НАЦІОНАЛЬНЕ АГЕНТСТВО ІЗ ЗАБЕЗПЕЧЕННЯ ЯКОСТІ ВИЩОЇ ОСВІТИ

ВІДОМОСТІ
про самооцінювання освітньої програми

Заклад вищої освіти	**Вінницький національний технічний університет**
Освітня програма	**59418 Безпека інформаційних і комунікаційних систем**
Рівень вищої освіти	**Магістр**
Спеціальність	**125 Кібербезпека та захист інформації**

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

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

Використані скорочення:

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

Загальні відомості

1. Інформація про ЗВО (ВСП ЗВО)

Реєстраційний номер ЗВО у ЄДЕБО	**137**
Повна назва ЗВО	**Вінницький національний технічний університет**
Ідентифікаційний код ЗВО	**02070693**
ПІБ керівника ЗВО	**Біліченко Віктор Вікторович**
Посилання на офіційний веб-сайт ЗВО	**www.vntu.edu.ua**

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

https://registry.edbo.gov.ua/university/137

3. Загальна інформація про ОП, яка подається на акредитацію

ID освітньої програми в ЄДЕБО	**59418**
Назва ОП	**Безпека інформаційних і комунікаційних систем**
Галузь знань	**12 Інформаційні технології**
Спеціальність	**125 Кібербезпека та захист інформації**
Спеціалізація (за наявності)	*відсутня*
Рівень вищої освіти	**Магістр**
Тип освітньої програми	**Освітньо-професійна**
Вступ на освітню програму здійснюється на основі ступеня (рівня)	**Бакалавр, Магістр (ОКР «спеціаліст»)**
Структурний підрозділ (кафедра або інший підрозділ), відповідальний за реалізацію ОП	**кафедра захисту інформації**
Інші навчальні структурні підрозділи (кафедра або інші підрозділи), залучені до реалізації ОП	**кафедра менеджменту та безпеки інформаційних систем, кафедра філософії та гуманітарних наук, кафедра іноземних мов**
Місце (адреса) провадження освітньої діяльності за ОП	**м. Вінниця, вул. Хмельницьке шосе, 95**
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	**192237**
ПІБ гаранта ОП	**Войтович Олеся Петрівна**
Посада гаранта ОП	**Доцент**
Корпоративна електронна адреса гаранта ОП	**voytovych.olesya@vntu.edu.ua**
Контактний телефон гаранта ОП	**+38(067)-728-81-61**
Додатковий телефон гаранта ОП	*відсутній*

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

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

26 січня 2023 року започатковано ОПП Безпека інформаційних і комунікаційних систем (далі - БІКС) за спеціальністю 125 Кібербезпека та захист інформації для продовження провадження освітньої діяльності за ОПП Безпека інформаційних і комунікаційних систем за спеціальністю 125 Кібербезпека, що вже функціонувала, без зміни по суті, що зумовлено Постановою Кабінету Міністрів України від 16 грудня 2022 року № 1392 «Про внесення змін до переліку галузей знань і спеціальностей, за якими здійснюється підготовка здобувачів вищої освіти». Загалом, підготовка здобувачів вищої освіти за напрямом інформаційна безпека ведеться на кафедрі захисту інформації (далі ЗІ), факультету інформаційних технологій та комп'ютерної інженерії (далі ІТКІ) Вінницького національного технічного університету (далі ВНТУ) з 2001 року. Кафедра ЗІ здійснювала підготовку спеціалістів (бакалаврів, магістрів) за спеціальністю 160105 «Захист інформації в комп'ютерних системах та мережах», потім 170101«Безпека інформаційний і комунікаційних систем». Із розвитком кіберпростору та змінами у галузі вищої освіти у 2016 році було запроваджено ОПП Безпека інформаційних і комунікаційних систем за спеціальністю 125 Кібербезпека за освітнім ступенем «магістр». Зміни до ОПП Безпека інформаційних і комунікаційних систем вносились у різних роках відповідно до потреб та пропозицій зацікавлених осіб. У 2021 році відповідно до Стандарту вищої освіти за спеціальністю 125 Кібербезпека для другого (магістерського) рівня вищої освіти (затверджено і введено в дію наказом Міністерства освіти і науки України від 18.03.2021 № 332) оновлено ОПП та внесено відповідні зміни.
Під час обговорення ОПП взимку 2023/2024 н.р. внесені зміни до компетентностей та програмних результатів навчання відповідно до пропозицій заінтересованих осіб (здобувачів, роботодавців, академічної спільноти та інших). Крім того, у зв'язку із прийняттям нової Стратегії розвитку ВНТУ на 2023-2027 роки (https://vntu.edu.ua/projects/development_strategy-2023.pdf) було внесено зміни до мети ОПП.

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

Рік навчання	Навчальний рік, у якому відбувся набір здобувачів відповідного року навчання	Обсяг набору на ОП у відповідному навчальному році	Контингент студентів на відповідному році навчання станом на 1 жовтня поточного навчального року	У тому числі іноземців
			ОД	*ОД*
1 курс	2023 - 2024	20	20	0
2 курс	2022 - 2023	26	22	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)	**59253 Кібербезпека інформаційних технологій та систем**
перший (бакалаврський) рівень	**59406 Безпека інформаційних і комунікаційних систем** **59407 Управління інформаційною безпекою** **59408 Кібербезпека інформаційних технологій та систем** **59409 Кібербезпека критичних систем**
другий (магістерський) рівень	**59418 Безпека інформаційних і комунікаційних систем** **59420 Кібербезпека інформаційних технологій та систем**
третій (освітньо-науковий/освітньо-творчий) рівень	**59431 Кібербезпека**

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

	Загальна площа	Навчальна площа
Усі приміщення ЗВО	121917	24172
Власні приміщення ЗВО (на праві власності, господарського відання або оперативного управління)	121917	24172

Приміщення, які використовуються на іншому праві, аніж право власності, господарського відання або оперативного управління (оренда, безоплатне користування тощо)	0	0
Приміщення, здані в оренду	5147	363

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	*125_m_biks_OPP_2023_z.pdf*	/EXVcqxiAYLX/xit5KFyUjsPGcg8ce9SAGJsMjQG3u4=
Навчальний план за ОП	*m_125_biks_2023_NP.pdf*	5TJMhhvISwaWM0RqgCBrLqLoNswP6Xoz8XXLDYoT2UQ=
Матеріали від ЗВО: пропозиції та рекомендації від роботодавців, таблиця відповідності публікацій наукових керівників напрямам (тематикам) досліджень аспірантів (для ОП третього рівня освіти)	*m_125_BIKS_WinInteractive_2023.pdf*	XUnEy+bU6lEsqrNJX7Y64koOfylBXCIghNSE/qkkRdA=
Матеріали від ЗВО: пропозиції та рекомендації від роботодавців, таблиця відповідності публікацій наукових керівників напрямам (тематикам) досліджень аспірантів (для ОП третього рівня освіти)	*m_125_BIKS_Rec_KASKAD_2023.PDF*	l2eFn59HBQWbu3EqYwrMmW50mPNoKlc7niwIHKBpiuY=
Матеріали від ЗВО: пропозиції та рекомендації від роботодавців, таблиця відповідності публікацій наукових керівників напрямам (тематикам) досліджень аспірантів (для ОП третього рівня освіти)	*m_125_BIKS_Rec_kIberpolice_2023.PDF*	3x93HtzgsOkJcZ9nsPoyqbol8Ey+BDry6Iz76hrOK+k=
Матеріали від ЗВО: пропозиції та рекомендації від роботодавців, таблиця відповідності публікацій наукових керівників напрямам (тематикам) досліджень аспірантів (для ОП третього рівня освіти)	*m_125_BIKS_Rec_TRUSTY_G_2023.pdf*	7eMDk9uov5SNgC9Q/KdHznfwLnP3gVExSQUHjTshvB4=
Матеріали від ЗВО: пропозиції та рекомендації від роботодавців, таблиця відповідності публікацій наукових керівників напрямам (тематикам) досліджень аспірантів (для ОП третього рівня освіти)	*m_125_biks_REC_Smirnov_2023.pdf*	83VXLgPC7EUiJINxhfQlNIVUYJW5Rt7m2UTSutRoZaA=

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?

Для спеціальності 125 Кібербезпека та захист інформації відсутній стандарт вищої освіти другого (магістерського) рівня вищої освіти, проте чинним залишається стандарт вищої освіти за спеціальністю 125 Кібербезпека, затверджений наказом МОНУ №332 від 18.03.2021 р.

(https://mon.gov.ua/storage/app/media/vyshcha/standarty/2021/03/19/125%20Kiberbezpeka_mahistr_18_03_21_332.docx). Стандарт містить РН01-РН23 для освітньо-професійних програм, які відображені в ОПП. Для їх досягнення в ОПП передбачено 11 обов'язкових освітніх компонентів. Матриця забезпечення програмних результатів навчання освітніми компонентами ОПП наведена у таблиці 1 Додатку Б ОПП. Зокрема, для досягнення РН8 в ОПП передбачено опанування таких освітніх компонентів: ОК5-ОК8, ОК10 та ОК11. Для досягнення РН12 в ОПП передбачено опанування таких освітніх компонентів: ОК6, ОК7 та ОК9. Для досягнення РН17 в ОПП передбачено опанування таких освітніх компонентів: ОК1, ОК2, ОК4, ОК10 та ОК11. Атестація здійснюється у формі публічного захисту магістерської кваліфікаційної роботи, що має на меті розв'язання складної задачі інформаційної безпеки та/або кібербезпеки і проведення досліджень та/або здійснення інновацій. Зміст ОПП сприяє досягненню ПРН шляхом вивчення її обов'язкових ОК з циклу загальної та професійної підготовки та підсилюються вибірковими компонентами.

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

Під час розробки та обговорення ОПП у 2023 р. було враховано (в тому числі за рекомендацією представників Відділу протидії кіберзлочинам НПУ) деякі вимоги професійних стандартів, а саме 2139.2 Аналітик з безпеки інформаційно-телекомунікаційних систем затверджений Наказом Адміністрації Держспецзв'язку 25.11.2022 №715 (https://register.nqa.gov.ua/uploads/0/435-profesijnij_standart_analitik_z_bezpeki_informacijno_telekomunikacijnih.pdf) та 2139.2 Адміністратор мереж і систем затверджений Наказом Адміністрації Держспецзв'язку 25.11.2022 №715 (https://register.nqa.gov.ua/uploads/0/434-profesijnij_standart_administrator_merez_i_sistem.pdf). Введено: КФ12 Здатність координувати діяльність із забезпечення безпеки інформаційно-комунікаційних систем та результати навчання РН25 Здатність контролювати процес встановлення, впровадження та налаштування компонентів системи щодо захисту інформації. РН26 Здатність надавати рекомендації щодо планів аварійного відновлення, непередбачених випадків та забезпечення безперервності операцій. Також наявні освітні компоненти ОК1 Філософія науки і техніки та ОК2 Інноваційні та психологічні аспекти сучасної освіти враховують вимоги професійного стандарту на групу професій Викладачі закладів вищої освіти затверджений Наказом МРЕТСГ України від 23.03.2021 №610 (https://mon.gov.ua/storage/app/sites/1/pto/standarty/2021/03/25/Standart%20na%20hrupu%20profesiy_Vykladachi%20zakladiv%20vyshchoyi%20osvity_25.03.pdf).

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

Під час розроблення ОПП БІКС у 2022-2023 н.р. було враховано інтереси та пропозиції здобувачів вищої освіти, що навчаються за спеціальністю 125 Кібербезпека (Кібербезпека та захист інформації) на другому (магістерському) рівні, також мали можливість надати свої пропозиції здобувачі третього (освітньо-наукового) рівня. Для врахування обґрунтованих пропозицій обговорювався проєкт ОПП, відбувалося регулярне спілкування гаранта ОПП та НПП зі здобувачами вищої освіти під час провадження освітнього процесу, проводилося спілкування щодо побажання здобувачів відносно наповненості магістерської програми освітніми компонентами. Наприклад, за пропозицією Генадія Л., до ОК8 Проектування систем кібербезпеки додано теми з формулювання вимог до систем захисту, оцінювання задач, CI/CD - процесів в контексті реалізації безпечної інтеграції та доставлення до користувача розроблюваної системи. За пропозицією випускника В. Селезньова до ОК5 Сучасні системи, технології та засоби інформаційної безпеки та кібербезпеки додано тему пов'язану з блокчейном (https://iq.vntu.edu.ua/edu_progs/v.php?id=1126).

- роботодавці

Під час формування та оновлення ОПП представники роботодавців брали участь у зовнішній експертизі ОП. Наприклад, під час формування фахових компетентностей та програмних результатів навчання ОПП у 2022-2023 н.р. було враховано пропозиції та зауваження представників Відділу протидії кіберзлочинам у Вінницькій області НПУ, ТОВ «КАСКАД БЕЗПЕКА», ТОВ Trustee Global, ТОВ «ВІНІНТЕРАКТИВ» та інших установ, які працюють у ІТ-сфері, зокрема в кібербезпеці. Зокрема знайшли своє відображення рекомендації від представників кіберполіції щодо врахування професійних стандартів з кібербезпеки та захисту інформації, як наслідок, додані компетентності та програмні результати навчання. Також враховані рекомендації роботодавців щодо посилення практичної складової, залучення професіоналів-практиків. Відбулось вдосконалення наповнення окремих ОК, поглиблення результатів навчання, пов'язаних з їх безпосередньою діяльністю, зокрема аудиту інформаційної безпеки (https://iq.vntu.edu.ua/edu_progs/v.php?id=1126).

- академічна спільнота

НПП кафедри захисту інформації є членами Вченої Ради ВНТУ, вченої ради факультету ІТКІ та активно беруть участь у обговоренні різних освітніх програм, зокрема, з кібербезпеки та захисту інформації. Так, у 2022-2023 н.р. тривало обговорення нової Стратегії розвитку ВНТУ на 2023-2027 роки, під час якого були внесені пропозиції щодо зміни мети та цілей підготовки здобувачів вищої освіти, що було враховано під час затвердження нової версії ОПП в 2023 році (https://iq.vntu.edu.ua/edu_progs/v.php?id=1127). Також за пропозицією доц. Ю. Баришева внесена К36, яка спрямована на посилення володіння англійською мовою здобувачами вищої освіти магістерського рівня (https://iq.vntu.edu.ua/edu_progs/v.php?id=1126). До обговорення були залучені і інші представники академічної спільноти, зокрема, Олексій Смірнов, д.т.н., проф. завідувач кафедри кібербезпеки та програмного забезпечення Центральноукраїнського національного технічного університету відзначив можливість набуття програмних результатів навчання передбачених ОПП.

- інші стейкхолдери

Під час розроблення змісту освітніх компонентів ОПП враховано інтереси та пропозиції інших стейкхолдерів через участь провідних викладачів випускової кафедри у наукових, науково-методичних та професійних об'єднаннях за спеціальністю. Так, зав. каф. ЗІ, проф. В. Лужецький є заступником голови комітету К3 «Інформаційні системи» Української федерація інформатики. Крім того, доц. Ю. Баришев є членом міжвідомчої робочої групи з координації наукового співтовариства під час проведення наукових досліджень і розробок у сфері кібербезпеки. НПП кафедри ЗІ є активними членами таких спільнот: Асоціація спеціалістів з кібербезпеки, Наукова асоціація кібербезпеки України, Міжнародна асоціація технологічного розвитку та інновацій, Федерація програмування. Також викладачі кафедри ЗІ, ВНТУ та інших ЗВО, здобувачі, випускники, представники ІТ-компаній беруть участь у регулярних засіданнях ІТ-клубу CyberSecPals (https://www.youtube.com/@cybersecpals), де обговорюються актуальні питання розвитку кібербезпеки та ІТ-напрямку в цілому.
Важливими стейкхолдерами є МОНУ та КМУ. У 2023 р. врахована Постанова КМУ № 1392 від 16 грудня 2022 року «Про внесення змін до переліку галузей знань і спеціальностей, за якими здійснюється підготовка здобувачів вищої освіти», а саме внесені зміни у назву спеціальності.

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

Мета ОПП відповідає місії та стратегії ВНТУ, що викладені у Стратегії розвитку Вінницького національного технічного університету на період 2023-2027 рр. (https://vntu.edu.ua/projects/development_strategy-2023.pdf). Відповідно до зазначеного документа місією ВНТУ є формування творчої особистості нового покоління, здатної успішно реалізовувати набуті сучасні професійні компетентності, інтелектуальний потенціал, навики практичного досвіду та інноваційної діяльності, а також соціально-патріотичні та морально-етичні цінності у глобальному суспільно-економічному просторі. Це свідчить, що розроблена ОПП в повній мірі відповідає місії та стратегії ВНТУ і спрямована на підготовку висококваліфікованих фахівців шляхом якісного надання освітніх послуг та з дотриманням сучасних стандартів вищої освіти у викладанні, науковій і професійній діяльності.

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

Для забезпечення актуальності ОПП гарантом та членами робочої групи відбувається постійний моніторинг тенденцій розвитку галузі кібербезпеки та захисту інформації і науки загалом. Наприклад, відповідно до аналізу прогнозу трендів кібербезпеки KPMG на 2022 рік (https://assets.kpmg.com/content/dam/kpmg/cn/pdf/en/2022/04/cyber-security-considerations-2022.pdf), який наголошує на важливості володіння дослідницькими навичками та творчим підходом для осіб, що обіймають керівні посади в галузі кібербезпеки, підтверджено коректність формулювання мети ОПП та важливість РН24 та РН26. Аналіз звітів про новини в галузі кібербезпеки від EC-Council (наприклад, звіт за грудень 2022 – https://www.eccouncil.org/cybersecurity-exchange/wp-content/uploads/2023/03/Cyber-brief-dec-2022.pdf) дозволяє враховувати появу нових тенденцій та вимог до навичок фахівців з кібербезпеки. Зокрема аналіз EC-Council ключових вимог до працівників профілю DevSecOps (https://www.youtube.com/watch?v=_FqTTiKmw1A) дозволив підтвердити актуальність РН25. Аналіз звітів CERT-EU (наприклад, https://cert.europa.eu/publications/threat-intelligence/cb22-12/) дозволяє робочій групі аналізувати ризики та визначати ландшафт кіберзагроз як в світових масштабах, так і зі специфікою європейського регіону.

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

На ринку праці існує потреба у досвідчених фахівцях із забезпечення інформаційної безпеки та кібербезпеки, що пов'язано зі стрімким розвитком та впровадження інформаційних технологій у всі галузі, в тому числі критичну інфраструктуру. Гарант та НПП постійно моніторять вимоги ринку праці (наприклад, https://jobs.dou.ua/vacancies/?category=Security), співпрацюють з роботодавцями. Крім того, вимоги до спеціалістів у сфері кібербезпеки обговорювалися на відкритих онлайн-засіданнях ІТ-клубу CyberSecPals (https://www.youtube.com/@cybersecpals) із представниками таких стейкхолдерів як 10Guard, IBM-Україна, Leviathan, Департамент кіберполіції тощо.
Під час формулювання мети ОПП та ПРН враховано галузевий та регіональний контекст Вінницької обл. Так, враховано завдання Стратегії збалансованого регіонального розвитку Вінн. обл. на період до 2027 р., де передбачається розвиток ІТ-інфраструктури регіону, мереж та е-сервісів, підтримка функціонування ІТ-структури Вінн. обл., для чого, в свою чергу, необхідним є створення інфраструктури захисту інформації (https://vinrada.gov.ua/upload/files/7sklikannya/42pozases/921(1).pdf, https://vinrada.gov.ua/upload/files/7sklikannya/42pozases/921(2).pdf). Кафедра ЗІ активно співпрацює та враховує пропозиції провідних компаній регіону: ТОВ Вінінтерактив, ТОВ Trustee Global та ін., а також регіональних державних структур та їх підрозділів (СБУ, ДССЗЗІ України, Кіберполіція тощо) та органів влади.

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

Під час формування мети та програмних результатів навчання ОПП розробники керувались Стандартом вищої освіти, пропозиціями стейкхолдерів, а також досвідом формування ОПП вітчизняними та іноземними ЗВО. Зокрема було враховано досвід таких ЗВО: Хмельницького національного університету (https://kb.khmnu.edu.ua/osvitni-programy/), Національного авіаційного університету (https://pk.nau.edu.ua/125-kiberbezpeka-2/), НУ Львівська політехніка (https://directory.lpnu.ua/majors), Харківського національного університету радіоелектроніки

(https://nure.ua/abituriyentam/spetsialnosti-ta-spetsializatsiyi/spetsialnist-125-kiberbezpeka-ta-zakhyst-informatsii/mahistr-125-kiberbezpeka-ta-zakhyst-informatsii) та інших. Зміст аналогічних освітніх програм неодноразово розглядався та аналізувався НПП кафедри ЗІ та робочою групою. Результати вивчення досвіду інших ОПП враховані шляхом покращення порядку вивчення ОК та їх наповнення, вдосконалення матриць відповідності між ОК та компетентностями і ПРН, які вони забезпечують.

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

Досвід іноземних ЗВО враховувався шляхом аналізу і запровадження в освітній процес сучасних підходів і практик навчання. Так, завдяки участі доц. Ю. Баришева в низці програм CRDF Global щодо покращення кібербезпеки в Україні, зокрема “Finalization of IT Audit Course and Integration into Curriculum” розроблено курс під керівництвом фахівців з Purdue University (м. Вест Лаффайєт, США). Проаналізовано аналогічні ОПП, які діють в Harvard Extension school Cybersecurity Master’s Degree Program (https://extension.harvard.edu/academics/programs/cybersecurity-graduate-program/#outcomes), EC-Council University (https://www.eccu.edu/academics/master-of-science-in-cyber-security/) та інші. В перших більше уваги приділяється практичним навичкам та професійним знанням, зокрема Software Applications: Security Lifecycle Threats, та Systems Programming and Machine Organization, що враховано в ОК8. В той час як, в інших академічних програмах багато уваги приділяється формуванню соціальних навичок, зокрема, лідерство, менеджмент, впровадження інновацій та ін., що відображено в ОК1, ОК2, ОК4. Майже всі розглянуті магістерські програми мають значний обсяг онлайн навчання і лише в деяких з них потребують проходження навчання в кампусах. Також враховані результати академічної мобільності викладачів кафедри ЗІ, зокрема, в Dresden University of Technology (Дрезден, Німеччина) та Barkhausen Institut (Дрезден, Німеччина) в контексті розширення тематики освітніх компонентів, в тому числі в ОК6 Кібербезпека та ОК7 Кібербезпека об’єктів критичної інфраструктури.

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)?

67

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

23

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

Теоретичний зміст предметної області: 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.
Вивчення обов’язкових освітніх компонентів та реалізація програмних результатів навчання повністю відповідає предметній області спеціальності. Зокрема, ОК5 Сучасні системи, технології та засоби інформаційної безпеки та кібербезпеки забезпечує такі об'єкти вивчення предметної області як "інформаційні системи (інформаційно-комунікаційні, інформаційно-телекомунікаційні, автоматизовані) та технології", "сучасні процеси дослідження, аналізу, створення та забезпечення функціонування інформаційних систем і технологій", її доповнює ОК7 Кібербезпека об’єктів критичної інфраструктури в контексті вимог до "об’єктах інформаційної діяльності та критичних інфраструктур". ОК7 також концентрується на об'єктах вивчення "інфраструктура об’єктів інформаційної діяльності та критичних інфраструктур" та "інформаційні ресурси різних класів (в т.ч. державні інформаційні ресурси)". ОК6 Кібербезпека та ОК8 Проектування систем кібербезпеки фокусуються на об'єктах вивчення "програмне та програмно-апаратне забезпечення (засоби) кіберзахисту", "технології, методи, моделі та засоби інформаційної безпеки та/або кібербезпеки", "системи та комплекси створення, обробки, передачі, зберігання, знищення, захисту та відображення даних (інформаційних потоків)" тощо. ОК9 Моніторинг та аудит кібербезпеки розкриває "системи управління інформаційною безпекою та/або кібербезпекою" та ін. Отже, ОП в повній мірі відповідає предметній області спеціальності 125 Кібербезпека (Кібербезпека та захист інформації). Обов’язкові освітні компоненти наведені в ОПП забезпечують формування загальних і фахових компетентностей фахівців та становлять логічну взаємопов’язану структуру.

Яким чином здобувачам вищої освіти забезпечена можливість формування індивідуальної освітньої

траєкторії?

Формування індивідуальної освітньої траєкторії забезпечується шляхом надання можливості вибирати: навчальні дисципліни обсягом – 23 кредити ЄКТС, що становить 25,5 % від загальної кількості кредитів передбачених ОПП та стандартом; керівника та тему магістерської кваліфікаційної роботи; а також програми внутрішньої та міжнародної академічної мобільності, результати навчання у неформальній та інформальній освіті.
Вибір дисциплін проводиться відповідно до Положення про вільний вибір навчальних дисциплін здобувачами вищої освіти ВНТУ (https://vntu.edu.ua/uploads/2024/P_vybir_2024_08_29.pdf). Для забезпечення здобувачам можливості вільно вибирати дисципліни в ОПП у ВНТУ використовується єдиний шаблон розподілу кредитів ЄКТС та аудиторних годин для дисциплін вільного вибору, що забезпечує здобувачу можливість формувати індивідуальну освітню траєкторію в рамках банку дисциплін вільного вибору затвердженого Вченою радою ВНТУ.
Здобувачі мають можливість отримати результати навчання в інших закладах вищої освіти України або країн світу користуючись академічною мобільністю, відповідно до Положення про академічну мобільність студентів, аспірантів, докторантів, наукових, науково-педагогічних, педагогічних та інших працівників (https://vntu.edu.ua/images/2018/mob.pdf).
Визначення академічної різниці та визнання результатів навчання для учасників програм академічної мобільності в іншому закладі вищої освіти регламентується Положенням про порядок перезарахування результатів навчання для учасників програм академічної мобільності ВНТУ.

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

Право на вільний вибір навчальних дисциплін регламентується Положенням про вільний вибір навчальних дисциплін здобувачами вищої освіти ВНТУ (https://vntu.edu.ua/uploads/2024/P_vybir_2024_08_29.pdf). Навчальним планом передбачено 4 навчальних дисципліни за вільним вибором здобувача. Перелік навчальних дисциплін, які входять до банку дисциплін вільного вибору, щорічно затверджується Вченою радою ВНТУ. Під час осіннього семестру, складається єдиний для магістрантів графік презентацій вибіркових навчальних дисциплін, доводиться до відома здобувачів та розміщується в розділі «Головна» на сайті факультету (https://fitki.vntu.edu.ua/archives/12589). Презентація вибіркових навчальних дисциплін може проводитись як дистанційно в онлайн-форматі, так і в аудиторіях. Інформація щодо кожної вибіркової дисципліни наведена у силабусі, ознайомитись з якими здобувачі можуть в інформаційній системі підтримки освітнього процесу JetIQ (https://iq.vntu.edu.ua/departs/index.php?id=246&mode=syllabus&spec_num=125°r=mag). Процедура вільного вибору дисциплін здобувачами проводиться з використанням системи підтримки навчання JetIQ. Для запобігання впливу на вибір здобувачами, вони можуть пройти опитування в зручний для себе час у відведений на це період. В результаті опитування автоматично формується та реєструється заява в електронному вигляді. На підставі поданих заяв навчальний відділ формує списки груп здобувачів за вибраними навчальними дисциплінами, які затверджуються на засіданні Ради з якості освіти ВНТУ. Вибрані здобувачем дисципліни включаються до його індивідуального плану і є обов'язковими для вивчення.

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

Для практичної підготовки здобувачів в ОПП та навчальному плані передбачена переддипломна практика (3 семестр, 15 кредитів ЄКТС). Переддипломна практика передбачає набуття практичних умінь, поглиблення та закріплення теоретичних знань для вирішення завдань в галузі кібербезпеки та захисту інформації, підбір матеріалів для магістерської кваліфікаційної роботи та посилює загальні компетентності КЗ1–КЗ4, і фахові компетентності КФ1–КФ9, КФ11.
Переддипломну практику можна проходити в організаціях та підприємствах. Основними базами для проходження практики є підприємства як державної, так і приватної форми власності незалежно від галузі, наприклад, Департамент кіберполіції, Вінницька міська рада, банки, медичні установи, ІТ-компанії та ін. (https://zi.vntu.edu.ua/partners.html). Здобувачам надається можливість долучитися до виконання науково-дослідних робіт, які виконуються на кафедрі ЗІ, вдосконалювати практичні навички у лабораторіях кафедри, відвідувати сектори кібербезпеки та ІТ-інфраструктури підприємств, семінари та інші заходи, спрямовані на підвищення практичної підготовки за спеціальністю, зокрема ІТ-клуб CyberSecPals (https://www.youtube.com/@cybersecpals), що функціонує як науково-практичний гурток кафедри ЗІ (https://zi.vntu.edu.ua/stud_itClub.html). Також здобувачі набувають практичних навичок в межах підготовки на практичних та лабораторних заняттях в лабораторіях кафедри, під час виконання курсової та магістерської кваліфікаційної роботи.

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

Соціальні навички (soft skills) розвиваються під час вивчення освітніх компонентів, в ході взаємодії під час виконання та презентації індивідуальних та групових завдань, виступах на конференціях та захисту робіт. Командні навички, лідерські якості та міжособистісна взаємодія розвиваються під час групового виконання завдань на практичних і лабораторних заняттях. Комунікаційні вміння та навички захисту власної позиції формуються при освоєнні загальних освітніх компонентів та закріплюються під час вивчення професійних компонентів. Навички презентації результатів роботи формуються через виступи на конференціях, захист курсової та випускової роботи. Критичне мислення розвивається при вивченні загальних та професійних освітніх компонентів і закріплюється під час написання магістерської кваліфікаційної роботи. Здобувачі мають можливість брати участь у наукових, навчальних, культурних та інших заходах, які регулярно організовуються у ВНТУ, більшість з яких є безкоштовними, зокрема курси з медіаграмотності, педагогічні майстер-класи, інтелектуальні та спортивні турніри. Зокрема, вивчення таких освітніх компонентів, як ОК1-ОК4 забезпечує набуття: КЗ1-КЗ6, КФ5, КФ10.

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

ОПП Безпека інформаційний і комунікаційних систем має чітку структуру і містить взаємопов'язану структурно-логічну схему освітніх компонентів, що спрощує розуміння зв'язків між ОК цієї ОПП для здобувачів та інших стейкхолдерів і загалом дозволяє досягти заявлених цілей та програмних результатів навчання. Програма складається з циклу обов'язкових освітніх компонентів - 67 кредитів ЄКТС (9 кредитів - загальні ОК та 58 кредитів - професійні ОК, серед яких переддипломна практика та атестації у формі захисту магістерської роботи), а також циклу вибіркових освітніх компонентів (23 кредити ЄКТС).
Загальні ОК, зокрема ОК1 Філософія науки і техніки, ОК2 Інноваційні та психологічні аспекти сучасної освіти, в тому числі, дозволяють опанувати загальні компетентності, що формують у здобувачів вміння аналізувати та приймати самостійні рішення на основі знань закономірностей суспільних процесів.
Для забезпечення програмних результатів навчання у ОПП передбачено 11 обов'язкових освітніх компонентів, які доповнюють одна одну та в сукупності дозволяють досягнути мети ОП.
Запропоновані вибіркові ОК (здобувач обирає чотири із загальної бази вибіркових дисциплін) не формують окремі програмні результати навчання, та в структурно-логічній схемі показані без зв'язків, оскільки передбачається вільний вибір навчальних дисциплін із загальної бази, проте запропоновані випусковою кафедрою на вибір навчальні дисципліни спрямовані на посилення програмних результатів навчання ОПП.

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 ВНТУ (https://vntu.edu.ua/uploads/2024/Pol_study_process.pdf), обсяг освітніх компонентів ОПП становить 90 кредитів ЄКТС. Відповідно до Положення про організацію самостійної роботи здобувачів вищої освіти у ВНТУ (https://vntu.edu.ua/uploads/n/np/4.pdf) передбачаються такі різновиди самостійної роботи: підготовка до аудиторних занять з відповідної дисципліни (лекційних, практичних та лабораторних робіт), виконання курсової роботи, ознайомлення з новітніми розробками у відповідних галузях та ін.
Для сприяння ефективній самостійній роботі здобувачів вищої освіти затверджено графіки консультацій, що надаються викладачами.
За даними соціологічних опитувань здобувачі задоволені фактичним навантаженням під час навчання (https://socio-lab.vntu.edu.ua/ukr/poll/): у групі БС-23м – 61 % здобувачів в цілому влаштовує обсяг матеріалу, який відведений на самостійне опрацювання дисциплін, також 61% здобувачів зазначили, що їм вистачає часу на опрацювання матеріалу самостійної роботи. Проте 39 % - не задоволені часом та обсягом матеріалів винесених на самостійний розгляд. Під час обговорення цієї проблеми зі здобувачами було з'ясовано, що основною причиною є працевлаштування здобувачів та відключення світла, що ускладнює їх можливість працювати (Протокол кафедри ЗІ №13 від 05.03.2024).

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

Для підвищення якості підготовки магістрів та покращення практикоорієнтованості ОП запроваджено традицію залучення до освітнього процесу кафедри ЗІ професіоналів-практиків та представників роботодавців (В. Гарнага, Roku Developer в EPAM, Л. Майданевич, юрист/адвокат в Раді адвокатів Він. обл., магістр з кібербезпеки). Організовуються виїзні екскурсії, наприклад, в Департаменті кіберполіції. На основі ІТ-клубу CyberSecPals (https://www.youtube.com/@cybersecpals), залучаються практики на вебінари, що дозволяють відобразити сучасний стан в кібербезпеці, основні виклики та потреби підприємств та організацій, вимоги ринку праці до випускників. Так, вебінари проводили представники Кіберполіції, Penetration tester в компанії Deloitte, Senior Python Developer, CEO ТОВ Каскад-Безпека, CEO Trustee Global, представники Gwara Media, Cybersecurity Specialist в компанії DigVel, міжнародний аудитор-консультант в галузі кібербезпеки та цифровізації, а також багато інших.
Переддипломна практика відбувається переважно на підприємствах ІТ-сектору, підприємствах критичної інфраструктури, органах міської влади та інше, де здобувачі можуть отримати досвід реальної роботи, побачити проблеми, з якими стикаються підприємства, в галузі кібербезпеки та захисту інформації, набути досвід їх вирішення, побачити перспективи подальшого кар'єрного зростання.
Крім того, здобувачі можуть поєднувати навчання з роботою за фахом, у формі індивідуального графіку.

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

ОПП БІКС забезпечує формування у здобувачів ключових навичок і компетентностей, які підтримують досягнення глобальних цілей сталого розвитку до 2030 року, проголошених резолюцією ООН та визначених Указом Президента України, оскільки усі закладені в ОПП компетентності відповідають предметній області ОПП, зокрема,

“...інформаційні системи (інформаційно-комунікаційні, інформаційно-телекомунікаційні, автоматизовані) та технології”. До особливостей ОПП входить підготовка професіоналів з питань кібербезпеки, що корелює з пп. “9.4 Сприяти прискореному розвитку високо- та середньовисокотехнологічних секторів переробної промисловості, які формуються на основі використання ланцюгів освіта-наука-виробництво та кластерного підходу за напрямами розвиток інноваційної екосистеми, розвиток інформаційно-телекомунікаційних технологій, застосування їх у АПК, енергетиці, транспорті та промисловості, ...”. Крім цього, ОПП включає ОК1, ОК2, що безпосередньо спрямовані на підвищення обізнаності студентів про глобальні проблеми, такі як зміни клімату, охорона здоров’я, гендерна рівність, якість освіти, економічне зростання та інновації. Ці ж ОК сприяють пп 1.4 “Забезпечення всеохоплюючої і справедливої якісної освіти та заохочення можливості навчання впродовж усього життя для всіх”. Виконання пп 1.5 “забезпечення гендерної рівності, ..” забезпечується шляхом дотримання Кодексу етики ВНТУ, який чітко визначає неприйнятність дискримінації осіб за будь-якими ознаками.

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

Інформація про правила прийому на навчання та вимоги до вступників ОП містяться за посиланнями:
https://vstup.vntu.edu.ua/
https://vstup.vntu.edu.ua/pravyla-pryiomu

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

Прийом до ВНТУ здійснюється на конкурсній основі в межах ліцензованого обсягу відповідно до джерел фінансування.
Вступити до ВНТУ на ОПП Безпека інформаційних і комунікаційних систем для здобуття ступеня магістра можуть особи, які мають ступінь бакалавра, магістра (освітньо-кваліфікаційний рівень спеціаліста).
Для конкурсного відбору на навчання для здобуття ступеня магістра враховуються бали:
- ЄВІ 2023 або 2024 років та єдиного державного кваліфікаційного іспиту (ЄДКІ) зі спеціальності 125 Кібербезпека та захист інформації 2024 року (тільки для вступників на спеціальність 125 Кібербезпека та захист інформації, які складали відповідний ЄДКІ 2024 року);
- ЄВІ 2023 або 2024 років та ЄФВВ 2024 року (крім вступників на спеціальність 125 Кібербезпека та захист інформації, які складали відповідний ЄДКІ 2024 року).
Відповідно до Правил прийому на 2024 рік для вступу за державним замовленням та за кошти фізичних та/або юридичних осіб потрібно надати мотиваційний лист для вступу, що повинен містити раціональне обґрунтування вибору вступником саме цієї ОПП, висвітлення його власного бачення майбутнього, а також огляд попередніх досягнень.
Оцінювання мотиваційних листів вступників у 2024 році проводилось відповідно до Порядку (https://vstup.vntu.edu.ua/images/2024/pravila_priomu/d8_mot_list.pdf).
Правила прийому на ОПП не містять дискримінаційних положень, а спрямовані на конкурсний відбір найкращих претендентів.

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?

У ВНТУ процедури визнання результатів навчання в інших ЗВО відбуваються відповідно Постанови КМУ від 12.08.15 № 579 Про затвердження Порядку реалізації права на академічну мобільність (зі змінами 2022), Положення про організацію освітнього процесу у ВНТУ (https://vntu.edu.ua/uploads/2024/Pol_study_process.pdf), Положення про академічну мобільність студентів, аспірантів, докторантів, наукових, науково-педагогічних, педагогічних та інших працівників (https://vntu.edu.ua/images/2018/mob.pdf) та правил прийому до ВНТУ (https://vstup.vntu.edu.ua/pravyla-pryiomu). Визнання результатів навчання здійснюється з використанням ЄКТС або з використанням системи оцінювання навчальних здобутків здобувачів, прийнятої у країні ЗВО-партнера. Перезарахування отриманих раніше кредитів здійснюється на підставі наданого здобувачем документа з переліком та результатами вивчення навчальних дисциплін, кількістю кредитів, завіреного в установленому порядку у ЗВО-партнера. Здобувачі вищої освіти отримують інформацію про можливість визнання результатів навчання з відповідних Положень, які наведені на сайті ВНТУ (https://vntu.edu.ua/uk/public-info/zag.html), а також під час зустрічей з адміністрацією ЗВО з приводу можливої участі у різноманітних програмах академічної мобільності. Роботу з безпосередньої організації навчання за програмами академічної мобільності проводять факультети за участю Центру міжнародних зв’язків та проєктів (https://int.vntu.edu.ua/uk/centr-uk/).

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

Випадків застосування для здобувачів вищої освіти на ОПП правил визнання результатів навчання, отриманих в інших ЗВО, ще не виникало.

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?

Визнання результатів навчання, отриманих у неформальній освіті, регулюється нормами Положення про порядок визнання результатів навчання, отриманих у неформальній освіті (https://vntu.edu.ua/uploads/2019/nefor.pdf), що регламентує види освітніх заходів неформальної освіти, вимоги до документів про участь у них тощо.
Процедура визнання та відповідного перезарахування результатів навчання, отриманих у неформальній освіті, здійснюється на добровільній основі та передбачає підтвердження того, що здобувач досяг результатів навчання, передбачених освітньою програмою, за якою він навчається.
Для визнання та перезарахування результатів неформальної освіти здобувач звертається із заявою та відповідними підтверджуючими документами до декана факультету, в якому навчається. Для розгляду поданої заяви створюється комісія, яка, як правило, складається із заступника декана з навчально-методичної роботи, завідувача випускової кафедри та/або гаранта освітньої програми, провідних науково-педагогічних працівників. Спільно вони визначають змістовну відповідність результатів неформального навчання та відповідних освітніх компонентів ОПП з метою визначення доцільності визнання результатів навчання та можливих обсягів перезарахування.

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

Практики застосування вказаних правил на ОПП Безпека інформаційний і комунікаційних систем для другого (магістерського) рівня вищої освіти наразі не було зафіксовано - здобувачі не надавали заяв щодо зарахування освітнього компоненту за результатами неформального навчання.

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?

Основні форми освітнього процесу та види навчальних занять наведено в Положенні про організацію освітнього процесу у ВНТУ (https://vntu.edu.ua/uploads/2024/Pol_study_process.pdf) та в тексті ОПП, що відповідає закону України про вищу освіту (ст.49 та 50). За ОПП БІКС передбачено лише інституційну (очну) форму здобуття освіти. Для досягнення результатів навчання на ОПП БІКС запропоновано: навчальні заняття, в тому числі онлайн, виконання лабораторних, практичних та індивідуальних завдань, курсові роботи, практики, контрольні заходи, самостійну роботу. Також застосовується комп'ютерне забезпечення занять, активні методи навчання (ситуаційні вправи, групова робота, дискусії), залучення здобувачів до наукового гуртка кафедри, участі у наукових семінарах, конференціях, олімпіадах, конкурсах, підготовка доповідей, свідоцтв на авторське право та наукових статей. Досягненню програмних результатів також сприяє проходження переддипломної практики, використання єдиної системи підтримки навчального процесу JetIQ (https://iq.vntu.edu.ua/). Система JetIQ є глобальним інформаційним базисом ВНТУ, за допомогою якого забезпечується управління навчальним процесом, облік результатів навчання та навчальної активності. Система JetIQ, в якій реалізовані функції дистанційного та змішаного навчання, надає можливість отримати інформацію про кожну дисципліну, викладача, робочу програму дисципліни, силабус, контрольні питання, систему оцінювання знань, навчальні матеріали тощо.

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?

Для забезпечення здобувачів всебічною інформацією про освітній процес використовується електронна система JetIQ (https://iq.vntu.edu.ua), е-пошта, чати Viber, веб-сайти кафедри та інших підрозділів ВНТУ, сторінки у Facebook та Instagram. На основі інтересів здобувачів освіти, які визначаються на вступних бесідах, будується студентоцентрований підхід у ВНТУ, з'ясовуються очікування та мотивація кожного здобувача вищої освіти. Викладачі ОПП надають максимальну увагу кожному здобувачеві, максимально залучають здобувачів до групової роботи на практичних та лабораторних заняттях, до обговорень на лекціях. Здобувачі освіти не обмежені в академічній свободі та мають можливість отримувати консультації від викладачів з будь-якого питання, яке їх цікавить. Студентоцентрованість проявляється через можливість вільного вибору навчальних дисциплін, тем курсової і кваліфікаційної робіт, місця проходження практики з урахуванням власних уподобань здобувачів. Студентоцентрованість виявляється і в отриманні зворотного зв'язку від здобувачів шляхом проведення бесід та опитувань (http://sociolab.vntu.edu.ua/ukr/poll/). Здобувачі ОПП мали змогу висловити свої пропозиції/зауваження щодо покращення освітнього процесу за ОПП. Зауваження і пропозиції здобувачів щодо освітньої програми розглядаються на засіданнях кафедри (https://iq.vntu.edu.ua/edu_progs/go2fileman.php?id=177&f_n=3).

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

Відповідно до Положення про організацію освітнього процесу у ВНТУ (https://vntu.edu.ua/uploads/2024/Pol_study_process.pdf) п. 6.1 «Освітній процес базується на принципах академічної свободи, науковості, гуманізму, демократизму, наступності та безперервності». Майданчиком для реалізації академічної свободи викладачів є методичні та наукові семінари кафедри, які формалізують,

удосконалюють та забезпечують впровадження ініціативи викладачів. Академічна свобода повністю забезпечується методами навчання і викладання на ОПП, оскільки передбачається їх максимальна варіативність, урахування свободи слова і творчості, поширення знань та інформації, проведення актуальних наукових досліджень в галузі інформаційних технологій та кібербезпеки. Освітні компоненти мають достатнє методологічне наповнення, здобувачі вищої освіти в процесі навчання мають можливість вибирати навчальні дисципліни, тему курсової роботи, керівника кваліфікаційної роботи; тематику та напрям кваліфікаційної роботи, що забезпечує індивідуальну траєкторію навчання. Здобувачі мають право оформляти індивідуальний графік навчання (https://vntu.edu.ua/uploads/2022/Ind_grafik.pdf), який передбачає можливість вільного відвідування лекцій і самостійного опрацювання теоретичного матеріалу і при цьому отримувати необхідну допомогу НПП. Також здобувачів кафедри ЗІ запрошують до студії регіональної радіостанції «Місто над Бугом» як гостей-експертів з питань кібербезпеки (https://www.youtube.com/watch?v=8tDqwIrXbjs; https://zi.vntu.edu.ua/stud_news.html).

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

Інформація про зміст, цілі та очікувані результати навчання, порядок та критерії оцінювання в межах окремих освітніх компонентів у вигляді силабусів міститься на сайті кафедри (https://iq.vntu.edu.ua/departs/index.php?id=246&mode=syllabus&spec_num=125°r=mag) та робочих програм (https://jetiq.vntu.edu.ua/departs/index.php?id=246&mode=progs&spec_num=125°r=mag). Інформація щодо окремих освітніх компонентів у постійному доступі надається в ресурсах загальноуніверситетської електронної системи управління освітнім процесом JetIQ в особистому кабінеті кожного учасника освітнього процесу за посиланням: https://iq.vntu.edu.ua/. Крім цього, викладачі на першому занятті з дисципліни обов'язково надають інформацію про порядок та критерії оцінювання, а також інформують здобувачів освітнього процесу про цілі, зміст та очікувані результати навчання з посиланням на сайт кафедри та ресурси системи JetIQ. Така форма інформування дає можливість здобувачам вищої освіти використовувати різні методи пошуку необхідної інформації з використанням комп'ютерів та смартфонів.

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

У ВНТУ створені належні умови для поєднання здобувачами вищої освіти навчальної та дослідницької діяльності. Науково-педагогічним працівникам та здобувачам надано безкоштовний доступ до міжнародних наукометричних БД Scopus та WoS. Здобувачі заохочуються до виконання творчих і наукових робіт: участі в олімпіадах, конкурсах, конференціях; за це здобувачу можуть нараховуватися додаткові бали з відповідного ОК. Результати досліджень оформляються у вигляді презентацій, друкованих наукових робіт, тез доповідей, свідоцтв на авторське право, патентів, статей у наукових фахових виданнях.
Здобувачі активно беруть участь у науково-дослідній роботі кафедри, щорічних науково-технічних конференціях викладачів, співробітників та студентів ВНТУ (https://conferences.vntu.edu.ua/index.php/allvntu/all-vntu-2023/), Всеукраїнській науково-практичній інтернет-конференції студентів, аспірантів та молодих науковців Молодь в науці: дослідження, проблеми, перспективи (https://conferences.vntu.edu.ua/index.php/mn/mn2023) та інших міжнародних та всеукраїнських конференціях. Елементи дослідницької роботи здобувачі опановують на ОК4, ОК10, ОК11 та інших. Здобувачі кафедри ЗІ є активними учасниками та переможцями численних творчих ІТ-конкурсів, хакатонів, змагань з кібербезпеки, конкурсів науково-дослідних робіт та олімпіад (https://zi.vntu.edu.ua/stud_olimp.html). Результати численних наукових досліджень представлено у тезах доповідей та матеріалах конференцій, в статтях періодичних видань, підтверджуються авторськими свідоцтвами та патентами (https://zi.vntu.edu.ua/stud_patent.html). Значна частина науково-дослідницької активності на кафедрі ЗІ відбувається в межах наукових гуртків (https://zi.vntu.edu.ua/Images/Nauka/Gurtki_24.pdf), результати якої представлено у студентських публікаціях (https://zi.vntu.edu.ua/stud_nauka.html).

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

Відповідно до Положення про порядок розробки і затвердження робочих програм та силабусів навчальних дисциплін у ВНТУ (https://vntu.edu.ua/uploads/2024/P_RNPD_sylab_2024_2024_08_29.pdf) РПНД складаються/оновлюються відповідно до чинної ОПП та щороку переглядаються. За необхідності (під час оновлення/удосконалення ОПП) в РПНД вносяться необхідні зміни. Підставами для оновлення РПНД є ініціатива викладача щодо врахування нових наукових досягнень та сучасних практик у відповідній області, зауваження або пропозиції здобувачів, які прослухали курс, поради роботодавців та інших стейкхолдерів, гаранта, декана, завідувача кафедри й колег.
Відповідно до напряму викладацької діяльності викладачі беруть участь у різного роду тренінгах, форумах, конференціях, опануванні різних програм та курсів, що дає змогу врахувати сучасні тенденції розвитку науки і техніки.
Так, проф. В. Лужецький постійно оновлює зміст ОК5 Сучасні системи, технології та засоби інформаційної та кібербезпеки на основі участі у міжнародних конференціях (є співорганізатором https://journal.comp-sc.if.ua/test/index.php/ITCM), має наукові публікації, керує аспірантами з напряму кібербезпеки тощо.
Доц. В. Лукічов у ОК6 Кібербезпека використовує свої напрацювання, в.т.ч., наукові: Метод адаптивного багатошарового захисту інформації на основі стеганографії та криптографії, Математична модель оцінки кіберзагроз та інформаційних впливів у мікроконтролерах та інші написані за результатами наукових досліджень, зокрема при співпраці з Barkhausen Institut.
Доц. Ю. Баришев у ОК7 Кібербезпека об'єктів критичної інфраструктури використовує власні наукові здобутки, в.т.ч., опубліковані фахових журналах та журналах з НМБД: Метод захищеного зберігання медичних даних на основі реляційної бази даних та блокчейну, Дискреційна модель та метод розмежування прав доступу до

розподілених інформаційних ресурсів, A Methodology For Optimal Obfuscation, Модель політики інформаційної безпеки для об'єктів критичної інфраструктури, Blockchain Tree as Solution for Distributed Storage of Personal ID Data and Document Access Control та інші.
Доц. Л. Куперштейн проводить дослідження у напрямку проєктування систем інформаційної безпеки та кібербезпеки, що знайшло відображення у ОК8 Проектування систем кібербезпеки, зокрема, через публікації: Remote Host Operation System Type Detection Based on Machine Learning Approach, DDoS-attack detection using artificial neural networks in Matlab та інші.
Доц. О. Войтович у ОК9 Моніторинг та аудит кібербезпеки враховує власні наукові публікації: Моделі інформаційної підтримки управління комплексною інформаційною безпекою, Модель політики інформаційної безпеки для об'єктів критичної інфраструктури та інші.
Викладачі також оновлюють зміст навчальних дисциплін на основі інших матеріалів власних монографій, статей, матеріалів конференцій інших розробок (комп'ютерних програм тощо) захищених свідоцтвом про реєстрацію авторського права (https://zi.vntu.edu.ua/staff.html).

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

ВНТУ сприяє участі працівників і здобувачів в міжнародних освітніх та наукових програмах, їх мовній підготовці, публікації наукових результатів в міжнародних виданнях. У ВНТУ забезпечено доступ до баз Scopus та WoS, інших ресурсів на сайті НТБ (http://lib.vntu.edu.ua). Викладачі кафедри ЗІ, у т.ч. за останні 5 років опублікували статті, що індексуються в МНБД Scopus (https://zi.vntu.edu.ua/staff.html).
Лукічов В. пройшов у Barkhausen Institut (Німеччина) міжнародне стажування за програмою Privacy of the 6G sensed data (2023,2024), а Баришев Ю. – міжнародне наукове стажування за темою Secure processors development for critical infrastructure (2024). Також Лукічов В., Баришев Ю. пройшли міжнародне наукове стажування в Technische Universitat Dresden (Німеччина) за програмою Unlinkability in Automated Driving Systems. Improving vehicle drivers` privacy (2022). У 2021 Баришев Ю. пройшов стажування в CRDF Global (США) на тему Розробка та інтеграція ІТ курсу з елементами кібербезпеки в навчальний план українських університетів. У 2021 Войтович О., Баришев Ю. пройшли стажування, організоване спільно London King`s College (UK), The Middlebury Institute of International Studies (США), CRDF Global (США) за темою Управління передачею конфіденційних технологій за межі науково-дослідних організацій та інші. Участь в міжнародному підвищенні кваліфікації (https://fitki.vntu.edu.ua/archives/10269, https://iq.vntu.edu.ua/departs/index.php?id=246&id_news=2028&mode=full_news).

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?

Відповідно до Положення про організацію освітнього процесу у ВНТУ (https://vntu.edu.ua/uploads/2024/Pol_study_process.pdf) формами контрольних заходів є вхідний, поточний, підсумковий контроль. Вхідний контроль може проводитись перед вивченням нового освітнього компоненту з метою визначення рівня підготовки здобувачів вищої освіти. Під час проведення поточного контролю у здобувачів освіти за ОПП викладачі використовують технології змішаного навчання за допомогою системи JetIQ (https://iq.vntu.edu.ua/). Поточний контроль дозволяє викладачеві повною мірою відслідковувати прогрес у досягненні результатів навчання у кожного із здобувачів освіти.
Підсумковий контроль здійснюється з метою оцінювання рівня знань, умінь та навичок, сформованих компетентностей та програмних результатів навчання здобувачів вищої освіти за певний етап навчання і складається з модульного, семестрового та атестації здобувачів вищої освіти.
Зазначені форми контрольних заходів у межах освітніх компонентів ОПП Безпека інформаційних і комунікаційних систем є чіткими, зрозумілими, оприлюднюються заздалегідь та надають можливість встановити досягнення здобувачем програмних результатів навчання. Адже на етапі укладання робочих програм навчальних дисциплін зміст контрольних заходів узгоджується з результатам навчання.

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

Всі види форм контрольних заходів визначено у Положенні про організацію освітнього процесу (https://vntu.edu.ua/uploads/2024/Pol_study_process.pdf). Вони відображені у робочих програмах навчальних дисциплін, силабусах та на сторінках дисциплін у системі JetIQ. Чіткість і зрозумілість контрольних заходів забезпечується: доступністю силабусів та робочих навчальних програм дисциплін на сайті випускової кафедри ЗІ та у системі JetIQ, інформуванням про них викладачем на початку вивчення кожного освітнього компонента. Перелік питань, які виносяться на залік, диференційований залік або іспит, доводиться до відома здобувачів (розміщується у системі JetIQ). Критерії оцінювання знань, умінь та навичок визначаються викладачем, відповідальним за освітній компонент, вносяться до робочої програми навчальної дисципліни / силабусу і доводяться до відома здобувачів викладачем, який проводить лекційні заняття, або викладачем, який проводить практичні або лабораторні заняття.

Яким чином і у які строки інформація про форми контрольних заходів та критерії оцінювання

доводяться до здобувачів вищої освіти?

Інформація про форми контрольних заходів та критерії оцінювання оновлюється щорічно на початку навчального року та надається здобувачам вищої освіти на першому занятті викладачами, які забезпечують відповідний освітній компонент. Форми контрольних заходів та критерії оцінювання відображаються у робочих програмах навчальних дисциплін, а також доступні у силабусах на сайті кафедри (https://iq.vntu.edu.ua/departs/index.php?id=246&mode=syllabus&spec_num=125°r=mag) і у вільному доступі через JetIQ. В робочих програмах навчальних дисциплін (https://jetiq.vntu.edu.ua/departs/index.php?id=246&mode=progs&spec_num=125°r=mag) та силабусах, крім загальних критеріїв оцінювання знань, обов'язково присутні критерії оцінювання кожного виду робіт, передбачених програмою (лабораторні роботи, практичні роботи, колоквіуми тощо).

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

Атестація здобувачів вищої освіти другого (магістерського) рівня, які навчаються за ОПП Безпека інформаційних і комунікаційних систем за спеціальністю 125 Кібербезпека та захист інформації, відбувається у формі публічного захисту магістерської кваліфікаційної роботи, що передбачено стандартом вищої освіти спеціальності 125 Кібербезпека для другого (магістерського) рівня.
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 на офіційному сайті ВНТУ. Оприлюднення кваліфікаційних робіт з обмеженим доступом здійснюється відповідно до вимог законодавства. Захищені кваліфікаційні роботи розміщені на офіційному сайту ВНТУ у системі JetIQ (https://iq.vntu.edu.ua/departs/index.php?id=246&mode=dpl_wrks&publyear=2023&bc_id=340).

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

Процедура проведення контрольних заходів у ВНТУ регулюється низкою інституційних документів, зокрема, Положення про організацію освітнього процесу у ВНТУ (https://vntu.edu.ua/uploads/2024/Pol_study_process.pdf), Положення про рейтингову систему оцінювання навчальних досягнень здобувачів вищої освіти у ВНТУ (https://vntu.edu.ua/uploads/n/np/6.pdf), Порядок організації та проведення заліків, диференційованих заліків, екзаменів у ВНТУ (https://vntu.edu.ua/uploads/n/np/7.pdf), Положення про порядок ліквідації академічної заборгованості, академічної різниці та надання платної послуги з проведення занять з вивчення окремої навчальної дисципліни понад обсяги, встановлені навчальним планом (https://vntu.edu.ua/uploads/2020/academ.PDF). Документи знаходяться у вільному доступі на сайті ВНТУ. До всіх документів здобувачі і викладачі ВНТУ мають доступ через електронну систему JetIQ.

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

У Кодексі етики ВНТУ (https://vntu.edu.ua/uploads/2019/etika.pdf) встановлено моральні принципи та правила етичної поведінки працівників університету, які забезпечують об'єктивність екзаменаторів під час оцінювання знань здобувачів вищої освіти. Процедури врегулювання конфлікту інтересів регламентуються Антикорупційною програмою ВНТУ (https://vntu.edu.ua/images/2017/antikor.pdf). Основними процедурами врегулювання конфлікту інтересів є відсторонення від участі у прийнятті рішення, усунення особи від виконання завдання, вчинення дій, прийняття рішення або участі в його прийнятті, застосування зовнішнього контролю за виконанням завдання чи прийняттям рішень, перегляд обсягу службових повноважень, переведення на іншу посаду. Питання пов'язані з конфліктом інтересів вирішуються відповідно до https://vntu.edu.ua/uk/topic/zapobigannya-korupcii-996.html. Крім цього, згідно Порядку організації і проведення заліків, диференційованих заліків, екзаменів у ВНТУ під час заліково-екзаменаційної сесії викладачі зобов'язані приймати у здобувачів заліки, диференційовані заліки та екзамени лише в терміни, визначені розкладом сесії в присутності асистента, призначеного завідувачем кафедри. За час здійснення освітньої діяльності на ОПП конфліктних ситуацій щодо об'єктивності екзаменаторів та оцінювання результатів навчання не виникало.

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

Відповідно до Положення про організацію освітнього процесу (https://vntu.edu.ua/uploads/2024/Pol_study_process.pdf), якщо в результаті складання заліково-екзаменаційної сесії здобувач освіти отримав з дисципліни оцінку FX за шкалою ЄКТС, то підсумковий контроль з цієї дисципліни він має право складати повторно, протягом двох тижнів після завершення заліково-екзаменаційної сесії. Якщо до початку заліково-екзаменаційної сесії здобувач отримав оцінку F за шкалою ЄКТС, то він має право на повторне вивчення дисципліни та складання контрольного заходу з неї за окремою угодою в терміни, визначені відповідно до Положення про порядок ліквідації академічної заборгованості, академічної різниці та надання платної послуги з проведення занять з вивчення навчальної дисципліни понад обсяги, встановлені навчальним планом (https://vntu.edu.ua/uploads/2020/academ.PDF). Визначений термін повторного вивчення дисципліни повинен бути завершений не пізніше, ніж за 2 тижні до початку наступної заліково-екзаменаційної сесії (крім останнього семестру випускного курсу); до здачі підсумкового контролю з переддипломної практики (в останньому семестрі випускного

курсу).

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

Оскарження процедури та результатів проведення контрольних заходів регулюється Порядком організації і проведення заліків, диференційованих заліків, екзаменів у ВНТУ (https://vntu.edu.ua/uploads/n/np/7.pdf). У випадку незгоди здобувача з результатами контрольного заходу він може звернутися з письмовою апеляцією до завідувача кафедри, який разом із лектором з дисципліни чи іншим викладачем, призначеним завідувачем кафедри, зобов'язані розглянути апеляцію в присутності здобувача протягом двох робочих днів і прийняти остаточне рішення щодо оцінювання екзаменаційної роботи. У випадках конфліктної ситуації, за мотивованою заявою здобувача чи викладача, деканом створюється комісія для приймання іспиту/заліку. Відповідно до Положення про освітнього омбудсмена з прав студентів (https://vntu.edu.ua/uploads/2020/1054.pdf) кожен здобувач вищої освіти ВНТУ, його батьки, законні представники, мають безперешкодне право безпосереднього звернення до омбудсмена (письмово або усно) і отримання аргументованої відповіді на своє звернення стосовно проведення контрольних заходів. За період навчання за ОПП Безпека інформаційний і комунікаційних систем оскарження процедури та результатів проведення контрольних заходів не було.

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

Політика, стандарти і процедури дотримання академічної доброчесності викладені у документах ЗВО: Кодекс етики ВНТУ (https://vntu.edu.ua/uploads/2019/etika.pdf), Положення про академічну доброчесність у ВНТУ (https://vntu.edu.ua/uploads/2022/acad.pdf), Положення про запобігання академічному плагіату та порядок його виявлення у наукових, кваліфікаційних, навчальних та науково-методичних роботах у ВНТУ (https://vntu.edu.ua/uploads/2024/Stateofplag.pdf), Антикорупційна програма ВНТУ (https://vntu.edu.ua/images/2017/antikor.pdf), Положення про уповноважену особу з питань запобігання та виявлення корупції (https://vntu.edu.ua/images/2018/0.pdf), Положення про Комісію з оцінки корупційних ризиків та моніторингу виконання антикорупційної програми у ВНТУ (https://vntu.edu.ua/images/2017/riz.pdf), Положення про комісію з питань оцінки вартості, вирішення питання щодо можливості використання, місця та строку зберігання подарунка, одержаного працівниками та ректором ВНТУ (https://vntu.edu.ua/uploads/2021/n184.pdf). У 2020-2022 рр. ВНТУ брав участь у проекті Ініціатива академічної доброчесності та якості освіти (проєкт Academic IQ), ініційованого Американською Радою з міжнародної освіти у співпраці із МОН України, Національним агентством із забезпечення якості вищої освіти та за підтримки Посольства США.

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

Виявлення ознак академічного плагіату у навчальних та кваліфікаційних роботах здобувачів є однією із складових академічної доброчесності, для якої можна скористатись технічними засобами. Відповідно до Положення про запобігання академічному плагіату та порядок його виявлення у наукових, кваліфікаційних, навчальних та науково-методичних роботах у ВНТУ (https://vntu.edu.ua/uploads/2024/Stateofplag.pdf) для перевірки на плагіат з 2024 року використовується платформа Turnitin, про що укладено відповідний договір.
Технічним адміністратором та координатором використання систем перевірки на плагіат створюються облікові записи операторів системи (призначених осіб, зазвичай на випускових кафедрах, що здійснюють перевірку робіт на відповідній ОП) та розподіляються права на перевірку робіт. Технологічна складова перевірки навчальних і кваліфікаційних робіт на наявність текстових запозичень визначена відповідною інструкцією. Банк кваліфікаційних робіт формується в університетському репозиторії (https://iq.vntu.edu.ua/departs/index.php?id=246&mode=dpl_wrks&publyear=2023&bc_id=340).
Інші прояви академічної недоброчесності (списування, фальсифікація результатів, використання чужої роботи, штучного інтелекту тощо) контролюються викладачами, які повідомляють здобувачам про їх недопустимість під час озвучення вимог до навчальних робіт. Для мінімізації ризиків академічної недоброчесності використовуються такі прийоми: варіативність завдань, обмеження часу на виконання контрольних завдань та одночасне проходження тестування усіма здобувачами.

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

Для популяризації академічної доброчесності в рамках роботи Центру забезпечення якості освіти ВНТУ сформовано постійно діючу комісію та робочу групу з академічної доброчесності (https://eqa.vntu.edu.ua/?id=340&mode=new_item&f=682/web/akaddobro.html). Фейсбук-сторінка Академічна доброчесність ВНТУ (https://www.facebook.com/a.integrityVNTU/) повідомляє про події, що пов'язані з формуванням культури академічної доброчесності, містить інформаційні матеріали, присвячені даній проблематиці. Інформаційно-консультативний супровід здобувачів освіти щодо питань академічної доброчесності складається з тренінгових занять щодо цінностей академічної доброчесності. Інструментами залучення науково-педагогічних працівників до формування культури академічної доброчесності є: Програма підвищення кваліфікації Розвиток професійно-педагогічної компетентності викладачів ВНТУ, яка включає теми «Академічна доброчесність як інструмент підвищення якості освіти» та опанування технологіями студентоцентрованого викладання; щорічне проведення Академічних асамблей (https://vntu.edu.ua/uk/news/akademichna-asambleya-vntu-2023-vidbulasya-2046.html, https://vntu.edu.ua/uk/news/v-akademichna-asambleya-vntu-vidbulasya-2803.html) як майданчиків для обговорення механізмів формування середовища нульової терпимості до порушень академічної доброчесності.
Крім того, питання академічної доброчесності розглядається також під час публікації тез та наукових статей

здобувачами вищої освіти.

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

Відповідно до Положення про академічну доброчесність у ВНТУ (https://vntu.edu.ua/uploads/2022/acad.pdf) учасники освітньо-наукового процесу несуть адміністративну та дисциплінарну відповідальність за недоброчесну поведінку. З метою виконання норм цього Положення в університеті створено Комісію з питань академічної доброчесності. Будь-який учасник освітньо-наукового процесу, якому стали відомі обґрунтовані факти порушення академічної доброчесності чи наміри про можливість такого порушення, повинен звернутися до Комісії з письмовою заявою. За результатами проведених засідань Комісія готує вмотивовані рішення у вигляді висновків щодо порушення чи не порушення академічної доброчесності, які подаються ректору/ проректору для вибору відповідних заходів морального, дисциплінарного чи адміністративного характеру.
Наслідками за порушення академічної доброчесності здобувачами освіти можуть бути: повторне проходження оцінювання, повторне проходження освітнього компоненту, відрахування із закладу освіти, позбавлення академічної стипендії. Порушення академічної доброчесності працівниками університету можуть мати наслідки: відмова у присудженні (позбавлення) наукового ступеня чи вченого звання, позбавлення права брати участь у роботі визначених законом органів чи займати визначені законом посади. Випадків порушення академічної доброчесності здобувачами ОПП Безпека інформаційних і комунікаційних систем другого (магістерського) рівня вищої освіти не було виявлено.

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

Академічна та професійна кваліфікація НПП, задіяного до реалізації ОПП, забезпечує досягнення цілей та програмних результатів навчання та відповідає чинним Ліцензійним вимогам щодо кадрового забезпечення провадження освітньої діяльності у сфері вищої освіти (Таблиця 2).
Так, доц. В. Лукічов, який викладає ОК6 Кібербезпека, є к.т.н. із спеціальності 05.13.21, має стажування у Barkhausen Institut gGmbH (Німеччина), де працював над проектами, пов'язаними із захистом даних, зокрема в контексті 6G-технологій; брав участь у міжнародних семінарах, наприклад в Технічному університеті Дрездена, де досліджував питання приватності в автоматизованих системах водіння, що є актуальним для ОК6, оскільки охоплюють захист інформації в сучасному кіберпросторі. Має публікації на тему кібербезпеки (https://www.scopus.com/authid/detail.uri?authorId=26323690700). Крім того, пройшов курс Тестування безпеки веб-застосунків, що є важливим аспектом для практичного викладання кібербезпеки.
Доц. Л. Куперштейн спроможний забезпечити ОК8 Проєктування систем кібербезпеки, оскільки має низку розробок, наприклад Система веб-пасток для зловмисників, Засіб для визначення типу операційної системи, що ілюструють практичний досвід у створенні інструментів для кібербезпеки. Має низку публікацій (https://www.scopus.com/authid/detail.uri?authorId=55645302100, http://kupershtein.vk.vntu.edu.ua/pub) пов'язаних з розробкою різних систем кіберзахисту. Активно підвищує кваліфікацію на теми пов'язані з системами кібербезпеки (https://zi.vntu.edu.ua/kvalifik.html). Під керівництвом Л. Куперштейна здобувачі здобули призові місця у різноманітних конкурсах та хакатонах з кібербезпеки (https://zi.vntu.edu.ua/stud_olimp.html).
Доц. О. Войтович, яка викладає ОК9 Моніторинг та аудит кібербезпеки, має низку публікацій з кібербезпеки, в тому числі з систем моніторингу та аудиту, (https://www.scopus.com/authid/detail.uri?authorId=57191865911, http://voytovych.vk.vntu.edu.ua/pub). Проходила підвищення кваліфікації з кібербезпеки, та, зокрема аудиту - Cybersecurity East Project, funded by the EU та інші (http://voytovych.vk.vntu.edu.ua/), також стажування у ТОВ Каскад-безпека з аудиту інформаційної безпеки. Має досвід практичної роботи як Директор центру забезпечення якості освіти ВНТУ, є експертом НА за спеціальністю 125 Кібербезпека.
Доц. Ю. Баришев, який викладає ОК7 Кібербезпека об'єктів критичної інфраструктури, проходив низку міжнародних наукових стажувань за напрямом цієї дисципліни в іноземних університетах (США, Німеччина, Сполучене Королівство) та міжнародних компаніях (Google, EPAM Systems), що дозволило йому опанувати сучасні виклики, які стоять перед об'єктами критичної інфраструктури, методи та засоби, які використовуються для відповіді на ці виклики. Крім того, фокус його наукових досліджень безпосередньо пов'язаний з напрямом ОК7 (https://www.scopus.com/authid/detail.uri?authorId=56008056000 http://baryshev.vk.vntu.edu.ua/pub).

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

Для осіб, які претендують на зайняття вакантних посад науково-педагогічних працівників, у ВНТУ запроваджена процедура обрання за конкурсом відповідно до Положення про проведення конкурсного відбору на заміщення вакантних посад науково-педагогічних працівників у ВНТУ (https://vntu.edu.ua/uploads/2024/Porydok_konkurs_2024.pdf), Статуту Вінницького національного технічного університету (https://vntu.edu.ua/images/docs/vntustatut.pdf). Серед документів, які претендент подає на розгляд конкурсної комісії, є, зокрема, такі: список наукових праць; рецензія на відкриту лекцію (за рішенням кафедри); звіт за попередній термін роботи; підвищення кваліфікації, показники професійної активності та ін. Під час добору

відбувається голосування за претендентів на засіданні кафедри та вченій раді факультету (або Вченій раді ВНТУ для посад професора та завідувача кафедри), під час яких обирається кращий претендент. Важливим критерієм для підбору кадрів для викладання професійних дисциплін за ОПП є їх академічна та професійна відповідність спеціальності 125 Кібербезпека та захист інформації та/або дисципліні, що викладається, відповідність п. 37 і п. 38 Ліцензійних умов провадження освітньої діяльності.

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

Залучення роботодавців до організації та реалізації освітнього процесу на ОПП відбувається протягом реалізації всього освітнього процесу. Найбільш широко роботодавці залучаються під час проходження переддипломної практики на різних підприємствах з ІТ-галузі, об'єктах критичної інфраструктури, Кіберполіції тощо, де здобувачі набувають досвід професійної підготовки. Кваліфікаційні роботи також можуть виконуватися за тематикою, яка визначена роботодавцем.
Кафедра ЗІ в рамках ОПП БІКС співпрацює з такими роботодавцями як Департамент кіберполіції, Вінницька міська рада, 10Guards, Liviathan Security Groups, EPAM Systems та ін. На підприємствах проводяться екскурсії для здобувачів з метою ознайомлення з особливостями їх функціонування та забезпечення інформаційної безпеки. Роботодавці запрошуються як голови ЕК (у 2024 - з Кіберполіції).
Роботодавці залучаються до обговорення і подальшого періодичного оновлення ОПП, перспектив підготовки фахівців, внесення пропозицій щодо ОК, курсових, лабораторних, практичних робіт. Також в межах ІТ-клубу CyberSecPals відбуваються онлайн зустрічі із представниками роботодавців (Департамент кіберполіції, 10Guards, Liviathan Security Groups, EPAM Systems та ін.). Зі свого боку, кафедра проводить моніторинг тенденцій ринку праці, вимог і потреб роботодавців, можливості професійної підготовки та підвищення кваліфікації.
Кафедра ЗІ активно залучає до викладання професіоналів-практиків, експертів галузі, представників роботодавців (В. Селезньов, Л. Майданевич, В. Гарнага, Г. Шелепало).

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

Процедури, за якими ВНТУ стимулює розвиток викладацької майстерності, включають матеріальне і професійне заохочення. ВНТУ забезпечує підвищення кваліфікації НПП відповідно до Положення https://vntu.edu.ua/uploads/2020/polmiz.pdf, а також забезпечення показників професійної активності. Показники НПП відображені в модулі JetIQ.
Функціонує щорічний семінар підвищення кваліфікації викладачів за різною тематикою (https://eqa.vntu.edu.ua/?id=340&mode=new_item&f=682/web/seminar.html).
ВНТУ забезпечує проведення наукових конференцій (https://conferences.vntu.edu.ua/index.php). Результати досліджень можна безкоштовно опублікувати у власних фахових журналах (https://journals.vntu.edu.ua).
Доц. Ю. Баришев брав участь у міжнародному проєкті CRDF Global на тему «Розробка навчальних дисциплін з напряму кібербезпеки» в Purdue University, США у 2019 р., а у 2021 році він вже був залучений до аналогічного проєкту CRDF Global як ментор. В. Лужецький брав участь у проєкті з покращення обізнаності щодо кібергігієни здобувачами ВНТУ, який організував CRDF Global у 2020 р. Ю. Баришев та В. Лукічов пройшли міжнародне наукове стажування в Technische Universitat Dresden, Німеччина у 2022, 2023 та в Barkhausen Institute, Німеччина у 2024 р., де розглядали питання організації кібербезпеки на прикладі різних критичних систем. Гарант О. Войтович взяла участь у проєкті Cybersecurity East Project, Cybersecurity Training Marathon тощо.

Наведіть конкретні приклади заохочення розвитку викладацької майстерності

Процедури, за якими ВНТУ стимулює розвиток викладацької майстерності, включають матеріальне (https://vntu.edu.ua/uploads/2023/stymul_publik_aktiv_2023.pdf, https://vntu.edu.ua/uploads/2024/P_premiuvan.pdf, https://vntu.edu.ua/uploads/2024/P_nadbavk.pdf) і професійне заохочення, які провадяться через:
– конкурс пед. майстерності, конкурс на кращу навчальну літературу (https://eqa.vntu.edu.ua/?id=340&mode=new_item&f=682/web/konkurs.html), переможці якого отримують грамоти;
– щорічно нагороджуються кращі НПП: до Дня університету, Дня науки та інших свят вручаються премії, грамоти ВНТУ, міської та обласної рад, МОН України;
– викладачі ВНТУ можуть безкоштовно проходити постійнодіючі курси з підвищення кваліфікації (https://eqa.vntu.edu.ua/?id=340&mode=new_item&f=682/web/seminar.html).
– запроваджено систему фінансового преміювання співробітників за подані патенти, авторські свідоцтва, публікації у періодичних виданнях Scopus та WoS.
Так, у 2023 р., за викладацьку майстерність гарант О. Войтович отримала Почесну грамоту МОН України, а проф. В. Лужецького відзначено нагрудним знаком МОНУ «Відмінник освіти 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

Фінансові ресурси ОПП забезпечуються відповідно до фінансових звітів ВНТУ (https://vntu.edu.ua/uk/public-info), які передбачають фінансування за рахунок коштів держбюджету на умовах держзамовлення на оплату послуг з підготовки фахівців, науково-педагогічних і наукових кадрів та за рахунок інших джерел, не заборонених законодавством. У навчальному процесі використовується бібліотечний фонд Науково-технічної бібліотеки ВНТУ (http://lib.vntu.edu.ua), можна отримати вільний доступ до баз даних періодичних наукових видань, НМБ Scopus та WoS. У ВНТУ є електронний репозитарій, який забезпечує доступ до наукових та навчально-методичних робіт НПП ВНТУ (https://ir.lib.vntu.edu.ua/). Функціонує система підтримки навчального процесу JetIQ, яка забезпечує управління навчальним процесом; облік знань здобувачів; тестування знань; розміщення навчально-методичних матеріалів (https://jetiq.vntu.edu.ua/method/sem2.php?spec=4824&f_code=210). Матеріально-технічні ресурси ВНТУ (https://www.youtube.com/@VNTU), факультету ІТКІ (https://youtu.be/WqxHrd0B_vs) та випускової кафедри ЗІ (https://zi.vntu.edu.ua/mater.html) включають спеціалізовані лабораторії: захисту програмного забезпечення, технічних засобів захисту інформації, безпеки комп'ютерних систем і мереж, в яких використовується спеціалізоване програмне та апаратне забезпечення. Аудиторії кафедри ЗІ обладнані мультимедійними проекторами. Наявні гуртожитки, соціально-побутова та спортивна інфраструктура.

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

Підтримка здобувачів вищої освіти забезпечується розвинутою соціальною інфраструктурою та інформаційними ресурсами, доступ до яких є безкоштовним. Для здобувачів створено соціально-побутові умови: функціонують гуртожитки (https://vntu.edu.ua/uk/information-for-enrollee/gurtozhitki-vntu-1281.html), буфети, здоровпункт, клуб, спортивний комплекс з футбольним полем, майданчиками для спортивних ігор у баскетбол, волейбол, теніс, а також спортивні зали. Усі навчальні корпуси та гуртожитки розміщені компактно на земельній ділянці університету, поблизу наявні зупинки громадського транспорту. Також у корпусах ВНТУ розташовуються скриньки довіри, де можна залишити скарги, зауваження та пропозиції. Листа освітньому омбудсмену можна надіслати в електронному вигляді (https://soc.vntu.edu.ua/?id=332&mode= new_item&f=sites/332/ombudsman.html). Крім того, для врахування потреб та інтересів здобувачів вищої освіти на Раді з якості освіти та Вченій раді ВНТУ періодично розглядаються питання стану навчально-методичної та організаційної роботи факультетів. Адміністрація розробляє шляхи використовування можливостей інформаційних ресурсів в процесі викладання навчальних дисциплін, забезпечує відбір та рекомендації найбільш ефективних технологій навчання з урахуванням специфіки дисципліни та рівня підготовки здобувача вищої освіти. Регулярно проводяться опитування щодо задоволеності здобувачів (https://socio-lab.vntu.edu.ua/ukr/), за підсумками яких приймаються відповідні рішення.

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

Безпечність освітнього середовища для життя та здоров'я здобувачів вищої освіти забезпечується системою заходів щодо охорони праці, дотримання техніки безпеки, санітарних норм та правил, а також правил протипожежної безпеки. Санітарно-технічний стан усіх приміщень, навчальних аудиторій і лабораторій університету відповідає вимогам чинних норм і правил експлуатації та щороку контролюється відділом охорони праці. Інженерною службою постійно контролюється технічний стан будівель та споруд, також до цієї роботи залучаються спеціалізовані організації, аварійні ситуації оперативно усуваються. Перед початком занять в кожній лабораторії викладачами здійснюється інструктаж з техніки безпеки та пожежної безпеки. Гарантування безпечності освітнього середовища для життя та здоров'я здобувачів вищої освіти здійснюється, у тому числі, завдяки систематичній роботі практичних психологів ВНТУ (https://soc.vntu.edu.ua/?id=332&mode=new_item&f=sites/332/psychology.html), які працюють зі здобувачами та співробітниками і викладачами, а також проводять тренінги, семінари та майстер-класи.
Адміністрація факультету та університету постійно співпрацює зі студентським самоврядуванням, вирішуючи питання, які стосуються здобувачів вищої освіти, які активно долучаються до вирішення нагальних питань щодо освітнього середовища, а також формування стратегії розвитку університету.
На початку семестру студентам нагадують про обладнанні укриття для захисту життя під час повітряних тривог та маршрути до них.

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.

Основним документом, який регламентує надання освітньої та організаційної підтримки здобувачам вищої освіти є Положення про освітню, організаційну, інформаційну, консультаційну та соціальну підтримку здобувачів вищої освіти у ВНТУ (https://vntu.edu.ua/uploads/n/np/8.pdf) та Положення про організацію освітнього процесу у ВНТУ (https://vntu.edu.ua/uploads/2024/Pol_study_process.pdf). Центром забезпечення якості освіти, Центром соціально-організаційної роботи, гарантами освітніх програм, факультетами та кафедрами університету забезпечується в повній мірі освітня та організаційна підтримка здобувачів. Функціонує власна система підтримки освітнього процесу JetIQ. У корпусах ВНТУ функціонує wi-fi мережа VNTU Campus з вільним доступом до мережі Інтернет. Допомогу у вигляді консультацій здобувачам вищої освіти здійснюють: приймальна комісія; деканат факультету ІТКІ; Науково-технічна бібліотека; Центр міжнародних зв'язків та проєктів; Центр соціально-організаційної роботи; органи студентського самоврядування, профком студентів, Наукове товариство студентів та аспірантів ВНТУ. Соціальна підтримка здобувачів вищої освіти у ВНТУ передбачає також стипендіальне забезпечення, яке регулюється Положенням про порядок призначення і виплати стипендій у ВНТУ

https://vntu.edu.ua/uploads/2022/Stypendiya%20VNTU%202022ed2.pdf. В університеті працюють практичні психологи, які консультують здобувачів освіти, зокрема, за телефоном та анонімно (https://soc.vntu.edu.ua/?id=332&mode=new_item&f=sites/332/psychology.html). Умови доступності закладу освіти для навчання осіб з особливими освітніми потребами наведені (https://vntu.edu.ua/uk/topic/umovi-dostupnosti-vntu-dlya-navchannya-osib-z-osoblivimi-osvitnimi-potrebami-1385.html). Інформаційна підтримка здобувачів може здійснюватися такими шляхами: через офіційний сайт ВНТУ, паперові та електронні ресурси бібліотеки ВНТУ; використання інформаційної системи JetIQ з метою підвищення ефективності управління освітнім процесом, централізованої розсилки повідомлень; офіційні сторінки та канали ВНТУ, його підрозділів та студентських організацій в соціальних мережах, забезпечення публічності інформації про діяльність ВНТУ на сайті університету. Також, відповідно до Положення про освітнього омбудсмена з прав студентів ВНТУ (https://vntu.edu.ua/uploads/2020/1054.pdf) кожен здобувач вищої освіти має безперешкодне право на звернення до омбудсмена і отримання аргументованої відповіді на своє звернення стосовно забезпечення реалізації прав, свобод і законних інтересів здобувачів вищої освіти.

Яким чином ЗВО створює достатні умови для реалізації права на освіту особами з особливими освітніми потребами? Наведіть посилання на конкретні приклади створення таких умов на ОП (якщо такі були)

У ВНТУ створені умови для осіб з особливими освітніми потребами таким чином, щоб вони могли отримувати освітні послуги (https://vntu.edu.ua/uk/topic/umovi-dostupnosti-vntu-dlya-navchannya-osib-z-osoblivimi-osvitnimi-potrebami-1385.html). Для забезпечення підтримки здобувачів з особливими освітніми потребами у ВНТУ при Центрі соціально-організаційної роботи створюється група психолого-педагогічного супроводу. До складу групи залучаються НПП ВНТУ, представники адміністрації, студентських організацій та волонтери. З метою створення належних умов для забезпечення освітнього супроводу у ВНТУ можуть обладнуватися ресурсні кімнати; приміщення для надання консультацій психологом, відпочинку, особистої гігієни, медичного обслуговування тощо. У ВНТУ діє порядок супроводу (надання допомоги) для осіб з інвалідністю та інших маломобільних груп населення. Усі навчальні корпуси та гуртожитки мають висновок про доступність (https://iq.vntu.edu.ua/fm/fdb/682/web/mtz.html). Здобувачі, що цього потребують, можуть отримувати індивідуальний графік навчання відповідно до Положення про організацію індивідуального графіку навчання здобувачів вищої освіти у ВНТУ (https://vntu.edu.ua/uploads/2022/Ind_grafik.pdf).

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

Пунктом 7.6 23) Статуту університету (https://vntu.edu.ua/images/docs/vntustatut.pdf) визначено, що особи, які навчаються в Університеті, мають право на захист від будь-яких форм експлуатації, фізичного та психічного насильства, від дій співробітників ЗВО, які порушують права чи принижують їх честь і гідність. Унормування антикорупційних політик у ВНТУ забезпечується Антикорупційною програмою ВНТУ (https://vntu.edu.ua/images/2017/antikor.pdf), Кодексом етики спільноти ВНТУ (https://vntu.edu.ua/uploads/2019/etika.pdf) та Положенням про академічну доброчесність у ВНТУ (https://vntu.edu.ua/uploads/2022/acad.pdf), які визначають норми професійної етики працівників, ключові цінності, основні принципи й стандарти етичної поведінки, принципи справедливості, рівноправності та недискримінаційності. Процедури реагування на випадки цькування, дискримінації, сексуального домагання, інших конфліктних ситуацій, регламентуються Правилами попередження і боротьби із сексуальними домаганнями, неетичною поведінкою та дискримінацією у ВНТУ, які наведені у додатку 1 до Положення про Комісію з етики (https://vntu.edu.ua/uploads/2021/ke.pdf).
Здобувачі у випадку необхідності можуть звернутися до скриньки довіри (https://vntu.edu.ua/uk/topic/skrinya-doviri-959.html) або до відповідного уповноваженого (https://vntu.edu.ua/images/2017/osoba.pdf) або освітнього омбудсмена ВНТУ (https://soc.vntu.edu.ua/?id=332&mode=new_item&f=sites/332/ombudsman.html). Кодекс етики ВНТУ впроваджує загальні моральні принципи та правила етичної поведінки працівників та здобувачів університету, якими вони мають керуватись у своїй діяльності, в тому числі політику та процедури врегулювання конфліктних ситуацій (включаючи пов'язаних із сексуальними домаганнями, дискримінацією та корупцією (https://vntu.edu.ua/images/etic.pdf). У Кодексі етики передбачено функціонування Комісії з етики (https://vntu.edu.ua/uploads/2021/ke.pdf), яка відповідає за поширення інформації про політику та процедури врегулювання конфліктних ситуацій, сприяє обізнаності трудового колективу та здобувачів щодо попередження та процедур врегулювання конфліктних ситуацій, пов'язаних із сексуальними домаганнями, неетичною поведінкою та дискримінацією, надає інформаційну та консультативну підтримку керівництву структурних підрозділів щодо попередження вказаних явищ, отримує і розглядає відповідні скарги. Згідно з процедурою до Комісії з етики у письмовій формі подається скарга, яка повинна містити факти, що підтверджують конфлікту ситуацію. На підставі рішення Комісії керівництво університету приймає відповідні рішення, передбачені та дозволені законодавством. У випадку виникнення конфліктних ситуацій до їх розв'язання залучається освітній омбудсмен з прав здобувачів відповідно до Положення про освітнього омбудсмена з прав студентів ВНТУ (https://vntu.edu.ua/uploads/2020/1054.pdf).
Випадків порушення таких процедур унаслідок конфліктних ситуацій на ОПП, що акредитується, 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

У Вінницькому національному технічному університеті процедури розроблення, затвердження, моніторингу та періодичного перегляду ОПП регулюються Положенням про розроблення та супроводження освітніх програм у ВНТУ (https://vntu.edu.ua/uploads/n/np/1.pdf).

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

Для забезпечення високої якості освіти гарант ОПП проводить моніторинг і періодично переглядає ОПП, з метою забезпечення відповідності меті, зазначеній у ОПП, а також потребам стейкхолдерів, в тому числі інтересів здобувачів вищої освіти та суспільства в цілому. Перегляд ОПП відбувається не рідше одного разу на рік відповідно до Положення про розроблення і супроводження освітніх програм. В результаті перегляду здійснюється оновлення, вдосконалення ОПП на основі відгуків, рекомендацій та пропозицій стейкхолдерів, або ОПП залишається без змін. Також під час перегляду ОПП до уваги беруться результати зовнішнього забезпечення якості вищої освіти (зокрема, зауваження і пропозиції, сформульовані під час акредитації інших ОПП). Зміни до ОПП вносяться за поданням гаранта ОПП, розглядаються на засіданнях робочої групи, кафедри, Студентської ради факультету, вченої ради факультету, Раді з якості ВНТУ, ухвалюються Вченою Радою ВНТУ та затверджуються наказом ректора. Усі зацікавлені сторони інформуються про будь-які заплановані, а також реалізовані зміни упродовж цього процесу. Відповідна інформація розміщується у модулі Освітні програми на сайті кафедри (https://iq.vntu.edu.ua/departs/?id=246&lid=3&mode=lp).
26 січня 2023 р. було започатковано ОПП Безпека інформаційних і комунікаційних систем зі спеціальності 125 Кібербезпека та захист інформації для продовження провадження освітньої діяльності за ОПП Безпека інформаційних і комунікаційних систем зі спеціальності 125 Кібербезпека, яка вже функціонувала, без зміни по суті, що зумовлено Постановою Кабінету Міністрів України від 16 грудня 2022 р. № 1392 «Про внесення змін до переліку галузей знань і спеціальностей, за якими здійснюється підготовка здобувачів вищої освіти». Під час обговорення було враховані пропозиції, які пов'язані з введенням професійних стандартів у галузі Кібербезпеки, зокрема, 2139.2 Аналітик з безпеки інформаційно-телекомунікаційних систем та 2139.2 Адміністратор мереж і систем, додані відповідні компетентності та результати навчання (КФ12, РН25, РН26) та інші.
У зв'язку із затвердження нової стратегії розвитку ВНТУ на 2023-2027 рр. (https://vntu.edu.ua/projects/development_strategy-2023.pdf) змінено мету ОПП.
Ці та інші зміни, а також їх автори, приведені в узагальненій таблиці результатів обговорення ОПП Безпека інформаційних і комунікаційних систем, що наведені на сайті кафедри ЗІ (https://iq.vntu.edu.ua/departs/?id=246&lid=3&mode=lp) у модулі Освітні програми.
Пропозиції щодо вдосконалення ОПП приймаються від усіх зацікавлених осіб та організацій і аналізуються протягом навчального року. Для цього на сайті кафедри розміщується проект наступної ОПП з контактами для надання пропозицій.

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

У ВНТУ системно організована робота постійно діючої моніторингової Лабораторії соціологічних досліджень (https://socio-lab.vntu.edu.ua/ukr), яка, в тому числі, залучає здобувачів до опитування щодо якості ОПП та навчального процесу. Таким чином, здобувачі вищої освіти на постійній основі залучені до процесу перегляду ОПП та інших процедур забезпечення її якості.
Питання про перегляд ОК та ОПП розглядаються на засіданнях кафедри (щонайменше один раз на рік), вченої ради факультету, Ради з якості освіти ВНТУ, Вченої ради ВНТУ. На засідання кафедри запрошуються зацікавлені здобувачі вищої освіти, випускники та роботодавці.
Під час обговорення ОПП у 2023 враховані пропозиції ст. Геннадія Л. щодо поглиблення вивчення процесів проектування, та Дмитра Р. покращити підготовку із протидій та виявлення фішінгових атак. У 2024 у усній формі здобувач Іван С. вніс пропозицію ввести в перелік обов'язкових ОК дисципліну пов'язану з розробкою програм, зокрема комп'ютерних ігор, яка була відхилена.

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

Студентське самоврядування бере активну участь у процедурах внутрішнього забезпечення якості ОПП через членство у Вченій раді ВНТУ, Раді з якості освіти ВНТУ та вченій раді факультету – відповідно до чинних положень університету (https://vntu.edu.ua/uploads/2020/Sts.pdf).
Органи студентського самоврядування беруть участь в обговореннях та прийнятті рішень щодо питань внутрішнього забезпечення якості освіти, в тому числі й якості ОПП БІКС шляхом внесення пропозицій щодо контролю за якістю навчального процесу та пропозицій щодо ОПП.
Студентська рада факультету розглядає та схвалює проект ОПП, що є обов'язковим етапом її затвердження і перегляду. Так, ОПП було розглянуто та схвалено на засіданні Студентської ради факультету інформаційних технологій та комп'ютерної інженерії від 13.01.2023 протокол № 10.
Крім цього, представники студентського самоврядування факультету беруть активну участь у мотивуванні здобувачів освіти до участі в опитуваннях (https://socio-lab.vntu.edu.ua/ukr/poll/).
У 2023 р. за ініціативи студентського самоврядування було прийнято рішення щодо деякого урегулювання самостійної роботи здобувачів, а саме виділення в робочих програмах не менше 3-х годин на одну лабораторну

роботу (протокол Вченої ради № 3 від 28.09.2023).
Студентський уряд бере активну участь у житті студентства, в тому числі адаптації першокурсників (https://vntu.edu.ua/uk/news/zustrich-studentskoyi-rady-vntu-iz-administratsiyeyu-universytetu-2917.html)

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

Роботодавці беруть участь в обговоренні ОПП та її складових (зокрема змісту ОК) під час спільних зустрічей з гарантом, завідувачем кафедри або іншими НПП, вони залучаються до семінарів та конференцій, які відбуваються у ВНТУ.
В процесі обговорення ОПП враховані пропозиції:
- начальника УПК у Вінницький обл. ДКП НПУ О. Ульяненкова, який запропонував врахувати особливості професійних стандартів Адміністратор мереж і систем, а також Аналітик з безпеки інформаційно-телекомунікаційних систем;
- директора ТОВ ВІНІНТЕРАКТИВ О. Томашпольського, який запропонував посилити практичну складову навчання та залучення практиків до викладання навчальних дисциплін для покращення професійної орієнтованості здобувачів вищої освіти;
- директора ТОВ Trustee Global В. Груші, який запропонував включити до програми навчальної дисципліни Моніторинг та аудит кібербезпеки особливості сертифікації щодо відповідності інформаційних процесів стандартам безпеки, особливу увагу звернути на викладення вимог PCI DSS;
- директора ТОВ Каскад-Безпека Л. Шестопалюк, яка запропонувала залучати професіоналів-практиків для викладання окремих дисциплін або факультативів.
Пропозиції роботодавців, які були враховані в ОПП, наведені на сайті кафедри ЗІ у модулі освітні програми (https://iq.vntu.edu.ua/departs/index.php?id=246&lid=3&mode=lp).

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

Кафедра ЗІ на постійній основі прослідковує кар'єрні шляхи випускників магістратури через періодичний телефонний контакт з ними та соціальні мережі, участь випускників у засіданнях ІТ-клубу CyberSecPals. Гарант ОПП та співробітники кафедри підтримують зв'язки з випускниками минулих років. Список найуспішніших випускників представлений на сайті кафедри (https://zi.vntu.edu.ua/vipuskniki.html) й постійно оновлюється.
Кафедра ЗІ активно співпрацює з випускниками, які мають достатній практичний досвід, та запрошуються для участі в різних формах навчального процесу, урочистих та профорієнтаційних заходах. Відстежується інформація про працевлаштування та професійне зростання випускників через контакти із роботодавцями. Кафедра ЗІ регулярно запрошує успішних випускників для проведення зустрічей зі здобувачами з метою підвищення мотивації до навчання за рахунок передачі свого досвіду кар'єрного росту та сучасних передових технологій в сфері інформаційних технологій, кібербезпеки та захисту інформації.
Наприклад, випускник кафедри ЗІ Сінчук Андрій – senior java developer провів лекцію на тему Конфіденційність користувацьких даних у сучасних комерційних системах (https://iq.vntu.edu.ua/departs/index.php?id=246&id_news=2501&mode=full_news),
Вячеслав Козачок – Платформа Splunk як система керування подіями та інцидентами SIEM (https://www.youtube.com/watch?v=EdopoQZ3ZoY) та багато інших на каналі клубу.
Результати взаємодії з випускниками враховуються як пропозиції під час розроблення та переглядання ОПП.

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

Відповідно до Положенням про розроблення та супроводження освітніх програм у ВНТУ (https://vntu.edu.ua/uploads/n/np/1.pdf) внутрішнє забезпечення якості освіти в університеті реалізується через такі заходи:
– моніторинг і періодичний перегляд ОПП з послідовним дотриманням визначених процедур їх оновлення;
– залучення здобувачів вищої освіти та органів студентського самоврядування до процесу періодичного перегляду ОПП;
– залучення роботодавців та їх асоціацій до процесу періодичного перегляду ОПП;
– збір, аналіз і врахування інформації щодо кар'єрного шляху випускників;
– дотримання принципів академічної доброчесності працівниками Університету та здобувачами вищої освіти.
Результати аналізу внутрішнього забезпечення якості представляються директором Центру забезпечення якості освіти виносяться на засідання Ради з якості ВНТУ, далі на Вчену раду ВНТУ, рішення якої затверджуються наказом ректора (https://eqa.vntu.edu.ua/?id=340&mode=new_item&f=682/web/monitoring.html).
Необхідність організації онлайн-навчання під час локдауну вимагала, в тому числі, поліпшення доступу магістрантів до методичного забезпечення дисциплін, автоматизації поточного та підсумкового тестування. Завдяки діючій системі забезпечення якості ЗВО було реалізовано загально університетську систему освітнього процесу JetIQ, що дозволило створити єдиний інформаційний простір для всіх учасників освітнього процесу з постійнодіючим доступом до всіх необхідних інформаційних ресурсів.
Крім того, залучено професіоналів-практиків до проведення занять; переглянуто зміст робочих навчальних програм дисциплін та силабусів відповідно до сучасного розвитку інформаційних технологій, кібербезпеки та захисту інформації; проводяться заходи щодо міжнародної академічної мобільності здобувачів вищої освіти.
Результати опитувань здобувачів ВНТУ публікуються на сайті (https://socio-lab.vntu.edu.ua/ukr/) та доповідаються на Вченій раді ВНТУ (https://vntu.edu.ua/uploads/2024/BPdecision250124.pdf). Результати опитувань розглядаються

на засіданні кафедри (Протокол кафедри ЗІ №13 від 05.03.2024).

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?

ОПП Безпека інформаційних і комунікаційних систем другого (магістерського) рівня вищої освіти спеціальності 125 Кібербезпека та захист інформації враховує рекомендації попередніх акредитацій інших освітніх програм. Зокрема, під час перегляду ОПП та оновлення її змісту за традицією залучаються здобувачі вищої освіти; продовжується практика вивчення досвіду ОПП з кібербезпеки іноземних ЗВО щодо їх змісту та матеріально-технічного забезпечення; підвищується рівень інформаційної обізнаності здобувачів щодо можливостей академічної мобільності та визнання результатів навчання, отриманих в інших ЗВО та у неформальній освіті; здійснюється постійне оновлення джерел в робочих програмах навчальних дисциплін; забезпечується залучення професіоналів-практиків до аудиторних занять; постійно оновлюється матеріально-технічна база кафедри; розширюється перелік організацій і установ для стажування викладачів та практики здобувачів.
За результатами акредитації інших ОПП було зроблено зауваження щодо публікації проекту освітніх програм, як наслідок у ВНТУ в системі JetIQ запроваджено модуль “Освітні програми”, який дозволяє здійснювати керування оприлюдненням ОПП та їх проектів на сайтах кафедр.
Також, під час акредитації ОПП 24799 Кібербезпека інформаційних технологій та систем ІІ (магістерського) рівня надана рекомендація ГЕР «Розширити кількість баз практик, особливо у профільних роботодавців, які спеціалізуються саме на проєктуванні та встановленні комплексних систем захисту інформації». В 2024 р. магістранти за ОПП БІКС проходять практику у Вінницькій міській раді (на об’єктах критичної інфраструктури, де потрібно побудувати систему захисту). Рекомендації цієї ж ГЕР щодо покращення інформування здобувачів з різних процесів ВНТУ знайшло відображення у змінах до Положення про порядок розробки і затвердження робочих програм та силабусів навчальних дисциплін ВНТУ (рішення Вченої ради ВНТУ від 29.08.2024 № 2, https://vntu.edu.ua/uploads/2024/P_RNPD_sylab_2024_2024_08_29.pdf), де обов’язковим розділом є «Академічні права та обов’язки».
Відповідно до рекомендацій наданих ЕГ/ГЕР під час акредитації ОПП 5374 Безпека інформаційних і комунікаційних систем та ОПП 32027 Кібербезпека критичних систем І (бакалаврського) рівня щодо покращення МТЗ, отримано на кафедру ЗІ два корпоративних сервери для проведення навчальних занять, які можуть використовуються для здобувачів всіх рівнів вищої освіти, а також запропоновані вибіркові дисципліни пов’язані із використанням штучного інтелекту в задачах кібербезпеки.

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

Учасники академічної спільноти постійно залучені до процедур забезпечення якості ОПП. Насамперед, через обговорення проєктів та рецензування ОПП, систему підвищення кваліфікації викладачів, комплекс наукових і методичних заходів різного рівня.
До процедур внутрішнього забезпечення якості ОПП залучені кафедри, що забезпечують викладання окремих ОК. Викладачі беруть участь у роботах методичних й наукових семінарів та засідань кафедри, метою яких є оптимізація структури та змісту освітніх компонентів, обмін досвідом щодо методик викладання дисциплін кафедри, обговорення можливостей використання сучасних технологій у навчанні, розвиток навчально-методичного та матеріально-технічного забезпечення освітньої програми, а також пошук шляхів вдосконалення педагогічної майстерності.
Зауваження, які виникають в процесі обговорення чинних положень та процесів, враховуються у подальшій роботі кафедри та за потреби виносяться на розгляд рад та комісій різного рівня.
Науково-педагогічні працівники, як постійні члени Вченої ради факультету (В. Лужецький, Н. Кондратенко, О. Войтович, А. Дудатьєв), Ради з якості освіти (О. Войтович) та Вченої ради ВНТУ (В. Лужецький, О. Войтович) розглядають питання стану якості ОПП, обговорюють та ухвалюють рішення щодо конкретних дій для забезпечення якості ОПП на рівні ВНТУ.

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

У ВНТУ сформована та постійно розвивається культура якості освіти з метою забезпечення всебічного розвитку здобувачів вищої освіти ВНТУ та їх якісної підготовки до професійної діяльності.
Розподіл обов’язків такий:
– Ректор та Вчена рада відповідає за розвиток та підтримання політики із забезпечення якості освіти;
– Проректор з науково-педагогічної роботи та організації освітнього процесу ВНТУ відповідає за організацію освітнього процесу;
– Проректор з наукової роботи – за підтримку наукових досліджень та їх інтеграцію в освітній процес;
– Проректор з науково-педагогічної роботи, міжнародного співробітництва та молодіжної політики – за підтримку соціально-організаційної роботи та міжнародне співробітництво;
– кафедри та факультет відповідають за удосконалення навчальних дисциплін, освітніх програм та якості викладання, профорієнтацію;
– Центр забезпечення якості освіти відповідає за професійний розвиток викладачів, участь у вдосконаленні ОПП та якості викладання, дотримання норм академічної доброчесності, опитування, зовнішнє та внутрішнє забезпечення якості освіти (https://eqa.vntu.edu.ua/?id=340&mode=new_item&f=682/web/monitoring.html);
– Центр соціально-організаційної роботи відповідає за організацію позанавчальної активності студентів, сприяння самореалізації та персонального зростання здобувачів.

Система внутрішнього забезпечення якості освіти ВНТУ сертифікована за ДСТУ ISO 9001:2015 (https://vntu.edu.ua/images/2019/cert_9001/cert_9001.pdf).

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?

Права та обов'язки учасників освітнього процесу регулюються такими документами ЗВО:
- Статут ВНТУ (https://vntu.edu.ua/images/docs/vntustatut.pdf);
- Правила внутрішнього розпорядку для працівників ВНТУ та осіб, що навчаються в ньому (https://vntu.edu.ua/uploads/2022/Pravilavnytrrozp2022.pdf);
- Положення про організацію освітнього процесу у ВНТУ (https://vntu.edu.ua/uploads/2024/Pol_study_process.pdf);
- іншими документами, які розміщені у розділі «Загальна публічна інформація» ((http://vntu.edu.ua/uk/public-info/zag.html) на сайті ВНТУ.

Усі документи є у вільному доступі на офіційному сайті ВНТУ.
Крім цього у ВНТУ для інформування здобувачів та співробітників про введення і дію, зміни, відміну нормативних документів тощо використовується система електронних особистих кабінетів у системі JetIQ, яка підтримує особисті повідомлення та централізовані розсилки інформації.

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

У системі JetIQ передбачений модуль Освітні програми, в якому гаранти виставляють для обговорення проекти освітніх програм, отримані зауваження та пропозиції, таблиці обговорення та самі затверджені освітні програми (https://iq.vntu.edu.ua/departs/?id=246&lid=3&mode=lp)

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

У системі JetIQ передбачений модуль Освітні програми, з якого формується загальноуніверситетська сторінка з усіма освітніми програмами, навчальними планами, (https://jetiq.vntu.edu.ua/edu_progs/ep_list.php?l=2) та посиланнями на сторінки кафедр, де є можливість побачити всі ресурси, зокрема, робочі програми навчальних дисциплін, силабуси, в тому числі вибіркових дисциплін.
Можливості формування індивідуальної освітньої траєкторії здобувачів вищої освіти викладені в Положенні про вільний вибір навчальних дисциплін здобувачами вищої освіти ВНТУ (https://vntu.edu.ua/uploads/2024/P_vybir_2024_08_29.pdf)

11. Перспективи подальшого розвитку ОП

Якими загалом є сильні та слабкі сторони ОП?

Сильні сторони ОПП:
– ОПП розроблено з урахуванням досвіду роботодавців, фахівців з провідних університетів України та іноземних ЗВО;
– використання для підтримки освітнього процесу власної системи JetIQ, яка дозволяє автоматизувати процеси управління освітнім процесом, зокрема моніторинг та аудит забезпечення якості освіти, надає всім учасникам освітнього процесу інформацію щодо навчальних компонентів та інших видів забезпечення, що особливо важливо в період воєнного стану;
– систематичне врахування пропозицій та зауважень всіх груп стейкхолдерів, що сприяє динамічному розвитку ОПП;
– наявність у ВНТУ Комісії з етики, Комісії з академічної доброчесності, освітнього омбудсмена з прав студентів;
– наявність системи внутрішнього забезпечення якості освіти сертифікованої за ДСТУ ISO 9001:2015 (https://vntu.edu.ua/images/2019/cert_9001/cert_9001.pdf).
Слабкими сторонами є:
– відсутність практики викладання дисциплін ОПП іноземною мовою, що мало б значно розширити можливості академічної мобільності, міжнародної академічної мобільності.

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

Стратегічні перспективи розвитку ОПП повністю відповідають Стратегії розвитку ВНТУ на 2023–2027 рр.

Розвиток ОПП передбачає такі заходи:
– започаткувати викладання англійською мовою освітніх компонентів за вільним вибором здобувачів;
– більш активно залучати роботодавців та професіоналів-практиків до викладання вибіркових дисциплін повністю або частково;
– підвищити рівень академічної мобільності здобувачів вищої освіти ОПП, відповідно до укладених угод про співпрацю;
– подальше вдосконалення матеріально-технічної бази;
– розширювати форми співпраці з академічними та бізнес стейкхолдерами через їх активне залучення до проведення лекцій, практичних занять за ОПП, семінарів, круглих столів.

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: Тужанський Станіслав Євгенович

Дата: 18.09.2024 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	
Інноваційні та психологічні аспекти сучасної освіти	навчальна дисципліна	*02_ІПАСО_125_2023.pdf*	nHYH99hMAnuwWG41qsbg33r1apbI9iLuxu2HnSNkBEM=	*проектор, мультимедійний екран, комп'ютер, електронна система ВНТУ JetIQ, google.meet*
Ділова іноземна мова	навчальна дисципліна	*03_ІМ_125_2024.pdf*	454axe/4c09iSAyErwOOdJDcsyRvUy/WFRxMrOhuqYk=	*проектор, плакати, мультимедійний екран, комп'ютер, електронна система ВНТУ JetIQ, google.meet*
Методологія та організація наукових досліджень в кібербезпеці	навчальна дисципліна	*04_МОНДКБ_125_2024.pdf*	GWAnud2dPepOGmEpYLLDaF6jKrMBPYhSi8vZmLgLcmI=	*ауд. 2425 (проектор, мультимедійний екран), електронна система ВНТУ JetIQ, google.meet*
Сучасні системи, технології та засоби інформаційної безпеки та кібербезпеки	навчальна дисципліна	*05_ССТЗІБ_125_2024.pdf*	nt9/UNZjugJ84k5G6S5rn2/Dt+iYpnPeto+YQmj902g=	*ауд. 2425 (проектор, мультимедійний екран), лаб. 2423 (Docker, Docker compose, Traefik, The Social-Engineer Toolkit (SET), Gophish - Open Source Phishing Framework, XCA (X - Certificate and Key management), Nginx, Apache (опціонально), Authentik, Portainer (опціонально), OpenVPN Access Server, WireGuard (wg-easy), OSSEC, CrowdSec, Honeypress, Masscanned, Sslscan, OWASP ZAP, Burp Suite), електронна система ВНТУ JetIQ, google.meet*
Кібербезпека	навчальна дисципліна	*06_КБ_125_2024.pdf*	UmKnLRWH6Y1B4jPGMz/IR5XxSBMtN7sD1SZJzoFqJnI=	*ауд. 2425 (проектор, мультимедійний екран), ауд. 2422 (Kali Linux, Virtual Box, Wireshark, tcpdump, Nmap, Metasploit, Burp Suite, Xprobe, Netcat, Wafw00f, Openssl, OWASP ZAP, slowhttptest, Nginx, Apache HTTP Server, SQLmap.) електронна система ВНТУ JetIQ, google.meet*
Кібербезпека об'єктів критичної інфраструктури	навчальна дисципліна	*07_КОКІ_125_2024.pdf*	5eIfQLfjoe0xhP2GvQkNrltbfG5xiCsvqtA22lBjfEg=	*ауд. 2425 (проектор, мультимедійний екран), лаб. 2429 (CentOS Linux, PyCharm Community Edition, Oracle VirtualBox, Ghidra, Android-x86, Open LDAP, VS Code, Comodo Free Antivirus), електронна система ВНТУ JetIQ, google.meet*
Проектування систем кібербезпеки (в т.ч. курсова робота)	навчальна дисципліна	*08_ПСК_125_2024.pdf*	vO9anD4TN7ujeZqCKa2wpCJ5ea8tsL+pnAJGtaYQMJs=	*ауд. 2425 (проектор, мультимедійний екран), лаб. 2423 (ProjectLibre, Atlassian Jira (trial)Atlassian Trello, Atlassian Confluence, Atlasian Opsgenie, Git, PyCharm Community, Visual Studio, SonarQube Community, Snyk Code), електронна система ВНТУ JetIQ, google.meet*
Моніторинг та аудит кібербезпеки	навчальна дисципліна	*09_МАКБ_125_2024.pdf*	q65DHEJj6IN5k7h9JAoAh9zhQnzBB1Q8jwNJpBv4GoQ=	*ауд. 2425 (проектор, мультимедійний екран); лаб. 2423 (Kali Linux, VirtualBox, AccessData FTK Imager); електронна система ВНТУ JetIQ, google.meet*

Переддипломна практика	практика	*10_Переддип_прак_125_2024.pdf*	gXFaTI8n1DO4bBiyJ/UyL4ssw7sGC4NylZo8Yx0m4vQ=	*матеріально-технічна база кафедри або місця проведення практики*
Магістерська кваліфікаційна робота	підсумкова атестація	*11_МВ_МКР_2024.pdf*	ax4u9I6baWb+C3HqmS7yv39T2+yTN8IimHon6ZFqHRU=	
Філософія науки і техніки	навчальна дисципліна	*01_ФНТ_125_2024.pdf*	w3iTyAq8jtjoHfZbjLZ4AyQGLbrhBcybYwtH+W3pTgw=	*проектор, мультимедійний екран, комп'ютер, електронна система ВНТУ JetIQ, google.meet*

* 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)
282379	Кот Сергій Олександрович	Доцент, Основне місце роботи	Факультет будівництва, цивільної та екологічної інженерії	Диплом спеціаліста, Вінницький державний педагогічний інститут, рік закінчення: 1997, спеціальність: російська мова і зарубіжна література та англійська мова, Диплом кандидата наук ДК 040973, виданий 10.05.2007	19	Ділова іноземна мова	Освіта: Вінницький педагогічний інститут ім. М.Коцюбинського, 1997, "російська мова і зарубіжна література та англійська мова" Підвищення кваліфікації 1. ГО МІЖНАРОДНА ФУНДАЦІЯ НАУКОВЦІВ ОСВІТЯН, інша, участь у вебінарі, USING THE OPPORTUNITIES OF CLOUD SERVICES FOR MASTERS AND POSTGRADUATE STUDENTS, з 04.10.2021 по 11.10.2021, Certificate ESN№8252.2021, 2021-10-11, 45 год, 1,5 кред. 2. ТОВ "НАУКОВІ ПУБЛІКАЦІЇ", участь у вебінарі, International experience in the field of publishing. Successful publications in Scopus and Web of Science., з 20.01.2022 по 11.02.2022, Certificate AA №3522/11.02.2022, 2022-02-11, 30 год, 1 кред. 3. ГО МІЖНАРОДНА ФУНДАЦІЯ НАУКОВЦІВ ОСВІТЯН, участь у вебінарі, THE CLOUD STORAGE SERVICE FOR THE ONLINE STUDYING ON THE EXAMPLE OF THE ZOOM PLATFORM, 28.09.2020-05.10.2020, Certificate

							ES №1732/2020, 2020-10-05, 45 год, 1,5 кред. 4. Zustricz Foundation. Department of Polish-Ukrainian Studies of Jagiellonian University in Krakow. Career Development Center of NGO Sobornist. Luhansk Regional Institute of Postgraduate Pedagogical Education., online-курс, участь у семінарі, FUNDRAISING AND ORGANIZATION OF PROJECT ACTIVITIES IN EDUCATIONAL ESTABLISHMENTS: EUROPEAN EXPERIENCE., з 12.02.2022 по 20.03.2022, English-language Competence of Higher Education Teachers, Certificate SZFL-001639, 2022-03-20, 180 год, 6 кред. Публікації: Nykyporets S. S., Kot S. O., Hadaichuk N. M., Melnyk M. B., Boiko Y. V. Innovative pedagogical strategies for utilizing online platforms in foreign language acquisition. Актуальні питання у сучасній науці. Серія «Педагогіка» : журнал. 2024. No. 5(23). P. 730–743. Nykyporets S. S., Kot S. O., Boiko Yu. V., Melnyk M. B., Chopliak V. V. Advanced integration of virtual information environments (VIEs) in contemporary educational methodologies. Society and national interests. Series «Education/Pedagogy». 2024. No. 4(4). Pp. 139–154. Kot S. O., Nykyporets S. S. Utilization of artificial intelligence in enhancing English language proficiency in tertiary education. Science and Education in the Third Millennium : Information Technology, Education, Law, Psychology, Social Sphere, Management : International collective monograph. Lublin, Polska, 2024. Chap. 10. P. 250-274. URI: https://doi.org/10.5281/zenodo.11279390. Абрамович Г. В. English for Computing I [Текст] : навчальний

							посібник / Г. В. Абрамович, О. С. Кот, Н. П. Хоменко. – Вінниця : ВНТУ, 2015. - 104 с. Досвід професійної роботи: Член української асоціації когнітивної лінгвістики і поетики Здійснення підприємницької діяльності з 08.04.2002 року за КВЕД 74.30 - Надання послуг перекладу.
331087	Карпінець Василь Васильович	Доцент, Суміщення	Факультет менеджменту та інформаційної безпеки	Диплом спеціаліста, Вінницький національний технічний університет, рік закінчення: 2007, спеціальність: 7.03060101 менеджмент організацій і адміністрування, Диплом магістра, Вінницький національний технічний університет, рік закінчення: 2006, спеціальність: 091501 Комп'ютерні системи та мережі, Диплом кандидата наук ДК 006688, виданий 17.05.2012, Атестат доцента 12ДЦ 040420, виданий 22.12.2014	12	Методологія та організація наукових досліджень в кібербезпеці	Науковий ступінь: Кандидат технічних наук, спеціальність 05.13.21 - Системи захисту інформації; тема дисертації: «Методи та засоби захисту векторних зображень зі зменшеним спотворенням внаслідок вбудовування цифрових водяних знаків». Завідувач кафедри менеджменту та безпеки інформаційних систем, доцент. Підвищення кваліфікації 1. Центр інформаційних технологій і захисту інформації, Вінницький національний технічний університет, очна, навчання за освітньою програмою професійного розвитку, «Захист інформації в інформаційно-комунікаційних системах та на об'єктах інформаційної діяльності», з 14.06.2021 по 29.06.2021, СПК №301838, 29.06.2021 р., 2021-06-29, 78 год, 2,6 кред. 2. Lublin University of Technology, Faculty Electrical Engineering and Computer Science, дистанційна, стажування, Development of information technologies through the use of new technologies in the field of research of image processing, machine learning, deep learning, artificial intelligence, intelligent data analysis, neural networks, security technologies,

							development of information-measuring systems diagnostic monitoring, з 06.03.2023 по 06.05 2023, Сертифікат № 8-2023-VNTU, 2023-05-06, 180 год, 6 кред. Публікації: 1. Підвищення стійкості цифрових водяних знаків у потокових відеозаписах на основі диференціального вбудовування енергії (DEW) [Текст] / Ю. Є. Яремчук, В. В. Карпінець, І. С. Зоря, Д. О. Козак // Вісник Вінницького політехнічного інституту. 2023. – № 1. – С. 55–64. 2. Салієва О. В., Карпінець В. В., Грицак А.В., Павловський П. В., Бондаренко І. О. Підвищення стійкості криптографічних алгоритмів у багатокористувацьких Web-ресурсах на основі генераторів випадкових чисел, що враховують ентропію поведінки користувача. Вимірювальна та обчислювальна техніка в технологічних процесах. 2023. № 1. С. 167-173. 3. Засіб захисту аналогового телефонного зв`язку на основі скремблера зі зміною коефіцієнтів вейвлет-перетворення [Текст] / В. В. Карпінець, В. С. Катаєв, П. В. Павловський, Д. Ю. Гереш // Вісник Вінницького політехнічного інституту. – 2023. – № 2. – С. 89–96. 4. Kataiev V., Yevhrafov D., Karpinets V., Yaremchuk Yu., Kunanets N. Noise generator of interfering signals for suppression information leakage signal generated by liquid crystal monitor screen. Proceedings of the 2nd International Conference on Conflict Management in Global Information Networks (CMiGiN 2022), Kyiv, Ukraine, November 30, 2022. 2022. P. 61-70. 5. Method of user authentication by keyboard handwriting based on neural

							networks and genetic algorithm / Andrii Pryimak, Yurii Yaremchuk, Olha Salieva, Vasyl Karpinets, Nataliia Kunanets // Proceedings of the International Workshop of IT-professionals on Artificial Intelligence (ProfIT AI 2021). – Kharkiv, Ukraine, September 20-21, 2021, P. 141-149. (Scopus). 1. Програма для захисту від несанкціонованого доступу шляхом використання графічного тесту авторизації : Свідоцтво про реєстрацію авторського права на твір (Комп'ютерна програма) №115963. Дата реєстрації 19.01.2023. автори: Карпінець В.В., Салієва О. В., Присяжний Д.П., Павловський П.В., Шиян А.А. 2. Програма для захисту коду будь-якої іншої програми від статичного дослідження шляхом внесення надлишкового коду : Свідоцтво про реєстрацію авторського права на твір (Комп'ютерна програма) №115961. Дата реєстрації 19.01.2023. автори: Карпінець В.В., Салієва О. В., Присяжний Д.П., Павловський П.В., Шиян А.А. 3. Програма захисту від несанкціонованого доступу шляхом обмеження функціональних можливостей : Свідоцтво про реєстрацію авторського права на твір (Комп'ютерна програма) №115962. Дата реєстрації 19.01.2023. автори: Карпінець В.В., Салієва О. В., Присяжний Д.П., Павловський П.В., Шиян А.А. 4. Програма для захисту від несанкціонованого доступу шляхом використання серверу авторизації на основі власного протоколу : Свідоцтво про реєстрацію авторського права на

							твір (Комп'ютерна програма) №115964. Дата реєстрації 19.01.2023. автори: Карпінець В.В., Салієва О. В., Присяжний Д.П., Павловський П.В., Шиян А.А. 5. Програма для захисту від несанкціонованого доступу шляхом використання серверу авторизації на основі протоколу HTTP: github : Свідоцтво про реєстрацію авторського права на твір (Комп'ютерна програма) №115965. Дата реєстрації 19.01.2023. автори: Карпінець В.В., Салієва О. В., Присяжний Д.П., Павловський П.В., Шиян А.А. Член редакційної колегії наукового-технічного збірника «Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні». Загальний досвід практичної роботи у галузі захисту інформації – 14 років. З 2008 р. виконував роботи із захисту інформації згідно ліцензії Вінницького національного технічного університету на провадження господарської діяльності з надання послуг у галузі криптографічного захисту інформації та технічного захисту інформації (чинна ліцензія ВНТУ видана Адміністрацією Державної служби спеціального зв'язку та захисту інформації України згідно наказу №115 від 15.02.2017 р.).
144072	Лужецький Володимир Андрійович	Завідувач кафедри, професор, Основне місце роботи	Факультет інформаційних технологій та комп`ютерної інженерії	Диплом спеціаліста, Таганроський радіотехнічний інститут, рік закінчення: 1972, спеціальність: 0642 Інформаційна вимірювальна техніка, Диплом доктора наук ДД 003524, виданий 14.04.2004,	43	Сучасні системи, технології та засоби інформаційної безпеки та кібербезпеки	Науковий ступінь: доктор технічних наук, спеціальність: 01.05.02 - Математичне моделювання та обчислювальні методи/ 05.13.05 - Комп'ютерні системи та компоненти, тема: Теорія "фібоначчієвих" моделей даних, методів обчислень і операційних пристроїв високої продуктивності та

				Атестат професора 02ПР 003307, виданий 21.04.2005			надійності Вчене звання: професор кафедри захисту інформації. Підвищення кваліфікації: 1. ТОВ "Лабораторія комп`ютерної криміналістики", стажування, Експертиза електронних комунікацій, з 02.10.2023 р. по 08.12. 2023 р., Довідка про проходження онлайн-курсу, 2023-12-15, 180 год, 6,0 кред. 2. ТОВ "Каскад-Безпека", очна, стажування, Сучасні системи кіберзахисту, з 03.06 2024 р. по 02. 08 2024 р., Участь у реалізації проєктів, що виконуються ТОВ "Каскад-Безпека", Довідка про проходження стажування, 2024-08-02, 120 год, 4,0 кред. Публікації: 1. Селезньов В. І., Лужецький В. А. Метод малоресурсного гешування типу «дані – генератор». Кібербезпека: освіта, наука, техніка. 2023. 2(22). С. 84-95. 2. Лужецький В. А. Спеціалізований процесор для ущільнення даних [Текст] / В. А. Лужецький, Л. А. Савицька, В. А. Каплун // Інформаційні технології та комп'ютерна інженерія. – 2022. – № 2. – С. 15-25. 1. Лужецький В. А., Шелепало Г.В. Прості числа: властивості та застосування в криптографії. – Вінниця: ВНТУ, 2023. – 160 с. 2. В Лужецький, Л Савицька, В Каплун Спеціалізований процесор для ущільнення даних. Інформаційні технології та комп'ютерна інженерія, 2022, 54 (2), 15-25. 3. Editorial. Preface. Bezkorovainyi, V., Bychkov, O., Luzhetskyi, V. et al. CEUR Workshop Proceedings, 2021, 3126 4. Luzhetskyi, V., Semerenko, V. Automaton Presentations of Reed-

							Solomon Codes. 2019 3rd International Conference on Advanced Information and Communications Technologies, AICT 2019 - Proceedings, 2019 , pp. 50–53, 8847892 5. P. Mykhailo and V. Luzhetskyi, "Ternary Bitwise Balancing Analogto-Digital Converter," 2019 IEEE 2nd Ukraine Conference on Electrical and Computer Engineering (UKRCON), Lviv, Ukraine, 2019, pp. 1-5, doi: 10.1109/UKRCON.2019.8879792. Заступник головного редактора Міжнародного науково-технічного журналу "Інформаційні технології та комп'ютерна інженерія", член редакційної колегії журналу "Вісник Вінницького політехнічного інституту", член редакційної колегії електронного наукового журналу "Наукові праці Вінницького національного технічного університету" П.10) Участь у проєкті CRDF Global (США) "Promotion of the Cyber Hygiene ELearning course in Vinnytsia National Technical University» у 2020 році як Principal Investigator Член журі Всеукраїнського конкурсу студентських наукових робіт, секція "Інформатика". Участь у громадській організації "Асоціація спеціалістів кібербезпеки".
8288	Лукічов Віталій Володимирович	Доцент, Основне місце роботи	Факультет інформаційних технологій та комп`ютерної інженерії	Диплом магістра, Вінницький національний технічний університет, рік закінчення: 2004, спеціальність: 091401 Системи управління і автоматики, Диплом кандидата наук ДК 064503, виданий	13	Кібербезпека	Науковий ступінь: кандидат технічних наук. Спеціальність: 05.13.21, тема: Методи та засоби стеганографічного захисту інформації в комп'ютерних системах і мережах на основі вейвлет-перетворень. Вчене звання: Доцент кафедри захисту інформації Підвищення кваліфікації: 1. ВНТУ, очна,

				22.12.2010, Атестат доцента АД 011523, виданий 23.12.2022			стажування, Конференція “Контроль і управління в складних системах” (КУСС–2022), 15.11-2022-17.11.2022, Сертифікат, 2022-11-17, 30 год, 1 кред. 2. ВНТУ, дистанційна, навчання за освітньою програмою професійного розвитку, Використання хмарних технологій в освітньому процесі, з 24 вересня 2020 по 28 травня 2021р, Свідоцтво про підвищення кваліфікації. Серия ПК №020706930236 - 21, 2021-09-08, 120 год, 4 кред. 3. Barkhausen Institut gGmbH, Dresden, дуальна, стажування за кордоном, Privacy of the 6G sensed data, 17.07.2023 - 16.08.2023., Certificate №1-2023-VNTU, 2023-08-27, 120 год, 4 кред. 4. Technische Universitat Dresden, Dresden, Germany., очна, стажування за кордоном, International research seminar on the topic: "Unlinkability in Automated Driving Systems" Towards improving vehicle drivers` privacy., 05.07.2022 - 16.08.2022, Затверджено Вченою радою ВНТУ протокол №2 від 29/09/2022, Certificate №1-2022-VNTU, 2022-08-31, 180 год, 6 кред. 5. CyberBionic Systematics. Information Technology Video Developer Network. Інформаційний відеосервіс для розробників програмного забезпечення. https://itvdn.com, online-курс, участь у вебінарі, «Тестування безпеки веб-застосунків», з 20 лютого 2023 по 27 лютого 2023р, Тестування: набрав 982 балів із 1000, Certificate №TP31079710, 2023-02-27, 30 год, 1 кред. 6. CyberBionic Systematics. Information Technology Video Developer Network.

							Інформаційний відеосервіс для розробників програмного забезпечення. https://itvdn.com,, online-курс, участь у вебінарі, «Python Базовий», з 10 Березня 2023 по 17 березня 2023 р, Тестування: набрав 756 балів із 1000, Certificate №TP58958640, 2023-03-17, 30 год, 1 кред. 7. Громадська організація "Наукова спільнота» та Wyższej Szkoły Społeczno-Gospodarcza w Przeworsku (Польща), дистанційна, участь у вебінарі, «ПІДХОДИ ПІДВИЩЕННЯ ІНФОРМАЦІЙНОГО ЗАХИСТУ ПЕРЕДАЧІ ДАНИХ В ІНТЕРФЕЙС-КАНАЛАХ ІНТЕРНЕТУ РЕЧЕЙ (IOT), 20-21 червня 2023 року, СЕРТИФІКАТ № ЕС-000166, 2023-06-21, 18 год, 0,6 кред. 8. Barkhausen Institut gGmbH, дуальна, стажування за кордоном, Privacy of the 6G sensed data, 01.07.2024 - 31.07.2024, Certificate №1-2024-VNTU, 2024-08-01, 180 год, 6 кред. Публікації: 1. Маліновський В. І., Куперштейн Л. М ., Лукічов В. В. Математична модель оцінки кіберзагроз та інформаційних впливів у мікроконтролерах. Інформаційні технології та комп'ютерна інженерія, №. 59(1), 2024, с. 69-82, 2. Маліновський В. І.,Куперштейн Л. М., Лукічов В. В., Дудатьєв А. В. Проблематика і підходи підвищення рівня захисту в каналах передачі даних систем і пристроїв Інтернету речей/ В. І. Маліновський, Л. М. Куперштейн, В. В. Лукічов, А. В. Дудатьєв // Наукові праці ВНТУ. – 2024 – № 4. – С.105-115 3. Zolotavkin, Y., Baryshev, Y., Lukichov, V., Mähn, J. and Köpsell, S. (2023). Improving

							Unlinkability in C-ITS: A Methodology For Optimal Obfuscation. In Proceedings of the 9th International Conference on Information Systems Security and Privacy - ICISSP, ISBN 978-989-758-624-8, ISSN 2184-4356, pages 677-685. DOI: 10.5220/0011786900003405 4. Метод адаптивного багатошарового захисту інформації на основі стеганографії та криптографії [Текст] / В. В. Лукічов, Ю. В. Баришев, Н. Р. Кондратенко, В. І. Маліновський // Інформаційні технології та комп`ютерна інженерія. – 2023. – № 3. – С. 4-11. 5. T. Martyniuk, B. Krukivskyi, L. Kupershtein, V. Lukichov. Neural network model of heteroassociative memory for the classification task. Radioelectronic and Computer Systems. 2022. NO. 2(102). pp.108-117. DOI: 10.32620/reks.2022.2.09. ISSN 1814-4225. 6. Malinovskyi V. Cybersecurityand Data Stability Analysis of IoT Devices [Text] / V. Malinovskyi, L. Kupershtein, V. Lukichov // IEEE International Scientific-Practical Conference «Problems of Infocommunications. Science and Technology (PIC S and T 2022)» - 2022. – Pp. 259-264. Міжнародні проєкти: 1. International research seminar on the topic: "Unlinkability in Automated Driving Systems" Towards improving vehicle drivers' privacy. Technische Universitat Dresden, Dresden, Germany. Period: 05.07.2022 - 16.08.2022. Certificate №1-2022-VNTU. Затверджено Вченою радою ВНТУ протокол №2 від 29/09/2022. 2. International research activities related to the following topic: "Privacy of the 6G sensed data", проєкт «KOMSENS-6G» Barkhausen Institut gGmbH, Dresden, Period:

							17.07.2023 - 16.08.2023, Certificate №1-2023-VNTU, 2023-08-27. Затверджено Вченою радою ВНТУ протокол №3 від 28/09/2023. 3. International research activities related to the following topic: "Privacy of the 6G sensed data", проєкт «Горизонт Європа Неха-Х-ІІ» Barkhausen Institut gGmbH, Dresden, Period: 01.07.2024 - 31.07.2024, Certificate №1-2024-VNTU, 2024-08-01. Затверджено Вченою радою ВНТУ протокол №1 від 28/08/2024. Професійний досвід: Повноправний асоційований член ГО "Наукова асоціація кібербезпеки України" сертифікат № АМ055 від 26/04/2023, https://scsa.org.ua/ ФОП з 14.01.2003 по теперішній час. Види діяльності: 62.01 - Комп'ютерне програмування; 62.02 - Консультування з питань інформатизації.
278146	Баришев Юрій Володимирович	Доцент, Основне місце роботи	Факультет інформаційних технологій та комп`ютерної інженерії	Диплом магістра, Вінницький національний технічний університет, рік закінчення: 2008, спеціальність: Захист інформації в комп'ютерних системах та мережах, Диплом кандидата наук ДК 006705, виданий 17.05.2012, Атестат доцента АД 011522, виданий 23.12.2022	14	Кібербезпека об'єктів критичної інфраструктури	Освіта: 2008 р. Вінницький національний технічний університет, диплом магістра, спеціальність - Захист інформації в комп'ютерних системах та мережах, кваліфікація - магістр з інформаційної безпеки Науковий ступінь: кандидат технічних наук, 05.13.05 - Комп'ютерні системи та компоненти, тема дисертації «Методи та засоби швидкого багатоканального хешування даних в комп'ютерних системах» Вчене звання: Доцент кафедри захисту інформації Підвищення кваліфікації: 1. CRDF Global (USA), стажування за кордоном, Розробка та інтеграція ІТ курсу з елементами кібербезпеки в навчальний план українських університетів, з 26.01.2021 р. по 10.12.2021 р., Сертифікат CRDF Global, 2021-12-10, 180

							год, 6 кред. 2. London King`s College (UK), The Middlebury Institute of International Studies at Monterey (USA), CRDF Global (USA), дистанційна, стажування за кордоном, Управління передачею конфіденційних технологій за межі науково-дослідних організацій, з .11.11.2021 р. по 30.11.2021 р., Сертифікат про проходження курсу, 2021-11-30, 60 год, 2 кред. 3. EPAM Systems, очна, стажування, IT Ukraine Association Teacher`s Internship program, January-February 2020, Certificate 0192, 2020-03-18, 108 год, 3,5 кред. 4. Barkhausen Institute Technische Universitat Dresden, дистанційна, стажування за кордоном, Unlinkability in Automated Driving Systems: Towards improving vehicle drivers` privacy, 05.07.2022-16.08.2022, №2-2022-VNTU, 2022-08-31, 195 год, 6,5 кред. 5. Distributed Lab, online-курс, навчання за освітньою програмою професійного розвитку, Cryptography, з 26.04.2023 р по 23.07.2023, Ідентифікатор сертифікату 3bbe71f7416742c11089, 2023-07-25, 45 год, 1,5 кред. 6. Google, online-курс, навчання за освітньою програмою професійного розвитку, Play It Safe: Manage Security Risks, з 16.06.2023 р. по 16.07.2023, Сертифікат Q3H9JJLHLY49, 2023-07-16, 15 год, 0,5 кред. 7. Google, online-курс, навчання за освітньою програмою професійного розвитку, Foundations of Cybersecurity, з 30.05.2023 р по 14.06.2023, Сертифікат ZREM5C4VSZXK, 2023-06-14, 15 год, 0,5 кред.

							8. Barkhausen institut, дистанційна, стажування за кордоном, Secure processors development for critical infrastructure, з 03.06.2024 р. по 03.07.2024 р., №2-2024-VNTU, 2024-08-14, 120 год, 4 кред. Публікації: 1. Y. Zolotavkin, Y. Baryshev, V. Lukichov, J. Mähn and S. Köpsel. Improving Unlinkability in C-ITS: A Methodology For Optimal Obfuscation. In Proceedings of the 9th International Conference on Information Systems Security and Privacy (2023)- ICISSP-2023, ISBN 978-989-758-624-8, ISSN 2184-4356, pages 677-685. URL:https://www.scitepress.org/Link.aspx?doi=10.5220/0011786900003405. 2. Баришев Ю. В., Кондратенко Н. Р. , Казміревський В. В., Кирилащук Т. Г. Нечіткі множини типу-2 в задачах моделювання та оцінювання станів критичних систем з недовизначеними вхідними даними та використанням експертів. Інформаційні технології та комп`ютерна інженерія. №2 (Т. 57). 2023. С. 13-24 3. Баришев Ю. В. Метод захищеного зберігання медичних даних на основі реляційної бази даних та блокчейну [Електронний ресурс] / Ю. В. Баришев, В. С. Ланова // Наукові праці ВНТУ. – 2023. – № 3. – Режим доступу: https://praci.vntu.edu.ua/index.php/praci/article/view/701. 4. Метод адаптивного багатошарового захисту інформації на основі стеганографії та криптографії [Текст] / В. В. Лукічов, Ю. В. Баришев, Н. Р. Кондратенко, В. І. Маліновський // Інформаційні технології та комп`ютерна інженерія. – 2023. – № 3. – С. 4-11. 5. Баришев Ю. В. Метод та засіб

							підвищення стійкості зрозумілих користувачам текстових паролів [Електронний ресурс] / Ю. В. Баришев, М. М. Чайкін, О. В. Кохан // Наукові праці ВНТУ. – 2022. – № 2. – Режим доступу: https://praci.vntu.edu.ua/index.php/praci/article/view/655. 6. Kushch, S., Baryshev, Y., Ranise, S. Blockchain Tree as Solution for Distributed Storage of Personal ID Data and Document Access Control. Sensors 2020, 20, 3621. https://doi.org/10.3390/s20133621 Науковий керівник НДР №0120U103549 "ІДЕНТИФІКАЦІЯ МОДЕЛЕЙ ОБРОБЛЕННЯ ТРАНЗАКЦІЙ ПРИ ГЕНЕРУВАННІ НОВИХ БЛОКІВ В ТЕХНОЛОГІЯХ РОЗПОДІЛЕНОГО РЕЄСТРУ НА ПРИКЛАДІ БЛОКЧЕЙНУ BITCOIN", 2020 рік Рецензент видань Sensors, Electronics, Applied Sciences, Software що входить до переліку наукометричних баз Участь у проекті CRDF Global (США), "Finalization of IT Audit Course and Integration into Curriculum of VNTU, Ukraine" як Principal Investigator №CYB0-20-66626-0 від 29.05.2020 Участь у проекті CRDF Global (США) щодо розробки курсів з кібербезпеки у ВНЗ України у 2021 році як ментор
203451	Куперштейн Леонід Михайлович	Доцент, Основне місце роботи	Факультет інформаційних технологій та комп`ютерної інженерії	Диплом спеціаліста, Вінницький державний технічний університет, рік закінчення: 2003, спеціальність: 0911 Лазерна та оптоелектронна техніка, Диплом кандидата наук ДК 042300, виданий 20.09.2007, Атестат доцента 12ДЦ 024388,	18	Проектування систем кібербезпеки (в т.ч. курсова робота)	Науковий ступінь: кандидат технічних наук, спеціальність: 05.13.05, тема: Методи та засоби нейроподібної обробки даних для систем керування. Підвищення кваліфікації: 1. Distributed Lab, online-курс, участь у практикумі, Cryprography, 15.05.23-15.07.23, 713f468de7c2bda27382, 2023-08-10, 45 год, 1.5 кред. 2. SoftServ Academy, online-курс, стажування, TECH

				виданий 14.04.2011			SUMMER BOOTCAMP FOR TEACHERS, 27.07.23 - 1.09.23, Series DY № 14205/2023, 2023-09-01, 10 год, 0.3 кред. 3. DataWorkshop, дистанційна, участь у практикумі, Machine Learning in e-commerce, 02.05.23, certificate ID: a9f7705/dwthon, 2023-05-02, 15 год, 0.5 кред. 4. ITVDN, online-курс, участь у практикумі, Web Application Security Testing, 21.03.23 - 28.03.23, ID: TP88455581, 2023-03-28, 15 год, 0.5 кред. 5. Sigma Software University, дистанційна, участь у семінарі, SSWU TCHR001: TEACHERS` SMARTUP: SUMMER EDITION, 1.08.22-5.08.22, Certificate ID Number: 25fa7f835c0a4a82b88764eeb8b5fe92, 2022-08-09, 30 год, 1 кред. 6. Асоціація "IT Ukraine" / Epam Systems, дистанційна, стажування, "Розуміння сучасної IT-галузі". Модуль 1. Проектний менеджмент, Модуль 2. Загальні технології, Модуль 3. Спеціальні технології, Модуль 4. Софт скіли, липень 2020 - серпень 2020, Сертифікат №297, 2020-08-31, 108 год, 3,6 кред. 7. Deeplearning.ai / Coursera, online-курс, участь у тренінгу, Neural Networks and Deep Learning, 01.05.2020 - 01.06.2020, Сертифікат coursera.org/verify/KRXCHJLK5ZUY, 2020-06-02, 30 год, 1 кред. 8. EIT Digital / Coursera, online-курс, участь у тренінгу, Security and Privacy for Big Data, 14 серпня 2020, Сертифікат coursera.org/verify/SZVXFH FFVXTR, 2020-08-14, 4 год, 0,13 кред. 9. University of Michigan / Coursera, online-курс, участь у тренінгу, Introduction to Data Science in Python, з 01.07.2020 по 28.07.2020, Сертифікат coursera.org/verify/DSG8QUVP5X5J, 2020-07-28, 30 год, 1 кред.

							10. CRDFGlobal, online-курс, участь у тренінгу, Базові правила інформаційної безпеки, з 29.05.2020 по 29.05.2020, Сертифікат, 2020-05-29, 5 год, 0,17 кред. 11. Prometeus, online-курс, участь у тренінгу, Машинне навчання, 1.03.2020 - 29.03.2020, Сертифікат https://courses.prometheus.org.ua:18090/cert/35cd5453f4ff45fb8df7f2084b662c4a, 2020-03-29, 30 год, 1 кред. 12. datacamp, online-курс, участь у тренінгу, Supervised Learning with scikit-learn, з 29.04.2021 по 30.04.2021, Сертифікат 15,674,792, 2021-04-30, 6 год, 0,2 кред. 13. datacamp, online-курс, участь у тренінгу, Intermediate SQL Server, з 07.09.2020 по 07.09.2020, Сертифікат 15678288, 2020-09-07, 6 год, 0,2 кред. 14. DeepLearning.AI, online-курс, участь у тренінгу, Sequences, Time Series and Prediction, з 1.05.2021 по 15.06.2021, Сертифікат coursera.org/verify/V4WDDRYGY3QZ, 2021-06-15, 24 год, 0,8 кред. 15. DataWorkshop, мережева, участь у практикумі, Car Price Prediction, з 25.09.2021 по 27.09.2021, certificate ID: a9f7705/dwthon2, 2021-09-27, 15 год, 0,5 кред. 16. DataWorkshop, дистанційна, участь у практикумі, Taiwanese Bankruptcy Prediction, 26.11.2021-27.11.2021, certificate ID: a9f7705/taiwan, 2021-11-27, 15 год, 0,5 кред. 17. DeepLearning.AI, online-курс, участь у тренінгу, Improving Deep Neural Networks: Hyperparameter Tuning, Regularization and Optimization, 2.01.2022-19.01.2022, Verif y at coursera.org/verify/H2GEEDFA94GZ, 2022-01-19, 30 год, 1 кред. 18. Асоціація "IT Ukraine" / Epam Systems, дистанційна, стажування, Модуль 1.

							Проектний менеджмент, Модуль 2. Загальні технології, Модуль 3. Спеціальні технології, серпень 2022 - вересень 2022, Сертифікат №946, 2022-09-12, 180 год, 6 кред. 19. DeepLearning.AI, online-курс, участь у практикумі, TensorFlow Developer, 5.05.23 - 05.09.23, Verify at: https://coursera.org/verify/profession al-cert/85GDAKH5H84L, 2023-09-05, 120 год, 4 кред. 20. Дія.Освіта (Міністерство цифрової транформації України), online-курс, участь у практикумі, ChatGPT для підвищення власної ефективності, 28.09.2023, Сертифікат №T0052853640, 2023-09-28, 3 год, 0,1 кред. Публікації: 1. Маліновський В. І., Куперштейн Л. М ., Лукічов В. В. Математична модель оцінки кіберзагроз та інформаційних впливів у мікроконтролерах. Інформаційні технології та комп'ютерна інженерія. 2024. №. 59. С. 69-82. 2. Л. М. Куперштейн, А. В. Притула, В. І. Маліновський, «АНАЛІЗ ТЕХНОЛОГІЙ ТЕСТУВАННЯ НА ПРОНИКНЕННЯ WEB-ДОДАТКІВ», НаукПраці ВНТУ, вип. 2, Чер 2024. 3. М. Д. Кренцін, Л. М. Куперштейн, «ГІБРИДНА БАГАТОФАКТОРНА АВТЕНТИФІКАЦІЯ ВУЗЛІВ ПІРИНГОВОЇ МЕРЕЖІ», НаукПраці ВНТУ, вип. 2, Чер 2024. 4. Куперштейн Л.М., Луцишин Г.Л., Кренцін М.Д. ІНФОРМАЦІЙНА ТЕХНОЛОГІЯ МОНІТОРИНГУ БЕЗПЕКИ ДАНИХ ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ. Кібербезпека: освіта, наука, техніка. №3. 2024 5. Дудатьєв А. В. Інформаційне

							протиборство: моделі реалізації та оцінювання інформаційних операцій [Електронний ресурс] / А. В. Дудатьєв, Л. М. Куперштейн, О. П. Войтович // Кібербезпека: освіта, наука, техніка. – 2023. – № 4(20). – С. 72–80. Режим доступу: https://csecurity.kubg.edu.ua/index.php/journal/article/view/468. 6. Куперштейн Л. М. Модель політики інформаційної безпеки для об'єктів критичної інфраструктури [Текст] / Л. М. Куперштейн, А. В. Дудатьєв, О. П. Войтович, Я. О. Ясінська // Вимірювальна та обчислювальна техніка в технологічних процесах. – 2021. – № 2. – С. 30-38. 7. Інформаційна технологія прогнозування курсу криптовалют на основі комплексної інженерії ознак [Текст] / В. Б. Мокін, С. О. Жуков, Л. М. Куперштейн, О. В. Слободянюк // Вісник ВПІ. – 2022. – № 2. – С. 81-93. 8. Аналіз проблем безпеки пірингових мереж [Текст] / Л. М. Куперштейн, М. Д., А. В. Дудатьєв, В. А. Каплун // Інформаційні технології та комп'ютерна інженерія. – 2022. – № 2. – С. 5-13. 9. Маліновський В. І. Аналіз загроз безпеки мікроконтролерів [Текст] / В. І. Маліновський, Л. М. Куперштейн // Інформаційні технології та комп`ютерна інженерія. – 2022. – № 3. – С. 21-32. 10. Маліновський В. І. Аналіз основних інформаційних загроз і впливів у сучасних мікроконтролерних системах (аналітичний огляд) [Текст] / В. І. Маліновський, Л. М. Куперштейн, В. А. Каплун // Оптико-електронні інформаційно-енергетичні

							технології. – 2022. – № 2. – С. 100-113. 11. Voitovych, O. Detection of Fake Accounts in Social Media [Електронний ресурс] / O. Voitovuch, L. Kupershtein, V. Holoenko // Кібербезпека: освіта, наука, техніка. – 2022. – Том 2, № 18. – С. 86-98. Режим доступу: https://csecurity.kubg.edu.ua/index.php/journal/article/view/406. 12. Malinovskyi V. Cybersecurityand Data Stability Analysis of IoT Devices [Text] / V. Malinovskyi, L. Kupershtein, V. Lukichov // IEEE International Scientific-Practical Conference «Problems of Infocommunications. Science and Technology (PIC S and T 2022)» - 2022. – Pp. 259-264. 13. Мартинюк Т.Б., Куперштейн Л.М., Кренцін М.Д. Особливості процесу класифікації об`єктів на базі дискримінантних функцій //Математичні машини і системи. - №3. - 2021. - С. 81-87. URL: http://www.immsp.kiev.ua/publications/articles/2021/2021_3/03_21_Martyniuk.pdf 14. Куперштейн Л.М., Кренцін М.Д. Аналіз тенденцій розвитку піринговых мереж // Вісник Хмельницького національного університету. – №4. – 2021. – С.25-29 URL: http://journals.khnu.km.ua/vestnik/wp-content/uploads/2021/11/299-text_2021_4_t.pdf 15. Remote Host Operation System Type Detection Based on Machine Learning Approach [Text] / L. Kupershtein, T. Martyniuk, O. Voitovych, A. Borusevych // Selected Papers of the II International Scientific Symposium "Intelligent Solutions" (IntSol-2021). Workshop Proceedings, September 28-30, 2021, Kyiv - Uzhhorod. – 2021. № 3106. – P. 65–81. Рецензент іноземного наукового видання "Asian Journal of

							Research in Computer Science" Керівник науково-практичного гуртка "IT-Club "CyberSecPals" Член громадської організації "Асоціація спеціалістів з кібербезпеки" (Довідка № АСКБ/27 від 27 квітня 2023 р.)
147768	Хома Олег Ігорович	Завідувач кафедри, професор, Основне місце роботи	Факультет електроенергетики та електромеханіки	Диплом спеціаліста, Київський ордена Леніна і ордена Жовтневої революції державний університет імені Т.Г. Шевченка, рік закінчення: 1990, спеціальність: 2011 філософія, Диплом доктора наук ДД 001209, виданий 12.04.2000, Атестат професора ПР 002275, виданий 19.06.2003	33	Філософія науки і техніки	Освіта: Київський державний університет ім. Т. Г. Шевченка (1990 рік), спеціальність: «Філософія». Кваліфікація «Філософ. Викладач філософії». Доктор філософських наук, спеціальність 09.00.04 – «Філософська антропологія, філософія культури»; тема докторської дисертації: «Модерна та постмодерна перспективи у філософії культури». Завідувач кафедри філософії та гуманітарних наук, професор. Підвищення кваліфікації: Науково-видавниче об'єднання «Дух і Літера», м. Київ, стажування. Ознайомлення зі сучасними практиками наукової експертизи перекладних текстів. Неперекладність у викладанні філософії. Філософсько-термінологічні аспекти сучасного філософського тексту. З 27.06.2020 по 27.01.2021 р. Посвідчення № 2021/1.1, 210 год, 7 кред. Показники наукової та професійної активності (1,3,7,8,9,10,12,13,14,19). 1. Хома О. І. Скептичні вислови в «Нарисах піронізму» і Декартів проєкт «Медитацій про першу філософію» [Текст] / О. І. Хома // Sententiae. – 2022. – № 2. – С. 24-65. 2. Хома О. І. Концептуалізація усної історії філософії: проблема інтерв`ю [Текст] / О. І. Хома // Sententiae. – 2023. – № 1. – С. 69-82. 3. Хома, О. (2021). “Аристократична метафізика” і

							стереотипи. Jolibert, B. (2020). Descartes en questions: l`urgence d`un retour aux textes. Paris: L`Hrarmattan. Sententiae, 40(2), 111–114. https://doi.org/10.31649/sent40.02.111 4. Хома, О. (2020). Коментар до українського перекладу «Нарисів піронізму» Секста Емпірика (I, 1-13). Sententiae, 39(2), 170–172. https://doi.org/10.31649/sent39.02.170 5. Хома, О. (2020). Спіноза у фокусі національних традицій. Stetter, J., & Ramond, C. (Eds.). (2019). Spinoza in 21st-century American and French philosophy: metaphysics, philosophy of mind, moral and political philosophy. London: Bloomsbury Academic. Sententiae, 39(2), 207–209. https://doi.org/10.31649/sent39.02.207 6. Хома О. Чого шукає історик філософії? Marion, J.-L. (2021). Questions cartésiennes III: Descartes sous le masque du cartésianisme. Paris: PUF. [Текст] / О. Хома // Sententiae. – 2022. – № 1. – С. 130-140. Головний редактор фахового видання SENTENTIAE, включеного в міжнародної бібліометричної бази SCOPUS. Член редколегії фахового видання «Філософська думка» Голова Вінницького відділення Українського філософського фонду (з 1997 року посьогодні); Голова Спілки дослідників модерної філософії (Паскалівського товариства) з 1999 року посьогодні.
155976	Залюбівська Оксана Броніславівна	Доцент, Основне місце роботи	Факультет електроенергетики та електромеханіки	Диплом спеціаліста, Вінницький державний педагогічний інститут, рік закінчення: 1992, спеціальність: Російська мова та література, Диплом	31	Інноваційні та психологічні аспекти сучасної освіти	Освіта: Кандидат педагогічних наук, спеціальність: 13.00.04 «Теорія і методика професійної освіти» Тема дисертації: «Формування риторичної культури майбутніх викладачів технічних університетів у

				кандидата наук ДК 032916, виданий 15.12.2015			процесі магістерської підготовки»; доцент кафедри філософії та гуманітарних наук Підвищення кваліфікації: 1. ВГО «Інноваційний університет»; Міжнародний фонд досліджень освітньої політики, очна, навчання за освітньою програмою професійного розвитку, Кращі практики організації міждисциплінарних та міжгалузевих освітніх і освітньо–наукових програм в Україні, з 7.07.2021 по 2.12.2021, Міжуніверситетський науковий захід «Дискусійна платформа з міждисциплінарного діалогу» (онлайн, 23.11.2021). Організація, проведення, виступ з доповіддю, Сертифікат № 1094, 2021-12-04, 180 год, 6 кред. 2. Фонд Конрада Аденауера в Україні, Академія Української преси, Київ, дистанційна, участь у тренінгу, Ігри експертів: мистецтво маніпуляції Модуль 2. Верифікація: як переконатися в експертності за допомогою відкритих джерел, 20-21 жовтня 2020 рік, Сертифікат № AUP-197-OCT-20, 2020-10-21, 9 год, 0,2 кред. 3. Фонд Конрада Аденауера в Україні, Академія Української преси, Київ, очна, стажування, Ігри експертів: мистецтво маніпуляції Модуль 3. Ток-шоу: як визначити прийоми та техніки маніпуляції, 26-27 жовтня 2020 рік, Сертифікат № AUP-269-OCT-20, 2020-10-27, 9 год, 0,3 кред. 4. Фонд Конрада Аденауера в Україні, Академія Української преси, Київ,, дистанційна, стажування, Ігри експертів: мистецтво маніпуляції. Модуль 1. Вплив: як формують суспільні наративи, створюють інформаційні міфи та поширюють стереотипи», 15-16

							жовтня 2020 р., сертифікат № AUP-168-ОСТ-20, 2020-10-16, 9 год, 0,3 кред. 5. Академія української преси, Київ, online-курс, участь у тренінгу, Онлайн-школа «Digital-teacher: онлайн-інструменти у навчанні медіаграмотності», 28-30 вересня, 2020 р, Сертифікат № AUP-92-SEP-20, 2020-09-30, 15 год, 0,5 кред. 6. Академія української преси у партнерстві з Центром медіа- та цифрової грамотності Інституту медіа- та комунікаційних студій Вільного університету Берліна (Німеччина). Київ., очна, участь у тренінгу, Протидія дезінформації в контексті російсько-української війни, з 12.09.2023 по 14.09.2023, форма звітності: проведення тренінгів для здобувачів вищої освіти, Сертифікат № AUP-SEP-23/3129, 2023-09-14, 30 год, 1 кред. Публікації: 1. Прищак М. Д., Гречановська О. В., Залюбівська О. Б. Життєстійкість особистості: пошук системоутворювального поняття. Наукові перспективи : журнал. 2024. № 3(45). С. 1271–1282. 2. Залюбівська О. Б., Слободянюк О. М. Положення про академічну доброчесність: проблеми імплементації. Наукові записки Бердянського державного педагогічного університету. Серія: Педагогічні науки. Випуск 1, 2023. С 30-42. 3. Залюбівська О.Б. Розробка та впровадження програми курсу за вибором «Медіаграмотність та критичне мислення» на засадах міждисциплінарного (медіаріторичного) підходу. Інноваційний університет і лідерство: проєкт і мікропроєкти – V. / відпов. ред.: Т.

							Фініков, Р. Сухарскі. Варшава: Fundacja «Instytut Artes Liberales», Wydawnictwa Uniwersytetu Warszawskiego, 2021. С.471–485. Прищак, М. Д. Педагогіка, психологія та методика викладання у вищій школі : навчальний посібник / М. Д. Прищак, О.Б. Залюбівська. – Вінниця : ВНТУ, 2020. – 160 с. Членство у Всеукраїнському громадському об'єднанні "Інноваційний університет". До прикладів діяльності за спеціальністю в межах НГО: учасниця Літньої школи «Кращі практики організації міждисциплінарних та міжгалузевих освітніх і освітньо-наукових програм в Україні» (2021, Одеса); співорганізаторка «Дискусійної онлайн платформи з міждисциплінарного діалогу» (2021).
192237	Войтович Олеся Петрівна	Доцент, Основне місце роботи	Факультет інформаційних технологій та комп`ютерної інженерії	Диплом магістра, Вінницький державний технічний університет, рік закінчення: 2002, спеціальність: 091401 Системи управління і автоматики, Диплом кандидата наук ДК 035269, виданий 08.06.2006, Атестат доцента 12ДЦ 026223, виданий 20.01.2011	20	Моніторинг та аудит кібербезпеки	Науковий ступінь: кандидат технічних наук. спеціальність: 05.11.16 тема: Інформаційно-вимірювальна система діагностування безконтактних електромеханічних перетворювачів на основі нейронечітких алгоритмів. Вчене звання: Доцент кафедри захисту інформації. Підвищення кваліфікації: 1. IT Ukraine Association, дистанційна, навчання за освітньою програмою професійного розвитку, Teacher`s Internships program held by EPAM System, June-August 2020, Certificate №261, 2020-08-28, 108 год, 3,5 кред. 2. American Councils спільно з МОНУ, НАЗЯВО, ICAI, дистанційна, участь у тренінгу, Академічна доброчесність у системі внутрішнього забезпечення якості освіти, 23-27 листопада 2020,

							Сертифікат AcademicIQ, 2020-11-27, 15 год, 0,5 кред. 3. American Councils спільно з МОНУ, НАЗЯВО, ICAI, дистанційна, участь у тренінгу, Робота з даними та напрацювання стратегій для посилення академічної доброчесності та якості, 6-14 квітня 2021, Сертифікат AcademicIQ, 2021-04-14, 15 год, 0,5 кред. 4. ДП Вінницький науково-виробничий центр стандартизації, метрології та сертифікації, дистанційна, стажування, Впровадження систем управління якістю по ДСТУ EN ISO 9001:2018 Системи управління якістю. Вимоги (EN ISO 9001:2015, IDT, ISO 9001:2015, IDT) із застосуванням концепції сталого успіху організації по ДСТУ ISO 9004:2018 Управління якістю. Якість організації. Настанови щодо досягнення сталого успіху (ISO 9004:2018, IDT), з 12.07.2021 по 27.08.2021, Посвідчення № 741/002, 2021-09-28, 60 год, 2 кред. 5. King`s College London, CRDFGlobal, Department of State USA, Middlebury Institute of International Studies at Monterey (USA), дистанційна, участь у вебінарі, Управління передачею конфіденційних технологій за межі науково-дослідних організацій, 16-17 листопада 2021, Сертифікат, 2021-11-17, 8 год, 0.25 кред. 6. МОН України, Науково-методичний центр вищої та фахової передвищої освіти, дистанційна, навчання за освітньою програмою професійного розвитку, Основи тестології та розробки тестових завдань. Розробка та експертиза завдань ЄДКІ за спеціальністю 125 Кібербезпека, грудень 2022 - березень 2023,

							Сертифікат про підвищення кваліфікації (ліцензія Наказ МОНУ від 15.09.2021 №171-л), 2023-04-17, 30 год, 1 кред. 7. American Councils спільно з МОНУ, НАЗЯВО, ICAI, дистанційна, участь у тренінгу, Інтерпретація даних для якісних змін, 10, 15, 18 та 19 листопада, Сертифікат, 2021-11-19, 12 год, 0,4 кред. 8. Cybersecurity East Project, funded by the EU (https://eufordigital.eu/discover-eu/eu4digital-improving-cyber-resilience-in-the-eastern-partnership-countries/), дистанційна, участь у тренінгу, Cybersecurity Training Marathon, 12-20.07.2022, Certificate of attendance, 2022-08-29, 18 год, 0,5 кред. 9. Akademia Techniczno-Humanistyczna Bielsko-Biała, дистанційна, стажування за кордоном, Non-Functional Security Requirements in Software Development, Data protection and security in the digital workplace, Best practices for secure SDLC, з 10.12.22 по 05.03.2023, Сертифікат, 2023-03-06, 30 год, 1 кред. 10. Ukraine Global Faculty, дистанційна, участь у вебінарі, Introduction to the US System of Intellectual Property, 10.08.2023, Certificate of attendance 64d519846984cdf75104bofe, 2023-08-10, 1,5 год, 0,05 кред. 11. SoftServe Academy, дистанційна, навчання за освітньою програмою професійного розвитку, Tech Summer Bootcamp for Teachers, з 26.07.2023 по 01.09.2023, Certificate Series GV № 13831/2023, 2023-09-01, 10 год, 0,3 кред. 12. Національне агентство із забезпечення якості освіти, дистанційна, участь у тренінгу, Тренінг для експертів із написання звіту про

							результати акредитаційної експертизи, 27.12.2023, Сертифікат №684/2023(282), 2023-12-27, 30 год, 1 кред. 13. Офіс доброчесності НАЗК, Prometeus, online-курс, участь у вебінарі, Зрозуміло про конфлікт інтересів, 04.07.2024, Сертифікат: https://certs.prometheus.org.ua/cert/b8b364d2e0bf4704b8fed290f3c24b6e, 2024-07-04, 6 год, 0,2 кред. 14. Prometeus, online-курс, участь у семінарі, Безпека в інтернеті під час війни: практичний курс, 29.07.2024, Свідоцтво про підвищення кваліфікації: https://certs.prometheus.org.ua/cert/0644fbd9ef584894b536178178db939e, 2024-07-29, 15 год, 0.5 кред. 15. Prometeus, online-курс, участь у семінарі, Інформаційна гігієна під час війни, 24.07.2024, Сертифікат: https://certs.prometheus.org.ua/cert/a038fb2ae36e43779e61e1976183b7f1, 2024-07-24, 15 год, 0,5 кред. 16. ТОВ Каскад-БЕЗПЕКА, очна, стажування, Аудит інформаційної безпеки, 03.06.2024-02.08.2024, Довідка від 02 серпня 2024 № 02-08/24, 2024-08-02, 120 год, 4 кред. 17. SoftServe Academy, дистанційна, навчання за освітньою програмою професійного розвитку, Tech Summer for Educators: AI Edition, 23 липня 2024 – 13 серпня 2024, Сертифікат Серія ВО № 20786/2024, 2024-08-13, 30 год, 1 кред. Публікації: 1. Дудатьєв А. В. Інформаційне протиборство: моделі реалізації та оцінювання інформаційних операцій [Електронний ресурс] / А. В. Дудатьєв, Л. М. Куперштейн, О. П. Войтович // Кібербезпека: освіта, наука, техніка. – 2023. – № 4(20). – С. 72–80. Режим доступу:

							https://csecurity.kubg.edu.ua/index.php/journal/article/view/468. 2. Optical image processing technologies using generalized connectivity W-spectrum / Leonid Tymchenko, Natalia Kokriatska, Olesia Voitovych, ..., Saule Kumargazhanova // Proceedings of the SPIE, Volume 12985, id. 1298503 6 pp. (2023). https://doi.org/10.1117/12.3022277 3. Information System for the Fact-checker Support. Baryshev, Y. , Kupershtein, L. , Maidanovych, V. , Voitovych, O. , Prokopenko, S. / CEUR Workshop Proceedings, 2023, 3646, pp. 127–138 4. Куперштейн Л. М. Модель політики інформаційної безпеки для об`єктів критичної інфраструктури [Текст] / Л. М. Куперштейн, А. В. Дудатьєв, О. П. Войтович, Я. О. Ясінська // Вимірювальна та обчислювальна техніка в технологічних процесах. – 2021. – № 2. – С. 30-38. 5. Voitovych, O. Detection of Fake Accounts in Social Media [Електронний ресурс] / O. Voitovuch, L. Kupershtein, V. Holoenko // Кібербезпека: освіта, наука, техніка. – 2022. – Том 2, № 18. – С. 86-98. Режим доступу: https://csecurity.kubg.edu.ua/index.php/journal/article/view/406. 6. 3-D modeling capabilities for planning rhinologic surgical interventions CT-datasets [Electronic resource] / O. Avrunin, Y. Nosova, N. Shushliapina [et al.] // Proc. SPIE. Photonics Applications in Astronomy, Communications, Industry, and High Energy Physics Experiments, 12 December 2022. – Lublin, Poland, 2022. – Vol. 12476, 1247609. – Access mode: https://doi.org/10.1117/12.2659480. O. Avrunin, Y. Nosova, N.

							Shushliapina, I. Younouss Abdelhamid, O. Voitovych, A. Kalizhanova, A. Uvaysova, Z. Omiotek. 3-D modeling capabilities for planning rhinologic surgical interventions CT-datasets. Proc. SPIE. Photonics Applications in Astronomy, Communications, Industry, and High Energy Physics Experiments, 12 December 2022. Lublin, Poland, 2022. Vol. 12476, 1247609. URL: https://doi.org/10.1117/12.2659480. 7. Remote Host Operation System Type Detection Based on Machine Learning Approach [Text] / L. Kupershtein, T. Martyniuk, O. Voitovych, A. Borusevych // Selected Papers of the II International Scientific Symposium "Intelligent Solutions" (IntSol-2021). Workshop Proceedings, September 28-30, 2021, Kyiv - Uzhhorod. – 2021. № 3106. – P. 65–81. 8. Дудатьєв А. В. Інформаційно-аналітичні центри в управлінні інформаційною безпекою держави [Текст] / А. В. Дудатьєв, О. П. Войтович, В. В. Миронюк // Вісник Хмельницького національного університету. – 2020. – № 1 (281). – С. 105-109. Експерт Національного агентства із забезпечення якості вищої освіти зі спеціальностей 123, 125 1) Участь у проєкті «Ініціатива академічної доброчесності та якості освіти» (Academic Integrity and Quality Initiative, далі – проєкт Academic IQ), ініційованого Американською Радою з міжнародної освіти у співпраці із Міністерством освіти і науки України, Національним агентством із забезпечення якості вищої освіти та за

							підтримки Посольства США в Україні 2020-2022 рр. 2) Участь у програмі "Finalization of IT Audit Course and Integration into Curriculum of VNTU, Ukraine" від CRDF Global (Фонд цивільних досліджень та розвитку США), 2020 рік Участь у громадській організації "Асоціація спеціалістів кібербезпеки" з 5 січня 2022 р.(Довідка №АСКБ/27 від 27.04.2023) Участь у громадській організації "Міжнародна асоціація технологічного розвитку та інновацій" (International Association for Technological Development and Innovations - IATDI). № 0320 від 11.05.2022.

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
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.	☒	Проектування систем кібербезпеки (в т.ч. курсова робота)	При вивченні дисципліни використовуються: Дидактичні методи - лекції з використанням мультимедійних презентацій. Практичні методи: лабораторні та практичні роботи з використанням прикладного програмного забезпечення. Метод самостійного навчання. Активні методи: експрес опитування, тестування. Словесні методи навчання: лекції, консультації. Виконання індивідуального завдання у формі курсової роботи.	Поточний контроль: у формі фронтального, індивідуального чи комбінованого контролю знань здобувачів вищої освіти під час лекційного та лабораторного заняття, тестування, колоквіумів. Підсумковий контроль: іспит. Оцінювання курсових робіт проводиться у формі їх публічного захисту на відкритому засіданні комісії за участю керівника курсової роботи та ще не менше одного викладача кафедри.
		Методологія та організація наукових досліджень в кібербезпеці	Лекція, проблемна лекція, дискусія, ІТ-методи, командна робота, демонстрація, зокрема, з використанням мультимедійних засобів	Поточний контроль: у формі фронтального, індивідуального чи комбінованого контролю знань студентів під час практичного заняття,

			навчання, Internet-ресурсів, інформаційних баз, методичних розробок, спеціальної навчальної та наукової літератури, практичні заняття з використанням комп'ютерного обладнання, виконання проблемно-орієнтованих, пошукових, творчих завдань, пошук і аналіз літератури та електронних джерел інформації по заданій проблемі та обраній темі випускної кваліфікаційної роботи, елементи наукових досліджень.	оцінювання самостійного виконання індивідуальних завдань, тестування, тренінг проводиться з метою формування вмінь і навичок у студентів практичного спрямування, формування сучасного наукового мислення, вміння приймати відповідальні та ефективні рішення; самостійна робота дозволяє виявити вміння чітко, логічно і послідовно відповідати на поставлені запитання, вміння працювати самостійно; індивідуальна науково-дослідна робота студентів (ІНДР) проводиться з метою отримання практичних навичок та умінь щодо використання та опрацювання наукових джерел, написання статей, тез, оформлення звітів, розроблення презентаційного матеріалу, використання теоретичних та емпіричних методів дослідження. Підсумковий контроль: іспит.
		Магістерська кваліфікаційна робота	Виконання індивідуального завдання	Захист магістерської кваліфікаційної роботи
		Переддипломна практика	Виконання індивідуальних завдань практики	Підсумковий контроль знань здобувачів вищої освіти проводиться шляхом аналізу звіту та щоденника переддипломної практики, а також індивідуального опитування здобувачів вищої освіти під час диференційованого заліку.
		Моніторинг та аудит кібербезпеки	При вивченні дисципліни використовуються: Дидактичні методи - лекції з використанням мультимедійних презентацій. Практичні методи: лабораторні з використанням прикладного програмного забезпечення. Метод самостійного навчання. Активні методи: експрес опитування, тестування. Словесні методи навчання: лекції, консультації.	Поточний контроль: у формі фронтального, індивідуального чи комбінованого контролю знань здобувачів вищої освіти під час лекційного та лабораторного заняття, тестування, колоквіумів. Підсумковий контроль: іспит.
		Кібербезпека	При вивченні дисципліни використовуються: Дидактичні методи - лекції з використанням мультимедійних презентацій. Практичні методи: лабораторні роботи з використанням прикладного програмного забезпечення. Метод самостійного навчання. Активні методи: експрес опитування, тестування. Словесні методи навчання: лекції, консультації.	Поточний контроль: у формі фронтального, індивідуального чи комбінованого контролю знань здобувачів вищої освіти під час лекційного та лабораторного заняття, тестування, колоквіумів. Підсумковий контроль: іспит.
РН19. Обирати, аналізувати і розробляти	☒	Методологія та організація наукових досліджень в	Лекція, проблемна лекція, дискусія, ІТ-методи, командна робота,	Поточний контроль: у формі фронтального, індивідуального чи

придатні типові аналітичні, розрахункові та експериментальні методи кіберзахисту, розробляти, реалізовувати та супроводжувати проекти з захисту інформації у кіберпросторі, інноваційної діяльності та захисту інтелектуальної власності.		кібербезпеці	демонстрація, зокрема, з використанням мультимедійних засобів навчання, Internet-ресурсів, інформаційних баз, методичних розробок, спеціальної навчальної та наукової літератури, практичні заняття з використанням комп'ютерного обладнання, виконання проблемно-орієнтованих, пошукових, творчих завдань, пошук і аналіз літератури та електронних джерел інформації по заданій проблемі та обраній темі випускної кваліфікаційної роботи, елементи наукових досліджень.	комбінованого контролю знань студентів під час практичного заняття, оцінювання самостійного виконання індивідуальних завдань, тестування, тренінг проводиться з метою формування вмінь і навичок у студентів практичного спрямування, формування сучасного наукового мислення, вміння приймати відповідальні та ефективні рішення; самостійна робота дозволяє виявити вміння чітко, логічно і послідовно відповідати на поставлені запитання, вміння працювати самостійно; індивідуальна науково-дослідна робота студентів (ІНДР) проводиться з метою отримання практичних навичок та умінь щодо використання та опрацювання наукових джерел, написання статей, тез, оформлення звітів, розроблення презентаційного матеріалу, використання теоретичних та емпіричних методів дослідження. Підсумковий контроль: іспит.
		Проектування систем кібербезпеки (в т.ч. курсова робота)	При вивченні дисципліни використовуються: Дидактичні методи - лекції з використанням мультимедійних презентацій. Практичні методи: лабораторні та практичні роботи з використанням прикладного програмного забезпечення. Метод самостійного навчання. Активні методи: експрес опитування, тестування. Словесні методи навчання: лекції, консультації. Виконання індивідуального завдання у формі курсової роботи.	Поточний контроль: у формі фронтального, індивідуального чи комбінованого контролю знань здобувачів вищої освіти під час лекційного та лабораторного заняття, тестування, колоквіумів. Підсумковий контроль: іспит. Оцінювання курсових робіт проводиться у формі їх публічного захисту на відкритому засіданні комісії за участю керівника курсової роботи та ще не менше одного викладача кафедри.
		Переддипломна практика	Виконання індивідуальних завдань практики	Підсумковий контроль знань здобувачів вищої освіти проводиться шляхом аналізу звіту та щоденника переддипломної практики, а також індивідуального опитування здобувачів вищої освіти під час диференційованого заліку.
		Магістерська кваліфікаційна робота	Виконання індивідуального завдання	Захист магістерської кваліфікаційної роботи
РН18. Планувати навчання, а також супроводжувати та контролювати роботу з персоналом у напряму інформаційної безпеки та/або кібербезпеки.	☒	Інноваційні та психологічні аспекти сучасної освіти	Лекція, проблемна лекція, демонстрація, зокрема, з використанням мультимедійних засобів навчання, метод самостійного навчання, мікровикладання здобувачів, груповий проєкт (аналіз кейсів), навчальне есе, доповідь науково-дослідного характеру (зокрема, на щорічну	Поточний контроль: у формі фронтального, індивідуального чи комбінованого контролю знань здобувачів під час лекційного та практичного заняття, тестування, колоквіумів. Підсумковий контроль: враховуються результати всіх видів навчальної роботи згідно із структурою

			науково-технічну конференцію викладачів, співробітників та студентів ВНТУ), тестування (електронне, в системі JetIQ).	кредитів. Оцінювання рівня виконання індивідуальної роботи викладач здійснює на основі перевірки змісту роботи та її захисту у формі доповіді. Підсумковий контроль знань студентів проводиться шляхом складання недиференційованого заліку за темами, що охоплюють весь курс дисципліни. Недиференційований залік може проводитись за допомогою усного опитування та/або тестів у електронній системі університету та додаткової письмової роботи.
		Переддипломна практика	Виконання індивідуальних завдань практики	Підсумковий контроль знань здобувачів вищої освіти проводиться шляхом аналізу звіту та щоденника переддипломної практики, а також індивідуального опитування здобувачів вищої освіти під час диференційованого заліку.
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.	☒	Методологія та організація наукових досліджень в кібербезпеці	Лекція, проблемна лекція, дискусія, ІТ-методи, командна робота, демонстрація, зокрема, з використанням мультимедійних засобів навчання, Internet-ресурсів, інформаційних баз, методичних розробок, спеціальної навчальної та наукової літератури, практичні заняття з використанням комп'ютерного обладнання, виконання проблемно-орієнтованих, пошукових, творчих завдань, пошук і аналіз літератури та електронних джерел інформації по заданій проблемі та обраній темі випускної кваліфікаційної роботи, елементи наукових досліджень.	Поточний контроль: у формі фронтального, індивідуального чи комбінованого контролю знань студентів під час практичного заняття, оцінювання самостійного виконання індивідуальних завдань, тестування, тренінг проводиться з метою формування вмінь і навичок у студентів практичного спрямування, формування сучасного наукового мислення, вміння приймати відповідальні та ефективні рішення; самостійна робота дозволяє виявити вміння чітко, логічно і послідовно відповідати на поставлені запитання, вміння працювати самостійно; індивідуальна науково-дослідна робота студентів (ІНДР) проводиться з метою отримання практичних навичок та умінь щодо використання та опрацювання наукових джерел, написання статей, тез, оформлення звітів, розроблення презентаційного матеріалу, використання теоретичних та емпіричних методів дослідження. Підсумковий контроль: іспит.
		Проектування систем кібербезпеки (в т.ч. курсова робота)	При вивченні дисципліни використовуються: Дидактичні методи - лекції з використанням мультимедійних презентацій. Практичні методи: лабораторні та практичні роботи з використанням прикладного програмного забезпечення. Метод самостійного навчання.	Поточний контроль: у формі фронтального, індивідуального чи комбінованого контролю знань здобувачів вищої освіти під час лекційного та лабораторного заняття, тестування, колоквіумів. Підсумковий контроль: іспит. Оцінювання курсових робіт проводиться у формі їх

			Активні методи: експрес опитування, тестування. Словесні методи навчання: лекції, консультації. Виконання індивідуального завдання у формі курсової роботи.	публічного захисту на відкритому засіданні комісії за участю керівника курсової роботи та ще не менше одного викладача кафедри.
		Переддипломна практика	Виконання індивідуальних завдань практики	Підсумковий контроль знань здобувачів вищої освіти проводиться шляхом аналізу звіту та щоденника переддипломної практики, а також індивідуального опитування здобувачів вищої освіти під час диференційованого заліку.
		Магістерська кваліфікаційна робота	Виконання індивідуального завдання	Захист магістерської кваліфікаційної роботи
		Філософія науки і техніки	При вивченні дисципліни використовуються: Дидактичні методи – лекції з використанням мультимедійних презентацій. Практичні методи: практичні завдання. Метод самостійного навчання. Активні методи: експрес опитування, тестування. Словесні методи навчання: лекції, консультації.	Поточний контроль: фронтальний, індивідуальний чи комбінований контроль знань здобувачів під час лекційного та практичного заняття, тестування, колоквіумів. Підсумковий контроль: залік
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.	☒	Сучасні системи, технології та засоби інформаційної безпеки та кібербезпеки	При вивченні дисципліни використовуються: Дидактичні методи - лекції з використанням мультимедійних презентацій. Практичні методи: лабораторні роботи з використанням прикладного програмного забезпечення. Метод самостійного навчання. Активні методи: експрес опитування, тестування. Словесні методи навчання: лекції, консультації.	Поточний контроль: у формі фронтального, індивідуального чи комбінованого контролю знань студентів під час лекційного та лабораторного заняття, тестування, колоквіумів. Оцінювання результатів виконання індивідуального завдання здійснюється на основі перевірки змісту реферату та його подання у формі доповіді. Підсумковий контроль: іспит.
		Кібербезпека	При вивченні дисципліни використовуються: Дидактичні методи - лекції з використанням мультимедійних презентацій. Практичні методи: лабораторні роботи з використанням прикладного програмного забезпечення. Метод самостійного навчання. Активні методи: експрес опитування, тестування. Словесні методи навчання: лекції, консультації.	Поточний контроль: у формі фронтального, індивідуального чи комбінованого контролю знань здобувачів вищої освіти під час лекційного та лабораторного заняття, тестування, колоквіумів. Підсумковий контроль: іспит.
		Кібербезпека об'єктів критичної інфраструктури	Дидактичні методи – лекції з використанням мультимедійних презентацій. Практичні методи: лабораторні роботи з розробки та використанням прикладного програмного забезпечення та практичні завдання. Метод самостійного навчання. Активні методи: експрес опитування, фронтальне	Поточний контроль: у формі фронтального, індивідуального чи комбінованого контролю знань здобувачів вищої освіти під час лекційного та лабораторного заняття, тестування, колоквіумів. Підсумковий контроль: іспит.

			опитування. Словесні методи навчання: лекції, консультації.	
		Проектування систем кібербезпеки (в т.ч. курсова робота)	При вивченні дисципліни використовуються: Дидактичні методи - лекції з використанням мультимедійних презентацій. Практичні методи: лабораторні та практичні роботи з використанням прикладного програмного забезпечення. Метод самостійного навчання. Активні методи: експрес опитування, тестування. Словесні методи навчання: лекції, консультації. Виконання індивідуального завдання у формі курсової роботи.	Поточний контроль: у формі фронтального, індивідуального чи комбінованого контролю знань здобувачів вищої освіти під час лекційного та лабораторного заняття, тестування, колоквіумів. Підсумковий контроль: іспит. Оцінювання курсових робіт проводиться у формі їх публічного захисту на відкритому засіданні комісії за участю керівника курсової роботи та ще не менше одного викладача кафедри.
		Моніторинг та аудит кібербезпеки	При вивченні дисципліни використовуються: Дидактичні методи - лекції з використанням мультимедійних презентацій. Практичні методи: лабораторні з використанням прикладного програмного забезпечення. Метод самостійного навчання. Активні методи: експрес опитування, тестування. Словесні методи навчання: лекції, консультації.	Поточний контроль: у формі фронтального, індивідуального чи комбінованого контролю знань здобувачів вищої освіти під час лекційного та лабораторного заняття, тестування, колоквіумів. Підсумковий контроль: іспит.
		Переддипломна практика	Виконання індивідуальних завдань практики	Підсумковий контроль знань здобувачів вищої освіти проводиться шляхом аналізу звіту та щоденника переддипломної практики, а також індивідуального опитування здобувачів вищої освіти під час диференційованого заліку.
		Магістерська кваліфікаційна робота	Виконання індивідуального завдання	Захист магістерської кваліфікаційної роботи
РН24. Проєктувати, розробляти, тестувати системи забезпечення кібербезпеки в інформаційних і комунікаційних системах відповідно до завдань та загроз, що виникають на сучасному етапі розвитку інформаційних технологій.	☐	Кібербезпека об'єктів критичної інфраструктури	Дидактичні методи – лекції з використанням мультимедійних презентацій. Практичні методи: лабораторні роботи з розробки та використанням прикладного програмного забезпечення та практичні завдання. Метод самостійного навчання. Активні методи: експрес опитування, фронтальне опитування. Словесні методи навчання: лекції, консультації.	Поточний контроль: у формі фронтального, індивідуального чи комбінованого контролю знань здобувачів вищої освіти під час лекційного та лабораторного заняття, тестування, колоквіумів. Підсумковий контроль: іспит.
		Проектування систем кібербезпеки (в т.ч. курсова робота)	При вивченні дисципліни використовуються: Дидактичні методи - лекції з використанням мультимедійних презентацій. Практичні методи: лабораторні та практичні роботи з використанням прикладного програмного забезпечення. Метод	Поточний контроль: у формі фронтального, індивідуального чи комбінованого контролю знань здобувачів вищої освіти під час лекційного та лабораторного заняття, тестування, колоквіумів. Підсумковий контроль: іспит. Оцінювання курсових робіт

			самостійного навчання. Активні методи: експрес опитування, тестування. Словесні методи навчання: лекції, консультації. Виконання індивідуального завдання у формі курсової роботи.	проводиться у формі їх публічного захисту на відкритому засіданні комісії за участю керівника курсової роботи та ще не менше одного викладача кафедри.
		Моніторинг та аудит кібербезпеки	При вивченні дисципліни використовуються: Дидактичні методи - лекції з використанням мультимедійних презентацій. Практичні методи: лабораторні з використанням прикладного програмного забезпечення. Метод самостійного навчання. Активні методи: експрес опитування, тестування. Словесні методи навчання: лекції, консультації.	Поточний контроль: у формі фронтального, індивідуального чи комбінованого контролю знань здобувачів вищої освіти під час лекційного та лабораторного заняття, тестування, колоквіумів. Підсумковий контроль: іспит.
		Переддипломна практика	Виконання індивідуальних завдань практики	Підсумковий контроль знань здобувачів вищої освіти проводиться шляхом аналізу звіту та щоденника переддипломної практики, а також індивідуального опитування здобувачів вищої освіти під час диференційованого заліку.
		Магістерська кваліфікаційна робота	Виконання індивідуального завдання	Захист магістерської кваліфікаційної роботи
РН25. Здатність контролювати процес встановлення, впровадження та налаштування компонентів системи щодо захисту інформації.	☐	Сучасні системи, технології та засоби інформаційної безпеки та кібербезпеки	При вивченні дисципліни використовуються: Дидактичні методи - лекції з використанням мультимедійних презентацій. Практичні методи: лабораторні роботи з використанням прикладного програмного забезпечення. Метод самостійного навчання. Активні методи: експрес опитування, тестування. Словесні методи навчання: лекції, консультації.	Поточний контроль: у формі фронтального, індивідуального чи комбінованого контролю знань студентів під час лекційного та лабораторного заняття, тестування, колоквіумів. Оцінювання результатів виконання індивідуального завдання здійснюється на основі перевірки змісту реферату та його подання у формі доповіді. Підсумковий контроль: іспит.
		Кібербезпека	При вивченні дисципліни використовуються: Дидактичні методи - лекції з використанням мультимедійних презентацій. Практичні методи: лабораторні роботи з використанням прикладного програмного забезпечення. Метод самостійного навчання. Активні методи: експрес опитування, тестування. Словесні методи навчання: лекції, консультації.	Поточний контроль: у формі фронтального, індивідуального чи комбінованого контролю знань здобувачів вищої освіти під час лекційного та лабораторного заняття, тестування, колоквіумів. Підсумковий контроль: іспит.
		Кібербезпека об'єктів критичної інфраструктури	Дидактичні методи – лекції з використанням мультимедійних презентацій. Практичні методи: лабораторні роботи з розробки та використанням прикладного програмного забезпечення та практичні завдання. Метод	Поточний контроль: у формі фронтального, індивідуального чи комбінованого контролю знань здобувачів вищої освіти під час лекційного та лабораторного заняття, тестування, колоквіумів. Підсумковий контроль: іспит.

			самостійного навчання. Активні методи: експрес опитування, фронтальне опитування. Словесні методи навчання: лекції, консультації.	
		Проектування систем кібербезпеки (в т.ч. курсова робота)	При вивченні дисципліни використовуються: Дидактичні методи - лекції з використанням мультимедійних презентацій. Практичні методи: лабораторні та практичні роботи з використанням прикладного програмного забезпечення. Метод самостійного навчання. Активні методи: експрес опитування, тестування. Словесні методи навчання: лекції, консультації. Виконання індивідуального завдання у формі курсової роботи.	Поточний контроль: у формі фронтального, індивідуального чи комбінованого контролю знань здобувачів вищої освіти під час лекційного та лабораторного заняття, тестування, колоквіумів. Підсумковий контроль: іспит. Оцінювання курсових робіт проводиться у формі їх публічного захисту на відкритому засіданні комісії за участю керівника курсової роботи та ще не менше одного викладача кафедри.
		Переддипломна практика	Виконання індивідуальних завдань практики	Підсумковий контроль знань здобувачів вищої освіти проводиться шляхом аналізу звіту та щоденника переддипломної практики, а також індивідуального опитування здобувачів вищої освіти під час диференційованого заліку.
		Магістерська кваліфікаційна робота	Виконання індивідуального завдання	Захист магістерської кваліфікаційної роботи
РН26. Здатність надавати рекомендації щодо планів аварійного відновлення, непередбачених випадків та забезпечення безперервності операцій.	☐	Моніторинг та аудит кібербезпеки	При вивченні дисципліни використовуються: Дидактичні методи - лекції з використанням мультимедійних презентацій. Практичні методи: лабораторні з використанням прикладного програмного забезпечення. Метод самостійного навчання. Активні методи: експрес опитування, тестування. Словесні методи навчання: лекції, консультації.	Поточний контроль: у формі фронтального, індивідуального чи комбінованого контролю знань здобувачів вищої освіти під час лекційного та лабораторного заняття, тестування, колоквіумів. Підсумковий контроль: іспит.
		Кібербезпека об'єктів критичної інфраструктури	Дидактичні методи – лекції з використанням мультимедійних презентацій. Практичні методи: лабораторні роботи з розробки та використанням прикладного програмного забезпечення та практичні завдання. Метод самостійного навчання. Активні методи: експрес опитування, фронтальне опитування. Словесні методи навчання: лекції, консультації.	Поточний контроль: у формі фронтального, індивідуального чи комбінованого контролю знань здобувачів вищої освіти під час лекційного та лабораторного заняття, тестування, колоквіумів. Підсумковий контроль: іспит.
		Кібербезпека	При вивченні дисципліни використовуються: Дидактичні методи - лекції з використанням мультимедійних презентацій. Практичні методи: лабораторні роботи з використанням	Поточний контроль: у формі фронтального, індивідуального чи комбінованого контролю знань здобувачів вищої освіти під час лекційного та лабораторного заняття, тестування, колоквіумів.

			прикладного програмного забезпечення. Метод самостійного навчання. Активні методи: експрес опитування, тестування. Словесні методи навчання: лекції, консультації.	Підсумковий контроль: іспит.
РН21. Використовувати методи натурного, фізичного і комп'ютерного моделювання для дослідження процесів, які стосуються інформаційної безпеки та/або кібербезпеки.	☒	Проектування систем кібербезпеки (в т.ч. курсова робота)	При вивченні дисципліни використовуються: Дидактичні методи - лекції з використанням мультимедійних презентацій. Практичні методи: лабораторні та практичні роботи з використанням прикладного програмного забезпечення. Метод самостійного навчання. Активні методи: експрес опитування, тестування. Словесні методи навчання: лекції, консультації. Виконання індивідуального завдання у формі курсової роботи.	Поточний контроль: у формі фронтального, індивідуального чи комбінованого контролю знань здобувачів вищої освіти під час лекційного та лабораторного заняття, тестування, колоквіумів. Підсумковий контроль: іспит. Оцінювання курсових робіт проводиться у формі їх публічного захисту на відкритому засіданні комісії за участю керівника курсової роботи та ще не менше одного викладача кафедри.
		Переддипломна практика	Виконання індивідуальних завдань практики	Підсумковий контроль знань здобувачів вищої освіти проводиться шляхом аналізу звіту та щоденника переддипломної практики, а також індивідуального опитування здобувачів вищої освіти під час диференційованого заліку.
		Магістерська кваліфікаційна робота	Виконання індивідуального завдання	Захист магістерської кваліфікаційної роботи
		Методологія та організація наукових досліджень в кібербезпеці	Лекція, проблемна лекція, дискусія, ІТ-методи, командна робота, демонстрація, зокрема, з використанням мультимедійних засобів навчання, Internet-ресурсів, інформаційних баз, методичних розробок, спеціальної навчальної та наукової літератури, практичні заняття з використанням комп'ютерного обладнання, виконання проблемно-орієнтованих, пошукових, творчих завдань, пошук і аналіз літератури та електронних джерел інформації по заданій проблемі та обраній темі випускної кваліфікаційної роботи, елементи наукових досліджень.	Поточний контроль: у формі фронтального, індивідуального чи комбінованого контролю знань студентів під час практичного заняття, оцінювання самостійного виконання індивідуальних завдань, тестування, тренінг проводиться з метою формування вмінь і навичок у студентів практичного спрямування, формування сучасного наукового мислення, вміння приймати відповідальні та ефективні рішення; самостійна робота дозволяє виявити вміння чітко, логічно і послідовно відповідати на поставлені запитання, вміння працювати самостійно; індивідуальна науково-дослідна робота студентів (ІНДР) проводиться з метою отримання практичних навичок та умінь щодо використання та опрацювання наукових джерел, написання статей, тез, оформлення звітів, розроблення презентаційного матеріалу, використання теоретичних та емпіричних методів дослідження. Підсумковий контроль: іспит.

РН13. Досліджувати, розробляти, впроваджувати та використовувати методи та засоби криптографічного та технічного захисту інформації бізнес/операційних процесів, а також аналізувати і надавати оцінку ефективності їх використання в інформаційних системах, на об'єктах інформаційної діяльності та критичної інфраструктури.	☒	Кібербезпека	При вивченні дисципліни використовуються: Дидактичні методи - лекції з використанням мультимедійних презентацій. Практичні методи: лабораторні роботи з використанням прикладного програмного забезпечення. Метод самостійного навчання. Активні методи: експрес опитування, тестування. Словесні методи навчання: лекції, консультації.	Поточний контроль: у формі фронтального, індивідуального чи комбінованого контролю знань здобувачів вищої освіти під час лекційного та лабораторного заняття, тестування, колоквіумів. Підсумковий контроль: іспит.
		Кібербезпека об'єктів критичної інфраструктури	Дидактичні методи – лекції з використанням мультимедійних презентацій. Практичні методи: лабораторні роботи з розробки та використанням прикладного програмного забезпечення та практичні завдання. Метод самостійного навчання. Активні методи: експрес опитування, фронтальне опитування. Словесні методи навчання: лекції, консультації.	Поточний контроль: у формі фронтального, індивідуального чи комбінованого контролю знань здобувачів вищої освіти під час лекційного та лабораторного заняття, тестування, колоквіумів. Підсумковий контроль: іспит.
		Переддипломна практика	Виконання індивідуальних завдань практики	Підсумковий контроль знань здобувачів вищої освіти проводиться шляхом аналізу звіту та щоденника переддипломної практики, а також індивідуального опитування здобувачів вищої освіти під час диференційованого заліку.
		Магістерська кваліфікаційна робота	Виконання індивідуального завдання	Захист магістерської кваліфікаційної роботи
РН17. Мати навички автономного і самостійного навчання у сфері інформаційної безпеки та/або кібербезпеки і дотичних галузей знань, аналізувати власні освітні потреби та об'єктивно оцінювати результати навчання.	☒	Інноваційні та психологічні аспекти сучасної освіти	Лекція, проблемна лекція, демонстрація, зокрема, з використанням мультимедійних засобів навчання, метод самостійного навчання, мікровикладання здобувачів, груповий проєкт (аналіз кейсів), навчальне есе, доповідь науково-дослідного характеру (зокрема, на щорічну науково-технічну конференцію викладачів, співробітників та студентів ВНТУ), тестування (електронне, в системі JetIQ).	Поточний контроль: у формі фронтального, індивідуального чи комбінованого контролю знань здобувачів під час лекційного та практичного заняття, тестування, колоквіумів. Підсумковий контроль: враховуються результати всіх видів навчальної роботи згідно із структурою кредитів. Оцінювання рівня виконання індивідуальної роботи викладач здійснює на основі перевірки змісту роботи та її захисту у формі доповіді. Підсумковий контроль знань студентів проводиться шляхом складання недиференційованого заліку за темами, що охоплюють весь курс дисципліни. Недиференційований залік може проводитись за допомогою усного опитування та/або тестів у електронній системі університету та додаткової письмової роботи.
		Методологія та організація наукових досліджень в кібербезпеці	Лекція, проблемна лекція, дискусія, ІТ-методи, командна робота, демонстрація, зокрема, з	Поточний контроль: у формі фронтального, індивідуального чи комбінованого контролю

			використанням мультимедійних засобів навчання, Internet-ресурсів, інформаційних баз, методичних розробок, спеціальної навчальної та наукової літератури, практичні заняття з використанням комп'ютерного обладнання, виконання проблемно-орієнтованих, пошукових, творчих завдань, пошук і аналіз літератури та електронних джерел інформації по заданій проблемі та обраній темі випускної кваліфікаційної роботи, елементи наукових досліджень.	знань студентів під час практичного заняття, оцінювання самостійного виконання індивідуальних завдань, тестування, тренінг проводиться з метою формування вмінь і навичок у студентів практичного спрямування, формування сучасного наукового мислення, вміння приймати відповідальні та ефективні рішення; самостійна робота дозволяє виявити вміння чітко, логічно і послідовно відповідати на поставлені запитання, вміння працювати самостійно; індивідуальна науково-дослідна робота студентів (ІНДР) проводиться з метою отримання практичних навичок та умінь щодо використання та опрацювання наукових джерел, написання статей, тез, оформлення звітів, розроблення презентаційного матеріалу, використання теоретичних та емпіричних методів дослідження. Підсумковий контроль: іспит.
		Переддипломна практика	Виконання індивідуальних завдань практики	Підсумковий контроль знань здобувачів вищої освіти проводиться шляхом аналізу звіту та щоденника переддипломної практики, а також індивідуального опитування здобувачів вищої освіти під час диференційованого заліку.
		Магістерська кваліфікаційна робота	Виконання індивідуального завдання	Захист магістерської кваліфікаційної роботи
		Філософія науки і техніки	При вивченні дисципліни використовуються: Дидактичні методи – лекції з використанням мультимедійних презентацій. Практичні методи: практичні завдання. Метод самостійного навчання. Активні методи: експрес опитування, тестування. Словесні методи навчання: лекції, консультації.	Поточний контроль: фронтальний, індивідуальний чи комбінований контроль знань здобувачів під час лекційного та практичного заняття, тестування, колоквіумів. Підсумковий контроль: залік
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.	☒	Ділова іноземна мова	Розповідь-пояснення, бесіда, ілюстрація, демонстрація, зокрема, з використанням мультимедійних засобів навчання, практичні роботи, підготовка доповідей науково-дослідного характеру, зокрема, на щорічну науково-технічну конференцію викладачів, співробітників та студентів ВНТУ.	Поточний контроль: у формі фронтального, індивідуального чи комбінованого контролю знань студентів під час практичного заняття, тестування. Підсумковий контроль: залік.
		Магістерська кваліфікаційна робота	Виконання індивідуального завдання	Захист магістерської кваліфікаційної роботи
		Переддипломна практика	Виконання індивідуальних завдань практики	Підсумковий контроль знань здобувачів вищої

				освіти проводиться шляхом аналізу звіту та щоденника переддипломної практики, а також індивідуального опитування здобувачів вищої освіти під час диференційованого заліку.
РН2. Інтегрувати фундаментальні та спеціальні знання для розв'язування складних задач інформаційної безпеки та/або кібербезпеки у широких або мультидисциплінарних контекстах.	☒	Методологія та організація наукових досліджень в кібербезпеці	Лекція, проблемна лекція, дискусія, ІТ-методи, командна робота, демонстрація, зокрема, з використанням мультимедійних засобів навчання, Internet-ресурсів, інформаційних баз, методичних розробок, спеціальної навчальної та наукової літератури, практичні заняття з використанням комп'ютерного обладнання, виконання проблемно-орієнтованих, пошукових, творчих завдань, пошук і аналіз літератури та електронних джерел інформації по заданій проблемі та обраній темі випускної кваліфікаційної роботи, елементи наукових досліджень.	Поточний контроль: у формі фронтального, індивідуального чи комбінованого контролю знань студентів під час практичного заняття, оцінювання самостійного виконання індивідуальних завдань, тестування, тренінг проводиться з метою формування вмінь і навичок у студентів практичного спрямування, формування сучасного наукового мислення, вміння приймати відповідальні та ефективні рішення; самостійна робота дозволяє виявити вміння чітко, логічно і послідовно відповідати на поставлені запитання, вміння працювати самостійно; індивідуальна науково-дослідна робота студентів (ІНДР) проводиться з метою отримання практичних навичок та умінь щодо використання та опрацювання наукових джерел, написання статей, тез, оформлення звітів, розроблення презентаційного матеріалу, використання теоретичних та емпіричних методів дослідження. Підсумковий контроль: іспит.
		Сучасні системи, технології та засоби інформаційної безпеки та кібербезпеки	При вивченні дисципліни використовуються: Дидактичні методи - лекції з використанням мультимедійних презентацій. Практичні методи: лабораторні роботи з використанням прикладного програмного забезпечення. Метод самостійного навчання. Активні методи: експрес опитування, тестування. Словесні методи навчання: лекції, консультації.	Поточний контроль: у формі фронтального, індивідуального чи комбінованого контролю знань студентів під час лекційного та лабораторного заняття, тестування, колоквіумів. Оцінювання результатів виконання індивідуального завдання здійснюється на основі перевірки змісту реферату та його подання у формі доповіді. Підсумковий контроль: іспит.
		Кібербезпека	При вивченні дисципліни використовуються: Дидактичні методи - лекції з використанням мультимедійних презентацій. Практичні методи: лабораторні роботи з використанням прикладного програмного забезпечення. Метод самостійного навчання. Активні методи: експрес опитування, тестування. Словесні методи навчання: лекції, консультації.	Поточний контроль: у формі фронтального, індивідуального чи комбінованого контролю знань здобувачів вищої освіти під час лекційного та лабораторного заняття, тестування, колоквіумів. Підсумковий контроль: іспит.

		Переддипломна практика	Виконання індивідуальних завдань практики	Підсумковий контроль знань здобувачів вищої освіти проводиться шляхом аналізу звіту та щоденника переддипломної практики, а також індивідуального опитування здобувачів вищої освіти під час диференційованого заліку.
		Магістерська кваліфікаційна робота	Виконання індивідуального завдання	Захист магістерської кваліфікаційної роботи
		Філософія науки і техніки	При вивченні дисципліни використовуються: Дидактичні методи – лекції з використанням мультимедійних презентацій. Практичні методи: практичні завдання. Метод самостійного навчання. Активні методи: експрес опитування, тестування. Словесні методи навчання: лекції, консультації.	Поточний контроль: фронтальний, індивідуальний чи комбінований контроль знань здобувачів під час лекційного та практичного заняття, тестування, колоквіумів. Підсумковий контроль: залік
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.	☒	Інноваційні та психологічні аспекти сучасної освіти	Лекція, проблемна лекція, демонстрація, зокрема, з використанням мультимедійних засобів навчання, метод самостійного навчання, мікровикладання здобувачів, груповий проєкт (аналіз кейсів), навчальне есе, доповідь науково-дослідного характеру (зокрема, на щорічну науково-технічну конференцію викладачів, співробітників та студентів ВНТУ), тестування (електронне, в системі JetIQ).	Поточний контроль: у формі фронтального, індивідуального чи комбінованого контролю знань здобувачів під час лекційного та практичного заняття, тестування, колоквіумів. Підсумковий контроль: враховуються результати всіх видів навчальної роботи згідно із структурою кредитів. Оцінювання рівня виконання індивідуальної роботи викладач здійснює на основі перевірки змісту роботи та її захисту у формі доповіді. Підсумковий контроль знань студентів проводиться шляхом складання недиференційованого заліку за темами, що охоплюють весь курс дисципліни. Недиференційований залік може проводитись за допомогою усного опитування та/або тестів у електронній системі університету та додаткової письмової роботи.
		Методологія та організація наукових досліджень в кібербезпеці	Лекція, проблемна лекція, дискусія, ІТ-методи, командна робота, демонстрація, зокрема, з використанням мультимедійних засобів навчання, Internet-ресурсів, інформаційних баз, методичних розробок, спеціальної навчальної та наукової літератури, практичні заняття з використанням комп'ютерного обладнання, виконання проблемно-орієнтованих, пошукових, творчих завдань, пошук і аналіз літератури та електронних джерел інформації по заданій проблемі та обраній темі випускної кваліфікаційної	Поточний контроль: у формі фронтального, індивідуального чи комбінованого контролю знань студентів під час практичного заняття, оцінювання самостійного виконання індивідуальних завдань, тестування, тренінг проводиться з метою формування вмінь і навичок у студентів практичного спрямування, формування сучасного наукового мислення, вміння приймати відповідальні та ефективні рішення; самостійна робота дозволяє виявити вміння чітко, логічно і послідовно відповідати на поставлені запитання, вміння працювати самостійно;

			роботи, елементи наукових досліджень.	індивідуальна науково-дослідна робота студентів (ІНДР) проводиться з метою отримання практичних навичок та умінь щодо використання та опрацювання наукових джерел, написання статей, тез, оформлення звітів, розроблення презентаційного матеріалу, використання теоретичних та емпіричних методів дослідження. Підсумковий контроль: іспит.
		Проектування систем кібербезпеки (в т.ч. курсова робота)	При вивченні дисципліни використовуються: Дидактичні методи - лекції з використанням мультимедійних презентацій. Практичні методи: лабораторні та практичні роботи з використанням прикладного програмного забезпечення. Метод самостійного навчання. Активні методи: експрес опитування, тестування. Словесні методи навчання: лекції, консультації. Виконання індивідуального завдання у формі курсової роботи.	Поточний контроль: у формі фронтального, індивідуального чи комбінованого контролю знань здобувачів вищої освіти під час лекційного та лабораторного заняття, тестування, колоквіумів. Підсумковий контроль: іспит. Оцінювання курсових робіт проводиться у формі їх публічного захисту на відкритому засіданні комісії за участю керівника курсової роботи та ще не менше одного викладача кафедри.
		Переддипломна практика	Виконання індивідуальних завдань практики	Підсумковий контроль знань здобувачів вищої освіти проводиться шляхом аналізу звіту та щоденника переддипломної практики, а також індивідуального опитування здобувачів вищої освіти під час диференційованого заліку.
		Магістерська кваліфікаційна робота	Виконання індивідуального завдання	Захист магістерської кваліфікаційної роботи
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.	☒	Філософія науки і техніки	При вивченні дисципліни використовуються: Дидактичні методи – лекції з використанням мультимедійних презентацій. Практичні методи: практичні завдання. Метод самостійного навчання. Активні методи: експрес опитування, тестування. Словесні методи навчання: лекції, консультації.	Поточний контроль: фронтальний, індивідуальний чи комбінований контроль знань здобувачів під час лекційного та практичного заняття, тестування, колоквіумів. Підсумковий контроль: залік
		Магістерська кваліфікаційна робота	Виконання індивідуального завдання	Захист магістерської кваліфікаційної роботи
		Переддипломна практика	Виконання індивідуальних завдань практики	Підсумковий контроль знань здобувачів вищої освіти проводиться шляхом аналізу звіту та щоденника переддипломної практики, а також індивідуального опитування здобувачів вищої освіти під час диференційованого заліку.
		Методологія та організація наукових досліджень в кібербезпеці	Лекція, проблемна лекція, дискусія, ІТ-методи, командна робота, демонстрація, зокрема, з	Поточний контроль: у формі фронтального, індивідуального чи комбінованого контролю

			використанням мультимедійних засобів навчання, Internet-ресурсів, інформаційних баз, методичних розробок, спеціальної навчальної та наукової літератури, практичні заняття з використанням комп'ютерного обладнання, виконання проблемно-орієнтованих, пошукових, творчих завдань, пошук і аналіз літератури та електронних джерел інформації по заданій проблемі та обраній темі випускної кваліфікаційної роботи, елементи наукових досліджень.	знань студентів під час практичного заняття, оцінювання самостійного виконання індивідуальних завдань, тестування, тренінг проводиться з метою формування вмінь і навичок у студентів практичного спрямування, формування сучасного наукового мислення, вміння приймати відповідальні та ефективні рішення; самостійна робота дозволяє виявити вміння чітко, логічно і послідовно відповідати на поставлені запитання, вміння працювати самостійно; індивідуальна науково-дослідна робота студентів (ІНДР) проводиться з метою отримання практичних навичок та умінь щодо використання та опрацювання наукових джерел, написання статей, тез, оформлення звітів, розроблення презентаційного матеріалу, використання теоретичних та емпіричних методів дослідження. Підсумковий контроль: іспит.
РН4. Застосовувати, інтегрувати, розробляти, впроваджувати та удосконалювати сучасні інформаційні технології, фізичні та математичні методи і моделі в сфері інформаційної безпеки та/або кібербезпеки.	☒	Магістерська кваліфікаційна робота	Виконання індивідуального завдання	Захист магістерської кваліфікаційної роботи
		Сучасні системи, технології та засоби інформаційної безпеки та кібербезпеки	При вивченні дисципліни використовуються: Дидактичні методи - лекції з використанням мультимедійних презентацій. Практичні методи: лабораторні роботи з використанням прикладного програмного забезпечення. Метод самостійного навчання. Активні методи: експрес опитування, тестування. Словесні методи навчання: лекції, консультації.	Поточний контроль: у формі фронтального, індивідуального чи комбінованого контролю знань студентів під час лекційного та лабораторного заняття, тестування, колоквіумів. Оцінювання результатів виконання індивідуального завдання здійснюється на основі перевірки змісту реферату та його подання у формі доповіді. Підсумковий контроль: іспит.
		Кібербезпека	При вивченні дисципліни використовуються: Дидактичні методи - лекції з використанням мультимедійних презентацій. Практичні методи: лабораторні роботи з використанням прикладного програмного забезпечення. Метод самостійного навчання. Активні методи: експрес опитування, тестування. Словесні методи навчання: лекції, консультації.	Поточний контроль: у формі фронтального, індивідуального чи комбінованого контролю знань здобувачів вищої освіти під час лекційного та лабораторного заняття, тестування, колоквіумів. Підсумковий контроль: іспит.
		Проектування систем кібербезпеки (в т.ч. курсова робота)	При вивченні дисципліни використовуються: Дидактичні методи - лекції з використанням мультимедійних презентацій. Практичні методи: лабораторні та практичні роботи з використанням прикладного програмного	Поточний контроль: у формі фронтального, індивідуального чи комбінованого контролю знань здобувачів вищої освіти під час лекційного та лабораторного заняття, тестування, колоквіумів. Підсумковий контроль: іспит.

			забезпечення. Метод самостійного навчання. Активні методи: експрес опитування, тестування. Словесні методи навчання: лекції, консультації. Виконання індивідуального завдання у формі курсової роботи.	Оцінювання курсових робіт проводиться у формі їх публічного захисту на відкритому засіданні комісії за участю керівника курсової роботи та ще не менше одного викладача кафедри.
		Переддипломна практика	Виконання індивідуальних завдань практики	Підсумковий контроль знань здобувачів вищої освіти проводиться шляхом аналізу звіту та щоденника переддипломної практики, а також індивідуального опитування здобувачів вищої освіти під час диференційованого заліку.
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.	☒	Кібербезпека	При вивченні дисципліни використовуються: Дидактичні методи - лекції з використанням мультимедійних презентацій. Практичні методи: лабораторні роботи з використанням прикладного програмного забезпечення. Метод самостійного навчання. Активні методи: експрес опитування, тестування. Словесні методи навчання: лекції, консультації.	Поточний контроль: у формі фронтального, індивідуального чи комбінованого контролю знань здобувачів вищої освіти під час лекційного та лабораторного заняття, тестування, колоквіумів. Підсумковий контроль: іспит.
		Кібербезпека об'єктів критичної інфраструктури	Дидактичні методи – лекції з використанням мультимедійних презентацій. Практичні методи: лабораторні роботи з розробки та використанням прикладного програмного забезпечення та практичні завдання. Метод самостійного навчання. Активні методи: експрес опитування, фронтальне опитування. Словесні методи навчання: лекції, консультації.	Поточний контроль: у формі фронтального, індивідуального чи комбінованого контролю знань здобувачів вищої освіти під час лекційного та лабораторного заняття, тестування, колоквіумів. Підсумковий контроль: іспит.
		Моніторинг та аудит кібербезпеки	При вивченні дисципліни використовуються: Дидактичні методи - лекції з використанням мультимедійних презентацій. Практичні методи: лабораторні з використанням прикладного програмного забезпечення. Метод самостійного навчання. Активні методи: експрес опитування, тестування. Словесні методи навчання: лекції, консультації.	Поточний контроль: у формі фронтального, індивідуального чи комбінованого контролю знань здобувачів вищої освіти під час лекційного та лабораторного заняття, тестування, колоквіумів. Підсумковий контроль: іспит.
РН7. Обґрунтовувати використання, впроваджувати та аналізувати кращі світові стандарти, практики з метою розв'язання складних задач професійної діяльності в галузі	☒	Магістерська кваліфікаційна робота	Виконання індивідуального завдання	Захист магістерської кваліфікаційної роботи
		Переддипломна практика	Виконання індивідуальних завдань практики	Підсумковий контроль знань здобувачів вищої освіти проводиться шляхом аналізу звіту та щоденника переддипломної практики, а також індивідуального опитування здобувачів вищої освіти під час

інформаційної безпеки та/або кібербезпеки.				диференційованого заліку.
		Моніторинг та аудит кібербезпеки	При вивченні дисципліни використовуються: Дидактичні методи - лекції з використанням мультимедійних презентацій. Практичні методи: лабораторні з використанням прикладного програмного забезпечення. Метод самостійного навчання. Активні методи: експрес опитування, тестування. Словесні методи навчання: лекції, консультації.	Поточний контроль: у формі фронтального, індивідуального чи комбінованого контролю знань здобувачів вищої освіти під час лекційного та лабораторного заняття, тестування, колоквіумів. Підсумковий контроль: іспит.
		Кібербезпека	При вивченні дисципліни використовуються: Дидактичні методи - лекції з використанням мультимедійних презентацій. Практичні методи: лабораторні роботи з використанням прикладного програмного забезпечення. Метод самостійного навчання. Активні методи: експрес опитування, тестування. Словесні методи навчання: лекції, консультації.	Поточний контроль: у формі фронтального, індивідуального чи комбінованого контролю знань здобувачів вищої освіти під час лекційного та лабораторного заняття, тестування, колоквіумів. Підсумковий контроль: іспит.
РН9. Аналізувати, розробляти і супроводжувати систему управління інформаційною безпекою та/або кібербезпекою організації на базі стратегії і політики інформаційної безпеки.	☒	Кібербезпека	При вивченні дисципліни використовуються: Дидактичні методи - лекції з використанням мультимедійних презентацій. Практичні методи: лабораторні роботи з використанням прикладного програмного забезпечення. Метод самостійного навчання. Активні методи: експрес опитування, тестування. Словесні методи навчання: лекції, консультації.	Поточний контроль: у формі фронтального, індивідуального чи комбінованого контролю знань здобувачів вищої освіти під час лекційного та лабораторного заняття, тестування, колоквіумів. Підсумковий контроль: іспит.
		Кібербезпека об'єктів критичної інфраструктури	Дидактичні методи – лекції з використанням мультимедійних презентацій. Практичні методи: лабораторні роботи з розробки та використанням прикладного програмного забезпечення та практичні завдання. Метод самостійного навчання. Активні методи: експрес опитування, фронтальне опитування. Словесні методи навчання: лекції, консультації.	Поточний контроль: у формі фронтального, індивідуального чи комбінованого контролю знань здобувачів вищої освіти під час лекційного та лабораторного заняття, тестування, колоквіумів. Підсумковий контроль: іспит.
		Моніторинг та аудит кібербезпеки	При вивченні дисципліни використовуються: Дидактичні методи - лекції з використанням мультимедійних презентацій. Практичні методи: лабораторні з використанням прикладного програмного забезпечення. Метод самостійного навчання. Активні методи: експрес опитування, тестування. Словесні методи навчання:	Поточний контроль: у формі фронтального, індивідуального чи комбінованого контролю знань здобувачів вищої освіти під час лекційного та лабораторного заняття, тестування, колоквіумів. Підсумковий контроль: іспит.

			лекції, консультації.	
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.	☒	Моніторинг та аудит кібербезпеки	При вивченні дисципліни використовуються: Дидактичні методи - лекції з використанням мультимедійних презентацій. Практичні методи: лабораторні з використанням прикладного програмного забезпечення. Метод самостійного навчання. Активні методи: експрес опитування, тестування. Словесні методи навчання: лекції, консультації.	Поточний контроль: у формі фронтального, індивідуального чи комбінованого контролю знань здобувачів вищої освіти під час лекційного та лабораторного заняття, тестування, колоквіумів. Підсумковий контроль: іспит.
		Кібербезпека	При вивченні дисципліни використовуються: Дидактичні методи - лекції з використанням мультимедійних презентацій. Практичні методи: лабораторні роботи з використанням прикладного програмного забезпечення. Метод самостійного навчання. Активні методи: експрес опитування, тестування. Словесні методи навчання: лекції, консультації.	Поточний контроль: у формі фронтального, індивідуального чи комбінованого контролю знань здобувачів вищої освіти під час лекційного та лабораторного заняття, тестування, колоквіумів. Підсумковий контроль: іспит.
		Кібербезпека об'єктів критичної інфраструктури	Дидактичні методи – лекції з використанням мультимедійних презентацій. Практичні методи: лабораторні роботи з розробки та використанням прикладного програмного забезпечення та практичні завдання. Метод самостійного навчання. Активні методи: експрес опитування, фронтальне опитування. Словесні методи навчання: лекції, консультації.	Поточний контроль: у формі фронтального, індивідуального чи комбінованого контролю знань здобувачів вищої освіти під час лекційного та лабораторного заняття, тестування, колоквіумів. Підсумковий контроль: іспит.
		Проектування систем кібербезпеки (в т.ч. курсова робота)	При вивченні дисципліни використовуються: Дидактичні методи - лекції з використанням мультимедійних презентацій. Практичні методи: лабораторні та практичні роботи з використанням прикладного програмного забезпечення. Метод самостійного навчання. Активні методи: експрес опитування, тестування. Словесні методи навчання: лекції, консультації. Виконання індивідуального завдання у формі курсової роботи.	Поточний контроль: у формі фронтального, індивідуального чи комбінованого контролю знань здобувачів вищої освіти під час лекційного та лабораторного заняття, тестування, колоквіумів. Підсумковий контроль: іспит. Оцінювання курсових робіт проводиться у формі їх публічного захисту на відкритому засіданні комісії за участю керівника курсової роботи та ще не менше одного викладача кафедри.
		Переддипломна практика	Виконання індивідуальних завдань практики	Підсумковий контроль знань здобувачів вищої освіти проводиться шляхом аналізу звіту та щоденника переддипломної практики, а також індивідуального опитування здобувачів вищої освіти під час диференційованого заліку.

		Магістерська кваліфікаційна робота	Виконання індивідуального завдання	Захист магістерської кваліфікаційної роботи
РН11. Аналізувати, контролювати та забезпечувати ефективне функціонування системи управління доступом до інформаційних ресурсів відповідно до встановлених стратегії і політики інформаційної безпеки та/або кібербезпеки організації.	☒	Кібербезпека	При вивченні дисципліни використовуються: Дидактичні методи - лекції з використанням мультимедійних презентацій. Практичні методи: лабораторні роботи з використанням прикладного програмного забезпечення. Метод самостійного навчання. Активні методи: експрес опитування, тестування. Словесні методи навчання: лекції, консультації.	Поточний контроль: у формі фронтального, індивідуального чи комбінованого контролю знань здобувачів вищої освіти під час лекційного та лабораторного заняття, тестування, колоквіумів. Підсумковий контроль: іспит.
		Кібербезпека об'єктів критичної інфраструктури	Дидактичні методи – лекції з використанням мультимедійних презентацій. Практичні методи: лабораторні роботи з розробки та використанням прикладного програмного забезпечення та практичні завдання. Метод самостійного навчання. Активні методи: експрес опитування, фронтальне опитування. Словесні методи навчання: лекції, консультації.	Поточний контроль: у формі фронтального, індивідуального чи комбінованого контролю знань здобувачів вищої освіти під час лекційного та лабораторного заняття, тестування, колоквіумів. Підсумковий контроль: іспит.
		Проектування систем кібербезпеки (в т.ч. курсова робота)	При вивченні дисципліни використовуються: Дидактичні методи - лекції з використанням мультимедійних презентацій. Практичні методи: лабораторні та практичні роботи з використанням прикладного програмного забезпечення. Метод самостійного навчання. Активні методи: експрес опитування, тестування. Словесні методи навчання: лекції, консультації. Виконання індивідуального завдання у формі курсової роботи.	Поточний контроль: у формі фронтального, індивідуального чи комбінованого контролю знань здобувачів вищої освіти під час лекційного та лабораторного заняття, тестування, колоквіумів. Підсумковий контроль: іспит. Оцінювання курсових робіт проводиться у формі їх публічного захисту на відкритому засіданні комісії за участю керівника курсової роботи та ще не менше одного викладача кафедри.
		Моніторинг та аудит кібербезпеки	При вивченні дисципліни використовуються: Дидактичні методи - лекції з використанням мультимедійних презентацій. Практичні методи: лабораторні з використанням прикладного програмного забезпечення. Метод самостійного навчання. Активні методи: експрес опитування, тестування. Словесні методи навчання: лекції, консультації.	Поточний контроль: у формі фронтального, індивідуального чи комбінованого контролю знань здобувачів вищої освіти під час лекційного та лабораторного заняття, тестування, колоквіумів. Підсумковий контроль: іспит.
		Переддипломна практика	Виконання індивідуальних завдань практики	Підсумковий контроль знань здобувачів вищої освіти проводиться шляхом аналізу звіту та щоденника переддипломної практики, а також індивідуального опитування здобувачів вищої освіти під час

				диференційованого заліку.
РН14. Аналізувати, розробляти і супроводжувати систему аудиту та моніторингу ефективності функціонування інформаційних систем і технологій, бізнес\операційних процесів у сфері інформаційної та\або кібербезпеки в цілому.	☒	Проектування систем кібербезпеки (в т.ч. курсова робота)	При вивченні дисципліни використовуються: Дидактичні методи - лекції з використанням мультимедійних презентацій. Практичні методи: лабораторні та практичні роботи з використанням прикладного програмного забезпечення. Метод самостійного навчання. Активні методи: експрес опитування, тестування. Словесні методи навчання: лекції, консультації. Виконання індивідуального завдання у формі курсової роботи.	Поточний контроль: у формі фронтального, індивідуального чи комбінованого контролю знань здобувачів вищої освіти під час лекційного та лабораторного заняття, тестування, колоквіумів. Підсумковий контроль: іспит. Оцінювання курсових робіт проводиться у формі їх публічного захисту на відкритому засіданні комісії за участю керівника курсової роботи та ще не менше одного викладача кафедри.
		Кібербезпека	При вивченні дисципліни використовуються: Дидактичні методи - лекції з використанням мультимедійних презентацій. Практичні методи: лабораторні роботи з використанням прикладного програмного забезпечення. Метод самостійного навчання. Активні методи: експрес опитування, тестування. Словесні методи навчання: лекції, консультації.	Поточний контроль: у формі фронтального, індивідуального чи комбінованого контролю знань здобувачів вищої освіти під час лекційного та лабораторного заняття, тестування, колоквіумів. Підсумковий контроль: іспит.
		Моніторинг та аудит кібербезпеки	При вивченні дисципліни використовуються: Дидактичні методи - лекції з використанням мультимедійних презентацій. Практичні методи: лабораторні з використанням прикладного програмного забезпечення. Метод самостійного навчання. Активні методи: експрес опитування, тестування. Словесні методи навчання: лекції, консультації.	Поточний контроль: у формі фронтального, індивідуального чи комбінованого контролю знань здобувачів вищої освіти під час лекційного та лабораторного заняття, тестування, колоквіумів. Підсумковий контроль: іспит.
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.	☒	Інноваційні та психологічні аспекти сучасної освіти	Лекція, проблемна лекція, демонстрація, зокрема, з використанням мультимедійних засобів навчання, метод самостійного навчання, мікровикладання здобувачів, груповий проєкт (аналіз кейсів), навчальне есе, доповідь науково-дослідного характеру (зокрема, на щорічну науково-технічну конференцію викладачів, співробітників та студентів ВНТУ), тестування (електронне, в системі JetIQ).	Поточний контроль: у формі фронтального, індивідуального чи комбінованого контролю знань здобувачів під час лекційного та практичного заняття, тестування, колоквіумів. Підсумковий контроль: враховуються результати всіх видів навчальної роботи згідно із структурою кредитів. Оцінювання рівня виконання індивідуальної роботи викладач здійснює на основі перевірки змісту роботи та її захисту у формі доповіді. Підсумковий контроль знань студентів проводиться шляхом складання недиференційованого заліку за темами, що охоплюють весь курс дисципліни. Недиференційований залік може проводитись за допомогою усного

				опитування та/або тестів у електронній системі університету та додаткової письмової роботи.
		Ділова іноземна мова	Розповідь-пояснення, бесіда, ілюстрація, демонстрація, зокрема, з використанням мультимедійних засобів навчання, практичні роботи, підготовка доповідей науково-дослідного характеру, зокрема, на щорічну науково-технічну конференцію викладачів, співробітників та студентів ВНТУ.	Поточний контроль: у формі фронтального, індивідуального чи комбінованого контролю знань студентів під час практичного заняття, тестування. Підсумковий контроль: залік.
		Методологія та організація наукових досліджень в кібербезпеці	Лекція, проблемна лекція, дискусія, ІТ-методи, командна робота, демонстрація, зокрема, з використанням мультимедійних засобів навчання, Internet-ресурсів, інформаційних баз, методичних розробок, спеціальної навчальної та наукової літератури, практичні заняття з використанням комп'ютерного обладнання, виконання проблемно-орієнтованих, пошукових, творчих завдань, пошук і аналіз літератури та електронних джерел інформації по заданій проблемі та обраній темі випускної кваліфікаційної роботи, елементи наукових досліджень.	Поточний контроль: у формі фронтального, індивідуального чи комбінованого контролю знань студентів під час практичного заняття, оцінювання самостійного виконання індивідуальних завдань, тестування, тренінг проводиться з метою формування вмінь і навичок у студентів практичного спрямування, формування сучасного наукового мислення, вміння приймати відповідальні та ефективні рішення; самостійна робота дозволяє виявити вміння чітко, логічно і послідовно відповідати на поставлені запитання, вміння працювати самостійно; індивідуальна науково-дослідна робота студентів (ІНДР) проводиться з метою отримання практичних навичок та умінь щодо використання та опрацювання наукових джерел, написання статей, тез, оформлення звітів, розроблення презентаційного матеріалу, використання теоретичних та емпіричних методів дослідження. Підсумковий контроль: іспит.
		Моніторинг та аудит кібербезпеки	При вивченні дисципліни використовуються: Дидактичні методи - лекції з використанням мультимедійних презентацій. Практичні методи: лабораторні з використанням прикладного програмного забезпечення. Метод самостійного навчання. Активні методи: експрес опитування, тестування. Словесні методи навчання: лекції, консультації.	Поточний контроль: у формі фронтального, індивідуального чи комбінованого контролю знань здобувачів вищої освіти під час лекційного та лабораторного заняття, тестування, колоквіумів. Підсумковий контроль: іспит.
		Переддипломна практика	Виконання індивідуальних завдань практики	Підсумковий контроль знань здобувачів вищої освіти проводиться шляхом аналізу звіту та щоденника переддипломної практики, а також індивідуального опитування здобувачів

				вищої освіти під час диференційованого заліку.
		Магістерська кваліфікаційна робота	Виконання індивідуального завдання	Захист магістерської кваліфікаційної роботи
		Філософія науки і техніки	При вивченні дисципліни використовуються: Дидактичні методи – лекції з використанням мультимедійних презентацій. Практичні методи: практичні завдання. Метод самостійного навчання. Активні методи: експрес опитування, тестування. Словесні методи навчання: лекції, консультації.	Поточний контроль: фронтальний, індивідуальний чи комбінований контроль знань здобувачів під час лекційного та практичного заняття, тестування, колоквіумів. Підсумковий контроль: залік
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 оптимізації, прогнозування та прийняття рішень.	☒	Методологія та організація наукових досліджень в кібербезпеці	Лекція, проблемна лекція, дискусія, ІТ-методи, командна робота, демонстрація, зокрема, з використанням мультимедійних засобів навчання, Internet-ресурсів, інформаційних баз, методичних розробок, спеціальної навчальної та наукової літератури, практичні заняття з використанням комп'ютерного обладнання, виконання проблемно-орієнтованих, пошукових, творчих завдань, пошук і аналіз літератури та електронних джерел інформації по заданій проблемі та обраній темі випускної кваліфікаційної роботи, елементи наукових досліджень.	Поточний контроль: у формі фронтального, індивідуального чи комбінованого контролю знань студентів під час практичного заняття, оцінювання самостійного виконання індивідуальних завдань, тестування, тренінг проводиться з метою формування вмінь і навичок у студентів практичного спрямування, формування сучасного наукового мислення, вміння приймати відповідальні та ефективні рішення; самостійна робота дозволяє виявити вміння чітко, логічно і послідовно відповідати на поставлені запитання, вміння працювати самостійно; індивідуальна науково-дослідна робота студентів (ІНДР) проводиться з метою отримання практичних навичок та умінь щодо використання та опрацювання наукових джерел, написання статей, тез, оформлення звітів, розроблення презентаційного матеріалу, використання теоретичних та емпіричних методів дослідження. Підсумковий контроль: іспит.
		Кібербезпека	При вивченні дисципліни використовуються: Дидактичні методи - лекції з використанням мультимедійних презентацій. Практичні методи: лабораторні роботи з використанням прикладного програмного забезпечення. Метод самостійного навчання. Активні методи: експрес опитування, тестування. Словесні методи навчання: лекції, консультації.	Поточний контроль: у формі фронтального, індивідуального чи комбінованого контролю знань здобувачів вищої освіти під час лекційного та лабораторного заняття, тестування, колоквіумів. Підсумковий контроль: іспит.
		Кібербезпека об'єктів критичної інфраструктури	Дидактичні методи – лекції з використанням мультимедійних презентацій. Практичні методи: лабораторні роботи з розробки та	Поточний контроль: у формі фронтального, індивідуального чи комбінованого контролю знань здобувачів вищої освіти під час лекційного та

			використанням прикладного програмного забезпечення та практичні завдання. Метод самостійного навчання. Активні методи: експрес опитування, фронтальне опитування. Словесні методи навчання: лекції, консультації.	лабораторного заняття, тестування, колоквіумів. Підсумковий контроль: іспит.
		Проектування систем кібербезпеки (в т.ч. курсова робота)	При вивченні дисципліни використовуються: Дидактичні методи - лекції з використанням мультимедійних презентацій. Практичні методи: лабораторні та практичні роботи з використанням прикладного програмного забезпечення. Метод самостійного навчання. Активні методи: експрес опитування, тестування. Словесні методи навчання: лекції, консультації. Виконання індивідуального завдання у формі курсової роботи.	Поточний контроль: у формі фронтального, індивідуального чи комбінованого контролю знань здобувачів вищої освіти під час лекційного та лабораторного заняття, тестування, колоквіумів. Підсумковий контроль: іспит. Оцінювання курсових робіт проводиться у формі їх публічного захисту на відкритому засіданні комісії за участю керівника курсової роботи та ще не менше одного викладача кафедри.
		Моніторинг та аудит кібербезпеки	При вивченні дисципліни використовуються: Дидактичні методи - лекції з використанням мультимедійних презентацій. Практичні методи: лабораторні з використанням прикладного програмного забезпечення. Метод самостійного навчання. Активні методи: експрес опитування, тестування. Словесні методи навчання: лекції, консультації.	Поточний контроль: у формі фронтального, індивідуального чи комбінованого контролю знань здобувачів вищої освіти під час лекційного та лабораторного заняття, тестування, колоквіумів. Підсумковий контроль: іспит.
		Переддипломна практика	Виконання індивідуальних завдань практики	Підсумковий контроль знань здобувачів вищої освіти проводиться шляхом аналізу звіту та щоденника переддипломної практики, а також індивідуального опитування здобувачів вищої освіти під час диференційованого заліку.
		Магістерська кваліфікаційна робота	Виконання індивідуального завдання	Захист магістерської кваліфікаційної роботи
РН8. Досліджувати, розробляти і супроводжувати системи та засоби інформаційної безпеки та/або кібербезпеки на об'єктах інформаційної діяльності та критичної інфраструктури.	☒	Кібербезпека	При вивченні дисципліни використовуються: Дидактичні методи - лекції з використанням мультимедійних презентацій. Практичні методи: лабораторні роботи з використанням прикладного програмного забезпечення. Метод самостійного навчання. Активні методи: експрес опитування, тестування. Словесні методи навчання: лекції, консультації.	Поточний контроль: у формі фронтального, індивідуального чи комбінованого контролю знань здобувачів вищої освіти під час лекційного та лабораторного заняття, тестування, колоквіумів. Підсумковий контроль: іспит.
		Кібербезпека об'єктів критичної інфраструктури	Дидактичні методи – лекції з використанням мультимедійних презентацій. Практичні методи: лабораторні роботи	Поточний контроль: у формі фронтального, індивідуального чи комбінованого контролю знань здобувачів вищої

			з розробки та використанням прикладного програмного забезпечення та практичні завдання. Метод самостійного навчання. Активні методи: експрес опитування, фронтальне опитування. Словесні методи навчання: лекції, консультації.	освіти під час лекційного та лабораторного заняття, тестування, колоквіумів. Підсумковий контроль: іспит.
		Проектування систем кібербезпеки (в т.ч. курсова робота)	При вивченні дисципліни використовуються: Дидактичні методи - лекції з використанням мультимедійних презентацій. Практичні методи: лабораторні та практичні роботи з використанням прикладного програмного забезпечення. Метод самостійного навчання. Активні методи: експрес опитування, тестування. Словесні методи навчання: лекції, консультації. Виконання індивідуального завдання у формі курсової роботи.	Поточний контроль: у формі фронтального, індивідуального чи комбінованого контролю знань здобувачів вищої освіти під час лекційного та лабораторного заняття, тестування, колоквіумів. Підсумковий контроль: іспит. Оцінювання курсових робіт проводиться у формі їх публічного захисту на відкритому засіданні комісії за участю керівника курсової роботи та ще не менше одного викладача кафедри.
		Переддипломна практика	Виконання індивідуальних завдань практики	Підсумковий контроль знань здобувачів вищої освіти проводиться шляхом аналізу звіту та щоденника переддипломної практики, а також індивідуального опитування здобувачів вищої освіти під час диференційованого заліку.
		Магістерська кваліфікаційна робота	Виконання індивідуального завдання	Захист магістерської кваліфікаційної роботи
		Сучасні системи, технології та засоби інформаційної безпеки та кібербезпеки	При вивченні дисципліни використовуються: Дидактичні методи - лекції з використанням мультимедійних презентацій. Практичні методи: лабораторні роботи з використанням прикладного програмного забезпечення. Метод самостійного навчання. Активні методи: експрес опитування, тестування. Словесні методи навчання: лекції, консультації.	Поточний контроль: у формі фронтального, індивідуального чи комбінованого контролю знань студентів під час лекційного та лабораторного заняття, тестування, колоквіумів. Оцінювання результатів виконання індивідуального завдання здійснюється на основі перевірки змісту реферату та його подання у формі доповіді. Підсумковий контроль: іспит.
РН6. Аналізувати та оцінювати захищеність систем, комплексів та засобів кіберзахисту, технології створення та використання спеціалізованого програмного забезпечення.	☒	Магістерська кваліфікаційна робота	Виконання індивідуального завдання	Захист магістерської кваліфікаційної роботи
		Сучасні системи, технології та засоби інформаційної безпеки та кібербезпеки	При вивченні дисципліни використовуються: Дидактичні методи - лекції з використанням мультимедійних презентацій. Практичні методи: лабораторні роботи з використанням прикладного програмного забезпечення. Метод самостійного навчання. Активні методи: експрес опитування, тестування. Словесні методи навчання: лекції, консультації.	Поточний контроль: у формі фронтального, індивідуального чи комбінованого контролю знань студентів під час лекційного та лабораторного заняття, тестування, колоквіумів. Оцінювання результатів виконання індивідуального завдання здійснюється на основі перевірки змісту реферату та його подання у формі доповіді. Підсумковий контроль: іспит.

		Кібербезпека	При вивченні дисципліни використовуються: Дидактичні методи - лекції з використанням мультимедійних презентацій. Практичні методи: лабораторні роботи з використанням прикладного програмного забезпечення. Метод самостійного навчання. Активні методи: експрес опитування, тестування. Словесні методи навчання: лекції, консультації.	Поточний контроль: у формі фронтального, індивідуального чи комбінованого контролю знань здобувачів вищої освіти під час лекційного та лабораторного заняття, тестування, колоквіумів. Підсумковий контроль: іспит.
		Моніторинг та аудит кібербезпеки	При вивченні дисципліни використовуються: Дидактичні методи - лекції з використанням мультимедійних презентацій. Практичні методи: лабораторні з використанням прикладного програмного забезпечення. Метод самостійного навчання. Активні методи: експрес опитування, тестування. Словесні методи навчання: лекції, консультації.	Поточний контроль: у формі фронтального, індивідуального чи комбінованого контролю знань здобувачів вищої освіти під час лекційного та лабораторного заняття, тестування, колоквіумів. Підсумковий контроль: іспит.
		Переддипломна практика	Виконання індивідуальних завдань практики	Підсумковий контроль знань здобувачів вищої освіти проводиться шляхом аналізу звіту та щоденника переддипломної практики, а також індивідуального опитування здобувачів вищої освіти під час диференційованого заліку.