НАЦІОНАЛЬНЕ АГЕНТСТВО ІЗ ЗАБЕЗПЕЧЕННЯ ЯКОСТІ ВИЩОЇ ОСВІТИ

ВІДОМОСТІ
про самооцінювання освітньої програми

Заклад вищої освіти	**Західноукраїнський національний університет**
Освітня програма	**59703 Кібербезпека**
Рівень вищої освіти	**Магістр**
Спеціальність	**125 Кібербезпека та захист інформації**

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

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

Використані скорочення:

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

Загальні відомості

1. Інформація про ЗВО (ВСП ЗВО)

Реєстраційний номер ЗВО у ЄДЕБО	**171**
Повна назва ЗВО	**Західноукраїнський національний університет**
Ідентифікаційний код ЗВО	**33680120**
ПІБ керівника ЗВО	**Десятнюк Оксана Миронівна**
Посилання на офіційний веб-сайт ЗВО	**https://www.wunu.edu.ua/**

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

https://registry.edbo.gov.ua/university/171

3. Загальна інформація про ОП, яка подається на акредитацію

ID освітньої програми в ЄДЕБО	**59703**
Назва ОП	**Кібербезпека**
Галузь знань	**12 Інформаційні технології**
Спеціальність	**125 Кібербезпека та захист інформації**
Спеціалізація (за наявності)	*відсутня*
Рівень вищої освіти	**Магістр**
Тип освітньої програми	**Освітньо-професійна**
Вступ на освітню програму здійснюється на основі ступеня (рівня)	**Бакалавр, Магістр (ОКР «спеціаліст»)**
Структурний підрозділ (кафедра або інший підрозділ), відповідальний за реалізацію ОП	**Кафедра кібербезпеки**
Інші навчальні структурні підрозділи (кафедра або інші підрозділи), залучені до реалізації ОП	**Кафедра іноземних мов та інформаційно-комунікаційних технологій**
Місце (адреса) провадження освітньої діяльності за ОП	**46003, м. Тернопіль, вул. О.Теліги 8, навчальний корпус №6**
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	**313913**
ПІБ гаранта ОП	**Яцків Василь Васильович**
Посада гаранта ОП	**завідувач кафедри**
Корпоративна електронна адреса гаранта ОП	**vasyl.yatckiv@wunu.edu.ua**
Контактний телефон гаранта ОП	**+38(097)-218-68-22**
Додатковий телефон гаранта ОП	*відсутній*

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

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

Стрімке зростання кількості кібератак на інформаційні системи державного та приватного секторів, зокрема на об'єкти критичної інфраструктури (енергетика, транспорт, фінансова сфера тощо), починаючи з 2014 року, зумовило суспільну потребу у висококваліфікованих фахівцях з кібербезпеки. Усвідомлюючи актуальність цих викликів, Західноукраїнський національний університет (надалі – ЗУНУ або Університет) у 2018 році започаткував підготовку здобувачів другого (магістерського) рівня вищої освіти за освітньо-професійною програмою «Кібербезпека» (надалі – ОП) в межах спеціальності 125 «Кібербезпека».
Розроблення ОП ґрунтувалося на науковому та педагогічному досвіді викладачів кафедри кібербезпеки. Склад робочої групи за цей час періодично оновлювався з метою залучення нових висококваліфікованих кадрів, що забезпечує системне удосконалення освітнього процесу. Оновлення програми здійснюється відповідно до Положення про освітні програми в ЗУНУ (https://www.wunu.edu.ua/opp/zyao/pologenya_pro_OP.pdf), Порядку перегляду (оновлення) освітніх програм в ЗУНУ (https://www.wunu.edu.ua/opp/zyao/porjadok_peregljadu_op.pdf) на підставі результатів щорічних опитувань стейкхолдерів – здобувачів, роботодавців, науково-педагогічних працівників та інших зацікавлених сторін. Актуальні редакції ОП розміщуються у відкритому доступі на офіційному вебсайті Університету в розділі «Публічна інформація».
(https://www.wunu.edu.ua/opp/2024_OPP/magister/fkit/125_kiberbezpeka_mah_2024.pdf ; https://www.wunu.edu.ua/opp/2025_OPP/magister/fkit/F5_Kiberbezpeka_mag_2025.pdf)
Метою ОП є підготовка конкурентоспроможних фахівців у галузі кібербезпеки, здатних ефективно реагувати на сучасні виклики цифрового середовища та інтегруватися у глобальний професійний простір. Відмінністю програми є поєднання фундаментальної теоретичної підготовки з практичними навичками захисту інформації та протидії кіберзагрозам.
Випусковою кафедрою за ОП є кафедра кібербезпеки ЗУНУ (https://www.wunu.edu.ua/fkit/department-kb-fkit/). До освітнього процесу залучені науково-педагогічні працівники з багаторічним досвідом, відповідною кваліфікацією, активною участю в українських та міжнародних науково-практичних заходах, що відповідає Ліцензійним умовам провадження освітньої діяльності та вимогам Національного агентства із забезпечення якості вищої освіти. У 2019 році ОП було акредитовано Національним агентством (сертифікат про акредитацію № 5347 від 5 липня 2023 року).
Гарантом освітньої програми є Василь Яцків, доктор технічних наук, професор, завідувач кафедри кібербезпеки.

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

Рік навчання	Навчальний рік, у якому відбувся набір здобувачів відповідного року навчання	Обсяг набору на ОП у відповідному навчальному році	Контингент студентів на відповідному році навчання станом на 1 жовтня поточного навчального року		У тому числі іноземців	
			ОД	*З*	*ОД*	*З*
1 курс	2025 - 2026	60	24	7	0	0
2 курс	2024 - 2025	50	31	3	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	**59540 Кібербезпека**
другий (магістерський) рівень	**59703 Кібербезпека**
третій (освітньо-науковий/освітньо-творчий) рівень	**62233 Кібербезпека та захист інформації**

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

	Загальна площа	Навчальна площа
Усі приміщення ЗВО	81121	20456

Власні приміщення ЗВО (на праві власності, господарського відання або оперативного управління)	80698	20033
Приміщення, які використовуються на іншому праві, аніж право власності, господарського відання або оперативного управління (оренда, безоплатне користування тощо)	423	423
Приміщення, здані в оренду	2379	793

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

8. Документи щодо ОП

Документ	Назва файла	Хеш файла
Освітня програма	*OPP_kiberbezpeka_2024.pdf*	yYOYt9EvhANBG/EIcuhFtU6VapQ8kDHiAdhz9iJIyzA=
Освітня програма	*OPP_Kiberbezpeka_2025.pdf*	hC4/eHa+1/4g/qFHLTNsU3icd9vzThEcxb4a7h1n8AQ=
Навчальний план за ОП	*Navch_plan_mag_2024.pdf*	8hXVvJNTBmNgVCU66tlsN7WagQ7DzgBNT2Nj1HPyEsk=
Навчальний план за ОП	*Navch_plan_mag_2025.pdf*	IP2aFbNkmK9P3S5WN+Ope2Ytp7jjQXnBnJTwblC1Kwo=
Матеріали від ЗВО: пропозиції та рекомендації від роботодавців, таблиця відповідності публікацій наукових керівників напрямам (тематикам) досліджень аспірантів (для ОП третього рівня освіти)	*Результати обговорення ОП.pdf*	rWvtTX6KUN5J2PKti9ZFVAjLnOqzZjy1wycpoT1fMUo=
Матеріали від ЗВО: пропозиції та рекомендації від роботодавців, таблиця відповідності публікацій наукових керівників напрямам (тематикам) досліджень аспірантів (для ОП третього рівня освіти)	*Рецензії_2024.pdf*	pLw72XAofiQRYwl55SluEHSrcoUGXKvOPmK/e8Bv50c=
Матеріали від ЗВО: пропозиції та рекомендації від роботодавців, таблиця відповідності публікацій наукових керівників напрямам (тематикам) досліджень аспірантів (для ОП третього рівня освіти)	*Рецензії_2025.pdf*	Atnavv2roayoBkWduuiPDTvrHWhMe3VkJAckbfl7qZc=

1. Проєктування освітньої програми

Чи освітня програма дає можливість досягти результатів навчання, визначених стандартом вищої освіти за відповідною спеціальністю та рівнем вищої освіти? Якщо стандарт вищої освіти за відповідною спеціальністю та рівнем вищої освіти відсутній, поясніть, яким чином визначені ОП програмні результати навчання відповідають вимогам Національної рамки кваліфікацій для відповідного кваліфікаційного рівня?

ОП повністю відповідає вимогам Стандарту вищої освіти за спеціальністю 125 «Кібербезпека» для другого (магістерського) рівня, затвердженого наказом МОН України від 18.03.2021 № 332 (з урахуванням зміни назви спеціальності на «Кібербезпека та захист інформації», постанова КМУ від 16.12.2022 № 1392). Програмні результати навчання узгоджені зі Стандартом та відповідають дескрипторам Національної рамки кваліфікацій (7 рівень) і першого циклу Європейського простору вищої освіти. Структура програми передбачає 90 кредитів ЄКТС, з яких 15 ЄКТС відведено на практичну підготовку (переддипломна практика), що прямо відповідає вимогам Стандарту. Компетентності та ПРН, закладені в ОП, співвіднесені з дескрипторами НРК та узгоджені з переліком, визначеним у Стандарті, як і форма підсумкової атестації. Таким чином, ОП забезпечує здобувачам можливість досягти всіх результатів навчання, визначених Стандартом вищої освіти за спеціальністю 125 «Кібербезпека» на другому (магістерському) рівні.

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

ОП не передбачає присвоєння професійної кваліфікації.
Проте, наявність в ОП ОК «Тестування комп'ютерних систем на проникнення», «Дослідження та проектування систем захисту інформації», «Моніторинг та управління інформаційною безпекою» та «Аналіз шкідливого програмного забезпечення», вказує на приналежність ОП до професійного стандарту «Фахівець з тестування систем захисту інформації» та «Фахівець з криптографічного захисту інформації», які затверджено наказом Адміністрації Держспецзв'язку № 38 від 23 січня 2024 р.
ОП забезпечує здобувачів необхідними знаннями та навичками для проведення підготовчих робіт щодо процедур тестування на проникнення систем кібербезпеки та захисту інформації на всіх етапах (розроблення, впровадження та супроводження) життєвого циклу інформаційних системи та/або мереж а також аналізувати потреби та вимоги користувачів (замовників) щодо криптографічного захисту інформації з метою впровадження систем та комплексів захисту інформаці.

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

У процесі формулювання мети та програмних результатів було враховано пропозиції, запропоновані здобувачами вищої освіти у процесі участі у розширеному засіданні кафедри, де обговорювався проєкт ОП (https://www.wunu.edu.ua/opp/2025_proekt_opp/magister/F5_kiberbezpeka_proekt_mag_25.pdf). Пропозиції стейкхолдерів узагальнено в аналітичному звіті (https://www.wunu.edu.ua/opp/analit_zvit/magistr/F5_kiberbezpeka_mag_az_25.pdf) і враховано в остаточному варіанті ОП, розглянутому Вченою радою ЗУНУ і затвердженому ректором. Зокрема при перегляді даної ОП, за пропозицією здобувачки Анастасії Гнатюк, у робочу програму ОК «Дослідження і проектування систем захисту інформації» введено теми, пов'язані з вивченням постквантових алгоритмів шифрування.
Для отримання зворотного зв'язку зі здобувачами використовується електронне листування (vasyl.yatckiv@wunu.edu.ua), а також анонімне анкетування з різних аспектів організації освітнього процесу (https://www.wunu.edu.ua/public_information/ensuring-the-quality-of-education/16345-rezultati-montoringu-jakost-osvti.html)

- роботодавці

Залучення роботодавців до організації наукових подій, освітнього процесу та обговорення проєктів ОП на розширених засіданнях кафедри дозволяє врахувати позиції стейкголдерів і оновити зміст ОП. До обговорення проєктів ОП долучались представники Департаменту кіберполіції Національної поліції України, ТОВ «Distributed Lab», UnderDefense та інші.
За результатами обговорення прийнято такі пропозиції:
– Софія Цезарук, інспектор ВПК в Тернопільській області Департаменту кіберполіції Національної поліції України, щодо введення в робочу програму ОК «Цифрова криміналістика» тем, пов'язаних з криміналістикою мобільних пристроїв;
– Олена Волощук, к.т.н., доцент, керівник освітньої програми в Distributed Lab, щодо введення вибіркової дисципліни для вивчення математичних проблем розробки та використання технології блокчейн.

- академічна спільнота

Питання формування цілей та ПРН ОП обговорюються на засіданнях кафедри, зустрічах робочої групи ОП за участі академічної спільноти ЗУНУ та інших ЗВО. У процесі формування ОП 2025 р. було враховано рекомендацію к.т.н, доцента Дмитра Узуна (Національний аерокосмічний університет "ХАІ", ментора СофтСерв Академія) ввести вибіркову дисципліну «Безпека хмарних сервісів». На розширені засідання кафедри запрошуються фахівці за профілем ОП з інших ЗВО. Зокрема, при обговоренні проєкту ОП в 2025 році були присутні к.т.н., доцент Віктор Чешун (Хмельницький національний університет) та к.т.н, доцент Дмитро Узун (Національний аерокосмічний університет "ХАІ"), які висловили свої рекомендації щодо покращення ОП.

- інші стейкхолдери

При підготовці проєктів ОП 2024-2025 рр. враховано інтереси, пропозиції, рекомендації українських та іноземних стейкхолдерів, міжнародних та національних організацій, установ, підприємств, учасників професійних семінарів, наукових конференцій та інших науково-практичних заходів, зокрема, тих, які проводились на базі ЗУНУ: XIV міжнародна науково-технічна конференція «Безпека інформаційних технологій» 22-24 травня 2025 р., https://itsec2025.wunu.edu.ua); III міжнародної науково-практичної конференції «Кібербезпека державних інституцій та подолання кризових станів» 14 листопада 2024 року, Київ-Тернопіль; III Безпековий форум, 25 квітня 2025 року https://www.wunu.edu.ua/news/27799--bezpekovij-forum.html

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

Мета освітньо-професійної програми «Кібербезпека» повністю узгоджується з місією та Стратегією розвитку Західноукраїнського національного університету на 2024–2028 рр. (https://www.wunu.edu.ua/pdf/doc_zunu/ust_doc/str_rozvutky_zunu_2024.pdf). ОП орієнтована на підготовку висококваліфікованих фахівців у сфері кібербезпеки, здатних здійснювати наукові дослідження, впроваджувати інноваційні технології, проводити тестування на проникнення, здійснювати цифрову криміналістику та ефективно

працювати в міждисциплінарних командах. Така спрямованість напряму відповідає стратегічним пріоритетам Університету щодо розвитку інноваційного освітньо-наукового середовища, формування конкурентоспроможного кадрового потенціалу та забезпечення якісних освітніх послуг. Відповідність місії Університету реалізується у підготовці фахівців, які поєднують професійні компетентності з високими стандартами академічної доброчесності, корпоративної культури та соціальної відповідальності, готові служити інтересам громади й держави та ефективно реагувати на сучасні виклики у сфері кібербезпеки.

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

Мета ОП визначається з урахуванням актуальних тенденцій розвитку науки і спеціальності та спрямована на підготовку фахівців, здатних до дослідницької, інноваційної та практичної діяльності в галузі інформаційної та кібербезпеки. Програма розроблена відповідно до Стандарту вищої освіти за спеціальністю 125 «Кібербезпека» (з урахуванням перейменування на «Кібербезпека та захист інформації», постанова КМУ від 16.12.2022 № 1392) та бере до уваги чинний професійний стандарт ДССЗЗІ (2024), що забезпечує її відповідність вимогам сучасного ринку праці.
ПРН інтегрують сучасні наукові досягнення і практики кіберзахисту, зокрема через сучасні ОК: «Моніторинг та управління інформаційною безпекою» (SOC/ISMS), «Тестування комп'ютерних систем на проникнення», «Аналіз шкідливого ПЗ», «Цифрова криміналістика». Наукова складова реалізується через ОК «Методологія наукових досліджень», що формує у здобувачів здатність до проведення досліджень і критичного осмислення сучасних теорій та технологій.
Актуалізація змісту ОП здійснюється у співпраці зі стейкґолдерами – роботодавцями, випускниками та фахівцями галузі, що дозволяє враховувати динаміку розвитку кібербезпеки та інтегрувати новітні підходи до підготовки магістрів.

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

Мета ОП та визначені ПРН враховують сучасні тенденції розвитку ринку праці у сфері інформаційної та кібербезпеки. Зміст ОК безпосередньо відображає актуальні професійні ролі, зокрема SOC/ISMS («Моніторинг та управління ІБ»), пентест («Тестування комп'ютерних систем на проникнення»), DFIR («Цифрова криміналістика») та malware analysis («Аналіз шкідливого програмного забезпечення»). Таке наповнення дозволяє формувати компетентності та ПРН, що відповідають сучасним стандартам і практикам ризик-менеджменту, інцидент-респонсу, криптографічного захисту та аудиту інформаційної безпеки, і є затребуваними роботодавцями.
Галузевий і регіональний контекст реалізується через орієнтацію програми на цільові посади, визначені Національним класифікатором професій ДК 003:2010 (аналітик ІКТ-безпеки, фахівець із захисту інформації, аудитор інформаційної безпеки, тестувальник на проникнення тощо), а також через системний моніторинг ринку вакансій і співпрацю з ключовими стейкґолдерами. Важливим підтвердженням відповідності потребам регіону та країни є зовнішні рецензії на ОП від представників кіберполіції та Тернопільської обласної військової адміністрації.

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

При формуванні цілей та ПРН, визначенні ОК та їх змістового наповнення враховано досвід українських інституцій.
Визначення та уточнення цілей та РН ОП скорельовано згідно з досвідом таких ЗВО:
Національний університет «Львівська політехніка»: https://lpnu.ua/sites/default/files/2021/program/15951/125-mag-biks-2024.PDF
Харківський національний університет радіоелектроніки: https://nure.ua/wp-content/uploads/Education_programs/2024/2024_mag_125_opp_biks.pdf
https://nure.ua/wp-content/uploads/Education_programs/2024/2024_mag_125_opp_amszi.pdf
НТУУ «КПІ ім. І. Сікорського»: https://osvita.kpi.ua/sites/default/files/opfiles/125_oppm_stzi_2024.pdf
Київський національний університет імені Тараса Шевченка: https://fit.knu.ua/wp-content/uploads/2024/03/125_ОНП_маг_Кібербезпека_2023_КБтаЗІ_-1.pdf
Державний університет інформаційно-комунікаційних технологій:
https://duikt.edu.ua/uploads/p_1823_35003080.pdf?file=p_1823_35003080.pdf
Київський університет імені Бориса Грінченка:
https://kubg.edu.ua/images/stories/Departaments/vstupnikam/fitm/OPP_125_KBtaZI_mahistry.pdf
У результаті аналізу встановлено специфіку програм, обумовлену як інституційними чинниками, так і регіональними запитами. Досвід зазначених ЗВО був врахований при оновленні освітніх компонентів: Моніторинг та управління інформаційною безпекою; цифрова криміналістика та дослідження і проектування систем захисту інфоомації. Це формує у випускників актуальні компетентності та знання, придатні для реагування на сучасні кіберзагрози.

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

При формуванні цілей та ПРН, визначенні ОК та їх змістового наповнення враховано досвід закордонних ОП підготовки магістра з кібербезпеки, зокрема, Cyber Security, Edinburgh Napier University, Велика Британія; Master of Science in Cyber Security Engineering, University of San Diego, США; Master of Science in Cybersecurity Engineering Program Обернський університет, США; Master of Science in Cyber Security, EC-Council New Mexico, США.
Проведений аналіз ОП з кібербезпеки іноземних університетів показав наявність актуальних ОК, таких як

«Тестування на проникнення», «Цифрова криміналістика», «Аналіз шкідливих програм» та «Реверс інжиніринг». На основі проведеного аналізу було прийнято рішення ввести окремі ОК в ОП на етапі її вдосконалення.
При змістовному наповненні ОК враховано також зміст міжнародних професійних програм сертифікації, таких як: GIAC GCIA для SOC; Offensive Security: OSCP (PEN-200/OSCP+) та GIAC GPEN для пентесту; GIAC GCFE для цифрової криміналістики, що уможливлює отримання здобувачами відповідних професійних міжнародних сертифікатів.

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)?

65

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

25

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

Зміст ОП відповідає предметній області спеціальності Кібербезпека та захист інформації, має чітку, логічно взаємопов'язану та практико зорієнтовану структуру ОК і спрямований на досягнення визначених цілей. Структура ОП містить блок обов'язкових компонентів загальної і професійної підготовки та вибіркові дисципліни.
Відповідно до предметної області ОП:
Об'єктами вивчення та професійної діяльності магістра з кібербезпеки та захисту інформації є сучасні процеси дослідження, аналізу, створення та забезпечення функціонування інформаційних систем і технологій, інших бізнес-операційних процесів на об'єктах інформаційної діяльності та критичних інфраструктур сфери інформаційної безпеки та/або кібербезпеки;
– інформаційні системи (інформаційно-комунікаційні, інформаційно-телекомунікаційні, автоматизовані) та технології;
– інфраструктура об'єктів інформаційної діяльності та критичних інфраструктур;
– системи та комплекси створення, обробки, передачі, зберігання, знищення, захисту та відображення даних (інформаційних потоків);
– інформаційні ресурси різних класів (в т.ч. державні інформаційні ресурси);
– програмне та програмно-апаратне забезпечення (засоби) кіберзахисту;
– системи управління інформаційною безпекою та/або кібербезпекою;
– технології, методи, моделі та засоби інформаційної безпеки та/або кібербезпеки.
Цілі навчання - підготовка фахівців, здатних розв'язувати задачі дослідницького та/або інноваційного характеру у сфері інформаційної та/або кібербезпеки.
Теоретичний зміст предметної галузі: теоретичні засади наукоємних технологій, фізичні і математичні фундаментальні знання, теорії ідентифікації та прийняття рішень, системного аналізу, складних систем, моделювання та оптимізації процесів, теорія математичної статистики, криптографічного та технічного захисту інформації, теорії ризиків та інших міждисциплінарних теорій і практик у галузі інформаційної безпеки та/або кібербезпеки.
Методи, методики та технології: створення, обробки, передачі, приймання, знищення, відображення, захисту (кіберзахисту) інформаційних ресурсів у кіберпросторі, а також методи та моделі розробки та використання прикладного і 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.
Загалом, мета та зміст ОП відповідають предметній області спеціальності і забезпечують готовність здобувачів до виконання завдань професійної діяльності. Моніторинг змістового наповнення ОП здійснюється відповідно до Положення про систему внутрішнього забезпечення якості освіти в ЗУНУ (https://www.wunu.edu.ua/opp/zyao/systemu_vnutr_zabezp_yakosti_osvity.pdf).

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

Для конкретизації планування освітнього процесу за ОП щорічно формується індивідуальна траєкторія навчання здобувача. Можливість формування індивідуальної освітньої траєкторії реалізується на підставі Положення про формування вибіркової частини навчальних планів у Західноукраїнському національному університеті (https://www.wunu.edu.ua/pdf/nu_oop/pologenya-pro-formuvanna-vubirkovoi-chastunu_np_wunu.PDF)..

Каталог вибіркових навчальних дисциплін (https://www.wunu.edu.ua/opp/fkit/kiberbezpeka_magistr/Katalog_vub_Kiberbezpeka_mag.pdf) формується на підставі заявок кафедр Університету, які забезпечують загальну та професійну підготовку зі спеціальності (ОП). Формування заявок на викладання навчальних дисциплін здійснюється за принципом забезпечення викладання ОК не тільки профільними кафедрами, а й загальноуніверситетськими. Можливість формування індивідуальної освітньої траєкторії забезпечується вибором бази практики (у зв'язку з можливим/наявним місцем працевлаштування), а також можливістю репрезентувати результати наукової роботи на різних наукових заходах. Також індивідуальна освітня траєкторія забезпечується вільним вибором теми кваліфікаційної роботи, а також можливостями внутрішньої та зовнішньої мобільності (про що свідчать укладені угоди як з українськими, так і закордонними ЗВО).

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

Вибіркові дисципліни охоплюють 25 кредитів ЄКТС навчального плану ОП, що відповідає вимогам Закону України «Про вищу освіту». Для реалізації права на вибір дисциплін в університеті затверджено відповідне Положення (https://www.wunu.edu.ua/pdf/nu_oop/pologenya-pro-formuvanna-vubirkovoi-chastunu_np_wunu.PDF), в якому чітко прописана уся процедура вибору. Перелік дисциплін вибіркової частини робочих навчальних планів підготовки здобувачів вищої освіти на наступний навчальний рік готують випускові кафедри. Згідно з п.3. Положення про формування вибіркової частини навчальних планів вибіркові дисципліни обираються на навчальний рік здобувачами другого (магістерського) рівня вищої освіти протягом першого місяця навчання. Здобувач вищої освіти здійснює вибір дисципліни із запропонованого переліку за таким алгоритмом: відкриває сайт ЗУНУ у розділі «Студентське життя» та переходить за посиланням «Електронний кабінет студента». Здійснивши вхід за допомогою адреси електронної пошти та пароля, які одержує під час створення облікового запису в інформаційній системі «SMART Університет», та зайшовши у свій електронний кабінет, він може обрати картку навчання. Ознайомившись з усіма обов'язковими дисциплінами навчального плану, здобувач може обрати дисципліни із блоку вільного вибору. Із запропонованого переліку дисциплін для кожного семестру здобувачу необхідно обрати дисципліни, кількість кредитів ЄКТС яких би забезпечили необхідну суму кредитів, визначену для даного семестру. Вибравши усі дисципліни, здобувач вищої освіти підтверджує свій вибір. Обрані вибіркові дисципліни вносяться до робочих навчальних планів спеціальностей (освітніх програм) і визначають навчальне навантаження кафедр і конкретного викладача. Після остаточного визначення здобувачами вибіркових дисциплін автоматично формується індивідуальний навчальний план здобувача вищої освіти на навчальний рік.
Перелік вибіркових навчальних дисциплін формується у формі каталогу, в якому конкретизується найменування навчальної дисципліни. На сайті ЗУНУ розміщено перелік вибіркових дисциплін для ОП (https://www.wunu.edu.ua/opp/fkit/kiberbezpeka_magistr/Katalog_vub_Kiberbezpeka_mag.pdf) та підготовлено силабуси для детального ознайомлення зі змістом вибіркових дисциплін (https://www.wunu.edu.ua/master-). На кафедрах існує практика презентації вибіркових дисциплін викладачами, які їх забезпечують. Це дає змогу здобувачам ОП більш детально ознайомитися зі змістом навчальної дисципліни, її практичною спрямованістю, отримати відповіді на запитання.

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

Практична підготовка здобувачів вищої освіти здійснюється шляхом проходження ними переддипломної практики, що регулюється Положенням про проведення практик здобувачів ЗУНУ (https://www.wunu.edu.ua/pdf/pologenya/provedennia_praktyky.pdf). Відповідно до ОП, переддипломна практика охоплює 15 кредитів, та є обов'язковою компонентою практико зорієнтованої підготовки, що дає змогу сформувати у здобувачів відповідні компетентності та забезпечити досягнення ПРН.
Актуальність практичної підготовки забезпечується завдяки співпраці з роботодавцями, регіональним ІТ-кластером та іншими ЗВО, які беруть участь у формуванні програм практики. Важливу роль відіграє аналіз зворотного зв'язку від керівників практики на підприємствах, а також інтеграція результатів підвищення кваліфікації викладачів кафедри кібербезпеки в освітній процес.
Проходження практики здобувачем здійснюється відповідно до укладеного договору за індивідуальним календарним планом, що погоджується з керівником організації. На період проходження практики здобувачу призначається її керівник від кафедри.
За підсумками переддипломної практики здобувачі готують звіти і проходять процедуру захисту перед сформованою на кафедрі комісією. Підсумкова оцінка результативності проходження практики виставляється з урахуванням думки керівника практики від організації.
Окрім того, практична зорієнтованість підготовки здобувачів реалізується через проведення всіх організаційних заходів, тренінгів з дисциплін, виконання ситуативних завдань, зустрічей з провідними фахівцями-практиками.

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

ОП забезпечує формування у здобувачів вищої освіти ключових соціальних навичок (soft skills), необхідних для ефективної професійної діяльності в сучасному цифровому середовищі. У процесі навчання здобувачі розвивають критичне та системне мислення, навички усної та письмової комунікації (в тому числі вміння пояснювати складні технічні питання нетехнічній аудиторії), командну роботу й лідерство, відповідальність та етичність, уміння приймати рішення в умовах невизначеності, управляти часом і ризиками, презентувати результати власних досліджень.
Набуття зазначених навичок інтегровано в ОК програми через колективне виконання проєктів, презентацію результатів досліджень, захист лабораторних робіт, виступи на семінарських заняттях та участь у наукових

конференціях, у тому числі англійською мовою. Важливою складовою розвитку soft skills є позааудиторна діяльність здобувачів – участь в онлайн-заходах і тренінгах, що проводяться у межах проєкту «Кібербезпека критично важливої інфраструктури України» та інших професійних семінарів і конференцій.
Таким чином, ОП послідовно забезпечує формування у здобувачів соціальних навичок упродовж усього періоду навчання, що узгоджується з її метою та сприяє досягненню ПРН, орієнтованих на підготовку висококваліфікованих і конкурентоспроможних фахівців у сфері інформаційної безпеки та/або кібербезпеки.

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

Зміст ОП має чітку структуру, що базується на логічній послідовності та взаємозв'язку ОК. Навчальний план побудований таким чином, щоб забезпечити поетапне засвоєння знань, формування вмінь і розвиток компетентностей, які у своїй сукупності дають змогу досягти заявленої мети та ПРН.
ОК утворюють узгоджену систему, що поєднує фундаментальну теоретичну підготовку з практичною діяльністю. Це дозволяє здобувачам не лише опановувати професійні компетентності у сфері кібербезпеки та захисту інформації, але й розвивати загальнокультурні та громадянські компетентності, необхідні для особистісного становлення та успішної професійної реалізації.
Особлива увага приділяється формуванню у здобувачів критичного мислення, здатності самостійно аналізувати суспільні процеси та визначати їхні закономірності й тенденції. Такий підхід забезпечує не тільки готовність випускників ОП застосовувати здобуті знання у професійній діяльності, а й водночас формує активну громадянську позицію, здатність до міжкультурного діалогу, орієнтацію на підтримку демократичних цінностей та сприяє інтеграції України в європейський і світовий освітньо-культурний простір.

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, обсяг ОК (у кредитах ЄКТС) визначається навчальним планом, який містить відомості про кількість кредитів для засвоєння кожної ОК. Відповідно до навчального плану ОП загальний обсяг годин становить 2700/90 кредитів. Співвіднесення обсягу окремих ОК ОП із фактичним навантаженням здобувачів вищої освіти (включно із самостійною роботою) в ЗВО ґрунтується на принципах рівномірності, системності та пропорційності. Розподіл контактних годин між лекціями, практичними заняттями та консультаціями, а також між тижнями теоретичного чи практичного навчання, сесійного періоду є прерогативою ЗВО. Навчальний план формується з урахуванням ліміту тижневого навантаження та обсягу кредитів на семестр. На самостійну роботу відводиться від 1/3 до 2/3 годин від загального обсягу вивчення ОК. Для підвищення ефективності самостійного опрацювання матеріалів передбачено консультації з викладачем за затвердженим графіком. Для з'ясування завантаженості здобувачів застосовуються такі заходи: опитування здобувачів у формі анкетування та бесід з НПП; моніторинг з боку викладачів та кураторів із подальшим обговоренням на засіданнях кафедр та засіданнях вченої ради факультету. Така практика дає змогу ідентифікувати проблеми, з якими стикаються здобувачі під час самостійного вивчення дисципліни. Для вирішення цих проблем активно використовуються інформаційні ресурси (групи у Viber, електронна пошта, online-консультації, Zoom, Moodle та інші).

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

Практикоорієнтованість ОП забезпечується поєднанням ґрунтовної теоретичної підготовки з різноманітними формами практичної діяльності. Ключову роль у цьому відіграє переддипломна практика обсягом 15 кредитів ЄКТС, яка є обов'язковим компонентом навчального плану. Вона спрямована на формування у здобувачів професійних компетентностей, необхідних для подальшої діяльності у сфері кібербезпеки. Практика організовується на базах державних і приватних установ, які розробляють, досліджують та впроваджують системи захисту інформації або використовують сучасні програмно-апаратні засоби захисту активів у своїй діяльності. Її проведення регламентується силабусом та програмою практики, розміщеними на офіційному сайті Університету (https://www.wunu.edu.ua/master_fcit_op/). Практикоорієнтований підхід також реалізується через підготовку та публічний захист кваліфікаційної роботи, що дозволяє здобувачам застосовувати здобуті знання у вирішенні реальних проблемних завдань, а також через гостьові лекції та тренінги за участю провідних фахівців галузі, які знайомлять студентів із сучасними практиками кіберзахисту. Додатково практичні навички розвиваються під час виконання лабораторних і семінарських завдань, кейсів та ситуаційних вправ, що моделюють професійні контексти. Підготовка здобувачів вищої освіти за дуальною формою не передбачена.

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

ОП інтегрована з глобальними цілями сталого розвитку до 2030 року. Відповідність забезпечується через зміст ОК,

ПРН та механізми внутрішнього забезпечення якості. ОП реалізує:
• ЦСР 4 «Якісна освіта» – упровадження студентоцентрованого, проблемно- й практикоорієнтованого навчання, прозорих процедур оцінювання;
• ЦСР 8 «Гідна праця та економічне зростання» – орієнтація на перелік цільових посад, визначених у класифікаторі професій, і формування компетентностей, що забезпечують працевлаштованість випускників у сфері кібербезпеки;
• ЦСР 9 «Інновації та інфраструктура» – акцент на дослідницькій і проєктній діяльності та формування ПРН, спрямованих на інноваційні рішення та розвиток наукових досліджень;
• ЦСР 11 «Сталий розвиток громад» – підготовка фахівців для захисту критичної інфраструктури й безперервності бізнес-процесів, що підвищує стійкість міського й регіонального середовища;
• ЦСР 16 «Мир, справедливість та сильні інститути» – зміст ОК7, ОК5, дотримання вимог академічної доброчесності у кваліфікаційних роботах, орієнтація на співпрацю з державними і правоохоронними структурами у протидії кіберзлочинності;
• ЦСР 17 «Партнерства заради сталого розвитку» – розвиток академічної мобільності (зокрема Erasmus+), співпраця зі стейкґолдерами.
Механізми реалізації включають матриці відповідності компетентностей і ПРН, публічний захист і розміщення кваліфікаційних робіт у репозитарії, регулярне оновлення змісту ОП. У сукупності це гарантує набуття здобувачами навичок і компетентностей, спрямованих на досягнення ЦСР.

3. Доступ до освітньої програми та визнання результатів навчання

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

https://pk.wunu.edu.ua/degree/master/

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

Прийом на навчання для здобуття освітнього ступеня магістра на ОП відбуваються відповідно до Правил прийому на навчання для здобуття вищої освіти в Західноукраїнському національному університеті в 2024 році (https://pk.wunu.edu.ua/admission-rules/wunu-2024/), у 2025 році (https://pk.wunu.edu.ua/admission-rules/wunu-2025/), розроблених згідно із чинним законодавством. Регламент прийому документів вступників на навчання за освітніми програмами підготовки магістра на основі здобутого ступеня бакалавра (або магістра/спеціаліста) до ЗУНУ враховує особливості самої ОП, оскільки роботу зі вступниками проводять профільний факультет та кафедра кібербезпеки. Особливості вступу на ОП враховано таким чином: для зарахування на навчання здобувачі складають єдиний вступний іспит (ЄВІ), єдине фахове вступне випробування (ЄФВВ) з інформаційних технологій або єдиний державний кваліфікаційний іспит (ЄДКІ) зі спеціальності 125 «Кібербезпека та захист інформації» (https://pk.wunu.edu.ua/degree/master/educational-programs/view/kiberbezpeka/).
Необхідною умовою для конкурсного відбору є також мотиваційний лист, особливості розгляду якого детально описані в Додатку 16 Правил прийому (https://cdn.wunu.edu.ua/public-service/media/public/admission/rule/addition/admission-rule-addition.c9f1f63e-d692-4837-a044-85316e39ff16.pdf)

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

Питання визнання результатів навчання, отриманих в інших ЗВО, регулюється Положенням про організацію освітнього процесу в ЗУНУ (https://www.wunu.edu.ua/public_information/organization-of-the-educational-process/8369-polozhennia.html), зокрема пунктом 9. Трансфер кредитів. Окрім цього, результати навчання, отримані в інших ЗВО, визнаються відповідно до Положення про визнання в ЗУНУ результатів попереднього навчання (https://www.wunu.edu.ua/pdf/pologenya/Polozhennya_ruzult_poper_navch.pdf).

Відповідно до цих документів, перезарахування результатів навчання проводиться Комісією з визнання результатів навчання кафедри на підставі заяви на ім'я декана факультету таким чином: перезарахування кредитів, які були зараховані під час навчання на інших ОП, здійснюється на підставі документів про раніше здобуту освіту (додаток до диплома, академічна довідка, свідоцтво про підвищення кваліфікації), витягу з навчальної картки, у разі одночасного навчання за декількома програмами або академічної довідки ЄКТС; переведення оцінок з однієї шкали в іншу фіксується в окремій відомості, один примірник якої знаходиться в особовій справі здобувача, другий – у відділі обслуговування студентів факультету.

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

Застосування практики визнання результатів навчання, отриманих в інших ЗВО, на цій ОП не було.

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

Питання визнання результатів навчання, отриманих шляхом неформальної освіти, регулюється Положенням про визнання в ЗУНУ результатів попереднього навчання (https://www.wunu.edu.ua/pdf/pologenya/Polozhennya_ruzult_poper_navch.pdf), зокрема пунктом 9 «Трансфер кредитів». Окрім цього, процедура визнання результатів навчання, отриманих за результатами неформальної освіти, в ЗВО регулюється цим же Положенням, зокрема пунктом 8 «Порядок визнання результатів навчання, отриманих у неформальній/інформальній освіті» (https://www.wunu.edu.ua/pdf/pologenya/Polozhennya_ruzult_poper_navch.pdf). Про всі випадки трансферу кредитів у випадку визнання неформального навчання в обсязі понад 30 кредитів ЗУНУ інформує МОН України. Доступність документу забезпечено його розміщенням на офіційному вебсайті ЗВО (https://www.wunu.edu.ua/organization-of-the-educational-process). Доступність визнання результатів неформальної та інформальної освіти, окрім внутрішніх положень, регламентується Порядком, затвердженим МОН України (Наказ № 130 від 08.02.2022 р.), та реалізується на добровільних засадах. Доступність для учасників освітнього процесу забезпечується через можливість подання заяви та проходження процедури оцінювання, що підтверджує відповідність набутих у неформальній чи інформальній освіті компетентностей програмним результатам навчання за ОП.

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

Випадків практики застосування щодо визнання результатів навчання, отриманих у неформальній освіті, на ОП не було.

4. Навчання і викладання за освітньою програмою

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

Освітній процес за ОП відповідає Закону України «Про вищу освіту» (від 01.07.2014, зі змінами) (https://zakon.rada.gov.ua/laws/show/1556-18#Text), Стандарту вищої освіти за спеціальністю (https://mon.gov.ua/osvita-2/vishcha-osvita-ta-osvita-doroslikh/naukovo-metodichna-rada-ministerstva-osviti-i-nauki-ukraini/zatverdzheni-standarti-vishchoi-osviti), Національній рамці кваліфікацій (https://zakon.rada.gov.ua/laws/show/1341-2011-п#Text). Форми та методи навчання і викладання на ОП сприяють досягненню визначених цілей та ПРН. Методи навчання на ОП диференційовано відповідно до змістового наповнення й особливостей ОК, а їх вибір і поєднання здійснюється на засадах досягнення синергетичного ефекту, що забезпечує формування ПРН, які відповідають ОП. Впровадження традиційних, інноваційних форм і методів навчання та викладання: лекції, практичні та лабораторні заняття, консультації; робота в групах, тренінги, самонавчання, екзамени, практика, презентації, проєкти – забезпечує формування критичного мислення, загальних та спеціальних компетентностей, досягнення ПРН.

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

Студентоцентрований підхід є пріоритетним у підготовці здобувачів ВО і закріплений у Положенні про організацію освітнього процесу в ЗУНУ та Стратегії розвитку ЗУНУ на 2024-2028 рр. Він реалізується через забезпечення індивідуальної освітньої траєкторії, можливість вибору дисциплін, форм навчання та права навчання за індивідуальним графіком.
Здобувачі поінформовані про цілі ОП, зміст ОК, силабуси, критерії та механізми оцінювання, а також можуть впливати на вдосконалення ОП і окремих ОК, самостійно обирати тему та керівника кваліфікаційної роботи.
Викладачі застосовують активні методи навчання, тренінги, групові й індивідуальні дослідницькі завдання. Використовуються цифрові платформи Moodle, Zoom та інші інструменти, що сприяють розвитку самостійності й відповідальності здобувачів, створено умови для вибору навчальних дисциплін.
Практикоорієнтованість забезпечується завдяки участі у практиці, що створює умови для навчання «через досвід».
Важливим є забезпечення зворотного зв'язку для визначення рівня задоволеності здобувачів методами навчання і викладання – під час зустрічей і спілкування з гарантом ОП та проведення опитувань, які дозволяють гнучко адаптувати освітній процес до потреб студентів (https://www.wunu.edu.ua/public_information/ensuring-the-quality-of-education/16345-rezultati-montoringu-jakost-osvti.html). Така модель сприяє формуванню партнерських відносин викладачів і здобувачів, розвитку їхньої автономії, креативності та готовності до безперервного навчання.

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

Принципи академічної свободи учасників освітнього процесу закріплені у Статуті ЗУНУ. Вони гарантують самостійність у дослідженнях, незалежність навчання й викладання, а також право на вільне висловлення наукових ідей. Для НПП академічна свобода означає право обирати напрями наукових досліджень, апробовувати їх результати, формувати зміст ОК, добирати методи та технології викладання, адаптуючи їх до цілей і ПРН, що враховує ступінь підготовленості і пріоритети здобувачів, організаційні та технічні можливості тощо. Це дає змогу викладачам упроваджувати інноваційні підходи, інтерактивні технології, а також гнучко реагувати на запити

здобувачів і потреби ринку праці.
Академічна свобода здобувачів реалізується через право формувати індивідуальні навчальні плани, обирати ОК варіативної частини, тематику індивідуальних, самостійних і дослідницьких завдань, методи їх виконання та форми представлення результатів. Важливим інструментом є система дистанційного навчання Moodle, яка дозволяє організовувати навчання у зручному форматі та поєднувати його з іншими видами діяльності. Крім того, здобувачі залучаються до вдосконалення ОП через анкетування, участь у робочих групах та відкриті обговорення.

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 очікуваних ПРН, порядку і критеріїв оцінювання у межах окремих ОК учасникам освітнього процесу за ОП надається на початку навчального періоду. Отримання цієї інформації є початковою точкою циклу підготовки і формування викладацьким складом силабусів та робочих програм. Інформування НПП відбувається наступним чином: зміст освітніх компонентів ОП обговорюється на засіданнях кафедри, ухвалюється групою забезпечення спеціальності та гарантом ОП, затверджується першим проректором й оприлюднюється на сайті ЗВО. Силабуси та робочі програми розміщені у вільному доступі на офіційному сайті ЗУНУ та в системі Moodle. Порядок та критерії оцінювання у межах окремих ОК регламентуються Положенням про організацію освітнього процесу в ЗУНУ (https://www.wunu.edu.ua/organization-of-the-educational-process/). Зокрема, пункт 7 «Система оцінювання навчальних досягнень здобувачів вищої освіти» містить загальні положення та інформацію про форми і порядок контролю, критерії оцінювання, порядок ліквідації академічної заборгованості, використання результатів оцінювання результатів навчання. Ця інформація конкретизуються викладачами кафедри в робочих програмах та силабусах ОК за ОП (https://www.wunu.edu.ua/master_fcit_op/)
Здобувачам така інформація надається на першому занятті з дисципліни, на якому викладач звертає увагу на цілі, зміст, очікувані результати навчання, а також знайомить здобувачів ОП з порядком і критеріями оцінювання у межах конкретного ОК.

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

Викладачі, які працюють на ОП, публікуються у високорейтингових виданнях, що входять в Q1-Q2 наукометричної бази Scopus, входять у склад Організаційного і Програмного комітетів та активно беруть участь у роботі Міжнародних конференцій ACIT (https://acit.tech), IDAACS (https://www.idaacs.net/) та інших, матеріали яких індексуються в Scopus та WoS. Здобувачі та викладачі ОП мають можливості прослухати лекції зарубіжних гостьових професорів.
ЗУНУ є організатором та співорганізатором ряду наукових заходів, які безпосередньо пов'язані з даною ОП (участь НПП і здобувачів), зокрема: XIV міжнародна науково-технічна конференція «Безпека інформаційних технологій» 22-24 травня 2025 р. (https://itsec2025.wunu.edu.ua); III Міжнародної науково-практичної конференції «Кібербезпека державних інституцій та подолання кризових станів» 14 листопада 2024 року, Київ-Тернопіль; III Безпековий форум, 25 квітня 2025 року; (https://www.wunu.edu.ua/news/27799--bezpekovij-forum.html), II безпековий форум здобувачів освіти, (https://www.wunu.edu.ua/news/25378--bezpekovij-forum-zdobuvachv-osvti.html). Здобувачі ОП доповідають та публікують результати наукових досліджень в щорічних матеріалах науково-практичного симпозіуму «Захист інформації» та матеріалах науково-практичної конференції молодих вчених, аспірантів та студентів «Кібербезпека та комп'ютерно-інтегровані технології».
НПП, які забезпечують викладання на ОП, виконують міжнародні, держбюджетні та госпдоговорні проєкти: проект ЄС «ERASMUS+ SUDEM» № 2023-1-BG01-KA220-HED-000159479» «Цифровізація процесів сталого управління катастрофами та надзвичайними ситуаціями» (термін виконання: 01.11.2023 р. до 31.10.2025 року); Розробка навчального модуля: «Кіберстійкість систем» (Яцків В.В., Цаволик Т.Г.); проєкт № БФ /4-2025 - додаткова угода до договору № БФ/4-2021 від 01.06.2021 року - «Розроблення методів та алгоритмів шифрування даних, стійких до впливу завад» (термін виконання: 01.2025 – 12.2025 р.) (Яцків В.В., Касянчук М.М., Якименко І.З., Івасьєв С.В., Кулина С.В., Цаволик Т.Г.); КБ-49-2023 «Стійкі до криптоаналізу методи та засоби шифрування в поліноміальних системах залишкових класів» (держ. реєстраційний номер: 0123U104713). Обов'язковою умовою допуску до захисту кваліфікаційної роботи є наукова активність здобувачів, що підтверджується участю в конференціях та публікацією тез. Це забезпечує системне поєднання навчання й досліджень, розвиток дослідницьких умінь та формування у здобувачів наукової культури.

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

Оновлення змісту ОК здійснюється у рамках реалізації Стратегії розвитку Західноукраїнського національного університету на 2021-2025 роки та регулюється Положенням про організацію освітнього процесу в Західноукраїнському національному університеті, Положенням про порядок перегляду (оновлення) освітніх програм (https://www.wunu.edu.ua/opp/zyao/porjadok_peregljadu_op.pdf), Положенням про систему внутрішнього забезпечення якості освіти в Західноукраїнському національному університеті (https://www.wunu.edu.ua/opp/zyao/systemu_vnutr_zabezp_yakosti_osvity.pdf).
Науково-педагогічні працівники, які забезпечують реалізацію програми, регулярно проходять стажування та підвищення кваліфікації, результати яких інтегруються у зміст освітніх компонентів і відображаються у робочих програмах, дидактичних і методичних матеріалах. Викладачі активно беруть участь у наукових і науково-методичних заходах, що дає змогу впроваджувати нові підходи та змістові блоки відповідно до сучасних потреб галузі.
У програмі використовуються результати наукових досліджень викладачів кафедри кібербезпеки: докторська дисертація М. Касянчука (2020, спеціальність 05.13.21 – системи захисту інформації), дисертація С. Кулини на

здобуття ступеня доктора філософії (2023), докторська дисертація І. Якименка (готується до захисту у 2025 р.), а також дослідження В. Яцківа та ін. «Методика виконання тестів на проникнення з використанням MITRE ATT&CK» http://immm.op.edu.ua/files/archive/n2_v15_2025/immm_n2_v15_2025.pdf, яке застосовується ОК4 «Тестування комп'ютерних систем на проникнення».
Сучасні практики впроваджуються через участь здобувачів ОП у міжнародних змаганнях CTF на платформі HackTheBox, де університетська команда входить до сотні найкращих серед понад 2000 учасників і до десятки серед команд українських університетів. На основі цих практик розроблено лабораторні завдання, які враховують кращі практики віртуальних платформ з вивчення тестування безпеки.
Тематика кваліфікаційних робіт формується на основі актуальних наукових досліджень і практичних викликів у сфері кібербезпеки та захисту інформації. Вагомим джерелом оновлення змісту освітніх компонентів є також пропозиції стейкхолдерів.
Крім того, здобувачі активно залучені до наукової діяльності через співпрацю з Радою молодих учених (https://www.wunu.edu.ua/science/young-scientists-council/) та Студентським науковим товариством (https://www.wunu.edu.ua/science/student-society/), що сприяє інтеграції сучасних наукових результатів і практик в освітній процес у ЗУНУ.

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

Інтернаціоналізація є невід'ємною складовою реалізації ОП та діяльності ЗУНУ. ЗВО має угоди про співпрацю з багатьма закордонними університетами, що забезпечує академічну мобільність викладачів і здобувачів, участь у міжнародних наукових та освітніх проєктах.
Викладачі, які викладають ОК, пройшли закордонні стажування, зокрема в університетах Республіки Польща. У 2025 р. проф. М. Касянчук взяв участь у семінарі «Розширення успішної німецько-української освітньої мережі» в Університеті прикладних наук Анхальта (Німеччина), а доц. Т. Цаволик здобув стипендію CRASP та Elsevier для підвищення дослідницького потенціалу в Глівіце (Польща). Викладачі активно беруть участь у міжнародних професійних програмах підвищення кваліфікації та отримують сертифікати провідних компаній і університетів. Зокрема, В. Яцків завершив курс «Cloud Environment Configuration And Security» (SoftServe, 2024) та програму Trust4Future в межах ініціативи EIT Deep Tech Talent (2025), С. Івасьєв отримав сертифікат SoftServe з конфігурації та безпеки хмарних середовищ (2024), а С. Кулина пройшов курс «Digital Forensics» у проєкті USAID «Кібербезпека критично важливої інфраструктури України» (2021).
Науково-педагогічні працівники програми беруть участь у міжнародних проєктах, зокрема ЄС «ERASMUS+ SUDEM» № 2023-1-BG01-KA220-HED-000159479 «Цифровізація процесів сталого управління катастрофами та надзвичайними ситуаціями», в межах якого розроблено навчальний модуль «Кіберстійкість систем» (В. Яцків, Т. Цаволик).

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

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

Форми контрольних заходів та критерії оцінювання здобувачів вищої освіти за ОП спрямовані на перевірку досягнення ПРН як на рівні окремих освітніх компонентів, так і програми в цілому. Відповідно до п. 7 «Положення про організацію освітнього процесу в ЗУНУ», система оцінювання включає поточний, модульний та підсумковий контроль.
Поточний контроль здійснюється в межах аудиторних занять і передбачає тестування, розв'язання практичних завдань, презентації, усні відповіді та виконання лабораторних робіт. Це дозволяє оцінювати засвоєння окремих результатів навчання й формування практичних умінь. Модульний контроль забезпечує комплексну перевірку сформованості компетентностей у межах тематичних блоків ОК. Підсумковий контроль (заліки, іспити, захист звітів із практики та кваліфікаційної роботи) дає можливість оцінити рівень досягнення ПРН як у межах конкретного освітнього компонента, так і програми загалом.
Методи поточного та підсумкового контролю, а також критерії оцінювання визначені у робочих програмах і силабусах освітніх компонентів. Результати є відкритими для здобувачів у локальній мережі університету через персональні облікові записи, що гарантує прозорість і доступність.
Така система дозволяє оцінювати не лише знаннєвий компонент підготовки, а й практичні, дослідницькі та комунікативні навички, що забезпечує комплексну перевірку досягнення ПРН й відповідність програми її задекларованій меті.

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

Форми контрольних заходів та критерії оцінювання навчальних досягнень здобувачів регламентуються Положенням про організацію освітнього процесу в ЗУНУ та відображаються у робочих програмах дисциплін і силабусах. Це забезпечує їх чіткість, прозорість та зрозумілість для всіх учасників освітнього процесу.
Прозорість реалізується через комплекс заходів: розробку критеріїв оцінювання на рівні кафедр, їх погодження групою забезпечення спеціальності, систематичне роз'яснення здобувачам під час навчання, проведення методичних семінарів для викладачів, функціонування механізмів апеляції та повторного складання контрольних заходів.

Кожен викладач на першому занятті інформує студентів про форми контролю та критерії оцінювання у межах дисципліни. Критерії деталізовані у робочих програмах і містять кількісні показники (бали за окремі види діяльності), що дозволяє здобувачам чітко розуміти систему нарахування балів. Робочі програми і силабуси оприлюднені на сайті університету у відкритому доступі, а також на початку семестру викладачі завантажують робочу програму та силабус на платформу Moodle.
Для перевірки об'єктивності оцінювання застосовується моніторинг думок здобувачів, результати якого враховуються у вдосконаленні практики оцінювання. Такий підхід гарантує зрозумілість вимог та довіру до результатів контролю, що сприяє академічній доброчесності й справедливості в освітньому процесі

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

Інформування здобувачів про форми контрольних заходів та критерії оцінювання здійснюється завчасно та у кілька етапів.
• Попереднє інформування щодо форм контрольно-оцінювальних процедур та критеріїв оцінювання за кожним ОК здійснюється через ознайомлення здобувачів з робочими навчальними програмами та силабусами, що оприлюднюються на офіційному вебресурсі університету.
• На початку освітнього процесу викладач на першому занятті детально роз'яснює студентам форми контролю, порядок та критерії оцінювання результатів навчання з конкретної ОК.
• Строки контрольних заходів регламентуються графіком освітнього процесу й розкладом занять, які затверджуються адміністрацією університету та оприлюднюються на офіційному сайті до початку семестру (https://www.wunu.edu.ua/timetable/?do=cat&category=timetable/). Семестровий контроль (екзамени, заліки) з відповідного ОК реалізується в обсязі навчального матеріалу, визначеного його робочою програмою, у терміни, встановлені навчальним планом, індивідуальним навчальним планом здобувача та розкладом занять.
• Поточне інформування здійснюється через Moodle та інформаційні повідомлення, що надаються відділом обслуговування студентів факультету комп ' ютерних інформаційних технологій та викладачами кафедри.

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

Форми атестації здобувачів вищої освіти за даною ОП регламентуються Стандартом вищої освіти України, затвердженого наказом МОН України від 18 березня 2021 р., № 332, з урахуванням зміни назви спеціальності 125 Кібербезпека та захист інформації (Постанова Кабінету Міністрів України від 16 грудня 2022 р., № 1392) та Положенням про організацію освітнього процесу в ЗУНУ (https://www.wunu.edu.ua/organization-of-the-educational-process/). Процедури проведення атестації випускників визначаються Положенням про порядок створення та організацію роботи екзаменаційних комісій з атестації здобувачів вищої та фахової передвищої освіти ЗУНУ (https://www.wunu.edu.ua/pdf/pologenya/pol_pro_org%20rob-ekzam-kom.PDF).
Підсумкова атестація здобувачів вищої освіти за ОП реалізується через підготовку та захист кваліфікаційної роботи. Кваліфікаційна робота має розв'язувати складну задачу інформаційної безпеки та/або кібербезпеки і передбачати проведення досліджень та/або здійснення інновацій. Кваліфікаційна робота не повинна містити академічного плагіату, фабрикації, фальсифікації. Кваліфікаційна робота має бути розміщена у репозитарії ЗУНУ. Оприлюднення кваліфікаційних робіт з обмеженим доступом здійснюється відповідно до вимог законодавства. Атестація здійснюється відкрито і публічно.

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

Процедури здійснення контрольно-оцінювальних заходів регламентуються Положенням про організацію освітнього процесу в ЗУНУ та Положенням про порядок створення та організацію роботи екзаменаційних комісій з атестації здобувачів вищої та фахової передвищої освіти ЗУНУ. Процедурні аспекти проведення контрольних заходів з кожного ОК деталізуються у робочих програмах та силабусах, які розробляються науково-педагогічними працівниками кафедри, обговорюються на засіданнях кафедри та затверджуються відповідно до встановленого порядку. На початку навчального семестру науково-педагогічні працівники здійснюють інформування здобувачів освіти щодо процедур проведення контрольних заходів. Робочі програми дисциплін оприлюднено на офіційному вебсайті університету (https://www.wunu.edu.ua/master_fcit_op/). Результати анкетування здобувачів підтверджують їх повну обізнаність щодо форм контрольних заходів і критеріїв оцінювання.

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

Об'єктивність оцінювання результатів навчання забезпечується комплексом процедур, закріплених у Положенні про організацію освітнього процесу в ЗУНУ та Кодексі академічної доброчесності. Форми контролю та критерії оцінювання визначаються у робочих програмах і силабусах, які обговорюються та затверджуються на кафедрі. Це виключає можливість довільного трактування вимог і забезпечує прозорість для здобувачів.
У разі виникнення сумнівів щодо об'єктивності екзаменатора або наявності конфлікту інтересів здобувач має право подати заяву на ім'я декана факультету. За рішенням адміністрації створюється комісія з проведення іспиту, до складу якої входять щонайменше три викладачі, у тому числі незалежні від дисципліни. Цей механізм гарантує справедливість оцінювання. Здобувачі поінформовані про зазначені процедури через роз'яснення викладачів на початку семестру, спеціальні зустрічі з відповідальними особами для роз'яснення питань протидії корупції та

механізмів вирішення конфліктних ситуацій у процесі навчання. Результати опитування здобувачів ОП другого (магістерського) рівня вищої освіти «Рівень об'єктивності оцінювання» (https://tinyurl.com/3b83eyuw) свідчать про їхню поінформованість щодо правових механізмів і відсутність зафіксованих випадків конфлікту інтересів на ОП, відповіді підтверджують об'єктивність оцінювання рівня знань студентів під час екзаменів.
За період функціонування даної ОП випадків оскарження об'єктивності екзаменаторів не зафіксовано.

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

• Порядок повторного проходження контрольних заходів визначається згідно Положення про організацію освітнього процесу в ЗУНУ. Перескладання негативних результатів поточного та модульного контролю (чи неявок без поважних причин) дозволяється до дати проведення наступного модуля. У разі перескладання позитивна оцінка не може перевищувати рівень «задовільно».
• Здобувачам, які мають із ОК семестрову оцінку «незадовільно» (від 35 до 59 балів «FX» (незадовільно з можливістю повторного складання)) або не з'явилися на екзамен, дозволяється ліквідувати академічну заборгованість максимум за два перескладання (викладачу та комісії) після завершення сесії за заявою, поданою у відділ обслуговування студентів факультету, та відповідно до графіку ліквідації академічної заборгованості. Якщо здобувач отримав більше двох незадовільних оцінок із дисциплін, він підлягає відрахуванню за академічну неуспішність.
• Здобувачі, які отримали з ОК семестрову оцінку «незадовільно» від 1 до 34 балів «F» (незадовільно з обов'язковим повторним курсом) зобов'язані написати заяву про повторне вивчення дисципліни на умовах отримання додаткових консультацій у позаурочний час.
Усі повторні контрольні заходи проводяться у формах, аналогічних первинним (письмовий/усний іспит, захист звіту тощо). Результати ліквідації академічної заборгованості заносяться у відомість обліку успішності та автоматизовану систему супроводу освітнього процесу. Практика повторного проходження контрольних заходів за ОП відсутня.

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

ЗУНУ регулює процес оскарження процедури та результатів проведення контрольних заходів, що здійснюється відповідно до «Положення про організацію освітнього процесу ЗУНУ», Порядку оскарження результатів підсумкового контролю університету та іншими внутрішніми документами ЗВО.
Апеляції щодо поточних результатів подаються в день екзамену на ім'я декана факультету, після чого створюється комісія для вивчення обставин. У випадку незгоди з оцінкою з підсумкової атестації, здобувач має право подати апеляцію упродовж 12 годин наступного робочого дня на ім'я ректора. Розпорядженням ректора апеляційна комісія розглядає звернення протягом трьох робочих днів.
Здобувачі вищої освіти, які не захистили кваліфікаційну роботу у зв'язку з неявкою без поважних причин або отриманням незадовільної оцінки, мають право за окремим договором про надання освітніх послуг на повторну (з наступного навчального року) підсумкову атестацію протягом трьох років після відрахування з університету. У разі встановлення академічного плагіату повторний захист кваліфікаційної роботи на ту ж тему не допускається.
Застосування процедури оскарження результатів контрольних заходів на даній ОП не було.

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

Політика академічної доброчесності в університеті регламентується комплексом локальних документів та етичних принципів, що визначають організацію освітнього процесу та правила наукової й освітньої діяльності.
Відповідальність за впровадження та виконання вимог академічної доброчесності покладається на спеціалізовані комісії, структурні підрозділи (у межах їхніх повноважень), та адміністрацію закладу. У ЗУНУ також функціонує система особистих зобов'язань здобувачів і науково-педагогічних працівників щодо дотримання норм академічної доброчесності (https://www.wunu.edu.ua/past-and-present/academic-integrity/16284-akademchna-dobrochesnst.html).

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

Як превентивні заходи в контексті попередження академічної недоброчесності використовуються: інформування здобувачів вищої освіти про неприпустимість плагіату; проведення тренінгів для науково-педагогічних працівників та здобувачів освіти; формування тематики кваліфікаційних робіт, що зменшує можливості плагіату; перевірка текстів на унікальність.
На ОП як інструмент протидії порушенням академічної доброчесності застосовується спеціалізований онлайн-сервіс Strikeplagiarism для пошуку запозичених текстових фрагментів з відкритих джерел в мережі Інтернет чи внутрішньої бази документів ЗУНУ (https://www.wunu.edu.ua/pdf/academ_dob/Strikeplagiarism.PDF). Перевірка здійснюється відповідно до установчих документів з академічної доброчесності ЗУНУ (https://www.wunu.edu.ua/past-and-present/academic-integrity/16284-akademchna-dobrochesnst.html)
Кваліфікаційні роботи здобувачів другого (магістерського) рівня освіти розміщені в репозиторії за посиланням: https://dspace.wunu.edu.ua/handle/316497/834

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

Популяризація академічної доброчесності серед здобувачів вищої освіти є складником стратегії розвитку ЗУНУ та

здійснюється комплексно.
З 2016 р. ЗУНУ є учасником проєкту SAIUP – Проєкт сприяння академічній доброчесності в Україні, реалізованого Американськими Радами з міжнародної освіти за підтримки МОН України та Посольства США. У його рамках було започатковано низку тренінгів і публічних дискусій для студентів.
Університет систематично організовує просвітницькі заходи: вебінари, лекторії, семінари (https://www.youtube.com/@librarywunu3365/videos), зустрічі з експертами з питань академічної етики. Такі активності формують у здобувачів культуру доброчесності та запобігають недобросовісним практикам.
Також питання академічної доброчесності інтегровані в освітній процес: відповідні положення включено до силабусів дисциплін, у завданнях передбачено посилання на джерела, перевірку текстів на плагіат, розвиток навичок академічного письма. У ЗВО передбачена обов'язкова перевірка на плагіат на етапі допуску до захисту всіх дисертаційних робіт на здобуття ступеня магістра. За наявності критичних запозичень робота до захисту не допускається. Головна роль у профілактиці порушень академічної доброчесності здобувачами покладається на наукових керівників.

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

Університет керується Кодексом академічної доброчесності та наукової етики (https://www.wunu.edu.ua/pdf/academ_dob/kodeks-akadem-dobrochesnost.pdf).
Для моніторингу дотримання норм функціонує Комісія з доброчесності та наукової етики як дорадчий орган з правом розгляду заяв щодо порушень та надання пропозицій щодо санкцій (https://www.wunu.edu.ua/pdf/academ_dob/pologenya_ac_dob.PDF).
Організаційною формою діяльності Комісії є засідання для вирішення оперативних питань. Рішення приймаються відкритим голосуванням з оформленням протоколу, який підписується усіма членами комісії. За результатами розгляду справи Комісія готує письмовий висновок щодо наявності факту порушення Кодексу з рекомендаціями.
Санкції за порушення академічної доброчесності педагогічними, науково-педагогічними, науковими працівниками та здобувачами освіти детально описані у п. 5 «Академічна відповідальність» Кодексу академічної доброчесності ЗУНУ (нова редакція) (https://www.wunu.edu.ua/pdf/academ_dob/kodeks-akadem-dobrochesnost.pdf).
За порушення академічної доброчесності здобувачі освіти Університету можуть бути притягнені до такої академічної відповідальності: повторне оцінювання; повторне проходження освітнього компоненту ОП; відрахування із ЗВО; позбавлення академічної стипендії; позбавлення наданих закладом освіти пільг з оплати за навчання.
За період функціонування ОП прецедентів порушень академічної доброчесності здобувачами не зафіксовано.

6. Людські ресурси

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

Кадрове забезпечення освітньої діяльності за ОП здійснюється на основі Наказу МОН України «Про затвердження Рекомендацій щодо проведення конкурсного відбору при заміщенні вакантних посад науково-педагогічних працівників та укладання з ними трудових договорів (контрактів)» (http://wunu.edu.ua/pdf/doc_zunu/nauka/НАКАЗ%20МОН%20від%2005%20жовтня%202015%20року.pdf), Статуту ЗУНУ (https://www.wunu.edu.ua/pdf/licensing_accreditation/statut_zunu.pdf), Порядку проведення конкурсного відбору при заміщенні вакантних посад науково-педагогічних працівників та укладання з ними трудових договорів (контрактів) (http://wunu.edu.ua/pdf/doc_zunu/nauka/Порядок%20проведення%20конкурсного%20відбору%20.pdf). Конкурсні вимоги передбачають оцінювання науково-дослідної та навчально-методичної діяльності претендентів на відповідність кваліфікаційним критеріям. Претенденти зобов'язані надати матеріали, що підтверджують їх професійні досягнення та відповідність вимогам, встановленим законодавством й освітньою програмою. Оголошення про конкурс публікуються на офіційному сайті університету. Компетенція щодо визначення відповідного фахового рівня викладача покладається на профільну кафедру, гаранта ОП та групу забезпечення спеціальності. Від НПП вимагається не лише відповідна кваліфікація згідно з п. 37, 38 Ліцензійних умов провадження освітньої діяльності та Рекомендацій Національного агентства, але й підтверджений досвід участі в наукових дослідженнях, міжнародних проєктах, а також систематична публікаційна активність. Викладачі, які забезпечують ОП, також зобов'язані регулярно (як мінімум, один раз за п'ять років) підвищувати свою кваліфікацію в Україні або за кордоном, що забезпечує актуалізацію їхніх знань і впровадження освітніх технологій.

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

Процедури конкурсного відбору викладачів, відповідно до Порядку проведення конкурсного відбору при заміщенні вакантних посад науково-педагогічних працівників та укладання з ними трудових договорів (контрактів) (http://wunu.edu.ua/pdf/doc_zunu/nauka/Порядок%20проведення%20конкурсного%20відбору%20.pdf) побудовані на прозорих і недискримінаційних принципах. Кожен етап конкурсного відбору, включаючи подання заявок, оцінювання кваліфікацій та досягнень, є чітко визначеним та структурованим. Основними вимогами до кандидатів є наявність науково-педагогічного досвіду та відповідність кваліфікаційним вимогам, передбачених освітньою

програмою. Процес конкурсного відбору забезпечує прозорість через відкриті оголошення про вакансії та чіткі критерії оцінювання кандидатів. Це сприяє мінімізації можливостей для дискримінації та зловживань. Також передбачено послідовне застосування процедур конкурсного відбору для кожної посади, що гарантує однакові умови для всіх учасників та стабільний рівень професіоналізму викладачів. Завдяки такому підходу забезпечується успішна реалізація ОП, оскільки відбір здійснюється відповідно до актуальних вимог до професійних компетенцій, необхідних для забезпечення високого рівня освітнього процесу.

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

ЗУНУ активно залучає роботодавців до організації і реалізації освітнього процесу, використовуючи їх практичні навички і науковий потенціал для формування відповідних спеціальних компетентностей здобувачів освіти. Важливим моментом залучення роботодавців є укладання договорів про проходження переддипломної практики здобувачами ОП.
Роботодавці також беруть участь в обговоренні проєктів ОП, актуальних питань підготовки магістрів зі спеціальності, долучаються до обговорення тематики кваліфікаційних робіт і проведення атестації здобувачів. До організації та реалізації ОП 2025 р. залучались:
Олена Волощук, к.т.н., доцент, керівник освітнього департаменту Distributed Lab; Дмитро Узун, к.т.н, доцент, ментор СофтСерв Академія; Софія Цезарук, інспектор ВПК в Тернопільській області Департаменту Кіберполіції Національної поліції України; Максим Серватнюк, старший оперуповноважений відділу протидії кіберзлочинам в Тернопільській області Департаменту кіберполіції Національної поліції України.
В рамках VI Міжнародного тижня ЗУНУ проводились лекції: «Інформаційні технології – рушійні сили змін» професор Артур Рот, завідувач кафедри інформаційних систем Вроцлавського університету економіки та бізнесу (Польща); «Публікаційні стратегії для молодих науковців та аспірантів» професор Вольфганг Дорнер, віце-президент з наукової роботи Деггендорфського технологічного інституту (Німеччина) та ряд онлайн вебінарів в рамках проєкту USAID «Кібербезпека критично важливої інфраструктури України».

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

Відповідно до нормативних документів щодо підвищення кваліфікації науково-педагогічних працівників для забезпечення професійного фахового розвитку викладачів застосовуються різні види підвищення кваліфікації як в Україні, так і за її межами. Викладачі, які працюють на ОП, пройшли закордонне стажування, зокрема: Касянчук М.М., Якименко І.З., Івасьєв С.В. (Університет у Бєльсько-Бялій, Польща), Кулина С.В. (Університет комісії національної освіти в Кракові, Польща). Стажування здійснюється на основі річного Плану підвищення кваліфікації професорсько-викладацького складу за індивідуальними планами. Результати науково-педагогічних стажувань обговорюються на засіданнях кафедри і впроваджуються в освітній процес у частині оновлення змісту ОК, урізноманітнення форм та методів навчання тощо. Крім того, ЗУНУ провадить ініціативи щодо розвитку та підвищення кваліфікації своїх працівників через проведення семінарів, науково-практичних конференцій. Зокрема, проф. Касянчук М.М. в липні 2025 р. взяв участь у семінарі «Розширення успішної німецько-української освітньої мережі», що проходив на базі Університету прикладних наук Анхальта, м.Кьотен, Німеччина. В межах семінару проф. Касянчук М.М. провів гостьову лекцію.
Університет сприяє участі викладачів ОП у міжнародних наукових конференціях, зокрема: проф. Яцків В.В., доц. Якименко І.З. взяли участь в роботі міжн. конф. «Advanced Computer Information Technologies» 17 – 19 вересня 2025 року, м. Шибеник, Республіка Хорватія.

Наведіть конкретні приклади заохочення розвитку викладацької майстерності

Система заходів щодо заохочення розвитку викладацької майстерності в ЗУНУ охоплює матеріальні й моральні заохочення і регламентується Статутом Університету, Колективним договором між адміністрацією та комітетом первинної профспілкової організації, Положенням про преміювання наукових і науково-педагогічних працівників ЗУНУ. Матеріальне стимулювання НПП здійснюється за високі рейтингові показники у системі внутрішнього оцінювання, підготовку кадрів вищої кваліфікації, видання монографій/підручників, опублікування статей у виданнях Scopus і Web of Science, створення винаходу (корисної) моделі, наявність відомчої відзнаки «За наукові та освітні досягнення», звання «Почесний професор ЗУНУ». Гаранту ОП в академічне навантаження враховується 50 год. Моральні заохочення застосовують за вагомі успіхи у науково-педагогічній діяльності у таких формах: оголошення подяки ректора, грамоти, подання адміністрації ЗУНУ на відзначення регіональними та відомчими відзнаками. Зокрема, НПП з даної ОП були премійовані та відзначені грамотами ректора, подяками Тернопільської міської ради та обласної державної адміністрації. Професор М. Касянчук нагороджений Подякою МОН України. Крім університетських заохочень, проф. Яцків В.В., проф. Касянчук М.М. і доц. Якименко І.З. отримали подяки від НДІ воєнної розвідки України.

7. Освітнє середовище та матеріальні ресурси

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

Матеріально-технічні, фінансові ресурси, навчально-методичне забезпечення та бібліотечний фонд ЗУНУ відповідають ліцензійним умовам і забезпечують досягнення цілей, визначених ОП та її програмних результатів. В освітньому процесі ЗУНУ використовуються навчальні аудиторії з мультимедійним обладнанням та навчальні комп'ютерні лабораторії, оснащені сучасною технікою і ліцензійним та вільнорозповсюдженим програмним забезпеченням, підключені до внутрішньої мережі з можливістю Інтернет-з'єднання. Здобувачі ОП мають доступ, як з локальної мережі так і через VPN з'єднання, до віртуальної лабораторії побудованої на базі кіберполігону, для набуття практичних навиків, що забезпечують результати ОП. На усій території університету забезпечується вільний та безкоштовний доступ до WiFi для можливості підключення до мережі Інтернет та внутрішньої корпоративної мережі. У ЗУНУ функціонує бібліотека (https://library.wunu.edu.ua), інформаційні ресурси якої забезпечують потреби здобувачів у фаховій та навчально-методичній літературі, необхідної для реалізації цілей ОП. Для забезпечення академічної доброчесності в наукових роботах здобувачів вищої освіти працює система перевірки текстів на плагіат Turnitin Similarity. Навчально-методичне забезпечення ОК відповідає цілям ОП завдяки постійному оновленню матеріалів та адаптації їх змісту до тенденцій в сфері кібербезпеки та захисту інформації. Навчально-методичні матеріали доступні здобувачам вищої освіти в системі дистанційного навчання Moodle.

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

Західноукраїнський національний університет забезпечує викладачам і здобувачам вільний доступ до відповідної інфраструктури та інформаційних ресурсів відповідно до Закону України «Про вищу освіту», Ліцензійних умов провадження освітньої діяльності та інших законодавчих актів. Матеріально-технічна база освітнього середовища і вільний доступ до інформаційних ресурсів через електронні платформи (MOODLE) для організації навчання, доступ до наукових баз даних і електронних бібліотек, а також лабораторії та комп'ютерні класи для проведення практичних та лабораторних занять і наукових досліджень дозволяє задовольнити потреби здобувачів і викладачів. Крім того, університет надає доступ до інтернету, організовує наукові дослідження через співпрацю з іншими науковими установами, а також створює умови для дистанційного навчання через онлайн-курси та матеріали. Для науковців на сайті бібліотеки розміщені покликання на офіційні сайти наукометричних баз (Scopus, Web of Science, ін.). НПП додають у репозитарій свої наукові доробки (https://dspace.wunu.edu.ua/), користуються під час написання власних статей розміщеними там працями колег, рекомендують здобувачам ВО користуватися ним під час вивчення ОК та під час написання статей та кваліфікаційних робіт.

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

Освітнє середовище у ЗУНУ задовольняє потреби та інтереси здобувачів вищої освіти за ОП через надання вільного доступу до інформаційних ресурсів та методичних матеріалів, необхідних для навчання, а також можливості користування інфраструктурою університету (бібліотека, гуртожитки, спортивний центр, їдальні, кафе). Для задоволення освітніх потреб здобувачів у вільному доступі знаходяться два комп'ютерні зали бібліотеки ЗУНУ, обладнані комп'ютерами з доступом до мережі Інтернет. В освітньому процесі використовуються навчальні аудиторії загальноуніверситетської навчальної комп'ютерної лабораторії, обладнані сучасним комп'ютерним та мультимедійним обладнанням. Реалізацію наукових інтересів здобувачів вищої освіти здійснює студентське наукове товариство. Для особистісного розвитку та втілення навчальних інтересів здобувачів ОП доступні різні фахові гуртки та спортивні секції, виставкова зала, актова зала та студія звукозапису. Врахування потреб та інтересів здобувачів вищої освіти здійснюється шляхом систематичного опитування рівня задоволеності організацією освітнього процесу та його ресурсним забезпеченням у рамках реалізації ОП. У ЗУНУ працюють фахівці соціально-психологічної підтримки, котрі надають кваліфіковану допомогу у вирішенні соціально-психологічних проблем учасників освітнього процесу (https://www.wunu.edu.ua/centers/nncsppr/). Крім того, організаційно-виховної заходи із здобувачами ОП систематично проводяться кураторами академічних груп.

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

У ЗВО для здобувачів ОП постійно діє комплекс заходів для забезпечення комфортних умов проживання, проведення занять, проходження практики, надання консультацій, доступ до усіх інформаційних ресурсів, передбачених ОК. До послуг викладачів і здобувачів медичний пункт, а також кабінети лікувальної фізкультури, емоційного розвантаження, психотерапії, їдальні, кафе тощо. У ЗВО проводяться круглі столи, відкриті лекції та роз'яснювальна робота про етіологію булінг-акту, форми захисту від психологічного насильства, протидію нарко-, алкозалежності та тютюнопаління. Для вирішення психологічних проблем у ЗВО працює Навчально-науковий центр соціально-психологічної підтримки та резильєнтності ЗУНУ (https://www.wunu.edu.ua/centers/nncsppr/). Також зі здобувачами ОП виховну та роз'яснювальну роботу проводить гарант ОП та куратор академічної групи. Для забезпечення безпеки під час повітряних тривог усі навчальні та адміністративні будівлі обладнані належними укриттям з необхідною кількістю людино-місць. В укриттях присутня у вільному доступі вода, харчові продукти тривалого зберігання та медикаменти для надання невідкладної допомоги. Для орієнтування у внутрішньому просторі приміщень наявні необхідні вказівники та світлова індикація для аварійних виходів. У корпусах знаходяться портативні дефібрилятори.

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)

Згідно з ч. 2 ст. 30 Закону України «Про освіту» пункту про умови доступності закладу освіти для навчання осіб з особливими освітніми потребами в ЗВО проведено обстеження будівель та прилеглої до них території (https://www.wunu.edu.ua/logistics/) з метою визначення доступності навчальних приміщень для осіб з особливими освітніми потребами та інших маломобільних груп населення (МГН), враховуючи вимоги та нормативи Державних будівельних норм України «ДБН В.2.2-3:2018 Будинки і споруди. Заклади освіти»; ДСТУ-Н В.2.2-31-2011 «Настанова з облаштування будинків і споруд громадського призначення елементами доступності для осіб з вадами зору та слуху» та інших нормативно-правових документів, що регулюють забезпечення доступності навчальних приміщень для осіб з інвалідністю та інших маломобільних груп населення. Для доступності до навчальних приміщень для осіб з інвалідністю та інших маломобільних груп населення створено відповідні умови стосовно встановлених вимог (згідно із звітом від 1 жовтня 2020 року про проведення технічного обстеження стану забезпечення доступності навчальних приміщень ЗУНУ та його відокремлених підрозділів для осіб з інвалідністю та інших маломобільних груп населення) та Порядком супроводу (надання допомоги) осіб з інвалідністю та інших маломобільних груп населення у ЗУНУ та його відокремлених підрозділах, затвердженому наказом ректора ЗУНУ від 26 березня 2021 року № 129. Особи з особливими освітніми потребами на ОП не навчаються.

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

Антикорупційна політика проводиться відповідно до Антикорупційної програми ЗУНУ на 2024-2026 роки (www.wunu.edu.ua/corruption/2024/1_antukor_prog_2024.pdf). Для коригування роботи з даного напрямку призначається Уповноважений з антикорупційної діяльності (www.wunu.edu.ua/prevention-of-corruption/). Основними завданнями Уповноваженого є: підготовка, забезпечення та контроль за здійсненням заходів щодо запобігання корупції в Університеті, надання методичної та консультаційної допомоги з питань дотримання вимог антикорупційного законодавства працівникам, проведення організаційної та роз'яснювальної роботи із запобігання, виявлення і протидії корупції, здійснення контролю за дотриманням вимог законодавства щодо врегулювання конфлікту інтересів, здійснення контролю за дотриманням антикорупційного законодавства. Врегулювання конфліктних ситуацій між учасниками освітнього процесу в ЗУНУ регламентується Положенням про порядок врегулювання конфлікту інтересів та Положенням про політику та процедури врегулювання конфліктних ситуацій. У своїй діяльності ЗУНУ дотримується принципів цінності свободи, справедливості та безпеки, рівності прав і можливостей, інклюзивності, толерантності, недискримінації, відкритості та прозорості. Кожен учасник освітнього процесу має право на захист від будь-яких форм фізичного та психологічного насильства. Якщо здобувач вважає, що стосовно нього було порушено його права або здійснено протиправні дії, він може подати письмову скаргу до Комісії з врегулювання конфліктних ситуацій в електронному чи паперовому вигляді. Крім того, здобувачі ОП можуть скористатися скринькою довіри для письмового звернення у випадку виникнення конфліктної ситуації. Для надання професійної психологічної допомоги здобувачам вищої освіти та профілактики виникнення конфліктних ситуацій, проявів насилля і булінгу у ЗУНУ функціонує Навчально-науковий центр соціально-психологічної підтримки та резильєнтності. За період реалізації ОП випадків звернень стосовно вирішення конфліктних ситуацій, в тому числі пов'язаних із сексуальними домаганнями, корупцією, дискримінацією, 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 на своєму вебсайті

В ЗУНУ процедури розроблення, затвердження, моніторингу та періодичного перегляду ОП регулюються Положенням про систему внутрішнього забезпечення якості освіти в ЗУНУ (https://www.wunu.edu.ua/opp/zyao/systemu_vnutr_zabezp_yakosti_osvity.pdf); Положенням про організацію освітнього процесу (https://www.wunu.edu.ua/public_information/organization-of-the-educational-process/), Положенням про освітні програми (https://www.wunu.edu.ua/opp/zyao/pologenya_pro_OP.pdf), Порядком перегляду (оновлення) освітніх програм (https://www.wunu.edu.ua/opp/zyao/porjadok_peregljadu_op.pdf).

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 відбувається відповідно до Положення про систему внутрішнього забезпечення якості освіти в ЗУНУ (https://www.wunu.edu.ua/opp/zyao/systemu_vnutr_zabezp_yakosti_osvity.pdf) та регламентується Положенням про організацію освітнього процесу в ЗУНУ (https://www.wunu.edu.ua/public_information/organization-of-the-educational-process/) та Положенням про порядок перегляду (оновлення) освітніх програм (https://www.wunu.edu.ua/opp/zyao/porjadok_peregljadu_op.pdf) .
Підставою для оновлення ОП є ініціатива і пропозиції гаранта ОП та викладачів, які її реалізують, а також пропозиції здобувачів вищої освіти та стейкхолдерів.
Так, в ОП 2025 р. було враховано побажання здобувачів вищої освіти, пропозиції академічної спільноти та стейкхолдерів, зокрема: внесено зміни у ОК6; доповнено каталог вибіркових дисциплін та розширено тематику

кваліфікаційних робіт за напрямом моделювання кібератак та систем проактивного захисту.
Перегляд ОП також відбувається при зміні вимог державних стандартів освіти, стратегії розвитку університету, інших нормативних документів. Моніторинг організації освітнього процесу здійснюється систематично через анкетування здобувачів щодо задоволеності якістю навчання, методами викладання, прозорістю оцінювання та дотриманням принципів академічної доброчесності. Результати підтверджують відповідність освітнього процесу належному рівню та визначають напрями для подальшого удосконалення ОП.

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

Здобувачі вищої освіти за ОП активно залучені до процесу її періодичного перегляду та до інших процедур забезпечення якості. Їхня думка враховується через різні інструменти зворотного зв'язку, що діють на постійній основі.
За пропозицією здобувачки Анастасії Гнатюк внесено зміни в ОК6, які спрямовані на вивчення математичних засад постквантових криптосистем.
Крім індивідуальних ініціатив, у ЗУНУ систематично проводиться анонімне анкетування здобувачів з питань організації освітнього процесу, якості викладання, прозорості оцінювання, дотримання принципів академічної доброчесності. Результати опитувань узагальнюються і враховуються робочою групою під час оновлення ОП.
Здобувачі мають можливість брати участь у розширених засіданнях кафедри кібербезпеки та зустрічах із гарантом ОП, де обговорюються проєкти програми та робочі програми освітніх компонентів.
Крім того, здобувачі ознайомлені з робочими програмами та силабусами дисциплін (https://www.wunu.edu.ua/master_fcit_op/) і мають можливість вносити пропозиції щодо їх удосконалення.

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

Відповідно до вимог Закону України «Про вищу освіту» здобувачі залучаються до процедур внутрішнього забезпечення якості ОП в ЗУНУ, що відбувається через Університетську раду студентів, раду молодих вчених університету, вчених рад факультету та університету (https://www.wunu.edu.ua/studentske-samovriaduvannia-urs/).
Згідно з Положенням про студентське самоврядування ЗУНУ (https://www.wunu.edu.ua/pdf/doc_zunu/pologennya_str_pidr/polozhennja-pro-studentske-samovrjaduvannja-zunu.PDF), органи студентського самоврядування мають право: виносити пропозиції щодо контролю за якістю освітнього процесу; сприяти навчальній, науковій та творчій діяльності здобувачів; брати участь у вирішенні конфліктних ситуацій; спільно з відповідними структурними підрозділами університету сприяти забезпеченню інформаційної, правової, психологічної, фінансової, юридичної та іншої допомоги здобувачам; мають право бути представниками в колегіальних та робочих органах університету; вносити пропозиції щодо змісту навчальних планів та програм. Органи студентського самоврядування зобов'язані аналізувати та узагальнювати зауваження та пропозиції здобувачів щодо організації освітнього процесу і звертатися до адміністрації з пропозиціями щодо їх вирішення. Адміністрація та інші посадові особи ЗУНУ, за поданням виконавчого органу студентського самоврядування, зобов'язані вчасно та у повному обсязі інформувати самоврядування ЗУНУ про рішення, що стосуються безпосередньо здобувачів університету.

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

Інтереси роботодавців враховуються під час формування цілей і ПРН як у процесі розробки, так і під час періодичного перегляду ОП. Обговорення ОП відбувається на розширених засіданнях кафедри за участі провідних фахівців у сфері кібербезпеки та захисту інформації. За результатами таких зустрічей рекомендації роботодавців інтегруються у зміст лекційних і практичних занять, уточнюється структура навчальних планів, коригується тематика кваліфікаційних робіт та ін.
Зокрема, у 2025 році з урахуванням пропозицій стейкґолдерів було внесено такі зміни:
• в ОК7 «Цифрова криміналістика» розроблено лабораторні роботи, пов ′язані з розслідуванням кіберінцидентів та виявленням криптографічних доказів (ВПК в Тернопільській області Департаменту Кіберполіції Національної поліції України);
• до каталогу вибіркових дисциплін включено курс «Управління та захист хмарних інфраструктур», ініційований фахівцями IT-компанії SoftServe.
Ці та інші пропозиції стейкхолдерів були враховані під час оновлення ОП у 2025 році, що підтверджує реальний вплив роботодавців на зміст та якість підготовки здобувачів.

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

У ЗУНУ функціонує система зв'язків із випускниками, яка включає в себе збір та аналіз інформації про професійну діяльність випускників. Безпосередній зв'язок з випускниками реалізується шляхом особистісного спілкування працівників, відповідальних за профорієнтаційну роботу кафедри. В університеті щорічно проводять дні інститутів та факультетів, дні відкритих дверей, круглі столи, форуми, ярмарки вакансій, на які запрошуються випускники різних років. Додатковим інструментом підтримки зв'язку з випускниками є неформальні комунікаційні платформи (зокрема онлайн-групи), що дає змогу відстежувати їхній кар'єрний поступ та залучати до подальшої співпраці.

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

У ЗУНУ функціонує Науково-методична рада з питань якості вищої освіти та Комісія з моніторингу якості освіти, котра аналізує та узагальнює результати діяльності структурних підрозділів ЗУНУ із забезпечення якості освіти; організовує та проводить семінари, інструктивні заняття та наради з питань моніторингу якості освіти; взаємодіє з органами студентського самоврядування з питань організації й аналізу результатів моніторингу освітнього процесу; здійснює організацію моніторингових процесів в ЗУНУ, зокрема щосеместрово проводить опитування студентів ЗУНУ стосовно якості викладання навчальних дисциплін, аналізує та формує звіти за результатами опитувань; проводить опитування роботодавців, випускників ЗУНУ й інших стейкхолдерів стосовно якості підготовки фахівців у ЗУНУ; розробляє технології і процедури проведення освітнього моніторингу щодо забезпечення якості освіти та освітньої діяльності (https://www.wunu.edu.ua/opp/zyao/komisiu_z_monitoryngu_yakosti_osvity.pdf)
Результати моніторингу якості освіти шляхом опитувань усіх учасників освітнього процесу розміщено на сайті університету (https://www.wunu.edu.ua/public_information/ensuring-the-quality-of-education/16345-rezultati-montoringu-jakost-osvti.html).

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

Результати зовнішньої оцінки систематично обговорюються на засіданнях кафедри й Вченої ради із залученням стейкхолдерів, а відповідні висновки враховуються при перегляді структури та змісту програми. З урахуванням рекомендацій попередніх акредитаційних експертиз ЗВО вдосконалив локальні нормативні документи, забезпечив повну відповідність програм СВО, проводить систематичне анонімне опитування здобувачів, викладачів і роботодавців для моніторингу якості. Також на ОП розширено участь практиків та представників ЗВО в освітньому процесі, оновлено каталог вибіркових дисциплін, збільшено кількість баз практики, уточнено тематику кваліфікаційних робіт та зміст окремих ОК відповідно до сучасних потреб галузі.
Також в ОП враховано результати та надані рекомендації з її попередньої акредитації:
1. ЗВО варто зосередити свою увагу та діяльність на впровадженні затвердженої оновленої версії ОП та нового професійного стандарту, у разі його затвердження.
Після затвердження СВО підготовки магістрів спеціальності 125 Кібербезпека (2021 р.) відбулося оновлення компетентностей та ПРН. Для їх забезпечення оновлено ОК, зокрема: ОК3, ОК5, ОК7. Оновлення ОП також відбувалося з врахуванням професійних стандартів: «Фахівець з тестування систем захисту інформації» та «Фахівець з криптографічного захисту інформації», які затверджено наказом Адміністрації Держспецзв'язку № 38 від 23 січня 2024 р., зокрема при формуванні ОК4 та ОК6.
2. Викладачам кафедри, які забезпечують навчальний процес за ОП, варто більше свої навчально-методичну та наукову активності зосереджувати ближче безпосередньо до галузі інформаційної та кібербезпеки.
Від попередньої акредитації суттєво підвищився якісний склад НПП, які викладають на ОП: Касянчук М.М. захистив докторську дисертацію (05.13.21 – Системи захисту інформації); Кулина С.В. захистив дисертацію на здобуття ступеня доктора філософії (125 – Кібербезпека та захист інформації). Всі ОК ОП забезпечені відповідними методичними розробками (пункт 4 Ліцензійних умов), наукова діяльність НПП (пункт 1 Ліцензійних умов) відповідає інформаційній галузі й спеціальності кібербезпека та захист інформації.
З метою підвищення якісного складу НПП кафедри відкрито ОНП «Кібербезпека та захист інформації» третього (освітньо-наукового) рівня вищої освіти за спеціальністю Кібербезпека та захист інформації.
3. Для подальшого розвитку ОП варто було б розглянути можливість придбання сучасних програмних продуктів захисту інформації, мережевого обладнання, а також засобів технічного захисту інформації.
За сприяння керівництва університету, участі в українських та міжнародних проєктах (Erasmus + «Інтернет речей»; USAID «Кібербезпека критично важливої інфраструктури України») відбулося суттєве розширення номенклатури наявного спеціалізованого обладнання, яке використовується при виконанні лабораторних робіт та підготовки кваліфікаційних робіт (таблиця 1). За рахунок наявного потужного серверного та мережевого обладнання розширено можливості кіберполігону.

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

Процедури внутрішнього забезпечення якості вищої освіти здійснюються на основі Положення про систему внутрішнього забезпечення якості вищої освіти
(https://www.wunu.edu.ua/opp/zyao/systemu_vnutr_zabezp_yakosti_osvity.pdf). Участь академічної спільноти у цих процесах забезпечується шляхом громадського обговорення освітньо-професійних програм, а також завдяки роботі науково-педагогічних працівників кафедр у методичних семінарах, де розглядаються проблемні питання якості та висуваються пропозиції щодо вдосконалення змісту окремих ОК.
Оцінювання освітньої та науково-технічної діяльності кафедр і факультетів проводиться із використанням системи автоматизованого рейтингового оцінювання роботи науково-педагогічних кадрів. Важливими інструментами підвищення якості ОП є проведення викладачами відкритих занять, участь у науково-методичних семінарах та конференціях, публікаційна активність, членство у редколегіях фахових видань, проходження стажувань (у тому числі міжнародних), підвищення кваліфікації, а також функціонування ефективної системи запобігання та виявлення академічного плагіату й забезпечення академічної доброчесності.

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

У ЗУНУ формування культури якості освіти ґрунтується на принципах прозорості, доброчесності та постійного вдосконалення. Учасники академічної спільноти активно залучені до процедур внутрішнього забезпечення якості відповідно до Положення про систему внутрішнього забезпечення якості вищої освіти. Така участь передбачає регулярний моніторинг та перегляд ОП, обговорення їх змісту на засіданнях кафедр, рад факультетів і Вченої ради, залучення до громадського обговорення представників роботодавців, студентства та випускників.
Системно застосовуються інструменти незалежного оцінювання: комп'ютерні контрольні тестування для здобувачів, анонімне анкетування студентів для оцінювання якості викладання, система автоматизованого рейтингового оцінювання діяльності науково-педагогічних працівників. Це створює атмосферу довіри, підзвітності та орієнтації на результат.
Важливу роль у формуванні культури якості відіграють підвищення кваліфікації викладачів, міжнародні стажування, методичні семінари, а також розбудова дієвої системи запобігання та виявлення академічного плагіату й недоброчесності. Університет приділяє увагу не лише технічним аспектам якості, але й формуванню ціннісного підґрунтя – відданості ідеям чесності, академічної свободи, партнерської взаємодії.

9. Прозорість і публічність

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

У ЗУНУ існують процедури, що регулюють права та обов'язки всіх учасників освітнього процесу, які є детально описаними і доступними на сайті Університету: Правила внутрішнього розпорядку (https://www.wunu.edu.ua/pdf/doc_zunu/ust_doc/pravila-vnut-rozp.pdf), Статут (https://www.wunu.edu.ua/pdf/licensing_accreditation/statut_zunu.pdf); Положення про організацію освітнього процесу (https://www.wunu.edu.ua/organization-of-the-educational-process/); Положення про систему внутрішнього забезпечення якості освіти в ЗУНУ (www.wunu.edu.ua/opp/zyao/systemu_vnutr_zabezp_yakosti_osvity.pdf) та ін.; Кодекс академічної доброчесності ЗУНУ (https://www.wunu.edu.ua/past-and-present/academic-integrity/16284-akademchna-dobrochesnst.html); Етичний кодекс ЗУНУ,
Положення про політику та процедури врегулювання конфліктних ситуацій в Західноукраїнському національному університеті; Стратегія розвитку Західноукраїнського національного університету на 2024-2028 рр. (https://www.wunu.edu.ua/pdf/doc_zunu/ust_doc/str_rozvutky_zunu_2024.pdf); Колективний договір Західноукраїнського національного університету на 2024-2028 роки (https://www.wunu.edu.ua/pdf/prof_com/kol_dogovir.pdf).

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

https://www.wunu.edu.ua/opp/2025_proekt_opp/magister/F5_kiberbezpeka_proekt_mag_25.pdf

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

https://www.wunu.edu.ua/master_fcit_op/

11. Перспективи подальшого розвитку ОП

Якими загалом є сильні та слабкі сторони ОП?

Сильні сторони
• активне залучення здобувачів до науково-дослідної діяльності та публікація результатів у матеріалах міжнародних конференцій, індексованих у наукометричних базах (зокрема Scopus);
• формування освітніх компонентів із урахуванням вимог ринку праці та орієнтація на практичні компетентності випускників;
• участь здобувачів у профільних конкурсах і змаганнях;
• застосування сучасних практикоорієнтованих форм і засобів навчання.
Слабкі сторони
• відсутність практики викладання освітніх компонентів англійською мовою, що знижує рівень інтернаціоналізації;
• недостатнє залучення міжнародних стейкхолдерів до розроблення, перегляду та вдосконалення ОП.

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

У найближчі три роки передбачено комплекс заходів, спрямованих на розвиток та вдосконалення освітньої

програми. Зокрема, планується:
• розгорнути спеціалізовану платформу для збору й обміну інформацією про кіберзагрози на базі серверного обладнання кафедри кібербезпеки, що сприятиме розвитку наукових досліджень у сфері проактивного захисту;
• розширити співпрацю з вітчизняними та зарубіжними закладами вищої освіти щодо спільного виконання наукових проєктів із залученням здобувачів;
• укласти та реалізувати угоди про внутрішню і зовнішню академічну мобільність, що дозволить здобувачам брати участь у міжнародних освітніх і наукових програмах;
• поглибити взаємодію зі стейкхолдерами, зокрема шляхом виконання кваліфікаційних робіт під їхнім керівництвом і на їхнє замовлення.
Реалізація окреслених заходів сприятиме підвищенню якості підготовки магістрів з кібербезпеки, розширенню їхніх можливостей у науковій та професійній діяльності, а також інтеграції ОП у міжнародний академічний простір.

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: Десятнюк Оксана Миронівна

Дата: 02.10.2025 р.

Таблиця 1. Інформація про освітні компоненти ОП

Назва освітнього компонента	Вид освітнього компонента	Силабус або інші навчально-методичні матеріали		Якщо освітній компонент потребує спеціального матеріально-технічного та/або інформаційного забезпечення, наведіть відомості щодо нього*
		Назва файла	**Хеш файла**	
Методологія наукових досліджень	навчальна дисципліна	*Metodolohiya_naukovykh_doslidzhen.pdf*	UE4A/SO0Lg8MKOPY6aHfEPmSmFi/pacOYLxK6iFgqLQ=	*Мультимедійний проектор BenQ TH671ST, 2020 року виготовлення, рік введення в експлуатацію 2021. Комп'ютер на базі процесора Technic-Pro Intel Celeron (R) Dual-Core J4005 2.0 GHz. Оперативна пам'ять - DDR4 4GB, дата введення в експлуатацію 2021 рік, ремонтних робіт не проводилось. Монітор - AOC E2270S. Доступ до мережі Інтернет. Програмне забезпечення базових інформаційних технологій: сервіси Google (документи, таблиці, презентації), Google Chrome, Firefox. Доступ до наукометричної бази Scopus з локальної мережі університету. Курс на платформі Moodle, програма для організації відеоконференцій Zoom.*
Ділові комунікації англійською мовою	навчальна дисципліна	*Dilovi_komunikatsiyi_anhl_movoyu.pdf*	5laFrO7+APnmQ6l24LjKqyzVSnkT8UQqVojbjKZaOQU=	*Мультимедійний проектор Epson EB-S05, рік виготовлення 2020, рік ведення в експлуатацію 2020. Комп'ютер на базі процесора AMD Athlon II Dual Core 250 (3,0 GHz RAM 4Gb, SSD 240 Gb), дата введення в експлуатацію грудень 2020 року, ремонтних робіт не проводилось. Монітор BenQ G2220HDA (1 шт.) Базове програмне забезпечення: Базове програмне забезпечення: ОС Windows 10 – згідно ліцензії Microsoft IT Academy та Microsoft DreamSpark for Students. Програмне забезпечення базових інформаційних технологій: сервіси Google (документи, таблиці, презентації), Google Chrome, Firefox. Курс на платформі Moodle, програма для організації відеоконференцій Zoom.*
Моніторинг та управління інформаційною безпекою	навчальна дисципліна	*Monitorynh_ta_upravl_inform_bezpekoyu.pdf*	ELdFxB8SuFfOJf2+AaGmtpZWXa+pfsfAZ1P4MqYvE5I=	*Серверна кафедри кібербезпеки обладнана наступними засобами: Сервер Dell EMC PowerEdge R440 форм-фактор 1U, оснащений двома 8-ядерними процесорами 2-го покоління Intel Xeon Silver 4215 з тактовою частотою 2.5 ГГц, що в сумі надає 16 фізичних ядер для обчислень. Конфігурація включає 192 ГБ оперативної пам'яті DDR4 RDIMM (2x32GB, 2x64GB), з можливістю подальшого розширення завдяки 16 слотам для DIMM. Дискова підсистема організована на базі 2 ТБ на швидкісних SSD-накопичувачах та 3 ТБ на жорстких дисках HDD з підтримкою гарячої заміни, а керування масивом здійснюється за допомогою RAID-контролера.*

				Надійність роботи гарантують два блоки живлення з гарячою заміною та високою ефективністю (550W Platinum), а для віддаленого моніторингу та повного керування сервером призначений інтегрований модуль iDRAC9 Enterprise. Дата введення в експлуатацію 2021 рік, ремонтних робіт не проводилось. *Сервер HPE ProLiant ML350 Gen10 у форм-факторі Tower (5U) з можливістю монтажу в стійку, оснащений двома 12-ядерними процесорами Intel Xeon Scalable (P19792-L21 Intel Xeon-Silver 4214R (2.4GHz/12-core/100W) FIO Processor Kit for HPE ProLiant ML350 Gen10), що разом надає 24 фізичних ядра, та 128 ГБ оперативної пам'яті HPE DDR4 SmartMemory RDIMM (4шт P00924-B21 HPE 32GB (1x32GB) Dual Rank x4 DDR4-2933 CAS-21-21-21 Registered Smart Memory Kit) з можливістю розширення завдяки 24 слотам DIMM. Дискова підсистема складається з 2 ТБ швидкісних накопичувачів SSD та 8 ТБ жорстких дисків HDD, керованих RAID-контролером HPE Smart Array P408i-a/2GB. Для підключення до мережі передбачено вбудований 4-портовий адаптер HPE Ethernet 1Gb 369i, а живлення забезпечується двома блоками HPE 800W Flex Slot Platinum з гарячою заміною для забезпечення резервування. Віддалене керування сервером через модуль HPE iLO 5, 8 слотів PCIe 3.0. Дата введення в експлуатацію 2023 рік, ремонтних робіт не проводилось.* *Джерело безперебійного живлення HPE T1000 Gen5 INTL UPS with Management Card Slot. Джерело безперебійного живлення DIGITUS OnLine, 1500VA/1500W, LCD, 8xC13, RJ45, RS232, USB, Rack/Tower. Дата введення в експлуатацію 2023 рік, ремонтних робіт не проводилось.* *Комутатор HPE Aruba 6000 48G 4SFP має 48 гігабітних портів RJ-45 та 4 SFP-порти для аплінків, забезпечуючи комутаційну здатність 104 Гбіт/с та швидкість пересилання 77.3 млн пакетів/с. Дата введення в експлуатацію 2023 рік, ремонтних робіт не проводилось.* *Маршрутизатор Cisco ISR4221-SEC/K9, що забезпечує сукупну пропускну здатність 35 Мбіт/с з можливістю програмного оновлення до 75 Мбіт/с. На борту має 4 ГБ оперативної пам'яті (DRAM) та 8 ГБ флеш-пам'яті. Інтерфейсний набір включає 2 комбіновані порти GE (RJ45/SFP), 1 порт GE (RJ45), 1 порт Mini-USB Type B, 1 порт USB 2.0 Type A та 2 слоти для*

				модулів розширення NIM. Дата введення в експлуатацію 2020 рік, ремонтних робіт не проводилось. *Міжмережевий екран Cisco ASA5506-X, пропускна здатність IPsec VPN до 100 Мбіт/с, підтримує до 20,000 одночасних сесій та 5,000 нових з'єднань на секунду. Оснащений 8 гігабітними портами Ethernet (RJ45), 1 портом керування та 1 портом USB 2.0. Інтегрований з сервісами FirePOWER (NGFW) для розширеного захисту від загроз. Дата введення в експлуатацію 2020 рік, ремонтних робіт не проводилось.* *Cisco RV320 Gigabit Dual WAN VPN Router, оснащений 2 гігабітними WAN-портами з функціями балансування навантаження та відмовостійкості, а також 4-портовим гігабітним LAN-комутатором. Підтримує до 50 IPsec тунелів та 10 SSL VPN тунелів для віддаленого доступу. Пропускна здатність NAT становить до 900 Мбіт/с, а для IPsec VPN – до 100 Мбіт/с. Має 2 порти USB 2.0 для підключення 3G/4G-модемів. Дата введення в експлуатацію 2020 рік, ремонтних робіт не проводилось.* *Комутатор Cisco WS-C2960-24TC-L. Керований L2-комутатор у 1U стійковому форм-факторі, оснащений 24 портами Fast Ethernet (10/100 Мбіт/с) та 2 комбінованими гігабітними аплінк-портами (RJ45/SFP). Пропускна здатність його комутаційної матриці становить 16 Гбіт/с, а швидкість пересилання – 6.5 млн. пакетів на секунду. Дата введення в експлуатацію 2020 рік, ремонтних робіт не проводилось.* *Аудиторія 6101 (Кіберполігон): комп'ютери на базі процесора Technic-Pro Intel Celeron (R) Dual-Core J4005 2.0 GHz. Оперативна пам ' ять - DDR4 4GB (13 шт), дата введення в експлуатацію 2021 рік, ремонтних робіт не проводилось. Монітор - AOC E2270S (13 шт). Комутатор D-Link DES-1100. Комутатор D-Link DES-1200-24. ОС: Kali Linux 2024.3 - Linux Kernel 6.8.* *Програмне забезпечення: OpenVAS, RiskWatch, Snort, Suricata, John the Ripper, docker, Nmap, Burp Suite, Nikto, Sqlmap, Kismet, Aircrack-ng.* *Локальний доступ до цифрової інфраструктури кафедри з віртуальними лабораторіями і сервісами: Proxmox Virtual Environment, MISP, Zabbix, Wazuh, Prometheus/Grafana, KASM Workspaces, Jenkins(CI/CD), MicroK8s, Wazuh, Docker Engine,*

				Security Onion, Ansible, KVM/QEMU, Vault Hashicorp, OpenVPN. *Курс на платформі Moodle, програма для організації відеоконференцій Zoom.*
Тестування комп'ютерних систем на проникнення	навчальна дисципліна	*Test_komp_yuternykh_system_na_proniknennya.pdf*	5iXK508eq3v2rDdBsC6Joe/rKtvmRK87xQAe0ne0RL4=	*Локальний доступ до цифрової інфраструктури кафедри з віртуальними лабораторіями і сервісами: Proxmox Virtual Environment, MISP, Zabbix, Wazuh, Prometheus/Grafana, KASM Workspaces, Jenkins (CI/CD), MicroK8s, Wazuh, Docker Engine, Security Onion.* *Аудиторія 6101 (Кіберполігон): комп'ютери на базі процесора Technic-Pro Intel Celeron (R) Dual-Core J4005 2.0 GHz. Оперативна пам'ять - DDR4 4GB (13 шт), дата введення в експлуатацію 2021 рік, ремонтних робіт не проводилось. Монітор - AOC E2270S (13 шт). Комутатор D-Link DES-1100. Комутатор D-Link DES-1200-24. ОС: Kali Linux 2024.3 - Linux Kernel 6.8.* *Програмне забезпечення: Віртуалізація/контейнери: VirtualBox, Docker Engine + Docker Compose, Vagrant; ОС для пентесту: Kali Linux; Інфраструктурні вразливі машини: Metasploitable 2/3 (вільно поширювані), образи машин з VulnHub; Індексація/метадані: exiftool, theHarvester. Брут-інвентаризація: gobuster, dirsearc; Сканування та виявлення вразливостей: Nmap (скрипти NSE), OWASP ZAP; Експлойт-фреймворки: Metasploit Framework. Паролі, хеші, автентифікація: hashcat, John the Ripper (community), rockyou.txt. Трафік/аналіз: Wireshark, tcpdump. HTTP-клієнт: curl, httpie. Python 3 (+ pip, venv), openssl, OpenSSH.* *Курс на платформі Moodle, програма для організації відеоконференцій Zoom.*
Аналіз шкідливого програмного забезпечення	навчальна дисципліна	*Analiz_shkidlyvoho_prohramnoho_zab.pdf*	Jvm/rewt9ursH0u2WI+yPQzu1HRKx49o6j86ZrPB1OI=	*Аудиторія 6101 (Кіберполігон): комп'ютери на базі процесора Technic-Pro Intel Celeron (R) Dual-Core J4005 2.0 GHz. Оперативна пам'ять - DDR4 4GB (13 шт), дата введення в експлуатацію 2021 рік, ремонтних робіт не проводилось. Монітор - AOC E2270S (13 шт). Комутатор D-Link DES-1100. Комутатор D-Link DES-1200-24. ОС: Kali Linux 2024.3 - Linux Kernel 6.8.* *Програмне забезпечення: Python, SQLite, YARA, ClamAV, VirusTotal, Ghidra, radare2, VirtualBox, Cuckoo Sandbox, Wireshark, Sysinternals Suite (Procmon, Process Explorer), Frida, Burp Suite Community, OWASP ZAP, oletools, x64dbg, OllyDbg, PEStudio, Detect It Easy (DIE), UPX, Android Studio (емулятор /*

				ADB).
Дослідження і проектування систем захисту інформації	навчальна дисципліна	*Doslidzhennya_i_proekt_system_zakhystu_inform.pdf*	r1CdcN4ZFHnwykdixoZlYrWO/venlwl7Xd6Wu7Ro+hU=	*Аудиторія 6101 (Кіберполігон): комп'ютери на базі процесора Technic-Pro Intel Celeron (R) Dual-Core J4005 2.0 GHz. Оперативна пам'ять - DDR4 4GB (13 шт), дата введення в експлуатацію 2021 рік, ремонтних робіт не проводилось. Монітор - AOC E2270S (13 шт). Комутатор D-Link DES-1100. Комутатор D-Link DES-1200-24. ОС: Kali Linux 2024.3 - Linux Kernel 6.8.* *Локальний доступ до віртуальної лабораторії. (Кіберполігон), SPDX / CycloneDX, Grype (Anchore), Syft (Anchore), Trivy (Aqua Security), HashiCorp Vault, Cosmian KMS, Infisical,cryptsetup (LUKS), PostgreSQL pg_tde, BitLocker, hdparm, sha256sum, NGINX, Wireshark, OpenSSL, Open Quantum Safe (OQS, Docker).* *Курс на платформі Moodle, програма для організації відеоконференцій Zoom.*
Цифрова криміналістика	навчальна дисципліна	*Tsyfrova_kryminalistyka.pdf*	V6fZASQk+mt3rJ5UUTyQQ+B/Km8YB4TSQOULijdk/rA=	*Аудиторія 6101 (Кіберполігон): комп'ютери на базі процесора Technic-Pro Intel Celeron (R) Dual-Core J4005 2.0 GHz. Оперативна пам'ять - DDR4 4GB (13 шт), дата введення в експлуатацію 2021 рік, ремонтних робіт не проводилось. Монітор - AOC E2270S (13 шт). Комутатор D-Link DES-1100. Комутатор D-Link DES-1200-24. ОС: Kali Linux 2024.3 - Linux Kernel 6.8.* *Локальний доступ до віртуальної лабораторії (кіберполігону), FoxitReader, 7zip, Total Commander, Dev C++, Python 3.5.8, NirSoft ChromeHistoryView, Guymager, extundelete, ext4magic, PhotoRec, R-Undelete, CCleaner, John the Ripper.* *Курс на платформі Moodle, програма для організації відеоконференцій Zoom.*
Переддипломна практика	практика	*Pereddyplomna_praktyka.pdf*	lIuntzw4vW7IKLiobM99G7N28gnGg4wKFOoKwY37ijY=	*Використання бази проходження практики.*
Підготовка та захист кваліфікаційної роботи	підсумкова атестація	*Kvalifikacijna_Robota.pdf*	KFLstlzDLHmj20fIVN7njwpselV8Kyf2CGRQ1+zz6c0=	*Мультимедійний проектор Epson EB-FH08, 2025 року виготовлення, рік введення в експлуатацію 2025.* *Веб-камера Logitech UC ConferenceCam BCC950.* *Доступ до наукометричної бази Scopus з локальної мережі університету.* *Інформаційне забезпечення – ресурси бібліотеки ЗУНУ, в тому числі електронні фонди (https://library.wunu.edu.ua/?lang=uk).* *Осцилограф цифровий SIGLENT SDS1202X+ (1 шт.); одноплатні комп'ютери Raspbery PI 3 b+ (10 шт.); плата розширення для Compute Module 5. Raspberry Pi Compute Module CM5, 8GB RAM/32GB eMMC, Wireless.* *Криптографічна плата Infineon*

				Optiga SLB 9670 TPM 2.0 для Raspberry Pi.

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

Таблиця 2. Зведена інформація про відповідність НПП освітнім компонентам

ID викладача	ПІБ	Посада	Структурний підрозділ	Кваліфікація викладача	Стаж	Навчальні дисципліни, що їх викладає викладач на ОП	Обґрунтування відповідності освітньому компоненту (кваліфікація, професійний досвід, наукові публікації)
399824	Кулина Сергій Васильович	доцент, Основне місце роботи	Факультет комп'ютерних інформаційних технологій	Диплом бакалавра, Тернопільський національний економічний університет, рік закінчення: 2008, спеціальність: 0915 Комп'ютерна інженерія, Диплом магістра, Тернопільський національний економічний університет, рік закінчення: 2009, спеціальність: 091503 Спеціалізовані комп'ютерні системи, Диплом доктора філософії Н23 001532, виданий 20.10.2023	4	Цифрова криміналістика	Наявність вимог, викладених у пунктах 37-38 Ліцензійних умов провадження освітньої діяльності Освітня кваліфікація: Тернопільський національний економічний університет, 2018 р., комп'ютерна інженерія, магістр з комп'ютерної інженерії. Тернопільський національний економічний університет, 2009 р., спеціалізовані комп'ютерні системи, магістр з спеціалізованих комп'ютерних систем. Доктор філософії зі спеціальності 125 Кібербезпека та захист інформації, 2023 р. Тема дисертації: «Методи та алгоритми захищеного розподіленого зберігання даних на основі надлишкової системи залишкових класів». Досягнення у професійній діяльності: 1: Kulyna S., Yatskiv V., Kasianchuk M., Babala L. Digital forensics and cyber threat management during wartime: analysis of new legislative initiatives. Cyber Security and Data Protection II with CEUR-WS, CSDP-II, Lviv, Ukraine, July 31, 2025, pp. 216-225. Kulyna S. Evaluation of the reverse transformation methods complexity of the residual number system for secure data

							storage. Вісник Тернопільського національного технічного університету. 2022. № 107(3). С. 21-28. Кулина С. В. Виявлення та виправлення помилок у захищених системах зберігання даних на основі обчислення проекцій числа. Інформатика та математичні методи в моделюванні. 2022. Т. 12, № 4. С. 337-345. Kulyna S. V. Система розподіленого захищеного зберігання даних. Вісник Львівського державного університету безпеки життєдіяльності. 2023. № 27. С. 48-59. Kulyna S., Yatskiv V., Nyemkova E., Kulyna H., Ivasiev S. Data encryption method based on the redundant residue number system. CEUR Workshop Proceedings. 2024. Vol. 3675 : Proceedings of the 5th International workshop on intelligent information technologies & systems of information security with CEUR-WS, Khmelnytskyi, Ukraine, March 28, 2024. P. 223-235. Kulyna, S., Muliar, I., Anikin, V., Yatskiv, V., Humennyy, P., & Kulyna, H. Construction of Nonlinear Cryptographic Protocol based on Multiple Linear Cryptosystems. 14th International Conference on Advanced Computer Information Technologies (ACIT) Ceske Budejovice, Czech Republic, 2024, pp. 500-504. 4: Опорний конспект лекцій з дисципліни «Цифрова криміналістика» для студентів освітньо-професійної програми підготовки магістра галузі знань 12 «Інформаційні технології» спеціальності 125 «Кібербезпека та захист інформації» / Укл.: Яцків В.В., Кулина С.В. Тернопіль : ФОП Осадца Ю.В., 2024. 56 с. Методичні вказівки до виконання

							лабораторних робіт з курсу «Цифрова криміналістика» для здобувачів освітньо-професійної програми «Кібербезпека» другого (магістерського) рівня вищої освіти / Укл.: Кулина С.В. Тернопіль: ЗУНУ, 2025. 35 с. Методичні вказівки до вивчення курсу «Цифрова криміналістика» для здобувачів освітньо-професійної програми «Кібербезпека» другого (магістерського) рівня вищої освіти / Укл.: Кулина С.В. Тернопіль: ЗУНУ, 2025. 26 с. 5: Захист дисертації на здобуття наукового ступеня доктора філософії за спеціальністю 125 Кібербезпека та захист інформації. Тема дисертації: «Методи та алгоритми захищеного розподіленого зберігання даних на основі надлишкової системи залишкових класів» (2023 рік). https://lpnu.ua/rada-phd/75 10: Учасник міжнародного проєкту USAID «Кібербезпека критично важливої інфраструктури України». Номер проєкту технічної допомоги, визначений договором 72012120C00002. Термін проекту: 18 травня 2020 р. – 16 вересня 2025 р. 12: Kulyna S., & Mamuzić I. The main tasks and principles of digital forensics in the conditions of war. 18th International Symposium of Croatian Metallurgical Society SHMD 2025-Materials and Metallurgy. 2025. Vol. 64, No. 1-2, pp. 237-237. Кулина С. Цифрова криміналістика в умовах сьогодення. Збірник матеріалів науково-практичного симпозіуму «Захист інформації», 30.11. 2024, Тернопіль, 2024. С.64-67. Кулина С., Калушка М.. Концепція та

							принципи гібридного шифрування. Кібербезпека державних інституцій та подолання кризових станів: матеріали III Міжнар. наук.-практ. конф. в 2 т. (Київ – Прага – Таллінн – Тернопіль), 14.11.2024 р. / ІСЗЗІ КПІ ім. Ігоря Сікорського. Київ, 2024. Т. 1. С. 450. Кулина С., Калушка М. Схема та алгоритм гібридного шифрування. Збірник матеріалів науково-практичної конференції молодих вчених, аспірантів та студентів «Кібербезпека та комп'ютерно-інтегровані технології» (КБКІТ-2024), 2024, Тернопіль, С.100-103. Кулина С. Компоненти системи розподіленого захищеного зберігання даних на основі надлишкової системи зали-шкових класів. Збірник матеріалів проблемної наукової міжгалузевої конференції «Автоматизація та комп'ютерно-інтегровані технології» (АКІТ-2023). Тернопіль, 2023. С.176-178. Кулина С. Використання систем розподіленого захищеного зберігання даних для захисту конфіденційної інформації. Економічний і соціальний розвиток України в XXI столітті: національна візія та виклики глобалізації: матеріали XX Міжнародної науково-практичної конференції молодих вчених. Тернопіль, 2023. С. 719–722. Кулина С. Виявлення та виправлення помилок у захищених системах зберігання даних методом обчислення синдрому. Збірник матеріалів проблемної наукової міжгалузевої конференції «Автоматизація та комп'ютерно-інтегровані технології» (АКІТ-2022). Тернопіль,

							2022. С. 67–69. Кулина С. Виявлення та виправлення помилок у захищених системах зберігання даних методом обчислення проекції числа. Збірник матеріалів науково-практичної конференції молодих вчених, аспірантів та студентів «Кібербезпека та комп'ютерно-інтегровані технології» (КБКІТ-2022). Тернопіль, 2022. С. 13–16. Kulyna S. Comparative analysis of the residue number system inverse transform methods for secure data storage. Proceedings of VIII-th International Scientific and Technical Conferenc «Information protection and information systems security», November 11–12, Lviv, Ukraine, 2021, pp. 15-16. Кулина С., Кондратюк В. Дослідження систем захищеного зберігання даних. Збірник матеріалів проблемно-наукової міжгалузевої конференції «Автоматизація та комп'ютерно інтегровані технології», Тернопіль, 2021. С-157-159. 19: Учасник ГО «Автоматизація та кібербезпека» Стажування (підвищення кваліфікації): Тернопільський національний технічний університет ім. І. Пулюя, з 8 травня по 16 червня 2023 р., тема: «Ознайомлення з сучасними технологіями захисту інформації та вивчення досвіду викладання професійних дисциплін», довідка від 16.06. 2023 р. № 2/28-801 (180 годин / 6 кредитів ECTS). Університет у Кракові (Республіка Польща), з 12 вересня по 12 листопада 2024 р., тема: «Методи та технічні засоби захисту інформації / Methods and Technical

							Means of Information Protection», сертифікат від 14.11.2024 р. (180 годин / 6 кредитів ECTS). Сертифікат про закінчення курсу «Digital Forensics» від міжнародного проєкту USAID «Кібербезпека критично важливої інфраструктури України», 18 жовтня – 1 грудня 2021 р. (180 год / 6 кредитів ECTS).
206329	Івасьєв Степан Володимирович	доцент, Основне місце роботи	Факультет комп'ютерних інформаційних технологій	Диплом молодшого спеціаліста, Відокремлений підрозділ - Коледж Галицького інституту імені В'ячеслава Чорновола, рік закінчення: 2006, спеціальність: 080406 Експлуатація систем обробки інформації та прийняття рішень, Диплом бакалавра, Тернопільський національний економічний університет, рік закінчення: 2008, спеціальність: 0804 Комп'ютерні науки, Диплом магістра, Тернопільський національний економічний університет, рік закінчення: 2009, спеціальність: 080403 Програмне забезпечення автоматизованих систем, Диплом кандидата наук ДК 037950, виданий 29.09.2016, Атестат доцента АД 009401, виданий 29.09.2021	12	Аналіз шкідливого програмного забезпечення	Наявність вимог, викладених у пунктах 37-38 Ліцензійних умов провадження освітньої діяльності Освітня кваліфікація Тернопільський національний економічний університет, 2009 р., програмне забезпечення автоматизованих систем, магістр з комп'ютерних наук. Кандидат технічних наук, 2016 р., спеціальність 05.13.05 – комп'ютерні системи та компоненти. Тема дисертації: «Методи та обчислювальні засоби рішення задач теорії чисел в базисах Радемахера - Крестенсона» Доцент кафедри кібербезпеки, 2021 р. Досягнення у професійній діяльності: 1: Івасьєв С. В., Яцків В. В., Давлетова А. Я., Тимошенко Л. М. Методологія впровадження системи управління інформаційною безпекою на основі багаторівневої моделі кіберзахисту згідно з вимогами законодавства України. Інформатика та мат. методи в моделюванні / Informatics and Mathematical Methods in Simulation. Одеса, 2025. Т. 15, № 1. С. 137–148. Івасьєв С., Цаволик Т., Яцків В., Яцків Н. Виявлення недоліків у механізмах аутентифікації користувачів в SaaS-сервісах на основі MITRE ATT&CK. Вимірювальна та

							обчислювальна техніка в технологічних процесах. Технічні науки. 2023. №74. С.16 – 22. Stepan Ivasiev, Vasyl Yatskiv, Mykhailo Kasianchuk, Ihor Yakymenko, Andriy Sverstiuk. Same Bit-Size Moduli Formation of Residue Number System for Application in Asymmetric Cryptography. Proceedings of the 2nd International Workshop on Intelligent Information Technologies & Systems of Information Security with CEUR-WS, Khmelnytskyi, Ukraine, March 24-26, 2021. Volume 2853 of CEUR Workshop Proceedings, pages 301-308, CEUR-WS.org, 2021. Івасьєв С. В., Касянчук М. М., Лотоцький О. Я., Яцків С. В., Тимошенко Л. М. Розробка трьохмодульної криптосистеми Рабіна на основі операції додавання. Інформатика та мат. методи в моделюванні / Informatics and Mathematical Methods in Simulation. 2021. Т. 11, № 1-2. С. 16–26. Ivasiev S., Yatskiv V., Tsavolyk T., Yatskiv N., Koval V. Algorithm and data encoding/decoding devices based on two-dimensional modular correction codes. Proceedings of the 4th International Workshop on Intelligent Information Technologies & Systems of Information Security (IntelITSIS 2023), Khmelnytskyi, Ukraine, March 22–24, 2023, Vol-3373, 2023, P. 388-400. Ivasiev S., Tsmots I., Ihnatiev I. Very-large-scale integration device for parallel vertical group computing the sum of squared differences. Scientific Journal of TNTU. 2023. Vol 110. No 2. P. 5–14. 7. Ivasiev S., Segin A., Albanskiy I., Davletova A., Maslyiak B., Humenniy P. Special Processor for Correlation Signal Processing in the Polar Coordinate System. 13th International Conference on

							Advanced Computer Information Technologies (ACIT), Wrocław, Poland, 2023, pp. 460-463. Ivasiev, S., Yatskiv, V., Nyemkova, E., Kulyna, S., Kulyna, H. Data encryption method based on the redundant residue number syste. CEUR Workshop ProceedingsThis link is disabled. 2024, 3675, pp. 223–235. Ivasiev S., Davletova A., Yatskiv V., Kulyna S., Tsavolyk T. and Drapak V. Enhancing Cryptographic System Security based on Finite Fields. 2024 14th International Conference on Advanced Computer Information Technologies (ACIT), Ceske Budejovice, Czech Republic, 2024, pp. 476-480. 4: Опорний конспект лекцій з курсу «Аналіз шкідливого програмного забезпечення» для здобувачів освітньо-професійної програми «Кібербезпека» другого (магістерського) рівня вищої освіти спеціальності «Кібербезпека та захист інформації» / Укл.: Івасьєв С.В., Бараннік Б. О. Тернопіль: ЗУНУ, 2024. 41 с. Методичні рекомендації до виконання лабораторних робіт з дисципліни «Аналіз шкідливого програмного забезпечення» для здобувачів освітньо-професійної програми «Кібербезпека» другого (магістерського) рівня вищої освіти спеціальності «Кібербезпека та захист інформації» / Укл.: Івасьєв С.В., Давлетова А.Я. Тернопіль 2023. 49 с. Методичні вказівки до вивчення курсу «Аналіз шкідливого програмного забезпечення» для здобувачів освітньо-професійної програми «Кібербезпека» другого (магістерського) рівня вищої освіти / Укл.: Івасьєв С.В.

							Тернопіль: ЗУНУ, 2025. 28 с. 10: Учасник міжнародного проєкту USAID «Кібербезпека критично важливої інфраструктури України». Номер проєкту технічної допомоги, визначений договором 72012120C00002. Термін проєкту: 18 травня 2020 р. – 16 вересня 2025 р. 12: Івасьєв С.В., Дживра П.І. Дослідження вразливостей mikrotik. Збірник матеріалів проблемно-наукової міжгалузевої конференції «Автоматизація та комп'ютерно-інтегровані технології» (АКІТ - 2023), Тернопіль, 2023. С. 146-150. Івасьєв С., Чубей О., Романів О. Алгоритми виявлення та захисту від зловмисного програмного забезпечення. Збірник матеріалів проблемно-наукової міжгалузевої конференції «Автоматизація та комп'ютерно-інтегровані технології» (АКІТ - 2024), Тернопіль, 2024. С. 73-76. Івасьєв С.В., Сава Л.М. Порівняльний аналіз асиметричних алгоритмів шифрування. Збірник тез доповідей XIX Міжнародної науково-практичної конференції молодих вчених (Тернопіль, 13 травня 2022 року), С.77-80. Івасьєв С.В., Кузик В.М., Продан Т.І., Слєпцова О.Я. Біометрична система аутентифікації з використанням голосових даних. Збірник матеріалів проблемно-наукової міжгалузевої конференції «Кібербезпека та комп'ютерно інтегровані технології» (КБКІТ-2022), Тернопіль, 2022. С. 56-59. Івасьєв С.В., Кульчинська Н. З. Використання систем віртуалізації для опанування навиків адміністрування

							операційних систем. Інформатика та комп'ютерні дисципліни у профільній загальноосвітній підготовці. Збірник матеріалів науково-практичної онлайн конференції (м. Тернопіль 20 травня 2024р.). Тернопіль: Галицький фаховий коледж імені В'ячеслава Чорновола», 2024. С. 10-14 Івасьєв С., Янік І. Шляхи оптимізації обчислювальних операцій в алгоритмі RSA. Матеріали науково-практичного симпозіуму «Захист інформації», Тернопіль, 2024. С.107-111. Івасьєв С., Кобиця В. Інструменти динамічного аналізу шкідливого програмного забезпечення. ITSec: Безпека інформаційних технологій: матеріали XIV Міжнар. наук.-техн. конф., м. Тернопіль, 22-24 трав. 2025 р. Тернопіль-Київ: ЗУНУ-ДУІКТ, 2025. С. 83-85 Івасьєв С., Лизун Я., Кобиця В. Факторизація багаторозрядного числа з використанням асоціативної пам'яті. Збірник тез доповідей II всеукраїнської наково-практичної конференції «Інноваційні підходи до розвитку технологій та економіки» (м.Свалява, Червень 6,2025). Свалява, 2025. С.183-187. 19: Учасник ГО «Автоматизація та кібербезпека». Участь в фундації захисту Інтернету OWASP. Membership ID #2287933 Стажування (підвищення кваліфікації) Університет у Бєльсько-Бялій, Польща, з 30.11.2020 р. до 26.02.2021 р., тема: «Ефективні алгоритми факторизації багаторозрядних чисел», сертифікат від 26.02.2021 р. (240 год.

							8 кредитів ECTS). ТОВ Апіко «Україна», з 20.02.2025 р. до 4.04.2025 р., тема: «Аналіз методів захисту програмного забезпечення від стороннього втручання», довідка №14 від 4.04.2025 р. (180 годин / 6 кредитів ECTS). Сертифікати: Сертифікат про закінчення курсу «Foundations of Computer and Network Security» від міжнародного проєкту USAID «Кібербезпека критично важливої інфраструктури України», з 11 липня до 31 серпня 2021 р., (180 год / 6 кредитів ECTS). Сертифікат про закінчення курсу «Cloud Environment Configuration And Security» від компанії SoftServe, з 07 березня 2024 до 02 квітня 2024 р., Series CS № 17533/2024 (120 год. / 4 кредитів ECTS).
313913	Яцків Василь Васильович	завідувач кафедри, Основне місце роботи	Факультет комп'ютерних інформаційних технологій	Диплом спеціаліста, Івано-Франківський державний технічний університет нафти і газу, рік закінчення: 1996, спеціальність: Автоматизація технологічних процесів і виробництв, Диплом доктора наук ДД 005950, виданий 29.09.2016, Диплом кандидата наук ДК 011249, виданий 04.07.2001, Атестат доцента 02ДЦ 001496, виданий 28.04.2004, Атестат професора АП 003277, виданий 27.09.2021	27	Методологія наукових досліджень	Наявність вимог, викладених у пунктах 37-38 Ліцензійних умов провадження освітньої діяльності Освітня кваліфікація: Івано-Франківський державний технічний університет нафти і газу, 1996 р., автоматизація технологічних процесів і виробництв, інженер з автоматизації. Кандидат технічних наук, 2001 р., спеціальність 05.13.13 – обчислювальні машини, системи та мережі. Тема дисертації: «Методи кодування та цифрової обробки повідомлень в розподілених системах з оптичним каналом зв'язку» Доцент кафедри спеціалізованих комп'ютерних систем, 2004 р. Доктор технічних наук, 2016 р., спеціальність 05.13.05 – комп'ютерні системи та компоненти. Тема дисертації: «Теоретичні основи створення і структурна організація

							компонентів безпровідних сенсорних мереж підвищеної ефективності». Професор кафедри кібербезпеки, 2021 р. Досягнення у професійній діяльності: 1: Яцків В.В., Яцків Н.Г., Возняк С.І., Кондратюк В.М. Методика виконання тестів на проникнення з використання MITRE ATT&CK. Інформатика та математичні методи в моделюванні. 2025. Том 15, № 2. С. 288-297. DOI 10.15276/imms.v15.no2.288 Яцків В.В., Івасьєв С.В., Давлетова А.Я., Тимошенко Л.М. Методологія впровадження системи управління інформаційною безпекою на основі багаторівневої моделі кіберзахисту згідно з вимогами законодавства України. Інформатика та математичні методи в моделюванні. 2025. Том 15, № 1. С. 137-149. DOI 10.15276/imms.v15.no1.137 Yatskiv, V., Tymoshchuk, D., Tymoshchuk, V., & Yatskiv, N. Interactive Cybersecurity Training System Based on Simulation Environments. Measuring And Computing Devices in Technological Processes. 2024. №4. P. 215–220. Yatskiv V., Tymoshchuk D. Using Hypervisors To Create A Cyber Polygon. Measuring And Computing Devices In Technological Processes, №3, 2024. – С.52-56. Яцків В., Цаволик Т., Яцків Н., Івасьєв С. Виявлення недоліків у механізмах аутентифікації користувачів в SaaS-сервісах на основі MITRE ATT&CK. Вимірювальна та обчислювальна техніка в технологічних процесах. Технічні

							науки. 2023. С.16 – 22. Yatskiv, V., Davletova, A., Ivasiev, S., & Karpinskyi, M. Encryption Method Based on Codes. ACPS. 2024; Volume 9, Number 1: pp. 24 – 31 V. Yatskiv, A. Sachenko, J. Sieck, Jun Su. Image Transmission in WMSN Based on Residue Number System. International Journal of Computing, Volume 2024. №23(1). Pp. 126-133. 4: Опорний конспект лекцій з курсу «Методологія наукових досліджень» для здобувачів освітньо-професійної програми «Кібербезпека» другого (магістерського) рівня вищої освіти спеціальності Кібербезпека та захист інформації / Укл. В. Яцків. Тернопіль: ЗУНУ, 2024. 74 с. Методичні рекомендації до проведення практичних занять з дисципліни «Методологія наукових досліджень» для здобувачів спеціальності Кібербезпека та захист інформації. / Укл.: Яцків В. В. Тернопіль: ЗУНУ. 2025. 16 с. Методичні вказівки до вивчення курсу «Методологія наукових досліджень» для здобувачів освітньо-професійної програми «Кібербезпека» другого (магістерського) рівня вищої освіти / Укл.: Яцків В.В. Тернопіль: ЗУНУ, 2025. 28 с. Методичні рекомендації до виконання кваліфікаційної роботи з освітньо-професійної програми «Кібербезпека» спеціальності «Кібербезпека та захист інформації» за другим (магістерським) рівнем вищої освіти. /Укл. Яцків В.В., Касянчук М.М., Якименко І.З., Івасьєв С.В., Цаволик Т.Г. Тернопіль: ЗУНУ, 2024. 36 с. 6: Науковий керівник:

							Кулина С.В., доктор філософії за спеціальністю 125 Кібербезпека. Дата захисту: 30.09.2023 рік. https://lpnu.ua/rada-phd/757: Член спеціалізованої вченої ради Д58.082.02 Західноукраїнського національного університету (спеціальність і 05.13.05 - комп'ютерні системи та компоненти), наказ МОН № 641 від 28.04.2025 р. Член спеціалізованої вченої ради Д70.052.06 Хмельницького національного університету (спеціальність і 05.13.05 - комп'ютерні системи та компоненти), наказ МОН № 641 від 28.04.2025 р. Офіційний опонент дисертації Кучковського В.В., поданої на здобуття наукового ступеня доктора філософії на тему «Інформаційна технологія блокчейн для опрацювання великих даних» за спеціальністю 122 Комп'ютерні науки, 2023 р. Офіційний опонент дисертації Александрова М.О., поданої на здобуття наукового ступеня доктора філософії на тему «Нейромережеве синхронне генерування ключів підвищеної надійності для симетричних систем шифрування», за спеціальністю 122 Комп'ютерні науки, 2023 р. Офіційний опонент дисертації Дячка Р. В., поданої на здобуття наукового ступеня доктора філософії на тему «Методи та засоби інтелектуалізації інформаційно-вимірювальних систем з мультисенсорною конфігурацією», за спеціальністю 123 Комп'ютерна інженерія, 2023 р. Офіційний опонент дисертації Грибняка С.С., поданої на здобуття наукового

							ступеня доктора філософії на тему «Моделі та методи підвищення ефективності обробки транзакцій у розподілених реєстрах», за спеціальністю 122 Комп'ютерні науки, 2023 р. Офіційний опонент дисертації Лобачева І.М., поданої на здобуття наукового ступеня доктора філософії на тему «Моделі та методи підвищення ефективності розподілених трансдюсерних мереж на основі машинного навчання та периферійних обчислень», за спеціальністю 122 Комп'ютерні науки 2021 р. 8: Керівник проєкту: БФ/4-2021, держ. реєстраційний номер 0121U114705 "Розробка методів та алгоритмів захищеного зберігання даних". Термін виконання: 06.2021 р. – 12.2021р. Керівник проєкту, КБ-12-2021 «Методи та алгоритми захищеного зберігання даних на основі кодів системи залишкових класів», номер держреєстрації 0121U107651. Термін виконання: 04 січня 2021 р. до 31 грудня 2021 р. Керівник проєкту КБ-35-2022 «Розробка алгоритмів розвідки кіберзагроз на базі платформи з відкритим кодом», □ держ. реєстраційний номер: 0122U200863. Термін виконання: 09.2022 р. – 12.2022 р. Керівник проєкту: № БФ /4-2025 додаткова угода до договору № БФ/4-2021 від 01.06.2021 року, «Розроблення методів та алгоритмів шифрування даних, стійких до впливу завад», номер держ. реєстраційний номер 0121U114705. Термін виконання: 01.2025 – 12.2025 р. Член редакційної колегії: журнал «Безпека інфокомунікаційних

							систем та Інтернету речей» https://journals.chnu.edu.ua/sisiot/about/editorialTeam ; журнал «Eastern-European Journal of Enterprise Technologies» https://journals.uran.ua/eejet/about/editorialTeam 10: – Виконавець міжнародного проекту ЄС «ERASMUS+ SUDEM» № 2023-1-BG01-KA220-HED-000159479» «Цифровізація процесів сталого управління катастрофами та надзвичайними ситуаціями». Термін виконання: 01.11.2023 р. до 31.10.2025 року. – Координатор та учасник міжнародного проєкту USAID «Кібербезпека критично важливої інфраструктури України». Номер проекту технічної допомоги, визначений донором: 72012120C00002. Термін проекту: 18 травня 2020 р. – 16 вересня 2025 р. 12: Яцків В., Івасьєв С., Яцків Н. Криптосистема McEliece на основі коригуючих кодів системи залишкових класів. ITSec: Безпека інформаційних технологій: матеріали XIV Міжнар. наук.-техн. конф., м. Тернопіль, 22-24 трав. 2025 р. Тернопіль-Київ: ЗУНУ-ДУІКТ, 2025. С. 229 -231 Yatskiv V., Tymoshchuk D., Slowloris DDOS Detection and Prevention in Real-Time. August 16, 2024; Oxford, UK: VII International Scientific and Practical Conference «Theoretical and Empirical Scientific Research: Concept and Trends», 2024, 171-176. Yatskiv V., Davletova, A., Ivasiev S., Kulyna S., Tsavolyk, T., & Drapak, V. Enhancing Cryptographic System Security Based on Finite Fields: proceedings of 14th International Conference on Advanced Computer

							Information Technologies (ACIT'2024) (19-21 September, Ceske Budejovice). CZECH REPUBLIC, 2024. P. 476-480. Yatskiv V., Nyemkova E., Kulyna S., Kulyna H., Ivasiev S. Data Encryption Method Based on the Redundant Residue Number System. Proceedings of the 5th International Workshop on Intelligent Information Technologies & Systems of Information Security with CEUR-WS, Khmelnytskyi, Ukraine, March 28, 2024, Vol-3675, 2024. P. 223-235. Yatskiv V., Tsavolyk T., Yatskiv N., Koval V., Ivasiev S. Algorithm and data encoding/decoding devices based on two-dimensional modular correction codes. Proceedings of the 4th International Workshop on Intelligent Information Technologies & Systems of Information Security (IntelITSIS 2023), Khmelnytskyi, Ukraine, March 22–24, 2023, Vol-3373, 2023. P. 388-400. Яцків В.В., Терещенко О.С. Розвідка кіберзагроз з використанням мови опису правил YARA. Матеріали науково-практична конференція молодих вчених, аспірантів та студентів «Кібербезпека та комп'ютерно-інтегровані технології» (КБКІТ - 2022), Тернопіль, 2022. С. 40-42. Яцків В.В., Терещенко О.С. Сучасні платформи розвідки кіберзагроз з відкритим кодом. Матеріали проблемно-наукової міжгалузевої конференції «Автоматизація та комп'ютерно-інтегровані технології» (АКІТ - 2022), Тернопіль, 2022. С. 100-103. 14: Член галузевої комісії Всеукраїнського конкурсу студентських наукових робіт з спеціальності "Кібербезпека", 2021

							р. 19: Член “Open Web Application Security Project, OWASP”. Membership Portal (WIP) Member Number: cus_Ig8KYMxmYVkL4L Голова ГО «Автоматизація та кібербезпека». Стажування (підвищення кваліфікації) ТОВ «Ті-СПАРК», з 13 січня 2025 року по 21 лютого 2025 року, тема: «Тестування безпеки комп'ютерних систем та хмарних сервісів» довідка № 1/21 від 21.02.2025 р. (180 годин/ 6 кредитів ЄКТС). Сертифікати: Сертифікат про закінчення курсу «Penetration Testing» від міжнародного проєкту USAID «Кібербезпека критично важливої інфраструктури України», 11 липня – 31 серпня 2022 р., (180 год / 6 кредитів ЄКТС). Сертифікат про закінчення курсу «Incident Response» від міжнародного проєкту USAID «Кібербезпека критично важливої інфраструктури України», 18 жовтня – 1 грудня 2021 р., (180 год / 6 кредитів ЄКТС). Сертифікат про закінчення курсу «Cloud Environment Configuration And Security» від компанії SoftServe, 07 березня 2024 – 02 квітня 2024 р., Series XG No 17569/2024 (120 год. / 4 кредитів ЄКТС). Сертифікат про закінчення курсу Trust4Future. За програмою, яка фінансується Ініціативою EIT Deep Tech Talent з Європейського інституту інновацій та технологій (EIT), 26 березня - 24 червня 2025 року Сертифікат про завершення безперервної освіти за успішне завершення 60 модулів, з 05.01.2021 по 07.01.2023, що

							еквівалентно 20 годинам навчання, наданих платформою RangeForce.
313913	Яцків Василь Васильович	завідувач кафедри, Основне місце роботи	Факультет комп'ютерних інформаційних технологій	Диплом спеціаліста, Івано-Франківський державний технічний університет нафти і газу, рік закінчення: 1996, спеціальність: Автоматизація технологічних процесів і виробництв, Диплом доктора наук ДД 005950, виданий 29.09.2016, Диплом кандидата наук ДК 011249, виданий 04.07.2001, Атестат доцента 02ДЦ 001496, виданий 28.04.2004, Атестат професора АП 003277, виданий 27.09.2021	27	Тестування комп’ютерних систем на проникнення	Наявність вимог, викладених у пунктах 37-38 Ліцензійних умов провадження освітньої діяльності Освітня кваліфікація: Івано-Франківський державний технічний університет нафти і газу, 1996 р., автоматизація технологічних процесів і виробництв, інженер з автоматизації. Кандидат технічних наук, 2001 р., спеціальність 05.13.13 – обчислювальні машини, системи та мережі. Тема дисертації: «Методи кодування та цифрової обробки повідомлень в розподілених системах з оптичним каналом зв’язку» Доцент кафедри спеціалізованих комп’ютерних систем, 2004 р. Доктор технічних наук, 2016 р., спеціальність 05.13.05 – комп’ютерні системи та компоненти. Тема дисертації: «Теоретичні основи створення і структурна організація компонентів безпровідних сенсорних мереж підвищеної ефективності». Професор кафедри кібербезпеки, 2021 р. Досягнення у професійній діяльності: 1: 1. Яцків В.В., Яцків Н.Г., Возняк С.І., Кондратюк В.М. Методика виконання тестів на проникнення з використання MITRE ATT&CK. Інформатика та математичні методи в моделюванні. 2025. Том 15, № 2. – С. 288-297. DOI 10.15276/imms.v15.no2.288 2. Яцків В.В., Івасьєв С.В., Давлетова А.Я., Тимошенко Л.М. Методологія впровадження

							системи управління інформаційною безпекою на основі багаторівневої моделі кіберзахисту згідно з вимогами законодавства України. Інформатика та математичні методи в моделюванні. 2025. Том 15, № 1. – С. 137-149. DOI 10.15276/imms.v15.no1.137 3. Yatskiv, V., Tymoshchuk, D., Tymoshchuk, V., & Yatskiv, N. (2024). Interactive Cybersecurity Training System Based on Simulation Environments. Measuring And Computing Devices in Technological Processes, (4), 215–220. 4. Yatskiv V., Tymoshchuk D., Using Hypervisors To Create A Cyber Polygon. Measuring And Computing Devices In Technological Processes. 2024. №3. С.52-56. 5. Яцків В., Цаволик Т., Яцків Н., Івасьєв С. Виявлення недоліків у механізмах аутентифікації користувачів в SaaS-сервісах на основі MITRE ATT&CK. Вимірювальна та обчислювальна техніка в технологічних процесах. Технічні науки. 2023. С.16 – 22. 6. Yatskiv, V., Davletova, A., Ivasiev, S., & Karpinskyi, M. Encryption Method Based on Codes. ACPS. 2024; Volume 9, Number 1: pp. 24 – 31 7. V. Yatskiv, A. Sachenko, J. Sieck, Jun Su. Image Transmission in WMSN Based on Residue Number System. International Journal of Computing, 2024. №.23(1). Pp. 126-133. 4: Опорний конспект лекцій з курсу «Тестування комп'ютерних систем на проникнення» для здобувачів освітньо-професійної програми «Кібербезпека» другого (магістерського) рівня вищої освіти спеціальності

							«Кібербезпека та захист інформації» / Укл. В. Яцків, С. Возняк. Тернопіль: ЗУНУ, 2025. 94 с. Методичні рекомендації до виконання лабораторних робіт з дисципліни «Тестування комп'ютерних систем на проникнення» для здобувачів спеціальності Кібербезпека та захист інформації. / Укл.: Яцків В. В. Тернопіль: ЗУНУ. 2025. 52 с. Методичні вказівки до вивчення курсу «Тестування комп'ютерних систем на проникнення» для здобувачів освітньо-професійної програми «Кібербезпека» другого (магістерського) рівня вищої освіти / Укл.: Яцків В.В. Тернопіль: ЗУНУ, 2025. 29 с. 6: Науковий керівник: Кулина С.В., доктор філософії за спеціальністю 125 Кібербезпека. Дата захисту: 30.09.2023 рік. https://lpnu.ua/rada-phd/75 7: Член спеціалізованої вченої ради Д58.082.02 Західноукраїнського національного університету (спеціальність і 05.13.05 - комп'ютерні системи та компоненти), наказ МОН № 641 від 28.04.2025 р. Член спеціалізованої вченої ради Д70.052.06 Хмельницького національного університету (спеціальність і 05.13.05 - комп'ютерні системи та компоненти), наказ МОН № 641 від 28.04.2025 р. Офіційний опонент дисертації Кучковського В.В., поданої на здобуття наукового ступеня доктора філософії на тему «Інформаційна технологія блокчейн для опрацювання великих даних» за спеціальністю 122 Комп'ютерні науки, 2023 р. Офіційний опонент

							дисертації Александрова М.О., поданої на здобуття наукового ступеня доктора філософії на тему «Нейромережеве синхронне генерування ключів підвищеної надійності для симетричних систем шифрування», за спеціальністю 122 Комп'ютерні науки, 2023 р. Офіційний опонент дисертації Дячка Р. В., поданої на здобуття наукового ступеня доктора філософії на тему «Методи та засоби інтелектуалізації інформаційно-вимірювальних систем з мультисенсорною конфігурацією», за спеціальністю 123 Комп'ютерна інженерія, 2023 р. Офіційний опонент дисертації Грибняка С.С., поданої на здобуття наукового ступеня доктора філософії на тему «Моделі та методи підвищення ефективності обробки транзакцій у розподілених реєстрах», за спеціальністю 122 Комп'ютерні науки, 2023 р. Офіційний опонент дисертації Лобачева І.М., поданої на здобуття наукового ступеня доктора філософії на тему «Моделі та методи підвищення ефективності розподілених трансдюсерних мереж на основі машинного навчання та периферійних обчислень», за спеціальністю 122 Комп'ютерні науки 2021 р.
							8: Керівник проєкту: БФ/4-2021, держ. реєстраційний номер 0121U114705 "Розробка методів та алгоритмів захищеного зберігання даних". Термін виконання: 06.2021 р. – 12.2021р. Керівник проєкту, КБ-12-2021 «Методи та алгоритми захищеного зберігання даних на основі кодів системи залишкових класів»,

							номер держреєстрації 0121U107651. Термін виконання: 04 січня 2021 р. до 31 грудня 2021 р. Керівник проєкту КБ-35-2022 «Розробка алгоритмів розвідки кіберзагроз на базі платформи з відкритим кодом», □ держ. реєстраційний номер: 0122U200863. Термін виконання: 09.2022 р. – 12.2022 р. Керівник проєкту: № БФ /4-2025 додаткова угода до договору № БФ/4-2021 від 01.06.2021 року, «Розроблення методів та алгоритмів шифрування даних, стійких до впливу завад», номер держ. реєстраційний номер 0121U114705. Термін виконання: 01.2025 – 12.2025 р. Член редакційної колегії: журнал «Безпека інфокомунікаційних систем та Інтернету речей» https://journals.chnu.edu.ua/sisiot/about/editorialTeam ; журнал «Eastern-European Journal of Enterprise Technologies» https://journals.uran.ua/eejet/about/editorialTeam 10: – Виконавець міжнародного проекту ЄС «ERASMUS+ SUDEM» № 2023-1-BG01-KA220-HED-000159479» «Цифровізація процесів сталого управління катастрофами та надзвичайними ситуаціями». Термін виконання: 01.11.2023 р. до 31.10.2025 року. – Координатор та учасник міжнародного проєкту USAID «Кібербезпека критично важливої інфраструктури України». Номер проекту технічної допомоги, визначений донором: 72012120C00002. Термін проекту: 18 травня 2020 р. – 16 вересня 2025 р. 12: Яцків В., Івасьєв С., Яцків Н. Криптосистема McEliece на основі коригуючих кодів

							системи залишкових класів. ITSec: Безпека інформаційних технологій: матеріали XIV Міжнар. наук.-техн. конф., м. Тернопіль, 22-24 трав. 2025 р. Тернопіль-Київ: ЗУНУ-ДУІКТ, 2025. С. 229 -231 Yatskiv V., Tymoshchuk D., Slowloris DDOS Detection and Prevention in Real-Time. August 16, 2024; Oxford, UK: VII International Scientific and Practical Conference «Theoretical and Empirical Scientific Research: Concept and Trends», 2024. P. 171-176. Yatskiv V., Davletova, A., Ivasiev S., Kulyna S., Tsavolyk, T., & Drapak, V. Enhancing Cryptographic System Security Based on Finite Fields: proceedings of 14th International Conference on Advanced Computer Information Technologies (ACIT'2024) (19-21 September, Ceske Budejovice). CZECH REPUBLIC, 2024. P. 476-480. Yatskiv V., Nyemkova E., Kulyna S., Kulyna H., Ivasiev S. Data Encryption Method Based on the Redundant Residue Number System. Proceedings of the 5th International Workshop on Intelligent Information Technologies & Systems of Information Security with CEUR-WS, Khmelnytskyi, Ukraine, March 28, 2024, Vol-3675, 2024. P. 223-235. Yatskiv V., Tsavolyk T., Yatskiv N., Koval V., Ivasiev S. Algorithm and data encoding/decoding devices based on two-dimensional modular correction codes. Proceedings of the 4th International Workshop on Intelligent Information Technologies & Systems of Information Security (IntelITSIS 2023), Khmelnytskyi, Ukraine, March 22–24, 2023, Vol-3373, 2023. P. 388-400. Яцків В.В., Терещенко О.С. Розвідка кіберзагроз з

							використанням мови опису правил YARA. Матеріали науково-практична конференція молодих вчених, аспірантів та студентів «Кібербезпека та комп'ютерно-інтегровані технології» (КБКІТ - 2022), Тернопіль, 2022. С. 40-42. Яцків В.В., Терещенко О.С. Сучасні платформи розвідки кіберзагроз з відкритим кодом. Матеріали проблемно-наукової міжгалузевої конференції «Автоматизація та комп'ютерно-інтегровані технології» (АКІТ - 2022), Тернопіль, 2022. С. 100-103. 14: Член галузевої комісії Всеукраїнського конкурсу студентських наукових робіт з спеціальності "Кібербезпека", 2021 р. 19: Член "Open Web Application Security Project, OWASP". Membership Portal (WIP) Member Number: cus_Ig8KYMxmYVkL4L Голова ГО «Автоматизація та кібербезпека». Стажування (підвищення кваліфікації) ТОВ «Ті-СПАРК», з 13 січня 2025 року по 21 лютого 2025 року, тема: «Тестування безпеки комп'ютерних систем та хмарних сервісів» довідка № 1/21 від 21.02.2025 р. (180 годин/ 6 кредитів ECTS). Сертифікати: Сертифікат про закінчення курсу «Penetration Testing» від міжнародного проєкту USAID «Кібербезпека критично важливої інфраструктури України», 11 липня – 31 серпня 2022 р., (180 год / 6 кредитів ECTS). Сертифікат про закінчення курсу «Incident Response» від міжнародного проєкту USAID «Кібербезпека критично важливої

							інфраструктури України», 18 жовтня – 1 грудня 2021 р., (180 год / 6 кредитів ECTS). Сертифікат про закінчення курсу «Cloud Environment Configuration And Security» від компанії SoftServe, 07 березня 2024 – 02 квітня 2024 р., Series XG No 17569/2024 (120 год. / 4 кредитів ECTS). Сертифікат про закінчення курсу Trust4Future. За програмою, яка фінансується Ініціативою EIT Deep Tech Talent з Європейського інституту інновацій та технологій (EIT), 26 березня - 24 червня 2025 року Сертифікат про завершення безперервної освіти за успішне завершення 60 модулів, з 05.01.2021 по 07.01.2023, що еквівалентно 20 годинам навчання, наданих платформою RangeForce.
139234	Касянчук Михайло Миколайович	професор, Основне місце роботи	Факультет комп'ютерних інформаційних технологій	Диплом спеціаліста, Тернопільський державний педагогічний університет, рік закінчення: 1994, спеціальність: 7.080101 математика і фізика, Диплом магістра, Тернопільський національний економічний університет, рік закінчення: 2018, спеціальність: 123 Комп'ютерна інженерія, Диплом доктора наук ДД 010473, виданий 26.11.2020, Диплом кандидата наук ДК 013489, виданий 09.01.2002, Атестат доцента 02ДЦ 015376, виданий 19.10.2005, Атестат професора АП	27	Моніторинг та управління інформаційною безпекою	Наявність вимог, викладених у пунктах 37-38 Ліцензійних умов провадження освітньої діяльності Освітня кваліфікація: Тернопільський державний педагогічний інститут, 1994 р., математика і фізика, вчитель математики і фізики. Тернопільський національний економічний університет, 2018 р., комп'ютерна інженерія, магістр з комп'ютерної інженерії. Кандидат фізико-математичних наук, 2002 р., спеціальність 01.04.10 – фізика напівпровідників і діелектриків. Тема дисертації: «Електронні та фононні теплові хвилі у напівпровідниках». Доцент кафедри безпеки інформаційних технологій, 2005 р. Доктор технічних наук, 2020 р., спеціальність 05.13.21 – системи захисту інформації. Тема дисертації: «Методи опрацювання

				004070, виданий 06.06.2022			багаторозрядних чисел в асиметричних криптосистемах на основі модулярної арифметики». Професор кафедри кібербезпеки, 2022 р. Досягнення у професійній діяльності: 1: Kasianchuk, M., Shevchuk, R., Adamyk, B., Benson, V., Shylinska, I., & Holembiovskyi, M. Affine Cipher Encryption Technique Using Residue Number System. Cryptography. 2025. № 9(2). P. 26. Kasianchuk, M., Shevchuk, R., Lishchynskyy, I., Ciura, M., Lyzun, M., Kozak, R. Application of Blockchain Technology in Emergency Management Systems: A Bibliometric Analysis. Applied Sciences. 2025. № 15(10). P. 5405. Kasianchuk, M., Yakymenko, I., Martyniuk, O., & Martyniuk, S. A Symmetric Cryptoalgorithm Based on a Hierarchical Residue Number System. International Journal of Computing. 2025. № 24(1). P. 92-101. Kasianchuk M., Yakymenko I., Martyniuk O., Martyniuk S., Yakymenko Y. Hierarchical Encryption in a Residual Number System. Proceedings. International Conference on Advanced Computer Information Technologies, ACIT, 2024. P. 496–499. Kasianchuk M., Shevchuk R., Yakymenko I. Encryption Using Residue Number System: Research Trends and Future. Proceedings. International Conference on Advanced Computer Information Technologies, ACIT, 2024. P. 552–559. Kasianchuk M., Yakymenko I., Karpinski M., Shevchuk R. Symmetric Encryption Algorithms in a Polynomial Residue Number System. Journal of Applied

							Mathematics. Hindawi. vol. 2024. P. 1-12. Kasianchuk M., Kovalchuk O., Karpinski M., Banakh S., Shevchuk R., Zagorodna N. Prediction Machine Learning Models on Propensity Convicts to Criminal Recidivism. Information. 2023. № 14. P. 161. Kasianchuk M., Kovalchuk O., Karpinski M., Babala L., and Shevchuk R. The Canonical Discriminant Model of the Environmental Security Threats. Complexity. 2023. Vol. 2023, Article ID 5584750. 15 pages. Kasianchuk M., Kovalchuk O., Karpinski M., Babala L., and Shevchuk R. Decision-Making Supporting Models Concerning the Internal Security of the State. Intl Journal of Electronics and Telecommunications. 2023. Vol. 69, N. 2. P. 301-307. Kasianchuk M., Yakymenko I., Yatskiv V., Karpinski M., Yatskiv S. Method of Multi-Bit Numbers Multiplication in Residue Number System for Asymmetric Cryptosystems. CEUR Workshop Proceedings. 2022. Vol. 3156. P. 365–377. Kasianchuk M.M., Nykolaychuk Ya.M., Yakymenko I.Z., Vozna N.Ya. Residue Number System Asymmetric Cryptoalgorithms. Cybernetics and Systems Analysis. 2022. Vol. 58, No. 4, P. 611-618. Касянчук М.М., Лотоцький О.Я., Яцків С.В., Івасьєв С.В., Тимошенко Л.М. Розробка трьохмодульної криптосистеми Рабіна на основі операції додавання та дослідження її часової складності. Інформатика та математичні методи в моделюванні. 2021. Т.11, №1-2. С. 16–26. 4: Опорний конспект лекцій з курсу «Моніторинг та управління інформаційною безпекою» для

							здобувачів освітньо-професійної програми «Кібербезпека» другого (магістерського) рівня вищої освіти спеціальності «Кібербезпека та захист інформації» / Укл.: Касянчук М.М., Івасьєв С.В. Тернопіль: ЗУНУ, 2024. 21 с. Методичні рекомендації до виконання лабораторних робіт з дисципліни «Моніторинг та управління інформаційною безпекою» для здобувачів освітньо-професійної програми «Кібербезпека» другого (магістерського) рівня вищої освіти спеціальності «Кібербезпека та захист інформації» / Укл.: Касянчук М.М., Івасьєв С.В., Нетребяк М. Р. Тернопіль: ЗУНУ, 2025. 29 с. Методичні вказівки до вивчення курсу «Моніторинг та управління інформаційною безпекою» для здобувачів освітньо-професійної програми «Кібербезпека» другого (магістерського) рівня вищої освіти / Укл.: Касянчук М.М., Івасьєв С.В. Тернопіль: ЗУНУ, 2025. 28 с. 5: Захист у 2020 р. докторської дисертації зі спеціальності 05.13.21 – системи захисту інформації. Тема дисертації: «Методи опрацювання багаторозрядних чисел в асиметричних криптосистемах на основі модулярної арифметики». 7: Член спеціалізованої вченої ради Д 58.082.02 Західноукраїнського національного університету, наказ МОН № 641 від 28.04.2025 р. 8: Член редакційної колегії: International Journal of Computing (Scopus) Комп'ютерно-інтегровані технології:

							освіта, наука, виробництво (категорія Б) 12: Касянчук М., Карпів В., Момотюк О. Математична модель захисту інформації на основі цілочисельного розщеплення. Кібербезпека та комп'ютерно-інтегровані технології. 2024. С. 115-117. Касянчук М., Гнатюк А. Метод формування квантового ключа за протоколом BB84 на основі системи залишкових класів. Кібербезпека державних інституцій та подолання кризових станів : матеріали III Міжнар. наук.-практ. конф. в 2 т. (Київ – Прага – Таллінн – Тернопіль), 14 листоп. 2024 р. / ІСЗЗІ КПІ ім. Ігоря Сікорського. Київ, 2024. Т. 1. С. 398-399. Касянчук М., Карпінський М., Голембйовський М. Афінний шифр зсуву в системі залишкових класів. Матеріали XIII Міжнар. наук.-техн. конф. Безпека інформаційних технологій (ITSec-24). Львів: ЛНУ ім. І. Франка. 2024. С. 114. Касянчук М., Ковальчук О., Бабій С. Модель оцінювання ефектів цінового шоку ринку природного газу ЄС за умов припинення експорту російського газу. Інформаційні технології та суспільство. Київ: Міжрегіональна Академія управління персоналом, 2022. Випуск 4 (6). С. 27-33. Касянчук М.М., Мельник А.О., Басістий П.В. Дослідження та порівняння машин факторизації для системи Android. Збірник матеріалів проблемної наукової міжгалузевої конференції «Кібербезпека та комп'ютерно-інтегровані технології» (КБКІТ-2022). Тернопіль, 2022. С.79-81. Kasianchuk M., Mokhun S., Fedchyshyn O., Chopyk P., Basistyi P., Matsyuk V. Stellarium Software as a

							Means of Development of Students' Research Competence While Studying Physics and Astronomy. 12th International Conference on Advanced Computer Information Technologies, ACIT 2022, 2022. P. 587–591. 15: Керівництво школярем (Руснак Андрій), який зайняв ІІ місце на ІІІ етапі Всеукраїнських конкурсів-захистів науково-дослідницьких робіт учнів - членів Національного центру «Мала академія наук України», 2022 р. 19: Учасник ГО «Автоматизація та кібербезпека». Стажування (підвищення кваліфікації): Університет у Бєльсько-Бялій (Республіка Польща), кафедра інформатики та автоматики, з 03.10.2022 р. до 02.12.2022 р., тема: «Опрацювання багаторозрядних чисел в асиметричних криптосистемах», сертифікат від 02.12.2022 р. (240 годин / 8 кредитів ECTS). ТОВ «АПІКО Україна», з 20.02.2025 р. до 04.04.2025 р., тема: «Моніторинг мережевої безпеки», довідка №15 від 2025 р. (180 годин / 6 кредитів ECTS).
324042	Шилінська Інна Феодосіївна	доцент, Основне місце роботи	Навчально-науковий інститут міжнародних відносин ім. Б.Д. Гаврилишина	Диплом спеціаліста, Чернівецький ордена Трудового Червоного Прапора державний університет, рік закінчення: 1991, спеціальність: Романо-германська філологія, Диплом кандидата наук ДК 010214, виданий 26.10.2012, Атестат доцента АД 008150, виданий	33	Ділові комунікації англійською мовою	Наявність вимог, викладених у пунктах 37-38 Ліцензійних умов провадження освітньої діяльності Освітня кваліфікація Чернівецький державний університет, 1991 р., романо-германська філологія, філолог-германіст, викладач англійської мови та літератури Кандидат педагогічних наук, 2012 р., спеціальність 13.00.04 - теорія і методика професійної освіти. Тема дисертації: «Формування культури

				29.06.2021			професійного мовлення майбутніх фахівців економічного профілю в процесі вивчення гуманітарних дисциплін» Доцент кафедри іноземних мов та інформаційно-комунікаційних технологій, 2021 р. Досягнення у професійній діяльності: 1: Шилінська І., Кузів М., Паничок Т., Бичок А. Проєктна робота на занятті з іноземної мови. Вісник науки та освіти. Серія «Філологія». 2025. № 2(32). С. 333 – 342. Шилінська І.Ф. Сучасні методи і підходи до навчання іноземних мов у вищій школі. Актуальні питання гуманітарних наук. 2024. Вип. 82, том 2, С. 441 – 446. Шилінська І., Штохман Л., Молотай Л. Лексико-синтаксичні особливості перекладу науково-технічної статті. Вчені записки Таврійського національного університету імені В. І. Вернадського. Серія: Філологія. Журналістика». 2023. Том 34 (73) № 2 Том 1. С. 221 – 225. Шилінська І.Ф., П'ятничка Т.В. Культурологічні аспекти науково-технічного перекладу як різновиду міжкультурної комунікації. Закарпатські філологічні студії. 2023. № 28. Том 2, С. 171–177. Шилінська І., Штохман Л. Формування умінь і навичок науково-технічного перекладу. Науковий вісник Міжнародного гуманітарного університету. Серія: Філологія. 2022. № 58. С. 317-320. Shylinska I., Piatnychka T. Developing verbal and analytical reasoning of IT specialists on the basis of the thesaurus centered approach. Нова філологія. Збірник наукових

							праць. Запоріжжя: Видавничий дім «Гельветика». 2021. № 81. Т.ІІ. С. 198–203. Шилінська І.Ф., Кузів М.З. Використання систем машинного перекладу під час навчання перекладу науково-технічних текстів Науковий вісник Міжнародного гуманітарного університету. Серія: Філологія. 2022. № 53. Том 2. С. 149 – 152. 10: Участь у Міжнародній програмі академічних обмінів для педагогічних працівників Erasmus + Staff Mobility for Training (Стамбул, Туреччина, університет Мармара (26 листопада – 3 грудня 2022р.). 11: Консультативні послуги з питань перекладу і редагування іноземної л-ри видавництву «Лібра Терра» з 2016 р. до тепер. 12: Шилінська І., Кавун Ю. Аналіз сучасних підходів до визначення сутності поняття «міжкультурна компетентність». Матеріали Міжнародної науково-практичної конференції «Сучасні тенденції у філологічних і педагогічних дослідженнях6 вітчизняний і міжнародний вимір». Тернопіль: ЗУНУ, 2025. С. 211 – 214 Шилінська І.Ф., Кузів М.З., Юрчишин Т. В., Бєлінська І. Д. Роль інтерактивних технологій на занятті з іноземної мови. European congress of scientific discovery. Proceedings of the 1st International scientific and practical conference. Barca Academy Publishing. Madrid, Spain. 2024. Pp. 46 - 52. Шилінська І., Штохман Л. Концептуальні підходи до методики викладання іноземних мов у немовному ЗВО. Актуальні проблеми філології та методики викладання іноземних мов у сучасному

							мультилінгвальному просторі : матеріали Всеукраїнської науково-практичної конференції, 30 жовтня 2024 р. Вінниця / гол. ред. О. М. Ігнатова. Вінниця : ТОВ «Друк». 2024. С. 75 – 77. Stockman L., Shylinska I. Teaching translation in non-linguistic university. Зб. матеріалів міжнародної наук.-практ. конф-ї.” Vocational education and training in Ukraine and the world under the conditions of European integration challenges and civilization changes in the 21-st century”, Переяслав, 14-15 вересня 2023 року. С. 185 – 188. Шилінська І.Ф., П’ятничка Т.В. Сучасні методи навчання іноземної мови майбутніх філологів. Актуальні проблеми розвитку педагогічної освіти: інновації, виклики, перспективи: збірник тез доповідей за матеріалами Міжнародної науково-практичної конференції (15 березня 2024 р., м. Мукачево). Мукачево : Вид-во МДУ, 2024. С. 132 – 134. 19: Член ГО «Асоціація викладачів англійської мови «Тісол Україна» (TESOL Ukraine), міжнародної філії TESOL Inc.» Свідоцтво №23/0023 Член ГО «Прогресильні» свідоцтво №1098/25 Стажування (підвищення кваліфікації) Тернопільський національний педагогічний університет імені Володимира Гнатюка, з 15 січня до 26 лютого 2025 року, тема: «Сучасні методи і технології викладання іноземних мов у вищій школі», довідка від 03.03. 2025р. № 51-33 (180 годин / 6 кредитів ECTS). «Міждисциплінарність у викладанні»: Майстер-клас від Острівців Прогресильності ОНУ імені І.І. Мечникова,

							ЗУНУ та ХНУ, з 22 січня до 16 лютого 2025 р., сертифікат №449/25 (60 год. / 2 кредити ECTS). Курс «Академічна доброчесність: он-лайн курс для викладачів», наданий викладачами курсу через платформу масових відкритих он-лайн курсів Prometheus, сертифікат від 16.09.2025 р. (60 годин / 2 кредити ECTS).
313785	Якименко Ігор Зіновійович	декан, Основне місце роботи	Факультет комп'ютерних інформаційних технологій	Диплом спеціаліста, Київський університет імені Тараса Шевченка, рік закінчення: 1998, спеціальність: 080101 Математика, Диплом магістра, Західноукраїнський національний університет, рік закінчення: 2022, спеціальність: 125 Кібербезпека, Диплом кандидата наук ДК 009081, виданий 26.09.2012, Атестат доцента АД 001127, виданий 05.07.2018	18	Дослідження і проектування систем захисту інформації	Наявність вимог, викладених у пунктах 37-38 Ліцензійних умов провадження освітньої діяльності Освітня кваліфікація: Київський університет ім. Т.Шевченка, 1998 р., математика, математик-викладач. Західноукраїнський національний університет, 2022 р., кібербезпека, магістр з кібербезпеки. Кандидат технічних наук, 2012 р., спеціальність 05.13.05 – комп'ютерні системи та компоненти. Тема дисертації: «Методи та засоби опрацювання інформаційних потоків в комп'ютерних мережах за умови застосування еліптичних кривих». Доцент кафедри комп'ютерної інженерії, 2018 р. Досягнення у професійній діяльності: 1: Yakymenko I., Kasianchuk, M., Martyniuk, O., & Martyniuk, S. A Symmetric Cryptoalgorithm Based on a Hierarchical Residue Number System. International Journal of Computing. 2025. № 24(1). P. 92-101. Yakymenko I., Kasianchuk M., Shylinska I. A Method for Polynomial Recovery from its Resudues Based on Addition in Z[x] Ring. Informatics and Mathematical Methods in Simulation. 2024. Vol.14, No. 4. P. 305-313.

							Yakymenko I., Karpinski M., Shevchuk R., Kasianchuk M. Symmetric Encryption Algorithms in a Polynomial Residue Number System. Journal of Applied Mathematics. 2024. P. 1-12. Yakymenko I., Kasianchuk M., Yatskiv S., Gomotiuk O., Bilovus L. The Method of Joint Execution of the Basic Operations of the Rabin Cryptosystem. CEUR Workshop Proceedings. 2023, № 3373. P. 425–436. Yakymenko I., Kasianchuk M., Yatskiv V., Karpinski M., Yatskiv S. Method of Multi-Bit Numbers Multiplication in Residue Number System for Asymmetric Cryptosystems. CEUR Workshop Proceedings, 2022. № 3156. P. 365–377. Yakymenko I., Nykolaychuk Ya., Vozna N., Kasianchuk M. Residue Number System Asymmetric Cryptoalgorithms. Cybernetics and Systems Analysis. 2022. Vol. 58, No. 4, P.611-618. Якименко І.З., Касянчук М.М., Николайчук Я.М. Симетричні криптоалгоритми у системі залишкових класів. Cybernetics and Systems Analysis. 2021. Vol 57, Issue 2. P.184-189. 4: Опорний конспект лекцій з дисципліни «Дослідження і проектування систем захисту інформації» для студентів освітньо-професійної програми підготовки магістра галузі знань 12 «Інформаційні технології» спеціальності 125 «Кібербезпека та захист інформації» / Укл.: Якименко І.З. Тернопіль : ФОП Осадца Ю.В., 2024. 89 с. Методичні рекомендації до виконання лабораторних робіт з дисципліни «Дослідження і проектування систем захисту інформації» для здобувачів

							спеціальності Кібербезпека та захист інформації. / Укл.:Якименко І.З., Кулина С.В. Тернопіль: ЗУНУ. 2024. 57 с. Методичні вказівки до вивчення курсу «Дослідження і проектування систем захисту інформації» для здобувачів освітньо-професійної програми «Кібербезпека» другого (магістерського) рівня вищої освіти / Укл.: Якименко І.З. Тернопіль: ЗУНУ, 2025. 31 с. 8: Керівник проєкту КБ-49-2023 «Стійкі до криптоаналізу методи та засоби шифрування в поліноміальних системах залишкових класів», держ. реєстраційний номер: 0123U104713. Термін виконання: 10.2023 р. – 12.2023 р. 12: Yakymenko I., Shevchuk R., Kasianchuk M. Encryption Using Residue Number System: Research Trends and Future Challenges. Proceedings International Conference on Advanced Computer Information Technologies, ACIT2024, 2024, pp. 552–559. Yakymenko I., Martyniuk O., Martyniuk S., Yakymenko Y., Kasianchuk M. Hierarchical Encryption in a Residual Number System. Proceedings International Conference on Advanced Computer Information Technologies, ACIT, 2024, pp. 496–499. Yakymenko I., Shevchuk R., Karpinski M., Kasianchuk M., Melnyk A., Tykhyi R. Software for Improve the Security of Kubernetes-based CI/CD Pipeline. Proceedings International Conference on Advanced Computer Information Technologies, ACIT2023, 2023, pp. 420–425. Yakymenko I.,

							Kasianchuk M., Shylinska I., Shevchuk R., Yatskiv V., Karpinski M. Polynomial Rabin Cryptosystem Based on the Operation of Addition. 12th International Conference on Advanced Computer Information Technologies, ACIT 2022, 2022, pp. 345–350. Yakymenko I., Kasianchuk M., Yatskiv V., Shevchuk R., Koval V., Yatskiv S. Sustainability and Time Complexity Estimation of Cryptographic Algorithms Main Operations on Elliptic Curves. 2021 11th International Conference on Advanced Computer Information Technologies (ACIT). Pp. 494-498. 19: Учасник ГО «Автоматизація та кібербезпека». Стажування (підвищення кваліфікації): Університет у Бєльсько-Бялій (Республіка Польща), кафедра інформатики та автоматики, з 03.10.2022 р. до 02.12.2022 р., тема: «Комплексні системи захисту інформації», сертифікат від 02.12.2022 р. (240 годин / 8 кредитів ECTS). ТОВ «Ті-СПАРК» з 13 січня 2025 року по 21 лютого 2025 року, тема: «Застосування методів дискретної математики для моделювання та проектування систем інформаційної безпеки», довідка № 2/21 від 21.02.2025 р. (180 годин/ 6 кредитів ECTS). Сертифікати: Сертифікат про закінчення курсу «Digital Forensic» від міжнародного проєкту USAID «Кібербезпека критично важливої інфраструктури України», з 11 липня по 31 серпня 2022 р. (180 год / 6 кредитів ECTS).

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**
РН24. Впроваджувати повний цикл аналізу артефактів; проводити відновлення видалених / пошкоджених файлів та інших даних з цифрових носіїв та / або систем.	☐	Цифрова криміналістика	лекції, лабораторні роботи, тренінги, індивідуальні заняття, самостійне навчання на основі підручників і конспектів.	поточне тестування та поточне опитування; підсумкове модульне тестування та опитування за кожним заліковим модулем; оцінювання виконання лабораторних робіт; оцінювання відповідей на питання тренінгу; оцінювання самостійної роботи.
		Переддипломна практика	індивідуальні консультації з керівником практики; самостійна робота; аналіз та систематизація результатів досліджень і спостережень.	оцінювання змісту та оформлення звіту; захист результатів практики.
		Підготовка та захист кваліфікаційної роботи	аналіз, синтез, систематизація, узагальнення; наукове консультування; самостійний пошук та критичний аналіз наукових джерел і літератури; формування висновків і рекомендацій.	перевірка роботи на відсутність ознак академічного плагіату та відповідність вимогам до оформлення; оцінювання змісту та актуальності роботи, рівня теоретичної і практичної підготовки здобувача, обґрунтованості висновків та рекомендацій, презентації результатів; захист кваліфікаційної роботи.
РН22. Планувати та виконувати експериментальні і теоретичні дослідження, висувати і перевіряти гіпотези, обирати для цього придатні методи та інструменти, здійснювати статистичну обробку даних, оцінювати достовірність результатів досліджень, аргументувати висновки.	☒	Підготовка та захист кваліфікаційної роботи	аналіз, синтез, систематизація, узагальнення; наукове консультування; самостійний пошук та критичний аналіз наукових джерел і літератури; формування висновків і рекомендацій.	перевірка роботи на відсутність ознак академічного плагіату та відповідність вимогам до оформлення; оцінювання змісту та актуальності роботи, рівня теоретичної і практичної підготовки здобувача, обґрунтованості висновків та рекомендацій, презентації результатів; захист кваліфікаційної роботи.
		Переддипломна практика	індивідуальні консультації з керівником практики; самостійна робота; аналіз та систематизація результатів досліджень і спостережень.	оцінювання змісту та оформлення звіту; захист результатів практики.
		Дослідження і проектування систем захисту інформації	лекції, лабораторні роботи, тренінги, індивідуальні заняття, робота в групах, робота в Інтернет, самостійне навчання на основі підручників і конспектів.	поточне тестування та поточне опитування; підсумкове модульне тестування та опитування за кожним змістовим модулем; оцінювання виконання лабораторних робіт; оцінювання відповідей на питання тренінгу; оцінювання самостійної роботи; підсумковий

				екзамен.
		Тестування комп'ютерних систем на проникнення	лекції, лабораторні роботи, тренінги, індивідуальні заняття, робота в Інтернет, самостійне навчання на основі підручників і конспектів.	поточне опитування; оцінювання виконання лабораторних робіт; підсумковий модульний контроль за кожним змістовим модулем; оцінювання тренінгу; оцінювання результатів самостійної роботи; підсумковий екзамен.
		Методологія наукових досліджень	лекції, практичні заняття, самостійне навчання на основі підручників і конспектів, тренінги, індивідуальні заняття, робота в Інтернет.	поточне опитування; поточне оцінювання; підсумковий модульний контроль за кожним змістовим модулем; оцінювання тренінгів; оцінювання результатів самостійної роботи; підсумковий екзамен.
РН21. Використовувати методи натурного, фізичного і комп'ютерного моделювання для дослідження процесів, які стосуються інформаційної безпеки та/або кібербезпеки.	☒	Підготовка та захист кваліфікаційної роботи	аналіз, синтез, систематизація, узагальнення; наукове консультування; самостійний пошук та критичний аналіз наукових джерел і літератури; формування висновків і рекомендацій.	перевірка роботи на відсутність ознак академічного плагіату та відповідність вимогам до оформлення; оцінювання змісту та актуальності роботи, рівня теоретичної і практичної підготовки здобувача, обґрунтованості висновків та рекомендацій, презентації результатів; захист кваліфікаційної роботи.
		Переддипломна практика	індивідуальні консультації з керівником практики; самостійна робота; аналіз та систематизація результатів досліджень і спостережень.	оцінювання змісту та оформлення звіту; захист результатів практики.
		Дослідження і проектування систем захисту інформації	лекції, лабораторні роботи, тренінги, індивідуальні заняття, робота в групах, робота в Інтернет, самостійне навчання на основі підручників і конспектів.	поточне тестування та поточне опитування; підсумкове модульне тестування та опитування за кожним змістовим модулем; оцінювання виконання лабораторних робіт; оцінювання відповідей на питання тренінгу; оцінювання самостійної роботи; підсумковий екзамен.
РН20. Ставити та вирішувати складні інженерно-прикладні та наукові задачі інформаційної безпеки та/або кібербезпеки з урахуванням вимог вітчизняних та світових стандартів та кращих практик.	☒	Підготовка та захист кваліфікаційної роботи	аналіз, синтез, систематизація, узагальнення; наукове консультування; самостійний пошук та критичний аналіз наукових джерел і літератури; формування висновків і рекомендацій.	перевірка роботи на відсутність ознак академічного плагіату та відповідність вимогам до оформлення; оцінювання змісту та актуальності роботи, рівня теоретичної і практичної підготовки здобувача, обґрунтованості висновків та рекомендацій, презентації результатів; захист кваліфікаційної роботи.
		Переддипломна практика	індивідуальні консультації з керівником практики; самостійна робота; аналіз та систематизація результатів досліджень і спостережень.	оцінювання змісту та оформлення звіту; захист результатів практики.
		Дослідження і проектування систем захисту інформації	лекції, лабораторні роботи, тренінги, індивідуальні заняття, робота в групах, робота в Інтернет, самостійне навчання на	поточне тестування та поточне опитування; підсумкове модульне тестування та опитування за кожним змістовим модулем;

			основі підручників і конспектів.	оцінювання виконання лабораторних робіт; оцінювання відповідей на питання тренінгу; оцінювання самостійної роботи; підсумковий екзамен.
		Моніторинг та управління інформаційною безпекою	лекції, лабораторні роботи, тренінги, індивідуальні заняття, робота в Інтернет, самостійне навчання на основі підручників і конспектів	поточне тестування та опитування; підсумкове тестування за кожним змістовим модулем; оцінювання виконання лабораторних робіт; оцінювання тренінгів; оцінювання результатів самостійної роботи; підсумковий екзамен.
РН19. 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.	☒	Цифрова криміналістика	лекції, лабораторні роботи, тренінги, індивідуальні заняття, самостійне навчання на основі підручників і конспектів.	поточне тестування та поточне опитування; підсумкове модульне тестування та опитування за кожним заліковим модулем; оцінювання виконання лабораторних робіт; оцінювання відповідей на питання тренінгу; оцінювання самостійної роботи.
		Дослідження і проектування систем захисту інформації	лекції, лабораторні роботи, тренінги, індивідуальні заняття, робота в групах, робота в Інтернет, самостійне навчання на основі підручників і конспектів.	поточне тестування та поточне опитування; підсумкове модульне тестування та опитування за кожним змістовим модулем; оцінювання виконання лабораторних робіт; оцінювання відповідей на питання тренінгу; оцінювання самостійної роботи; підсумковий екзамен.
		Підготовка та захист кваліфікаційної роботи	аналіз, синтез, систематизація, узагальнення; наукове консультування; самостійний пошук та критичний аналіз наукових джерел і літератури; формування висновків і рекомендацій.	перевірка роботи на відсутність ознак академічного плагіату та відповідність вимогам до оформлення; оцінювання змісту та актуальності роботи, рівня теоретичної і практичної підготовки здобувача, обґрунтованості висновків та рекомендацій, презентації результатів; захист кваліфікаційної роботи.
		Переддипломна практика	індивідуальні консультації з керівником практики; самостійна робота; аналіз та систематизація результатів досліджень і спостережень.	оцінювання змісту та оформлення звіту; захист результатів практики.
РН18. Планувати навчання, а також супроводжувати та контролювати роботу з персоналом у напряму інформаційної безпеки та/або кібербезпеки.	☒	Тестування комп'ютерних систем на проникнення	лекції, лабораторні роботи, тренінги, індивідуальні заняття, робота в Інтернет, самостійне навчання на основі підручників і конспектів.	поточне опитування; оцінювання виконання лабораторних робіт; підсумковий модульний контроль за кожним змістовим модулем; оцінювання тренінгу; оцінювання результатів самостійної роботи; підсумковий екзамен.
		Моніторинг та управління інформаційною безпекою	лекції, лабораторні роботи, тренінги, індивідуальні заняття, робота в Інтернет, самостійне навчання на основі підручників і конспектів	поточне тестування та опитування; підсумкове тестування за кожним змістовим модулем; оцінювання виконання лабораторних робіт;

				оцінювання тренінгів; оцінювання результатів самостійної роботи; підсумковий екзамен.
		Переддипломна практика	індивідуальні консультації з керівником практики; самостійна робота; аналіз та систематизація результатів досліджень і спостережень.	оцінювання змісту та оформлення звіту; захист результатів практики.
		Підготовка та захист кваліфікаційної роботи	аналіз, синтез, систематизація, узагальнення; наукове консультування; самостійний пошук та критичний аналіз наукових джерел і літератури; формування висновків і рекомендацій.	перевірка роботи на відсутність ознак академічного плагіату та відповідність вимогам до оформлення; оцінювання змісту та актуальності роботи, рівня теоретичної і практичної підготовки здобувача, обґрунтованості висновків та рекомендацій, презентації результатів; захист кваліфікаційної роботи.
РН17. Планувати та виконувати експериментальні і теоретичні дослідження, висувати і перевіряти гіпотези, обирати для цього придатні методи та інструменти, здійснювати статистичну обробку даних, оцінювати достовірність результатів досліджень, аргументувати висновки	☒	Підготовка та захист кваліфікаційної роботи	аналіз, синтез, систематизація, узагальнення; наукове консультування; самостійний пошук та критичний аналіз наукових джерел і літератури; формування висновків і рекомендацій.	перевірка роботи на відсутність ознак академічного плагіату та відповідність вимогам до оформлення; оцінювання змісту та актуальності роботи, рівня теоретичної і практичної підготовки здобувача, обґрунтованості висновків та рекомендацій, презентації результатів; захист кваліфікаційної роботи.
		Переддипломна практика	індивідуальні консультації з керівником практики; самостійна робота; аналіз та систематизація результатів досліджень і спостережень.	оцінювання змісту та оформлення звіту; захист результатів практики.
		Ділові комунікації англійською мовою	лекції, практичні заняття, тренінги, самостійне навчання на основі підручників і конспектів.	поточне опитування; залікове модульне тестування та опитування; оцінювання результатів виконання самостійної роботи; оцінка за виконані завдання під час тренінгу; залік; інші види індивідуальних та групових завдань.
		Методологія наукових досліджень	лекції, практичні заняття, самостійне навчання на основі підручників і конспектів, тренінги, індивідуальні заняття, робота в Інтернет.	поточне опитування; поточне оцінювання; підсумковий модульний контроль за кожним змістовим модулем; оцінювання тренінгів; оцінювання результатів самостійної роботи; підсумковий екзамен.
РН16. 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	☒	Підготовка та захист кваліфікаційної роботи	аналіз, синтез, систематизація, узагальнення; наукове консультування; самостійний пошук та критичний аналіз наукових джерел і літератури; формування висновків і рекомендацій.	перевірка роботи на відсутність ознак академічного плагіату та відповідність вимогам до оформлення; оцінювання змісту та актуальності роботи, рівня теоретичної і практичної підготовки здобувача, обґрунтованості висновків та рекомендацій, презентації результатів; захист кваліфікаційної роботи.
		Переддипломна	індивідуальні консультації з	оцінювання змісту та

оптимізації, прогнозування та прийняття рішень.		практика	керівником практики; самостійна робота; аналіз та систематизація результатів досліджень і спостережень.	оформлення звіту; захист результатів практики.
		Моніторинг та управління інформаційною безпекою	лекції, лабораторні роботи, тренінги, індивідуальні заняття, робота в Інтернет, самостійне навчання на основі підручників і конспектів	поточне тестування та опитування; підсумкове тестування за кожним змістовим модулем; оцінювання виконання лабораторних робіт; оцінювання тренінгів; оцінювання результатів самостійної роботи; підсумковий екзамен.
РН15. Зрозуміло і 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.	☒	Підготовка та захист кваліфікаційної роботи	аналіз, синтез, систематизація, узагальнення; наукове консультування; самостійний пошук та критичний аналіз наукових джерел і літератури; формування висновків і рекомендацій.	перевірка роботи на відсутність ознак академічного плагіату та відповідність вимогам до оформлення; оцінювання змісту та актуальності роботи, рівня теоретичної і практичної підготовки здобувача, обґрунтованості висновків та рекомендацій, презентації результатів; захист кваліфікаційної роботи.
		Цифрова криміналістика	лекції, лабораторні роботи, тренінги, індивідуальні заняття, самостійне навчання на основі підручників і конспектів.	поточне тестування та поточне опитування; підсумкове модульне тестування та опитування за кожним заліковим модулем; оцінювання виконання лабораторних робіт; оцінювання відповідей на питання тренінгу; оцінювання самостійної роботи.
		Ділові комунікації англійською мовою	лекції, практичні заняття, тренінги, самостійне навчання на основі підручників і конспектів.	поточне опитування; залікове модульне тестування та опитування; оцінювання результатів виконання самостійної роботи; оцінка за виконані завдання під час тренінгу; залік; інші види індивідуальних та групових завдань.
		Методологія наукових досліджень	лекції, практичні заняття, самостійне навчання на основі підручників і конспектів, тренінги, індивідуальні заняття, робота в Інтернет.	поточне опитування; поточне оцінювання; підсумковий модульний контроль за кожним змістовим модулем; оцінювання тренінгів; оцінювання результатів самостійної роботи; підсумковий екзамен.
		Переддипломна практика	індивідуальні консультації з керівником практики; самостійна робота; аналіз та систематизація результатів досліджень і спостережень.	оцінювання змісту та оформлення звіту; захист результатів практики.
РН14. Аналізувати, розробляти і супроводжувати систему аудиту та моніторингу ефективності функціонування інформаційних систем і технологій, бізнес\операційних	☒	Підготовка та захист кваліфікаційної роботи	аналіз, синтез, систематизація, узагальнення; наукове консультування; самостійний пошук та критичний аналіз наукових джерел і літератури; формування висновків і рекомендацій.	перевірка роботи на відсутність ознак академічного плагіату та відповідність вимогам до оформлення; оцінювання змісту та актуальності роботи, рівня теоретичної і практичної підготовки здобувача, обґрунтованості висновків та рекомендацій, презентації результатів;

процесів у сфері інформаційної та\або кібербезпеки в цілому.				захист кваліфікаційної роботи.
		Переддипломна практика	індивідуальні консультації з керівником практики; самостійна робота; аналіз та систематизація результатів досліджень і спостережень.	оцінювання змісту та оформлення звіту; захист результатів практики.
		Моніторинг та управління інформаційною безпекою	лекції, лабораторні роботи, тренінги, індивідуальні заняття, робота в Інтернет, самостійне навчання на основі підручників і конспектів	поточне тестування та опитування; підсумкове тестування за кожним змістовим модулем; оцінювання виконання лабораторних робіт; оцінювання тренінгів; оцінювання результатів самостійної роботи; підсумковий екзамен.
РН23. Обґрунтовувати вибір програмного забезпечення, устаткування 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.	☒	Підготовка та захист кваліфікаційної роботи	аналіз, синтез, систематизація, узагальнення; наукове консультування; самостійний пошук та критичний аналіз наукових джерел і літератури; формування висновків і рекомендацій.	перевірка роботи на відсутність ознак академічного плагіату та відповідність вимогам до оформлення; оцінювання змісту та актуальності роботи, рівня теоретичної і практичної підготовки здобувача, обґрунтованості висновків та рекомендацій, презентації результатів; захист кваліфікаційної роботи.
		Переддипломна практика	індивідуальні консультації з керівником практики; самостійна робота; аналіз та систематизація результатів досліджень і спостережень.	оцінювання змісту та оформлення звіту; захист результатів практики.
		Тестування комп'ютерних систем на проникнення	лекції, лабораторні роботи, тренінги, індивідуальні заняття, робота в Інтернет, самостійне навчання на основі підручників і конспектів.	поточне опитування; оцінювання виконання лабораторних робіт; підсумковий модульний контроль за кожним змістовим модулем; оцінювання тренінгу; оцінювання результатів самостійної роботи; підсумковий екзамен.
		Моніторинг та управління інформаційною безпекою	лекції, лабораторні роботи, тренінги, індивідуальні заняття, робота в Інтернет, самостійне навчання на основі підручників і конспектів	поточне тестування та опитування; підсумкове тестування за кожним змістовим модулем; оцінювання виконання лабораторних робіт; оцінювання тренінгів; оцінювання результатів самостійної роботи; підсумковий екзамен.
		Методологія наукових досліджень	лекції, практичні заняття, самостійне навчання на основі підручників і конспектів, тренінги, індивідуальні заняття, робота в Інтернет.	поточне опитування; поточне оцінювання; підсумковий модульний контроль за кожним змістовим модулем; оцінювання тренінгів; оцінювання результатів самостійної роботи; підсумковий екзамен.
РН13. Досліджувати, розробляти, впроваджувати та використовувати методи та засоби криптографічного та технічного захисту інформації	☒	Підготовка та захист кваліфікаційної роботи	аналіз, синтез, систематизація, узагальнення; наукове консультування; самостійний пошук та критичний аналіз наукових джерел і літератури; формування висновків і рекомендацій.	перевірка роботи на відсутність ознак академічного плагіату та відповідність вимогам до оформлення; оцінювання змісту та актуальності роботи, рівня теоретичної і практичної підготовки здобувача, обґрунтованості

бізнес/операційних процесів, а також аналізувати і надавати оцінку ефективності їх використання в інформаційних системах, на об'єктах інформаційної діяльності та критичної інфраструктури.				висновків та рекомендацій, презентації результатів; захист кваліфікаційної роботи.
		Переддипломна практика	індивідуальні консультації з керівником практики; самостійна робота; аналіз та систематизація результатів досліджень і спостережень.	оцінювання змісту та оформлення звіту; захист результатів практики.
		Дослідження і проектування систем захисту інформації	лекції, лабораторні роботи, тренінги, індивідуальні заняття, робота в групах, робота в Інтернет, самостійне навчання на основі підручників і конспектів.	поточне тестування та поточне опитування; підсумкове модульне тестування та опитування за кожним змістовим модулем; оцінювання виконання лабораторних робіт; оцінювання відповідей на питання тренінгу; оцінювання самостійної роботи; підсумковий екзамен.
		Тестування комп'ютерних систем на проникнення	лекції, лабораторні роботи, тренінги, індивідуальні заняття, робота в Інтернет, самостійне навчання на основі підручників і конспектів.	поточне опитування; оцінювання виконання лабораторних робіт; підсумковий модульний контроль за кожним змістовим модулем; оцінювання тренінгу; оцінювання результатів самостійної роботи; підсумковий екзамен.
РН10. Забезпечувати безперервність бізнес/операційних процесів, а також виявляти уразливості інформаційних систем та ресурсів, аналізувати та оцінювати ризики для інформаційної безпеки та/або кібербезпеки організації.	☒	Підготовка та захист кваліфікаційної роботи	аналіз, синтез, систематизація, узагальнення; наукове консультування; самостійний пошук та критичний аналіз наукових джерел і літератури; формування висновків і рекомендацій.	перевірка роботи на відсутність ознак академічного плагіату та відповідність вимогам до оформлення; оцінювання змісту та актуальності роботи, рівня теоретичної і практичної підготовки здобувача, обґрунтованості висновків та рекомендацій, презентації результатів; захист кваліфікаційної роботи.
		Переддипломна практика	індивідуальні консультації з керівником практики; самостійна робота; аналіз та систематизація результатів досліджень і спостережень.	оцінювання змісту та оформлення звіту; захист результатів практики.
		Аналіз шкідливого програмного забезпечення	лекції, лабораторні роботи, тренінги, індивідуальні заняття, робота в Інтернет, самостійне навчання на основі підручників і конспектів.	поточне тестування та опитування; підсумкове тестування за кожним змістовим модулем; оцінювання виконання лабораторних робіт; оцінювання тренінгів; оцінювання результатів самостійної роботи; підсумковий екзамен.
		Тестування комп'ютерних систем на проникнення	лекції, лабораторні роботи, тренінги, індивідуальні заняття, робота в Інтернет, самостійне навчання на основі підручників і конспектів.	поточне опитування; оцінювання виконання лабораторних робіт; підсумковий модульний контроль за кожним змістовим модулем; оцінювання тренінгу; оцінювання результатів самостійної роботи; підсумковий екзамен.
РН11. Аналізувати, контролювати та забезпечувати ефективне	☒	Підготовка та захист кваліфікаційної роботи	аналіз, синтез, систематизація, узагальнення; наукове консультування;	перевірка роботи на відсутність ознак академічного плагіату та відповідність вимогам до

функціонування системи управління доступом до інформаційних ресурсів відповідно до встановлених стратегії і політики інформаційної безпеки та/або кібербезпеки організації.			самостійний пошук та критичний аналіз наукових джерел і літератури; формування висновків і рекомендацій.	оформлення; оцінювання змісту та актуальності роботи, рівня теоретичної і практичної підготовки здобувача, обґрунтованості висновків та рекомендацій, презентації результатів; захист кваліфікаційної роботи.
		Переддипломна практика	індивідуальні консультації з керівником практики; самостійна робота; аналіз та систематизація результатів досліджень і спостережень.	оцінювання змісту та оформлення звіту; захист результатів практики.
		Тестування комп'ютерних систем на проникнення	лекції, лабораторні роботи, тренінги, індивідуальні заняття, робота в Інтернет, самостійне навчання на основі підручників і конспектів.	поточне опитування; оцінювання виконання лабораторних робіт; підсумковий модульний контроль за кожним змістовим модулем; оцінювання тренінгу; оцінювання результатів самостійної роботи; підсумковий екзамен.
		Моніторинг та управління інформаційною безпекою	лекції, лабораторні роботи, тренінги, індивідуальні заняття, робота в Інтернет, самостійне навчання на основі підручників і конспектів	поточне тестування та опитування; підсумкове тестування за кожним змістовим модулем; оцінювання виконання лабораторних робіт; оцінювання тренінгів; оцінювання результатів самостійної роботи; підсумковий екзамен.
РН12. 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.	☒	Підготовка та захист кваліфікаційної роботи	аналіз, синтез, систематизація, узагальнення; наукове консультування; самостійний пошук та критичний аналіз наукових джерел і літератури; формування висновків і рекомендацій.	перевірка роботи на відсутність ознак академічного плагіату та відповідність вимогам до оформлення; оцінювання змісту та актуальності роботи, рівня теоретичної і практичної підготовки здобувача, обґрунтованості висновків та рекомендацій, презентації результатів; захист кваліфікаційної роботи.
		Цифрова криміналістика	лекції, лабораторні роботи, тренінги, індивідуальні заняття, самостійне навчання на основі підручників і конспектів.	поточне тестування та поточне опитування; підсумкове модульне тестування та опитування за кожним заліковим модулем; оцінювання виконання лабораторних робіт; оцінювання відповідей на питання тренінгу; оцінювання самостійної роботи.
		Переддипломна практика	індивідуальні консультації з керівником практики; самостійна робота; аналіз та систематизація результатів досліджень і спостережень.	оцінювання змісту та оформлення звіту; захист результатів практики.
		Аналіз шкідливого програмного забезпечення	лекції, лабораторні роботи, тренінги, індивідуальні заняття, робота в Інтернет, самостійне навчання на основі підручників і конспектів.	поточне тестування та опитування; підсумкове тестування за кожним змістовим модулем; оцінювання виконання лабораторних робіт; оцінювання тренінгів; оцінювання результатів самостійної роботи; підсумковий екзамен.

РН1. 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.	☒	Підготовка та захист кваліфікаційної роботи	аналіз, синтез, систематизація, узагальнення; наукове консультування; самостійний пошук та критичний аналіз наукових джерел і літератури; формування висновків і рекомендацій.	перевірка роботи на відсутність ознак академічного плагіату та відповідність вимогам до оформлення; оцінювання змісту та актуальності роботи, рівня теоретичної і практичної підготовки здобувача, обґрунтованості висновків та рекомендацій, презентації результатів; захист кваліфікаційної роботи.
		Переддипломна практика	індивідуальні консультації з керівником практики; самостійна робота; аналіз та систематизація результатів досліджень і спостережень.	оцінювання змісту та оформлення звіту; захист результатів практики.
		Ділові комунікації англійською мовою	лекції, практичні заняття, тренінги, самостійне навчання на основі підручників і конспектів.	поточне опитування; залікове модульне тестування та опитування; оцінювання результатів виконання самостійної роботи; оцінка за виконані завдання під час тренінгу; залік; інші види індивідуальних та групових завдань.
		Методологія наукових досліджень	лекції, практичні заняття, самостійне навчання на основі підручників і конспектів, тренінги, індивідуальні заняття, робота в Інтернет.	поточне опитування; поточне оцінювання; підсумковий модульний контроль за кожним змістовим модулем; оцінювання тренінгів; оцінювання результатів самостійної роботи; підсумковий екзамен.
РН2. Інтегрувати фундаментальні та спеціальні знання для розв'язування складних задач інформаційної безпеки та/або кібербезпеки у широких або мультидисципліна рних контекстах.	☒	Підготовка та захист кваліфікаційної роботи	аналіз, синтез, систематизація, узагальнення; наукове консультування; самостійний пошук та критичний аналіз наукових джерел і літератури; формування висновків і рекомендацій.	перевірка роботи на відсутність ознак академічного плагіату та відповідність вимогам до оформлення; оцінювання змісту та актуальності роботи, рівня теоретичної і практичної підготовки здобувача, обґрунтованості висновків та рекомендацій, презентації результатів; захист кваліфікаційної роботи.
		Переддипломна практика	індивідуальні консультації з керівником практики; самостійна робота; аналіз та систематизація результатів досліджень і спостережень.	оцінювання змісту та оформлення звіту; захист результатів практики.
		Дослідження і проектування систем захисту інформації	лекції, лабораторні роботи, тренінги, індивідуальні заняття, робота в групах, робота в Інтернет, самостійне навчання на основі підручників і конспектів.	поточне тестування та поточне опитування; підсумкове модульне тестування та опитування за кожним змістовим модулем; оцінювання виконання лабораторних робіт; оцінювання відповідей на питання тренінгу; оцінювання самостійної роботи; підсумковий екзамен.
		Аналіз шкідливого програмного забезпечення	лекції, лабораторні роботи, тренінги, індивідуальні заняття, робота в Інтернет, самостійне навчання на основі підручників і конспектів.	поточне тестування та опитування; підсумкове тестування за кожним змістовим модулем; оцінювання виконання лабораторних робіт;

				оцінювання тренінгів; оцінювання результатів самостійної роботи; підсумковий екзамен.
		Методологія наукових досліджень	лекції, практичні заняття, самостійне навчання на основі підручників і конспектів, тренінги, індивідуальні заняття, робота в Інтернет.	поточне опитування; поточне оцінювання; підсумковий модульний контроль за кожним змістовим модулем; оцінювання тренінгів; оцінювання результатів самостійної роботи; підсумковий екзамен.
РН3. Провадити дослідницьку та/або інноваційну діяльність в сфері інформаційної безпеки та/або кібербезпеки, а також в сфері технічного та криптографічного захисту інформації у кіберпросторі	☒	Підготовка та захист кваліфікаційної роботи	аналіз, синтез, систематизація, узагальнення; наукове консультування; самостійний пошук та критичний аналіз наукових джерел і літератури; формування висновків і рекомендацій.	перевірка роботи на відсутність ознак академічного плагіату та відповідність вимогам до оформлення; оцінювання змісту та актуальності роботи, рівня теоретичної і практичної підготовки здобувача, обґрунтованості висновків та рекомендацій, презентації результатів; захист кваліфікаційної роботи.
		Переддипломна практика	індивідуальні консультації з керівником практики; самостійна робота; аналіз та систематизація результатів досліджень і спостережень.	оцінювання змісту та оформлення звіту; захист результатів практики.
		Дослідження і проектування систем захисту інформації	лекції, лабораторні роботи, тренінги, індивідуальні заняття, робота в групах, робота в Інтернет, самостійне навчання на основі підручників і конспектів.	поточне тестування та поточне опитування; підсумкове модульне тестування та опитування за кожним змістовим модулем; оцінювання виконання лабораторних робіт; оцінювання відповідей на питання тренінгу; оцінювання самостійної роботи; підсумковий екзамен.
		Методологія наукових досліджень	лекції, практичні заняття, самостійне навчання на основі підручників і конспектів, тренінги, індивідуальні заняття, робота в Інтернет.	поточне опитування; поточне оцінювання; підсумковий модульний контроль за кожним змістовим модулем; оцінювання тренінгів; оцінювання результатів самостійної роботи; підсумковий екзамен.
РН4. Застосовувати, інтегрувати, розробляти, впроваджувати та удосконалювати сучасні інформаційні технології, фізичні та математичні методи і моделі в сфері інформаційної безпеки та/або кібербезпеки.	☒	Підготовка та захист кваліфікаційної роботи	аналіз, синтез, систематизація, узагальнення; наукове консультування; самостійний пошук та критичний аналіз наукових джерел і літератури; формування висновків і рекомендацій.	перевірка роботи на відсутність ознак академічного плагіату та відповідність вимогам до оформлення; оцінювання змісту та актуальності роботи, рівня теоретичної і практичної підготовки здобувача, обґрунтованості висновків та рекомендацій, презентації результатів; захист кваліфікаційної роботи.
		Переддипломна практика	індивідуальні консультації з керівником практики; самостійна робота; аналіз та систематизація результатів досліджень і спостережень.	оцінювання змісту та оформлення звіту; захист результатів практики.
		Дослідження і проектування систем захисту інформації	лекції, лабораторні роботи, тренінги, індивідуальні заняття, робота в групах, робота в Інтернет,	поточне тестування та поточне опитування; підсумкове модульне тестування та опитування за

			самостійне навчання на основі підручників і конспектів.	кожним змістовим модулем; оцінювання виконання лабораторних робіт; оцінювання відповідей на питання тренінгу; оцінювання самостійної роботи; підсумковий екзамен.
РН6. Аналізувати та оцінювати захищеність систем, комплексів та засобів кіберзахисту, технології створення та використання спеціалізованого програмного забезпечення.	☒	Тестування комп'ютерних систем на проникнення	лекції, лабораторні роботи, тренінги, індивідуальні заняття, робота в Інтернет, самостійне навчання на основі підручників і конспектів.	поточне опитування; оцінювання виконання лабораторних робіт; підсумковий модульний контроль за кожним змістовим модулем; оцінювання тренінгу; оцінювання результатів самостійної роботи; підсумковий екзамен.
		Аналіз шкідливого програмного забезпечення	лекції, лабораторні роботи, тренінги, індивідуальні заняття, робота в Інтернет, самостійне навчання на основі підручників і конспектів.	поточне тестування та опитування; підсумкове тестування за кожним змістовим модулем; оцінювання виконання лабораторних робіт; оцінювання тренінгів; оцінювання результатів самостійної роботи; підсумковий екзамен.
		Підготовка та захист кваліфікаційної роботи	аналіз, синтез, систематизація, узагальнення; наукове консультування; самостійний пошук та критичний аналіз наукових джерел і літератури; формування висновків і рекомендацій.	перевірка роботи на відсутність ознак академічного плагіату та відповідність вимогам до оформлення; оцінювання змісту та актуальності роботи, рівня теоретичної і практичної підготовки здобувача, обґрунтованості висновків та рекомендацій, презентації результатів; захист кваліфікаційної роботи.
		Переддипломна практика	індивідуальні консультації з керівником практики; самостійна робота; аналіз та систематизація результатів досліджень і спостережень.	оцінювання змісту та оформлення звіту; захист результатів практики.
РН7. Обґрунтовувати використання, впроваджувати та аналізувати кращі світові стандарти, практики з метою розв'язання складних задач професійної діяльності в галузі інформаційної безпеки та/або кібербезпеки.	☒	Підготовка та захист кваліфікаційної роботи	аналіз, синтез, систематизація, узагальнення; наукове консультування; самостійний пошук та критичний аналіз наукових джерел і літератури; формування висновків і рекомендацій.	перевірка роботи на відсутність ознак академічного плагіату та відповідність вимогам до оформлення; оцінювання змісту та актуальності роботи, рівня теоретичної і практичної підготовки здобувача, обґрунтованості висновків та рекомендацій, презентації результатів; захист кваліфікаційної роботи.
		Переддипломна практика	індивідуальні консультації з керівником практики; самостійна робота; аналіз та систематизація результатів досліджень і спостережень.	оцінювання змісту та оформлення звіту; захист результатів практики.
		Дослідження і проектування систем захисту інформації	лекції, лабораторні роботи, тренінги, індивідуальні заняття, робота в групах, робота в Інтернет, самостійне навчання на основі підручників і конспектів.	поточне тестування та поточне опитування; підсумкове модульне тестування та опитування за кожним змістовим модулем; оцінювання виконання лабораторних робіт; оцінювання відповідей на питання тренінгу; оцінювання самостійної

				роботи; підсумковий екзамен.
		Моніторинг та управління інформаційною безпекою	лекції, лабораторні роботи, тренінги, індивідуальні заняття, робота в Інтернет, самостійне навчання на основі підручників і конспектів	поточне тестування та опитування; підсумкове тестування за кожним змістовим модулем; оцінювання виконання лабораторних робіт; оцінювання тренінгів; оцінювання результатів самостійної роботи; підсумковий екзамен.
РН8. Досліджувати, розробляти і супроводжувати системи та засоби інформаційної безпеки та/або кібербезпеки на об'єктах інформаційної діяльності та критичної інфраструктури.	☒	Підготовка та захист кваліфікаційної роботи	аналіз, синтез, систематизація, узагальнення; наукове консультування; самостійний пошук та критичний аналіз наукових джерел і літератури; формування висновків і рекомендацій.	перевірка роботи на відсутність ознак академічного плагіату та відповідність вимогам до оформлення; оцінювання змісту та актуальності роботи, рівня теоретичної і практичної підготовки здобувача, обґрунтованості висновків та рекомендацій, презентації результатів; захист кваліфікаційної роботи.
		Переддипломна практика	індивідуальні консультації з керівником практики; самостійна робота; аналіз та систематизація результатів досліджень і спостережень.	оцінювання змісту та оформлення звіту; захист результатів практики.
		Дослідження і проектування систем захисту інформації	лекції, лабораторні роботи, тренінги, індивідуальні заняття, робота в групах, робота в Інтернет, самостійне навчання на основі підручників і конспектів.	поточне тестування та поточне опитування; підсумкове модульне тестування та опитування за кожним змістовим модулем; оцінювання виконання лабораторних робіт; оцінювання відповідей на питання тренінгу; оцінювання самостійної роботи; підсумковий екзамен.
		Моніторинг та управління інформаційною безпекою	лекції, лабораторні роботи, тренінги, індивідуальні заняття, робота в Інтернет, самостійне навчання на основі підручників і конспектів	поточне тестування та опитування; підсумкове тестування за кожним змістовим модулем; оцінювання виконання лабораторних робіт; оцінювання тренінгів; оцінювання результатів самостійної роботи; підсумковий екзамен.
РН9. Аналізувати, розробляти і супроводжувати систему управління інформаційною безпекою та/або кібербезпекою організації на базі стратегії і політики інформаційної безпеки.	☒	Підготовка та захист кваліфікаційної роботи	аналіз, синтез, систематизація, узагальнення; наукове консультування; самостійний пошук та критичний аналіз наукових джерел і літератури; формування висновків і рекомендацій.	перевірка роботи на відсутність ознак академічного плагіату та відповідність вимогам до оформлення; оцінювання змісту та актуальності роботи, рівня теоретичної і практичної підготовки здобувача, обґрунтованості висновків та рекомендацій, презентації результатів; захист кваліфікаційної роботи.
		Моніторинг та управління інформаційною безпекою	лекції, лабораторні роботи, тренінги, індивідуальні заняття, робота в Інтернет, самостійне навчання на основі підручників і конспектів	поточне тестування та опитування; підсумкове тестування за кожним змістовим модулем; оцінювання виконання лабораторних робіт; оцінювання тренінгів; оцінювання результатів

				самостійної роботи; підсумковий екзамен.
		Переддипломна практика	індивідуальні консультації з керівником практики; самостійна робота; аналіз та систематизація результатів досліджень і спостережень.	оцінювання змісту та оформлення звіту; захист результатів практики.
РН5. Критично осмислювати проблеми інформаційної безпеки та/або кібербезпеки, у тому числі на міжгалузевому та міждисциплінарному рівні, зокрема на основі розуміння нових результатів інженерних і фізико-математичних наук, а також розвитку технологій створення та використання спеціалізованого програмного забезпечення.	☒	Підготовка та захист кваліфікаційної роботи	аналіз, синтез, систематизація, узагальнення; наукове консультування; самостійний пошук та критичний аналіз наукових джерел і літератури; формування висновків і рекомендацій.	перевірка роботи на відсутність ознак академічного плагіату та відповідність вимогам до оформлення; оцінювання змісту та актуальності роботи, рівня теоретичної і практичної підготовки здобувача, обґрунтованості висновків та рекомендацій, презентації результатів; захист кваліфікаційної роботи.
		Переддипломна практика	індивідуальні консультації з керівником практики; самостійна робота; аналіз та систематизація результатів досліджень і спостережень.	оцінювання змісту та оформлення звіту; захист результатів практики.
		Дослідження і проектування систем захисту інформації	лекції, лабораторні роботи, тренінги, індивідуальні заняття, робота в групах, робота в Інтернет, самостійне навчання на основі підручників і конспектів.	поточне тестування та поточне опитування; підсумкове модульне тестування та опитування за кожним змістовим модулем; оцінювання виконання лабораторних робіт; оцінювання відповідей на питання тренінгу; оцінювання самостійної роботи; підсумковий екзамен.
		Методологія наукових досліджень	лекції, практичні заняття, самостійне навчання на основі підручників і конспектів, тренінги, індивідуальні заняття, робота в Інтернет.	поточне опитування; поточне оцінювання; підсумковий модульний контроль за кожним змістовим модулем; оцінювання тренінгів; оцінювання результатів самостійної роботи; підсумковий екзамен.