) містить додаткові фахові компетентності та програмні результати навчання, що забезпечуються обов'язковими освітніми компонентами та задають специфіку освітньої програми, що акредитується:
КФ11. Здатність аналізувати електронні комунікаційні мережі та протистояти діям, що становлять загрозу доступності, цілісності чи конфіденційності таких мереж і послуг, а також даних, що зберігаються, передаються чи обробляються, та пов'язаних із ними послуг, зокрема в економіці.
РН24. Приймати обґрунтовані рішення та вживати відповідних технічних та організаційних заходів для забезпечення безпеки електронних комунікаційних мереж та послуг з метою гарантування цілісності власних електронних комунікаційних мереж, безперервності надання електронних комунікаційних послуг, недопущення несанкціонованого доступу до електронних комунікаційних мереж.
Отже, в розробленій ОП «Безпека систем електронних комунікацій в економіці» реалізовано компетентнісний підхід, що дозволяє досягти результатів навчання, визначених Стандартом вищої освіти України другого (магістерського) рівня, галузі знань 12 «Інформаційні технології», спеціальності 125 «Кібербезпека».

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

Стандарт вищої освіти України для другого (магістерського) рівня вищої освіти галузі знань 12 «Інформаційні технології» спеціальності 125 «Кібербезпека» затверджений та введений в дію наказом Міністерства освіти і науки України від 18.03.2021р. №332 (http://surl.li/katas).

2. Структура та зміст освітньої програми

Яким є обсяг ОП (у кредитах ЄКТС)?

90

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

66

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

24

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

Зміст ОП «Безпека систем електронних комунікацій в економіці» повністю відповідає предметній області заявленої для неї спеціальності 125 «Кібербезпека», що визначена СВО другого (магістерського) рівня вищої освіти (http://surl.li/katas), згідно якого об'єкти професійної діяльності забезпечуються вивченням таких основних ОК:
- сучасні процеси дослідження, аналізу, створення та забезпечення функціонування інформаційних систем і технологій, інших бізнес-операційних процесів на об'єктах інформаційної діяльності та критичних інфраструктур сфери інформаційної безпеки та/або кібербезпеки (ОК5, ОК6, ОК7);
- інформаційні системи (інформаційно-комунікаційні, інформаційно-телекомунікаційні, автоматизовані) та технології (ОК6, ОК7);
- системи та комплекси створення, обробки, передачі, зберігання, знищення, захисту та відображення даних (інформаційних потоків) (ОК6, ОК7);
- інформаційні ресурси різних класів (ОК4, ОК5);
- програмне та програмно-апаратне забезпечення кіберзахисту (ОК2, ОК3, ОК5);
- системи управління інформаційною безпекою та/або кібербезпекою (ОК5, ОК6, ОК7);
- технології, методи, моделі та засоби інформаційної безпеки та/або кібербезпеки (ОК2, ОК3, ОК5).
Згідно стандарту, складовими теоретичного змісту предметної області є теоретичні засади наукоємних технологій, фундаментальні знання, теорії ідентифікації та прийняття рішень, системного аналізу, складних систем, моделювання та оптимізації процесів, криптографічного та технічного захисту інформації, теорії ризиків та інших міждисциплінарних теорій і практик у галузі інформаційної безпеки та кібербезпеки, що в повному обсязі описано у змісті основних освітніх компонент: ОК2-ОК7.
Відповідно до стандарту складовими методами, методиками та технологіями є:
- Методи, моделі, методики та технології створення, обробки, передачі, приймання, знищення, відображення, захисту інформаційних ресурсів у кіберпросторі, а також методи та моделі розробки та використання прикладного і спеціалізованого програмного забезпечення для вирішення професійних задач в галузі інформаційної безпеки та/або кібербезпеки.
- Технології, методи та моделі дослідження, аналізу, управління та забезпечення бізнес/операційних процесів із застосуванням сукупності нормативно-правових та організаційно-технічних методів і засобів захисту інформаційних ресурсів у кіберпросторі.

Ці вимоги стандарту детальніше розкриті в програмних результатах навчання освітньої програми: РН4-РН6, РН12-РН14, РН21-РН23. Вивчення освітніх компонент ОП надає можливість виконати вимоги СВО спеціальності щодо теоретичного змісту предметної області, методів, методик та технологій навчання в повному обсязі. Отже, компетентності та програмні РН, що формуються основними дисциплінами ОП, відповідають зазначеним у СВО, а основні ОК (http://surl.li/kvyhm) забезпечують виконання в повному обсязі вимог стандарту спеціальності «Кібербезпека» другого (магістерського) рівня вищої освіти щодо змісту предметної області, методів, методик та технологій навчання.

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

Відповідно до п.2.10 «Положення про організацію освітнього процесу студентів» від 03.02.2022 р. наказ №45 (http://surl.li/czzlo), здобувачам вищої освіти ДТЕУ забезпечена можливість формування індивідуальної освітньої траєкторії через складання індивідуального навчального плану студента, який є основним документом організації навчального процесу, що визначає послідовність, форму і темп засвоєння здобувачем освіти освітніх компонентів ОП з метою реалізації його індивідуальної освітньої траєкторії та розробляється університетом у взаємодії із здобувачем освіти за наявності необхідних для цього ресурсів. Процедура формування даного документу регламентується «Положенням про індивідуальний план здобувача вищої освіти ДТЕУ» від 03.02.2022 р. наказ №45 (http://surl.li/eekoj).
Щороку до 15 лютого поточного навчального року студенти ОП ознайомлюються з переліком вибіркових дисциплін та самостійно записуються для вивчення дисциплін за встановленою деканатом факультету процедурою. Про можливість формувати індивідуальну освітню траєкторію свідчать навчальні плани, в яких передбачено широкий вибір дисциплін різних напрямків та уникнення блокової структури (http://surl.li/kvzqt).
Крім вибору ОК, індивідуальна освітня траєкторія здобувачів другого (магістерського) рівня вищої освіти формується і шляхом вибору теми кваліфікаційної роботи та наукового керівника, вибору місця проходження практичної підготовки та врахування результатів неформальної освіти й академічної мобільності здобувачів.

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

Право на вибір навчальних дисциплін здобувачам вищої освіти ДТЕУ надається згідно з «Положенням про організацію освітнього процесу студентів» (http://surl.li/czzlo), відповідно до п.2.10 даного положення здобувачі вищої освіти мають право на вибір навчальних дисциплін у межах, передбачених відповідною ОП та навчальним планом, в обсязі, що становить не менш як 25 % загальної кількості кредитів ЄКТС, передбачених для даного рівня вищої освіти. Порядок обрання дисциплін за вибором студента визначений згідно з п. 2.12., 2.13. У період з 1 по 15 лютого поточного навчального року за розкладом, розробленим навчальним відділом, НПП проводять презентації навчальних дисциплін для студентів з метою ознайомлення їх з детальним описом цих дисциплін, методами навчання, очікуваними результатами навчання тощо. До 15 лютого поточного навчального року студенти очної та заочної форм навчання самостійно записуються для вивчення дисциплін за встановленою деканатом факультету процедурою. При цьому здобувачі певного рівня вищої освіти мають право вибирати навчальні дисципліни, що пропонуються для інших рівнів вищої освіти, за погодженням з гарантом ОП та деканом відповідного факультету. Загальна кількість навчальних дисциплін, запланованих до вивчення, регламентується трудомісткістю необхідних виконаних навчальних робіт, що становить 60 кредитів ЄКТС на навчальний рік з розподілом за семестрами та не повинна перевищувати 5 дисциплін на кожен навчальний семестр. Обсяг навчальної дисципліни становить не менше 6 кредитів ЄКТС. Обрані студентом навчальні дисципліни за вибором включають до індивідуального навчального плану студента. При складанні індивідуальних навчальних планів студентів першого курсу магістратури не пізніше 2 вересня декани факультетів доводять до відома здобувачів перелік дисциплін за вибором у межах навчальних семестрів, після ознайомлення з яким, студенти до 3 вересня включають обрані дисципліни до індивідуальних навчальних планів на поточний навчальний рік. Відповідальність за виконання ІНП покладається на студента відповідно до п.13 «Положення про індивідуальний план здобувача вищої освіти ДТЕУ» (http://surl.li/eekoj).
При виборі освітніх компонент здобувачі вищої освіти мають можливість ознайомитись із пулом вибіркових дисциплін та їх змістом при аналізі інформаційного пакету освітньої програми (http://surl.li/kbvjb), переліку дисциплін, розміщених на сайті ДТЕУ (http://surl.li/kbvaz) та в Системі дистанційного навчання (http://surl.li/kbvhz). Гарант та група забезпечення спеціальності можуть консультувати студентів щодо обрання ними вибіркових дисциплін з метою формування індивідуальної освітньої траєкторії. Відповідальність за набуття програмних результатів навчання (компетентностей), якими повинен оволодіти здобувач відповідного ступеня вищої освіти, покладається на НПП. Контроль за виконанням студентом індивідуального навчального плану покладено на декана відповідного факультету та гаранта освітньої програми (http://surl.li/eekoj).

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

Практична підготовка магістрів ОП «Безпека систем електронних комунікацій в економіці» передбачається навчальним планом та регламентується «Положенням про практичну підготовку здобувачів вищої освіти» (http://surl.li/dacsd), згідно якому, є обов'язковою складовою освітнього процесу, цілеспрямованою діяльністю щодо набуття практичних навичок з обраної ОП на різних етапах навчання. Практика спрямована на закріплення та поглиблення знань, отриманих студентами в процесі вивчення циклу навчальних дисциплін, формування практичних умінь зі спеціальності, передбачає підбір матеріалу для виконання навчально-дослідних завдань, проводиться на базах практики згідно договорів про співробітництво (http://surl.li/jysef). Практика на випускному курсі проводиться з метою поглиблення, узагальнення і вдосконалення здобутих знань, набуття професійного досвіду та збору фактичних матеріалів для виконання випускної кваліфікаційної роботи. На другому

(магістерському) рівні практична підготовка передбачає проведення наукових досліджень з проблем відповідної галузі з метою набуття здобувачами навичок науково-дослідної або управлінської діяльності. За даною ОП заплановано Практична підготовка 1 в другому семестрі обсягом 12 кредитів ЄКТС та Практична підготовка 2 в третьому семестрі – 3 кредити ЄКТС. Здобувачі можуть самостійно обирати бази практики за умови узгодження з випусковою кафедрою. Зміст практичної підготовки і послідовність її проведення для здобувачів другого (магістерського) рівня вищої освіти визначено програмою та робочими програмами.

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

ОП «Безпека систем електронних комунікацій в економіці» дозволяє набути здобувачам вищої освіти соціальних навичок (softskills), що відповідають цілям і результатам навчання ОП. Всі ОК, що відносяться до циклу професійної підготовки, передбачають формування softskills на лабораторних, практичних, семінарських заняттях. Зокрема, обов'язкові компоненти ОП (ОК1, ОК2, ОК3, ОК4, ОК5, ОК6, ОК7) спрямовані на розвиток соціальних, комутативних та мовних навичок, здатність застосовувати знання у практичних ситуаціях (ОК1, ОК2, ОК3, ОК4, ОК5, ОК6, ОК7), здатність проводити дослідження на відповідному рівні (ОК1, ОК2, ОК3, ОК4, ОК5, ОК7), здатність до абстрактного мислення, аналізу та синтезу (ОК5, ОК6, ОК7), здатність забезпечувати якість виконуваних робіт (ОК3, ОК5, ОК6), здатність спілкуватися з представниками інших професійних груп різного рівня (з експертами з інших галузей знань / видів економічної діяльності) (ОК1, ОК2, ОК4, ОК5, ОК7). Крім того, забезпечується досягнення програмних РН, що безпосередньо пов'язані з соціальними навичками, а саме: РН1 (ОК1, ОК2, ОК4, ОК7) та РН2 (ОК1, ОК2, ОК6, ОК7). Практична підготовка дає можливості для розкриття та реалізації лідерських якостей, формування логічного та системного мислення, навичок командної роботи. Отже, ОП дозволяє здобувачеві набути ті навички, що зумовлені цілями ОП, а саме: здатність розв'язувати задачі дослідницького та/або інноваційного характеру у сфері інформаційної та/або кібербезпеки, в тому числі, пов'язані з системами електронних комунікацій, зокрема в економіці.

Яким чином зміст ОП ураховує вимоги відповідного професійного стандарту?

На момент розробки ОП «Безпека систем електронних комунікацій в економіці» Професійні стандарти за спеціальністю 125 «Кібербезпека» були відсутні. Зміст ОП враховує вимоги Стандарту вищої освіти за спеціальністю 125 «Кібербезпека» для другого (магістерського) рівня вищої освіти (http://surl.li/katas), а також береться до уваги Національна рамка кваліфікацій, QF-EHEA та EQF for LLL. Крім того, зміст ОП, що акредитується, відповідає вимогам щодо переліку професій даної галузі згідно Класифікатору професій (http://surl.li/ffdte).
На теперішній час в Україні затверджено шість професійних стандартів для таких професій: «Розробник систем захисту інформації» (http://surl.li/kchtk); «Адміністратор мереж і систем» (http://surl.li/kchtv); «Фахівець сфери захисту інформації» (http://surl.li/kchus); «Аналітик з безпеки інформаційно-телекомунікаційних систем» (http://surl.li/kchvg); «Фахівець з питань безпеки» (http://surl.li/kchvx); «Інструктор-методист з інформаційної безпеки та кібербезпеки» (http://surl.li/kchwh).
Крім того, для обговорення оприлюднено проєкти нових розроблених професійних стандартів у сфері інформаційної безпеки та кібербезпеки (http://surl.li/kchxq).
Зміст освітньої програми та навчальний матеріал будуть вдосконалені та врахують спрямування різних професійних стандартів з кібербезпеки та захисту інформації при оновленні ОП «Безпека систем електронних комунікацій в економіці» другого (магістерського) рівня вищої освіти на 2024 рік.

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

Відповідно до «Положення про організацію освітнього процесу студентів» (http://surl.li/czzlo), підготовка фахівців з вищою освітою у ДТЕУ здійснюється за освітніми програмами. Обсяг кредитів ЄКТС освітніх програм для ОС магістра становить 90 кредитів ЄКТС. Основним нормативним документом, що розробляється на основі ОП і визначає перелік навчальних дисциплін і логічну послідовність їх вивчення, є навчальний план (http://surl.li/kvzqt), що складається групою забезпечення ОП, склад якої затверджується Ректором щорічно, із залученням представників студентського самоврядування та роботодавців. НП містить календарний графік на весь період навчання, бюджет часу студентів, де зазначено час на аудиторні заняття, самостійну роботу, контрольні заходи, практичну підготовку, канікули, атестацію. У НП визначено обсяг годин на кожну дисципліну, кількість кредитів ЄКТС і форми підсумкового контролю. Обсяг кредиту ЄКТС становить 30 академічних годин, а річне навчальне навантаження здобувача – 60 кредитів ЄКТС. Аудиторне навантаження здобувачів денної форми навчання на другому (магістерському) рівні підготовки становить, як правило, 18 години на тиждень. Для ОП «Безпека систем електронних комунікацій в економіці» семестрове аудиторне навантаження складає близько 30% від загального часу студента. ОК містять від 6 до 12 кредитів і загалом мають обсяг 66 кредитів ЄКТС, вибіркові компоненти містять всі дисципліни по 6 кредитів і мають загальний обсяг 24 кредити. Зміст самостійної роботи студента визначається робочими програмами дисциплін.

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

Підготовка здобувачів вищої освіти за дуальною формою освіти за ОП «Безпека систем електронних комунікацій в економіці», що акредитується, не передбачена. Проте, ДТЕУ має розроблене «Тимчасове положення про дуальну

форму здобуття вищої освіти у Державному торговельно-економічному університеті» (http://surl.li/dablz), а з 2021 року було започатковано впровадження дуальної освіти на освітній програмі першого (бакалаврського) рівня вищої освіти за спеціальністю 241 «Готельно-ресторанна справа».

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://knute.edu.ua/blog/read/?pid=44883&uk

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

Конкурсний відбір щодо вступу на навчання за ОП «Безпека систем електронних комунікацій в економіці» другого (магістерського) рівня вищої освіти проводиться в межах ліцензійного обсягу 50 осіб на денну форму навчання та 30 осіб на заочну форму (http://surl.li/kghvz). Станом на 01.09.2023 р. на навчання за денною формою зараховано 43 здобувача, що становить 86 % від ліцензійного обсягу. Набір на контрактну форму навчання триває до 30.11.2023 р. Для абітурієнтів є обов'язковим наявність документа про вищу освіту (ступеня бакалавра http://surl.li/kghyb, спеціаліста чи магістра http://surl.li/kghyw). В 2022 році у зв'язку з військовим станом та спрощеними умовами вступу в ЗВО в країні, абітурієнти, що претендували на бюджетні місця, вступали за результатами фахового іспиту в ДТЕУ та мотиваційного листа, а на контрактну форму – лише за результатами конкурсу мотиваційних листів, вимоги до яких розміщені на сайті ДТЕУ (http://surl.li/kgkyl). Програми фахових іспитів розміщені у відкритому доступі на сайті університету (http://surl.li/kglak). На другому курсі освітньої програми, що акредитується, зараз навчається 39 студентів на денній формі навчання та 18 на заочній. Отже, відбір абітурієнтів для навчання за ОП «Безпека систем електронних комунікацій в економіці» здійснюється з урахуванням специфіки підготовки та необхідних базових, початкових компетентностей, які визначаються за результатами вступних фахових випробувань.

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

В ДТЕУ встановлені правила визнання результатів навчання, отриманих в інших закладах освіти під час переведення (http://surl.li/kgkyq), а також під час академічної мобільності, що є чіткими і зрозумілими, а також відповідають Конвенції про визнання кваліфікацій з вищої освіти в Європейському регіоні (Лісабон, 1997 р.), є допустимими для всіх учасників освітнього процесу та їх послідовно дотримуються під час навчання за ОП «Безпека систем електронних комунікацій в економіці». У ЗВО затверджене та діє «Положення про порядок реалізації права на академічну мобільність у Державному торговельно-економічному університеті», яке розміщене у відкритому доступі на сайті університету (http://surl.li/djyok), є складовою системи внутрішнього забезпечення якості освітньої діяльності та якості вищої освіти і встановлює порядок організації програм академічної мобільності для учасників освітнього процесу Державного торговельно-економічного університету на території України чи поза її межами та учасників освітнього процесу іноземних вищих навчальних закладів (наукових установ). Повна та актуальна інформація щодо програм навчання у закордонних ЗВО розміщена на сторінці Центру європейської освіти ДТЕУ (http://surl.li/kgijq).

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

Практики застосування вказаних правил на ОП «Безпека систем електронних комунікацій в економіці» не було. Відділ міжнародних зв'язків, деканат та НПП кафедри доводять до відома здобувачів освіти інформацію про актуальні можливості реалізації академічної мобільності.

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

Питання визнання результатів навчання, отриманих у неформальній освіті, в ДТЕУ регулюється «Тимчасовим положенням про порядок визнання результатів навчання, набутих у неформальній освіті у ДТЕУ», затвердженого Вченою Радою ДТЕУ (протокол №1, п.6 від 02.02.2022 р.) та введеного в дію Наказом ДТЕУ №808 від 03.02.2022 р., що розміщено у відкритому доступі на сайті ЗВО (http://surl.li/dabvh). В Положенні прописаний порядок та процедури визнання результатів, зокрема, вказано, що результати навчання, здобуті у неформальній освіті, поширюються на здобувачів усіх рівнів вищої освіти та можуть бути визнані для дисциплін, які починають викладатися з другого семестру. Здобувач має право звернутися із заявою на ім'я Ректора університету з проханням визнати відповідні результати (до заяви додаються відповідні документи, що підтверджують результати навчання). Для визнання результатів навчання у неформальній освіті наказом Ректора, за поданням декана, створюється предметна комісія, що ухвалює рішення щодо перезарахування результатів навчання, здобутих у неформальній або інформальній освіті. За підсумками оцінювання предметна комісія формує протокол з висновком для деканату про зарахування чи не зарахування відповідної дисципліни. Здобувач звільняється від вивчення перезарахованої дисципліни в наступному семестрі. Здобувачі вищої освіти ДТЕУ мають право на зарахування змістовного модулю

чи окремої теми в межах вивчення навчальної дисципліни. Рішення про зарахування ухвалює викладач даної дисципліни, виходячи зі змісту програми.

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

Викладачі, задіяні в реалізації ОП «Безпека систем електронних комунікацій в економіці», постійно заохочують здобувачів вищої освіти підвищувати рівень своєї фахової підготовки та розподіляють критерії оцінювання з урахуванням наукової роботи та неформальної освіти. Зокрема, при викладанні обов'язкових та вибіркових освітніх компонент (ОК2, ОК6, ВК3) застосовують сертифікаційні курси Networking Academy Cisco при виконанні лабораторних робіт та тестуванні, а також враховуються як окремі складові з різних дисциплін й інші види підвищення професійного рівня, що підтверджені документально, які здобувачі обирають за своєю ініціативою. Отже, при завершенні вивчення дисциплін здобувачі вищої освіти отримують не лише систематизовані теоретичні знання та практичні навички, а й сертифікати, що нададуть перевагу випускникам при працевлаштуванні. Проте, прикладів перезарахування результатів навчання, отриманих у неформальній освіті, повністю дисципліни згідно з діючим «Положенням про порядок визнання результатів навчання, набутих у неформальній освіті» на ОП, що акредитується, поки не було.

4. Навчання і викладання за освітньою програмою

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

Відповідно до «Положення про організацію освітнього процесу студентів» (http://surl.li/czzlo), навчання в ДТЕУ здійснюється за наступними формами: навчальні заняття, самостійна робота, практична підготовка та контрольні заходи, а також забезпечується якісними та сучасними навчально-методичними матеріалами відповідно до діючої Системи управління якістю ДТЕУ (http://surl.li/afloq).
Форми та методи навчання і викладання на ОП «Безпека систем електронних комунікацій в економіці» регламентуються діючими положеннями та здійснюються у формі лекцій, лабораторних і практичних занять, самостійної та наукової роботи студентів і випускної кваліфікаційної роботи. Окремою формою навчання є практична підготовка, що дає можливість систематизувати та поглибити теоретичні знання, набути практичних навичок в професійній діяльності. Навчальні програми ОК містять матриці відповідності тем дисципліни компетентностям та програмним результатам навчання за ОП. Методичною радою Університету (протокол №5 від 07.02.2020 р.) зазначено, що мінімум 20% обсягу кожної дисципліни повинно бути направлене на використання інтерактивних методів навчання. У ДТЕУ здійснюється постійний аналіз та контроль застосування форм і методів навчання і викладання на ОП, згідно якого, можна зробити висновки про перевагу застосування інноваційних методів викладання (кейсів, ділових ігор, вебінарів, імітаційних ситуацій, наочних методів навчання тощо). В таблиці 3 додатку наведено відповідність методів навчання і програмних результатів навчання за кожною ОК.

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?

Базовим принципом освітньої діяльності ДТЕУ є студентоцентрований підхід, який регламентується «Положенням про систему забезпечення якості освітньої діяльності та якості вищої освіти (систему внутрішнього забезпечення якості)» (http://surl.li/dabyq), «Положенням про організацію освітнього процесу студентів» (http://surl.li/czzlo), «Статутом ДТЕУ» (http://surl.li/czrot), згідно чого здобувач є суб'єктом з власними унікальними інтересами та потребами, які враховуються та забезпечується акцентування на особистісно-орієнтованій складовій навчання. Освітній процес та освітні програми ДТЕУ орієнтовані на стимулювання мотивації здобувачів та залучення їх до удосконалення освітнього процесу. Студентоцентроване навчання та викладання на ОП «Безпека систем електронних комунікацій в економіці» підтримує відчуття автономності у здобувачів, забезпечуючи супровід і підтримку з боку викладача, враховуючи їх різноманітність та потреби. Відповідно до «Положення про систему рейтингової оцінки діяльності НПП» (http://surl.li/dabyj) визначається рівень задоволеності здобувачів методами навчання і викладання, застосовуючи зворотний зв'язок, що здійснюється у форматі анкетування студентів і враховується при обчисленні рейтингу НПП (http://surl.li/kdghj). Результати опитування обговорюються на засіданнях кафедри, вченої ради факультету та університету, під час звітів Центру педагогічних та психологічних досліджень ДТЕУ. Можна зробити висновок за результатами опитування, що більшість здобувачів задоволена методами навчання та викладання на ОП.

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

Відповідно до Статуту ДТЕУ (http://surl.li/czrot), Університет дотримується принципів академічної свободи, а саме: викладачі мають свободу викладання, вибір форм, методів і засобів навчання, що відповідають освітній програмі; використання наукових досліджень та участь здобувачів у наукових конференціях; вибір навчальних дисциплін здобувачами вищої освіти; врахування потреб здобувачів з обмеженими можливостями тощо. Кожен викладач у своїй професійній діяльності має забезпечувати свободу слова і толерантність у спілкуванні зі студентами, притримуючись принципів академічної свободи при розробці та змістовному наповненні дисциплін, обранні форм

та методів навчання та врахування результатів неформальної освіти, на що особливу увагу звертає керівництво ЗВО. Форми та методи навчання і викладання сприяють досягненню заявлених у ОП «Безпека систем електронних комунікацій в економіці» цілей та програмних результатів навчання здобувачів другого (магістерського) рівня вищої освіти спеціальності «Кібербезпека», відповідають вимогам студентоцентрованого підходу та принципам академічної свободи, згідно з «Положенням про розроблення та реалізацію освітніх програм ДТЕУ фахового передвищого, початкового (короткого), першого (бакалаврського) та другого (магістерського) рівнів вищої» освіти (Наказ ДТЕУ №45 від 03.02.2022 р.): http://surl.li/czrpb. За результатами опитування здобувачі вищої освіти дають переважно схвальні відгуки щодо забезпечення відповідності методів навчання та викладання принципам академічної свободи.

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

Інформація щодо цілей, змісту та програмних результатів навчання, порядку та критеріїв оцінювання в межах окремих ОК своєчасно надається усім учасникам освітнього процесу в доступній та зрозумілій формі, є прозорою та регламентується «Положенням про організацію освітнього процесу студентів» (https://surl.li/czzlo). На сайті ДТЕУ щорічно оновлюються Інформаційні пакети (http://surl.li/kdnuf), з якими студенти можуть ознайомитись заздалегідь для уявлення про зміст та очікувані ПРН за відповідною ОП (http://surl.li/kbvjb). Крім того, інформація розміщується на сторінці кафедри (http://surl.li/ktrjr), а програми та робочі програми всіх дисциплін в системі дистанційного навчання (http://surl.li/kbvhz).
Графік навчального процесу на поточний навчальний рік складається навчальним відділом на підставі робочих навчальних планів, є публічним і доводиться до відома усіх учасників освітнього процесу. Розклад занять розміщується на стенді деканату та на офіційному веб-сайті університету (http://surl.li/afjkv) та системі «MIA: Освіта» (http://surl.li/kdqls).
Кожен викладач на першому занятті інформує студентів щодо системи оцінювання та накопичення балів з дисципліни, її місце у формуванні фахових (спеціальних) компетентностей через силабус. Для реалізації навчального процесу для всіх учасників освітнього процесу, що проводиться через систему дистанційного навчання (http://surl.li/kbvhz), згідно з положенням «Про дистанційне навчання у ДТЕУ» (http://surl.li/dacch). При анкетуванні здобувачі підтверджують обізнаність за даними питаннями.

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

Поєднання навчання і досліджень під час реалізації ОП сприяє розвитку у здобувачів ВО дослідницьких навиків і орієнтоване на прагнення до навчання та наукового пошуку. Здобувачі залучаються до виконання науково-дослідних тем кафедр, що відповідають їх науковим інтересам. План науково-дослідної роботи університету розміщується на сайті університету, в особистому кабінеті (Е-кампус). Здобувачі представляють результати досліджень на наукових заходах, інформація про які оприлюднюються на сайті університету (http://surl.li/kwqvq, http://surl.li/kwrsc). П'ять здобувачів даної ОП 13 квітня 2023 р. презентували результати наукових досліджень на студентській науково-практичній конференції «Інформаційні технології та кібербезпека в умовах воєнного часу». Студенти даної ОП активно брали участь в науковому семінарі «Інформаційно-інтелектуальні системи в бізнесі». Проведення студентських олімпіад дозволяє об'єктивно виявити та відібрати обдаровану студентську молодь. На базі Київського університету ім. Б.Грінченка команди студентів кафедри ІПЗ та кібербезпеки 22 жовтня 2022 р. змагалися в Студентській першості світу з програмування ICPC/ACM у Південно-східній Європі, яка є складовою частиною відбіркових змагань Міжнародної командної студентської олімпіади з програмування (ICPC – International Collegiate Programming Contest) під егідою Асоціації обчислювальної техніки (ACM – Association for Computing Machinery) (http://surl.li/kwrua).
Участь у Всеукраїнському конкурсі студентських наукових робіт з галузей знань та спеціальностей стимулює до активної творчої праці студентів у процесі навчання та оволодіння спеціальністю (http://surl.li/kwrsc).
Результати наукових досліджень здобувачі вищої освіти мають можливість публікувати у журналах ДТЕУ (http://surl.li/kwrwg). Журнал «Трактат Сови» випускається під редакцією студентів факультету ФІТ, де викладачі кафедри (Хорольська К.В., Криворучко О.В.) є членами організаційного комітету, а студентка даної ОП (Шаяхметова О.Р.) має в ньому публікацію. Варто зазначити, що статті інших студентів 125 спеціальності ОС бакалавр також були надруковані в даному журналі (http://surl.li/kwryt). Відповідно до положення «Про випускну кваліфікаційну роботу» п. 1.5 результати ВКР здобувача другого (магістерського) рівня вищої освіти обов'язково повинні бути опубліковані в Збірнику наукових статей університету або в іншому науковому фаховому виданні України. Переважна більшість студентів публікує результати своїх досліджень у збірнику «Cybersecurity And Software Engineering In The Era Of Evolving Threats And Complex Systems». Під егідою Наукового товариства студентів, аспірантів, докторантів і молодих вчених ДТЕУ в університеті функціонують дискусійні клуби та гуртки, відкрито SMART-бібліотеку (http://surl.li/agcam), створені зони коворкінгу «SUTE HUB» і «Phygital Hub» – простір для творчої та інтелектуальної роботи, що обладнано робочими зонами та залами зустрічей.

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

Гарант та група забезпечення ОП постійно аналізують стан та зміст навчально-методичного забезпечення, здійснюючи необхідні коригуючі дії згідно з процедурами, передбаченими Системою внутрішнього забезпечення якості освітньої діяльності. Наповнення, внесення змін до змісту ОК проводиться регулярно, до початку навчального року. За результатами аналізу, зібраних відгуків, рекомендацій, зауважень від здобувачів освіти, роботодавців, випускників, відстеження розвитку тенденцій, новітніх наукових напрямків, методологій у галузі кібербезпеки, формуються пропозиції щодо внесення змін до ОП та відповідних ОК, оновленню навчально-методичних

матеріалів. Пропозиції подаються гарантом ОП на розгляд засідання кафедри інженерії програмного забезпечення та кібербезпеки.
Рішення про рекомендацію до видання програм та робочих програм дисциплін згідно «Положення про порядок погодження, затвердження та подання рукописів наукових, навчальних та навчально-методичних видань» (http://surl.li/eefln), що діє в Університеті, ухвалюється вченою радою ДТЕУ. Підготовлені рукописи навчальних, навчально-методичних та наукових видань рецензуються провідними фахівцями з навчальних дисциплін, НПП, яким присуджені наукові ступені та присвоєні вчені звання з відповідних випускових кафедр, гарантами освітніх програм, стейкхолдерами. В процесі зовнішнього рецензування стейкхолдери надають експертні оцінки щодо відповідності змісту, завдань та наповнення ОК формуванню заявлених компетентностей та ПРН.
НПП, що викладають дисципліни на ОП «Безпека систем електронних комунікацій в економіці», постійно займаються науковою діяльністю, беруть участь у міжнародних наукових і практичних конференціях, семінарах тощо. Результати підвищення кваліфікації шляхом стажування у провідних ІТ-компаніях, наукових установах та ЗВО, впроваджуються у навчальних дисциплінах. Слід відмітити, що Савченко Т.В. та Костюк Ю.В. є сертифікованими інструкторами Мережевої академії Cisco (Cisco Networking Academy Program) (2020-2023 рр.). Савченко Т.В., Котенко Н.А., Костюк Ю.В. пройшли стажування «Teacher's Internship Program» від експертів EPAM та IT Ukraine Association (2020-2021 рр.); Власенко Л.О. пройшла стажування «Modern practices of secure automated production using industrial robots» в Lukasiewicz Research Network – Industrial Research Institute for Automation and Measurement PIAP, Warsaw, Poland (2022 р.); Савченко Т.В., Костюк Ю.В. пройшли курси підвищення кваліфікації у Державному університеті телекомунікацій за темою: «Системи технічного захисту інформації» (2020 р.), Савченко Т.В. брала участь у проєкті «Посилення спроможностей українських державних органів у сфері кібергігієни та кібербезпеки», реалізованого Координатором проєктів OSCE Project Co-ordinator in Ukraine та Українською школою урядування (2021-2022 рр.). Більш детальна інформація про наукові досягнення викладачів та впровадження результатів в освітні компоненти ОП надана у додатку 2 та на сторінках кафедри (http://surl.li/kwtbu).

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

Університетом укладені договори про співробітництво між ДТЕУ та ЗВО, в рамках яких здійснюється партнерський обмін та навчання здобувачів ВО; надається можливість брати участь у програмах міжнародної академічної мобільності (подвійне дипломування, семестровий обмін, Еразмус+); викладання іноземними викладачами в ДТЕУ; можливість виїзду викладачам ДТЕУ для викладання в закордонних ЗВО в рамках Еразмус+, а також на індивідуальні запрошення. В ДТЕУ існують бакалаврські та магістерські програми англійською мовою викладання. Зокрема, для проходження навчання за індивідуальним планом до Познанського економічного університету (Польща) був направлений Фефєлов М.А., студент 12 гр. д.ф.н., що здобув ОС «бакалавр» за спец. 125 «Кібербезпека» на умовах держ.замов., з 29.09.2021 р. по 20.02.2022 р. (Наказ №2799 від 17.09.2021 р.)
Крім того, викладачі кафедри Криворучко О.В., Десятко А.М., Жирова Т.О., Котенко Н.О. 12.04-12.07.2021 р. проходили міжнародне стажування «Programming, Software Testing, Cloud Technologies in the Economics, Security of Information Systems in the Economics, IT Project Management and Artificial Intelligence», Болгарія, Софія; Сашньова М.В. проходила стажування на базі IBR LPNT ГО «Міжнародна фундація науковців та освітян», Lublin, Republic of Poland (November, 2020). Також всі викладачі кафедри беруть участь у міжнародних конференціях та публікують роботи у наукових журналах, що реферуються у міжнародних наукометричиних БД

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 контрольними заходами в ДТЕУ передбачено вхідний, поточний, підсумковий модульний, підсумковий семестровий (залік або екзамен) контроль, атестація та контроль залишкових знань (ректорський). Оцінювання досягнень студентів та проведення контрольних заходів відбувається відповідно до вимог нормативних документів, що діють в університеті та є невід'ємною складовою Системи управління якістю ДТЕУ: «Положення про організацію освітнього процесу студентів» (http://surl.li/czzlo), «Положення про атестацію здобувачів вищої освіти та екзаменаційну комісію з атестації у ДТЕУ» (http://surl.li/dacre), «Положення про оцінювання результатів навчання студентів і аспірантів у Державному торговельно-економічному університеті» (http://surl.li/kfzef).
Оцінювання результатів навчання студентів ДТЕУ проводиться за 100-баловою шкалою, де 60-100 балів – результати навчання, що дають можливість здобути кредити ЄКТС; 0-59 балів – незадовільні результати, що не дають студенту такої можливості. Результат підсумкового (семестрового) контролю з навчальної дисципліни для студента очної форми навчання визначається як середнє арифметичне суми балів підсумкового контролю та екзамену.
Для визначення вхідного рівня знань студентів та для успішної організації вивчення дисципліни передбачено проведення вхідного контролю. Поточний контроль проводиться на семінарських, практичних/лабораторних заняттях та за результатами виконання завдань самостійної роботи з метою оцінювання теоретичної підготовки студентів із зазначеної теми та набутих практичних навичок під час виконання завдань. Для визначення результатів за період теоретичного навчання студентів, проводиться підсумковий модульний контроль, як окреме заняття в межах годин, відведених на лабораторні (практичні) або семінарські заняття. Поточна робота студентів оцінюється від 0 до 100 балів і являє собою суму балів, накопичених студентом за виконання всіх видів поточних навчальних занять та на підсумковому модульному контролі. Підсумкове оцінювання результатів навчання студентів за семестр у формі заліку чи екзамену є підсумковим семестровим контролем, оцінюється від 0 до 100 балів і має на меті оцінити результати навчання студентів на певному освітньому ступені або на окремих його завершальних етапах.

Для встановлення відповідності результатів навчання здобувачів вищої освіти, визначених ОП, вимогам стандарту вищої освіти проводиться їх атестація, а для визначення ефективності навчання з дисципліни, ступеня засвоєння навчального матеріалу, передбаченого програмою, рівня сформованості необхідних компетентностей, проводиться контроль перевірки залишкових знань.
Для кожного виду контрольних заходів визначені критерії оцінювання навчальних досягнень, форми його проведення. Головною метою цих заходів є визначення рівня компетентності. Така структурована система контролю забезпечує перевірку та об'єктивне оцінювання досягнення здобувачами програмних результатів навчання освітніх компонентів ОП.

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

Чіткість і зрозумілість форм контрольних заходів і критеріїв оцінювання навчання здобувачів вищої освіти в ДТЕУ забезпечується наданням інформації про терміни їх проведення в графіках освітнього процесу (http://surl.li/afjkv) та в інших документах, що знаходяться у відкритому доступі: «Положення про організацію освітнього процесу студентів» (http://surl.li/czzlo), «Положення про оцінювання результатів навчання студентів і аспірантів у ДТЕУ» (http://surl.li/kfzef), «Положення про атестацію здобувачів вищої освіти та екзаменаційну комісію з атестації у ДТЕУ» (http://surl.li/dacre).
Інформація є прозорою і доступною для всіх здобувачів, а критерії оцінювання досягнень наведені в робочих програмах та силабусах ОК, що доступні на платформі дистанційного навчання (http://surl.li/kbvhz) та доводяться до здобувачів викладачем на першому занятті.
Основними контрольними заходами на ОП є поточний, підсумковий модульний, підсумковий семестровий (залік або екзамен) контроль, атестація. Для оцінки навчальних досягнень та оцінки результатів навчання студентів на рівні окремої ОК використовуються такі методи контролю, як екзамени, форма проведення яких визначається навчальним планом, а питання, включені до екзаменаційних білетів, корелюються з ПРН.
В Університеті працює система МІА: Освіта (http://surl.li/kdqls). В особистому кабінеті студент може переглянути свої поточні, підсумкові бали, результати контрольних заходів, розклад занять і екзаменаційної сесії в будь-який час.

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

Згідно «Положення про оцінювання результатів навчання студентів і аспірантів у Державному торговельно-економічному університеті» (http://surl.li/kfzef) визначені форми контрольних заходів та критерії оцінювання знань здобувачів вищої освіти для кожного ОК, які відображені в робочих програмах та силабусах. Згідно «Положення про організацію освітнього процесу студентів» (http://surl.li/czzlo) студентам забезпечується вільний доступ до програм, робочих програм, силабусів та інших складових НМКД, зокрема, в системі дистанційного навчання (http://surl.li/kbvhz). Ознайомлення зі структурою курсу, формами, строками, критеріями оцінювання та процедурами проведення контрольних заходів для визначення степені оволодіння студентом знань та навичок проводиться НПП на першому занятті дисципліни. Перед кожним контрольним заходом НПП роз'яснює студентам процедуру проведення заходу і критерії оцінювання. Кожен здобувач вищої освіти може переглянути результати поточних і підсумкових контрольних заходів в особистому електронному кабінеті «МІА: Освіта» (http://surl.li/kdqls) в будь-який момент часу. Графік навчального процесу на поточний навчальний рік є публічним, складається навчальним відділом згідно робочих навчальних планів та доводиться до всіх без винятку учасників освітнього процесу. Розклад екзаменаційної сесії розташовується на офіційному сайті університету (http://surl.li/afjkv), в системі «МІА: Освіта» (http://surl.li/kdqls) та на стенді деканату не пізніше, ніж за тиждень.

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

Атестація здобувачів вищої освіти ОП «Безпека систем електронних комунікацій в економіці» здійснюється відповідно до Законів України «Про освіту», «Про вищу освіту», постанови Кабінету Міністрів України «Про затвердження Національної рамки кваліфікацій» (http://surl.li/gkrz), СВО за спеціальністю 125 «Кібербезпека», «Статуту ДТЕУ», «Положення про організацію освітнього процесу студентів», «Положення про оцінювання результатів навчання студентів і аспірантів у Державному торговельно-економічному університеті» тощо.
У Стандарті вищої освіти за спеціальністю 125 «Кібербезпека» другого (магістерського) рівня вищої освіти (http://surl.li/kwzjh) зазначено, що атестація здійснюється у формі публічного захисту кваліфікаційної роботи.
Порядок організації та проведення атестації на ОП регламентується: «Положенням про атестацію здобувачів вищої освіти та екзаменаційну комісію з атестації у ДТЕУ» (http://surl.li/dacre), «Положенням про випускну кваліфікаційну роботу (проєкт)» (http://surl.li/dactw), «Положенням про дотримання академічної доброчесності педагогічними, науково-педагогічними, науковими працівниками та здобувачами вищої освіти» (http://surl.li/disgq), Методичними рекомендаціями до виконання кваліфікаційної роботи (проектів).

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

Процедура проведення контрольних заходів в ДТЕУ регулюється наступними документами, які розміщені у вільному доступі для всіх учасників освітнього процесу на офіційному сайті університету (http://surl.li/kfzgg): «Положення про систему забезпечення якості освітньої діяльності та якості вищої освіти (систему внутрішнього забезпечення якості) ДТЕУ» (http://surl.li/dabyq), «Положення про оцінювання результатів навчання студентів і аспірантів у Державному торговельно-економічному університеті» (http://surl.li/kfzef), «Положення про організацію освітнього процесу студентів» (http://surl.li/czzlo), «Положення про атестацію здобувачів вищої освіти та

екзаменаційну комісію з атестації у ДТЕУ» (http://surl.li/dacre), «Положення про дистанційне навчання у Державному торговельно-економічному університеті» (http://surl.li/dacch), «Положення про дотримання академічної доброчесності педагогічними, науково-педагогічними, науковими працівниками та здобувачами вищої освіти ДТЕУ» (http://surl.li/disgq).

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 дотриманням і виконанням всіх учасників освітнього процесу чітко розроблених правил щодо проведення контрольних заходів, що прописані в «Положенні про дотримання академічної доброчесності педагогічними, науково-педагогічними, науковими працівниками та здобувачами вищої освіти ДТЕУ» (http://surl.li/disgq). В університеті діє Комісія з питань етики та академічної доброчесності, як незалежний орган, що керується у своїй діяльності Конституцією України, законодавством у сфері освіти та вищої освіти, нормативно-правовими актами Міністерства освіти і науки України, Статутом, Правилами внутрішнього розпорядку, іншими нормативними документами ДТЕУ. Порядок і процедури попередження, виявлення та врегулювання конфліктних ситуацій, що можуть виникнути, регламентовані в наступних документах: «Положення про апеляцію результатів підсумкового контролю знань у ДТЕУ» (http://surl.li/daffm), «Положення про врегулювання конфліктних ситуацій в ДТЕУ» (http://surl.li/kxhoz), «Положення про організацію освітнього процесу студентів» (http://surl.li/czzlo).
За час функціонування ОП «Безпека систем електронних комунікацій в економіці» випадків конфлікту інтересів здобувачів і викладачів не було. За результатами опитування (http://surl.li/kxhyn) 85,2 % здобувачів ОП задовольняє існуюча в ДТЕУ система оцінювання знань, а 92,6% здобувачі зазначили, що ознайомлені з процедурами врегулювання конфліктних ситуацій в ДТЕУ (включаючи дискримінацію та інші види утисків).

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

Порядок повторного проходження контрольних заходів в ЗВО регулюється «Положенням про оцінювання результатів навчання студентів та аспірантів» (http://surl.li/kfzef), згідно якого студенти, які за результатами вивчення дисципліни отримали незадовільний результат (0-59 балів), повинні для підвищення рівня своїх знань виконати додаткові індивідуальні завдання і повторно скласти підсумковий контроль (п. 1.4). Ліквідація академічної заборгованості проводиться після закінчення екзаменаційної сесії, не пізніше наступного тижня після сесії, за окремим розкладом, складеним деканатом факультету та узгодженим із навчальним відділом. При отриманні незадовільної оцінки з першої спроби з даної дисципліни, другий раз призначається комісія, створена деканом. Повторна ліквідація академічної заборгованості призначається не раніше наступного дня після попередньої. Для студента, який не проходив підсумковий модульний контроль згідно графіку навчання через відсутність та під час ліквідації академічної заборгованості, оцінка, отримана під час ліквідації академічної заборгованості на комісії, є остаточною. Підсумкова оцінка з дисципліни під час ліквідації академічної заборгованості виставляється без урахування балів підсумкового модульного контролю. Студент, який не склав екзамен на комісії під час ліквідації академічної заборгованості відраховується з університету. Під час опитування 100% опитаних здобувачів ОП «Безпека систем електронних комунікацій в економіці» зазначили, що ознайомлені з порядком повторного проходження контрольних заходів.

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

Порядок оскарження процедури та результатів проведення контрольних заходів регулюється «Положенням про апеляцію результатів підсумкового контролю знань у ДТЕУ» (http://surl.li/daffm). Студент може подати заяву на ім'я Ректора з проханням переглянути отриману під час екзамену оцінку, якщо не погоджується з нею. Заява продається особисто студентом в день оголошення результатів підсумкового (семестрового) контролю декану. Заява погоджується керівництвом університету та реєструється у Журналі реєстрації апеляцій, що знаходиться у навчальному відділі та передається до деканату. З метою захисту прав осіб щодо оскарження оцінки з дисципліни, отриманої під час підсумкового контролю знань, наказом ректора створюється апеляційна комісія ДТЕУ в складі: голови, заступника голови, керівника групи забезпечення спеціальності, не менше 2-х членів комісії, представника РСС факультету чи наукового товариства студентів, аспірантів, докторантів та молодих вчених, секретаря комісії, який обирається з числа членів комісії. Результати апеляції оголошуються здобувачу вищої освіти одразу після закінчення розгляду його роботи, про що здобувач особисто робить відповідний запис у протоколі засідання апеляційної комісії. Прикладів оскарження результатів контрольних заходів на ОП «Безпека систем електронних комунікацій в економіці» не було. 100% опитаних здобувачів ОП засвідчили, що ознайомлені з порядком оскарження процедури та результатів проведення контрольних заходів.

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

В «Положенні про дотримання академічної доброчесності педагогічними, науково-педагогічними, науковими працівниками та здобувачами вищої освіти ДТЕУ» (http://surl.li/disgq), затвердженому вченою радою ДТЕУ від 02 лютого 2022 р. (протокол №1, п.6), введеному в дію наказом ДТЕУ від 03.02.2022 № 45, визначені права і обов'язки, відповідальність учасників освітнього процесу та порядок організації роботи Комісії з питань етики та академічної доброчесності. Політика, стандарти і процедури дотримання академічної доброчесності відображені в Настанові з якості (прийнятої 16 червня 2009 р. зі змінами та доповненнями 2015, 2018 рр.) та «Положенні про систему забезпечення якості освітньої діяльності та якості вищої освіти (систему внутрішнього забезпечення якості) ДТЕУ»

(http://surl.li/dabyq), Наказ №45 від 03.02.2022 р. Здобувачі вищої освіти ДТЕУ дотримуються Етичного кодексу здобувача ДТЕУ, а в ЗВО прийнятий план заходів щодо популяризації та дотримання академічної доброчесності, відповідні документи, які містять політику, стандарти і процедури дотримання академічної доброчесності розміщено на сайті (http://surl.li/aleeb, http://surl.li/kxiun). Під час опитування 96.3% опитаних здобувачів ОП «Безпека систем електронних комунікацій в економіці» зазначили, що ознайомлені з документами ДТЕУ, які містять процедури дотримання академічної доброчесності.

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

З метою протидії порушенням академічної доброчесності в університеті діє «Положення про дотримання академічної доброчесності педагогічними, науково-педагогічними, науковими працівниками та здобувачами вищої освіти ДТЕУ» (http://surl.li/disgq). Згідно п. 5 положення в межах ОП організовано перевірку на академічний плагіат випускних кваліфікаційних робіт здобувачів. Перевірка на наявність запозичень здійснюється з використанням відповідних технологій та комп'ютерних програм, які знаходяться у відкритому доступі у мережі Інтернет та UNICHECK. Між ДТЕУ і ТОВ «Антиплагіат» укладено договір на безкоштовне використання програми UNICHECK (https://unicheck.com/uk-ua). Контроль якості виконання ВКР здобувачів покладено на наукових керівників і проводиться за наступним алгоритмом: науковий керівник надсилає ВКР відповідальному по кафедрі, який здійснює перевірку ВКР на наявність академічного плагіату, що є підставою для подальшого прийняття рішення про допущення робіт до захисту. У разі виявлення у випускних атестаційних роботах елементів плагіату, про це повідомляють Комісію з питань етики та академічної доброчесності. Результати перевірки можуть бути оскаржені автором через подання апеляції на ім'я ректора у 3-денний термін після офіційного визнання наявності плагіату. В ДТЕУ на базі бібліотеки діє репозиторій наукових та навчально-методичних праць, дисертаційних робіт, випускних кваліфікаційних та курсових робіт, який забезпечує внутрішню перевірку на плагіат та використовується для постійного поповнення Національного репозиторію.

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

Здобувачі вищої освіти ДТЕУ обізнані в політиці академічної доброчесності, яку проводить університет, про що свідчить постійна популяризація розроблених та впроваджених документів, а саме: «Положення про дотримання академічної доброчесності педагогічними, науково-педагогічними, науковими працівниками та здобувачами вищої освіти ДТЕУ» (http://surl.li/disgq), «Етичний кодекс здобувача вищої освіти ДТЕУ» (http://surl.li/djuhy), Довідник студента (http://surl.li/afjlp). Для популяризації академічної доброчесності серед здобувачів ОП «Безпека систем електронних комунікацій в економіці» ведеться роз'яснювальна робота НПП в межах своїх дисциплін, під час консультацій керівниками випускних кваліфікаційних робіт та зустрічей з гарантом ОП, використовується комплекс профілактичних заходів для запобігання недотримання норм та правил академічної доброчесності під час екзаменаційних сесій (http://surl.li/aleeb). Результати опитування засвідчили, що 96,3% опитаних здобувачів ОП «Безпека систем електронних комунікацій в економіці» відповіли схвально, щодо проведення ДТЕУ популяризації академічної доброчесності (http://surl.li/kxhyn).

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

Питання відповідальності здобувачів освіти за порушення академічної доброчесності регулюється п.7 «Положення про дотримання академічної доброчесності педагогічними, науково-педагогічними, науковими працівниками та здобувачами вищої освіти ДТЕУ» (http://surl.li/disgq). Згідно цього Положення, при виявленні порушення академічної доброчесності здобувачі вищої освіти можуть бути притягнені до наступних видів академічної відповідальності: повторного проходження оцінювання (контрольна робота, іспит, залік тощо); повторного проходження відповідного освітнього компонента ОП; відрахування з Університету; позбавлення академічної стипендії; позбавлення наданих закладом освіти пільг з оплати навчання; відмова у присудженні відповідного ступеня вищої освіти, скасування рішення спеціалізованої вченої ради про присудження наукового ступеня та видачу відповідного диплома. Цим же документом в п.6 прописані види відповідальності педагогічних, науково-педагогічних та наукових працівників ДТЕУ за порушення академічної доброчесності. На ОП «Безпека систем електронних комунікацій в економіці», що акредитується, порушень академічної доброчесності виявлено не було.

6. Людські ресурси

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

Вимоги до рівня професіоналізму НПП визначено у «Положенні про порядок конкурсного відбору науково-педагогічних працівників Державного торговельно-економічного університету» (http://surl.li/kocvh). Конкурсна комісія перевіряє відповідність претендентів основним кваліфікаційним вимогам відповідно до Закону «Про вищу освіту» України та Ліцензійних умов провадження освітньої діяльності. Для оцінки кваліфікації кандидата кафедра може запропонувати йому прочитати відкриті лекції, провести лабораторні та практичні заняття для подальшого обговорення на засіданні кафедри. Професіоналізм викладачів ОП «Безпека систем електронних комунікацій в економіці» підтверджується також їх публікаціями у наукометричних базах даних, фахових виданнях, доповідями на наукових та науково-практичних конференціях в Україні та за кордоном, інших видах професійної діяльності, що

зазначено в Таблиці 2, а також при опитуванні здобувачів вищої освіти щодо якості викладання на освітній програмі. В процесі конкурсного відбору можуть також враховуватися досвід роботи, пройдене підвищення кваліфікації, професійна кваліфікація за фахом, сертифікацій згідно профілю кафедри тощо. Процедура конкурсного відбору викладачів ОП є прозорою і здатна забезпечити рівень професіоналізму викладацького складу, необхідний для успішної реалізації ОП.

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

Бізнес-партнери кафедри інженерії програмного забезпечення та кібербезпеки залучаються до спільної науково-практичної діяльності в рамках двосторонніх меморандумів, у тому числі з Департаментом кіберполіції Національної поліції України, ТОВ «IT-biz solutions», EPAM Ukraine, IBM, Microsoft Ukraine, корпорація Linkos Group ТОВ «M.E.Doc», ГО «Кіберковчег», та ін. (http://surl.li/jysef); рецензування ОП «Безпека систем електронних комунікацій в економіці» (Звєрєв В.П., Чорноус С.М.); проведення практичної підготовки згідно з укладеними договорами (http://surl.li/jyurs); навчальних безкоштовних курсів на платформах Coursera і Cisco Networking Academy завдяки партнерським угодам з університетом, зокрема, на випусковій кафедрі функціонує філіал Cisco Networking Academy; онлайн тренінгів і майстер-класів; реалізації заходів стажування і сертифікації викладачів кафедри (Таблиця 2); реалізації науково-освітніх заходів (http://surl.li/kxmef, http://surl.li/kxmfz, http://surl.li/kxmgl, http://surl.li/kxmhc, http://surl.li/kxmhq, http://surl.li/kxmio); головування екзаменаційної комісії із захисту ВКР ОС магістр (начальник управління Державного центру кіберзахисту, куратор технічної архітектури кіберполігону Держспецзв'язку Козаченко І.М.), випуск відбудеться в грудні 2023 р.

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

Фахівці-практики працюють на кафедрі інженерії програмного забезпечення за сумісництвом: Звєрєв В.П. заст. керівника служби з питань інформаційної безпеки та кібербезпеки – керівник управління інформаційної безпеки Апарату РНБО України, к.т.н., доцент (залучається до ОК «Інформаційні технології у системі забезпечення економічної безпеки держави»); Чубаєвський В.І. директор Директорату стратегічного планування та європейської інтеграції МВС, полковник поліції заступник начальника Департаменту інформаційно-аналітичної підтримки Національної поліції України, д.е.н., доцент (ОК «Етичний хакінг»).
В рамках ОК проводяться аудиторні заняття із залученням професіоналів-практиків, наприклад: Черноус С.М., заст. директора ТОВ «IT-biz solutions», ОК «Безпека мережевої та SMART інфраструктури», лекція «Основні стандарти розгортання локальних мереж» (23.03.2023р.); Козаченко І.М., нач. управління Державного центру кіберзахисту, куратор технічної архітектури кіберполігону Держспецзв'язку, дійсний член Української Академії кібербезпеки, ОК «Технології безпеки безпроводових та мобільних мереж», лекція «Основні алгоритми захисту програмного забезпечення» (20.09.2022р.).
Також стейкхолдери проводять відкриті лекції для здобувачів, наприклад, старший інспектор Управління протидії кіберзлочинам в м.Києві Департаменту кіберполіції Національної поліції України капітаном поліції Чепур І.М. (http://surl.li/kxmhq); у рамках заходу «KNUTE Career Week-2022» проведено вебінар «Можливості старту кар'єри в IT від SoftServe» (http://surl.li/kxnon) тощо.

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

Підвищення кваліфікації науково-педагогічних працівників регламентується «Положенням про підвищення кваліфікації та стажування науково-педагогічних, педагогічних і наукових працівників ДТЕУ» (http://surl.li/kodpa). Метою підвищення кваліфікації науково-педагогічних працівників ДТЕУ є їх професійний розвиток відповідно до державної політики у галузі освіти та забезпечення якості освіти. Раз на п'ять років усі викладачі проходять підвищення кваліфікації відповідно до офіційно затвердженого в установленому порядку Плану підвищення кваліфікації науково-педагогічних працівників ДТЕУ. З метою забезпечення високої якості викладання навчальних дисциплін та професійного розвитку викладачів в Університеті функціонує Академія освітнього дизайну ДТЕУ. Професійному розвитку викладачів сприяє проведення короткострокових науково-методичних семінарів, тематика яких визначається з урахуванням побажань НПП і носить актуальний характер. Центр європейської освіти ДТЕУ (http://surl.li/afinp) проводить заняття з інтенсивного вивчення іноземної мови. В Університеті діє система рейтингової оцінки діяльності НПП (http://surl.li/kdghj). Додатком до контракту є перспективний план, що визначає мінімальні зобов'язання з навчально-методичної, наукової, організаційної роботи, міжнародної діяльності тощо, що є критерієм і стимулом до професійного розвитку. Викладачі, які забезпечують освітній процес на ОП «Безпека систем електронних комунікацій в економіці», постійно проходять підвищення кваліфікації, що відтворено в Таблиці 2.

Продемонструйте, що ЗВО стимулює розвиток викладацької майстерності

Адміністрація Університету стимулює розвиток педагогічної майстерності: згідно п.3.19 та 3.21 Статуту ДТЕУ (http://surl.li/czrot), передбачає встановлення працівникам надбавок до посадового окладу відповідно до індивідуального внеску кожної особи у виконану роботу, вислуги років, премій та інших форм заохочення. Ректор Університету відповідно до законодавства, Статуту ДТЕУ та Колективного договору між адміністрацією та трудовим колективом Університету (http://surl.li/kodww) визначає процес, встановлює розміри додаткової оплати праці, надбавок, премій, матеріального забезпечення та заохочення педагогічних, науково-педагогічних, наукових та інших працівників закладу. За досягнення високих результатів у роботі зазначені працівники Університету можуть нагороджуватися державними нагородами, почесними званнями, нагородами, грамотами, цінними подарунками та

іншими формами заохочення. В ДТЕУ функціонує «Положення про систему рейтингової оцінки діяльності науково-педагогічних працівників» (http://surl.li/dabyj), яким передбачено врахування рейтингу при моральному та матеріальному стимулюванні та призначенні на посаду. На сайті університету оприлюднюються результати рейтингового оцінювання (http://surl.li/kdghj).

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?

Забезпечення досягнення визначених ОП цілей і ПРН фінансовими ресурсами передбачається фінансовим планом Університету та регулюється бухгалтерією за погодженням із деканом та завідувачем випускової кафедри. Фінансові аспекти діяльності ДТЕУ відображаються на офіційному сайті у розділі «Публічна інформація». Матеріально-технічна база Університету відповідає міжнародним стандартам щодо забезпечення освітнього процесу комп'ютерною технікою, програмним забезпечення, лабораторним обладнанням згідно «Статуту ДТЕУ» (http://surl.li/czrot), що дозволяє повною мірою досягти визначених ОП цілей та ПРН. Навчальні аудиторії оснащені демонстраційним обладнанням, комп'ютерами, а лекційні аудиторії – широкоформатними LED дисплеями. Функціонує бібліотечний комплекс «SMART-бібліотека» з комп'ютерами і шоломами віртуальної реальності (http://surl.li/agcam). В 2023 році ДТЕУ пройшов реєстрацію на платформі Research4Life, що надає можливість науково-педагогічним працівниками Університету та студентам отримати безкоштовний доступ до ресурсів провідних видавців наукової літератури. На випусковій кафедрі (http://surl.li/kxrax) облаштовано спеціалізовану лабораторію з кібербезпеки (http://surl.li/kxrbi). До складу лабораторії входять сучасні комп'ютери та спеціалізоване обладнання. Детальна інформація про матеріально-технічні ресурси ОП представлена у Таблиці 1. Навчально-методичне забезпечення ОП, що сприяє досягненню цілей, завдань та ПРН розташоване в СДН Moodle (http://surl.li/kbvhz) та є в доступі в корпоративному просторі Microsoft Teams.

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?

В ДТЕУ створені сприятливі соціально-побутові умови, які гарантують безпечність життя та здоров'я здобувачів вищої освіти. Якісна матеріально-технічна база освітнього середовища і вільний доступ до інформаційних ресурсів дозволяє повністю задовольнити потреби та інтереси здобувачів ОП, для яких створено сприятливі соціально-побутові умови: функціонують гуртожитки, кафетерії та їдальні, медпункти, пральня та інші побутові пункти. Унікальний спортивний комплекс, до якого входять футбольне поле зі штучним покриттям, майданчики для спортивних ігор, тренажерні зали. Кампус університету, окрім навчальних корпусів, налічує: 7 гуртожитків, 7 кафетеріїв та 5 їдальнь, різноманітні спортивні об'єкти (16 спортивних секцій), 2 бази відпочинку на Чорному морі. У 2021 році Президентом України було урочисто відкрито гуртожиток №7 ДТЕУ із сучасним рівнем комфортності проживання (http://surl.li/kxssr). Керівництво ДТЕУ постійно проводить опитування здобувачів вищої освіти щодо їхніх потреб та інтересів та враховує у стратегічних планах. Вплив студентів на формування та розвиток освітнього середовища реалізується через участь у Раді студентського самоврядування ДТЕУ (http://surl.li/agcau), Науковому товаристві студентів, аспірантів, докторантів і молодих вчених ДТЕУ, радах студентського самоврядування факультетів тощо. Так, відповідно до виявлених потреб, розширено мережу пунктів харчування, змінено розклад дзвінків, забезпечена можливість дистанційної підтримки вивчання освітніх компонент за допомогою корпоративного простору.

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

Стратегією розвитку ДТЕУ до 2030 року передбачено формування корпоративної культури, соціальної та екологічної відповідальності, підвищення мотивації та дотримання безпечних умов праці (http://surl.li/afifh). Безпечність освітнього середовища для життя та здоров'я здійснюється забезпеченням дотримання правил санітарної, пожежної безпеки, охорони праці. Проводяться інструктажі з техніки безпеки та пожежної безпеки на початку навчання у кожній технологічній та комп'ютерній лабораторії та перед початком проходження практики. Забезпечено доступність навчальних приміщень та іншої інфраструктури для осіб з особливими потребами. Функціонує пропускна система турнікетів за індивідуальними перепустками та працює професійна охорона, гарантуючи безпеку життя. На території ДТЕУ є медичний пункт, працює Центр педагогічних та психологічних досліджень (http://surl.li/diyvb), працівники якого здійснюють дослідження якості освітнього процесу та виявляють його проблемні зони, проводять соціально-психологічні тренінги. В ДТЕУ надається безкоштовна психологічна підтримка практичними психологами (http://surl.li/kxokg) та діє Юридична клініка «Центр правового захисту» (http://surl.li/diyvm). В університеті є діюча Скринька довіри, через яку студенти анонімно можуть порушити будь-яке питання. Керівництвом ДТЕУ регулярно проводяться опитування студентів щодо задоволеності освітнім середовищем та «Якість викладання навчальних дисциплін у ДТЕУ». Опитування студентів підтверджують, що ДТЕУ забезпечує безпечність освітнього середовища.

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?

В ДТЕУ відпрацьовано механізми освітньої, організаційної, інформаційної, консультативної та соціальної підтримки здобувачів вищої освіти, що здійснюється на різних ланках освітнього середовища Університету. За різними напрямками та різними інформаційними засобами здійснюється освітня, організаційна, інформаційна, консультативна та соціальна підтримка здобувачів другого (магістерського) рівня вищої освіти: адміністрацією факультету постійно проводяться організаційні збори, здійснюється постійна взаємодія зі старостами груп, на факультеті діє студентське самоврядування, яке керується «Положенням про студентське самоврядування» (http://surl.li/djlgs). Студентське самоврядування здійснює взаємозв'язок студентства з адміністрацією, забезпечує захист прав та інтересів здобувачів вищої освіти і наділене всіма необхідними ресурсами для самореалізації студентства, його гармонійного розвитку. В ДТЕУ функціонують відділ організаційно-виховної роботи та інформаційного забезпечення, навчальний відділ, студмістечко, відділ обліку студентів, Культурно-мистецький центр, Центр педагогічних та психологічних досліджень тощо. З метою інформаційної підтримки студентів активно функціонують сайт ДТЕУ (http://surl.li/drtbm) та соціальні мережі (Facebook, Instagram, Telegram), а також інформаційні екрани, стенди тощо. На сайтах кафедр Університету вказано дні та години консультацій викладачів, на кафедрі інженерії програмного забезпечення та кібербезпеки крім очних консультацій, викладачі проводять онлайн консультації з використанням Microsoft Teams. Там же розміщено всі необхідні навчально-методичні матеріали дисциплін, які викладаються на кафедрі: силабус, лекційні матеріали, методичні рекомендації до виконання лабораторних та самостійних робіт тощо.
У вкладці Студенту на сайті ДТЕУ в Довіднику студента (http://surl.li/afjlp) знаходиться повний перелік усіх нормативних положень університету, які окреслюють права та обов'язки здобувача, порядок формування індивідуального навчального плану, порядок відвідування занять та проходження практики тощо. Низка посилань з Довідника присвячений соціальному захисту студентів університету. Здобувачі мають право на отримання соціальної допомоги у випадках, встановлених законодавством та інші необхідні умови для здобуття освіти, у тому числі для осіб з особливими освітніми потребами та із соціально незахищених верств населення. Здобувачі ЗВО мають можливість брати участь у різноманітних студентських об'єднаннях та студентському самоврядуванні Університету. Центр розвитку кар'єри проводить заходи та консультації щодо інформації про вакансії тимчасового та постійного працевлаштування випускників і здобувачів (Ярмарки вакансій, Дні кар'єри, майстер-класи, презентації, тренінги, круглі столи тощо). Відповідно до результатів опитування здобувачів, рівень задоволення щодо освітньої, організаційної, інформаційної, консультативної та соціальної підтримки є високим.

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)

Організація навчального процесу осіб з особливими освітніми потребами здійснюється з урахуванням чинних норм законодавства. Відповідно до Статуту ДТЕУ п.3.6 (http://surl.li/czrot): «Університет зобов'язаний створювати необхідні умови для здобуття вищої освіти особами з особливими потребами». В університеті забезпечено доступ осіб з особливими потребами до приміщень ЗВО, гуртожитків: навчальний корпус А обладнаний підйомною платформою та ліфтом для осіб з обмеженими фізичними можливостями; у навчальному корпусі Д, актовій залі Конгрес-центру (корпус В), гуртожитках № 2, 4 є пандуси для заїзду візків; у гуртожитках № 2, 4, 7 спеціально обладнані кімнати для осіб з обмеженими фізичними можливостями (туалет та ванна обладнані спеціальними поручнями); сходові майданчики обладнані поручнями; в університеті є кнопки виклику ліфта, світлові вимикачі, розміщені на рівні доступу сидячої людини. Здобувачі з вадами опорно-рухового апарату отримують ключі від ліфтів. У центральному корпусі та Конгрес-центрі обладнані санвузли для осіб з обмеженими фізичними можливостями. Для забезпечення їх соціальної адаптації надається психологічна підтримка практичних психологів. Усі основні приміщення університету мають природне освітлення, враховано розташування меблів і обладнання відповідно до санітарних вимог. На освітній програмі «Безпека систем електронних комунікацій в економіці», що акредитується, студентів з особливими потребами немає

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?

В Університеті врегулювання конфліктних ситуацій здійснюється в рамках «Статуту ДТЕУ» (http://surl.li/czrot), «Колективного договору між трудовим колективом та адміністрацією ДТЕУ» (http://surl.li/kodww), «Контракту між адміністрацією ДТЕУ і здобувачем вищої освіти про навчання та виконання Правил внутрішнього розпорядку в ДТЕУ», «Етичного кодексу здобувача вищої освіти ДТЕУ» (http://surl.li/djuhy), «Антикорупційної програми ДТЕУ», «Положення про дотримання академічної доброчесності педагогічними, науково-педагогічними, науковими працівниками та здобувачами вищої освіти ДТЕУ» (http://surl.li/eekri), «Положення про інституційний репозитарій Державного торговельно-економічного університету» (http://surl.li/kxtwc), перевірки на наявність запозичень у дисертаційних і випускних кваліфікаційних роботах, наукових статтях за допомогою програмного продукту Unicheck, оприлюднення тексту дисертаційних робіт на офіційному сайті ДТЕУ.
В Університеті для вирішення конфліктів, пов'язаних із дотриманням академічної доброчесності, вченою радою ДТЕУ створено Комісію з питань етики та академічної доброчесності, затверджено Положення про дотримання академічної доброчесності педагогічними, науково-педагогічними, науковими працівниками та здобувачами вищої освіти ДТЕУ. Для забезпечення прозорості освітнього процесу, запобігання і протидії корупції, налагодження взаємних комунікацій в університеті діє «Електронна скринька довіри» та телефон гарячої лінії, за яким кожен здобувач може звернутися зі скаргою, надати пропозиції або висловити побажання. Серед здобувачів інформація поширюється шляхом доведення політик та процедур врегулювання конфліктних ситуацій як безпосередньо викладачами під час навчальних занять, консультацій, так і з використанням сучасних інформаційних технологій на

сайті університету. Під час реалізації ОП «Безпека систем електронних комунікацій в економіці» другого (магістерського) рівня вищої освіти випадків подібних конфліктних ситуацій зафіксовано не було.

8. Внутрішнє забезпечення якості освітньої програми

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

Процедури розроблення, затвердження, моніторингу та періодичного перегляду освітньої програми «Безпека систем електронних комунікацій в економіці» здійснюються відповідно до «Положення про розроблення та реалізацію освітніх програм ДТЕУ початкового, першого та другого рівнів вищої освіти» (http://surl.li/czrpb) та «Положення про систему забезпечення якості освітньої діяльності та якості вищої освіти (систему внутрішнього забезпечення якості) ДТЕУ» (http://surl.li/dabyq), згідно якого (п.3) освітні програми знаходяться в центрі місії ДТЕУ, пов'язаної з освітнім процесом, забезпечуючи відповідність його змісту запитам суспільства – студентів, роботодавців, держави. Освітні програми розробляються із залученням здобувачів вищої освіти та інших стейкхолдерів; вміщують перелік дисциплін у структурно-логічній послідовності та конкретні результати навчання (компетентності). Гарант ОП призначається наказом ректора з числа членів робочої групи, а його функції регламентуються «Положенням про гаранта освітньої програми у Державному торговельно-економічному університеті» (http://surl.li/dacju). Моніторинг та удосконалення освітніх програм ДТЕУ в процесі їх реалізації проводиться з метою забезпечення відповідності встановленим цілям діяльності, а також потребам здобувачів, суспільства в цілому. Всі документи розміщені у відкритому доступі на сайті ДТЕУ.

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

Перегляд ОП «Безпека систем електронних комунікацій в економіці» другого (магістерського) рівня вищої освіти відбувається щорічно відповідно до «Положення про розроблення та реалізацію освітніх програм ДТЕУ початкового, першого та другого рівнів вищої освіти» (http://surl.li/czrpb). Зацікавлені сторони інформуються заздалегідь про будь-які дії, заплановані або вжиті для удосконалення ОП. Регулярний моніторинг та удосконалення освітніх програм ДТЕУ в процесі їх реалізації організовує гарант освітньої програми із залученням членів робочої групи з метою забезпечення належного рівня освітніх послуг, формування конкурентоспроможних компетентностей та створення сприятливого й ефективного освітнього середовища для здобувачів вищої освіти. Актуальність ОП визначається наступними показниками: ступінь оновлюваності освітніх програм, участі роботодавців у розробці та внесенні змін і задоволеності здобувачів вищої освіти, що визначається за результатами опитування; рівень працевлаштування випускників на момент випуску з ДТЕУ, що визначається за результатами анкетування; участь у міжнародних програмах академічної мобільності; рейтинг за оцінками роботодавців або інша відповідна інформація від стейкхолдерів.
Оновлені освітні програми є складовою внутрішньої системи забезпечення якості освітньої діяльності та якості вищої освіти системи управління якістю ДТЕУ, включаються до Інформаційних пакетів ЄКТС, які щорічно оприлюднюються на офіційному сайті ДТЕУ (http://surl.li/kdnuf). Зокрема, перегляд та оновлення ОП, що акредитується, відбулося в 2022 році (http://surl.li/kvyhm). За рекомендаціями стейкхолдерів, у відповідності до зазначених в стандарті компетентностей та програмних результатів навчання було додано унікальні компетентності та програмні результати навчання, які не визначені відповідним СВО, проте забезпечуються обов'язковими освітніми компонентами та задають специфіку освітньої програми, що акредитується, а саме: КФ11 та РН24. Крім того, було змінено послідовність вивчення освітніх компонент (ОК5 «Цифрова криміналістика» перенесена в перший семестр з другого, а ОК7 «Етичний хакінг» навпаки). Також було вдосконалено зміст програми та робочої програми ОК «Англійська мова інформаційних технологій» з урахуванням специфіки спеціальності. Всі зміни в ОП оприлюднені на сайті у відкритому доступі (http://surl.li/kttpu), а зауваження та пропозиції від зацікавлених сторін можна надіслати гаранту ОП для обговорення та врахування при вдосконаленні в майбутньому.

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

Згідно «Положення про розроблення та реалізацію освітніх програм ДТЕУ початкового, першого та другого рівнів вищої освіти» (http://surl.li/czrpb) робоча група ОП, до складу якої входять здобувачі вищої освіти, здійснює моніторинг, аналізує ситуацію на ринку праці, вивчає потреби суспільства, професійного середовища відповідної спеціальності тощо. Крім того, реалізація студентоцентрованого підходу в ДТЕУ регламентується «Положенням про організацію освітнього процесу студентів» (http://surl.li/czzlo), «Положенням про систему забезпечення якості освітньої діяльності та якості вищої освіти (систему внутрішнього забезпечення якості)» (http://surl.li/dabyq), «Статутом ДТЕУ» (http://surl.li/czrot). Також здобувачі долучаються до перегляду ОП «Безпека систем електронних комунікацій в економіці» через органи студентського самоврядування. Зокрема, до складу робочої групи ОП, що акредитується, входили здобувачі: Бойко Т.В. (ФІТ, 4 курсу, 11 групи, спец. «Кібербезпека»; Чудік М.І. (ФІТ, 2 курсу, 6м групи, спец. «Інженерія програмного забезпечення», що надавали пропозицій щодо проєкту ОП за спеціальністю 125 «Кібербезпека» (http://surl.li/kvyhm). Зокрема, було змінено послідовність вивчення ОК та за побажаннями здобувачів було вдосконалено зміст програми та робочої програми ОК «Англійська мова інформаційних технологій» з урахуванням специфіки спеціальності. Всі зміни фіксуються в протоколах засідань робочої групи з розробки ОП «Безпека систем електронних комунікацій в економіці» другого (магістерського) рівня

вищої освіти.

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

Процедури внутрішнього забезпечення якості освітньої діяльності в ДТЕУ регламентуються «Статутом ДТЕУ» (http://surl.li/czrot) та «Системою управління якістю ДТЕУ» (http://surl.li/dabyq), відповідно до яких діють принципи прозорості і студентоцентризму, а студентське самоврядування бере учать у засіданнях Вченої ради ДТЕУ, зокрема, під час розгляду питань про затвердження програм та робочих програм навчальних дисциплін. До Ради студентського самоврядування (РСС) включено науковий сектор, члени якого входять до складу Наукового товариства здобувачів, аспіранті, докторантів та молодих вчених. Процедури внутрішнього забезпечення якості освітньої діяльності в ДТЕУ здійснюються завдяки включенню представників студентського самоврядування до робочих груп розробки і реалізації ОП, погодженню проєкту ОП з Головою РСС факультету інформаційних технологій. Представники РСС запрошуються на засідання робочої групи з розробки та реалізації ОП «Безпека систем електронних комунікацій в економіці». Роль РСС та її представників визначається «Положенням про студентське самоврядування» (http://surl.li/djlgs).
Вагоме значення РСС має щодо оцінки рівня задоволення якістю освітніх послуг та формуванню рейтингової оцінки освітньої діяльності НПП. Думка здобувачів також береться до уваги при опитуванні щодо організації та якості освітньої діяльності за ОП, що проводиться Центром педагогічних та психологічних досліджень ДТЕУ. Більшість здобувачів задоволені організацією та якістю освіти за ОП «Безпека систем електронних комунікацій в економіці».

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

Роботодавці безпосередньо залучені до процесу періодичного перегляду ОП «Безпека систем електронних комунікацій в економіці» та інших процедур забезпечення її якості, стейкхолдери беруть участь у засіданнях робочих груп з обговорення ОП, вносять пропозиції щодо актуалізації змісту окремих дисциплін, удосконалення інформаційного забезпечення ОП. Зокрема, ОП, що акредитується (http://surl.li/kvyhm), погоджена з В.П. Звєрєвим, заступником керівника служби з питань інформаційної безпеки та кібербезпеки, керівником управління інформаційної безпеки Апарату РНБО України та С.М. Чорноусом, заступником директора ТОВ «IT-biz solution». Кафедра інженерії програмного забезпечення та кібербезпеки, де впроваджується ОП «Безпека систем електронних комунікацій в економіці», має багато зовнішніх партнерів (http://surl.li/jysef), з якими укладено меморандуми про співпрацю, що дає можливість залучати досвід, професійні компетенції та ресурси стейкхолдерів. Так, враховуючи думку професійної спільноти, в останній редакції ОП (2023 р.), було додано унікальні компетентності та програмні результати навчання, які не визначені відповідним СВО, проте забезпечуються обов'язковими освітніми компонентами та задають специфіку освітньої програми, що акредитується. Щорічно на Ярмарку вакансій і Дні кар'єри та у разі потреби Центром розвитку кар'єри спільно з Центром педагогічних та психологічних досліджень шляхом опитування збираються пропозиції від роботодавців для удосконалення освітньої програми, після чого вносяться актуальні зміни.

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

Одним із структурних підрозділів Університету є Центр розвитку кар'єри (http://surl.li/aflss), який функціонує з 2001 року та має завдання координувати роботи факультетів та випускових кафедр щодо моніторингу кар'єрного шляху випускників, залучення їх до заходів, що сприяють кар'єрному розвитку студентів і аспірантів (майстер-класи, відкриті лекції, презентації, Дні університету та інші заходи).
Центром розвитку кар'єри та Центром педагогічних та психологічних досліджень (http://surl.li/kfamm) спільно з випусковими кафедрами щорічно проводиться опитування випускників поточного року, таким чином формується база випускників минулих років щодо їх кар'єрного шляху. Опитування відбувається щорічно під час проведення Дня Університету, а також протягом року шляхом розповсюдження он-лайн форми анкети через соціальні мережі та електронні адреси випускників. Пропозиції випускників вивчаються та враховуються при формуванні та оновленні освітніх програм. Також відслідковується траєкторія кар'єри успішних випускників, результатом цієї роботи є видання трьох збірників «Випускники КНТЕУ»: 2006 р., 2008 р., 2016 р. останній розміщено на сайті університету в розділі «Загальна інформація» підрозділі «Видання» (http://surl.li/afnyw). За ОП «Безпека систем електронних комунікацій в економіці» перший випуск магістрів відбудеться в грудні 2023 року.

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?

Кафедра інженерії програмного забезпечення та кібербезпеки за визначеною періодичністю успішно проходила процедури внутрішнього аудиту моніторингу Системи управління якістю (http://surl.li/afloq). У ході здійснення процедур внутрішнього забезпечення якості за час реалізації освітньої програми «Безпека систем електронних комунікацій в економіці» другого (магістерського) рівня вищої освіти проходить постійне вдосконалення змісту та форм освіти, що віддзеркалюється в нових редакціях програм та робочих програм освітніх компонент і нових редакціях ОП (http://surl.li/ktrjr). Зазначені зміни не сприймаються як недоліки, а являють собою еволюційний розвиток ОП, на який впливають як зовнішні фактори змін (військовий стан, пандемія COVID-19, запровадження карантинних заходів та перехід на дистанційну форму навчання тощо), так і побажання всіх груп професійної спільноти. За «Положенням про систему забезпечення якості освітньої діяльності та якості вищої освіти (систему

внутрішнього забезпечення якості) ДТЕУ» (http://surl.li/dabyq) та «Положенням про розроблення та реалізацію освітніх програм ДТЕУ фахового передвищого, початкового (короткого), першого (бакалаврського) та другого (магістерського) рівнів вищої освіти» (http://surl.li/czrpb) підготовка та реалізація ОП має чітку взаємопов'язаність між Стандартами вищої освіти МОН за відповідною спеціальністю, Стандартами ДТЕУ, положеннями ОПП, навчальними планами та програмами відповідних ОК, що забезпечує ефективність виправлення можливих недоліків. Аналіз звітів внутрішніх і зовнішніх аудиторів свідчать про те, що вони були повністю задоволені рівнем якості надання освітніх послуг за ОП «Безпека систем електронних комунікацій в економіці» і результатами діяльності кафедри, а саме: покращенням документообігу в електронній формі, наявністю усіх документів, що регулюють освітній процес за ОП «Безпека систем електронних комунікацій в економіці», навчально-методичним забезпеченням ОП. Зауважень у звітах щодо проведення процедур СУЯ кафедри інженерії програмного забезпечення та кібербезпеки не було.

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?

Акредитація за освітньою програмою «Безпека систем електронних комунікацій в економіці» є первинною. Проте, для забезпечення якості та удосконалення освітньої діяльності за ОП було враховано особливості та пропозиції за результатами інших акредитацій у ДТЕУ (http://surl.li/kfhir), а також було взято до уваги зауваження та побажання експертної групи з акредитації ОП «Безпека інформаційних і комунікаційних систем в економіці» першого (бакалаврського) рівня вищої освіти (акредитація проходила в грудні 2021 року). Зокрема, приділялась увага розвитку soft skills здобувачів при формуванні змісту програм всіх обов'язкових освітніх компонент (ОК1, ОК2, ОК4, ОК5, ОК7); кафедрою інженерії програмного забезпечення та кібербезпеки проводилась роз'яснювальна робота серед здобувачів щодо визнання результатів навчання, отриманих у неформальній освіті; до керівництва кваліфікаційними роботами випускників залучались НПП, які мають науковий ступінь та фахівці-практики, які проводять наукові дослідження за відповідним напрямком. Крім того, згідно рекомендацій експертів під час попередніх акредитацій ДТЕУ, постійно здійснюється активна діяльність щодо забезпечення необхідної кваліфікації співробітників кафедри інженерії програмного забезпечення та кібербезпеки, підвищення наукової активності науково-педагогічних працівників кафедри і членів групи забезпечення ОП «Безпека систем електронних комунікацій в економіці» щодо наукових публікацій та підвищення кваліфікації у сфері захисту інформації та кібербезпеки.

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

Залучення учасників академічної спільноти до процедур внутрішнього забезпечення якості освітньо-професійних програм регламентується «Положенням про розроблення та реалізацію освітніх програм ДТЕУ фахового передвищого, початкового (короткого), першого (бакалаврського) та другого (магістерського) рівнів вищої освіти» (http://surl.li/czrpb), згідно якого регулярний моніторинг та удосконалення освітніх програм ДТЕУ в процесі їх реалізації організовує керівник групи забезпечення спеціальності із залученням її членів з метою забезпечення належного рівня освітніх послуг, формування конкурентоспроможних компетентностей та створення сприятливого й ефективного середовища для студентів. Крім того, критерії, за якими відбувається моніторинг та удосконалення ОП «Безпека систем електронних комунікацій в економіці», формуються в результаті зворотного зв'язку з науково-педагогічними працівниками, здобувачами вищої освіти, випускниками, партнерами та іншими стейкхолдерами, а також є наслідком прогнозування розвитку спеціальностей та потреб суспільства. Центром педагогічних та психологічних досліджень ДТЕУ проводяться опитування (http://surl.li/kfifw), результати яких (http://surl.li/kxhyn) враховуються при залученні академічної спільноти до процедур внутрішнього забезпечення якості освітніх програм. Також з широким залученням академічної спільноти протягом місяця відбувався щотижневий навчально-методичний семінар для гарантів освітніх програм «Менеджмент якості освітніх програм ДТЕУ» (наказ ректора ДТЕУ № 2050 від 13.09.2022 р.).

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

Відповідно до п. 1.5 «Положення про систему забезпечення якості освітньої діяльності та якості вищої освіти (систему внутрішнього забезпечення якості) ДТЕУ» (http://surl.li/dabyq) відповідальними за функціонування та постійне удосконалення СВЗЯ ДТЕУ є ректор та, за його дорученням, керівник СУЯ ДТЕУ. Відповідальними за процеси СВЗЯ та діяльності в межах процесів є проректори, декани факультетів, завідувачі кафедр, керівники підрозділів, керівники груп забезпечення спеціальностей, гаранти освітніх програм та уповноважені особи. Відповідальні за процеси СВЗЯ та діяльність в межах процесів є підзвітними з питань забезпечення результативного функціонування та постійного удосконалення системи управління якістю керівнику СУЯ ДТЕУ. Керівник СУЯ ДТЕУ є підпорядкованим та підзвітним безпосередньо ректору ДТЕУ. Завданнями Центру педагогічних та психологічних досліджень ДТЕУ (http://surl.li/kfamm) є: проведення інтерактивних соціологічних досліджень для отримання зворотного зв'язку щодо якості підготовки фахівців в університеті від учасників освітнього процесу; проведення соціально-психологічних тренінгів, основна мета який формування soft skills студентів та з оволодіння практичними навичками; проведення діагностичного тестування щодо вибору майбутнього професійного спрямування вступників; надання психологічних консультацій учасникам освітнього процесу.

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?

Важливими чинниками регулювання прав та обов'язків усіх учасників освітнього процесу є дотримання положень Законів України «Про освіту», «Про вищу освіту», «Стандартів і рекомендацій щодо забезпечення якості в Європейському просторі вищої освіти» та інших законодавчих актів у сфері освіти. Здобувачі вищої освіти протягом свого навчання керуються установчими документами ЗВО (http://surl.li/kfzhh), такими як «Статут ДТЕУ» (http://surl.li/czrot), «Правила внутрішнього розпорядку в ДТЕУ» (http://surl.li/eekmy), «Положення про організацію освітнього процесу студентів» (http://surl.li/czzlo), «Положення про дистанційне навчання у ДТЕУ» (http://surl.li/dacch), «Положення про дотримання академічної доброчесності педагогічними, науково-педагогічними, науковими працівниками та здобувачами вищої освіти ДТЕУ» (http://surl.li/disgq), «Положення про оцінювання результатів навчання здобувачів і аспірантів (http://surl.li/kfzef) тощо (http://surl.li/kfzfb). Крім того, права та обов'язки учасників освітнього процесу прописані у Договорі між адміністрацією ДТЕУ і здобувачем про виконання Правил внутрішнього розпорядку в ДТЕУ. Установчі документи, якими керується університет є у вільному доступі на офіційному сайті. Згідно «Статуту ДТЕУ» права та обов'язки науково-педагогічних, наукових, педагогічних працівників, навчально-допоміжного, адміністративного, обслуговуючого персоналу визначаються «Правилами внутрішнього розпорядку в ДТЕУ» та посадовими інструкціями. Вся інформація розміщена на сайті ЗВО у вільному доступі (http://surl.li/kfzgg).

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

З метою отримання зауважень та пропозицій заінтересованих осіб (стейкхолдерів) щодо ОП «Безпека систем електронних комунікацій в економіці» другого (магістерського) рівня вищої освіти вся необхідна інформація міститься на офіційній сторінці кафедри інженерії програмного забезпечення та кібербезпеки ДТЕУ за посиланням: http://surl.li/ktrjr.

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

Інформація про освітню програму, що акредитується, оприлюднена у відкритому доступі на сайті ДТЕУ: http://surl.li/kvyhm. Рецензії стейкхолдерів: http://surl.li/kxvkn.

11. Перспективи подальшого розвитку ОП

Якими загалом є сильні та слабкі сторони ОП?

Сильні сторони ОП «Безпека систем електронних комунікацій в економіці»:
- ОП «Безпека систем електронних комунікацій в економіці» в ДТЕУ має за мету підготувати висококваліфікованих фахівців у сфері кібербезпеки та захисту інформації, зокрема в економіці, що підкреслює унікальність ОП та галузеве спрямування ЗВО, відповідає актуальним тенденціям розвитку спеціальності 125 «Кібербезпека» та ринку праці, враховує галузевий та регіональний контекст.
- Потужна база договорів про співпрацю із стейкхолдерами, залучення фахівців-практиків до освітнього процесу.
- Високий рівень студентоцентризму, можливість обирати гнучку індивідуальну освітню траєкторію та залучення здобувачів до перегляду змісту освітньої програми.
- Політики, стандарти і процедури дотримання академічної доброчесності за ОП є чіткими і зрозумілими; правила і процедури, що регулюють права та обов'язки всіх учасників освітнього процесу, послідовно дотримуються під час реалізації ОП.
- Навчально-педагогічні працівники, що залучені до освітнього процесу на ОП «Безпека систем електронних комунікацій в економіці», активно підвищують свою кваліфікацію в галузі інформаційної безпеки та кібербезпеки, постійно проявляють наукову активність та проходять стажування.
- ДТЕУ має потужну внутрішню систему забезпечення якості освіти, а також високий рівень інформаційної підтримки, що забезпечує відкритість, прозорість та вільний доступ усіх учасників освітнього процесу до інформаційних ресурсів та визначає високий рівень підготовки фахівців.

Слабкі сторони ОП «Безпека систем електронних комунікацій в економіці»:
- Невеликий відсоток штатних НПП, що мають базову освіту або науковий ступінь за спеціальністю 125 «Кібербезпека».
- Низький рівень фінансування та обмеження можливостей на закупівлю обладнання у сфері кібербезпеки та захисту інформації.

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

Перспективи розвитку ОП «Безпека систем електронних комунікацій в економіці» ґрунтуються на вдосконаленні освітнього процесу та наближення змісту навчання за ОП до потреб реального сектору економіки. У зв'язку з цим, упродовж найближчих років планується:

- здійснення першого випуску магістрів за освітньою програмою «Безпека систем електронних комунікацій в економіці» у грудні 2023 року;
- залучення кращих випускників до навчання в аспірантурі та викладацької діяльності на кафедрі інженерії програмного забезпечення та кібербезпеки для збільшення штатних НПП за даним напрямком;
- подальше оновлення та вдосконалення навчальної матеріально-технічної бази кафедри інженерії програмного забезпечення та кібербезпеки, її наповнення сучасними зразками комп'ютерної техніки та програмно-апаратних комплексів;
- активне залучення фахівців-практиків до викладання дисциплін на ОП;
- активізація академічної мобільності шляхом залучення на навчання за ОП «Безпека систем електронних комунікацій в економіці» іноземних студентів;
- практичне впровадження принципів неформальної та дуальної освіти, як елементів набуття здобувачами вміння саморозвитку та визнання його результатів.

Керівництво Державного торговельно-економічного університету забезпечує повну підтримку ОП «Безпека систем електронних комунікацій в економіці» другого (магістерського) рівня вищої освіти в реалізації зазначених перспектив розвитку.

Запевнення

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

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

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

Додатки:

Таблиця 1. Інформація про обов'язкові освітні компоненти ОП

Таблиця 2. Зведена інформація про викладачів ОП

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

***

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

Документ підписаний кваліфікованим електронним підписом/кваліфікованою електронною печаткою.

Інформація про КЕП

ПІБ:

Дата:

Таблиця 1. Інформація про обов'язкові освітні компоненти ОП

Назва освітнього компонента	Вид компонента	Силабус або інші навчально-методичні матеріали		Якщо освітній компонент потребує спеціального матеріально-технічного та/або інформаційного забезпечення, наведіть відомості щодо нього*
		Назва файла	Хеш файла	
Технології безпеки безпроводових та мобільних мереж	навчальна дисципліна	*ОК2_Технології безпеки безпроводових та мобільних мереж_2022.pdf*	4MGhAOHf13WY1xd TaWGH4rtutlJx9obX 9iNIIw+NQpU=	*Лекційні заняття:* *Мультимедійне обладнання (ПК, проектор, колонки)* *SMART-бібліотека ДТЕУ* *Лабораторні заняття проводяться в лабораторії Б-514:* *Апаратне забезпечення (кількість комп'ютерів – 24, рік введення в експлуатацію – 2020):* *OctalCore Intel Core i7-9700, 4600 MHz, Asus Prime H310M-R R2.0, 8 Gb DDR4-2666 DDR4 SDRAM, ST1000DM010-2EP102 1 ТБ, 7200 RMP, SATA-III* *Монітори (Acer V226HQL bid; 21,5□) (17 мм)* *SMART-дошка* *Ліцензійне програмне забезпечення:* *• Microsoft Windows 10 Professional* *• Microsoft Office Professional Plus 2016* *• 7-Zip 19.00* *• Adobe Acrobat Reader* *• MPC-BE x64 1.5.3.4488* *• ESET NOD32 Antivirus* *• Google Chrome 80.0.3987.122* *• Mozilla Firefox 72.0* *Програмне забезпечення вільного доступу:* *Nmap, Steghide, Oracle VM VirtualBox, Cisco Packet Tracer, PyCharm* *Корпоративні інформаційні ресурси:* *Бібліотека ДТЕУ* *http://libtomcat.knute.edu.ua/library/DocSearchForm* *Система дистанційного навчання ДТЕУ* *https://cdn.knute.edu.ua/course/index.php* *Корпоративна платформа Microsoft Office 365*
Англійська мова інформаційних технологій	навчальна дисципліна	*ОК1_Англійська мова інформаційних технологій_2022.pdf*	uKXfKpXy/3sOGDx OXsYduPmcUXLUsX FQMFvtvD9sdFo=	*Практичні заняття проводяться в Л-217:* *Мультимедійне обладнання (ПК, проектор, колонки).* *Апаратне забезпечення (кількість комп'ютерів – 25, рік введення в експлуатацію – 2017, рік останнього ремонту – 2020):* *QuadCore Intel Core i5-3340, 3200 MHz (32 x 100)* *ECS H61H-G11* *2 ГБ DDR3-1333 + 2 ГБ DDR3-1333* *Intel HD Graphics 2500* *TOSHIBA DT01ACA100 (1 ТБ, 7200 RPM, SATA-III)* *Ліцензійне програмне забезпечення:* *• Microsoft Windows 10 Pro x64*

				• *360 Total Security* • *Adobe Reader* • *Google Chrome* • *Microsoft Office Professional Plus 2016* • *Mozilla Firefox* • *Opera* • *VLC media player* • *XDocument Converter* *Спеціальне ліцензійне програмне забезпечення:* *SketchUp 2017* *Snetclass V8.3* *EuroTalk Movie Talk* *Корпоративні інформаційні ресурси:* *Бібліотека ДТЕУ* *http://libtomcat.knute.edu.ua/library/DocSearchForm* *Система дистанційного навчання ДТЕУ* *https://cdn.knute.edu.ua/course/index.php* *Корпоративна платформа Microsoft Office 365*
Технології безпеки Web-ресурсів	навчальна дисципліна	*ОК3_Технології безпеки WEB-ресурсів_2022.pdf*	k/CIzLIWMGCmPQTb9b7iIyryzdysJUAcpHrK+FbmE6Q=	*Лекційні заняття:* *Мультимедійне обладнання (ПК, проектор, колонки).* *SMART-бібліотека ДТЕУ* *Лабораторні заняття проводяться в лабораторії Б-504:* *Апаратне забезпечення (кількість комп'ютерів – 15, рік введення в експлуатацію – 2013, рік останнього ремонту – 2020):* *DualCore Intel Core i3-3220, 3300 MHz* *MSI H61M-P31/G3 (MS-7788)* *4059 МБ DDR3* *GeForce GT 630 (1 ГБ)* *Hitachi HDS721010CLA330 ATA Device* *Монітори (LG LED 22EN33) (17 мм)* *Ліцензійне програмне забезпечення:* • *Microsoft Windows 10 Home Single Language x64* • *7-Zip 18.01* • *Google Chrome* • *Java 9.0.4* • *Microsoft Office Professional Plus 2016* • *MySQL* • *Opera* • *STDU Viewer version 1.6.375.0* • *Sublime Text 3* *Програмне забезпечення вільного доступу:* *Python 2.7, MySQL, Java Development Kit, LabVIEW 8.6, ERwin-CASE, Corel Draw X4, Cisco Packet Tracer, Adobe Captivate 4, Adobe Illustrator CS, Adobe Photoshop CSS, Macromedia Autorware 6, Macromedia Director 8.5, MS Project, Hot Potatoes 6, ShadowDefender, WinDJView, Pretty Good Privacy, XAMPP, M.E. Dos IS, Eclipce, GPPS, Stata, Статистика, NetCracker Professional 3.1, Oracle VM VirtualBox, KaliLinux, VS Code*

				Корпоративні інформаційні ресурси: *Бібліотека ДТЕУ* *http://libtomcat.knute.edu.ua/library/DocSearchForm* *Система дистанційного навчання ДТЕУ* *https://cdn.knute.edu.ua/course/index.php* *Корпоративна платформа Microsoft Office 365*
Правове забезпечення інформаційної безпеки в економічних системах	навчальна дисципліна	*ОК4_Правове забезпечення інформаційної безпеки в економічних системах_2022.pdf*	PKgdQvONo6LarZFGr5DpoB6mvxiVuKsvmR8z9oh4baY=	*Лекційні заняття:* *Мультимедійне обладнання (ПК, проектор, колонки).* *Корпоративні інформаційні ресурси:* *Бібліотека ДТЕУ* *http://libtomcat.knute.edu.ua/library/DocSearchForm* *Система дистанційного навчання ДТЕУ* *https://cdn.knute.edu.ua/course/index.php* *Корпоративна платформа Microsoft Office 365*
Етичний хакінг	навчальна дисципліна	*ОК5_Етичний хакінг_2022.pdf*	XW/MaW+o5RrzOaH4gjeDzAymG5MEOFDOekYAw6iblIQ=	*Лекційні заняття:* *Мультимедійне обладнання (ПК, проектор, колонки).* *SMART-бібліотека ДТЕУ* *Лабораторні заняття проводяться в лабораторії Б-514:* *Апаратне забезпечення (кількість комп'ютерів – 24, рік введення в експлуатацію – 2020):* *OctalCore Intel Core i7-9700, 4600 MHz, Asus Prime H310M-R R2.0, 8 Gb DDR4-2666 DDR4 SDRAM, ST1000DM010-2EP102 1 ТБ, 7200 RMP, SATA-III* *Монітори (Acer V226HQL bid; 21,5□) (17 мм)* *SMART-дошка* *Ліцензійне програмне забезпечення:* *• Microsoft Windows 10 Professional* *• Microsoft Office Professional Plus 2016* *• 7-Zip 19.00* *• Adobe Acrobat Reader* *• MPC-BE x64 1.5.3.4488* *• ESET NOD32 Antivirus* *• Google Chrome 80.0.3987.122* *• Mozilla Firefox 72.0* *Програмне забезпечення вільного доступу:* *Nmap, Steghide, Oracle VM VirtualBox, Cisco Packet Tracer, PyCharm* *Корпоративні інформаційні ресурси:* *Бібліотека ДТЕУ* *http://libtomcat.knute.edu.ua/library/DocSearchForm* *Система дистанційного навчання ДТЕУ* *https://cdn.knute.edu.ua/course/index.php* *Корпоративна платформа Microsoft Office 365*
Безпека мережевої та SMART інфраструктури	навчальна дисципліна	*ОК6_Безпека мережевої та SMART*	z5qG/ENh+8sTynQkaQ6ZWg8wAE7qTYYk/olo4VecEQo=	*Лекційні заняття:* *Мультимедійне обладнання (ПК, проектор, колонки).*

		інфраструктури_2022.pdf		*SMART-бібліотека ДТЕУ* *Лабораторні заняття проводяться в лабораторії Б-504:* *Апаратне забезпечення (кількість комп'ютерів – 15, рік введення в експлуатацію – 2013, рік останнього ремонту – 2020):* *DualCore Intel Core i3-3220, 3300 MHz* *MSI H61M-P31/G3 (MS-7788)* *4059 МБ DDR3* *GeForce GT 630 (1 ГБ)* *Hitachi HDS721010CLA330 ATA Device* *Монітори (LG LED 22EN33) (17 мм)* *Ліцензійне програмне забезпечення:* *• Microsoft Windows 10 Home Single Language x64* *• 7-Zip 18.01* *• Google Chrome* *• Java 9.0.4* *• Microsoft Office Professional Plus 2016* *• MySQL* *• Opera* *• STDU Viewer version 1.6.375.0* *• Sublime Text 3* *Програмне забезпечення вільного доступу:* *Python 2.7, MySQL, Java Development Kit, LabVIEW 8.6, ERwin-CASE, Corel Draw X4, Cisco Packet Tracer, Adobe Captivate 4, Adobe Illustrator CS, Adobe Photoshop CSS, Macromedia Autorware 6, Macromedia Director 8.5, MS Project, Hot Potatoes 6, ShadowDefender, WinDJView, Pretty Good Privacy, XAMPP, M.E. Dos IS, Eclipce, GPPS, Stata, Статистика, NetCracker Professional 3.1, Oracle VM VirtualBox, KaliLinux, VS Code* *Корпоративні інформаційні ресурси:* *Бібліотека ДТЕУ* *http://libtomcat.knute.edu.ua/library/DocSearchForm* *Система дистанційного навчання ДТЕУ* *https://cdn.knute.edu.ua/course/index.php* *Корпоративна платформа Microsoft Office 365*
Цифрова криміналістика	навчальна дисципліна	*ОК7_Цифрова криміналістика_2022.pdf*	b67yZWAIqQZqRDQhuJE+vB4p/ZDzaaBpo08n3ufkhKs=	*Лекційні заняття:* *Мультимедійне обладнання (ПК, проектор, колонки).* *Лабораторні заняття проводяться в лабораторії Б-510:* *Апаратне забезпечення (кількість комп'ютерів – 15, рік введення в експлуатацію – 2016):* *Intel Pentium 3,2 GHz, DDR2 8Gb, HDD 620 Gb* *Монітори – ACER K192HQL (19□), Sumsung S19D300 (19□)* *Ліцензійне програмне забезпечення:* *• MS Windows 8.1* *• Ubuntu* *• ABYY FineReader*

				• *MS Office 2010* • *Java Development Kit* • *Eclipce* • *ESET NOD32* • *Mozilla Firefox* • *Google Chrome* *Програмне забезпечення вільного доступу:* *Java Development Kit, Eclipse, NetCracker Professional 3.1* *Корпоративні інформаційні ресурси:* *Бібліотека ДТЕУ* *http://libtomcat.knute.edu.ua/library/DocSearchForm* *Система дистанційного навчання ДТЕУ* *https://cdn.knute.edu.ua/course/index.php* *Корпоративна платформа Microsoft Office 365*
Практична підготовка	практика	*Програма практики 2022.pdf*	CQSfE73ZeQiQQovvr5h1KPypKIGlTYqEOKwF4AhRewg=	*Інформаційне забезпечення бази практики*
Практична підготовка 1	практика	*РП_Практ_підготовка_1_2022.pdf*	r3kNLwVoiPx6BohNJxuu59Hk1KNicZY5oclvYFM4Ekw=	*Інформаційне забезпечення бази практики*
Практична підготовка 2	практика	*РП_Практ_підготовка_2_2022.pdf*	ZNr/hXpRmJQj5N+/szlYOsjCaXWY3sOn2HBudaUD+Do=	*Інформаційне забезпечення бази практики*
Випускна кваліфікаційна робота	підсумкова атестація	*МР_ВКР_125М_2022.pdf*	oiZKT2IwUhQxVptNa3GMW7VkBHku8zp39kYQ9DGUNyo=	*Інформаційне забезпечення відповідно до напряму дослідження та теми випускної кваліфікаційної роботи*

* 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
414268	Власенко Лідія Олександрівна	Доцент, Основне місце роботи	Факультет інформаційних технологій	Диплом бакалавра, Київська православна богословська академія, рік закінчення: 2022, спеціальність: 041 Богослов'я, Диплом магістра, Національний університет харчових технологій, рік закінчення: 2003, спеціальність: 092502 Комп'ютерно-інтегровані технологічні	20	Цифрова криміналістика	Освіта: вища Науковий ступінь: кандидат технічних наук Вчене звання: доцент Рівень наукової та професійної активності відповідає пунктам Кадрових вимог 1, 3, 4, 7, 8, 12, 19 1) Публікації, включені до міжнародних наукометричних баз Scopus, Web of Science: 1. Zaiets, N., Vlasenko, L., Lutska, N. (2023). Neural Network Model for Predicting Technological Losses of

				процеси і виробництва, Диплом кандидата наук ДК 066152, виданий 26.01.2011, Атестат доцента 12ДЦ 037364, виданий 17.01.2014			a Sugar Factory. In: Szewczyk, R., Zieliński, C., Kaliczyńska, M., Bučinskas, V. (eds) Automation 2023: Key Challenges in Automation, Robotics and Measurement Techniques. AUTOMATION 2023. Lecture Notes in Networks and Systems, vol 630. Springer, Cham. (Scopus) https://doi.org/10.1007/978-3-031-25844-2_92. Vlasenko, L., Zaiets, N., Lutska, N., Savchuk, O. (2023). Neural Network Model for Predicting the Resource Efficiency of the Defecosaturation Department of a Sugar Factory. In: Vasant, P., Weber, GW., Marmolejo-Saucedo, J.A., Munapo, E., Thomas, J.J. (eds) Intelligent Computing & Optimization. ICO 2022. Lecture Notes in Networks and Systems, vol 569. Springer, Cham. https://doi.org/10.1007/978-3-031-19958-5_12 (Scopus) 3. Vlasenko, L.; Lutska, N.; Zaiets, N.; Korobiichuk, I.; Hrybkov, S. Core Ontology for Describing Production Equipment According to Intelligent Production. Appl. Syst. Innov. 2022, 5 (5), 98. https://doi.org/10.3390/asi5050098 (Web of Science) 4. Effective robust optimal control system for a lamellar pasteurization-cooling unit under the conditions of intense external perturbations . Nataliia Lutska, Nataliia Zaiets, Lidiia Vlasenko, Volodymyr Shtepa .Ukrainian Food Journal. 2018. Volume 7. Issue 3. Page 511 – 521 (Web of Science) 5. Modern development technologies and investigation of food production technological complex automated systems Korobiichuk, I., Ladanyuk, A,. Zaiets, N., Vlasenko, L. 2018, Pages 52–56. ICMSCE 2018: 2018 2nd International Conference on Mechatronics Systems and Control Engineering, 2018, Amsterdam,

							Netherlands February, February, 2018 DOI: 10.1145/3185066.3185075 (Scopus) 6. System modeling for construction of the diagnostic subsystem of the integrated automated control system for the technological complex of food industries Zaiets, N., Vlasenko, L., Lutskaya, N., Usenko, S. 2019, Pages 93–98. ICMRE'19: Proceedings of the 5th International Conference on Mechatronics and Robotics Engineering, 2019, Rome, Italy,: February 2019 DOI: 10.1145/3314493.331523 (Scopus) 7. Zaiets, N.A., Savchuk O.V., Shtepa V.M., Lutska N.M., Vlasenko L.O. The synthesis of strategies for the efficient performance of sophisticated technological complexes based on the cognitive simulation modelling. Науковий вісник Національного гірничого університету. – 2021. – №2. – с. 110-117. https://doi.org/10.33271/nvngu/20212/110. (Scopus) Наукові статті у фахових виданнях: 1. Луцька, Н. М., Байдаєв, Р. В., Герасименко, Т. М., & Власенко, Л. О. (2022). Системи керування технологічними об'єктами харчової промисловості з прогнозувальними моделями. Наукові праці НУХТ 2022. Том 28, No 3, стор 7-19 DOI: 10.24263/2225-2924-2022-28-3-3 2. Власенко Л.О., Савченко Т.В., Луцька Н.М. Вибір ієрархії та онтології верхнього рівня для розробки інтелектуальних автоматизованих систем управління промисловим підприємством // Наукові праці Національного університету харчових технологій. – 2021. – Т. 27, № 4. – С. 16-27. 3. Луцька Н.М., Власенко Л.О., Ладанюк А.П. Проєктування інтелектуальних автоматизованих

								систем керування технологічними процесами харчових виробництв засобами SysML. Частина1: огляд діаграм SysML, розробка діаграми вимог // Наукові праці Національного університету харчових технологій. – 2021. – Т. 27, № 3. – С . 15-24. 4. Луцька Н.М., Власенко Л.О., Пупена О.М. Технічні аспекти інтеграції відкритих онтологічних баз знань із сучасними автоматизованими системами управління // Наукові праці Національного університету харчових технологій. – 2021. – Т. 27, № 1. – С . 8-21. 5. Ладанюк А.П. Ефективність інтелектуальних систем керування технологічними об'єктами. Частина 1. Основні положення // А.П. Ладанюк, Н.М. Луцька, Я.В. Смітюх, Л.О. Власенко, М.В. Сашньова / Харчова промисловість, 2019. – №25. – С. 141-147. 3) Підручники, навчальні посібники, монографії 1. Луцька Н.М., Заєць Н.А., Власенко Л.О. Оптимізаційні рішення для автоматизованого управління складними технологічними комплексами: монографія. – Київ: Видавництво Ліра-К, 2022. – 328 с 2. Ладанюк А.П. Методологія наукових досліджень: Навч. посіб. / А.П. Ладанюк, Л.О. Власенко, В.Д. Кишенько. – Київ : Видавництво Ліра-К, 2018. – 352 с. 3. Методи сучасної теорії управління: підручник / А.П. Ладанюк, Н.М. Луцька, В.Д. Кишенько, Л.О. Власенко, В.В. Іващук – К.: Видавництво Ліра-К, 2018. – 368 с. 4) Навчально-методичні видання: 1. Програма дисципліни «Безпека мережевої та SMART інфраструктури» призначена для студентів освітнього ступеня «магістр»

							галузі знань 12 «Інформаційні технології» спеціальності 125 «Кібербезпека», ОП «Безпека систем електронних комунікацій в економіці». – К.: КНТЕУ, 2021. 2. Програма дисципліни «Цифрова криміналістика» призначена для студентів освітнього ступеня «магістр» галузі знань 12 «Інформаційні технології» спеціальності 125 «Кібербезпека», ОП «Безпека систем електронних комунікацій в економіці». – К.: КНТЕУ, 2021. 3. Пашорін В.І., Власенко Л.О., Десятко А.М., Рзаєва С.Л., Савченко Т.В., Сашньова М.В., Самойленко Ю.О., Костюк Ю.В., Чубаєвський В.І., Захаров Р.Г. Методичні рекомендації до виконання випускного кваліфікаційного проекту для студ. ОС «бакалавр», спец. 125 «Кібербезпека». – К.: КНТЕУ, 2021. – 43 с. 4. Пашорін В.І. Костюк Ю.В., Самойленко Ю.О., Власенко Л.О., Савченко Т.В. Методичні рекомендації до виконання курсової роботи студентів з курсу «Безпека інформаційних систем та мереж» для студ. ОС «бакалавр», спец. 125 «Кібербезпека». – К.: КНТЕУ, 2021. – 42 с. 5. Браіловський М.М., Костюк Ю.В., Самойленко Ю.О., Власенко Л.О., Савченко Т.В. Методичні рекомендації до виконання курсової роботи студентів з курсу «Організація комп'ютерних мереж» для студ. ОС «бакалавр», спец. 125 «Кібербезпека». – К.: КНТЕУ, 2021. – 72 с. 6. Лукова-Чуйко Н.В., Фесенко А.О., Власенко Л.О., Савченко Т.В., Сашньова М.В., Костюк Ю.В. Криптографічні

							методи захисту інформації. Робоча програма для студ. ОС «бакалавр», спец. 125 «Кібербезпека». – К.: КНТЕУ, 2021. – 19 с. 7. Самойленко Ю.О., Власенко Л.О., Савченко Т.В., Сашньова М.В., Костюк Ю.В., Безпека програмного забезпечення. Програма для студ. ОС «бакалавр», спец. 125 «Кібербезпека». – К.: КНТЕУ, 2021. – 14 с. 7) Участь в атестації наукових кадрів, як офіційного апонента, або члена постійної спеціалізованої вченої ради: Вчений секретар спеціалізованої вченої ради К 26.058.05 у Національному університеті харчових технологій 2017 – 2021 р.р. 8) Науковий керівник, відповідальний виконавець наукової теми, член редакційної колегії (кат Б) «Моделювання інформаційно-аналітичної системи контролю якості процесу виробництва продукці» (термін 01.2021-12.2024р.р.; державний реєстраційний номер: 0121U109155 дата реєстрації: 03-03-2021р.) 12) Наявність апробаційних та/або науково-популярних, та/або консультаційних (дорадчих), та/або науково-експертних публікацій з наукової або професійної тематики: 1. Щербак І.І., Власенко Л.О. Захист комерційної інформації приватного підприємства на основі симетричних алгоритмів шифрування / І.В. Щербак, Л.О. Власенко // Матеріали VIII Міжнародної науково-технічної Internet-конференції «Сучасні методи, інформаційне, програмне та технічне забезпечення систем керування

організаційно-технічними та технологічними комплексами», 26 листопада 2021. [Електронний ресурс] – К: НУХТ, 2021 р. – С. 295-296 — Режим доступу: https://drive.google.com/file/d/1F_XOymRYbUgyH5-T49VPYyTCel2YsH2W/view
2. Власенко Л.О., Луцька Н.М., Десятко А.М. Основні види ризиків кіберзагроз промислового суб'єкта господарювання в умовах Industry 4.0 // Збірник тез V Всеукраїнської науково-практичної конференції «Нові інформаційні технології управління бізнесом». – Київ: Спілка автоматизаторів бізнесу, 2022. – С. 38-40.
3. Власенко Л.О., Грибков С.В., Савченко Т.В. Проектування інформаційної системи захисту промислової інформації з урахуванням тенденцій Industry 4.0 // Тези доповідей дев'ятої міжнародної науково-практичної конференції «Управління розвитком технологій». Тема: Інформаційні технології розвитку змісту освіти. – К. : КНУБА, 2022. – С. 61-62.
4. Власенко Л.О. Моделювання бази даних автомаизованої системи формування документів для вступних випробовувань на основі семантичних підходів / Л.О. Власенко, І.В. Мурга // Наукові праці Третьої міжнар. наук.-практ. конф. «Сучасні тенденції розвитку інформаційних систем і телекомунікаційних технологій», 25–26 січня 2021 р. (Київ, Україна). – К. : НУХТ, 2021. С. 55-57.
5. Lutskaya N., Vlasenko L., Zaiets N., Shtepa V. (2021) Ontological Aspects of Developing Robust Control Systems for Technological Objects.

							In: Vasant P., Zelinka I., Weber GW. (eds) Intelligent Computing and Optimization. ICO 2020. Advances in Intelligent Systems and Computing, vol 1324. Springer, Cham. https://doi.org/10.1007/978-3-030-68154-8_107 19) Участь у професійних об'єднаннях: Діяльність за спеціальністю у формі участі у професійних та/або громадських об'єднаннях ГО «Кіберковчег» Стажування: 1. Інфораційна гігієна. Як розпізнати брехню в соцмережах, в інтернеті та на телебаченні. (45 год., 1,5 кредити ЄКТС) 2. Участь у Всеукраїнському науково-практичному семінарі «Досвід Європейського Союзу у сфері реагування на виклики безпеки» у межах реалізації проєкту Еразмус+ Модулі Жана Моне «Європейська політична інтеграція: історична ретроспектива та сучасність» 621046-EPP-1-2020-1-UA-EPPJMO-MODULE 9 грудня 2021 р. Сертифікат НВ №2795 3. Участь в онлайн-школі для освітян «НАТО - альянс можливостей» (6 годин), який провела ГО «Інтерньюз-Україна» в рамках проєкту «НАТО - це люди», що фінансується Урядом Сполученого Королівства Великобританії та Північної Ірландії, що діє через Міністерство закордонних справ і у справах Співдружності націй Великої Британії («FCDO») 9-10 грудня 2021 року. 4. Участь у V Всеукраїнської науково-практичної конференції "Нові інформаційні технології управління бізнесом" в об'ємі 8 академічних годин, 16 лютого 2022 р. Свідоцтво № 16022022110 5. Участь у семінарі

							«Girls in ICT 2022», 28.04.2022 р.
414268	Власенко Лідія Олександрівна	Доцент, Основне місце роботи	Факультет інформаційних технологій	Диплом бакалавра, Київська православна богословська академія, рік закінчення: 2022, спеціальність: 041 Богослов'я, Диплом магістра, Національний університет харчових технологій, рік закінчення: 2003, спеціальність: 092502 Комп'ютерно-інтегровані технологічні процеси і виробництва, Диплом кандидата наук ДК 066152, виданий 26.01.2011, Атестат доцента 12ДЦ 037364, виданий 17.01.2014	20	Безпека мережевої та SMART інфраструктури	Освіта: вища Науковий ступінь: кандидат технічних наук Вчене звання: доцент Рівень наукової та професійної активності відповідає пунктам Кадрових вимог 1, 3, 4, 7, 8, 12, 19 1) Публікації, включені до міжнародних наукометричних баз Scopus, Web of Science: 1. Zaiets, N., Vlasenko, L., Lutska, N. (2023). Neural Network Model for Predicting Technological Losses of a Sugar Factory. In: Szewczyk, R., Zieliński, C., Kaliczyńska, M., Bučinskas, V. (eds) Automation 2023: Key Challenges in Automation, Robotics and Measurement Techniques. AUTOMATION 2023. Lecture Notes in Networks and Systems, vol 630. Springer, Cham. (Scopus) https://doi.org/10.1007/978-3-031-25844-2_9 2. Vlasenko, L., Zaiets, N., Lutska, N., Savchuk, O. (2023). Neural Network Model for Predicting the Resource Efficiency of the Defecosaturation Department of a Sugar Factory. In: Vasant, P., Weber, GW., Marmolejo-Saucedo, J.A., Munapo, E., Thomas, J.J. (eds) Intelligent Computing & Optimization. ICO 2022. Lecture Notes in Networks and Systems, vol 569. Springer, Cham. https://doi.org/10.1007/978-3-031-19958-5_12 (Scopus) 3. Vlasenko, L.; Lutska, N.; Zaiets, N.; Korobiichuk, I.; Hrybkov, S. Core Ontology for Describing Production Equipment According to Intelligent Production. Appl. Syst. Innov. 2022, 5 (5), 98. https://doi.org/10.3390/asi5050098 (Web of Science) 4. Effective robust optimal control system for a lamellar pasteurization-cooling unit under the

conditions of intense external perturbations . Nataliia Lutska, Nataliia Zaiets, Lidiia Vlasenko, Volodymyr Shtepa .Ukrainian Food Journal. 2018. Volume 7. Issue 3. Page 511 – 521 (Web of Science)
5. Modern development technologies and investigation of food production technological complex automated systems Korobiichuk, I., Ladanyuk, A,. Zaiets, N., Vlasenko, L. 2018, Pages 52–56. ICMSCE 2018: 2018 2nd International Conference on Mechatronics Systems and Control Engineering, 2018, Amsterdam, Netherlands February, February, 2018 DOI: 10.1145/3185066.3185075 (Scopus)
6. System modeling for construction of the diagnostic subsystem of the integrated automated control system for the technological complex of food industries Zaiets, N., Vlasenko, L., Lutskaya, N., Usenko, S. 2019, Pages 93–98. ICMRE'19: Proceedings of the 5th International Conference on Mechatronics and Robotics Engineering, 2019, Rome, Italy,: February 2019 DOI: 10.1145/3314493.331523 (Scopus)
7. Zaiets, N.A., Savchuk O.V., Shtepa V.M., Lutska N.M., Vlasenko L.O. The synthesis of strategies for the efficient performance of sophisticated technological complexes based on the cognitive simulation modelling. Науковий вісник Національного гірничого університету. – 2021. – №2. – с. 110-117. https://doi.org/10.33271/nvngu/20212/110. (Scopus)

Наукові статті у фахових виданнях:
1. Луцька, Н. М., Байдаєв, Р. В., Герасименко, Т. М., & Власенко, Л. О. (2022). Системи керування технологічними об'єктами харчової промисловості з прогнозувальними

моделями. Наукові праці НУХТ 2022. Том 28, No 3, стор 7-19 DOI: 10.24263/2225-2924-2022-28-3-3
2. Власенко Л.О., Савченко Т.В., Луцька Н.М. Вибір ієрархії та онтології верхнього рівня для розробки інтелектуальних автоматизованих систем управління промисловим підприємством // Наукові праці Національного університету харчових технологій. – 2021. – Т. 27, № 4. – С. 16-27.
3. Луцька Н.М., Власенко Л.О., Ладанюк А.П. Проєктування інтелектуальних автоматизованих систем керування технологічними процесами харчових виробництв засобами SysML. Частина1: огляд діаграм SysML, розробка діаграми вимог // Наукові праці Національного університету харчових технологій. – 2021. – Т. 27, № 3. – С . 15-24.
4. Луцька Н.М., Власенко Л.О., Пупена О.М. Технічні аспекти інтеграції відкритих онтологічних баз знань із сучасними автоматизованими системами управління // Наукові праці Національного університету харчових технологій. – 2021. – Т. 27, № 1. – С . 8-21.
5. Ладанюк А.П. Ефективність інтелектуальних систем керування технологічними об'єктами. Частина 1. Основні положення // А.П. Ладанюк, Н.М. Луцька, Я.В. Смітюх, Л.О. Власенко, М.В. Сашньова / Харчова промисловість, 2019. – №25. – С. 141-147.

3) Підручники, навчальні посібники, монографії 1. Луцька Н.М., Заєць Н.А., Власенко Л.О. Оптимізаційні рішення для автоматизованого управління складними технологічними комплексами: монографія. – Київ: Видавництво Ліра-К, 2022. – 328 с
2. Ладанюк А.П.

							Методологія наукових досліджень: Навч. посіб. / А.П. Ладанюк, Л.О. Власенко, В.Д. Кишенько. – Київ : Видавництво Ліра-К, 2018. – 352 с. 3. Методи сучасної теорії управління: підручник / А.П. Ладанюк, Н.М. Луцька, В.Д. Кишенько, Л.О. Власенко, В.В. Іващук – К.: Видавництво Ліра-К, 2018. – 368 с. 4) Навчально-методичні видання: 1. Програма дисципліни «Безпека мережевої та SMART інфраструктури» призначена для студентів освітнього ступеня «магістр» галузі знань 12 «Інформаційні технології» спеціальності 125 «Кібербезпека», ОП «Безпека систем електронних комунікацій в економіці». – К.: КНТЕУ, 2021. 2. Програма дисципліни «Цифрова криміналістика» призначена для студентів освітнього ступеня «магістр» галузі знань 12 «Інформаційні технології» спеціальності 125 «Кібербезпека», ОП «Безпека систем електронних комунікацій в економіці». – К.: КНТЕУ, 2021. 3. Пашорін В.І., Власенко Л.О., Десятко А.М., Рзаєва С.Л., Савченко Т.В., Сашньова М.В., Самойленко Ю.О., Костюк Ю.В., Чубаєвський В.І., Захаров Р.Г. Методичні рекомендації до виконання випускного кваліфікаційного проекту для студ. ОС «бакалавр», спец. 125 «Кібербезпека». – К.: КНТЕУ, 2021. – 43 с. 4. Пашорін В.І. Костюк Ю.В., Самойленко Ю.О., Власенко Л.О., Савченко Т.В. Методичні рекомендації до виконання курсової роботи студентів з курсу «Безпека інформаційних систем та мереж» для студ.

							ОС «бакалавр», спец. 125 «Кібербезпека». – К.: КНТЕУ, 2021. – 42 с. 5. Браіловський М.М., Костюк Ю.В., Самойленко Ю.О., Власенко Л.О., Савченко Т.В. Методичні рекомендації до виконання курсової роботи студентів з курсу «Організація комп'ютерних мереж» для студ. ОС «бакалавр», спец. 125 «Кібербезпека». – К.: КНТЕУ, 2021. – 72 с. 6. Лукова-Чуйко Н.В., Фесенко А.О., Власенко Л.О., Савченко Т.В., Сашньова М.В., Костюк Ю.В. Криптографічні методи захисту інформації. Робоча програма для студ. ОС «бакалавр», спец. 125 «Кібербезпека». – К.: КНТЕУ, 2021. – 19 с. 7. Самойленко Ю.О., Власенко Л.О., Савченко Т.В., Сашньова М.В., Костюк Ю.В., Безпека програмного забезпечення. Програма для студ. ОС «бакалавр», спец. 125 «Кібербезпека». – К.: КНТЕУ, 2021. – 14 с. 7) Участь в атестації наукових кадрів, як офіційного апонента, або члена постійної спеціалізованої вченої ради: Вчений секретар спеціалізованої вченої ради К 26.058.05 у Національному університеті харчових технологій 2017 – 2021 р.р. 8) Науковий керівник, відповідальний виконавець наукової теми, член редакційної колегії (кат Б) «Моделювання інформаційно-аналітичної системи контролю якості процесу виробництва продукці» (термін 01.2021-12.2024р.р.; державний реєстраційний номер: 0121U109155 дата реєстрації: 03-03-2021р.) 12) Наявність апробаційних та/або науково-популярних, та/або

							консультаційних (дорадчих), та/або науково-експертних публікацій з наукової або професійної тематики: 1. Щербак І.І., Власенко Л.О. Захист комерційної інформації приватного підприємства на основі симетричних алгоритмів шифрування / І.В. Щербак, Л.О. Власенко // Матеріали VIII Міжнародної науково-технічної Internet-конференції «Сучасні методи, інформаційне, програмне та технічне забезпечення систем керування організаційно-технічними та технологічними комплексами», 26 листопада 2021. [Електронний ресурс] – К: НУХТ, 2021 р. – С. 295-296 — Режим доступу: https://drive.google.com/file/d/1F_XOymRYbUgyH5-T49VPYyTCel2YsH2W/view 2. Власенко Л.О., Луцька Н.М., Десятко А.М. Основні види ризиків кіберзагроз промислового суб'єкта господарювання в умовах Industry 4.0 // Збірник тез V Всеукраїнської науково-практичної конференції «Нові інформаційні технології управління бізнесом». – Київ: Спілка автоматизаторів бізнесу, 2022. – С. 38-40. 3. Власенко Л.О., Грибков С.В., Савченко Т.В. Проектування інформаційної системи захисту промислової інформації з урахуванням тенденцій Industry 4.0 // Тези доповідей дев'ятої міжнародної науково-практичної конференції «Управління розвитком технологій». Тема: Інформаційні технології розвитку змісту освіти. – К. : КНУБА, 2022. – С. 61-62. 4. Власенко Л.О.

Моделювання бази даних автомаизованої системи формування документів для вступних випробовувань на основі семантичних підходів / Л.О. Власенко, І.В. Мурга // Наукові праці Третьої міжнар. наук.-практ. конф. «Сучасні тенденції розвитку інформаційних систем і телекомунікаційних технологій», 25–26 січня 2021 р. (Київ, Україна). – К. : НУХТ, 2021. С. 55-57.
5. Lutskaya N., Vlasenko L., Zaiets N., Shtepa V. (2021) Ontological Aspects of Developing Robust Control Systems for Technological Objects. In: Vasant P., Zelinka I., Weber GW. (eds) Intelligent Computing and Optimization. ICO 2020. Advances in Intelligent Systems and Computing, vol 1324. Springer, Cham. https://doi.org/10.1007/978-3-030-68154-8_107

19) Участь у професійних об'єднаннях:
Діяльність за спеціальністю у формі участі у професійних та/або громадських об'єднаннях ГО «Кіберковчег»

Стажування:
1. Інфораційна гігієна. Як розпізнати брехню в соцмережах, в інтернеті та на телебаченні. (45 год., 1,5 кредити ЄКТС)
2. Участь у Всеукраїнському науково-практичному семінарі «Досвід Європейського Союзу у сфері реагування на виклики безпеки» у межах реалізації проєкту Еразмус+ Модулі Жана Моне «Європейська політична інтеграція: історична ретроспектива та сучасність» 621046-EPP-1-2020-1-UA-EPPJMO-MODULE 9 грудня 2021 р. Сертифікат НВ №2795
3. Участь в онлайн-школі для освітян «НАТО - альянс можливостей» (6 годин), який провела ГО «Інтерньюз-Україна» в рамках

							проєкту «НАТО - це люди», що фінансується Урядом Сполученого Королівства Великобританії та Північної Ірландії, що діє через Міністерство закордонних справ і у справах Співдружності націй Великої Британії («FCDO») 9-10 грудня 2021 року. 4. Участь у V Всеукраїнської науково-практичної конференції "Нові інформаційні технології управління бізнесом" в об'ємі 8 академічних годин, 16 лютого 2022 р. Свідоцтво № 16022022110 5. Участь у семінарі «Girls in ICT 2022», 28.04.2022 р.
414678	Гарбуза Тетяна Віталіївна	Завідувач кафедри, Основне місце роботи	Факультет міжнародної торгівлі та права	Диплом спеціаліста, Томський державний педагогічний університет, рік закінчення: 2000, спеціальність: Лінгвістика і міжкультурна комунікація, Диплом магістра, Національний університет державної податкової служби України, рік закінчення: 2008, спеціальність: 060101 Правознавство, Диплом кандидата наук ДК 028888, виданий 30.06.2015, Атестат доцента АД 004076, виданий 26.02.2020	20	Англійська мова інформаційних технологій	Освіта: вища Науковий ступінь: кандидат педагогічних наук Вчене звання: доцент Рівень наукової та професійної активності відповідає пунктам Кадрових вимог 1, 4, 12, 19. 1) Публікації, включені до міжнародних наукометричних баз Scopus, Web of Science: 1. Teaching English Business to Future Economists Using Multimedia Textbook / [O.P. Bykonia, I.V. Borysenko, T.V. Harbuza та ін.]. // International Journal of Higher Education. – 2019. Vol. 8. – Issue №4. – С. 115–123. – Retrieved: http://www.sciedupress.com/journal/index.php/ijhe/article/view/15893/9901 (Scopus) 2. Nozhovnik O., Harbuza T., Starosta H., Radchenko Yu. & Zatserkovnyi O. (2022). Best Practices of Fostering Undergraduates' Cross-Cultural Competence Involving Training Them in Foreign Languages: Systemic Review. International Journal of Educational Methodology, 8 (4), 655-668. (Scopus) 3. Taxonomic Manifestations of the Concept "Man" in

Digital Communication / Teslenko, N., Nezhyva, O., Ivashchenko, V., Harbuza, T. // Lecture Notes in Networks and Systemsthis link is disabled, 2023, 485, P. 805–819. (Scopus)
4. Gender Dimension of the European Union's Communication Ecology Problems in High-Technology Sectors / Oksana, V., Tetiana, H., Natalia, T., Volodymyr, T. // Lecture Notes in Networks and Systemsthis link is disabled, 2023, 495 LNNS, P. 1303–1315. (Scopus)
5. Kyrychok A., Harbuza, T., Teslenko N., Okhrimenko O., Zalizniuk V. Training civil servants in promoting the reputation of the country in the settings of crisis communication. Teaching Public Administration, 2023. (Scopus)

Наукові статті у фахових виданнях:
1. Гарбуза Т. Застосування моделі Blended Learning під час викладання курсу "Іноземна мова за професійним спрямуванням" / Тетяна Гарбуза. // Молодь і ринок. – 2018. – №12 (167). – С. 68–71.
2. Гарбуза Т. Поняття професійної підготовки вчителя іноземної мови за дистанційною формою навчання (на прикладі Великої Британії) / Тетяна Гарбуза. // Науковий часопис Національного педагогічного університету імені М.П. Драгоманова. Серія № 15. Науково-педагогічні проблеми фізичної культури (фізична культура і спорт). – 2018. – №11. – С. 26–30.
3. Гарбуза Т. Тьютор як суб'єкт освітнього процесу в системі дистанційного навчання / Тетяна Гарбуза. // Молодь і ринок. – 2019. – №1 (168). – С. 71–74.
4. Гарбуза Т. Формування іншомовної

							комунікативної компетенції у студентів немовних спеціальностей / Тетяна Гарбуза. // Інноваційна Педагогіка. – 2019. – №9. – С. 77–80. 5. Гарбуза Т.В., Тесленко Н.О. Інноваційний розвиток вищої освіти в умовах трансформаційних змін українського суспільства Науковий журнал «Педагогічні науки: теорія та практика». – Запоріжжя: Запорізький національний університет, 2021. – № 2. – С. 217-223. (Index Copernicus (Польща), Norwegian Register for Scientific Journals, Series and Publishers (Норвегія)) 6. Durdas, A., Harbuza, T., Radchenko, Y., Starosta, H., & Kostenko, O. (2022). DEVELOPMENT OF CREATIVITY OF FUTURE SPECIALISTS AT FOREIGN LANGUAGE CLASSES: CONDITIONS AND OPPORTUNITIES. SUBJECTIVE WELL-BEING. Continuing Professional Education: Theory and Practice, (2), 52–59. https://doi.org/10.28925/1609-8595.2022.2.6 7. Durdas, A., Harbuza, T., Radchenko, Y., Ternova, O., & Poidyn, M. (2022). DEVELOPMENT OF STUDENTS' CREATIVITY AT FOREIGN LANGUAGE CLASSES: SCIENTIFIC DISCOURSE. Continuing Professional Education: Theory and Practice, (1), 82–88. https://doi.org/10.28925/1609-8595.2022.1.9 8. Durdas, A., Harbuza, T., Radchenko, Y., & Starosta, H. (2022). TEACHING FOREIGN LANGUAGES EFFICIENTLY: THE ROLE OF CREATIVE WRITING. Continuing Professional Education: Theory and Practice, (3), 33–38. https://doi.org/10.28925/1609-8595.2022.3.4 9. Durdas A.P., Harbuza T.V., Borshchovetska V.D., Radchenko Yu.P., Starosla H.A. (2023). Higher education

							quality assurance: recent trends. Continuing Professional Education: Theory and Practice, 75 (2). 25-32. DOI: https://doi.org/10.28925/1609-8595.2023.2.3 4) Навчально-методичні видання: 1. Програма дисципліни «Іноземна мова за професійним спрямуванням (англійська мова)» призначена для студентів денної форми навчання галузі знань 07 Управління та адміністрування, за спеціальністю 072 Фінанси, банківська справа та страхування, спеціалізація «Корпоративні фінанси». К. : ДТЕУ, 2023. 2. Робоча програма дисципліни «Іноземна мова за професійним спрямуванням (англійська мова)» призначена для студентів денної форми навчання галузі знань 07 Управління та адміністрування, за спеціальністю 072 Фінанси, банківська справа та страхування, спеціалізація «Корпоративні фінанси». К. : ДТЕУ, 2023. 3. Програма дисципліни «Англійська мова в міжнародних стандартах фінансової звітності» призначена для здобувачів освітнього ступеня «магістр» галузі знань 07 «Управління та адміністрування», спеціальності 071 «Облік і оподаткування», освітньо-професійних програм «Облік і податковий консалтинг», «Облік і оподаткування в міжнародному бізнесі». К. : ДТЕУ, 2023. Програма навчальної дисципліни «Іноземна мова за професійним спрямуванням» для студентів ОС «бакалавр» спеціалізацій «Міжнародні відносини та економічна дипломатія». К. : КНТЕУ, 2022.

							4. Робоча програма навчальної дисципліни «Іноземна мова за професійним спрямуванням» для студентів ОС «бакалавр» спеціалізацій «Міжнародні відносини та економічна дипломатія». К. : КНТЕУ, 2022. 5. Програма навчальної дисципліни «Іноземна мова за професійним спрямуванням» для студентів ОС «бакалавр» спеціалізацій «Банківська справа» та «Фінансове посередництво». К. : КНТЕУ, 2021. 6. Робоча програма навчальної дисципліни «Іноземна мова за професійним спрямуванням» для студентів ОС «бакалавр» спеціалізацій «Банківська справа» та «Фінансове посередництво». К. : КНТЕУ, 2021. 7. Іноземна мова за професійним спрямуванням (англійська): збірник граматичних вправ. К.: Київ. нац. торг.-екон. ун-т, 2018. 8. Іноземна мова за професійним спрямуванням (англійська): збірник текстів та завдань для самостійної роботи студентів К.: Київ. нац. торг.-екон. ун-т, 2018. 12) Наявність апробаційних та/або науково-популярних, та/або консультаційних (дорадчих), та/або науково-експертних публікацій з наукової або професійної тематики: 1. Гарбуза Т.В. Перспективи використання змішаного навчання іноземних мов у підготовці майбутніх економістів / Тетяна Гарбуза // Педагогічна компаративістика і міжнародна освіта – 2018: трансформації та інновації в освіті у глобалізаційному світі: матеріали II Міжнародної наук.-практ. конференції (Київ, 7- 8 червня

2018 р.). – Київ-Дрогобич: ТзОВ «Трек-ЛТД», 2018. – С. 150–151.
2. Гарбуза Т. В. Змішане навчання професійного іншомовного спілкування студентів немовних спеціальностей / Тетяна Гарбуза // Вища освіта: удосконалення якості підготовки фахівців: збірник тез II Міжнародної наукової Інтернет конференції, (м. Київ, 26–27 квітня 2018 р.). – Київ: Альфа-ПІК, 2018. – С. 165–168.
3. Гарбуза Т.В. Іншомовна професійна комунікативна компетенція майбутніх юристів / Тетяна Гарбуза // Глобальні імперативи розвитку бізнесу та права [Текст] : тези доп. Міжнар. наук.-практ. конф. (Київ, 15-16 листоп. 2018 р.). - Київ: КНТЕУ, 2018. – С. 327-330.
4. Міжкультурні аспекти навчання іноземних мов у закладах вищої освіти / Тетяна Гарбуза // Стратегії міжкультурної комунікації в мовній освіті сучасних університетів: зб. матеріалів Міжнар. наук.-практ. конф., м. Київ (11– 12 квітня 2019 р.). – К.: КНЕУ, 2019. – С. 18–20.
5. Гарбуза Т. В. Використання технології «case study» під час занять з іноземної мови / Тетяна Гарбуза // Пріоритети розвитку педагогічних та психологічних наук у XXI столітті: Збірник наукових робіт учасників міжнародної науково-практичної конференції (20–21 березня 2020 р., м. Одеса). – Одеса: ГО «Південна фундація педагогіки», 2020. – С. 117-119.
6. Гарбуза Т. В. Використання хмарних технологій під час навчання іншомовного спілкування у закладах вищої освіти / Тетяна Гарбуза // Актуальні проблеми

іншомовної комунікації: лінгвістичні, методичні та соціально-психологічні аспекти: зб. Матеріалів III Всеукраїнської науково-методичної Інтернет-конференції, 26 березня 2020 року, Луцьк / Луцький національний технічний університет – Луцьк: ІВВ Луцького НТУ, 2020. – С. 14-15.

7. Гарбуза Т. В. Професійний саморозвиток викладача іноземної мови в немовному університеті / Тетяна Гарбуза // Актуальні питання сучасних педагогічних та психологічних наук: Збірник наукових робіт учасників міжнародної науково-практичної конференції (19–20 лютого 2021 р., м. Одеса). – Одеса: ГО «Південна фундація педагогіки», 2021. – С. 68-71.

8. Гарбуза Т. В. Хмарні технології як засіб навчання іншомовного спілкування / Тетяна Гарбуза // Формування іншомовної комунікативної компетентності у майбутніх фахівців немовних закладів вищої освіти: проблеми та перспективи: збірник тез Міжвузівської науково-практичної Інтернет-конференції (Ірпінь, 4 березня 2021р.) – Ірпінь: УДФСУ, 2021. – С. 19-22.

9. Гарбуза Т. В. Професійний саморозвиток викладача іноземної мови в немовному університеті / Тетяна Гарбуза // Використання дистанційних освітніх технологій у викладанні іноземних мов: тези доп. Міжвуз. наук.-метод. семінару (Київ, 15 лютого 2022р.). – Київ: Держ. торг.-екон. ун-т, 2022. – С. 30-32.

10. Дурдас А.П., Гарбуза Т.В. Розвиток креативності студентів на заняттях з іноземної мови за

								використанням спеціальних прийомів та соціальних мереж / Алла Дурдас, Тетяна Гарбуза // Психологічні проблеми творчості: матеріали XXII Міжнародної науково-практичної конференції, 23 липня 2022 року. Київ: Інститут психології імені Г.С. Костюка НАПН України, 2022. – С. 88-91. 11. Дурдас А., Гарбуза Т. Creative writing in learning and teaching a foreign language / Алла Дурдас, Тетяна Гарбуза // Розвиток професійної майстерності педагога в умовах нової соціокультурної реальності: збірник матеріалів V Міжнародної науково-практичної конференції (м. Тернопіль, Україна, 29-30 вересня 2022 року). – Тернопіль: СМП "Тайп", 2022. – С. 117-120. 12. Гарбуза Т.В. Використання інтерактивних технологій та методів під час викладання дисципліни «Іноземна мова». Сімдесят треті економіко-правові дискусії. Серія: Соціальні та гуманітарні науки: матеріали Міжнародної мультидисциплінарної наукової інтернет-конференції (м. Львів, Україна – м. Переворськ, Польща, 22-23 березня 2023 р.). ГО "Наукова спільнота"; WSSG w Przeworsku. – Львів : ФО-П Шпак В.Б., 2022. С. 104-109. 13. Гарбуза Т.В., Дурдас А.П. Питання якості вищої освіти у європейському вимірі. Ways of science development in modern crisis conditions: матеріали IV Міжнародної науково-практичної інтернет конференції (м. Дніпро, Україна, 8-9 червня 2023 р.). 2023. 19) Участь у професійних об'єднаннях: Член Міжнародної асоціації викладачів англійської мови як іноземної в Україні

							(IATEFL) Стажування: 1. Міжнародна програма наукового стажування у Празькому інституті підвищення кваліфікації 20-27 листопада 2016 р. (Чеська Республіка, Прага), 108 год. Сертифікат № 112016014. 2. II Міжнародна програма підвищення кваліфікації керівників закладів освіти і науки, а також педагогічних та науково-педагогічних працівників «Разом із Визначними Лідерами Сучасності: Цінності, Досвід, Знання, Компетентності і Технології для Формування Успішної Особистості та Трансформації Оточуючого Світу», 12.08.2021 – 12.10.2021, онлайн, 180 год., 6 кредитів ECTS, виданий 12.10.2021. сертифікат № 2099
414552	Ситніченко Олена Михайлівна	Доцент, Основне місце роботи	Факультет міжнародної торгівлі та права	Диплом спеціаліста, Київський національний університет внутрішніх справ, рік закінчення: 2006, спеціальність: Правознавство, Диплом магістра, Національна академія внутрішніх справ, рік закінчення: 2011, спеціальність: Правознавство, Диплом кандидата наук ДК 016542, виданий 10.10.2013, Атестат доцента АД 012214, виданий 20.02.2023	8	Правове забезпечення інформаційної безпеки в економічних системах	Освіта: вища Науковий ступінь: кандидат юридичних наук, Вчене звання: доцент Рівень наукової та професійної активності відповідає пунктам Кадрових вимог 1, 3, 4, 7, 12, 20. 1) Публікації, включені до міжнародних наукометричних баз Scopus, Web of Science: 1. H.Bukanov, S.Skakovska, V.Kulbaka, O.Sytnichenko, O.Kulbaka. Training and implementation of the environmental, economic, and legal development policy of the regions: main practice-oriented approaches // Cuestions politicas. Instituto de Estudios Políticos y Derecho Público "Dr. Humberto J. La Roche"de la Facultad de Ciencias Jurídicas y Políticas de la Universidad del Zulia Maracaibo, Venezuela- 2020 –c.200-214. DOI: https://doi.org/10.46398/cuestpol.382e.15 (Web of Science)

											Наукові статті у фахових виданнях (8 публікацій): 1. Ситніченко О.М., Курзова В.В. Щодо питання адміністративно-правового статусу Мінприроди України у сфері забезпечення екологічної складової частити системи біобезпеки України // Право і суспільсто. – 2018. №2. – С. 135 – 144. 2. Ситніченко О.М. Актуальні питання правової охорони атмосферного повітря від забруднюючих речовин у відпрацьованих газах транспортних засобів. Юридичний вісник повітряне і космічне право. – 2018. №4. – С.32-38. 3. Петлюк.Ю.С., Ситніченко О.М. Праова категорія «Екологічна безпека»: наукоі підходи до інтерпретації. Юридичний вісник повітряне і космічне право. – 2019-№4. (Index Copernicus International, Scientific Indexing Services (SIS)-С.9-13. 4. Ситніченко О.М, Петлюк Ю.С. Правова охорона атмосферного повітря від забруднюючих речовин у контексті євроінтеграційних процесів України. «NATIONAL LAW JOURNAL:THEORY AND PRATICE» L.L.C. – 2020. №4 (44). – С. 129-134. 5. Ситніченко О.М. Окремі аспекти нормативно-правового регулювання забезпечення інформаційної безпеки // Вчені записки Таврійського національного університету імені В.І. Вернадського. Серія: Юридичні науки. – Том 32(71). №1 2021. – С.86-90. 6. Sitnichenko O.M. Information Security System of Ukraine: Theoretical and Legal Analysis // European Reforms Bulletin, scientific peer-reviewed journal No. 2№2.-2021.-С.92-96. 7.Мушенок В.В., Ситніченко О.М. Юридична

							відповідальність за економічні правопорушення // Право і суспільство. 2023. – №2. Т.2 – С. 167-173. 8.Бондаренко Н., Ситніченко О. Організаційно-правове забезпечення інформаційної безпеки підприємств. Зовнішня торгівля: економіка, фінанси, право. – 2023. № 2. С. 76-87. Серія. Юридичні науки. 3) Підручники, навчальні посібники, монографії 1. V.Myshenok, O.Sitnichenko. Environmental taxation: the eu paradigm and its implementation into Ukrainian legislation/Strategies, models and technologies of economic systems management in hthe context of international economik integration.- Riga: Institute of Economics of the Latvian Academy of Sciences, 2020-P.401-409. 4) Навчально-методичні видання: 1. Програма та робоча програма з дисципліни «Кримінальне право» за освітнім ступенем «бакалавр» КНТЕУ, за галуззю знань 08 «Право», спеціальністю 081 «Право» 293 «Міжнародне право», спеціалізації «Правове забезпечення безпеки підприємницької діяльності», «Комерційне право», «Фінансове право», «Цивільне право і процес». – К.: КНТЕУ, 2018. – 140 с. 2. Програма та робоча програма навчальної дисципліни «Правове забезпечення інформаційної безпеки» для здобувачів вищої освіти ОС «магістр», галуззь знань 12 «Інформаційні технології», спеціальність 122 «Комп'ютерні науки» – К.: КНТЕУ, 2020. – 24 с. 3. Програма навчальної дисципліни «Правове забезпечення

								інформаційної безпеки» для здобувачів вищої освіти ОС «бакалавр», галуззь знань 12 «Інформаційні технології», спеціальність 125 «Кібербезпека», спеціалізації «Безпека інформаційних і комунікаційних систем в економіці» – К.: КНТЕУ, 2020. – 24 с. 4. Програма та робоча програма навчальної дисципліни «Правове забезпечення інформаційної безпеки в економічних системах» для здобувачів вищої освіти другого (магістерського) рівня зі спеціальності 125 «Кібербезпека» ОП «Безпека систем електронних комунікацій в економіці» – К.: КНТЕУ, 2021. – 28 с. 7) Участь в атестації наукових кадрів, як офіційного апонента, або члена постійної спеціалізованої вченої ради: Офіційний опонент в спеціалізованій вченій раді Д 26.142.02 на захисті дисертації Голубицький С.Г. за спеціальністю 12.00.07 «Адміністративне право і процес, фінансове право, інформаційне право», 2019 р. 12) Наявність апробаційних та/або науково-популярних, та/або консультаційних (дорадчих), та/або науково-експертних публікацій з наукової або професійної тематики: 1. Ситніченко О.М., Мушенок В.В. Tax control as an element of tax relationships // II Міжнародна науково-практична конференція «Глобальні імперативи розвитку бізнесу та права» 10-11 жовтня 2019 року, – К.: КНТЕУ, 2019 р. – С.209-211. 2. Шведова Г.Л. Ситніченко О.М. Економічна безпека України як об'єкт кримінально-правової

											охорони // II Міжнародна науково-практична конференція «Глобалізаційні виклики розвитку національних економік» 19 – 20 жовтня 2021 року. – К.: КНТЕУ, 2021. – С.158-161. 3. Мушенок В.В., Ситніченко О.М. Право платника податків на податкову амністію. // XII International Scientific Conference «HUMAN RIGHTS IN DIGITAL TRANSFORMATIONS ERA» Том І від 25 лютого 2022 року, м.Київ- 2022 р. – С.96-99. 4. Bondarenko N., Sytnichenko O. Organizacijno-pravove zabezpechennja informacijnoi' bezpeky pidpryjemstv. Zovnishnja torgivlja: ekonomika, finansy, pravo. – 2023. – No2. S. 76-87. Serija. Jurydychni nauky. https://doi.org/10.31617/3.2023(127)05 5. О.М. Ситніченко. Характеристика юридичної відповідальності деяких видів (груп) правопорушень у сфері економічної діяльності // Матеріали всеукраїнського науково-педагогічного підвищення кваліфікації, «Сучасні аспекти та актуальні підходи в навчанні, викладанні й дослідженні державно-правових дисциплін» 27 лютого – 9 квітня – Одеса: Видавничий дім «Гельветика». – 2023. – С.159-164. 20) Досвід практичної роботи за спеціальністю не менше п'яти років (крім педагогічної, науково-педагогічної, наукової діяльності). Служба в ОВС з 2004 року по 2014 рік. Стажування: 1. Центральноукраїнський державний університет імені Володимира Вінніченка, Центр українсько-європейського наукового співробітництва

							«Сучасні аспекти та актуальні підходи в навчанні, викладанні й дослідженні державно-правових дисциплін» Сертифікат про підвищення кваліфікації № ADV-270255-LSI від 09.04.2023, 27.02.2023-09.04.2023, 180 годин – 6 кредитів ЄКТС. 2. Програма закордонного стажування та підвищення професійних навичок в Університеті Ясар, факультет бізнесу та відділу логістичного управління (м. Ізмір, Туреччина); з 1 квітня по 30 червня 2022 року про що видано Certificate of completion 01/2022.
414237	Котенко Наталія Олексіївна	Доцент, Основне місце роботи	Факультет інформаційних технологій	Диплом спеціаліста, Вінницький національний технічний університет, рік закінчення: 2015, спеціальність: Комп'ютерні системи та мережі, Диплом спеціаліста, Вінницький державний педагогічний університет імені Михайла Коцюбинського, рік закінчення: 2005, спеціальність: 010103 Педагогіка і методика середньої освіти. Математика, Диплом магістра, Вінницький державний педагогічний університет імені Михайла Коцюбинського, рік закінчення: 2006, спеціальність: 010103 Педагогіка і методика середньої освіти. Математика, Диплом кандидата наук ДК 013042, виданий	6	Технології безпеки Web-ресурсів	Освіта: вища Науковий ступінь: кандидат педагогічних наук Вчене звання: доцент Рівень наукової та професійної активності відповідає пунктам Кадрових вимог 1, 4, 8, 9, 12, 19 1) Публікації, включені до міжнародних наукометричних баз Scopus, Web of Science: 1. Zhyrova, T., Kotenko, N., Bebeshko, B., Khorolska, K., Shevchenko, S. Benchmarking between the DQL Index and the Web Application Accessibility Index using Automatic Test Tools. CEUR Workshop Proceedings this link is disabled, 2022, 3288, pp. 110 – 116 (Scopus). 2. Adilia Batorshyna, Volodymyr Tokar, Serhii Chekhovych, Andrii Homotiuk Nataliia Kotenkoc The Impact of Awareness Stimulating Activities and Events on Global Islamic Finance Assets: Enhancing Financial Risk Management and Economic Security in Non-Muslim Countries. CEUR Workshop Proceedingsthis link is disabled, 2021, 3187, pp. 13–26. 3. Bebeshko, B. Khorolska, K. Kotenko, N. Desiatko, A. Sauanova, K. Sagyndykova, S.

				25.04.2013, Атестат доцента АД 009720, виданий 01.02.2022			Tyshchenko, D. 3D modelling by means of artificial intelligence. Journal of Theoretical and Applied Information Technologythis link is disabled, 2021, 99(6), pp. 1296–1308 (Scopus) 4. Bebeshko, B., Khorolska, K., Kotenko, N., Kharchenko, O., Zhyrova, T. Use of neural networks for predicting cyberattacks. CEUR Workshop Proceedingsthis link is disabled, 2021, 2923, pp. 213–223 (Scopus) 5. Lakhno, V. Malyukov, V. Kasatkin, D. Blozva, A. Zhyrova, T. Kotenko, N. Kotova, M. Model for Supporting Decisions of Investors, Taking into Consideration Multifactoriality and Turnover. Communications in Computer and Information Sciencethis link is disabled, 2021, 1388 CCIS, pp. 525-535 (Scopus) Наукові статті у фахових виданнях: 1. Т. Жирова, Н. Котенко, В. Токар, К. Хорольська, Б. Бебешко Testing the accessibility of web-applications / INTERNATIONAL SCIENTIFIC JOURNAL: Computer Systems and Information Technologies, № 3 (2021), ст. 89-95 ISSN 2710-0766DOI 10.31891/CSIT http://csitjournal.khmnu.edu.ua/index.php/csit/article/view/89 DOI: https://doi.org/10.31891/CSIT-2021-5-12. 2. Kryvoruchko O., Bebeshko B., Khorolska K., Desiatko A., Kotenko N. Artificial intelligence face recognition for authentication Kryvoruchko O., Bebeshko B., Khorolska K., Desiatko A., Kotenko N. Artificial intelligence face recognition for authentication. Technical sciences and technologies: scientific journal / Chernihiv National University of Technology. – Chernihiv : Chernihiv National University of Technology, 2020. – №

2 (20). – 324 р. С.139-149.
3. Н. Котенко, Т. Жирова, М. Кулеба, «Дослідження особливостей тестування мобільних додатків», Управління розвитком складних систем, вип. 41, 2020, с. 55-60.
4. Н. О. Котенко, Т. О. Жирова, А. М. Десятко, К. В. Хорольська, Б. Т. Бебешко, К. О. Тогжанова UX-дизайн інформаційної системи підприємства торгівлі. Вісник КрНУ імені Михайла Остроградського. Випуск 3/2020 (122) http://visnikkrnu.kdu.edu.ua/statti/2020_3_2020-3-67.pdf
5. Котенко Н.О., Жирова Т.О., Чубаєвський В.І., Десятко А.М. Дослідження основних тенденцій сучасної розробки вебсайтів // Кібербезпека: освіта, наука, технікаN° 1 (5), 2019. – С. 6 -15.
6. Цюцюра М.І., Криворучко О.В., Жирова Т.О., Котенко Н.О. Сучасні технології тестування та захисту веб-сторінок. // Управління розвитком складних систем. Випуск №39, 2019. - С. 100-10
7. Жирова Т.О., Котенко Н.О., Цюцюра М.І. Альтернативне середовище програмування мовою C# для навчальних закладів. Управління розвитком складних систем: Зб. наук. праць.: – К.: КНУБА, 2017. – Вип. 31. – № 31. – Стор. 153-158.

4) Навчально-методичні видання:
1. Котенко Н.О., Жирова Т.О., Савченко Т.В. Збірник тестових завдань з дисципліни «Інформаційні технології у професійній діяльності» для студентів освітнього ступеня «бакалавр» спеціальності 121 «Інженерія програмного забезпечення» та 125 «Кібербезпека». – К.: ДТЕУ, 2022.

2. Робоча програма Інформаційні технології в професійній діяльності для спеціальності 121 Інженерія програмного забезпечення / Т.О. Жирова, Н.О. Котенко, М.А. Костюк. – К.: КНТЕУ, 2021.
3. Програма «Автоматизація тестування програмного забезпечення» для спеціальності 121 «Інженерія програмного забезпечення» ОС «магістр» / Т.О. Жирова, Н.О. Котенко, Т.Б. Бебешко. – К.: КНТЕУ, 2021.
4. Програма та робоча програма «Методи обробки відеоінформації» для спеціальності 121 «Інженерія програмного забезпечення» ОС «магістр» / Т.О. Жирова, Н.О. Котенко, Гнатченко Д.Д.. – К.: КНТЕУ, 2019.
5. Програма «Технологія розробки та тестування програмного забезпечення» для спеціальності 121 «Інженерія програмного забезпечення» ОС «бакалавр» / Т.О. Жирова, Н.О. Котенко, Т.В. Бебешко – К.: КНТЕУ, 2020.
6. Робоча програма «Технології розробки та тестування програмного забезпечення» для спеціальності 122 «Комп'ютерні науки» ОС «бакалавр» / Т.О. Жирова, Н.О. Котенко, – К.: КНТЕУ, 2021.
7. Котенко Н.О., Жирова Т.О., Хорольська К.В., Бебешко Б.Т. «Web-дизайн та Web-програмування». Програма для студентів освітнього ступеня «бакалавр». – К.: КНТЕУ, 2021.
8. Котенко Н.О., Жирова Т.О. Збірник тестових завдань з дисципліни «Web-дизайн та Web-програмування». – К.: КНТЕУ, 2019.
9. Котенко Н.О.,

							Жирова Т.О., Савченко Т.В. Інформаційні технології у професійній діяльності програма для студентів освітнього ступеня «бакалавр» спеціальності 121 «Інженерія програмного забезпечення». – К.: КНТЕУ, 2020. 8) Відповідальний виконавець наукової теми: 1. Відповідальний виконавець наукової теми: «Розпізнавання графічних образів методом клітинних автоматів». 2. Відповідальний виконавець наукової теми: «Проектування інформаційних технологій освітнього середовища». 3. Відповідальний виконавець наукової теми: «Удосконалення методики викладання дисциплін спеціальності 125 «Кібербезпека» для освітнього ступеню «бакалавр». 9) Робота експерта: Участь у роботі семи експертних комісіях Національного агентства із забезпечення якості вищої освіти 12) Наукове консультування підприємств (3 роки), публікації професійної тематики (5 одиниць): 1. Жирова Т.О., Котенко Н.О. Європейський досвід тестування банківських систем за допомогою штучного інтелекту // Збірник тез VI Всеукраїнської науково-практичної конференції «Нові інформаційні технології управління бізнесом». – Київ: Спілка автоматизаторів бізнесу, 2023. – 166 с., С. 48-50. 2. Жирова Т.О., Котенко Н.О. Вимоги до програмного забезпечення в умовах інклюзивного навчання // Тези доповідей дев'ятої міжнародної науково-практичної конференції

«Управління розвитком технологій». Тема: Інформаційні технології розвитку змісту освіти. – К. : КНУБА, 2022. – 87 с., С. 65-66.
3. Жирова Т.О. Котенко Н.О. Формування soft skills у студентів технічних спеціальностей під час вивчення фахових дисциплін // Збірник тез IV Всеукраїнської науково-практичної конференції «Нові інформаційні технології управління бізнесом». – Київ: Спілка автоматизаторів бізнесу, 2021. – 532 с., С. 145-148.
4. Жирова Т.О, Котенко Н.О., Чудік М.І. Застосування фракталів у game dev // Матеріали IV Міжнародної науково-практичної конференції «Інформаційна безпека та комп'ютерні технології»: тези доповідей, 15–16 квітня 2021 р. – Кропивницький: ЦНТУ, 2021. – 81 с., С. 15-16.
5. Жирова Т.О. Котенко Н.О. Організація анонімних опитувань студентів. // Збірник матеріалів III Всеукраїнської конференції «Теоретико-практичні проблеми використання математичних методів та комп'ютерно-орієнтованих технологій в освіті та науці» с. 53-54.
6. Жирова Т.О. Котенко Н.О. Особливості тестування безпеки інтернет-банкінгу. // Проблеми кібербезпеки інформаційно-телекомунікаційних систем: Збірник матеріалів доповодідей та тез; м. Київ, 15-16 квітня 2021 року; Київський національний університет імені Тараса Шевченка / Редкол.: О.К. Закусило. (голова) та ін. –К.:ВПЦ «Київський університет» 2021 – 191 с. – С. 50-52.

7. Жирова Т.О., Котенко Н.О., Дакова Л.В. Дослідження фреймворків для розробки мобільних додатків. //Комплексне забезпечення якості технологічних процесів та систем (КЗЯТПС – 2021) : матеріали тез доповідей XI Міжнародної науково-практичної конференції (м. Чернігів, 26–27 травня 2021 р.) : у 2 т. / Національний університет «Чернігівська політехніка» [та ін.] ; відп. за вип.: Єрошенко Андрій Михайлович [та ін.]. – Чернігів : НУ «Чернігівська політехніка», 2021. – Т. 2. – 236 с. – С. 171-172.
8. Жирова Т.О., Котенко Н.О. Дослідження інструментальних засобів тестування безпеки мобільних додатків. 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. / Національний університет «Чернігівська політехніка» [та ін.]; відп. за вип.: Єрошенко Андрій Михайлович [та ін.]. – Чернігів : ЧНТУ, 2020. – Т. 1. – 272 с. С. 180-182.
9. Жирова Т.О., Котенко Н.О. Особливості автоматизації тестування безпеки Web-додатків. Перспективні напрямки захисту інформації: матеріали шостої всеукраїнської наук.-пр. Конф. - м. Одеса, 02 – 06 вересня 2020 р. - Одеса: Бондаренко М.О., 2020 – 120с. С. 27-30.

19) Участі у професійних об'єднаннях:
ГО «Кіберковчег» Асоційований член ГО "Наукова асоціація кібербезпеки

								України". Стажування: 1. Стажування "Teacher's Internship Program" від експертів EPAM та IT Ukraine Association, July - August 2021. Сертифікат в обсязі 108 академічних годин 2. Науково-практичний курс серії вебінарів компанії Linkos Group ТОВ «M.E.Doc» «Інформаційні технології в економіці: інноваційні рішення захисту даних підприємства» в обсязі 180 академічних годин. Сертифікат від 26.05.2021. 3. English For IT: Starter від 06.09.2021 року (32 год) 4. Сертифікат, що підтверджує рівень B2 (English) від 02.04.2021р. 5. Міжнародне стажування "Programming, Software Testing, Cloud Technologies in the Economics, Security of Information Systems in the Economics, IT Project Management and Artificial Intelligence" (180 годин) 12 April 2021-12 July 2021, Sofia, Bulgaria. 6. Участь у науково-практичній інтернет конференції «Mathematics and Informatics in Higher Education: Challenges of Modernity». Сертифікат в обсязі 24 години. May 20-21, 2021. 7. Підвищення кваліфікації експерта Національного агентства із забезпечення якості вищої освіти. Тренінг для керівників експертних груп обсягом 30 годин (1 кредит ЄКТС). Реєстраційний № 0090/2021(165) від 27 квітня 2021 року. 8. «Принципи гнучкої роботи. Agile для викладачів», GlobalLogic Education, 2020, (50 год.). 9. «Початок та практика роботи у MicrosoftTeams» LizardSoft (18 годин) від 6.19.2020. 10. Teachers Internship

							Program, EPAM Systems, January-February 2018, Kyiv, Ukraine. (108 год.) 11. «Використання хмарних сервісів Microsoft в освітньому просторі» (150 год.), 9 листопада 2018. 12. EPAM training center, Teachers Internship Program, Introduction to Project Management, Introduction to Front End, травень 2018, EPAM Systems, Kyiv office, Ukraine. (36 год.) 13. «Word та Excel: інструменти і лайфхаки» платформа масових відкритих онлайн-курсів Prometheus (36 годин) від 22.10.2019. 14. EdEra «Основи веб-розробки (HTML, CSS, JavaScript)» (30 год.) від 05.04.2020 15. «Критичне мислення для освітян» платформа масових відкритих онлайн-курсів Prometheus (30 годин) від 22.04.2020.
414197	Савченко Тетяна Віталіївна	Доцент, Основне місце роботи	Факультет інформаційних технологій	Диплом спеціаліста, Український державний університет харчових технологій, рік закінчення: 1997, спеціальність: Автоматизація технологічних процесів і виробництв, Диплом спеціаліста, Інститут дистанційного навчання Національного педагогічного університету імені М.П. Драгоманова, рік закінчення: 2007, спеціальність: Психологія, Диплом кандидата наук ДК 015282, виданий 03.07.2002, Атестат доцента 12ДЦ 019765, виданий 03.07.2008	25	Технології безпеки безпроводових та мобільних мереж	Освіта: вища Науковий ступінь: кандидат технічних наук Вчене звання: доцент Рівень наукової та професійної активності відповідає пунктам Кадрових вимог 1, 4, 9, 12, 19. 1) Публікації, включені до міжнародних наукометричних баз Scopus, Web of Science: 1. Improving the quality of the technological process of packaging shape formation based on the information structure of an automated system. Eastern-European Journal of Enterprise Technologies – №3/2 (105)2020. – С. 28-36 (Scopus). 2. Identification of the mathematical models of the technological objects for robust control systems. Radio Electronics, Computer Science, Control. —– Zaporizhzhia National Technical University, 2019. – № 3. – С. 163-172 (Web of Science). Наукові статті у фахових виданнях:

1. Підвищення метрологічної надійності цифрових засобів вимірювальної техніки при використанні фізичного діагностування. Автори: Глухов С.І., Бабій О.С., Семеха С.М., Савченко Т.В., Гальоса А.О. – Харків: Харківський національний університет Повітряних сил імені Івана Кожедуба, «Системи озброєння і військова техніка». – 2022, №1(69). – С.88-95.
2. Implementation of Procedure for the Identification of Dynamic Systems Based on Neural Networks. Olena Kryvoruchko, Yuliia Kostiuk, Tetyana Savchenko, Dmytro Hnatchenko. SECS-2022: International Conference «Challenges and Reality of the IT-space: Software Engineering and Cybersecurity» – Kyiv, Ukraine, October 25-26, 2022.
3. Власенко Л.О., Савченко Т. В., Луцька Н.М. Вибір ієрархії та онтології верхнього рівня для розробки інтелектуальних автоматизованих систем управління промисловим підприємством. // Наукові праці НУХТ. – К.: НУХТ, 2021. – Том 27 №4. – С. 16 – 27.

4) Навчально-методичні видання:
1. Функціональне та логічне програмування. Опорний конспект лекцій для студентів освітнього ступеня «магістр» спеціальності 121 «Інженерія програмного забезпечення». — К.: КНТЕУ, 2020. — 137 с.
2. Технології безпеки безпроводових та мобільних мереж. Програма для студентів освітнього ступеня «магістр» спеціальності 125 «Кібербезпека» – К.: КНТЕУ, 2021. – 15 с.
3. Цифрова криміналістика. Програма для студентів освітнього

							ступеня «магістр» спеціальності 125 «Кібербезпека» – К.: КНТЕУ, 2021. – 16 с. 4. Безпека інформаційних систем та мереж. Програма для студентів освітнього ступеня «бакалавр» спеціальності 125 «Кібербезпека». — К.: КНТЕУ, 2021. — 22 с. 5. Безпека мережевої та SMART інфраструктури. Програма для студентів освітнього ступеня «магістр» спеціальності 125 «Кібербезпека». — К.: КНТЕУ, 2022. — 21 с. 6. Збірник тестових завдань «Безпека програмного забезпечення» для здобувачів першого (бакалаврського) рівня вищої освіти галузі знань 12 «Інформаційні технології» спеціальностей 121 «Інженерія програмного забезпечення» та 125 «Кібербезпека». – К.: КНТЕУ, 2022. – 42 с. 7. Методичні рекомендації до виконання курсових робіт з дисципліни «Організація комп'ютерних мереж» для здобувачів першого (бакалаврського) рівня вищої освіти галузі знань 12 «Інформаційні технології» спеціальностей 121 «Інженерія програмного забезпечення» та 125 «Кібербезпека». – К.: КНТЕУ, 2022. – 70 с. 8. Методичні рекомендації до виконання курсових робіт з дисципліни Безпека інформаційних систем та мереж для здобувачів першого (бакалаврського) рівня вищої освіти галузі знань 12 «Інформаційні технології» спеціальності 125 «Кібербезпека». – К.: КНТЕУ, 2022. – 42 с. 9) Робота експерта: Експерт Національного агентства із забезпечення якості вищої освіти для

							проведення акредитацій освітніх програм (спеціальності: 121 «Інженерія програмного забезпечення», 125 «Кібербезпека», 151 «Автоматизація та комп'ютерно-інтегровані технології»), з 2020 р. 12) Наявність апробаційних та/або науково-популярних, та/або консультаційних (дорадчих), та/або науково-експертних публікацій з наукової або професійної тематики: 1. Проектування інформаційної системи захисту промислової інформації з урахуванням тенденції Industry 4.0. Тези доповідей дев'ятої міжнародної науково-практичної конференції «Управління розвитком технологій». Тема: Інформаційні технології розвитку змісту освіти. – К.: КНУБА, 2022. – 87 с. – С. 61-62. 2. Криптографічні механізми інфраструктури відкритих ключів. Комплексне забезпечення якості технологічних процесів та систем (КЗЯТПС – 2021): матеріали тез доповідей XI Міжнародної науково-практичної конференції (м. Чернігів, 26–27 травня 2021 р.): у 2 т. / Національний університет «Чернігівська політехніка» [та ін.]. – Чернігів : НУ «Чернігівська політехніка», 2021. – Т. 2. – 236 с. С. 191-192. 3. Моделювання оцінки ризику інформаційної безпеки підприємства. Збірник матеріалів доповідей та тез IV Міжнародної науково-практичної конференції «Проблеми кібербезпеки інформаційно-телекомунікаційних систем (PCSITS)», 15-16 квітня 2021 р. —

Київ: Київський національний університет імені Тараса Шевченка, 2021. — 190 с. — С. 129-130.
4. Таксономія атак та механізмів безпеки в мережі. Матеріали наукових семінарів «Кібергігієна. Кібербезпека. Безпека держави», 27 листопада 2020 р. — Київ: КНТЕУ, 2020. — 101 с. — С. 18-20.
5. Methodical approach to evaluate the younger specialists competence level in the specialization of «topo-geodesic and navigation support of troops (forces)» in the training center. Математичне та імітаційне моделювання систем. МОДС 2020 : тези доповідей П'ятнадцятої міжнародної науково-практичної конференції (29 червня – 01 липня 2020 р., м. Чернігів) / М-во освіти і науки України; Нац. Акад. наук України; Академія технологічних наук України; Інженерна академія України та ін. – Чернігів: ЧНТУ, 2020. – 370 с. — С. 291-295.
6. Аналіз сучасних технологій квантової криптографії. Збірник тез І Міжнародної практичної конференції «Безпека ресурсів інформаційних систем», 16-17 квітня 2020 року. — Чернігів: НУЧП, 2020. С. 160-164.

19) Участь у професійних об'єднаннях:
Співпраця з Мережною Академією CISCO та виконання функцій інструктора.
Співпраця з Організацією з безпеки та співробітництва в Європі (ОБСЄ) та Українською школою урядування (УШУ).

Стажування:
Курси підвищення кваліфікації у Державному університеті телекомунікацій за темою: «Системи технічного захисту

							інформації» (120 годин), 23.11-04.12.2020. IT Ukraine Association Teacher's Internship program held by EPAM Systems, period June-August 2020 (108 hours). CISCO: Introduction Cybersecurity (09.06.2020); Cybersecurity Essentials (23.09.2020); CCNA Cybersecurity Operations (03.10.2020); CCNA Security (28.10.2020); CCNAv7: Introduction to Networks (15.02.2021). Учасниця проєкту «Посилення спроможностей українських державних органів у сфері кібергігієни та кібербезпеки», реалізованого Координатором проєктів OSCE Project Co-ordinator in Ukraine та Українською школою урядування за фінансової підтримки Міністерства закордонних справ і у справах Співдружності націй Великої Британії та Федерального міністерства закордонних справ Німеччини. Підвищення кваліфікації за спеціальною професійною (сертифікатною) програмою «Тренінг для тренерів з питань кібергігієни» (60 год.), 2021-2022 рр.
414858	Чубаєвський Віталій Іванович	Доцент, Основне місце роботи	Факультет інформаційних технологій	Диплом магістра, Львівський регіональний інститут державного управління Національної академії державного управління при Президентові України, рік закінчення: 2010, спеціальність: 1501 Державне управління, Диплом магістра, Національна академія внутрішніх справ України, рік закінчення:	5	Етичний хакінг	Освіта: вища Науковий ступінь: доктор економічних наук Вчене звання: доцент Рівень наукової та професійної активності відповідає пунктам Кадрових вимог 1, 3, 4, 5, 12, 16, 20. 1) Публікації, включені до міжнародних наукометричних баз Scopus, Web of Science: 1. Lakhno V., Kasatkin D., Desiatko A., Chubaievskyi V., Tsuitsuira S., Tsuitsuira M. Indicators Systematization of Unauthorized Access to Corporate Information

				2003, спеціальність: Правознавство, Диплом доктора наук ДД 013039, виданий 20.06.2023, Диплом кандидата наук ДК 039715, виданий 13.12.2016, Атестат доцента АД 003059, виданий 15.10.2019			// Rajakumar G., Du K. L., Vuppalapati C., Beligiannis G. N. (eds) Intelligent Communication Technologies and Virtual Mobile Networks : Lecture Notes on Data Engineering and Communications Technologies. Singapore : Springer, 2023. Vol. 131. P. 569–580.) 2. Lakhno V., Mazaraki A., Kasatkin D., Kryvoruchko O., Khorolska K., Chubaievskyi V. Models and Algorithms for Optimization of the Backup Equipment for the Intelligent Automated Control System Smart City // Inventive Communication and Computational Technologies. Lecture Notes in Networks and Systems : Proceedings of ICICCT 2022 / Editors: G. Ranganathan, Xavier Fernando, Álvaro Rocha. Singapore : Springer, 2022. Vol. 383. P. 749–762. 3. Lakhno V., Kozlovskyi V., Klobukov V., Chubaievskyi V., Tyshchenko D. Software Package for Information Leakage Threats Relevance Assessment // Lecture Notes in Networks and Systemsthis : Computer Science On-line Conference / Conference Paper. 2022. Vol. 503. P. 290–301. 4. Lakhno V., Malyukov V., Kryvoruchko O., Chubaievskyi V., Misiura M., Pashorin V. Methodology for placing components of a video surveillance system for smart city based on a composite cost optimization model // Lecture Notes in Networks and Systemsthis : Computer Science On-line Conference / Conference Paper. Springer, Cham, 2022. Vol. 501. P. 13–23. 5. Chubaievskyi V., Blakyta H., Matusova O., Adamenko V., Hamula I. Assessing the state of the corporate information area in Ukraine // Міждисциплінарні дослідження складних

систем = Interdisciplinary Studies of Complex Systems : Збірник наукових праць. Київ : Вид-во НПУ імені М. П. Драгоманова, 2022. № 20. С. 35–45.
6. Chubaievskyi V., Blakyta H., Bogma O., Shtuler I., Batrakova T. Protection of information resources as an integral part of economic security of the enterprise // Naukovyi Visnyk Natsionalnoho Hirnychoho Universytetuthis. 2022. № 4. P. 117–122.
7. Lakhno V., Akhmetov B., Mohylnyi H., Chubaievskyi V., Kryvoruchko O., Desiatko A. Multi-criterial optimization composition of cyber security circuits based on genetic algorithm // Journal of Theoretical and Applied Information Technologythis. 2022. Vol. 100. № 7. P. 1996–2006.
8. Lakhno V., Bereke M., Adilzhanova S., Chubaievskyi V., Desiatko A., Palaguta K. Genetic algorithm for solving the problem of scaling a cloud-oriented object of informatization // Journal of Theoretical and Applied Information Technologythis link is disabled. 2022. Vol. 100. № 6. P. 1693–1705.
9. Lakhno V., Blozva A., Kasatkin D., Chubaievskyi V., Tyshchenko D., Brzhanov R. Experimental studies of the features of using waf to protect internal services in the zero trust structure // Journal of Theoretical and Applied Information Technologythis. 2022. Vol. 100. № 3. P. 705–721.
10. Akhmetov B., Lakhno V., Chubaievskyi V., Kaminskyi S., Adilzhanova S., Ydyryshbayeva M. Automation of Information Security Risk Assessment // International Journal of Electronics and Telecommunicationsthis. 2022. Vol. 3. № 68.

P. 549–555.
11. Lakhno V., Akhmetov B., Mazaraki A., Chubaievskyi V., Desiatko A. Methodology for assessing the effectiveness of measures aimed at ensuring information security of the object of informatization // Journal of Theoretical and Applied Information Technologythis. 2021. Vol. 14. № 99. P. 3417–3427.
12. Sahun A., Khaidurov V., Lakhno V., Opirskyy I., Chubaievskyi V., Kryvoruchko O., Desiatko A. Devising a Method for improving crypto resistance of the symmetric block cryptosystem Rc5 using nonlinear shift functions // Eastern-European Journal of Enterprise Technologies. 2021. Vol. 5. № 9. P. 17–29.
13. .Lakhno V., Akhmetov B., Chubaievskyi V., Desiatko A., Palaguta K., Blozva A., Chasnovskyi Y. Information security audit method based on the use of a neuro-fuzzy system // Proceedings of the 5th Computational Methods in Systems and Software 2021. Springer, Cham, 2021. P. 171–184. (Scopus).
14. Lakhno, V., Malyukov, V., Kasatkin, D., Chubaieskyi, V., Rzaieva, S., & Rzaiev, D. (2023). Continuous investing in advanced fuzzy technologies for smart city doi:10.1007/978-981-19-3391-2_24 Retrieved from www.scopus.com

Наукові статті у фахових виданнях:
1. Чубаєвський В. Світова практика управління подіями інформаційної безпеки корпорацій // Зовнішня торгівля: економіка, фінанси, право. 2022. № 6. С. 73–82.
2. Чубаєвський В.І. Методичний підхід до оцінки економічної ефективності системи захисту корпоративної інформації // Електронний журнал

«Ефективна економіка». 2022. № 11. – URL: https://nayka.com.ua/index.php/ee/article/view/730/738.
3. Чубаєвський В.І. Прогресивність розвитку системи захисту корпоративної інформації // Економіка та суспільство. 2022. № 44. – URL: https://economyandsociety.in.ua/index.php/journal/article/view/1793.
4. Чубаєвський В. Корпоративний інформаційний простір: сутність та еволюція // Scientia Fructuosa (Вісник Київського національного торговельно-економічного університету). 2022. № 4. С. 84–97.
5. Чубаєвський В.І. Особливості формування системи захисту інформаційних ресурсів корпоративних структур // Фаховий електронний науково-практичний журнал «Проблеми сучасних трансформацій. Серія: економіка та управління». 2022. № 5. – URL: https://reicst.com.ua/pmt/article/view/2022-5-04-10/2022-5-04-10.
6. Чубаєвський В.І. Методи управління корпоративною інформаційною безпекою. Економіка та суспільство. 2022. № 43. – URL: https://economyandsociety.in.ua/index.php/journal/article/view/1732.
7. Chubaievskyi V., Tereshchenko E., Andryeyeva V., Stoianenko I. Model for assessing technological resources in the economic security of business in the process of European integration // Information-analytical journal «Economics. Finances. Law». 2022. № 8. P. 13–16 (Index Copernicus).
8. Чубаєвський В., Десятко А., Криворучко О., Лахно В., Блозва А., Місюра М. Застосування СППР у завданнях організаційно-

економічного забезпечення захисту інформації // Інформаційні технології та суспільство. – 2022. № 2(4). – С. 107–116.
9. Чубаєвський В.І., Жук Т.В. Економічна ефективність інформаційної безпеки підприємств торгівлі // Scientia Fructuosa (Вісник Київського національного торговельно-економічного університету). – 2022. № 1. – С. 106–117.
10. Чубаєвський В.І., Богма О.С., Сілакова Г.В. Методика оцінки ефективності систем захисту корпоративної інформації вітчизняних підприємств // Економічний простір. – 2022. № 177. – С. 56–61.
11. Чубаєвський В. Стратегічні орієнтири формування корпоративної політики інформаційної безпеки // Причорноморські економічні студії. – 2021. Вип. 72. (Ч. 2). – С. 24–30.
12. Чубаєвський В., Лахно В., Ахметов Б., Криворучко О., Касаткін Д., Десятко А., Литовченко Т. Оптимізації резерву обладнання для інтелектуальних автоматизованих систем // Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка». – 2021. Т. 2. № 14. – С. 87–99.
13. Чубаєвський В., Лахно В., Криворучко О., Касаткін Д., Десятко А., Блозва А., Гусєв Б. Методика мінімізації витрат на побудову багатоконтурної системи захисту на основі генетичного алгоритму // Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка». – 2021. Т. 1. № 13. – С. 16–28.
14. Чубаєвський В., Лахно В., Криворучко О., Касаткін Д., Десятко А., Блозва А. Ефективність методики розрахунку

показників інвестицій в системи інформаційної безпеки об'єктів інформатизації // Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка». – 2021. Т. 4. № 12. – С. 96–107.
15. Чубаєвський В., Волосович С. Безпека корпоративної інформації в екосистемі FinTech // Foreign trade: Economics, Finance, Law. – 2021. Т. 119. № 6. – С. 98–108.

3) Підручники, навчальні посібники, монографії:
1. Чубаєвський В. І. Корпоративна інформаційна безпека : монографія / В.І. Чубаєвський. – Київ : Держ. торг.-екон. ун-т, 2022. – 272 с.
2. Чубаєвський В.І та ін.. Протидія злочинам у сфері використання інформаційних технологій: інтегр. навч.-практ. посіб. / В.І. Чубаєвський, М.В. Карчевський, В.В. Коваленко, В.Є. Комлєв, О.Ю. Мартиш, В.В. Невгад, О.О. Токарєв, Р.А. Усманов, М.О. Яковлєв та ін.; за ред. М.В. Карчевського. – Харків : Право, 2019. – 188 с.

4) Навчально-методичні видання:
1. Програма дисципліни «Етичний хакінг» призначена для студентів освітнього ступеня «магістр» галузі знань 12 «Інформаційні технології» спеціальності 125 «Кібербезпека», спеціалізації «Безпека систем електронних комунікацій в економіці». – К.: ДТЕУ, 2022.
2. Програма дисципліни «Технології проектування інформаційних систем», для студентів освітнього ступеню «магістр» галузь знань: 12 «Інформаційні технології» спеціальність: 121 «Інженерія програмного

забезпечення»/ авт. О.В. Криворучко, С.В. Цюцюра, В.І. Чубаєвський, А.М. Десятко – 2018. – 8 с.
3. Програма та Робоча програма дисципліни «Об'єктно-орієнтоване програмування», для студентів освітнього ступеню «бакалавр» галузь знань: 12 «Інформаційні технології» спеціальність: 121 «Інженерія програмного забезпечення»/ О.В. Криворучко, М.І. Цюцюра, В.І. Чубаєвський, А.М. Десятко – 2018. – 42 с.
4. Робоча програма «Безпека інформаційних систем і мереж», для студентів освітнього ступеня «бакалавр», галузь знань: 12 «Інформаційні технології», спеціальність: 121 «Інженерія програмного забезпечення»/ В.І. Пашорін, В.І., Чубаєвський В.І. – К: КНТЕУ, 2018. – 28с.
5. Методичні рекомендації до виконання випускної кваліфікаційної роботи для студентів освітнього ступеня «бакалавр», галузь знань: 12 «Інформаційні технології» спеціальність 121 «Інженерія програмного забезпечення» / О.А. Харченко, О.В. Криворучко, В.І. Чубаєвський, С.В. Цюцюра, С.Л. Рзаєва, В.Я Рассамакін. – К: КНТЕУ, 2018 – 38с
6. Програма дисципліни «Економічна інформатика», для студентів освітнього ступеню «бакалавр» галузь знань: 12 «Інформаційні технології» спеціальність: 125 «Кібербезпека»/ авт. В.І. Чубаєвський, Т.О. Жирова, К.О. Котенко. – 2019. – 8 с.
7. Програма дисципліни «Організація комп'ютерних мереж», для студентів освітнього ступеню «бакалавр» галузь знань: 12

«Інформаційні технології» спеціальностей: 121 «Інженерія програмного забезпечення», 125 «Кібербезпека»/ авт. В.І. Чубаєвський, Я.І. Шестак. – 2018. – 8 с.

5) Захист дисертації на здобуття наукового ступеня:
1. Захист дисертації на здобуття наукового ступеня доктора економічних наук, спеціальності 08.00.04 – Економіка та управління підриємствами (за видами економічної діяльності). Тема дисертації: «Економічна ефективність систем захисту корпоративної інформації». Диплом – ДД № 013039 від 20.06.2023р.

12) Наявність апробаційних та/або науково-популярних, та/або консультаційних (дорадчих), та/або науково-експертних публікацій з наукової або професійної тематики:
1. Чубаєвський В.І. Особливості оцінки економічної ефективності інвестування в об'єкти інформаційної безпеки корпорацій // Сучасні проблеми економіки та бізнесу : матеріали XII Міжнародної науково-практичної конференції (Київ, 10–11 листопада 2022 р.). – Київ : НАУ, 2022. – С. 220–222.
2. Чубаєвський В.І. Реалізація методичного підходу до оцінки економічної ефективності системи захисту корпоративної інформації // Сучасні тренди соціально-економічних перетворень та інтелектуалізації суспільства в умовах сталого розвитку : тези доповідей Міжнародної науково-практичної конференції (10 листопада, м. Запоріжжя). Запоріжжя НУ «Запорізька політехніка», 2022. – С. 372–374.
3. Chubaievskyi V.

Directions of assessment of technological resources of economic security of business in the process of European Integration // Стратегічні орієнтири розвитку економіки, фінансів, обліку і права збірник тез доповідей міжнародної науково-практичної конференції (Полтава, 30 липня 2022 р.). – Полтава : ЦФЕНД, 2022. – С. 17–19.
4. Чубаєвський В.І., Франчук Т.М. Проблеми захисту персональних даних в електронно-інформаційному середовищі // Кібергігієна. Кібербезпека. Безпека держави : матеріали наукових семінарів (м. Київ, 27 листопада 2020 р.) / відп. ред. А. М. Десятко. – Київ : Київ. нац. торг.-екон. ун-т, 2020. – С. 34–36.
5. Чубаєвський В.І., Терешенко Е.Ю. Особливості моніторингу оцінки інформаційної безпеки України // Інформаційно-аналітичне забезпечення управління фінансово-економічною безпекою держави, регіону, суб'єктів господарювання в умовах COVID-19 : матеріали X Міжнар. наук.-практ. конф., Харків, 18-19 листопада 2021 року / Харків. нац. ун-т міськ. госп-ва ім. О.М. Бекетова. Харків : ХНУМГ ім. О.М. Бекетова, 2021. – С. 294–297.
6. Чубаєвський В., Криворучко О., Десятко А. Оцінка якості програмного забезпечення інформаційно-управляючих систем // Глобалізаційні виклики розвитку національних економік : тези доповідей II Міжнар. наук.-практ. конф. (Київ, 19 жовтня 2021 р.) / відп. ред. А. А. Мазаракі. Київ : Київ. нац. торг.-екон. ун-т, 2021. – С. 278–281.
7. Лахно В., Ахметов Б., Чубаєвський В., Криворучко О., Десятко А., Пашорін

							В. Оцінювання ефективності заходів щодо забезпечення інформаційної безпеки об'єкта інформатизації // Глобальні та регіональні проблеми інформатизації в суспільстві і природокористуванні 2021 : збірник матеріалів IX Міжнар. наук.-практ. інтернет конф., м. Київ, 13-14 трав. 2021 р. – Київ : НУБіП України, 2021. – С. 45-48. 8. Чубаєвський В., Макоєдова В. Застосування багаторівневого підходу як засіб протидії кіберзагрозам // Проблеми кібербезпеки інформаційно-телекомунікаційних систем : Збірник матеріалів доповідей та тез; м. Київ, 15-16 квітня 2021 року; Київський національний університет імені Тараса Шевченка / Редкол.: О.К. Закусило. (голова) та ін. Київ : ВПЦ «Київський університет», 2021. – С. 18-19. 16) Наявність статусу учасника бойових дій Учасник бойових дій (посвідчення серії МВ № 031819), перебував у зоні проведення АТО (Донецька область м. Дебальцеве). 20) Досвід практичної роботи за спеціальністю не менше п'яти років (крім педагогічної, науково-педагогічної, наукової діяльності). 25 років, робота з 1998 р. по 2023 р. на різних посадах у підрозділах МВС України, зокрема: - оперуповноважений відділу по боротьбі зі злочинністю в бюджетній сфері при УДСБЕЗ УМВС України Рівненській області; - начальник Рівненського МВ УМВС України в Рівненській області; - начальник відділу кримінальної міліції у справах дітей УМВС України в Рівненській області;

								- оперуповноважений сектору Державної служби боротьби з економічною злочинністю Здолбунівського РВ УМВС України в Рівненській області; - заступник начальника відділу захисту прав інтелектуальної власності ДДСБЕЗ МВС України; - начальник відділу аналітичного забезпечення УБК МВС України; - заступник начальника Департаменту кіберполіції Національної поліції України; - заступник начальника Департаменту інформаційно-аналітичної підтримки Національної поліції України; - начальник управління організаційної роботи Департаменту інформаційно-аналітичної підтримки Національної поліції України; - директор Директорату стратегічного планування та європейської інтеграції МВС України; - начальник Управління ліцензування МВС України. Стажування: 1. Professional developer at European universities of Slovak republic "International internship of the scientific research organization and innovation technologies implementation in education process" (120 hours or 4 credits ECTS) – 2019, April. 2 CERTIFICATE № 103-17 , Level (B2), Taras Shevchenko National Universiti of Kyiv, Foreign Language Center, ENGLISH FOR PROFESSIONAL PURPOSES, 2017.

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
23. Обґрунтовувати вибір програмного забезпечення, устат-кування та інструментів, інженерних технологій і процесів, а також обмежень щодо них в галузі інформаційної безпеки та/або кібербезпеки на основі сучасних знань у суміжних галузях, наукової, технічної та довідкової літератури та іншої доступної інформації.	☒	Технології безпеки Web-ресурсів	Під час проведення лекцій використовуються наступні методи. Словесний метод – для чіткого пояснення матеріалу. Інтерактивний метод – для активної участі аудиторії, забезпечення контакту зі студентами. Відеометод у поєднанні з інформаційними технологіями дистанційного навчання – для зручності та наочності матеріалу. Пояснювально-ілюстративний метод – для логічної послідовності та наочної демонстрації матеріалу. Під час практичних занять використовуються такі методи. Практичний метод – через проведення колоквіумів та дискусій для глибшого розуміння тем. Словесний метод – для додаткового пояснення і обговорення матеріалу. Усний, письмовий контроль та тестування – через опитування, комп'ютерні тести та творчі завдання, спрямовані на закріплення навичок використання вивченого теоретичного матеріалу та методів розв'язання завдань.	Протягом семестру результати навчання студентів оцінюються за результатами поточного і підсумкового контролю: поточний контроль – опитування, колоквіуми, тестування; підсумковий контроль – екзамен.
		Англійська мова інформаційних технологій	Під час проведення лекційних та практичних занять використовуються різні підходи з метою підсилення зрозумілості пояснення та підвищення зацікавленості учасників навчального процесу до теоретичного матеріалу. Зокрема, словесний метод спілкування, інтерактивний підхід, що залучає аудиторію до активної участі. Додатково, використовується відеометод у поєднанні з сучасними інформаційними технологіями та засобами навчання, такими як дистанційні, мультимедійні та веб-орієнтовані засоби. Це дозволяє створити більш глибоке та наочне розуміння матеріалу завдяки візуальному контенту та використанню комп'ютерних інструментів. Засвоєння матеріалу підкріплюється наочним	При поточному контролі проводяться опитування та тестування студентів та контрольні роботи, також використовуються методи самоконтролю і самооцінювання. Формою підсумкового контролю є екзамен.

			методом, використовується ілюстративний підхід, який допомагає наочно продемонструвати матеріал.	
		Безпека мережевої та SMART інфраструктури	Проведення тематичних і проблемних лекцій характеризується поєднанням традиційних та нетрадиційних методів викладання з використанням інноваційних технологій дистанційної, мультимедійної та веб-орієнтованої. Практичні роботи направлені на поглиблене засвоєння студентами теоретичного матеріалу, отримання практичних навичок при виконанні тренінгових завдань та комп'ютерного тестування. Метод роботи з навчально-методичною літературою забезпечує поглиблення здобувачів освіти з тем навчальної дисципліни та закладає основи майбутньої науково-дослідної роботи.	Проведення поточного контролю передбачає проведення опитувань, тестувань, задач з використанням усного, письмового, тестового методів, перевірки індивідуальних завдань. Методи самоконтролю і самооцінки дозволяють студентам проводити контроль своїх знань особисто. Форма підсумкового контролю – екзамен.
		Цифрова криміналістика	Лекційні та лабораторні роботи проводяться в поєднанні традиційних і нетрадиційних методів викладання з використанням інноваційних технологій: лекції (тематичні, проблемні); лабораторні заняття. Методи, які використовуються: словесний, практичний, наочний, робота з навчально-методичною літературою, відеометод із залученням дистанційних, мультимедійних та веб-орієнтованих технологій; метод проектів.	Навчання студентів оцінюється на основі результатів поточного контролю у формі усного та письмового опитування, контрольних робіт; підсумкового контролю – екзамену.
21. Використовувати методи натурного, фізичного і комп'ютерного моделювання для дослідження процесів, які стосуються інформаційної безпеки та/або кібербезпеки.	☒	Цифрова криміналістика	Лекційні та лабораторні роботи проводяться в поєднанні традиційних і нетрадиційних методів викладання з використанням інноваційних технологій: лекції (тематичні, проблемні); лабораторні заняття. Методи, які використовуються: словесний, практичний, наочний, робота з навчально-методичною літературою, відеометод із залученням дистанційних, мультимедійних та веб-орієнтованих технологій; метод проектів.	Навчання студентів оцінюється на основі результатів поточного контролю у формі усного та письмового опитування, контрольних робіт; підсумкового контролю – екзамену.
		Безпека мережевої та SMART інфраструктури	Проведення тематичних і проблемних лекцій характеризується поєднанням традиційних та нетрадиційних методів викладання з використанням інноваційних технологій дистанційної,	Проведення поточного контролю передбачає проведення опитувань, тестувань, задач з використанням усного, письмового, тестового методів, перевірки індивідуальних завдань. Методи самоконтролю і

			мультимедійної та веб-орієнтованої. Практичні роботи направлені на поглиблене засвоєння студентами теоретичного матеріалу, отримання практичних навичок при виконанні тренінгових завдань та комп'ютерного тестування. Метод роботи з навчально-методичною літературою забезпечує поглиблення здобувачів освіти з тем навчальної дисципліни та закладає основи майбутньої науково-дослідної роботи.	самооцінки дозволяють студентам проводити контроль своїх знань особисто. Форма підсумкового контролю – екзамен.
20. Ставити та вирішувати складні інженерно-прикладні та наукові задачі інформаційної безпеки та/або кібербезпеки з урахуванням вимог вітчизняних та світових стандартів та кращих практик.	☒	Цифрова криміналістика	Лекційні та лабораторні роботи проводяться в поєднанні традиційних і нетрадиційних методів викладання з використанням інноваційних технологій: лекції (тематичні, проблемні); лабораторні заняття. Методи, які використовуються: словесний, практичний, наочний, робота з навчально-методичною літературою, відеометод із залученням дистанційних, мультимедійних та веб-орієнтованих технологій; метод проектів.	Навчання студентів оцінюється на основі результатів поточного контролю у формі усного та письмового опитування, контрольних робіт; підсумкового контролю – екзамену.
		Безпека мережевої та SMART інфраструктури	Проведення тематичних і проблемних лекцій характеризується поєднанням традиційних та нетрадиційних методів викладання з використанням інноваційних технологій дистанційної, мультимедійної та веб-орієнтованої. Практичні роботи направлені на поглиблене засвоєння студентами теоретичного матеріалу, отримання практичних навичок при виконанні тренінгових завдань та комп'ютерного тестування. Метод роботи з навчально-методичною літературою забезпечує поглиблення здобувачів освіти з тем навчальної дисципліни та закладає основи майбутньої науково-дослідної роботи.	Проведення поточного контролю передбачає проведення опитувань, тестувань, задач з використанням усного, письмового, тестового методів, перевірки індивідуальних завдань. Методи самоконтролю і самооцінки дозволяють студентам проводити контроль своїх знань особисто. Форма підсумкового контролю – екзамен.
		Етичний хакінг	Вивчення дисципліни проводиться шляхом лекційних та практичних занять словесними, практичними, наочними методами, відеометодами у сполучені з новітніми інформаційними технологіями та комп'ютерними засобами навчання, що забезпечують закріплення теоретичних знань, сприяють засвоєнню практичних навичок.	Під час навчання проходить поточний контроль у вигляді комп'ютерного тестування, опитування, перевірки індивідуальних завдань. В кінці вивчення дисципліни проводиться підсумковий контроль у формі екзамену.
		Технології безпеки	Під час лекцій та	Поточний контроль знань

		безпроводових та мобільних мереж	практичних занять використовуються різноманітні методи для зрозумілого пояснення матеріалу та активізації участі здобувачів освіти в навчальному процесі. Активно використовуються інформаційні технології для дистанційного навчання. Всі лекції викладаються за допомогою пояснювально-ілюстративного методу, що дозволяє наочно демонструвати матеріал послідовно і логічно. Аудиторна робота передбачає використання практичного підходу (практичні заняття), репродуктивних методів та методів навчання для закріплення практичних навичок вивченого теоретичного матеріалу та методів вирішення поставлених завдань. Виконання індивідуальних завдань з використанням персональних комп'ютерів та контрольних робіт базується на застосуванні пізнавального методу для всебічного освітлення тем.	студентів проводиться на практичних заняттях у вигляді контрольних робіт, опитувань; Підсумковим контролем знань студентів з навчальної дисципліни є екзамен.
19. Обирати, аналізувати і розробляти придатні типові аналітичні, розрахункові та експериментальні методи кіберзахисту, розробляти, реалізовувати та супроводжувати проекти з захисту інформації у кіберпросторі, інноваційної діяльності та захисту інтелектуальної власності.	☒	Технології безпеки Web-ресурсів	Під час проведення лекцій використовуються наступні методи. Словесний метод – для чіткого пояснення матеріалу. Інтерактивний метод – для активної участі аудиторії, забезпечення контакту зі студентами. Відеометод у поєднанні з інформаційними технологіями дистанційного навчання – для зручності та наочності матеріалу. Пояснювально-ілюстративний метод – для логічної послідовності та наочної демонстрації матеріалу. Під час практичних занять використовуються такі методи. Практичний метод – через проведення колоквіумів та дискусій для глибшого розуміння тем. Словесний метод – для додаткового пояснення і обговорення матеріалу. Усний, письмовий контроль та тестування – через опитування, комп'ютерні тести та творчі завдання, спрямовані на закріплення навичок використання вивченого теоретичного матеріалу та методів розв'язання завдань.	Протягом семестру результати навчання студентів оцінюються за результатами поточного і підсумкового контролю: поточний контроль – опитування, колоквіуми, тестування; підсумковий контроль – екзамен.
18. Планувати навчання, а також супроводжувати та контролювати роботу з персоналом у напряму інформаційної безпеки та/або	☒	Етичний хакінг	Вивчення дисципліни проводиться шляхом лекційних та практичних занять словесними, практичними, наочними методами, відеометодами у сполучені з новітніми інформаційними технологіями та	Під час навчання проходить поточний контроль у вигляді комп'ютерного тестування, опитування, перевірки індивідуальних завдань. В кінці вивчення дисципліни проводиться підсумковий контроль у

кібербезпеки.			комп'ютерними засобами навчання, що забезпечують закріплення теоретичних знань, сприяють засвоєнню практичних навичок.	формі екзамену.
17. Мати навички автономного і самостійного навчання у сфері інформаційної безпеки та/або кібербезпеки і дотичних галузей знань, аналізувати власні освітні потреби та об'єктивно оцінювати результати навчання.	☒	Англійська мова інформаційних технологій	Під час проведення лекційних та практичних занять використовуються різні підходи з метою підсилення зрозумілості пояснення та підвищення зацікавленості учасників навчального процесу до теоретичного матеріалу. Зокрема, словесний метод спілкування, інтерактивний підхід, що залучає аудиторію до активної участі. Додатково, використовується відеометод у поєднанні з сучасними інформаційними технологіями та засобами навчання, такими як дистанційні, мультимедійні та веб-орієнтовані засоби. Це дозволяє створити більш глибоке та наочне розуміння матеріалу завдяки візуальному контенту та використанню комп'ютерних інструментів. Засвоєння матеріалу підкріплюється наочним методом, використовується ілюстративний підхід, який допомагає наочно продемонструвати матеріал.	При поточному контролі проводяться опитування та тестування студентів та контрольні роботи, також використовуються методи самоконтролю і самооцінювання. Формою підсумкового контролю є екзамен.
		Технології безпеки безпроводових та мобільних мереж	Під час лекцій та практичних занять використовуються різноманітні методи для зрозумілого пояснення матеріалу та активізації участі здобувачів освіти в навчальному процесі. Активно використовуються інформаційні технології для дистанційного навчання. Всі лекції викладаються за допомогою пояснювально-ілюстративного методу, що дозволяє наочно демонструвати матеріал послідовно і логічно. Аудиторна робота передбачає використання практичного підходу (практичні заняття), репродуктивних методів та методів навчання для закріплення практичних навичок вивченого теоретичного матеріалу та методів вирішення поставлених завдань. Виконання індивідуальних завдань з використанням персональних комп'ютерів та контрольних робіт базується на застосуванні пізнавального методу для всебічного освітлення тем.	Поточний контроль знань студентів проводиться на практичних заняттях у вигляді контрольних робіт, опитувань; Підсумковим контролем знань студентів з навчальної дисципліни є екзамен.
		Безпека мережевої та SMART інфраструктури	Проведення тематичних і проблемних лекцій характеризується поєднанням традиційних та нетрадиційних методів	Проведення поточного контролю передбачає проведення опитувань, тестувань, задач з використанням усного,

	викладання з використанням інноваційних технологій дистанційної, мультимедійної та веб-орієнтованої. Практичні роботи направлені на поглиблене засвоєння студентами теоретичного матеріалу, отримання практичних навичок при виконанні тренінгових завдань та комп'ютерного тестування. Метод роботи з навчально-методичною літературою забезпечує поглиблення здобувачів освіти з тем навчальної дисципліни та закладає основи майбутньої науково-дослідної роботи.	письмового, тестового методів, перевірки індивідуальних завдань. Методи самоконтролю і самооцінки дозволяють студентам проводити контроль своїх знань особисто. Форма підсумкового контролю – екзамен.
Етичний хакінг	Вивчення дисципліни проводиться шляхом лекційних та практичних занять словесними, практичними, наочними методами, відеометодами у сполучені з новітніми інформаційними технологіями та комп'ютерними засобами навчання, що забезпечують закріплення теоретичних знань, сприяють засвоєнню практичних навичок.	Під час навчання проходить поточний контроль у вигляді комп'ютерного тестування, опитування, перевірки індивідуальних завдань. В кінці вивчення дисципліни проводиться підсумковий контроль у формі екзамену.
Цифрова криміналістика	Лекційні та лабораторні роботи проводяться в поєднанні традиційних і нетрадиційних методів викладання з використанням інноваційних технологій: лекції (тематичні, проблемні); лабораторні заняття. Методи, які використовуються: словесний, практичний, наочний, робота з навчально-методичною літературою, відеометод із залученням дистанційних, мультимедійних та веб-орієнтованих технологій; метод проектів.	Навчання студентів оцінюється на основі результатів поточного контролю у формі усного та письмового опитування, контрольних робіт; підсумкового контролю – екзамену.
Правове забезпечення інформаційної безпеки в економічних системах	Під час лекцій використовуються: словесний метод; інтерактивний метод для більшого залучення аудиторії до навчального процесу, організації контакту із студентами; відеометод у сполученні із застосуванням інформаційних технологій дистанційного навчання, також лекції викладаються із застосуванням пояснювально-ілюстративного методу для наочної демонстрації матеріалу в логічній послідовності. Під час практичних занять використовуються практичний і словесний методи - проводяться колоквіуми і дискусії для	Протягом семестру результати навчання студентів оцінюються за результатами поточного і підсумкового контролю: – поточний контроль: опитування, колоквіуми, тестування; – підсумковий контроль: екзамен.

			більш глибшого розуміння тем та формування світоглядних думок студентів. Методи усного, письмового контролю та тестовий використовуються при проведенні опитувань, комп'ютерного тестування, творчих завдань, що направлені на закріплення практичних навичок застосування вивченого теоретичного матеріалу і методів розв'язування поставлених завдань.	
16. Приймати обґрунтовані рішення з організаційно-технічних питань інформаційної безпеки та/або кібербезпеки у складних і непередбачуваних умовах, у тому числі із застосуванням сучасних методів та засобів оптимізації, прогнозування та прийняття рішень.	☒	Безпека мережевої та SMART інфраструктури	Проведення тематичних і проблемних лекцій характеризується поєднанням традиційних та нетрадиційних методів викладання з використанням інноваційних технологій дистанційної, мультимедійної та веб-орієнтованої. Практичні роботи направлені на поглиблене засвоєння студентами теоретичного матеріалу, отримання практичних навичок при виконанні тренінгових завдань та комп'ютерного тестування. Метод роботи з навчально-методичною літературою забезпечує поглиблення здобувачів освіти з тем навчальної дисципліни та закладає основи майбутньої науково-дослідної роботи.	Проведення поточного контролю передбачає проведення опитувань, тестувань, задач з використанням усного, письмового, тестового методів, перевірки індивідуальних завдань. Методи самоконтролю і самооцінки дозволяють студентам проводити контроль своїх знань особисто. Форма підсумкового контролю – екзамен.
		Технології безпеки Web-ресурсів	Під час проведення лекцій використовуються наступні методи. Словесний метод – для чіткого пояснення матеріалу. Інтерактивний метод – для активної участі аудиторії, забезпечення контакту зі студентами. Відеометод у поєднанні з інформаційними технологіями дистанційного навчання – для зручності та наочності матеріалу. Пояснювально-ілюстративний метод – для логічної послідовності та наочної демонстрації матеріалу. Під час практичних занять використовуються такі методи. Практичний метод – через проведення колоквіумів та дискусій для глибшого розуміння тем. Словесний метод – для додаткового пояснення і обговорення матеріалу. Усний, письмовий контроль та тестування – через опитування, комп'ютерні тести та творчі завдання, спрямовані на закріплення навичок використання вивченого теоретичного матеріалу та методів розв'язання завдань.	Протягом семестру результати навчання студентів оцінюються за результатами поточного і підсумкового контролю: поточний контроль – опитування, колоквіуми, тестування; підсумковий контроль – екзамен.
15. Зрозуміло і	☒	Етичний хакінг	Вивчення дисципліни	Під час навчання проходить

недвозначно доносити власні висновки з проблем інформаційної безпеки та/або кібербезпеки, а також знання та пояснення, що їх обґрунтовують до персоналу, партнерів та інших осіб.		проводиться шляхом лекційних та практичних занять словесними, практичними, наочними методами, відеометодами у сполучені з новітніми інформаційними технологіями та комп'ютерними засобами навчання, що забезпечують закріплення теоретичних знань, сприяють засвоєнню практичних навичок.	поточний контроль у вигляді комп'ютерного тестування, опитування, перевірки індивідуальних завдань. В кінці вивчення дисципліни проводиться підсумковий контроль у формі екзамену.
	Технології безпеки Web-ресурсів	Під час проведення лекцій використовуються наступні методи. Словесний метод – для чіткого пояснення матеріалу. Інтерактивний метод – для активної участі аудиторії, забезпечення контакту зі студентами. Відеометод у поєднанні з інформаційними технологіями дистанційного навчання – для зручності та наочності матеріалу. Пояснювально-ілюстративний метод – для логічної послідовності та наочної демонстрації матеріалу. Під час практичних занять використовуються такі методи. Практичний метод – через проведення колоквіумів та дискусій для глибшого розуміння тем. Словесний метод – для додаткового пояснення і обговорення матеріалу. Усний, письмовий контроль та тестування – через опитування, комп'ютерні тести та творчі завдання, спрямовані на закріплення навичок використання вивченого теоретичного матеріалу та методів розв'язання завдань.	Протягом семестру результати навчання студентів оцінюються за результатами поточного і підсумкового контролю: поточний контроль – опитування, колоквіуми, тестування; підсумковий контроль – екзамен.
	Технології безпеки безпроводових та мобільних мереж	Під час лекцій та практичних занять використовуються різноманітні методи для зрозумілого пояснення матеріалу та активізації участі здобувачів освіти в навчальному процесі. Активно використовуються інформаційні технології для дистанційного навчання. Всі лекції викладаються за допомогою пояснювально-ілюстративного методу, що дозволяє наочно демонструвати матеріал послідовно і логічно. Аудиторна робота передбачає використання практичного підходу (практичні заняття), репродуктивних методів та методів навчання для закріплення практичних навичок вивченого теоретичного матеріалу та методів вирішення поставлених завдань. Виконання індивідуальних завдань з використанням	Поточний контроль знань студентів проводиться на практичних заняттях у вигляді контрольних робіт, опитувань; Підсумковим контролем знань студентів з навчальної дисципліни є екзамен.

			персональних комп'ютерів та контрольних робіт базується на застосуванні пізнавального методу для всебічного освітлення тем.	
14. Аналізувати, розробляти і супроводжувати систему аудиту та моніторингу ефективності функціонування інформаційних систем і технологій, бізнес\операційних процесів у сфері інформаційної та\або кібербезпеки в цілому.	☒	Безпека мережевої та SMART інфраструктури	Проведення тематичних і проблемних лекцій характеризується поєднанням традиційних та нетрадиційних методів викладання з використанням інноваційних технологій дистанційної, мультимедійної та веб-орієнтованої. Практичні роботи направлені на поглиблене засвоєння студентами теоретичного матеріалу, отримання практичних навичок при виконанні тренінгових завдань та комп'ютерного тестування. Метод роботи з навчально-методичною літературою забезпечує поглиблення здобувачів освіти з тем навчальної дисципліни та закладає основи майбутньої науково-дослідної роботи.	Проведення поточного контролю передбачає проведення опитувань, тестувань, задач з використанням усного, письмового, тестового методів, перевірки індивідуальних завдань. Методи самоконтролю і самооцінки дозволяють студентам проводити контроль своїх знань особисто. Форма підсумкового контролю – екзамен.
		Правове забезпечення інформаційної безпеки в економічних системах	Під час лекцій використовуються: словесний метод; інтерактивний метод для більшого залучення аудиторії до навчального процесу, організації контакту із студентами; відеометод у сполученні із застосуванням інформаційних технологій дистанційного навчання, також лекції викладаються із застосуванням пояснювально-ілюстративного методу для наочної демонстрації матеріалу в логічній послідовності. Під час практичних занять використовуються практичний і словесний методи – проводяться колоквіуми і дискусії для більш глибшого розуміння тем та формування світоглядних думок студентів. Методи усного, письмового контролю та тестовий використовуються при проведенні опитувань, комп'ютерного тестування, творчих завдань, що направлені на закріплення практичних навичок застосування вивченого теоретичного матеріалу і методів розв'язування поставлених завдань.	Протягом семестру результати навчання студентів оцінюються за результатами поточного і підсумкового контролю: – поточний контроль: опитування, колоквіуми, тестування; – підсумковий контроль: екзамен.
13. Досліджувати, розробляти, впроваджувати та використовувати методи та засоби криптографічного та технічного захисту інформації	☒	Етичний хакінг	Вивчення дисципліни проводиться шляхом лекційних та практичних занять словесними, практичними, наочними методами, відеометодами у сполучені з новітніми інформаційними	Під час навчання проходить поточний контроль у вигляді комп'ютерного тестування, опитування, перевірки індивідуальних завдань. В кінці вивчення дисципліни проводиться

бізнес/операційних процесів, а також аналізувати і надавати оцінку ефективності їх використання в інформаційних системах, на об'єктах інформаційної діяльності та критичної інфраструктури.			технологіями та комп'ютерними засобами навчання, що забезпечують закріплення теоретичних знань, сприяють засвоєнню практичних навичок.	підсумковий контроль у формі екзамену.
		Технології безпеки безпроводових та мобільних мереж	Під час лекцій та практичних занять використовуються різноманітні методи для зрозумілого пояснення матеріалу та активізації участі здобувачів освіти в навчальному процесі. Активно використовуються інформаційні технології для дистанційного навчання. Всі лекції викладаються за допомогою пояснювально-ілюстративного методу, що дозволяє наочно демонструвати матеріал послідовно і логічно. Аудиторна робота передбачає використання практичного підходу (практичні заняття), репродуктивних методів та методів навчання для закріплення практичних навичок вивченого теоретичного матеріалу та методів вирішення поставлених завдань. Виконання індивідуальних завдань з використанням персональних комп'ютерів та контрольних робіт базується на застосуванні пізнавального методу для всебічного освітлення тем.	Поточний контроль знань студентів проводиться на практичних заняттях у вигляді контрольних робіт, опитувань; Підсумковим контролем знань студентів з навчальної дисципліни є екзамен.
		Безпека мережевої та SMART інфраструктури	Проведення тематичних і проблемних лекцій характеризується поєднанням традиційних та нетрадиційних методів викладання з використанням інноваційних технологій дистанційної, мультимедійної та веб-орієнтованої. Практичні роботи направлені на поглиблене засвоєння студентами теоретичного матеріалу, отримання практичних навичок при виконанні тренінгових завдань та комп'ютерного тестування. Метод роботи з навчально-методичною літературою забезпечує поглиблення здобувачів освіти з тем навчальної дисципліни та закладає основи майбутньої науково-дослідної роботи.	Проведення поточного контролю передбачає проведення опитувань, тестувань, задач з використанням усного, письмового, тестового методів, перевірки індивідуальних завдань. Методи самоконтролю і самооцінки дозволяють студентам проводити контроль своїх знань особисто. Форма підсумкового контролю – екзамен.
22. Планувати та виконувати експериментальні і теоретичні дослідження, висувати і перевіряти гіпотези, обирати для цього придатні методи та інструменти,	☒	Цифрова криміналістика	Лекційні та лабораторні роботи проводяться в поєднанні традиційних і нетрадиційних методів викладання з використанням інноваційних технологій: лекції (тематичні, проблемні); лабораторні заняття. Методи, які використовуються:	Навчання студентів оцінюється на основі результатів поточного контролю у формі усного та письмового опитування, контрольних робіт; підсумкового контролю – екзамену.

здійснювати стати-стичну обробку даних, оцінювати достовірність результатів досліджень, аргументувати висновки.			словесний, практичний, наочний, робота з навчально-методичною літературою, відеометод із залученням дистанційних, мультимедійних та веб-орієнтованих технологій; метод проектів.	
		Правове забезпечення інформаційної безпеки в економічних системах	Під час лекцій використовуються: словесний метод; інтерактивний метод для більшого залучення аудиторії до навчального процесу, організації контакту із студентами; відеометод у сполученні із застосуванням інформаційних технологій дистанційного навчання, також лекції викладаються із застосуванням пояснювально-ілюстративного методу для наочної демонстрації матеріалу в логічній послідовності. Під час практичних занять використовуються практичний і словесний методи - проводяться колоквіуми і дискусії для більш глибшого розуміння тем та формування світоглядних думок студентів. Методи усного, письмового контролю та тестовий використовуються при проведенні опитувань, комп'ютерного тестування, творчих завдань, що направлені на закріплення практичних навичок застосування вивченого теоретичного матеріалу і методів розв'язування поставлених завдань.	Протягом семестру результати навчання студентів оцінюються за результатами поточного і підсумкового контролю: – поточний контроль: опитування, колоквіуми, тестування; – підсумковий контроль: екзамен.
		Технології безпеки Web-ресурсів	Під час проведення лекцій використовуються наступні методи. Словесний метод – для чіткого пояснення матеріалу. Інтерактивний метод – для активної участі аудиторії, забезпечення контакту зі студентами. Відеометод у поєднанні з інформаційними технологіями дистанційного навчання – для зручності та наочності матеріалу. Пояснювально-ілюстративний метод – для логічної послідовності та наочної демонстрації матеріалу. Під час практичних занять використовуються такі методи. Практичний метод – через проведення колоквіумів та дискусій для глибшого розуміння тем. Словесний метод – для додаткового пояснення і обговорення матеріалу. Усний, письмовий контроль та тестування – через опитування, комп'ютерні тести та творчі завдання, спрямовані на закріплення	Протягом семестру результати навчання студентів оцінюються за результатами поточного і підсумкового контролю: поточний контроль – опитування, колоквіуми, тестування; підсумковий контроль – екзамен.

			навичок використання вивченого теоретичного матеріалу та методів розв'язання завдань.	
12. Досліджувати, розробляти та впроваджувати методи і заходи протидії кіберінцидентам, здійснювати процедури управління, контролю та розслідування, а також надавати рекомендації щодо попередження та аналізу кіберінцидентів в цілому.	☒	Цифрова криміналістика	Лекційні та лабораторні роботи проводяться в поєднанні традиційних і нетрадиційних методів викладання з використанням інноваційних технологій: лекції (тематичні, проблемні); лабораторні заняття. Методи, які використовуються: словесний, практичний, наочний, робота з навчально-методичною літературою, відеометод із залученням дистанційних, мультимедійних та веб-орієнтованих технологій; метод проектів.	Навчання студентів оцінюється на основі результатів поточного контролю у формі усного та письмового опитування, контрольних робіт; підсумкового контролю – екзамену.
		Правове забезпечення інформаційної безпеки в економічних системах	Під час лекцій використовуються: словесний метод; інтерактивний метод для більшого залучення аудиторії до навчального процесу, організації контакту із студентами; відеометод у сполученні із застосуванням інформаційних технологій дистанційного навчання, також лекції викладаються із застосуванням пояснювально-ілюстративного методу для наочної демонстрації матеріалу в логічній послідовності. Під час практичних занять використовуються практичний і словесний методи - проводяться колоквіуми і дискусії для більш глибшого розуміння тем та формування світоглядних думок студентів. Методи усного, письмового контролю та тестовий використовуються при проведенні опитувань, комп'ютерного тестування, творчих завдань, що направлені на закріплення практичних навичок застосування вивченого теоретичного матеріалу і методів розв'язування поставлених завдань.	Протягом семестру результати навчання студентів оцінюються за результатами поточного і підсумкового контролю: – поточний контроль: опитування, колоквіуми, тестування; – підсумковий контроль: екзамен.
		Технології безпеки Web-ресурсів	Під час проведення лекцій використовуються наступні методи. Словесний метод – для чіткого пояснення матеріалу. Інтерактивний метод – для активної участі аудиторії, забезпечення контакту зі студентами. Відеометод у поєднанні з інформаційними технологіями дистанційного навчання – для зручності та наочності матеріалу. Пояснювально-ілюстративний метод – для логічної послідовності та	Протягом семестру результати навчання студентів оцінюються за результатами поточного і підсумкового контролю: поточний контроль – опитування, колоквіуми, тестування; підсумковий контроль – екзамен.

			наочної демонстрації матеріалу. Під час практичних занять використовуються такі методи. Практичний метод – через проведення колоквіумів та дискусій для глибшого розуміння тем. Словесний метод – для додаткового пояснення і обговорення матеріалу. Усний, письмовий контроль та тестування – через опитування, комп'ютерні тести та творчі завдання, спрямовані на закріплення навичок використання вивченого теоретичного матеріалу та методів розв'язання завдань.	
10. Забезпечувати безперервність бізнес/операційних процесів, а також виявляти уразливості інформаційних систем та ресурсів, аналізувати та оцінювати ризики для інформаційної безпеки та/або кібербезпеки організації.	☒	Технології безпеки Web-ресурсів	Під час проведення лекцій використовуються наступні методи. Словесний метод – для чіткого пояснення матеріалу. Інтерактивний метод – для активної участі аудиторії, забезпечення контакту зі студентами. Відеометод у поєднанні з інформаційними технологіями дистанційного навчання – для зручності та наочності матеріалу. Пояснювально-ілюстративний метод – для логічної послідовності та наочної демонстрації матеріалу. Під час практичних занять використовуються такі методи. Практичний метод – через проведення колоквіумів та дискусій для глибшого розуміння тем. Словесний метод – для додаткового пояснення і обговорення матеріалу. Усний, письмовий контроль та тестування – через опитування, комп'ютерні тести та творчі завдання, спрямовані на закріплення навичок використання вивченого теоретичного матеріалу та методів розв'язання завдань.	Протягом семестру результати навчання студентів оцінюються за результатами поточного і підсумкового контролю: поточний контроль – опитування, колоквіуми, тестування; підсумковий контроль – екзамен.
		Етичний хакінг	Вивчення дисципліни проводиться шляхом лекційних та практичних занять словесними, практичними, наочними методами, відеометодами у сполучені з новітніми інформаційними технологіями та комп'ютерними засобами навчання, що забезпечують закріплення теоретичних знань, сприяють засвоєнню практичних навичок.	Під час навчання проходить поточний контроль у вигляді комп'ютерного тестування, опитування, перевірки індивідуальних завдань. В кінці вивчення дисципліни проводиться підсумковий контроль у формі екзамену.
		Безпека мережевої та SMART інфраструктури	Проведення тематичних і проблемних лекцій характеризується поєднанням традиційних та нетрадиційних методів викладання з використанням інноваційних технологій	Проведення поточного контролю передбачає проведення опитувань, тестувань, задач з використанням усного, письмового, тестового методів, перевірки індивідуальних завдань.

			дистанційної, мультимедійної та веб-орієнтованої. Практичні роботи направлені на поглиблене засвоєння студентами теоретичного матеріалу, отримання практичних навичок при виконанні тренінгових завдань та комп'ютерного тестування. Метод роботи з навчально-методичною літературою забезпечує поглиблення здобувачів освіти з тем навчальної дисципліни та закладає основи майбутньої науково-дослідної роботи.	Методи самоконтролю і самооцінки дозволяють студентам проводити контроль своїх знань особисто. Форма підсумкового контролю – екзамен.
		Технології безпеки безпроводових та мобільних мереж	Під час лекцій та практичних занять використовуються різноманітні методи для зрозумілого пояснення матеріалу та активізації участі здобувачів освіти в навчальному процесі. Активно використовуються інформаційні технології для дистанційного навчання. Всі лекції викладаються за допомогою пояснювально-ілюстративного методу, що дозволяє наочно демонструвати матеріал послідовно і логічно. Аудиторна робота передбачає використання практичного підходу (практичні заняття), репродуктивних методів та методів навчання для закріплення практичних навичок вивченого теоретичного матеріалу та методів вирішення поставлених завдань. Виконання індивідуальних завдань з використанням персональних комп'ютерів та контрольних робіт базується на застосуванні пізнавального методу для всебічного освітлення тем.	Поточний контроль знань студентів проводиться на практичних заняттях у вигляді контрольних робіт, опитувань; Підсумковим контролем знань студентів з навчальної дисципліни є екзамен.
9. Аналізувати, розробляти і супроводжувати систему управління інформаційною безпекою та/або кібербезпекою організації на базі стратегії і політики інформаційної безпеки.	☒	Етичний хакінг	Вивчення дисципліни проводиться шляхом лекційних та практичних занять словесними, практичними, наочними методами, відеометодами у сполучені з новітніми інформаційними технологіями та комп'ютерними засобами навчання, що забезпечують закріплення теоретичних знань, сприяють засвоєнню практичних навичок.	Під час навчання проходить поточний контроль у вигляді комп'ютерного тестування, опитування, перевірки індивідуальних завдань. В кінці вивчення дисципліни проводиться підсумковий контроль у формі екзамену.
		Технології безпеки безпроводових та мобільних мереж	Під час лекцій та практичних занять використовуються різноманітні методи для зрозумілого пояснення матеріалу та активізації участі здобувачів освіти в навчальному процесі. Активно використовуються інформаційні технології для дистанційного навчання. Всі	Поточний контроль знань студентів проводиться на практичних заняттях у вигляді контрольних робіт, опитувань; Підсумковим контролем знань студентів з навчальної дисципліни є екзамен.

			лекції викладаються за допомогою пояснювально-ілюстративного методу, що дозволяє наочно демонструвати матеріал послідовно і логічно. Аудиторна робота передбачає використання практичного підходу (практичні заняття), репродуктивних методів та методів навчання для закріплення практичних навичок вивченого теоретичного матеріалу та методів вирішення поставлених завдань. Виконання індивідуальних завдань з використанням персональних комп'ютерів та контрольних робіт базується на застосуванні пізнавального методу для всебічного освітлення тем.	
11. Аналізувати, контролювати та забезпечувати ефективне функціонування системи управління доступом до інформаційних ресурсів відповідно до встановлених стратегії і політики інформаційної безпеки та/або кібербезпеки організації.	☒	Етичний хакінг	Вивчення дисципліни проводиться шляхом лекційних та практичних занять словесними, практичними, наочними методами, відеометодами у сполучені з новітніми інформаційними технологіями та комп'ютерними засобами навчання, що забезпечують закріплення теоретичних знань, сприяють засвоєнню практичних навичок.	Під час навчання проходить поточний контроль у вигляді комп'ютерного тестування, опитування, перевірки індивідуальних завдань. В кінці вивчення дисципліни проводиться підсумковий контроль у формі екзамену.
		Технології безпеки Web-ресурсів	Під час проведення лекцій використовуються наступні методи. Словесний метод – для чіткого пояснення матеріалу. Інтерактивний метод – для активної участі аудиторії, забезпечення контакту зі студентами. Відеометод у поєднанні з інформаційними технологіями дистанційного навчання – для зручності та наочності матеріалу. Пояснювально-ілюстративний метод – для логічної послідовності та наочної демонстрації матеріалу. Під час практичних занять використовуються такі методи. Практичний метод – через проведення колоквіумів та дискусій для глибшого розуміння тем. Словесний метод – для додаткового пояснення і обговорення матеріалу. Усний, письмовий контроль та тестування – через опитування, комп'ютерні тести та творчі завдання, спрямовані на закріплення навичок використання вивченого теоретичного матеріалу та методів розв'язання завдань.	Протягом семестру результати навчання студентів оцінюються за результатами поточного і підсумкового контролю: поточний контроль – опитування, колоквіуми, тестування; підсумковий контроль – екзамен.
		Технології безпеки безпроводових та мобільних мереж	Під час лекцій та практичних занять використовуються різноманітні методи для	Поточний контроль знань студентів проводиться на практичних заняттях у вигляді контрольних робіт,

			зрозумілого пояснення матеріалу та активізації участі здобувачів освіти в навчальному процесі. Активно використовуються інформаційні технології для дистанційного навчання. Всі лекції викладаються за допомогою пояснювально-ілюстративного методу, що дозволяє наочно демонструвати матеріал послідовно і логічно. Аудиторна робота передбачає використання практичного підходу (практичні заняття), репродуктивних методів та методів навчання для закріплення практичних навичок вивченого теоретичного матеріалу та методів вирішення поставлених завдань. Виконання індивідуальних завдань з використанням персональних комп'ютерів та контрольних робіт базується на застосуванні пізнавального методу для всебічного освітлення тем.	опитувань; Підсумковим контролем знань студентів з навчальної дисципліни є екзамен.
1. Вільно спілкуватись державною та іноземною мовами, усно і письмово для представлення і обговорення результатів досліджень та інновацій, забезпечення бізнес\операційних процесів та питань професійної діяльності в галузі інформаційної безпеки та/або кібербезпеки.	☒	Етичний хакінг	Вивчення дисципліни проводиться шляхом лекційних та практичних занять словесними, практичними, наочними методами, відеометодами у сполучені з новітніми інформаційними технологіями та комп'ютерними засобами навчання, що забезпечують закріплення теоретичних знань, сприяють засвоєнню практичних навичок.	Під час навчання проходить поточний контроль у вигляді комп'ютерного тестування, опитування, перевірки індивідуальних завдань. В кінці вивчення дисципліни проводиться підсумковий контроль у формі екзамену.
		Правове забезпечення інформаційної безпеки в економічних системах	Під час лекцій використовуються: словесний метод; інтерактивний метод для більшого залучення аудиторії до навчального процесу, організації контакту із студентами; відеометод у сполученні із застосуванням інформаційних технологій дистанційного навчання, також лекції викладаються із застосуванням пояснювально-ілюстративного методу для наочної демонстрації матеріалу в логічній послідовності. Під час практичних занять використовуються практичний і словесний методи - проводяться колоквіуми і дискусії для більш глибшого розуміння тем та формування світоглядних думок студентів. Методи усного, письмового контролю та тестовий використовуються при проведенні опитувань, комп'ютерного тестування, творчих завдань, що направлені на закріплення	Протягом семестру результати навчання студентів оцінюються за результатами поточного і підсумкового контролю: – поточний контроль: опитування, колоквіуми, тестування; – підсумковий контроль: екзамен.

			практичних навичок застосування вивченого теоретичного матеріалу і методів розв'язування поставлених завдань.	
		Технології безпеки безпроводових та мобільних мереж	Під час лекцій та практичних занять використовуються різноманітні методи для зрозумілого пояснення матеріалу та активізації участі здобувачів освіти в навчальному процесі. Активно використовуються інформаційні технології для дистанційного навчання. Всі лекції викладаються за допомогою пояснювально-ілюстративного методу, що дозволяє наочно демонструвати матеріал послідовно і логічно. Аудиторна робота передбачає використання практичного підходу (практичні заняття), репродуктивних методів та методів навчання для закріплення практичних навичок вивченого теоретичного матеріалу та методів вирішення поставлених завдань. Виконання індивідуальних завдань з використанням персональних комп'ютерів та контрольних робіт базується на застосуванні пізнавального методу для всебічного освітлення тем.	Поточний контроль знань студентів проводиться на практичних заняттях у вигляді контрольних робіт, опитувань; Підсумковим контролем знань студентів з навчальної дисципліни є екзамен.
		Англійська мова інформаційних технологій	Під час проведення лекційних та практичних занять використовуються різні підходи з метою підсилення зрозумілості пояснення та підвищення зацікавленості учасників навчального процесу до теоретичного матеріалу. Зокрема, словесний метод спілкування, інтерактивний підхід, що залучає аудиторію до активної участі. Додатково, використовується відеометод у поєднанні з сучасними інформаційними технологіями та засобами навчання, такими як дистанційні, мультимедійні та веб-орієнтовані засоби. Це дозволяє створити більш глибоке та наочне розуміння матеріалу завдяки візуальному контенту та використанню комп'ютерних інструментів. Засвоєння матеріалу підкріплюється наочним методом, використовується ілюстративний підхід, який допомагає наочно продемонструвати матеріал.	При поточному контролі проводяться опитування та тестування студентів та контрольні роботи, також використовуються методи самоконтролю і самооцінювання. Формою підсумкового контролю є екзамен.
2. Інтегрувати фундаментальні та спеціальні знання для розв'язування	☒	Безпека мережевої та SMART інфраструктури	Проведення тематичних і проблемних лекцій характеризується поєднанням традиційних та нетрадиційних методів	Проведення поточного контролю передбачає проведення опитувань, тестувань, задач з використанням усного,

складних задач інформаційної безпеки та/або кібербезпеки у широких або мультидисципліна рних контекстах.			викладання з використанням інноваційних технологій дистанційної, мультимедійної та веб-орієнтованої. Практичні роботи направлені на поглиблене засвоєння студентами теоретичного матеріалу, отримання практичних навичок при виконанні тренінгових завдань та комп'ютерного тестування. Метод роботи з навчально-методичною літературою забезпечує поглиблення здобувачів освіти з тем навчальної дисципліни та закладає основи майбутньої науково-дослідної роботи.	письмового, тестового методів, перевірки індивідуальних завдань. Методи самоконтролю і самооцінки дозволяють студентам проводити контроль своїх знань особисто. Форма підсумкового контролю – екзамен.
		Етичний хакінг	Вивчення дисципліни проводиться шляхом лекційних та практичних занять словесними, практичними, наочними методами, відеометодами у сполучені з новітніми інформаційними технологіями та комп'ютерними засобами навчання, що забезпечують закріплення теоретичних знань, сприяють засвоєнню практичних навичок.	Під час навчання проходить поточний контроль у вигляді комп'ютерного тестування, опитування, перевірки індивідуальних завдань. В кінці вивчення дисципліни проводиться підсумковий контроль у формі екзамену.
		Технології безпеки безпроводових та мобільних мереж	Під час лекцій та практичних занять використовуються різноманітні методи для зрозумілого пояснення матеріалу та активізації участі здобувачів освіти в навчальному процесі. Активно використовуються інформаційні технології для дистанційного навчання. Всі лекції викладаються за допомогою пояснювально-ілюстративного методу, що дозволяє наочно демонструвати матеріал послідовно і логічно. Аудиторна робота передбачає використання практичного підходу (практичні заняття), репродуктивних методів та методів навчання для закріплення практичних навичок вивченого теоретичного матеріалу та методів вирішення поставлених завдань. Виконання індивідуальних завдань з використанням персональних комп'ютерів та контрольних робіт базується на застосуванні пізнавального методу для всебічного освітлення тем.	Поточний контроль знань студентів проводиться на практичних заняттях у вигляді контрольних робіт, опитувань; Підсумковим контролем знань студентів з навчальної дисципліни є екзамен.
		Англійська мова інформаційних технологій	Під час проведення лекційних та практичних занять використовуються різні підходи з метою підсилення зрозумілості пояснення та підвищення зацікавленості учасників навчального процесу до	При поточному контролі проводяться опитування та тестування студентів та контрольні роботи, також використовуються методи самоконтролю і самооцінювання. Формою підсумкового

			теоретичного матеріалу. Зокрема, словесний метод спілкування, інтерактивний підхід, що залучає аудиторію до активної участі. Додатково, використовується відеометод у поєднанні з сучасними інформаційними технологіями та засобами навчання, такими як дистанційні, мультимедійні та веб-орієнтовані засоби. Це дозволяє створити більш глибоке та наочне розуміння матеріалу завдяки візуальному контенту та використанню комп'ютерних інструментів. Засвоєння матеріалу підкріплюється наочним методом, використовується ілюстративний підхід, який допомагає наочно продемонструвати матеріал.	контролю є екзамен.
4. Застосовувати, інтегрувати, розробляти, впроваджувати та удосконалювати сучасні інформаційні технології, фізичні та математичні методи і моделі в сфері інформаційної безпеки та/або кібербезпеки.	☒	Цифрова криміналістика	Лекційні та лабораторні роботи проводяться в поєднанні традиційних і нетрадиційних методів викладання з використанням інноваційних технологій: лекції (тематичні, проблемні); лабораторні заняття. Методи, які використовуються: словесний, практичний, наочний, робота з навчально-методичною літературою, відеометод із залученням дистанційних, мультимедійних та веб-орієнтованих технологій; метод проектів.	Навчання студентів оцінюється на основі результатів поточного контролю у формі усного та письмового опитування, контрольних робіт; підсумкового контролю – екзамену.
		Безпека мережевої та SMART інфраструктури	Проведення тематичних і проблемних лекцій характеризується поєднанням традиційних та нетрадиційних методів викладання з використанням інноваційних технологій дистанційної, мультимедійної та веб-орієнтованої. Практичні роботи направлені на поглиблене засвоєння студентами теоретичного матеріалу, отримання практичних навичок при виконанні тренінгових завдань та комп'ютерного тестування. Метод роботи з навчально-методичною літературою забезпечує поглиблення здобувачів освіти з тем навчальної дисципліни та закладає основи майбутньої науково-дослідної роботи.	Проведення поточного контролю передбачає проведення опитувань, тестувань, задач з використанням усного, письмового, тестового методів, перевірки індивідуальних завдань. Методи самоконтролю і самооцінки дозволяють студентам проводити контроль своїх знань особисто. Форма підсумкового контролю – екзамен.
		Етичний хакінг	Вивчення дисципліни проводиться шляхом лекційних та практичних занять словесними, практичними, наочними методами, відеометодами у сполучені з новітніми інформаційними	Під час навчання проходить поточний контроль у вигляді комп'ютерного тестування, опитування, перевірки індивідуальних завдань. В кінці вивчення дисципліни проводиться

			технологіями та комп'ютерними засобами навчання, що забезпечують закріплення теоретичних знань, сприяють засвоєнню практичних навичок.	підсумковий контроль у формі екзамену.
		Технології безпеки Web-ресурсів	Під час проведення лекцій використовуються наступні методи. Словесний метод – для чіткого пояснення матеріалу. Інтерактивний метод – для активної участі аудиторії, забезпечення контакту зі студентами. Відеометод у поєднанні з інформаційними технологіями дистанційного навчання – для зручності та наочності матеріалу. Пояснювально-ілюстративний метод – для логічної послідовності та наочної демонстрації матеріалу. Під час практичних занять використовуються такі методи. Практичний метод – через проведення колоквіумів та дискусій для глибшого розуміння тем. Словесний метод – для додаткового пояснення і обговорення матеріалу. Усний, письмовий контроль та тестування – через опитування, комп'ютерні тести та творчі завдання, спрямовані на закріплення навичок використання вивченого теоретичного матеріалу та методів розв'язання завдань.	Протягом семестру результати навчання студентів оцінюються за результатами поточного і підсумкового контролю: поточний контроль – опитування, колоквіуми, тестування; підсумковий контроль – екзамен.
		Технології безпеки безпроводових та мобільних мереж	Під час лекцій та практичних занять використовуються різноманітні методи для зрозумілого пояснення матеріалу та активізації участі здобувачів освіти в навчальному процесі. Активно використовуються інформаційні технології для дистанційного навчання. Всі лекції викладаються за допомогою пояснювально-ілюстративного методу, що дозволяє наочно демонструвати матеріал послідовно і логічно. Аудиторна робота передбачає використання практичного підходу (практичні заняття), репродуктивних методів та методів навчання для закріплення практичних навичок вивченого теоретичного матеріалу та методів вирішення поставлених завдань. Виконання індивідуальних завдань з використанням персональних комп'ютерів та контрольних робіт базується на застосуванні пізнавального методу для всебічного освітлення тем.	Поточний контроль знань студентів проводиться на практичних заняттях у вигляді контрольних робіт, опитувань; Підсумковим контролем знань студентів з навчальної дисципліни є екзамен.
3. Провадити	☒	Цифрова	Лекційні та лабораторні	Навчання студентів

дослідницьку та/або інноваційну діяльність в сфері інформаційної безпеки та/або кібербезпеки, а також в сфері технічного та криптографічного захисту інформації у кіберпросторі.		криміналістика	роботи проводяться в поєднанні традиційних і нетрадиційних методів викладання з використанням інноваційних технологій: лекції (тематичні, проблемні); лабораторні заняття. Методи, які використовуються: словесний, практичний, наочний, робота з навчально-методичною літературою, відеометод із залученням дистанційних, мультимедійних та веб-орієнтованих технологій; метод проектів.	оцінюється на основі результатів поточного контролю у формі усного та письмового опитування, контрольних робіт; підсумкового контролю – екзамену.
		Етичний хакінг	Вивчення дисципліни проводиться шляхом лекційних та практичних занять словесними, практичними, наочними методами, відеометодами у сполучені з новітніми інформаційними технологіями та комп'ютерними засобами навчання, що забезпечують закріплення теоретичних знань, сприяють засвоєнню практичних навичок.	Під час навчання проходить поточний контроль у вигляді комп'ютерного тестування, опитування, перевірки індивідуальних завдань. В кінці вивчення дисципліни проводиться підсумковий контроль у формі екзамену.
6. Аналізувати та оцінювати захищеність систем, комплексів та засобів кіберзахисту, технології створення та використання спеціалізованого програмного забезпечення.	☒	Технології безпеки Web-ресурсів	Під час проведення лекцій використовуються наступні методи. Словесний метод – для чіткого пояснення матеріалу. Інтерактивний метод – для активної участі аудиторії, забезпечення контакту зі студентами. Відеометод у поєднанні з інформаційними технологіями дистанційного навчання – для зручності та наочності матеріалу. Пояснювально-ілюстративний метод – для логічної послідовності та наочної демонстрації матеріалу. Під час практичних занять використовуються такі методи. Практичний метод – через проведення колоквіумів та дискусій для глибшого розуміння тем. Словесний метод – для додаткового пояснення і обговорення матеріалу. Усний, письмовий контроль та тестування – через опитування, комп'ютерні тести та творчі завдання, спрямовані на закріплення навичок використання вивченого теоретичного матеріалу та методів розв'язання завдань.	Протягом семестру результати навчання студентів оцінюються за результатами поточного і підсумкового контролю: поточний контроль – опитування, колоквіуми, тестування; підсумковий контроль – екзамен.
		Цифрова криміналістика	Лекційні та лабораторні роботи проводяться в поєднанні традиційних і нетрадиційних методів викладання з використанням інноваційних технологій: лекції (тематичні, проблемні); лабораторні заняття. Методи, які	Навчання студентів оцінюється на основі результатів поточного контролю у формі усного та письмового опитування, контрольних робіт; підсумкового контролю – екзамену.

			використовуються: словесний, практичний, наочний, робота з навчально-методичною літературою, відеометод із залученням дистанційних, мультимедійних та веб-орієнтованих технологій; метод проектів.	
		Безпека мережевої та SMART інфраструктури	Проведення тематичних і проблемних лекцій характеризується поєднанням традиційних та нетрадиційних методів викладання з використанням інноваційних технологій дистанційної, мультимедійної та веб-орієнтованої. Практичні роботи направлені на поглиблене засвоєння студентами теоретичного матеріалу, отримання практичних навичок при виконанні тренінгових завдань та комп'ютерного тестування. Метод роботи з навчально-методичною літературою забезпечує поглиблення здобувачів освіти з тем навчальної дисципліни та закладає основи майбутньої науково-дослідної роботи.	Проведення поточного контролю передбачає проведення опитувань, тестувань, задач з використанням усного, письмового, тестового методів, перевірки індивідуальних завдань. Методи самоконтролю і самооцінки дозволяють студентам проводити контроль своїх знань особисто. Форма підсумкового контролю – екзамен.
		Правове забезпечення інформаційної безпеки в економічних системах	Під час лекцій використовуються: словесний метод; інтерактивний метод для більшого залучення аудиторії до навчального процесу, організації контакту із студентами; відеометод у сполученні із застосуванням інформаційних технологій дистанційного навчання, також лекції викладаються із застосуванням пояснювально-ілюстративного методу для наочної демонстрації матеріалу в логічній послідовності. Під час практичних занять використовуються практичний і словесний методи - проводяться колоквіуми і дискусії для більш глибшого розуміння тем та формування світоглядних думок студентів. Методи усного, письмового контролю та тестовий використовуються при проведенні опитувань, комп'ютерного тестування, творчих завдань, що направлені на закріплення практичних навичок застосування вивченого теоретичного матеріалу і методів розв'язування поставлених завдань.	Протягом семестру результати навчання студентів оцінюються за результатами поточного і підсумкового контролю: – поточний контроль: опитування, колоквіуми, тестування; – підсумковий контроль: екзамен.
7. Обґрунтовувати використання, впроваджувати та аналізувати кращі	☒	Цифрова криміналістика	Лекційні та лабораторні роботи проводяться в поєднанні традиційних і нетрадиційних методів	Навчання студентів оцінюється на основі результатів поточного контролю у формі усного та

світові стандарти, практики з метою розв'язання складних задач професійної діяльності в галузі інформаційної безпеки та/або кібербезпеки.			викладання з використанням інноваційних технологій: лекції (тематичні, проблемні); лабораторні заняття. Методи, які використовуються: словесний, практичний, наочний, робота з навчально-методичною літературою, відеометод із залученням дистанційних, мультимедійних та веб-орієнтованих технологій; метод проектів.	письмового опитування, контрольних робіт; підсумкового контролю – екзамену.
		Безпека мережевої та SMART інфраструктури	Проведення тематичних і проблемних лекцій характеризується поєднанням традиційних та нетрадиційних методів викладання з використанням інноваційних технологій дистанційної, мультимедійної та веб-орієнтованої. Практичні роботи направлені на поглиблене засвоєння студентами теоретичного матеріалу, отримання практичних навичок при виконанні тренінгових завдань та комп'ютерного тестування. Метод роботи з навчально-методичною літературою забезпечує поглиблення здобувачів освіти з тем навчальної дисципліни та закладає основи майбутньої науково-дослідної роботи.	Проведення поточного контролю передбачає проведення опитувань, тестувань, задач з використанням усного, письмового, тестового методів, перевірки індивідуальних завдань. Методи самоконтролю і самооцінки дозволяють студентам проводити контроль своїх знань особисто. Форма підсумкового контролю – екзамен.
		Правове забезпечення інформаційної безпеки в економічних системах	Під час лекцій використовуються: словесний метод; інтерактивний метод для більшого залучення аудиторії до навчального процесу, організації контакту із студентами; відеометод у сполученні із застосуванням інформаційних технологій дистанційного навчання, також лекції викладаються із застосуванням пояснювально-ілюстративного методу для наочної демонстрації матеріалу в логічній послідовності. Під час практичних занять використовуються практичний і словесний методи - проводяться колоквіуми і дискусії для більш глибшого розуміння тем та формування світоглядних думок студентів. Методи усного, письмового контролю та тестовий використовуються при проведенні опитувань, комп'ютерного тестування, творчих завдань, що направлені на закріплення практичних навичок застосування вивченого теоретичного матеріалу і методів розв'язування	Протягом семестру результати навчання студентів оцінюються за результатами поточного і підсумкового контролю: – поточний контроль: опитування, колоквіуми, тестування; – підсумковий контроль: екзамен.

			поставлених завдань.	
		Технології безпеки Web-ресурсів	Під час проведення лекцій використовуються наступні методи. Словесний метод – для чіткого пояснення матеріалу. Інтерактивний метод – для активної участі аудиторії, забезпечення контакту зі студентами. Відеометод у поєднанні з інформаційними технологіями дистанційного навчання – для зручності та наочності матеріалу. Пояснювально-ілюстративний метод – для логічної послідовності та наочної демонстрації матеріалу. Під час практичних занять використовуються такі методи. Практичний метод – через проведення колоквіумів та дискусій для глибшого розуміння тем. Словесний метод – для додаткового пояснення і обговорення матеріалу. Усний, письмовий контроль та тестування – через опитування, комп'ютерні тести та творчі завдання, спрямовані на закріплення навичок використання вивченого теоретичного матеріалу та методів розв'язання завдань.	Протягом семестру результати навчання студентів оцінюються за результатами поточного і підсумкового контролю: поточний контроль – опитування, колоквіуми, тестування; підсумковий контроль – екзамен.
		Англійська мова інформаційних технологій	Під час проведення лекційних та практичних занять використовуються різні підходи з метою підсилення зрозумілості пояснення та підвищення зацікавленості учасників навчального процесу до теоретичного матеріалу. Зокрема, словесний метод спілкування, інтерактивний підхід, що залучає аудиторію до активної участі. Додатково, використовується відеометод у поєднанні з сучасними інформаційними технологіями та засобами навчання, такими як дистанційні, мультимедійні та веб-орієнтовані засоби. Це дозволяє створити більш глибоке та наочне розуміння матеріалу завдяки візуальному контенту та використанню комп'ютерних інструментів. Засвоєння матеріалу підкріплюється наочним методом, використовується ілюстративний підхід, який допомагає наочно продемонструвати матеріал.	При поточному контролі проводяться опитування та тестування студентів та контрольні роботи, також використовуються методи самоконтролю і самооцінювання. Формою підсумкового контролю є екзамен.
8. Досліджувати, розробляти і супроводжувати системи та засоби інформаційної безпеки та/або кібербезпеки на об'єктах	☒	Безпека мережевої та SMART інфраструктури	Проведення тематичних і проблемних лекцій характеризується поєднанням традиційних та нетрадиційних методів викладання з використанням інноваційних технологій	Проведення поточного контролю передбачає проведення опитувань, тестувань, задач з використанням усного, письмового, тестового методів, перевірки індивідуальних завдань.

інформаційної діяльності та критичної інфраструктури.			дистанційної, мультимедійної та веб-орієнтованої. Практичні роботи направлені на поглиблене засвоєння студентами теоретичного матеріалу, отримання практичних навичок при виконанні тренінгових завдань та комп'ютерного тестування. Метод роботи з навчально-методичною літературою забезпечує поглиблення здобувачів освіти з тем навчальної дисципліни та закладає основи майбутньої науково-дослідної роботи.	Методи самоконтролю і самооцінки дозволяють студентам проводити контроль своїх знань особисто. Форма підсумкового контролю – екзамен.
		Етичний хакінг	Вивчення дисципліни проводиться шляхом лекційних та практичних занять словесними, практичними, наочними методами, відеометодами у сполучені з новітніми інформаційними технологіями та комп'ютерними засобами навчання, що забезпечують закріплення теоретичних знань, сприяють засвоєнню практичних навичок.	Під час навчання проходить поточний контроль у вигляді комп'ютерного тестування, опитування, перевірки індивідуальних завдань. В кінці вивчення дисципліни проводиться підсумковий контроль у формі екзамену.
		Технології безпеки безпроводових та мобільних мереж	Під час лекцій та практичних занять використовуються різноманітні методи для зрозумілого пояснення матеріалу та активізації участі здобувачів освіти в навчальному процесі. Активно використовуються інформаційні технології для дистанційного навчання. Всі лекції викладаються за допомогою пояснювально-ілюстративного методу, що дозволяє наочно демонструвати матеріал послідовно і логічно. Аудиторна робота передбачає використання практичного підходу (практичні заняття), репродуктивних методів та методів навчання для закріплення практичних навичок вивченого теоретичного матеріалу та методів вирішення поставлених завдань. Виконання індивідуальних завдань з використанням персональних комп'ютерів та контрольних робіт базується на застосуванні пізнавального методу для всебічного освітлення тем.	Поточний контроль знань студентів проводиться на практичних заняттях у вигляді контрольних робіт, опитувань; Підсумковим контролем знань студентів з навчальної дисципліни є екзамен.
5. Критично осмислювати проблеми інформаційної безпеки та/або кібербезпеки, у тому числі на міжгалузевому та міждисциплінарному рівні, зокрема на	☒	Англійська мова інформаційних технологій	Під час проведення лекційних та практичних занять використовуються різні підходи з метою підсилення зрозумілості пояснення та підвищення зацікавленості учасників навчального процесу до теоретичного матеріалу. Зокрема, словесний метод	При поточному контролі проводяться опитування та тестування студентів та контрольні роботи, також використовуються методи самоконтролю і самооцінювання. Формою підсумкового контролю є екзамен.

основі розуміння нових результатів інженерних і фізико-математичних наук, а також розвитку технологій створення та використання спеціалізованого програмного забезпечення.			спілкування, інтерактивний підхід, що залучає аудиторію до активної участі. Додатково, використовується відеометод у поєднанні з сучасними інформаційними технологіями та засобами навчання, такими як дистанційні, мультимедійні та веб-орієнтовані засоби. Це дозволяє створити більш глибоке та наочне розуміння матеріалу завдяки візуальному контенту та використанню комп'ютерних інструментів. Засвоєння матеріалу підкріплюється наочним методом, використовується ілюстративний підхід, який допомагає наочно продемонструвати матеріал.	
		Правове забезпечення інформаційної безпеки в економічних системах	Під час лекцій використовуються: словесний метод; інтерактивний метод для більшого залучення аудиторії до навчального процесу, організації контакту із студентами; відеометод у сполученні із застосуванням інформаційних технологій дистанційного навчання, також лекції викладаються із застосуванням пояснювально-ілюстративного методу для наочної демонстрації матеріалу в логічній послідовності. Під час практичних занять використовуються практичний і словесний методи - проводяться колоквіуми і дискусії для більш глибшого розуміння тем та формування світоглядних думок студентів. Методи усного, письмового контролю та тестовий використовуються при проведенні опитувань, комп'ютерного тестування, творчих завдань, що направлені на закріплення практичних навичок застосування вивченого теоретичного матеріалу і методів розв'язування поставлених завдань.	Протягом семестру результати навчання студентів оцінюються за результатами поточного і підсумкового контролю: – поточний контроль: опитування, колоквіуми, тестування; – підсумковий контроль: екзамен.
		Безпека мережевої та SMART інфраструктури	Проведення тематичних і проблемних лекцій характеризується поєднанням традиційних та нетрадиційних методів викладання з використанням інноваційних технологій дистанційної, мультимедійної та веб-орієнтованої. Практичні роботи направлені на поглиблене засвоєння студентами теоретичного матеріалу, отримання практичних навичок при виконанні тренінгових	Проведення поточного контролю передбачає проведення опитувань, тестувань, задач з використанням усного, письмового, тестового методів, перевірки індивідуальних завдань. Методи самоконтролю і самооцінки дозволяють студентам проводити контроль своїх знань особисто. Форма підсумкового контролю – екзамен.

			завдань та комп'ютерного тестування. Метод роботи з навчально-методичною літературою забезпечує поглиблення здобувачів освіти з тем навчальної дисципліни та закладає основи майбутньої науково-дослідної роботи.	