

ВІДОМОСТІ
про самооцінювання освітньої програми

Заклад вищої освіти	Державний університет інтелектуальних технологій і зв'язку
Освітня програма	78541 Кібербезпека та захист інформації
Рівень вищої освіти	Магістр
Спеціальність	F5 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	5780
Повна назва ЗВО	Державний університет інтелектуальних технологій і зв'язку
Ідентифікаційний код ЗВО	43997335
ПІБ керівника ЗВО	Назаренко Олександр Аскольдович
Посилання на офіційний веб-сайт ЗВО	https://suitt.edu.ua/

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

<https://registry.edbo.gov.ua/university/5780>

3. Загальна інформація про ОП, яка подається на акредитацію

ID освітньої програми в ЄДЕБО	78541
Назва ОП	Кібербезпека та захист інформації
Галузь знань	F Інформаційні технології
Спеціальність	F5 Кібербезпека та захист інформації
Спеціалізація (за наявності)	<i>відсутня</i>
Рівень вищої освіти	Магістр
Тип освітньої програми	Освітньо-професійна
Вступ на освітню програму здійснюється на основі ступеня (рівня)	Бакалавр, Магістр (ОКР «спеціаліст»)
Структурний підрозділ (кафедра або інший підрозділ), відповідальний за реалізацію ОП	Кафедра Кібербезпеки та технічного захисту інформації
Інші навчальні структурні підрозділи (кафедра або інші підрозділи), залучені до реалізації ОП	Кафедри менеджменту та маркетингу, кіберпсихології та реабілітації, лінгводидактики та іноземних мов
Місце (адреса) провадження освітньої діяльності за ОП	м.Одеса, вул. Кузнечна, 1
Освітня програма передбачає присвоєння професійної кваліфікації	<i>не передбачає</i>
Професійна кваліфікація, яка присвоюється за ОП (за наявності)	<i>відсутня</i>
Мова (мови) викладання	Українська
ID гаранта ОП у ЄДЕБО	388823
ПІБ гаранта ОП	Кільдішев Віталій Йосипович
Посада гаранта ОП	Доцент
Корпоративна електронна адреса гаранта ОП	v.y_kildishev@suitt.edu.ua
Контактний телефон гаранта ОП	+38(068)-202-76-45
Додатковий телефон гаранта ОП	+38(063)-011-46-86

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

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

У 2018 році було створено освітньо-професійну програму «Кібербезпека» підготовки здобувачів вищої освіти другого (магістерського) рівня за спеціальністю 125 Кібербезпека, галузі знань 12 Інформаційні технології. У 2019 році програма 125 Кібербезпека була акредитована на 5 років.

У 2022 році було вирішено оновити дану ОП відповідно до вимог нового професійного стандарту «Фахівець сфери захисту інформації» (за підтримки проєкту Агентства USAID «Кібербезпека критично важливої інфраструктури України» (https://www.facebook.com/CyberActivityUA/?locale=uk_UA, <https://suitt.edu.ua/wp-content/uploads/2024/10/porivnialni-tablytsi-kompetentsij-dlia-dystsyplin-op.pdf>).

Таким чином, було створено робочу групу з оновлення ОП (<https://suitt.edu.ua/wp-content/uploads/2024/10/sklad-robochoi-grupy-dlia-onovlennia-op.pdf>), дії якої полягали у наступному: визначення основних потреб ринку, стану ресурсного забезпечення ЗВО та кафедри, аналіз наявних професійних стандартів (<https://suitt.edu.ua/wp-content/uploads/2024/10/dii-z-onovlennia-osvitnoi-prohramy.pdf>). Після аналізу професійного стандарту було визначено основні компетентності, які було доцільним включити до нової освітньої програми, а саме: було додано 7 фахових компетентностей та 11 програмних результатів навчання; створено опис вимог до ОП (<https://suitt.edu.ua/wp-content/uploads/2024/10/vymohy-do-osvitnoi-prohramy.pdf>). На цій основі ОП було оновлено у 2023 році (https://suitt.edu.ua/wp-content/uploads/2024/10/opp_kb_mah_2023_duitz_draft.pdf). ОП відповідала більшості рекомендацій: як від USAID, так й стейкхолдерів (<https://suitt.edu.ua/wp-content/uploads/2024/10/perelik-komentariv-ta-propozitsij-vid-steykholderiv.pdf>).

У 2024 році було вирішено знову оновити дану ОП, а саме приділити увагу оновленню деяких її основних освітніх компонентів (https://suitt.edu.ua/wp-content/uploads/2024/10/opp_kb_mah_2024.pdf). Таким чином, ця ОП зазнала у 2024 р. деяких змін: було змінено зміст декількох освітніх компонентів, додано ОК11 – «Ділова іноземна мова», а також змінено навчальний план – 3 дисципліни для здобувачів вступу 2024 р. викладаються на 2 курсі магістратури. У зв'язку з відокремленням у 2024 році підготовки з управління інформаційною безпекою в окрему спеціальність у межах галузі знань К – «Безпека та оборона», у 2025 р. було вирішено об'єднати дві відповідні освітні компоненти «Менеджмент інформаційної безпеки» та «Процесний менеджмент в системі корпоративної безпеки» та скоротити їх обсяг у кредитах. Водночас управлінська складова залишається важливою для спеціальності F5 «Кібербезпека та захист інформації», тому в оновленій ОП передбачено освітній компонент «Менеджмент в системі корпоративної інформаційної безпеки» обсягом 5 кредитів (<https://suitt.edu.ua/wp-content/uploads/2026/09/opp-2025-f5-mah-proiekt-2.pdf>). У 2024 році програма 125 Кібербезпека та захист інформації була акредитована на 1 рік.

За рекомендаціями стейкхолдерів у 2026 р. було змінено назву освітнього компонента «Спеціальні вимірювання в галузі технічного захисту інформації» на «Комплекси технічного захисту інформації» з метою приведення назви компонента у відповідність до його сучасної спрямованості та змісту.

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

Рік навчання	Навчальний рік, у якому відбувся набір здобувачів відповідного року навчання	Обсяг набору на ОП у відповідному навчальному році	Контингент студентів на відповідному році навчання станом на 1 жовтня поточного навчального року		У тому числі іноземців	
			ОД	З	ОД	З
1 курс	2026 - 2027	75	17	8	0	0
2 курс	2025 - 2026	75	29	15	0	0

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

6. Інформація про інші ОП ЗВО за відповідною спеціальністю

Рівень вищої освіти	Інформація про освітні програми
початковий рівень (короткий цикл)	програми відсутні
перший (бакалаврський) рівень	програми відсутні
другий (магістерський) рівень	78541 Кібербезпека та захист інформації
третій (освітньо-науковий/освітньо-творчий) рівень	програми відсутні

7. Інформація про площі приміщень ЗВО станом на момент подання відомостей про

самооцінювання, кв. м.

	Загальна площа	Навчальна площа
Усі приміщення ЗВО	61587	29576
Власні приміщення ЗВО (на праві власності, господарського відання або оперативного управління)	61587	29576
Приміщення, які використовуються на іншому праві, ніж право власності, господарського відання або оперативного управління (оренда, безоплатне користування тощо)	0	0
Приміщення, здані в оренду	574	0

Примітка. Для ЗВО із ВСП інформація зазначається:

- ☐ щодо ОП, яка реалізується у базовому ЗВО – без урахування приміщень ВСП;
- ☐ щодо ОП, яка реалізується у ВСП – лише щодо приміщень даного ВСП.

8. Документи щодо ОП

Документ	Назва файла	Хеш файла
Освітня програма	<i>opp_m_f5_kiberbezpeka_ta_zakhys_t_informatsii_2026_1.pdf</i>	cIVMEiOuUbQvcYoYKkcVYfZD+Ta7GLd6dgTHzAHJmKE=
Навчальний план за ОП	<i>m_np_f5_denno_2026-2.pdf</i>	geGCQo1TBXJJJo/PGA7ByrvcXOb4meurtJDtXhB1RgEo=
Навчальний план за ОП	<i>m_np_f5_zaochna_2026-2.pdf</i>	7QO82Fnt7r2DoM8LxfgrkoOpRoNrLEHJFR1//o+DrA=
Матеріали від ЗВО: пропозиції та рекомендації від роботодавців, таблиця відповідності публікацій наукових керівників напрямом (тематикам) досліджень аспірантів (для ОП третього рівня освіти)	<i>Рецензія_КОБІ-2026-F.pdf</i>	MCENkQERfVnR9lQ+ONGS/zsVeRw9VXjyU1D/nPxtlMg=
Матеріали від ЗВО: пропозиції та рекомендації від роботодавців, таблиця відповідності публікацій наукових керівників напрямом (тематикам) досліджень аспірантів (для ОП третього рівня освіти)	<i>Рецензія-ACK-2026_F.pdf</i>	d2wsTRu7uiTdfN4crho1PNVKu6ZOMiMc1Fkouvi/b2k=
Матеріали від ЗВО: пропозиції та рекомендації від роботодавців, таблиця відповідності публікацій наукових керівників напрямом (тематикам) досліджень аспірантів (для ОП третього рівня освіти)	<i>Рецензія-БОШ-2026_F.pdf</i>	TXGJ1p55FycPoXHvqQR+fpq1ogo5CCmT9E7h6FiVGgs=

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?

У зв'язку з відсутністю Стандарту за спеціальністю F5 «Кібербезпека та захист інформації» для другого (магістерського) рівня вищої освіти, під час розробки ОПП за основу взято компетентності та результати навчання, визначені Стандартом вищої освіти за спеціальністю 125 «Кібербезпека» для другого рівня вищої освіти, затвердженим наказом Міністерства освіти і науки України № 332 від 18.03.2021 року. Слід зазначити, що член групи забезпечення цієї ОП - професор Василіу Є.В. – з 2019 по 2024 р. був членом Науково-методичної комісії Сектору вищої освіти Науково-методичної ради МОН України, підкомісія 125 "Кібербезпека", і брав участь у розробленні стандарту вищої освіти за спеціальністю 125 Кібербезпека другого (магістерського) рівня вищої освіти (затверджено наказом МОН України 18.03.2021 р., № 332).

Визначені в ОПП програмні результати навчання відповідають вимогам Національної рамки кваліфікацій для 7-го

кваліфікаційного рівня, що відповідає другому (магістерському) рівню вищої освіти. Відповідність забезпечується за основними дескрипторами НРК:

- знання – ПРН передбачають набуття та застосування спеціалізованих концептуальних і практичних знань, критичне осмислення теорій, принципів, методів і понять у сфері інформаційної та кібербезпеки, а також інтеграцію фундаментальних і спеціальних знань для розв'язання складних і мультидисциплінарних задач (ПРН2–ПРН8, ПРН20–ПРН23);
- уміння/навички – ПРН передбачають здатність розв'язувати складні професійні та дослідницькі задачі, проводити дослідження, застосовувати сучасні методи і технології, розробляти та впроваджувати системи і засоби кібербезпеки, працювати в умовах складності, невизначеності та неповної інформації (ПРН3–ПРН14, ПРН16, ПРН19–ПРН33);
- комунікація – ПРН забезпечують здатність усно і письмово представляти результати професійної та дослідницької діяльності, зрозуміло доносити висновки, знання та аргументацію до фахівців і нефахівців, здійснювати професійне спілкування українською та іноземною мовами (ПРН1, ПРН15, ПРН18, ПРН34);
- відповідальність і автономія – ПРН передбачають здатність приймати обґрунтовані рішення у складних і непередбачуваних умовах, здійснювати самостійне навчання та професійний розвиток, планувати і виконувати дослідження, керувати професійною діяльністю та відповідати за результати прийнятих рішень (ПРН16–ПРН22, ПРН24, ПРН34).

Таким чином, сукупність програмних результатів навчання ОПП охоплює всі основні дескриптори 7-го кваліфікаційного рівня НРК та забезпечує формування необхідних знань, умінь і навичок, комунікаційних компетентностей, а також здатності до самостійної професійної, дослідницької та інноваційної діяльності. Кожен визначений ПРН забезпечується відповідними освітніми компонентами ОПП, що відображено у матриці забезпечення програмних результатів навчання.

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

Зміст ОПП враховує вимоги професійного стандарту «Фахівець сфери захисту інформації». Під час оновлення ОПП проаналізовано трудові функції, професійні компетентності, знання та уміння, визначені стандартом, та адаптовано їх до змісту підготовки здобувачів вищої освіти (<https://suitt.edu.ua/wp-content/uploads/2024/10/porivnialni-tablytsi-kompetentsij-dlia-dystyplin-op.pdf>). За результатами аналізу до ОПП включено 7 фахових компетентностей та 11 програмних результатів навчання (наприклад, ПРН30. Проводити сканування вразливостей і розпізнання вразливостей в ІКС і системах безпеки).

Чи мета освітньої програми та програмні результати навчання визначаються з урахуванням потреб заінтересованих сторін (стейкхолдерів)?

- здобувачі вищої освіти та випускники програми

Регулярні зустрічі зі стейкхолдерами, зокрема представниками роботодавців та випускниками програми, проводяться для врахування змін у галузі кібербезпеки та захисту інформації. Під час оновлення ОПП враховано пропозиції здобувачів вищої освіти, отримані за результатами їх опитування щодо змісту магістерської програми та освітніх компонентів за 2025 р. (<https://drive.google.com/file/d/1wlGZFCbZfCpAT4lwLes9zzZOGJPpOQ7K/view>) та 2026 р. (https://suitt.edu.ua/wp-content/uploads/2026/06/4_f5_informats_anal_dovidka_zdobuvachi_vyshchoi_oshvity_mahistry_f5_kiberbezpeka-2.pdf). Зокрема, відповідні пропозиції були враховані під час перегляду ОК5 «Менеджмент в системі корпоративної інформаційної безпеки».

- роботодавці

Під час оновлення ОП були враховані пропозиції:

ТОВ «КОБІ СС» (<https://kobi.ua/>);

ГО «Асоціація спеціалістів кібербезпеки» (<https://scsa.org.ua>);

ТОВ «Роберт Бош ЛТД» (<https://www.bosch.ua>).

У процесі обговорення проєкту ОП було взято до уваги усі зауваження та пропозиції представників даних організацій (<https://suitt.edu.ua/reformuvannia-opp/>). На підприємствах роботодавців налагоджено проходження практики здобувачами вищої освіти цієї ОП, тому роботодавці вносять пропозиції щодо оновлення/включення тих чи інших освітніх компонент в освітню програму, ґрунтуючись на потребах власного виробництва. Гарант ОП та робоча група намагаються враховувати дані пропозиції.

Кафедра Кібербезпеки та технічного захисту інформації (КБ та ТЗІ) постійно веде роботу над розширенням списку таких підприємств. Реєстр стейкхолдерів на даний час <https://suitt.edu.ua/partnery-ta-stejkholdery/>.

- академічна спільнота

Врахування інтересів академічної спільноти здійснюється під час роботи робочої групи, засідань кафедри та обговорення пропозицій щодо вдосконалення ОПП (<https://suitt.edu.ua/reformuvannia-opp/>). На кафедрі регулярно обговорюються тенденції розвитку підготовки фахівців у сфері кібербезпеки та захисту інформації, результати чого враховуються під час подальшого оновлення ОПП (<https://suitt.edu.ua/reformuvannia-opp/> підрозділ "Рішення кафедри про оновлення освітньої програми").

- інші стейкхолдери

Пропозицій від інших стейкхолдерів не надходило.

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

Місія ДУІТЗ (<https://suitt.edu.ua/misiia-ta-viziia/>).

Стратегія ДУІТЗ (https://suitt.edu.ua/wp-content/uploads/2023/01/Strategiya-razvitiya_compressed.pdf).

Однією із складових стратегії ДУІТЗ є реформування лабораторної бази університету, а саме модернізація навчальних та лабораторних корпусів, створення сучасних лабораторій з тестування, дослідження та експлуатації технологій та обладнання провідних виробників з країн-членів ЄС та світу, сертифікаційних лабораторій (<https://suitt.edu.ua/pro-laboratorii-ktzi/>), що є й однією з цілей цієї ОП, оскільки підготовка професіоналів, здатних забезпечувати захищеність інформації, потребує відповідної лабораторної бази. На базі кафедри КБ та ТЗІ вже існують такі лабораторії, які постійно вдосконалюються та розширюються.

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

Мета та програмні результати навчання освітньої програми визначаються з урахуванням розвитку науки та спеціальності. Однією з цілей програми є інтеграція науково-дослідної роботи кафедри кібербезпеки та технічного захисту інформації в навчальний процес. Програма орієнтується на сучасні міжнародні вимоги та світові наукові досягнення та регулярно оновлюється. Таким чином, у 2023 р. дану програму було оновлено відповідно до професійного стандарту «Фахівець сфери захисту інформації» та пропозицій стейкхолдерів, (<https://suitt.edu.ua/wp-content/uploads/2024/10/dii-z-onovlennia-osvitnoi-prohramy.pdf>, <https://suitt.edu.ua/wp-content/uploads/2024/10/perelik-komentariv-ta-propozysij-vid-stejkkholderiv.pdf>, <https://suitt.edu.ua/wp-content/uploads/2024/10/plan-onovlennia-osvitnoi-prohramy.pdf>), а у 2024 р. на підставі аналізу кафедрою тенденцій розвитку кібербезпеки та опитувань здобувачів внесені додаткові зміни.

Стейкхолдерами запропоновано при подальшому оновленні ОПП посилити практичну складову підготовки здобувачів з питань проєктування та функціонування комплексних систем безпеки. Пропозицію враховано під час оновлення змісту освітнього компонента «Комплексні системи безпеки» у 2025 р. та компонента «Моніторинг та аудит інформаційно-комунікаційних систем» у 2026 р. (<https://suitt.edu.ua/reformuvannia-opp/> підрозділ "Рішення кафедри про оновлення освітньої програми").

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

Мета та програмні результати освітньої програми визначаються з урахуванням тенденцій розвитку ринку праці, галузевого та регіонального контексту. Цілі програми другого (магістерського) рівня вищої освіти, випускники якої стають фахівцями з кібербезпеки та захисту інформації високого рівня, повністю відповідають потребам цієї галузі, регіону та держави в цілому в таких фахівцях. В Одеській області багато державних установ та провідних високотехнологічних компаній, включаючи міжнародні, яким у зв'язку з постійно зростаючою кількістю кібератак потрібні професіонали-аналітики у галузі кібербезпеки та захисту інформації.

Однією з цілей програми є орієнтація на вимоги ринку праці. Програма регулярно переглядається та оновлюється відповідно до змін на ринку праці.

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

При формулюванні мети та програмних результатів ОПП було враховано досвід провідних вітчизняних університетів, зокрема Харківського національного університету імені В. Н. Каразіна, КНУ імені Тараса Шевченка та Національного авіаційного університету. Під час оновлення ОПП було проведено порівняння освітніх компонентів за спеціальністю F5 «Кібербезпека та захист інформації». Зокрема, під час удосконалення змісту ОПП враховано досвід КНУ ім. Тараса Шевченка щодо викладання дисциплін «Аудит інформаційних систем» та «Безпека критичної інформаційної інфраструктури», а НАУ — «Аудит інформаційної безпеки». Досвід ХНУ ім. В. Н. Каразіна враховано під час удосконалення змісту компонента «Моніторинг та аудит інформаційно-комунікаційних систем» з урахуванням відповідних дисциплін ХНУ ім. В. Н. Каразіна «Моніторинг та аудит безпеки та якості інформаційних систем та програмного забезпечення» та «Тестування, моніторинг та аудит інформаційно-комунікаційних систем на наявність загроз».

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

Під час оновлення освітньої програми у 2023-2026 рр. було враховано значний досвід, який отримали викладачі кафедри Кібербезпеки та технічного захисту інформації завдяки участі з 2020 р. у проєкті Агентства USAID "Кібербезпека критично важливої інфраструктури України", зокрема, підвищення кваліфікації в літніх школах для викладачів у 2021 та 2022 рр., які були організовані у межах цього проєкту (https://suitt.edu.ua/wp-content/uploads/2024/10/prez_op_ta_ps.pdf). Також оновлення ОП відповідно до трудових функцій та компетентностей професійного стандарту «Фахівець сфери захисту інформації» є врахуванням міжнародного досвіду, оскільки сам цей стандарт розроблено з урахуванням міжнародних вимог, зокрема стандартів американського NIST.

2. Структура та зміст освітньої програми

Яким є обсяг ОП (у кредитах ЄКТС)?

90

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

66

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

24

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

Зміст освітньо-професійної програми повністю відповідає предметній області заявленої спеціальності, яка охоплює різноманітні аспекти захисту інформації в інформаційних системах, управління інформаційною безпекою, розробку та впровадження технічних і організаційних засобів захисту даних.

Основні компоненти програми спрямовані на підготовку фахівців, здатних вирішувати складні завдання у сфері кібербезпеки та захисту інформації. Наприклад, дисципліна «Криптологія» (ОК8) готує здобувачів до роботи з алгоритмами шифрування, які є ключовим елементом захисту даних. «Кіберфізична безпека об'єктів критичної інфраструктури» (ОК7) навчає здобувачів захищати критичні інформаційно-комунікаційні системи, що є важливим для забезпечення національної безпеки в умовах цифрової трансформації.

Предметна область спеціальності включає вивчення сучасних інформаційних технологій, технічних систем та мереж, що забезпечують збереження, передавання, оброблення та захист інформації від несанкціонованого доступу, кібератак і кіберзагроз. Це охоплює як фізичні засоби захисту інформації, так і сучасні програмні технології для забезпечення кіберзахисту на всіх етапах обробки даних.

ОП забезпечує набуття здобувачами як загальних, так і фахових компетентностей, необхідних для професійної діяльності в галузі кібербезпеки. Наприклад, серед ключових компетентностей можна виділити – СК11, СК13, СК14. Зазначені компетентності відповідають вимогам професійного стандарту «Фахівець сфери захисту інформації», затвердженого Адміністрацією Держспецзв'язку, що визначає основні завдання фахівців у сфері кібербезпеки та захисту інформації.

Програма також передбачає міждисциплінарний підхід, який полягає в інтеграції знань з технічних, організаційних, правових та управлінських аспектів кібербезпеки. Це відображено у таких освітніх компонентах, як «Менеджмент в системі корпоративної інформаційної безпеки» (ОК5), що поєднує знання з управління та технологій захисту інформації, а також з процесного менеджменту, які дають здобувачам змогу застосовувати принципи управління в галузі інформаційної безпеки.

Програма розроблена з урахуванням сучасних вимог ринку праці, що підтверджується участю стейкхолдерів, таких як ГО «Асоціація спеціалістів кібербезпеки», ТОВ «КОБІ СС», а також представників компаній, що працюють у сфері інформаційної безпеки. Це дозволяє забезпечити актуальність програми та відповідність потребам роботодавців.

Освітньо-професійна програма «Кібербезпека та захист інформації» повністю відповідає предметній області заявленої спеціальності F5 «Кібербезпека та захист інформації». Вона забезпечує комплексну підготовку фахівців, здатних вирішувати дослідницькі та інноваційні завдання у сфері кібербезпеки, зокрема захисту критичної інфраструктури та інформаційних систем.

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

Формування індивідуальної освітньої траєкторії унормовується згідно з Положенням про індивідуальну освітню траєкторію здобувачів вищої освіти в ДУІТЗ (https://suitt.edu.ua/wp-content/uploads/2025/12/2.-polozhennia_pro_indyvidualnu_osvitniu_traiektoriiu_zdobuvachiv_vyshchoi.pdf).

Здобувачі вищої освіти мають можливість самостійно формувати свою освітню траєкторію на кожному етапі навчання згідно з Законом України "Про вищу освіту" (пункт 15 частини першої статті 62). Вони можуть обирати навчальні компоненти, орієнтуючись на власні інтереси та потреби. Для кращого розуміння специфіки різних вибірових компонентів викладачі проводять співбесіди, під час яких роз'яснюють компетентності, що розвиваються завдяки вибору тієї чи іншої дисципліни. Також здобувачам надається доступ до навчальних програм і силабусів (<https://suitt.edu.ua/vybirkovi-dystsypliny/>), що дозволяє самостійно обирати компоненти з доступного каталогу. Для формування індивідуальної траєкторії в межах ОП передбачено вибірові дисципліни обсягом 24 кредити ECTS. Формуванням освітньої траєкторії здобувача опікується керівництво факультету, завідувач спеціальної кафедри КБ та ТЗІ та відповідальні за вибір дисциплін здобувачами.

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

Здобувачі мають можливість вибирати вибіркові компоненти загальним обсягом 24 кредитів ECTS із загальної кількості 90 кредитів ECTS, що дозволяє формувати власну індивідуальну навчальну траєкторію. Процедура вибору освітніх компонентів регулюється Положенням про реалізацію права на вільний вибір навчальних дисциплін здобувачами вищої освіти ДУІТЗ (https://suitt.edu.ua/wp-content/uploads/2025/12/5.-polozhennia_pr.pdf). Механізм вибору навчальних дисциплін постійно вдосконалюється для полегшення процесу вибору здобувачами. Здобувачі вибирають дисципліни на основі їхніх інтересів та індивідуальних потреб. Для цього використовується каталог вибіркового навчальних дисциплін (<https://suitt.edu.ua/vybir-kovi-dystypliny/>), що дозволяє здобувачам гнучко підходити до вибору предметів та формувати освітню траєкторію, яка відповідає їх професійним цілям.

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

У програмі та навчальному плані передбачено практичні та лабораторні заняття, виконання курсової роботи, результатом якої є отримання практичних умінь. Курсова робота спрямована на набуття необхідних для майбутньої професійної діяльності навичок.

Також на 1-му та 2-му курсі здобувачі проходять виробничу практику на підприємствах в обсязі 15 кредитів. Метою виробничої практики є досягнення практичних результатів навчання, передбачених в освітній програмі. Положення про порядок проведення практичної підготовки здобувачів вищої освіти ДУІТЗ: https://suitt.edu.ua/wp-content/uploads/2025/12/7.-polozhennia_pro_poriado.pdf

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

Навчальна програма містить компоненти, спрямовані на розвиток соціальних soft-навичок у здобувачів (ЗКЗ, ЗК4, СК10).

Дисципліна «Ділова іноземна мова» (ОК10) дозволяє здобувачам вдосконалити уміння вести переговори та складати ділову документацію іноземною мовою. Дисципліна «Методологія наукових досліджень та академічна доброчесність» (ОК1) сприяє оволодінню методологічними принципами і підходами до наукового дослідження, формуванню методологічної і наукової культури, а також формує здатність виконувати вимоги академічної доброчесності. Курсовий проєкт у дисципліні «Менеджмент в системі корпоративної інформаційної безпеки» (ОК5) передбачає роботу в команді, що сприяє розвитку співпраці та розподілу обов'язків. Виробнича практика (ОК11) дає змогу здобути досвід практичної та командної роботи на підприємствах.

Дисципліни «Менеджмент в системі корпоративної інформаційної безпеки» (ОК5) та «Моніторинг та аудит інформаційно-комунікаційних систем» (ОК9) навчають приймати рішення в умовах невизначеності, аналізувати ризики й вирішувати проблеми кіберзагроз.

Захист магістерської роботи (ОК12) і робота в реальних умовах під час практики допомагають розвивати стресостійкість.

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

Освітня програма має чітку структуру, що забезпечує систематичність і послідовність навчання. Кожен компонент програми відіграє визначену роль у досягненні заявленої мети та програмних результатів навчання. Зміст програми розподілений на обов'язкові та вибіркові дисципліни. Обов'язкові дисципліни забезпечують фундаментальну та спеціальну підготовку, охоплюючи основи відповідної галузі, в той час як вибіркові дисципліни дозволяють здобувачам адаптувати навчання під свої професійні інтереси. Освітні компоненти взаємопов'язані: знання, отримані в одній дисципліні, використовуються і розвиваються в інших. Це створює інтегровану систему, що дозволяє глибше зрозуміти матеріал і застосовувати отримані навички в різних контекстах. Всі освітні компоненти спрямовані на досягнення конкретних результатів навчання, які були визначені як ключові для підготовки кваліфікованих фахівців.

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

В ДУІТЗ обсяг освітньої програми та навантаження здобувачів вимірюються в кредитах ECTS і регулюються відповідно до "Положення про організацію освітнього процесу в ДУІТЗ". При розробці навчальних планів і програм дотримуються встановлених нормативів. Загальний обсяг програми складає 90 кредитів ECTS (2700 годин), де 74% (66 кредитів) становлять обов'язкові компоненти, а 26% (24 кредити) — вибіркові. У навчальному плані за освітньою програмою передбачений такий розподіл годин: 740 годин відводиться на аудиторні заняття, а 1960 годин — на самостійну роботу здобувачів.

Положення про організацію освітнього процесу в ДУІТЗ:

<https://suitt.edu.ua/wp-content/uploads/2025/12/1.-polozhennia-pro-orhanizatsiiu-osvitnoho-protsesu-v-duitz.pdf>

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

Структура освітньої програми «Кібербезпека та захист інформації» забезпечує її практикоорієнтованість через поєднання теоретичних знань і реальних практичних завдань. Основні освітні компоненти, такі як виробнича практика (ОК11) та курсовий проєкт у рамках дисципліни «Менеджмент в системі корпоративної інформаційної безпеки» (ОК5), дають змогу здобувачам застосовувати отримані знання у реальних умовах. Виробнича практика проходить на підприємствах, де здобувачі вирішують завдання кіберзахисту, адаптуючись до потреб ринку.

- Дуальна форма здобуття освіти впроваджується відповідно до Положення про дуальну форму здобуття вищої освіти у ДУІТЗ та передбачає поєднання навчання в Університеті з практичним навчанням на робочих місцях підприємств-партнерів. Для ОПП передбачена можливість реалізації дуальної форми за моделлю поділеного тижня або блочною моделлю:

- модель поділеного тижня (кілька днів протягом тижня в Університеті, інша частина тижня – на робочому місці суб'єкта господарювання за вибіркоким блоком «Дуальна освіта»);
- блочна модель: навчання в Університеті та на робочому місці суб'єкта господарювання за вибіркоким блоком «Дуальна освіта» освітньо-професійної програми спеціальності певного рівня вищої освіти, що затверджена в установленому порядку.

На сьогодні здобувачів за цією ОПП, які навчаються за дуальною формою, немає.

Положення про дуальну форму здобуття вищої освіти у ДУІТЗ

https://suitt.edu.ua/wp-content/uploads/2025/12/6.-polozhennia_pro_du.pdf

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

ОП «Кібербезпека та захист інформації» спрямована на набуття здобувачами навичок і компетентностей, які сприяють досягненню глобальних цілей сталого розвитку до 2030 року, зокрема:

-Ціль 4: Якісна освіта. ОП забезпечує доступ до інноваційної освіти у сфері кібербезпеки та захисту інформації, використовуючи сучасні методи навчання, залучення стейкхолдерів. Це сприяє підвищенню кваліфікації та розвитку критичного мислення у здобувачів.

-Ціль 8: Гідна праця та економічне зростання. ОП спрямована на підготовку висококваліфікованих фахівців для ринку праці, що відповідають потребам цифрової економіки. Здобувачі отримують навички, які дозволяють їм працювати у високотехнологічних сферах, забезпечуючи зростання продуктивності праці.

-Ціль 9: Інновації та інфраструктура. ОП спрямована на підготовку фахівців, здатних розробляти та впроваджувати інноваційні рішення для забезпечення кібербезпеки, що сприяє створенню надійної цифрової інфраструктури.

-Ціль 16: Мир, справедливість та сильні інститути. Навички захисту інформації, здобуті здобувачами, сприяють зміцненню кібербезпеки на рівні державних та приватних установ, що є важливим елементом забезпечення стійких інституцій.

ОП інтегрує ці глобальні цілі через освітні компоненти та практичну діяльність здобувачів.

3. Доступ до освітньої програми та визнання результатів навчання

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

<https://suitt.edu.ua/umovy-vstupu/>

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

Вступники, які здобули ступінь бакалавра або магістра (ОКР «спеціаліст»), приймаються на навчання за ОПП на перший курс. Вступ на навчання для здобуття ступеня магістра здійснюється на основі НРК6 та НРК7 відповідно до Правил прийому до ДУІТЗ. Для спеціальності F5 «Кібербезпека та захист інформації» конкурсний відбір здійснюється за результатами ЄВІ та, залежно від наявності результату ЄДКІ зі спеціальності 125 у рік вступу, ЄДКІ або ЄФВВ.

Правила прийому на навчання за ОП оприлюднені на офіційному вебсайті ДУІТЗ (<https://suitt.edu.ua/umovy-vstupu/>).

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?

Це питання регулюється такими документами:

- Положення про організацію освітнього процесу в ДУІТЗ;
- Положення про порядок визнання результатів навчання, отриманих у неформальній освіті в ДУІТЗ;
- Положення про визнання (перезарахування) кредитів, отриманих здобувачами під час академічної мобільності в закордонних закладах вищої освіти ДУІТЗ;
- Положення про порядок відрахування, переривання навчання, поновлення і переведення осіб, а також надання їм

академічної відпустки;

– Положення про академічну мобільність здобувачів вищої освіти у ДУІТЗ;

– Положення про порядок визначення та ліквідації академічної різниці особами, що поновлюються або переводяться до ДУІТЗ.

Всі зазначені документи оприлюднені на офіційному вебсайті ДУІТЗ: (<https://suitt.edu.ua/polozhennia/>)

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

За ОП, що акредитується, таких прикладів не було.

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

Здобувач вищої освіти має можливість подати заяву до ректора для визнання цих результатів, додаючи необхідні документи щодо отримання цих результатів. Для розгляду заяви створюється спеціальна предметна комісія згідно з розпорядженням декана факультету. У складі комісії можуть бути представники деканату, гарант освітньої програми та викладачі з відповідних дисциплін. Комісія надає здобувачеві 10 робочих днів для підготовки до підсумкового контролю з кожної дисципліни, що розглядається, в формі екзамену. Після оцінювання комісія складає протокол із висновками щодо зарахування або незарахування дисциплін. У разі позитивного результату відповідні дані вносяться до навчальної картки здобувача.

Положення про порядок визнання результатів навчання отриманих у неформальній освіті в ДУІТЗ (<https://suitt.edu.ua/wp-content/uploads/2025/12/3.-polozhennya-pro-poryadok-vyznannya-rezul-tativ-.pdf>)

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

За ОП, що акредитується, таких випадків не було.

4. Навчання і викладання за освітньою програмою

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

Методологія викладання базується на здобувачоцентрованому та проблемно-орієнтованому підході, що включає лекції, практичні заняття, проектну діяльність та самостійну роботу. Інтерактивні мультимедійні лекції, дослідницькі та практичні завдання сприяють активному навчанню здобувачів. Курсовий проєкт, реальні кейси, хакатони та практична підготовка забезпечують здобуття практичних навичок. Використання новітніх технологій кіберзахисту, симуляційних інструментів та кіберполігонів дозволяє моделювати й аналізувати кіберзагрози, сприяючи досягненню мети та програмних результатів навчання програми.

Також значну роль відіграє індивідуальна робота здобувачів з викладачами, яка забезпечується за допомогою електронної пошти, телеграм-каналів та платформ відеозв'язку, таких як Zoom та Meet (<https://meet.suitt.edu.ua/>). Важливо зазначити, що дистанційне навчання також використовується для досягнення програмних результатів згідно з Положенням про дистанційне навчання в ДУІТЗ. Для цього використовуються платформи відеозв'язку та система дистанційного навчання Moodle (<http://e-learning2.suitt.edu.ua/>)

Положення про організацію освітнього процесу в ДУІТЗ:

<https://suitt.edu.ua/wp-content/uploads/2025/12/1.-polozhennnia-pro-orhanizatsiiu-osvitnoho-protsesu-v-duitz.pdf>

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?

Методи, засоби та технології навчання і викладання на ОПП «Кібербезпека та захист інформації» реалізуються з урахуванням вимог здобувачоцентрованого підходу. Індивідуалізація навчання забезпечується вибором здобувачами вибірових компонентів та формуванням індивідуальної освітньої траєкторії відповідно до Положення про реалізацію права на вільний вибір навчальних дисциплін здобувачами вищої освіти ДУІТЗ: (https://suitt.edu.ua/wp-content/uploads/2025/12/5.-polozhennia_pr.pdf).

Використовуються проєктне та проблемно-орієнтоване навчання, практичні заняття, дослідницькі проєкти та мультимедійні лекції. Залучення роботодавців і експертів-практиків, зокрема проведення гостьових лекцій: <https://suitt.edu.ua/reformuvannia-opp/>, забезпечує зв'язок теорії та практики. За результатами опитування 2025 року, 75–91,7 % респондентів позитивно оцінюють організацію освітнього процесу, 62,5 % вважають достатньою матеріально-технічну базу, а 75 % зазначили можливість впливати на зміст програми:

<https://drive.google.com/file/d/1wLGZFCbZfCpAT4lwLes9zzZOJGPpOQ7K/view>. Результати опитування 2026 року

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

Право на академічну свободу забезпечується для НПП та педагогічних працівників ЗВО відповідно до Закону України "Про освіту" №2145-VIII від 05.09.2017 року. Це означає, що вони мають можливість вільно обирати методи та засоби навчання. ЗВО не обмежує академічну свободу для своїх працівників і здобувачів, і не використовує їхні публічні заяви, включаючи соціальні мережі, як підставу для дисциплінарних санкцій, звільнень або відрахувань. Враховуючи це, викладачі здійснюють індивідуальний підхід у виборі форм, методів і засобів навчання, враховуючи потреби та особливості здобувачів, їхній рівень підготовки, інтереси, та інші аспекти. Закон України "Про освіту" №2145-VIII від 05.09.2017 року: <https://zakon.rada.gov.ua/laws/show/2145-19>

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

Мета, зміст і очікувані результати навчання чітко визначені в Освітніх програмах (ОП). Усі ОП, за якими в ДУІТЗ проводиться підготовка здобувачів вищої освіти, доступні для ознайомлення на офіційному сайті ЗВО, що забезпечує усім здобувачам доступ до цієї інформації (<https://suitt.edu.ua/prohramy-osvity/>). У силабусах освітніх компонентів наведені цілі, зміст і очікувані результати навчання, а також критерії та порядок оцінювання (<https://suitt.edu.ua/sylabusy-f5-opp-kiberbezpeka-ta-zakhyst-informatsii/>). Крім того, здобувачі мають можливість звернутися до методичних матеріалів і рекомендацій щодо організації самостійної роботи (<https://metod.suitt.edu.ua/>). Перед початком навчання гарант ОП організовує загальні збори, під час яких надає основну інформацію про очікувані результати навчання. Крім того, конкретні завдання, критерії оцінювання і методи навчання обов'язково пояснюються кожним викладачем на першому занятті для кожного окремого освітнього компоненту.

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

Поєднання навчання та досліджень у межах ОП «Кибербезпека та захист інформації» забезпечується інтеграцією науково-дослідної діяльності в освітній процес. Важливою складовою є дисципліна «Методологія наукових досліджень та академічна доброчесність» (ОК1), яка формує базові знання щодо проведення досліджень, планування експериментів та аналізу результатів. Здобувачі розвивають критичне мислення, уміння формулювати наукові гіпотези та застосовувати методи системного аналізу.

Особливістю програми є проєктне навчання. У дисциплінах «Моніторинг та аудит інформаційно-комунікаційних систем» (ОК9) та «Киберфізична безпека об'єктів критичної інфраструктури» (ОК7) здобувачі проводять дослідження з використанням симуляційних моделей, відпрацьовують сценарії кіберзагроз і вразливостей, виконують завдання з оцінювання ризиків та розроблення рекомендацій. Здобувачі також працюють у дослідницьких групах під керівництвом викладачів та виконують індивідуальні дослідницькі завдання (<https://suitt.edu.ua/2024/10/20/sertyfikaty-mahistriv/>).

Завершальним етапом є підготовка та захист магістерської роботи (ОК12), що передбачає самостійне виконання проєктних і науково-дослідних завдань. Результати досліджень можуть використовуватися на підприємствах, де здобувачі проходять практику.

У 2025 році в освітній процес кафедри кібербезпеки та технічного захисту інформації впроваджено результати дисертаційної роботи Аль-Файюмі Халеда «Методи підвищення захищеності інформації на основі прихованості передавання сигнально-кодових конструкцій» (https://suitt.edu.ua/spetsrada_phd/).

У 2026 році впроваджено результати дисертаційних робіт Кільдішева Віталія Йосиповича «Моделі та методи захисту інформації на основі параметричного перетворення передаваних сигнально-кодових конструкцій» (<https://suitt.edu.ua/zdobuvach-naukovoho-stupenia-kildishev-vitalij-josypovych/>) та Гавеля Сергія Миколайовича «Підвищення прихованості передавання інформації на основі прямого розширення спектра таймерних сигнальних конструкцій» (https://suitt.edu.ua/spetsrada_phd_g/).

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

Викладачі освітньо-професійної програми «Кибербезпека та захист інформації» активно оновлюють зміст освітніх компонентів на основі сучасних наукових досягнень та практик у галузі кібербезпеки та захисту інформації, забезпечуючи актуальність навчання та його відповідність сучасним вимогам ринку. Це відбувається завдяки постійній участі викладачів у науково-дослідній роботі, їхній співпраці з практиками (<https://suitt.edu.ua/partnery-ta-stejkholdery/>) та залученню до міжнародних проєктів, зокрема, проєкту Агентства USAID «Кибербезпека критичної інфраструктури України» з 2020 року (https://www.facebook.com/CyberActivityUA/?locale=uk_UA, <https://suitt.edu.ua/pidvyshchennia-kvalifikatsii-vykladachiv-kafedry-ktzi/>)

Так, у 2023 році для урахування вимог професійного стандарту «Фахівець сфери захисту інформації» було оновлено зміст трьох фахових освітніх компонентів та введено два нових. Також, наприклад, дисципліна «Криптологія» (ОК8)

оновлюється відповідно до останніх досліджень у сфері криптографічних методів захисту інформації. Викладачі, залучені до наукових конференцій з кібербезпеки, інтегрують у курс нові криптографічні протоколи, такі як протоколи квантової криптографії, що стають актуальними в умовах розвитку квантових обчислень. Крім того, вони використовують наукові статті та дослідження вітчизняних та закордонних експертів для оновлення навчальних матеріалів.

Інший приклад — курс «Моніторинг та аудит інформаційно-комунікаційних систем» (ОК9), який постійно адаптується до сучасних практик кібербезпеки. Викладачі впроваджують новітні технології моніторингу загроз та методи аудиту інформаційних систем, такі як використання сучасних програмних засобів для сканування вразливостей. Це відображає сучасні тренди у сфері кібербезпеки та забезпечує отримання здобувачами найсучасніших знань для своєї професійної діяльності.

Також, дисципліна «Кіберфізична безпека об'єктів критичної інфраструктури» (ОК7) постійно вдосконалюється на основі співпраці з підприємствами, що працюють у сфері захисту критичної інфраструктури. Викладачі програми оновлюють матеріали, враховуючи новітні загрози для об'єктів критичної інфраструктури та сучасні стандарти, як-от рекомендації Європейського агентства з кібербезпеки (ENISA).

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

Викладання та наукові дослідження в межах ОП тісно пов'язані з інтернаціоналізацією діяльності ДУІТЗ.

Інтернаціоналізація діяльності реалізується, зокрема, через участь здобувачів у міжнародних наукових конференціях, де вони отримують інформацію про новітні досягнення і тенденції розвитку галузі кібербезпеки, представляють результати своїх досліджень, обговорюють їх з провідними фахівцями (<https://suitt.edu.ua/2024/10/20/sertyfikaty-mahistriv/>).

Також здобувачі беруть участь у дистанційних вебінарах, що проводяться вітчизняними та іноземними провідними фахівцями з кібербезпеки, наприклад:

- Відкрита лекція за участі начальника 7-го відділу кіберполіції (організації технічного супроводження) Управління протидії кіберзлочинам в Одеській області;
- Гостьова лекція від компанії «Kobi Software» на тему «Інтелектуальні системи безпеки: як побудувати ефективний захист»;
- Гостьова лекція від компанії SIDCON;
- Семинар з експертом галузі кібербезпеки Аллою Кобозевою «Фундаментальні основи побудови крипто-стеганографічної системи», за підтримки Проєкту USAID "Кібербезпека критично важливої інфраструктури України";
- Семинар з експертом галузі кібербезпеки Владиславом Радецьким "Основи перевірки файлів або як створити власний SandBox", за підтримки Проєкту USAID "Кібербезпека критично важливої інфраструктури України";
- Семинар з експертом галузі кібербезпеки Микитою Книшем "Етичне полювання на неетичних хакерів".

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?

Протягом навчального семестру здобувачі періодично проходять перевірку своїх навчальних досягнень. Це включає усне та письмове опитування, виконання тестових завдань, звіти з лабораторних робіт, а також презентації. Форми контролю визначаються в ОП, навчальному плані, силабусах дисциплін і індивідуальних навчальних планах здобувачів. Семестровий екзаме́н або комбінований тест оцінює засвоєння здобувачами теоретичного та практичного матеріалу за семестр. Оцінка досягнень здобувачів за кожною навчальною дисципліною здійснюється за шкалами ECTS, 4-х бальною шкалою ("відмінно", "добре", "задовільно", "незадовільно" або "зараховано", "незараховано"), 100-бальною шкалою. Критерії оцінювання розробляються для кожної дисципліни і включаються в робочі програми (силабуси), які затверджуються на засіданнях кафедри.

Положення про контроль та оцінювання навчальних досягнень здобувачів вищої освіти в ДУІТЗ

<https://suitt.edu.ua/wp-content/uploads/2025/12/2.->

[polozhennia_pro_kontrol_ta_otsiniuvannia_navchalnykh_dosiakhnen.pdf](https://suitt.edu.ua/wp-content/uploads/2025/12/2.-polozhennia_pro_kontrol_ta_otsiniuvannia_navchalnykh_dosiakhnen.pdf)

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

В університеті використовуються чіткі та зрозумілі критерії оцінювання досягнень здобувачів.

Для забезпечення ясності та зрозумілості контрольних заходів та критеріїв оцінювання навчальних досягнень здобувачів вищої освіти застосовуються наступні практики: уважне планування та формування контрольних заходів кафедрами та постійна роз'яснювальна робота із здобувачами.

Відповідно до ОП, контрольні заходи містять поточний та підсумковий контроль, які спрямовані на перевірку рівня знань здобувачів. Поточний контроль проводиться під час різних видів навчальних занять і використовує рейтингову систему оцінювання, що відповідає встановленим стандартам. Підсумковий контроль може бути у формі заліку, екзаме́ну, захисту курсової роботи, а також захисту результатів практики. Оцінювання курсових робіт здобувачів також базується на рейтинговій системі оцінювання. Критерії оцінювання навчальних досягнень встановлюються викладачем і роз'яснюються здобувачам на початку кожного курсу. Для зручності підсумкового контролю використовуються, зокрема, форми Google, а також проводиться аудиторний та дистанційний спосіб

проведення тестування, що дозволяє швидко отримати результати та забезпечує особисту ідентифікацію кожного здобувача.

Положення про контроль та оцінювання навчальних досягнень здобувачів вищої освіти в ДУІТЗ
https://suitt.edu.ua/wp-content/uploads/2025/12/2.-polozhennia_pro_kontrol_ta_otciniuvannia_navchalnykh_dosiahnen.pdf

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

Інформація про форми контрольних заходів для здобувачів вищої освіти надається і уточнюється кілька разів протягом навчального періоду:

- На початку навчального семестру здобувачам роз'яснюється загальний порядок оцінювання знань, критерії оцінювання, а також форми та види контрольних заходів для кожної навчальної дисципліни.
- Форми та критерії оцінювання включаються до силабусу, до якого здобувачі мають доступ через електронну систему навчання.
- Наприкінці вивчення кожної дисципліни, під час консультацій, викладачі ще раз уточнюють форму підсумкового контролю та критерії оцінювання.
- Щорічно проводяться соціологічні опитування серед здобувачів та випускників щодо якості та об'єктивності системи оцінювання.

Положення про контроль та оцінювання навчальних досягнень здобувачів вищої освіти в ДУІТЗ:
https://suitt.edu.ua/wp-content/uploads/2025/12/2.-polozhennia_pro_kontrol_ta_otciniuvannia_navchalnykh_dosiahnen.pdf
Результати опитування здобувачів: <https://suitt.edu.ua/opytuvannia-2/>

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

Здобувачі, що навчаються за ОП, після завершення навчального плану проходять атестацію у визначеній в ОП формі відповідно до вимог законодавства у сфері вищої освіти.

Ця атестація включає публічний захист кваліфікаційної роботи перед спеціально утвореною екзаменаційною комісією (включаючи представників роботодавців), яку затверджує ректор університету. Згідно з вимогами стандарту вищої освіти, тема кваліфікаційної роботи передбачає вирішення складних спеціалізованих завдань або практичних проблем в галузі кібербезпеки та захисту інформації і передбачає проведення досліджень або здійснення інновацій.

Єдиний державний кваліфікаційний іспит за спеціальністю F5 – Кібербезпека та захист інформації на другому (магістерському) рівні не запроваджений.

Положення про екзаменаційну комісію з атестації здобувачів вищої освіти в ДУІТЗ
https://suitt.edu.ua/wp-content/uploads/2025/12/8.-polozhennia_pro_ekzamenatsijnu_komisiiu_z_atestatsii_zdobuvachiv_vyshchoi.pdf

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

Дана процедура регулюється наступними документами:

- Положення про організацію освітнього процесу в ДУІТЗ
<https://suitt.edu.ua/wp-content/uploads/2025/12/1.-polozhennia-pro-orhanizatsiiu-osvitnoho-protsesu-v-duitz.pdf>
- Положення про контроль та оцінювання навчальних досягнень здобувачів вищої освіти в ДУІТЗ.
https://suitt.edu.ua/wp-content/uploads/2025/12/2.-polozhennia_pro_kontrol_ta_otciniuvannia_navchalnykh_dosiahnen.pdf
- Положення про екзаменаційну комісію з атестації здобувачів вищої освіти в ДУІТЗ
https://suitt.edu.ua/wp-content/uploads/2025/12/8.-polozhennia_pro_ekzamenatsijnu_komisiiu_z_atestatsii_zdobuvachiv_vyshchoi.pdf

Дані документи доступні на офіційному сайті ЗВО <https://suitt.edu.ua/polozhennia/>

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

Для забезпечення об'єктивності та неупередженості оцінювання застосовуються такі заходи. Здобувачі ознайомлюються з прикладами завдань для семестрового контролю на початку семестру. Для проведення підсумкового контролю екзаменаційна комісія складається не менше ніж із двох осіб. З метою запобігання конфлікту інтересів оцінювання проводиться публічно. Для забезпечення неупередженості до складу голів та/або заступників голів екзаменаційних комісій із захисту кваліфікаційних робіт залучаються сторонні фахівці, які представляють потенційних роботодавців.

Положення про контроль та оцінювання навчальних досягнень здобувачів вищої освіти в ДУІТЗ
https://suitt.edu.ua/wp-content/uploads/2025/12/2.-polozhennia_pro_kontrol_ta_otsiniuvannia_navchalnykh_dosiahnen.pdf

Положення про Апеляційну комісію ДУІТЗ
https://suitt.edu.ua/wp-content/uploads/2026/01/4.10.-polozhennia_pro_apeliatsijnu_komisiiu_duitz-1.pdf

Положення про апеляцію результатів підсумкового контролю знань здобувачів вищої освіти в ДУІТЗ
https://suitt.edu.ua/wp-content/uploads/2025/12/9.-polozhennia_pro_apeliatsiiu_rezultativ_pidsumkovoho_kontroliu_znan_zdobuvachiv.pdf

Положення про запобігання та протидію булінгу, мобінгу, кібербулінгу, харасменту в ДУІТЗ.
https://suitt.edu.ua/wp-content/uploads/2025/12/4_polozhennia_pro_zap.pdf

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

Здобувачам, які не з'явилися в день, визначений для складання контрольного заходу, або отримали незадовільну оцінку, надається право на перескладання екзамену або заліку протягом сесії за графіком ліквідації академічних заборгованостей, встановленим кафедрою. Ця оцінка вважається отриманою поза терміном, за виключенням випадків, коли здобувачі працюють за індивідуальним графіком. Для здобувачів з індивідуальним графіком своєчасним терміном є дата, вказана в індивідуальному графіку для певної освітньої компоненти. Перескладання екзаменів може відбутися не більше ніж двічі з кожної дисципліни: перший раз - перед провідним лектором, другий раз - перед комісією, яка створюється розпорядженням декана факультету. Здобувач не може перескладати екзамен з дисципліни, поки не виконає всі вимоги, передбачені навчальним планом на семестр з цієї дисципліни.

Положення про контроль та оцінювання навчальних досягнень здобувачів вищої освіти в ДУІТЗ
https://suitt.edu.ua/wp-content/uploads/2025/12/2.-polozhennia_pro_kontrol_ta_otsiniuvannia_navchalnykh_dosiahnen.pdf

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

Положення про організацію навчального процесу чітко визначає академічні права та обов'язки здобувачів ВО університету. Відповідно до цього документу, здобувачі мають можливість оскаржити дії керівництва університету та інших посадових осіб, науково-педагогічних і педагогічних працівників. У випадку незгоди з оцінкою, здобувач може подати письмову апеляцію завідувачу кафедри в день оголошення оцінки або на наступний робочий день, вказавши конкретні причини своєї незгоди. Комісія, створена на основі цієї заяви, включає представників адміністрації, кафедри та самоврядування здобувачів. Ця комісія розглядає обставини скарги та приймає рішення щодо можливого призначення повторного екзамену чи невизнання скарги у випадку відсутності фактів порушення. Важливо зауважити, що за цією ОП не було випадків оскарження процедури та результатів проведення контрольних заходів.

Про систему внутрішнього забезпечення якості освітньої діяльності та якості вищої освіти ДУІТЗ
https://suitt.edu.ua/wp-content/uploads/2025/12/3_polozh_pro_systemu_vnutr_zabezpechennia_iakosti_duitz_08_12_2025.pdf

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

Наступний документ ЗВО містить політику, стандарти і процедури академічної доброчесності:
"Положення про систему забезпечення академічної доброчесності в ДУІТЗ" https://suitt.edu.ua/wp-content/uploads/2026/09/polozhennia_pro_systemu_zabezpechennia_akademichnoi_dobrochesnosti_v_derzhavnomu.pdf

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

У п. 6.5 Положення Про систему забезпечення академічної доброчесності в ДУІТЗ визначено, що ДУІТЗ забезпечує функціонування Системи виявлення порушень академічної доброчесності, що включає спеціалізоване програмне забезпечення, бази даних, організаційні заходи та посадових осіб (адміністратор Системи, оператори Системи), що забезпечують перевірку академічних творів і навчальних робіт на наявність ознак порушень академічної доброчесності. За результатами перевірки Система формує звіт подібності, до якого обов'язково включаються: точна дата і час проведеної перевірки; обсяг перевіреного тексту; перелік виявлених джерел текстових збігів (запозичень); кількість джерел в Інтернеті, використаних для перевірки; кількісні показники подібності з кожним джерелом та сукупно. Звіт подібності зберігається в електронній формі в Системі та надсилається керівнику роботи (відповідальній особі).

Репозиторій ДУІТЗ <https://repository.suitt.edu.ua/home>

Положення про систему забезпечення академічної доброчесності в ДУІТЗ
https://suitt.edu.ua/wp-content/uploads/2025/12/3_polozh_pro_systemu_vnutr_zabezpechennia_iakosti_duitz_08_12_2025.pdf

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

Перш за все, викладачі популяризують академічну доброчесність серед здобувачів ОП та роз'яснюють важливість її дотримання. Також академічна доброчесність підтримується за допомогою систематичної інформаційної роботи Комісії з питань системи внутрішнього забезпечення якості ДУІТЗ, проведення анкетування серед здобувачів та науково-педагогічних працівників, вивчення передового досвіду інших ЗВО. Проводиться тижень академічної доброчесності.

Результати опитування випускників ОПП "Кібербезпека та захист інформації другого (магістерського) рівня ВО" <https://drive.google.com/file/d/13i6FcQBjwLsi3fkboDRXhGDzkKgon2GA/view>

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

У ЗВО встановлено процедури реагування на випадки порушення академічної доброчесності відповідно до п. 5.4 Положення про систему забезпечення академічної доброчесності в ДУІТЗ. Залежно від характеру та наслідків порушення передбачено: відрахування; позбавлення ступеня (за наявності підстав); повторне виконання завдання або проходження освітнього компонента/оцінювання; попередження; тематичні заняття з академічної доброчесності та академічного письма; позбавлення академічної стипендії. Відповідальність передбачена за відчуження та приписування авторства, академічний плагіат і самоплагіат, фабрикацію та фальсифікацію, недоброчесне використання результатів, згенерованих ШІ, несамотійне виконання завдання, недозволену допомогу, академічний саботаж та схилення до порушення академічної доброчесності. Відрахування застосовується, зокрема, за повторного або особливо тяжкого порушення, а для окремих видів порушень – як безпосередній захід. У ДУІТЗ використовується Strike Plagiarism як офіційна система перевірки академічних робіт. Протягом дії ОП випадків порушення академічної доброчесності здобувачами не зафіксовано. Положення про систему забезпечення академічної доброчесності ДУІТЗ https://suitt.edu.ua/wp-content/uploads/2026/09/polozhennia_pro_systemu_zabezpechennia_akademichnoi_dobrochesnosti_v_derzhavnomu.pdf

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

Викладачі, залучені до реалізації ОП, мають відповідну кваліфікацію та професійний досвід і відповідають вимогам законодавства. На ОП читають лекції 40% докторів наук, професорів, інші кандидати наук. Викладачі мають наукові ступені, що відповідають їхнім навчальним дисциплінам. Деякі викладачі мають значний практичний досвід роботи в галузі.

Викладачі регулярно підвищують свою кваліфікацію на міжнародних курсах і стажуваннях. Наприклад, гарант ОП Кільдішев Віталій Йосипович, який викладає курс «Моніторинг та аудит інформаційно-комунікаційних систем» (ОК9), пройшов курс з аудиту безпеки та управління ризиками в рамках літніх шкіл проекту USAID для викладачів, а у 2025 р. захистив дисертацію на здобуття наукового ступеня доктора технічних наук за спеціальністю 05.13.21 – системи захисту інформації, що підтверджує його відповідність сучасним вимогам галузі.

Таким чином, завдяки науковим ступеням, публікаціям, професійному досвіду та регулярному підвищенню кваліфікації, викладачі здатні забезпечувати освітні компоненти програми відповідно до вимог законодавства. Інформація про підвищення кваліфікації викладачами кафедри Кібербезпеки та технічного захисту інформації наведена за посиланням <https://suitt.edu.ua/pidvyshchennia-kvalifikatsii-vykladachiv-kafedry-ktzi/>

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

Професійний рівень науково-педагогічних працівників (НПП) під час конкурсу для вакантних посад визначається через аналіз досягнень всіх кандидатів відповідно до ліцензійних вимог, встановлених Постановою КМУ №365 від 24.03.2021 р. «Про внесення змін до постанови КМУ №1187 від 30.12.2015 р. «Про затвердження Ліцензійних умов провадження освітньої діяльності». Зокрема, береться до уваги наявність наукових публікацій за тематикою дисципліни, що викладається, досвід викладання у системі вищої освіти, науковий авторитет, який можна оцінити

індексом цитування наукових робіт тощо.

Кандидатури розглядаються трудовим колективом відповідної кафедри, у присутності претендентів. Кафедра оцінює професійні якості кандидатів і надає пропозицію про обрання шляхом таємного голосування. Конкурсна комісія рекомендує претендентів для подальшого розгляду на Вченій Раді Університету. Претендентів запрошують на засідання Ради, де їм ставлять питання. На основі відповідей та таємного голосування лічильна комісія визначає переможця конкурсу, а Вчена Рада підтверджує результати голосування відкритим голосуванням.

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

Роботодавці беруть участь в удосконаленні освітнього процесу на всіх рівнях вищої освіти через укладання договорів про співпрацю та участь у спільних науково-дослідних та науково-технічних проєктах. Вони надають підтримку здобувачам шляхом консультацій і беруть участь у відкритих заходах для здобувачів, наприклад, гостьових лекціях (<https://suitt.edu.ua/fakultet-itk/> - підрозділ "Ініціативи").

Здобувачі, що навчаються на ОП, проходять виробничу практику на більш ніж двох десятках підприємств галузі кібербезпеки та захисту інформації (<https://suitt.edu.ua/partnery-ta-stejkholdery/>).

Під час оновлення та рецензування ОП до консультацій залучались представники ГО «Асоціація спеціалістів кібербезпеки», ТОВ «КОБІ СС» та ТОВ «Роберт Бош ЛТД».

Відгуки на ОП від роботодавців (<https://suitt.edu.ua/reformuvannia-opp/> - підрозділ "Проєкт ОПП та відгуки").

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

Підвищення кваліфікації науково-педагогічних працівників є важливою складовою забезпечення якості освіти.

Науково-педагогічні працівники мають можливість обирати форми підвищення кваліфікації: навчання за спеціалізованими програмами, стажування, участь у семінарах, тренінгах, вебінарах та інших заходах. ЗВО забезпечує підвищення кваліфікації та стажування протягом кожних п'яти років в обсязі не менше шести кредитів ЄКТС із збереженням середньої заробітної плати відповідно до законодавства України.

Зокрема, 10 викладачів кафедри кібербезпеки та технічного захисту інформації у 2021–2022 рр. підвищили кваліфікацію в обсязі 180 кредитів ЄКТС за програмою «Cybersecurity Summer Instructor Training Program» проєкту USAID «Кібербезпека критично важливої інфраструктури України». Викладачі також брали участь у міжнародних програмах, зокрема «Social and Technological Transformations in a Changing» (Mykolas Romeris University, 08.04–31.05.2026) та літній школі Erasmus+ Jean Monnet «The European experience for enhancement the resilience of critical entities in Ukraine» (21.07–08.08.2025). Відповідні сертифікати та програми підготовки розміщені за посиланням: <https://suitt.edu.ua/pidvyshchennia-kvalifikatsii-vykladachiv-kafedry-ktzi/>

Наведіть конкретні приклади заохочення розвитку викладацької майстерності

У ЗВО встановлені процедури, які сприяють розвитку викладацької майстерності та наукової активності, включаючи як матеріальні, так і нематеріальні заохочення. Матеріальні стимули призначені для підтримки педагогічної, наукової та творчої ініціативи викладачів та науковців університету. Нематеріальні заохочення включають в себе вручення відзнак за досягнення в науковій, педагогічній та громадській діяльності, а також за відзначення сумлінної праці тощо. Ці заохочення можуть надаватися як від адміністрації навчального закладу, так і від місцевих органів влади або Міністерства освіти та науки України. Наприклад:

- До дня науки відзначили кращих викладачів та здобувачів Університету <https://www.facebook.com/suitt.official>; <https://suitt.edu.ua/2025/05/17/profesor-ievhen-vasiliu-nahorodzhenyj-pochesnoiu-hramotoiu-odeskoi-oblasnoi-vijskovoi-administratsii/>

7. Освітнє середовище та матеріальні ресурси

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

Матеріально-технічна база ЗВО відповідає вимогам Державних будівельних норм України, санітарним та пожежним нормам, а також нормам з охорони праці, що забезпечує якісне здійснення освітнього процесу. Ці ресурси сприяють досягненню визначених цілей та програм розвитку закладу вищої освіти.

Фінансова діяльність ЗВО відбувається відповідно до річного фінансового звіту, який обговорюється на засіданні Вченої ради щорічно.

Здобувачі можуть виконувати дослідження у лабораторіях кафедри (<https://suitt.edu.ua/pro-laboratorii-ktzi/>).

Бібліотека ЗВО містить як друковані, так і електронні видання та інші інформаційні матеріали, що стосуються освітнього та наукового процесу (<https://suitt.edu.ua/biblioteka/>).

У всіх навчальних приміщеннях ЗВО забезпечено Wi-Fi доступ до мережі Інтернет.

Освітні програми, навчальні плани та силабуси представлені на сайті ДУІТЗ (<https://suitt.edu.ua/prohramy-osvity/>).

Навчально-методичні комплекси дисциплін представлені у системі Moodle (<http://e-learning2.suitt.edu.ua/>).

Продemonструйте, 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

Заклад надає викладачам і здобувачам доступ до електронних бібліотек, міжнародних наукових баз даних і спеціалізованих журналів з кібербезпеки та телекомунікацій, що сприяє використанню актуальних досліджень для підготовки до занять та наукової роботи. Бібліотека має електронні каталоги та надає доступ до наукових праць, що забезпечує якісну інформаційну підтримку навчального процесу (<https://repository.suitt.edu.ua/home>).

Для практичного навчання заклад оснащений сучасними лабораторіями з кібербезпеки та технічного захисту інформації. Лабораторії обладнані сучасним обладнанням з засобами технічного захисту інформації, комп'ютерами та спеціалізованим програмним забезпеченням для моделювання кіберзагроз, захисту інформаційних систем і криптографії. Використовується також спеціалізоване ПЗ для моніторингу та аудиту безпеки (<https://suitt.edu.ua/pro-laboratorii-ktzi/>)

Для дистанційного навчання використовується платформа Moodle, яка забезпечує доступ до матеріалів, тестів і завдань, а також інтерактивні форми навчання. Онлайн-лекції та семінари проводяться через платформи Zoom та/або Meet.

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

Університетське середовище, де навчаються здобувачі ОП, забезпечує їхню безпеку та враховує їхні потреби та інтереси. Всі приміщення, як навчальні, так і адміністративні, відповідають стандартам техніки безпеки та забезпечують необхідні умови для комфортного перебування, зокрема щодо освітлення, тепла та вентиляції, а також виконання спеціалізованих лабораторних робіт. Робочі режими навчального обладнання відповідають встановленим нормам. Здобувачі регулярно проходять інструктажі з охорони праці, а діяльність в цьому напрямку контролюється відділом охорони праці університету. Проводяться зустрічі з фахівцями з пожежного та цивільного захисту для забезпечення безпеки всіх працівників та здобувачів. Два корпуси ДУІТЗ мають укриття (вул. Кузнечна, 1 та вул. Пішнівська, 5).

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.

Здобувачам надається доступ до сучасних освітніх платформ, таких як Moodle, де розміщені всі необхідні навчальні матеріали, силабуси та завдання. Викладачі проводять регулярні консультації, як у форматі офлайн, так і онлайн, для допомоги в розумінні навчального матеріалу, підготовці до заліків та екзаменів, а також виконанні курсових і випускових кваліфікаційних робіт. Індивідуальні плани навчання дозволяють здобувачам адаптувати своє навчання відповідно до особистих потреб і ситуацій.

Заклад вищої освіти забезпечує здобувачів усією необхідною інформацією через офіційні канали, зокрема, веб-сайт, електронну пошту, месенджери та соціальні мережі (<https://www.facebook.com/suitt.official>, <https://www.facebook.com/FacultyITC>). Здобувачам надається інформація щодо навчального процесу, розкладу занять, екзаменів, а також про участь у конференціях, конкурсах і можливостях академічної мобільності. Регулярно проводяться зустрічі зі самоврядуванням здобувачів та адміністрацією, де здобувачі можуть висловити свої потреби та пропозиції.

Викладачі та куратори академічних груп регулярно надають консультації з академічних і професійних питань, допомагаючи здобувачам будувати індивідуальні траєкторії навчання та кар'єрного розвитку. Здобувачі мають можливість звертатися до викладачів за порадами стосовно науково-дослідницької діяльності, вибору дисциплін або підготовки до майбутньої професійної діяльності.

Заклад вищої освіти активно сприяє здоровому способу життя здобувачів через доступ до спортивних залів і секцій. Регулярно організовуються спортивні заходи, змагання та тренування. Для підтримки ментального здоров'я здобувачів вищої освіти в ДУІТЗ діє Центр психологічної допомоги та соціальної адаптації, який проводить індивідуальні консультації та тренінги на теми стресостійкості, саморегуляції та подолання емоційних проблем. Таким чином, університет забезпечує повноцінну підтримку здобувачів вищої освіти на всіх етапах їх навчання, сприяючи їхньому академічному, професійному та особистому розвитку.

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)

Правила прийому до вищого навчального закладу не обмежують можливість вступу осіб з особливими освітніми потребами. З метою забезпечення доступності освіти для цієї категорії осіб, у ДУІТЗ створено спеціальні умови. Наприклад, встановлено пандуси для зручного пересування на вході. Особам з особливими потребами надається можливість скласти індивідуальний графік навчання. При необхідності, навчальний процес може проводитися дистанційно.

Серед здобувачів ОПП «Кібербезпека та захист інформації» другого (магістерського) рівня вищої освіти не було осіб з особливими освітніми потребами.

Продemonструйте 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

Відповідно до законодавства України та Статуту ДУІТЗ прийнято Положення про систему забезпечення академічної доброчесності в ДУІТЗ. Для розгляду порушень створена Комісія з питань етики та академічної доброчесності. Університет також активно протидіє гендерному насильству, сексуальним домаганням, дискримінації та корупції шляхом проведення інформаційних та просвітницьких кампаній та створення Комісії для врегулювання конфліктних ситуацій та виявлення недоречної поведінки.

Серед здобувачів ОПП «Кібербезпека та захист інформації» конфліктні ситуації такого роду незафіксовані.

Положення про систему забезпечення академічної доброчесності ДУІТЗ

[https://suitt.edu.ua/wp-](https://suitt.edu.ua/wp-content/uploads/2026/09/polozhennia_pro_systemu_zabezpechennia_akademichnoi_dobrochesnosti_v_derzhavnomu.pdf)

[content/uploads/2026/09/polozhennia_pro_systemu_zabezpechennia_akademichnoi_dobrochesnosti_v_derzhavnomu.pdf](https://suitt.edu.ua/wp-content/uploads/2026/09/polozhennia_pro_systemu_zabezpechennia_akademichnoi_dobrochesnosti_v_derzhavnomu.pdf)

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

Наступними документами регулюються процедури розроблення, затвердження, моніторингу та періодичного перегляду ОП:

Положення про систему внутрішнього забезпечення якості освітньої діяльності та якості вищої освіти ДУІТЗ

[https://suitt.edu.ua/wp-](https://suitt.edu.ua/wp-content/uploads/2025/12/3_polozh_pro_systemu_vnutr_zabezpechennia_iakosti_duitz_08_12_2025.pdf)

[content/uploads/2025/12/3_polozh_pro_systemu_vnutr_zabezpechennia_iakosti_duitz_08_12_2025.pdf](https://suitt.edu.ua/wp-content/uploads/2025/12/3_polozh_pro_systemu_vnutr_zabezpechennia_iakosti_duitz_08_12_2025.pdf)

Положення про освітні програми ДУІТЗ

https://suitt.edu.ua/wp-content/uploads/2025/12/1-polozhennia_pro_osvitni_prohramy_duitz.pdf

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

Періодичний моніторинг, огляд і оновлення освітніх програм націлені на забезпечення високої якості надання освітніх послуг і створення сприятливого й ефективного навчального та наукового середовища для здобувачів. Критерії для перегляду освітніх програм визначаються через аналіз та прогнозування розвитку наукового, виробничого та навчального середовища на національному та міжнародному рівнях та з урахуванням відгуків від роботодавців, випускників та здобувачів. Освітні програми переглядаються щорічно, а оновлюються – за потребою. У 2023 ОП була суттєво оновлена за підтримки проекту Агентства USAID «Кібербезпека критично важливої інфраструктури України» з метою інтеграції до неї професійних компетентностей, знань, умінь та навичок з професійного стандарту «Фахівець сфери захисту інформації» (<https://suitt.edu.ua/reformuvannia-opp/>), що обґрунтовано в першу чергу потребами сучасного ринку праці для фахівців з кібербезпеки та захисту інформації. У 2025 році було введено освітню компоненту програми:

-ОК5 Менеджмент в системі корпоративної інформаційної безпеки

У 2026 році оновлено зміст ОК3 «Комплекси технічного захисту інформації» та змінено його назву зі «Спеціальні вимірювання в галузі технічного захисту інформації» на «Комплекси технічного захисту інформації».

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

Під час перегляду освітніх програм увага приділяється думці всіх учасників навчального процесу, включаючи здобувачів. Здобувачам надається можливість висловити свої враження щодо навчального процесу, змісту освітніх складових та подати пропозиції щодо поліпшення програми за допомогою анонімних анкет. Аналіз відгуків допомагає виявити переваги та недоліки освітніх програм

(<https://drive.google.com/file/d/1wlGZFCbZfCpAT4lwLes9zzZOJGPpOQ7K/view> та https://suitt.edu.ua/wp-content/uploads/2026/06/4_f5_informats_anal_dovidka_zdobuvachi_vyshchoi_osvity_mahistry_f5_kiberbezpeka-2.pdf).

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

Представники самоврядування здобувачів залучаються до процесів забезпечення якості освітніх програм. Вони беруть участь у засіданнях кафедр для оцінки та перегляду програм, а також можуть брати участь у розгляді та затвердженні програм на засіданнях Вченої Ради. Здобувач вищої освіти другого (магістерського) рівня за ОП «Кібербезпека та захист інформації» входить до складу робочої групи з оновлення ОП.

Продemonструйте, 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 та стейкхолдери залучені до періодичного перегляду ОП завдяки регулярним їх зустрічам з робочою групою та проведенню заходів в університеті.

Детальну інформацію про оновлення ОП за участю роботодавців та професійних об'єднань спеціалістів галузі кібербезпеки та захисту інформації розміщено за посиланням <https://suitt.edu.ua/reformuvannia-opp/>

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

Інформацію про професійний розвиток випускників збирають і аналізують співробітники, що відповідають за якість освіти в ДУІТЗ, а також викладачі кафедри КБ та ТЗІ. Як свідчать результати опитувань, більше половини здобувачів ОП працюють за фахом вже на 2-му курсі магістратури.

Викладачі кафедри КБ та ТЗІ та адміністрація університету сприяють працевлаштуванню випускників ОП, а також мають з ними постійний зв'язок, що дає змогу відстежувати їхній професійний розвиток.

Продemonструйте, 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

Система забезпечення якості закладу вищої освіти передбачає ефективний механізм моніторингу освітньої програми та освітньої діяльності, що реалізується через постійний аналіз результатів опитувань заінтересованих сторін, включаючи здобувачів, викладачів, роботодавців та випускників. Моніторинг здійснюється з використанням анкетувань, зворотного зв'язку та залучення стейкхолдерів до обговорення результатів навчання.

Здобувачі заповнюють анкети щодо якості викладання, змісту освітніх компонентів, матеріально-технічного забезпечення та відповідності навчального процесу їхнім очікуванням (https://suitt.edu.ua/wp-content/uploads/2026/06/4_f5_informats_anal_dovidka_zdobuvachi_vyshchoi_osvity_mahistry_f5_kiberbezpeka-2.pdf та <https://drive.google.com/file/d/1wGZFCbZfCpAT4lwLes9zzZOJGPpOQ7K/view>).

Узагальнення результатів опитувань здійснюється відповідальним за забезпечення якості освіти, а їх результати враховуються під час внесення змін до освітніх програм.

Роботодавці, як заінтересовані сторони, також беруть участь в опитуваннях і надають відгуки, у тому числі в усній формі, про готовність випускників до роботи, необхідні навички та компетентності. На основі таких відгуків було внесено зміни до програми, зокрема оновлено зміст дисциплін, пов'язаних із кібербезпекою критичної інфраструктури, та впроваджено нові методи навчання, орієнтовані на практичні кейси.

Кожен навчальний рік проводиться комплексний аналіз результатів опитувань усіх заінтересованих сторін, і на його основі розробляються рекомендації для вдосконалення освітнього процесу. Це включає коригування навчальних планів, зміни у методах викладання, покращення технічного та інформаційного забезпечення.

Зокрема, значну користь для оновлення ОП, перегляду змісту освітніх компонентів, підвищення кваліфікації викладачів принесла участь кафедри в проєкті Агентства USAID «Кібербезпека критично важливої інфраструктури України» з 2021 р. (https://www.facebook.com/CyberActivityUA/?locale=uk_UA)

Таким чином, система забезпечення якості оперативно реагує на результати моніторингу та постійно вдосконалює освітню програму на основі відгуків усіх заінтересованих сторін.

Продemonструйте, 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 ураховані під час удосконалення цієї ОП?

Під час удосконалення цієї ОП було враховано зауваження та рекомендації останньої акредитації (2024 р.).

Зазначені зауваження та рекомендації враховано шляхом таких заходів:

1. У 2025 та 2026 рр. проведено опитування здобувачів щодо актуалізації ОПП та внесення змін до її обов'язкових компонентів (<https://suitt.edu.ua/opytuvannia-2/>).
2. Внесено зміни до Положення про реалізацію права на вільний вибір навчальних дисциплін та Положення про індивідуальну освітню траєкторію здобувачів вищої освіти в ДУІТЗ (<https://suitt.edu.ua/polozhennia/>).
3. ОПП приведено у відповідність до Стандарту вищої освіти України спеціальності 125 Кібербезпека для другого (магістерського) рівня: виробнича практика складає 15 кредитів ЄКТС; удосконалено структурно-логічну схему ОПП.
4. Здобувачів ознайомлено з можливостями академічної мобільності та відповідним Положенням (<https://suitt.edu.ua/polozhennia/>).
5. Викладачі постійно оновлюють навчальні матеріали та розміщують їх у системі Moodle.
6. Керівництво факультету, куратори груп та керівники курсових і кваліфікаційних робіт систематично наголошують на важливості дотримання принципів академічної доброчесності.
7. Оновлено персональні сторінки викладачів (<https://suitt.edu.ua/sklad-kafedry-ktzi/>). Опубліковано 10 фахових статей, 8 статей у наукометричній базі Scopus, 2 монографії та 12 тез конференцій; підготовлено підручник, 2 навчальні посібники та 20 методичних рекомендацій.
8. Розроблено та прийнято Положення про організацію інклюзивного навчання здобувачів вищої освіти з особливими освітніми потребами в ДУІТЗ (<https://suitt.edu.ua/polozhennia/>).
9. Створено навчальну лабораторію з вивчення систем відеоаналітики «Проектна лабораторія Kobi Software: полігон з сучасних систем відеоаналітики».
10. Розроблено та прийнято Положення про опитування учасників освітнього процесу, Положення про гаранта освітньої програми та Положення про навчання здобувачів за індивідуальним графіком (<https://suitt.edu.ua/polozhennia/>).

11. У 2025 та 2026 рр. проекти ОПП розміщувалися для громадського обговорення. Пропозиції стейкхолдерів щодо посилення практичної складової з проектування та функціонування комплексних систем безпеки, а також моніторингу й аудиту інформаційно-комунікаційних систем враховано під час оновлення відповідних освітніх компонентів. Отримано рецензії від стейкхолдерів (<https://suitt.edu.ua/hromadske-obhovorennia-2/>).
12. Постійно оновлюється інформація про ОПП, навчальний план, силабуси (<https://suitt.edu.ua/osvitni-prohramy-2025/>), кадровий склад та матеріально-технічне забезпечення (<https://suitt.edu.ua/kafedra-ktzi/>).

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

Університет активно залучає академічну спільноту до внутрішніх аудитів системи управління якістю освітніх програм через наступні заходи:

- Розробка, моніторинг та регулярний перегляд освітніх програм за участю представників провідних кафедр відповідних спеціальностей.
- Регулярний аналіз навчальних планів та змісту робочих програм дисциплін за участю представників підприємств-партнерів.
- Обговорення проектів освітніх програм на засіданнях Вченої Ради із залученням усіх зацікавлених сторін академічної спільноти.
- Підвищення кваліфікації науково-педагогічних працівників у провідних наукових та навчальних закладах України та світу.
- Забезпечення ефективної системи виявлення та запобігання академічному плагіату в навчальному процесі.

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

Культура якості освіти формується завдяки організації внутрішнього забезпечення якості вищої освіти. Це відбувається на п'яти рівнях:

- Перший рівень – здобувачі та їхні ініціативні групи, які вносять пропозиції та зауваження щодо програм.
- Другий рівень – кафедри, гаранті програм, робочі групи, викладачі, а також представники стейкхолдерів.
- Третій рівень – структурні підрозділи, які займаються освітньою діяльністю, включаючи деканів факультетів, представники самоврядування здобувачів.
- Четвертий рівень – Загально-університетські структурні підрозділи, відповідальні за забезпечення якості, навчально-методична та науково-технічна ради університету.
- П'ятий рівень – Наглядова Рада, Ректорат, Вчена рада, функції яких визначаються законодавством та статутом університету.

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 усіх учасників освітнього процесу забезпечуються наступним документом:

Положення про організацію освітнього процесу в ДУІТЗ

<https://suitt.edu.ua/wp-content/uploads/2025/12/1.-polozhennnia-pro-orhanizatsiiu-osvitnoho-protsesu-v-duitz.pdf>

Документи розміщені на офіційному сайті ЗВО та є загальнодоступними для всіх учасників освітнього процесу: <https://suitt.edu.ua/polozhennia/>

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

Проекти ОП розміщені на сторінці <https://suitt.edu.ua/reformuvannia-opp/> - підрозділ "Проект ОПП та відгуки"

Зауваження, пропозиції стейкхолдерів, проекти програм навчальних дисциплін та інші матеріали щодо оновлення ОП розміщені на сторінці <https://suitt.edu.ua/reformuvannia-opp/>

Затверджені ОП розміщені на сторінці <https://suitt.edu.ua/prohramy-osvity/>

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

Освітня програма:

<https://suitt.edu.ua/prohramy-osvity/>

Навчальний план:

<https://suitt.edu.ua/prohramy-osvity/>

Силабуси обов'язкових компонентів:

<https://suitt.edu.ua/sylabusy-f5-opp-kiberbezpeka-ta-zakhyst-informatsii/>

Силабуси вибіркового компонентів:

<https://suitt.edu.ua/vybirkovi-dystsypliny/>

Положення про індивідуальний навчальний план здобувачів вищої освіти:

<https://suitt.edu.ua/wp-content/uploads/2025/12/4.-pro-individual-nyy-navchal-.pdf>

11. Перспективи подальшого розвитку ОП

Якими загалом є сильні та слабкі сторони ОП?

Сильні сторони ОП:

- ОП базується на багаторічному досвіді успішної підготовки здобувачів другого (магістерського) рівня вищої освіти у галузі кібербезпеки та захисту інформації (з 2010 р.);
- ОП оновлена у 2023 р. з урахуванням частини професійних компетентностей, знань, вмінь та навичок професійного стандарту «Фахівець сфери захисту інформації»;
- індивідуальний підхід до кожного здобувача, включаючи можливість вибору спеціалізованих дисциплін з урахуванням особистих потреб у працевлаштуванні або професійного зростання;
- висока кваліфікація і досвід викладачів та керівників кваліфікаційних робіт здобувачів, що забезпечує високу якість підготовки здобувачів;
- залучення до освітнього процесу фахівців з практики, які є потенційними роботодавцями; співпраця кафедри Кібербезпеки та технічного захисту інформації з багатьма державними та приватними установами в галузі кібербезпеки та захисту інформації;
- збереження зв'язків між викладачами кафедри та випускниками ОП, зокрема, з метою відстеження їх кар'єрного зростання та отримання пропозицій щодо оновлення ОП.

Слабкі сторони ОП:

- недостатньо розвинена академічна мобільність здобувачів, які навчаються за даною ОП, особливо в останні роки;
- наразі відсутні здобувачі, які навчаються за дуальною формою освіти, попри нормативно врегульовану можливість її реалізації.

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

- розширити коло фахівців, які беруть участь у навчальному процесі, зокрема залучити нових потенційних роботодавців, включаючи представників держав Європейського Союзу;
- збільшити кількість здобувачів, які обирають дуальну форму навчання шляхом розширення співпраці з вітчизняними підприємствами;
- підвищити ефективність профорієнтаційної роботи серед іноземних здобувачів та представників посольств їхніх країн з метою залучення на навчання за ОП іноземних здобувачів;
- раз на рік оновлювати зміст навчальних дисциплін ОП відповідно до новітніх тенденцій та перспективних напрямів розвитку галузі кібербезпеки та захисту інформації;
- максимально сприяти академічній мобільності здобувачів;
- збільшити активність викладачів у вивченні іноземних мов для розширення можливостей академічної мобільності та проведення занять англійською мовою.

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

ПБ: Назаренко Олександр Аскольдович

Дата: 23.09.2026 р.

Таблиця 1. Інформація про освітні компоненти ОП

Назва освітнього компонента	Вид освітнього компонента	Силабус або інші навчально-методичні матеріали		Якщо освітній компонент потребує спеціального матеріально-технічного та/або інформаційного забезпечення, наведіть відомості щодо нього*
		Назва файла	Хеш файла	
Методологія наукових досліджень та академічна доброчесність	навчальна дисципліна	<i>ok_1_metodologiya_naukovix_dosliden_ta_akademichna_dobrochesnist.pdf</i>	ZdOGip1moBvAvp58 FucUFXo1oHaD5MN JU3YU7DnyTUc=	Обладнання: 1. Мультимедійна аудиторія з проектором BenQ MS506 та екраном: 2. Комп'ютерний клас з ПК: Системний блок «Impression P», Монітор19;SamsungSM-10шт. OS Windows10. Література: 1. Чукурна О. П. Конспект лекцій з дисципліни «Методологія наукових досліджень» [для здобувачів другого (магістерський) рівня вищої освіти спеціальності 073 – «Менеджмент»] [Електронний ресурс] / О. П. Чукурна. – Одеса : ДУІТЗ, 2024. – 104 с. 2. Чукурна О. П. Методичні вказівки до вивчення навчальної дисципліни «Методологія наукових досліджень» [для здобувачів другого (магістерський) рівня вищої освіти спеціальності 073 – «Менеджмент»] [Електронний ресурс] / О. П. Чукурна. – Одеса : ДУІТЗ, 2024. – 25 с. 3. Гонюкова Л. В., Козаков В. М. (ред.) Дослідження державних політик: методологія, процедури та європейські практики : монографія. – Київ : НАДУ, 2018. – 400 с. 4. Євтушенко М. Ю., Хижняк М. І. Методологія та організація наукових досліджень : навч. посіб. / М. Ю. Євтушенко, М. І. Хижняк. – Київ : Центр учбової літератури, 2019. – 350 с. 5. Крушельницька О. В. Методологія та організація наукових досліджень : навч. посіб. / О. В. Крушельницька. – Київ : Кондор, 2019. – 206 с. 6. Григорук П. М., Хруц Н. А. Методологія і організація наукових досліджень : навч. посіб. / П. М. Григорук, Н. А. Хруц. – Київ : Кондор, 2017. – 206 с. 7. Петровський П. М. Методологія наукового дослідження в галузі державного управління : навч. посіб. / П. М. Петровський. – Львів : ЛРІДУ НАДУ, 2017. – 240 с. 8. Ладанюк А. П., Власенко Л. О., Кишенько В. Д. Методологія наукових досліджень : навч. посіб. / А. П. Ладанюк та ін. – Київ : Вид-во Ліра-К, 2018(розміщено за актуальним роком видання у списку). – 352 с. 9. Петровський П. М. Методологія наукового дослідження в галузі державного управління : навч. посіб. / П. М. Петровський. – Львів : ЛРІДУ

				НАДУ, 2015. – 240 с. 10. Загороднюк С. В., Євмешкіна О. Л., Леценко В. В. (упоряд.); Ващенко К. О. (ред.) <i>Методологія наукових досліджень з державного управління : хрестоматія</i>. – К. : НАДУ, 2014. – 180 с. 11. Безверхнюк Т. М. (уклад.) <i>Методологія, методи і засоби проектного менеджменту : метод. рек. з підготов. курсового проекту для слухачів ден. та заочн. форми навч. спеціальність – 8.18010013 Управління проектами</i>. – Одеса : ОРІДУ НАДУ, 2014. – 68 с.
Педагогіка та психологія вищої школи	навчальна дисципліна	ok2_pedagogika_ta_psihologia_vischoi_shkoli.pdf	ENkmO41ruyDNXFjZLlopykxeFKDHcy0AoZpgF4am7Ao=	Обладнання 1. Комп'ютер з доступом до інтернету 2. ОС Windows <i>Література:</i> 1. Кіберпсихологія у вимірах сучасного наукового дискурсу : монографія / авт. кол.: С. Хаджирадева, Ю. Левін, М. Тодорова [та ін.] ; за заг. ред. С. К. Хаджирадевої. Одеса : Астропринт, 2024. 240 с. 2. Коучинг конфліктів – вирішуйте проблеми, зміцнюючи відносини : практикум для тренерів / О. Редліх, О. Євтушенко, В. Ємельянов, Шиліна Н. Є. (п. 2.30) та ін. ; за заг. ред. проф. О. Редліха, С. Хаджирадевої та ін. 2023. 168 с. 3. Виноградова В. Є., Юрченко В. І. <i>Психологія вищої освіти: теоретичні та практичні аспекти</i> : навч. посіб. 2-е вид. Київ : Ліра-К, 2020. 296 с. 4. Кучинська І. О. <i>Педагогіка вищої школи</i> : навч. посіб. Кам'янець-Подільський : Зволейко Д. Г., 2020. 291 с. 5. <i>Педагогіка та психологія вищої школи</i> : навч. посіб. / Л. Г. Кайдалова, І. С. Сабатовська-Фролкіна Н. В. Альохіна Харків : НФаУ, 2019. 248 с. 6. Грабовська С. Л. <i>Психологія примирення</i> : навч. посіб. Львів : ЛНУ імені Івана Франка, 2019. 294 с. 7. <i>Інноваційні освітні технології</i> : навч.-метод. посіб. / упоряд. Л. М. Прокопів. Івано-Франківськ, 2020. 172 с. 8. Романова Т. А. <i>Формування основ професіоналізму в майбутніх фахівців зі спеціальної освіти у процесі професійної підготовки: теоретичний аспект. Педагогічні науки: реалії та перспективи</i>. 2021. Вип. 80, т. 2. Серія 5. С. 101–105.
Комплекси технічного захисту інформації	навчальна дисципліна	ok3_kompleksy-tekhnichnoho-zakhystu-informatsii-1-1.pdf	/jgBXbdmOOfRW1n5mDTaDjRqE/qIL1HpZtz9vZOnziA=	Обладнання 1. Мультимедійна аудиторія з проектором та екраном 2. Комп'ютерний клас з ПК <i>Література:</i> 1. Горохов С. М., Кондратьєва Н. В., Кононович В. Г., Стайкуца С. В. <i>Програми та методики державної експертизи інформаційної захищеності</i>

				телекомунікацій: навч. посіб. / за ред. чл.-кор. МАЗ В.Г. Кононовича. – Одеса : ОНАЗ ім. О.С. Попова, 2013. – 252 с. 2. Антіпов І. Є., Олейніков А. М., Ликов Ю. В. та ін. Засоби та системи технічного захисту інформації : навч. посіб. для студентів спеціальності 125 "Кібербезпека" / М-во освіти і науки України, Харків. нац. ун-т радіоелектроніки. – Харків : ХНУРЕ, 2019. – 216 с. 3. НД ТЗІ 3.7-003-2023 Порядок проведення робіт із створення комплексної системи захисту інформації в інформаційно-комунікаційній системі 4. НД ТЗІ 3.6-005-21 Порядок категоріювання безпеки інформаційної системи та інформації 5. НД ТЗІ 1.6-005-2013 Захист інформації на об'єктах інформаційної діяльності. Положення про категоріювання об'єктів, де циркулює інформація з обмеженим доступом, що не становить державної таємниці 6. НД ТЗІ 2.7-011-2012 Захист інформації на об'єктах інформаційної діяльності 7. НД ТЗІ 2.6-001-2011 Порядок проведення робіт з державної експертизи засобів технічного захисту інформації від несанкціонованого доступу та комплексних систем захисту інформації в інформаційно-телекомунікаційних системах 8. НД ТЗІ 3.6-003-2016 Порядок проведення робіт зі створення та атестації комплексів технічного захисту інформації, затверджений наказом Адміністрації Держспецзв'язку від 07.04.2016 № 41
Управління доступом до інформаційних ресурсів	навчальна дисципліна	ok4_upravlennya-dostupom-do-informacijnih-resursiv-2026-1.pdf	uJCrnycY5fkosa3Bt2zanjLe2SFCcLRyyVrl5PoQsAI=	Обладнання: - ПК-15шт - ОС Windows Література: - Юдін О. К., Бучик С. С. Аналіз загроз державним інформаційним ресурсам [Електронний ресурс] // Проблеми інформатизації та управління. – 2013. – № 4 (44). – С. 93–99. - Юдін О. К., Бучик С. С. Правові аспекти формування системи державних інформаційних ресурсів [Електронний ресурс] // Безпека інформації. – 2014. – Т. 20 (1). – С. 76–82. - Гребенюк А. М., Рибальченко Л. В. Основи управління інформаційною безпекою : навч. посібник. – Дніпро : Дніпроп. держ. ун-т внутріш. справ, 2020. – 144 с. - Корчинський В. В. Конспект лекцій з дисципліни «Управління доступом до інформаційних ресурсів». – ДУІТЗ, 2026 р. - Корчинський В. В. Практикум до лабораторних робіт з дисципліни «Управління доступом до інформаційних ресурсів». – ДУІТЗ, 2026 р.

				6. Корчинський В. В. Практикум до практичних робіт з дисципліни «Управління доступом до інформаційних ресурсів». – ДУІТЗ, 2026 р. 7. Корчинський В. В. Практикум до самостійних робіт з дисципліни «Управління доступом до інформаційних ресурсів». – ДУІТЗ, 2026 р.
Менеджмент в системі корпоративної інформаційної безпеки	навчальна дисципліна	ok5_menedzhment_v_systemi_korporativnoi_ib.pdf	YlEstPHVSRQPz8bp51aikyZ83KVeIXiY9i5W/wfru6g=	Обладнання: Комп'ютер із доступом до інтернету ОС Windows Література: 1. Корченко О. Г., Шелест М. Є., Казмірчук С. В. та ін. Менеджмент інформаційної безпеки : навч. посіб. Ніжин : ТПІК «Орхідея», 2019. 408 с. 2. Євсєєв С. П., Король О. Г., Воронай Н. Менеджмент інформаційної безпеки : навч. посіб. Харків : НТУ «ХПІ», 2022. 3. Носок С. О., Фаль О. М., Ткач В. М. Управління інформаційною безпекою : конспект лекцій. Київ : КПІ ім. Ігоря Сікорського, 2021. 258 с. 4. Гребенюк А. М., Рибальченко Л. В. Основи управління інформаційною безпекою : навч. посіб. Дніпро : Дніпропетровський державний університет внутрішніх справ, 2020. 144 с. 5. Костюк Ю. В., Складанний П. М., Бебешко Б. Т. та ін. Безпека інформаційно-комунікаційних систем : підручник. Київ : Київський столичний університет імені Бориса Грінченка, 2025. 1016 с. 6. Методи та засоби захисту інформації : навч. посіб. / В. А. Лахно, Є. В. Васіліу, В. М. Гладких, В. М. Домрачев, Н. М. Сивкова. Київ : ЦП «Компринт» О. В., 2021. 444 с. 7. ДСТУ EN ISO 22301:2021. Безпека та стабільність. Системи управління неперервністю бізнесу. Вимоги (EN ISO 22301:2019, IDT; ISO 22301:2019, IDT). Київ : ДП «УкрНДНЦ», 2022. 18 с. 8. ISO/IEC 27005:2022. Information security, cybersecurity and privacy protection — Guidance on managing information security risks. Geneva : International Organization for Standardization, 2022.
Комплексні системи безпеки	навчальна дисципліна	ok6_kompleksni-systemy-bezpeky.pdf	Td9q4OOcTFIhHKuuzIwcOLi+oKen2CXL9WjwXG2MQP8=	Обладнання 1. Навчальний макет інтегрованої системи безпеки «BoschBIS» 2. Навчальні макети та обладнання брендів Tiras, GreenVision, Ajax 3. Екосистема лабораторії сучасних систем відеоаналітики (проектна лабораторія KobiSoftware), програмно-апаратні рішення, ПЗ Guard Live, Guard Live User, Video Management Software тощо Література:

1. Стайкуца С.В., Заровський Р.В., Вихристюк О.А., Івахненко М.С., Комплексні системи безпеки. Сучасні системи відеоспостереження та відеоаналітики екосистеми Kobi Software: методичні вказівки до лабораторних робіт [для здобувачів другого (магістерський) рівня вищої освіти за спеціальністю F5 «Кібербезпека та захист інформації»]. – Одеса : ДУІТЗ, 2026. – 76 с.

2. Стайкуца С. В., Заровський Р. В., Івахненко М. С. (уклад.) Комплексні системи безпеки, навчально-методичні вказівки до виконання лабораторних робіт [для здобувачів другого (магістерського) рівня вищої освіти за спеціальністю «Кібербезпека та захист інформації»]. – Одеса : ДУІТЗ, 2025. – 90 с.

3. Стайкуца С. В. Конспект лекцій з дисципліни «Комплексні системи безпеки». – ДУІТЗ, 2024 р.

4. Балтовський О. А., Форос А. В., Пядишев В. Г. (уклад.) Безпека технічних систем : навчально-методичні матеріали. – Одеса : ОДУВС, 2024. – 36 с.

5. Собченко В. А. та ін. Технічні засоби охорони кордону. Частина I. Технічні засоби спостереження : навчальний посібник (електр. навч. вид.). – Хмельницький : Видавництво НАДПСУ, 2024. – 218 с.

6. Андрієнко А. О. Упровадження концепції «Smart City» в управління великими містами України : монографія. – Вінниця, Україна : ГО «Європейська наукова платформа», 2023. – 196 с.

7. Кушнір А. П., Чалий Д. О. Системи пожежної та охоронної сигналізації : навч. посіб. – Львів : СПОЛОМ, 2022. – 298 с.

8. Батчаєв В. К., Шадська У. С. Відеоспостереження у публічних місцях: основи захисту персональних даних (посібник для органів місцевого самоврядування). – К. : Компринт, 2021. – 98 с.

9. Хорошко В. О. та ін. Проектування комплексних систем захисту інформації. – Л. : Львівська політехніка, 2020. – 320 с.

10. Козюра В. Д., Хорошко В. О., Шелест М. Є., Ткач Ю. М., Усов Я. Ю. Комплексні системи захисту інформації в інформаційно-телекомунікаційних системах : навчальний посібник. – Ніжин, 2019. – 144 с.

11. Дудикевич В. Б., Хорошко В. О., Яремчук Ю. Є. Основи інформаційної безпеки : навчальний посібник. – Вінниця : ВНТУ, 2018. – 316 с.

Субботін С. О. Інтелектуальні інформаційні системи : навчальний посібник. – Київ : КНТ, 2016.

Кіберфізична безпека об'єктів критичної інфраструктури	навчальна дисципліна	<i>ok7_kiberfizichna_bezbeka_obektiv_kritichnoi_infrastryktyri.pdf</i>	xehObSppprdXuIx1GL5ZrOR7ppRjUmSj3JEBJAmAG8o=	Обладнання: 1. VirtualBox 2. OC Windows 3. OC Linux 4. Nmap 5. Wireshark 6. APS 7. Hashcat Література: 1. Кононович В. Г., Голев Д. В. «Кіберфізична безпека об'єктів критичної інфраструктури» : підручник та практикум. – Одеса : ДУІТЗ, 2025. – 406 с. 2. Лабораторний практикум з «Кіберфізичної безпеки об'єктів критичної інфраструктури» : методичний посібник та методичні вказівки. – Одеса : ДУІТЗ, 2025. – 40 с. 3. Лахно В. А., Васіліу Є. В. та ін. Методи та засоби захисту інформації : навчальний посібник. – К. : ЦП «Компринт» О. В., 2021. – 444 с. 4. НД ТЗІ 3.7-003-05 Порядок проведення робіт із створення комплексної системи захисту інформації в інформаційно-телекомунікаційній системі. Затверджено наказом ДСТСЗІ СБ України № 123 від 08.11.2005. (Серія видань «Нормативний документ»). 5. МЕК 61508. Функціональна безпека систем електричних, електронних, програмованих електронних, пов'язаних з безпекою (ІЕС 61508-х). – 600 с. (Міжнародний стандарт).
Криптологія	навчальна дисципліна	<i>ok8_2_m_f5_krypto lohiiia_sylabus.pdf</i>	heqbFe6gKvo62EoXnsrEt84f51NoOR6VSd53E8YnPdY=	Обладнання 1. Комп'ютер з доступом до інтернету 2. ОС Windows 3. Програмне забезпечення для виконання лабораторних робіт Література 1. Басов В. Є. Криптоаналіз сучасних криптосистем : методичні вказівки до лабор. занять / В. Є. Басов. – ДУІТЗ, 2025. – (Спеціальність 125 «Кібербезпека»). 2. Лімарь І. В. Основи квантової та постквантової криптографії : методичні вказівки до викон. практич. робіт / І. В. Лімарь. – ДУІТЗ, 2025. – (Спеціальність 125 «Кібербезпека»). 3. Методи та засоби захисту інформації: навч. посібник / В.А. Лахно, Є.В. Васіліу, В.М. Гладких, В.М. Домрачев, Н.М. Сивкова. – К.: ЦП «Компринт» О.В., 2021. – 444 с. 4. Сагун А. В., Хайдуrow В. В., Нікітенко Є. В., Мамченко С. М. Основи криптоаналізу : навч. посіб. / А. В. Сагун та ін. – Київ : Ін-т загальної енергетики НАН України, 2024. 5. Самойлов І. В., Матійко А. А., Сторчак А. С. Криптографія : навч. посіб. / І. В. Самойлов, А. А. Матійко, А. С. Сторчак. – КІП, 2023. – (Спеціальність 125 «Кібербезпека»). 6. Schneier B. Applied

				Cryptography: Protocols, Algorithms and Source Code in C: 20th Anniversary Edition. Wiley, 2015. 784 p. 7. Stavroulakis P., Stamp M. Handbook of Information and Communication Security. Berlin: Springer-Verlag, 2010. 863 p. 8. ДСТУ ISO/IEC 9798. (Стандарт без фіксованого єдиного року видання в тексті). 9. ДСТУ ISO/IEC 15946. (Стандарт без фіксованого єдиного року видання в тексті). 10. Рекомендації X.800. (Міжнародна рекомендація ITU-T без фіксованого року в тексті).
Моніторинг та аудит інформаційно-комунікаційних систем	навчальна дисципліна	ok9-monitoring-ta-audit-informaciino-komunikaciinix-sistem-1.pdf	jl8zJLCVWRFgv5LbSK2sv59ipTo/fYACrgnxf/fWZdQ=	Обладнання: 1. Обладнання з «Лабораторії Кібербезпеки 1» 2. ОС Kali Linux та наявні у ній інструменти тестування Література: 1. Живило Є. О. Тестування на проникнення : навч. посіб. Ч. 1 / за ред. Є. О. Живило. – П. : ПНТУ «Полтавська політехніка ім. Юрія Кондратюка», 2024. – 134 с. 2. Гребенюк А. М., Рибальченко Л. В. Основи управління інформаційною безпекою : навч. посібник. – Дніпро : Дніпроп. держ. ун-т внутріш. справ, 2020. – 144 с. 3. Лахно В. А., Васіліу Є. В., Гладких В. М., Домрачев В. М., Сивкова Н. М. Методи та засоби захисту інформації : навчальний посібник. – К. : ФОП Ямчинський О. В., 2020. – 445 с. 4. Гулак Г. М. Методологія захисту інформації. Аспекти кібербезпеки : підручник. – К. : Видавництво НА СБ України, 2020. – 256 с. 5. Кільдішев В.Й. Моніторинг та аудит інформаційно-комунікаційних систем: методичні вказівки до лабораторних робіт [для здобувачів другого (магістерський) рівня вищої освіти за спеціальністю F5 Кібербезпека та захист інформації] / Уклад.: Кільдішев В.Й., Севастеев Є.О.. Одеса: ДУІТЗ, 2026. 38 с. 6. Кільдішев В.Й. Моніторинг та аудит інформаційно-комунікаційних систем: методичні вказівки до практичних занять [для здобувачів другого (магістерський) рівня вищої освіти за спеціальністю F5 Кібербезпека та захист інформації] / Уклад.: Кільдішев В.Й. Одеса: ДУІТЗ, 2026. 46 с.
Ділова іноземна мова	навчальна дисципліна	ok10_dilova-inozemna-mova-1-1.pdf	/dai2EzzjDep6GJF9srKdLtPDdBWZ9TwYyjAediqL/c=	Література: 1. Chaney, Lillian H. The essential guide to business etiquette / Lillian Hunt Chaney and Jeanette St. Clair Martin. 187 p. URL: http://elibrary.gci.edu.np/bitstream/123456789/685/1/BM-783%20The%20Essential%20Guide%20to%20Business%20Etiquette%20by%20Lillian%20H.%20Chaney%2C%20Jeanette%20S.%20Martin.pdf

				2. Карпова О. Англійська мова для економістів : навчальний посібник. 2-е вид. Одеса: ОНУ, 2021. 132 с. 3. Палеха Ю. І. Етика ділових відносин: навч. посіб. К.: Кондор, 2007. 356 с. Інформаційні ресурси: 1. Baker C. (2023) Are leaders born or made? Leaders. URL: https://leaders.com/articles/leadership/are-leaders-born-or-made/ 2. Erich Power Institute. The Harvard Principles of Negotiations. URL: https://www.youtube.com/watch?v=RfTalFEeKKE&t=42s 3. Knight R. (2023) 8 Essential Qualities for Successful Leaders. Harvard Business Review. URL: https://hbr.org/2023/12/8-essential-qualities-of-successful-leaders 4. Kruse K. (2023) New Research: Women More Effective Than Men in All Leadership Measures. Forbes. URL: https://www.forbes.com/sites/kevinkruse/2023/03/31/new-research-women-more-effective-than-men-in-all-leadership-measures/ 5. Richinick M. (2024) Workplace Etiquette: 21 Dos and Don'ts of the Workplace. URL: https://graduate.northeastern.edu/knowledge-hub/workplace-etiquette/
Практика (виробнича)	практика	<i>ok11_praktyka-vyrobnycha-1.pdf</i>	UXLtqrKrGPxaMvYA BZgYgIktpThCrcpAp BvSP7Q1CwQ=	Обладнання: 1. Лабораторії кафедри Кібербезпеки та технічного захисту інформації. Обладнання на підприємствах стейкхолдерів Література: 1. Наскрізна програма практики за ОПП «Кібербезпека та захист інформації» [для здобувачів другого (магістерського) рівня вищої освіти зі спеціальності F5 Кібербезпека та захист інформації] / Авт.-уклад.: В. Кільдішев, С. Стайкуца, М. Івахненко. Одеса : ДУІТЗ, 2026. 11 с. 2. Стайкуца С.В., Белова Ю.В., Седов К.С., Севастеев Є.О. «Комплексні системи безпеки». Методичні вказівки для виконання лабораторних робіт, Одеса: ДУІТЗ, 2021, 80 с. 3. Методи та засоби захисту інформації [Навчальний посібник] / В.А. Лахно, Є.В. Васіліу, В.М. Гладких, В.М. Домрачев, Н.М. Сивкова. – К. : ФОП Ямчинський О.В., 2020. – 445 с. 4. Гулак Г.М. Методологія захисту інформації. Аспекти кібербезпеки: підручник/ Г.М. Гулак – К.: Видавництво НА СБ України, 2020. – 256 с.
Кваліфікаційна (магістерська) робота. Атестація	підсумкова атестація	<i>ok12_kvalifikatsiina-mahisterska-robota.pdf</i>	DSUbdWxFL+74PC BFQqwxpPkYL2l2hM eVz/aXUloim8=	Література: 1. Методичні вказівки до виконання кваліфікаційних робіт за спеціальністю F5 Кібербезпека та захист

				інформації [для здобувачів освіти першого (бакалаврського) та другого (магістерського) рівня вищої освіти, ОПП «Кібербезпека та захист інформації»] / Авт.-уклад.: Є.В. Васіліу, В.В. Корчинський, В.Й. Кільдішев. Одеса: ДУІТЗ 2026. 47 с. 2. Тестування на проникнення: навч. посіб. Ч.1 / [Є.О. Живило]; за ред. Є.О. Живило. – П.: ПНТУ "Полтавська політехніка ім. Юрія Кондратюка", 2024. – 134 с. 3. Стайкуца С.В., Белова Ю.В., Седов К.С., Севастеев Є.О. «Комплексні системи безпеки». Методичні вказівки для виконання лабораторних робіт, Одеса: ДУІТЗ, 2021, 80 с. 4. Методи та засоби захисту інформації [Навчальний посібник] / В.А. Лахно, Є.В. Васіліу, В.М. Гладких, В.М. Домрачев, Н.М. Сивкова. – К. : ФОП Ямчинський О.В., 2020. – 445 с. Гулак Г.М. Методологія захисту інформації. Аспекти кібербезпеки: підручник/ Г.М. Гулак – К.: Видавництво НА СБ України, 2020. – 256 с.
--	--	--	--	--

* 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)
415091	Чукурна Олена Павлівна	В.о. завідувача кафедри, Основне місце роботи	Бізнесу та соціальних комунікацій	Диплом спеціаліста, ДОНЕЦЬКИЙ ДЕРЖАВНИЙ УНІВЕРСИТЕТ ЕКОНОМІКИ І ТОРГІВЛІ, рік закінчення: 1999, спеціальність: 050108 Маркетинг, Диплом магістра, Національний університет "Одеська політехніка", рік закінчення: 2025, спеціальність: 053 Психологія, Диплом доктора наук ДД 009308, виданий 16.12.2019, Диплом кандидата наук	23	Методологія наукових досліджень та академічна доброчесність	Підвищення кваліфікації: 1. Участь у Міжнародній зимовій школі з підвищення кваліфікації на тему: Соціальні виміри європейських студій (120 год) Certificate № WS2022-000015, 17-28 грудня 2022р. 2. International scientific and practical internship "Information and communication technologies in the digital economy: socio-economic, political, psychological aspects and their impact on the education system" (м. Караганда, Республіка Казахстан, 20 березня 2023 р.- 20 червня 2023 р.). Сертифікат №000034 EF (180 годин, 6 кредитів ЕКТС) 3. International scientific and practical

				ДК 028472, виданий 13.04.2005, Атестат доцента 12ДЦ 022041, виданий 23.12.2008, Атестат професора АП 004056, виданий 06.06.2022		internship "Information and communication technologies in the digital economy: socio-economic, political, psychological aspects and their impact on the education system" (м. Караганда, Республіка Казахстан, 1 березня 2024 р.- 1 червня 2024 р.). Сертифікат №000052 EF (180 годин, 6 кредитів ЄКТС) 4. «Digital Future: Blended Learning» («Цифрове майбутнє: змішане навчання»). Digin.Net 2 Project. German-Ukrainian Digital Innovation Network 2. TOTAL: 180 hours. April 8, 2024 – May 31, 2024. Certificate DN 202405307 від 31.05.2024 р. Supported by DAAD German Academic Exchange Service Digin.Net 2 Project 5. International scientific and practical internship at the Kazakh University of Technology and Business named after K.K. Kulazhanova on the topic of «Data-Driven Marketing and Strategic Management: Analytics, Automation, Artificial Intelligence» (180 hours, 6 credits of ECTS)from «07» April 2025 to «20» September of 2025.CERTIFICATE № 00079 від 20.09.2025 6. Міжнародне підвищення кваліфікації «Implementation of artificial intelligence technologies in business, science and education: prospects and risks» (м. Астана, Республіка Казахстан, 1 червня 2024 р.- 1 вересня 2024 р.). Сертифікат №000135 від 01.09.2024р. (180 годин, 6 кредитів ЄКТС) 7. Тренінг з підвищення кваліфікації з сучасних методів навчання, аналізу останніх досліджень у відповідних галузях, розгляд кейсів із практики сучасних підприємств, а також розвиток управлінських навичок і компетенцій. (м. Астана, Республіка
--	--	--	--	--	--	--

							Казахстан, 2 вересня 2024 р.- 11 жовтня 2024 р.). Сертифікат №0000067 від 01.09.2024р. (180 годин, 6 кредитів ЄКТС) 8. Міжнародне стажування в HigherSchoolofSecurity andEconomicsPlovdiv, Bulgaria «Digital technologies in education and scientific research» (Plovdiv, Bulgaria, 01 April 2024-01 July 2024) Сертифікат BG/HSSENº018-2024, 180 годин (6 кредитів ЄКТС) 9. Тренінг-стажування «Основи організації дуальної форми здобуття освіти за освітніми програмами» в рамках роботи «Школа наставників ДФЗО», м. Івано-Франківськ, 14-24 червня 2024 р., 60 годин (2 кредити ЄКТС) 10. Підвищення кваліфікації з «24 лютого» 2025 року по «02 червня» 2025 р., пройшла навчання за курсом “Цифровізація, цифрова освіта та міграційні процеси: досвід ЄС для України” у ВНЗ «Університет імені Альфреда Нобеля» у рамках реалізації міжнародного проекту Еразмус+ Модуль Жан Моне «Цифровізація, цифрова освіта та міграційні процеси: досвід ЄС для України» у ВНЗ «Університет імені Альфреда Нобеля» №101176312 – DEMEu4U – ERASMUSJMO-2024-HEI-TCH-RSCH. 120 годин (4 кредити ЄКТС). Сертифікат 5681 Наукові публікації: 1. Babenko, V., Chukurn, O., Niekrasova, L., Stanislavyk, O., Tyukhtenko, N., Lytvynenko, O., & Davydko, S. (2023). Methodology for Assessing the Risk of Implementing the Strategy of Diversification of Enterprises in the Aspects of Information Technology
--	--	--	--	--	--	--	--

Management. Journal of Information Technology Management, 15(1), 192-207. doi: 10.22059/jitm.2023.91152 (Scopus Q3)

2. Niekrasova L., Chukurna O. The Methodology of SWOT-Analysis in the Case of Justification Diversification Strategy of the Industry Enterprise. Chapter 6. // Recent Trends in Business and Entrepreneurial Ventures // [Monograf], Edited by Syed Ahmed Salman, Sandeep Poddar, Vitalii Nitsenko. Nova Science Publishers, 2023 DOI: <https://doi.org/10.52305/KZZV1105> (Scopus Springer)

3. Babenko, V., Chukurna, O., Tardaskina, T., Yuliia, T., Pankovets, L. (2026). Methodology of Digital IT Projects Management in the Context of Sustainable Development Strategy. In: Magdi, D., Karam, E., Mamdouh, M., Amit, J. (eds) The Future of Inclusion: Bridging the Digital Divide with Emerging Technologies. ITAF 2024. Lecture Notes in Networks and Systems, vol 1339. Springer, Singapore. https://doi.org/10.1007/978-981-96-5013-2_24 (Scopus Springer).

4. Chukurna O., Tardaskina T., Chaikovska M., Nitsenko V., Tolkachova H., Kholostenko Y. (2025) Methodological principles of forming a marketing GTM strategy for an IT product in the digital economy. Naukovyi Visnyk Natsionalnoho Hirnychoho Universytetu, №5, 162-177 <https://doi.org/10.33271/nvngu/2025-5/162> (Scopus Q3)

5. Чукурна, О., Тардаскіна, Т., & Маслов, О. (2025). Формування AI-методології управління бізнес-моделями в умовах цифрової економіки. Економіка та суспільство, (81). DOI: <https://doi.org/10.32782/2524-0072/2025-81-74>

							Методичні публікації: 1. Чукурна О.П., Конспект лекцій з дисципліни «Методологія наукових досліджень» [для здобувачів другого (магістерський) рівня вищої освіти спеціальності 073 – «Менеджмент»] / [Електронний ресурс]. Одеса: ДУІТЗ. – Електронні текстові дані (1файл: 3751 Кб). 2024. – 104 с. 2. Чукурна О.П. Методичні вказівки до вивчення навчальної дисципліни «Методологія наукових досліджень» [для здобувачів другого (магістерський) рівня вищої освіти спеціальності 073 – «Менеджмент»] / [Електронний ресурс]. Одеса: ДУІТЗ. – Електронні текстові дані (1файл: 457 Кб). 2024. – 25 с.
543832	Снігур Людмила Анатоліївна	Завідувач кафедри, Основне місце роботи	Бізнесу та соціальних комунікацій	Диплом спеціаліста, Одеський державний педагогічний інститут імені К. Д. Ушинського, рік закінчення: 1984, спеціальність: педагогіка і психологія (дошкільна), Диплом доктора наук ДД 004573, виданий 15.12.2005, Атестат доцента ДЦ 001641, виданий 28.03.1995, Атестат професора 12ПР 004520, виданий 22.12.2006	45	Педагогіка та психологія вищої школи	Підвищення кваліфікації: 1. Курси підвищення кваліфікації науково-педагогічних працівників Військова академія (м. Одеса), 01.02.2021-03.03.2021р., Свідоцтво ВА24983020/17/217,2 кредити ЄКТС (216 годин) Наукові публікації: 1. Kryshtanovych, M., Snihur, L., Buzhyna, I., Tiurina, D., Imeridze, M. Development of new information systems with the involvement of artificial intelligence for the men and women's work: A methodical approach to assessment and selection of the optimal. Ingénierie des Systèmes d'Information, 2024. Vol. 29, No. 2, pp. 723-730. https://doi.org/10.18280/isi.290234 2. Психологія особистісного становлення захисника Батьківщини: монографія / за заг. ред. Л. Снігур. Одеса : Юридика, 2024. 322 с. 3. Методичні рекомендації до підготовки кваліфікаційних робіт другого

							(магістерського) рівня вищої освіти спеціальності 053 Психологія. Одеса : ОДУВС, 2024. 35 с. 4. Методичні рекомендації до проведення практики здобувачами вищої освіти другого (магістерського) рівня вищої освіти 053 Психологія. Одеса : ОДУВС, 2024. 31 с. 5. Остапчук Т. С., Снігур Л. А., Слівінський Я. С. Психолого-націологічні основи удосконалення теоретико-методичних засад професійної військової освіти. Філософсько-соціологічні та психолого-педагогічні проблеми підготовки особистості до виконання завдань в особливих умовах : зб. матеріалів наук.-прак. конф. (1 грудня 2022 р.). Київ : Національна академія оборони України, 2022. С. 122-124. 6. Гібало О. В., Остапчук Т. С., Снігур Л. А., Хаджипуло І. С. Мовна практика як засіб підвищення стресостійкості в умовах війни. Наука та освіта у сфері національної безпеки : Уроки російського вторгнення в Україну для ВВНЗ : матеріали міжвузів. наук.-практ. семінару (25 трав. 2022 р.). Одеса : Військова академія (м. Одеса), 2022. С. 10-11.
388876	Онацький Олексій Віталійович	Доцент, Основне місце роботи	Інформаційні технології та кібербезпеки	Диплом спеціаліста, Одеський державний політехнічний університет, рік закінчення: 1995, спеціальність: Радіотехніка, Диплом кандидата наук ДК 007533, виданий 27.06.2000, Атестат доцента 12ДЦ 045225, виданий 15.12.2015	31	Комплекси технічного захисту інформації	Підвищення кваліфікації: 1. Prometheus. Сертифікат «Цифрова безпека на персональному рівні», 2026, (0,2 кредиту ЄКТС) 2. Prometheus. Сертифікат «Інформаційна безпека», 2026,(0,2 кредиту ЄКТС) 3.Prometheus. Сертифікат «Дезінформація: види, інструменти та способи захисту», 2026,(0,2 кредиту ЄКТС) 4. Prometheus. Сертифікат «CS50: Вступ до кібербезпеки», 2026,(1 кредит ЄКТС) 5. Дія Освіта. Сертифікат «Аналітик

							із кібербезпеки», 2025, (0,1 кредит ЄКТС) 6. Дія Освіта. Сертифікат «Кібергігієна: як захиститися від фішингу», 2024, (0,1 кредит ЄКТС) 7. Дія Освіта. Сертифікат «Електронний підпис», 2024, (0,2 кредиту ЄКТС) 8. Дія Освіта. Сертифікат «Доступ до публічної інформації», 2024, (0,2 кредиту ЄКТС) 9. Дія Освіта. Сертифікат «Цифрові гроші», 2024, (0,1 кредиту ЄКТС) 10. Дія Освіта. Сертифікат. Курс «Персональні дані», 2023, (0,2 кредиту ЄКТС) 11. USAID. Certificate «Foundations of Computer and Network Security» – USAID Cybersecurity for Critical Infrastructure in Ukraine Activity, 2022, (6 ECTS credits, 180 годин) Наукові публікації: 1. Onatskiy Oleksiy. Two-Factor Authentication Protocol Based on Zero-Knowledge Proof Using Elliptic Curves. In: Ilchenko, M., Uryvsky, L., Globa, L. (eds) Advanced Smart Information and Communication Technology and Systems. MCT 2024. Lecture Notes in Networks and Systems, vol 1470. Springer, Cham. 2025. Pp. 3-26. DOI:10.1007/978-3-031-94799-5_1 2. Strelkovskaya Irina V., Onatskiy Oleksiy V., Yona Larysa G. Two-factor authentication protocol in access control systems. Information and telecommunication sciences : international research journal. 2023. Vol. 14, N. 2. Pp. 17-25. https://doi.org/10.20535/2411-2976.22023.17-25 3. Onatskiy O. Two-Factor Authentication Protocol with Zero-Knowledge over an Extended Field of Elliptic Curves, 2023 IEEE International Conference on Information and
--	--	--	--	--	--	--	--

							Telecommunication Technologies and Radio Electronics (UkrMiCo), Kyiv, Ukraine, 2023.Pp. 54-57, https://doi.org/10.1109/UkrMiCo61577.2023.10380362
							4. Онацький, О. Модифікація порогових схем розподілу секрету Шаміра та Блеклі на еліптичних кривих. Інфокомунікаційні та комп'ютерні технології, 1(03), 2022. С. 267-283. https://doi.org/10.36994/2788-5518-2022-01-03-16
							5. Онацький О.В. Методологія створення комплексної системи захисту інформації. Прикладная радиоэлектроника: нау ч.-техн. журнал ХНУР. Том 13,2014. С. 350-356.
							6. Onatskyi O., Zharova O. Comparative analysis of homomorphic properties of RSA and Paillier. ATICE'2025 : Proc. Int. Conf. Odesa, 2025. Pp. 68–72.
							7. Onatskyi O., Zharova O. Implementation of attribute-based encryption using the secp256k1 elliptic curve for ensuring data confidentiality in cloud environments. Proc. 80th Int. Sci. Conf. Odesa : DUITZ, 2025. Pp. 322–325.
							8. Onatskyi O., Zharova O., Dygalo Y. Cryptographic protocol key exchange on elliptic curves. ATICE'2024 : Proc. Conf. Odesa, 2024. Pp. 63–67.
							9. Onatskyi O., Marushyna K., Zharova O. Digital signatures Nyberg-Rueppel without message recovery on extended field supersingular elliptic curves. European congress of scientific achievements. Barcelona, 2024. Pp. 160–164.
							10. Onatskyi O., Humenna A., Zemliak S., Zharova O. Authentication protocol with zero-knowledge proof over the extended GF(2m) elliptic curve field. Modern research in world science. Lviv, 2022. Pp. 451–454.
							11. Onatskyi O., Kotienieva I., Zharova

								O. Threshold secret sharing scheme on the elliptic curves. Scientific research in the modern world. Toronto, 2022. P. 192–195. 12. Онацький О.В. Аналіз програмних і технічних засобів захисту інформації. Матеріали 72-га науково-технічної конференції професорсько-викладацького складу, науковців, молодих вчених, аспірантів та студентів ОНАЗ ім. О.С. Попова. Частина І. Одеса, 2017. С. 135 – 137. 13. Онацький О.В. Аналіз системи виявлення вторгнень. Матеріали 72-га науково-технічної конференції професорсько-викладацького складу, науковців, молодих вчених, аспірантів та студентів ОНАЗ ім. О.С. Попова. Одеса, 2017. С. 106 – 107. 14. Онацький О.В. Створення комплексної системи захисту інформації в інформаційно-телекомунікаційній системі. Матеріали 72-га науково-технічної конференції професорсько-викладацького складу, науковців, молодих вчених, аспірантів та студентів ОНАЗ ім. О.С. Попова. Одеса, 2017. С. 152 – 154. 15. Онацький О.В. Щодо питань захисту інформаційних ресурсів медичних підприємств. Матеріали 75-а науково-технічної конференції професорсько-викладацького складу, науковців, молодих вчених, аспірантів та студентів ОНАЗ ім. О.С. Попова. Одеса, 2020. С. 122 – 124. 16. Онацький О.В. Аналіз комплексів засобів захисту від несанкціонованого доступу на базі операційної системи. 73-я науково-технічна конференція професорсько-викладацького складу, науковців, аспірантів та студентів ОНАЗ ім. О.С. Попова. Одеса, 2018. С. 145 – 146. 17. Йона Л. Г., Онацький О. В.,
--	--	--	--	--	--	--	--	--

							Швець О. В. Системи банківської безпеки : навч. посіб. Одеса : ДУІТЗ, 2022. 192 с. 18. Онацький О. В., Йона Л. Г., Белова Ю. В. Криптографічний захист інформації : навч. посіб. з дисципліни «Криптографічний захист інформації». Одеса : Астропринт, 2023. 252 с.
388804	Корчинський Володимир Вікторович	Завідувач кафедри, Основне місце роботи	Інформаційні технології та кібербезпеки	Диплом спеціаліста, Одеський електротехнічний інститут зв'язку ім. О.С. Попова, рік закінчення: 1987, спеціальність: Автоматичний електрозв'язок, Диплом доктора наук ДД 004043, виданий 26.02.2015, Атестат доцента 12ДЦ 030616, виданий 17.02.2012, Атестат професора АП 002496, виданий 09.02.2021	28	Управління доступом до інформаційних ресурсів	Підвищення кваліфікації: 1. Корчинський В.В., Мар'ян М.О., Богданюк І. А., Аль-Файюмі Халед. Метод захисту інформації від несанкціонованого доступу на основі динамічного хаосу. Proceedings of the 4th International Scientific and Practical Conference «Diversity and Inclusion in Scientific Area» (March 26-28, 2024). Warsaw, Poland, Scientific Collection «InterConf» 2024. Р. 448-453. 12 год (0,4 кредити ЕКТС). https://archive.interconf.center/index.php/conference-proceeding/article/view/5775/5811 2. Корчинський В.В., Сокур Д. І., Белова Ю. В. Аналіз вразливостей та стратегії захисту веб-додатків від CSRF-атак // Scientific Collection «InterConf»: «Scientific Paradigm in the Context of Technologies and Society Development» held on August 26-28, 2024 in Boston, USA, P. 129-136. 12 год (0,4 кредити ЕКТС). https://archive.interconf.center/index.php/conference-proceeding/issue/view/26-28.08.2024/224 3. Корчинський В.В., Лімарь І. В., Белова Ю.В., Демешко В.В. Аналіз ефективності алгоритмів машинного навчання для виявлення аномалій у системах інформаційної безпеки. Impact of Artificial Intelligence and Other Technologies on Sustainable Development: Proceedings of the 2nd International Scientific and Practical Internet Conference, December

						18-19, 2024. FOP Marenichenko V.V., Dnipro, Ukraine, P. 111-112. 6 год (0,2 кредити ЄКТС). 4. Корчинський В.В., Шпильова М.І., Лімарь І.В., Попадюк В.О. Аналіз методів побудови системи керування доступу на основі симуляторів. Міжнародна науково-практична конференція «Development of education, science and business: Results 2024: Proceedings of the International Scientific and Practical Internet Conference, December 11-12, 2024. FOP Marenichenko V.V., Dnipro, Ukraine, P. 180-182. 6 год (0,2 кредити ЄКТС). 5. Корчинський В.В. Науково-практичний семінар «Електронні комунікації сьогодні і завтра». (м. Львів, 11 жовтня 2024 року). 6 год (0,2 кредити ЄКТС). Професійний досвід: Інженер-конструктор 1 категорії Спеціального конструкторського бюро "Молнія" Наукові публікації: 1. Korchynskiy V., Kildishev V., Bektursunov D., Havel S., Stepanov V., Slavych V., Petrovskiy R. Development of method foundations for generating noise-like signals based on direct sequence spread spectrum of timing signal structures. Technology audit and production reserves. 2026. №1(87). P. 18-24. https://doi.org/10.15587/2706-5448.2026.353067 2. Гавель, С., Корчинський, В., Степанов, В., & Куртіков, М. Методи підвищення криптографічної стійкості псевдовипадкових послідовностей на основі генераторів хаосу. Herald of Khmelnytskyi National University. Technical Sciences. 2026. 363(2), С. 149-154. https://doi.org/10.31891/2307-5732-2026-363-19 3. Kopytin, Y.,
--	--	--	--	--	--	---

						безпеки, навчально-методичні вказівки до виконання самостійних робіт (частина 1) [для здобувачів першого (бакалаврського) рівня вищої освіти за спеціальністю «Кібербезпека та захист інформації»]. / Уклад., Корчинський В.В., Шпильова М.І., Івахненко М.С., Одеса, ДУТЗ, 2025, 86 с. 9. Керування доступом в системах безпеки, навчально-методичні вказівки до виконання самостійних робіт (частина 2) [для здобувачів першого (бакалаврського) рівня вищої освіти за спеціальністю «Кібербезпека та захист інформації»]. / Уклад., Корчинський В.В., Шпильова М.І., Івахненко М.С., Одеса, ДУТЗ, 2025, 49 с. 10. Корчинський, В., Тарасенко, І., Рациборинський, С., Акаєв, О., & Хаджиогло, А. Автоматизовані системи керування доступом. Herald of Khmelnytskyi National University. Technical Sciences, 2024. 333(2). С. 140-145. https://doi.org/10.31891/2307-5732-2024-333-2-22 11. Семенко А.І., Бойко Ю.М., Шпур О.М., Стрелковська І.В., Корчинський В.В., Яровий Р.О. Сучасні технології інфокомунікаційних та комп'ютерних мереж: монографія / За загальною науковою редакцією А.І. Семенка. Київ: Європейський університет, Аграр Медіа Прінт, 2024. 562 с. ISBN 978-966-301-266-7. 12. Сталий розвиток і цифрові інновації: монографія / за заг. ред. Буркінського Б.В., Назаренко О.А., Лайко О.І., Хаджираєвої С.К. та ін.; НАН України, МОН України, ДУ «Ін-т ринку та економ.-екол. дослідж.», Державний університет інтелектуальних технологій і зв'язку. Одеса, ДУ ІРЕЕД НАНУ, 2024. 543 с.
--	--	--	--	--	--	--

							13. Корчинський В.В., Лімарь І. В., Белова Ю.В., Демешко В.В. Аналіз ефективності машинного навчання для виявлення аномалій у системах інформаційної безпеки. Impact of Artificial Intelligence and Other Technologies on Sustainable Development: Proceedings of the 2nd International Scientific and Practical Internet Conference, December 18-19, 2024. FOP Marenichenko V.V., Dnipro, Ukraine, P. 111-112. 14. Корчинський В.В., Шпильова М.І., Лімарь І.В., Попадюк В.О. Аналіз методів побудови системи керування доступу на основі симуляторів. Міжнародна науково-практична конференція «Development of education, science and business: Results 2024», December 11-12, 2024. FOP Marenichenko V.V., Dnipro, Ukraine, P. 180-182. 15. Korchynskiy V., Hordiichuk V., Kildishev V., Riabukha O., Staikutsa S., Khaled Alfaioni. Method of information protection based on the integration of probabilistic encryption and noise immune coding. Radioelectronic and computer systems, 2023.4.13, P.184-185. http://nti.khai.edu/ojs/index.php/reks/article/view/reks.2023.4.13 16. Корчинський, В., Рябуха, О., Халед, А.-Ф., Гавель, С., Міненко, В., & Криштафор, З. Дослідження варіаційних можливостей генераторів хаосу по формуванню псевдовипадкових послідовностей. Measuring and computing devices in technological processes, (1). 2023. С. 180–186. https://doi.org/10.31891/2219-9365-2023-73-1-24 17. Корчинський, В., Стайкуца, С. В., Виноградов, І., Швець, О. В., & Белова, Ю. В. Методи підвищення якості
--	--	--	--	--	--	--	--

							перетворення мови на текст в системах біометричної аутентифікації. Інфокомунікаційні та комп'ютерні технології, 2023. 1(05). С. 114-122. https://doi.org/10.36994/2788-5518-2023-01-05-13 18. Корчинський В.В. Халед Аль-Файюмі. Методи застосування динамічного хаосу в системах захисту інформації. Забезпечення кібероборони держави: збірник матеріалів IV науково-практичного вебінару 10 листопада 2023 року м. Київ. К.: НУОУ, 2023. С. 81-83. 19. Корчинський В.В., Рябуха О.М., Аль-Файюмі Х.О., Василенко А.Ю. Метод захисту інформації на основі ймовірнісного шифрування. 78-а Науково-технічна конференція професорсько-викладацького складу, науковців, аспірантів та студентів, Одеса, ДУІЗ, 21-22 листопада 2023 року. С. 154-156. 20. Korchynskyi V., Onyshchuk V., Kildishev V., Khaled Alfaiomi. Productivity of Modern Homomorphous Cryptosystems in Recommendation Systems of Web Services. Conference Proceedings 16th International Conference on Advanced Trends in Radioelectronics, Telecommunications and Computer Engineering (TCSET), February 22-26, 2022, P. 331-334. DOI: 10.1109/TCSET55632.2022.9766911
414119	Васіліу Євген Вікторович	Професор, Суміщення	Інформаційні технології та кібербезпеки	Диплом доктора наук ДД 001021, виданий 17.05.2012, Атестат професора 12ПР 010915, виданий 29.09.2015	31	Менеджмент в системі корпоративної інформаційної безпеки	Підвищення кваліфікації: 1. Erasmus + project Jean Monnet module, сертифікат, EU Best Practices for Trustworthy and Reliable AI, 2026, 40 годин (1,33 кредити). 2. Mykolas Romeris University, сертифікат, "Social and Technological Transformations in a Changing", 2025, 180 годин (6 кредитів).

						3. Universitat Gamburg, сертифікат «Освіта в фокусі сучасних трендів, викликів та технологій», 2025, 30 годин (1 кредит). 4. Erasmus + project Jean Monnet module, сертифікат, “The European experience for enhancement the resilience of critical entities in Ukraine”, 2025, 120 годин (4 кредити). 5. Агентство США з міжнародного розвитку (USAID), сертифікат, “Foundations of Computer and Network Security”, 2022, 180 годин (6 кредитів). Професійний досвід: 1. Координатор проекту USAID Cybersecurity for Critical Infrastructure in Ukraine з 2021 по 2024 рр.: 1. Сертифікат про подяку від 28 грудня 2022 року за взірцеву підтримку в узгодженні направлень на навчання інструкторів в Державному університеті інтелектуальних технологій і зв'язку. 2. Сертифікат про визнання від 28 грудня 2021 року за максимальні зусилля та досягнення високих результатів у злагодженості, направлення на навчання вчителів (викладачів) та організацію заходів з Державним університетом інтелектуальних технологій і зв'язку за проектом USAID «Кібербезпека для критичної інфраструктури в Україні». Наукові публікації: 1. Маніпулювання: технології й засоби впливу та шляхи захисту: навчальний посібник / Петрик В. М., Присяжнюк М. М., Черненко О. Є., Карпович О. М., Закаблуковська О. О. та ін. За заг. ред. В. М. Петрика, М. М. Присяжнюка. – К.: Видавничий центр “Кафедра”, 2026. – 336 с. 2. Методи та засоби захисту інформації : навч. посіб. / В. А.
--	--	--	--	--	--	--

Лахно, Є. В. Васіліу, В. М. Гладких, В. М. Домрачев, Н. М. Сивкова. Київ : ЦП «Компринт» О. В., 2021. 444 с.

3. Havel S., Vasiliu Y., Bardis N., Staikutsa S. Eavesdropping Attack of Two Eavesdroppers on the Ping-Pong Protocol with GHZ triplets // 2025 IEEE 13th International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications (IDAACS), Gliwice, Poland, 2025, pp. 1-5. <https://doi.org/10.1109/IDAACS68557.2025.11322111>

4. Vasiliu Y. Modern quantum technologies of cryptographic protection of information. Cybernetics and Systems Analysis. 2025. Vol. 61, No. 4. P. 671–684. <https://doi.org/10.1007/s10559-025-00801-y>

5. Васіліу Є. В. Сучасні квантові технології криптографічного захисту інформації. Кібернетика та системний аналіз. 2025. Т. 61, № 4. С. 160–175. <https://doi.org/10.34229/KCA2522-9664.25.4.13>

6. Younis M. M., Salim Jamil A., Abdulrazzaq A. H., Ahmed Mawla N., Khudhair R. M., Vasiliu Y. Progress and challenges in quantum computing algorithms for NP-hard problems. Proceedings of the 36th Conference of Open Innovations Association (FRUCT). Lappeenranta, Finland, 2024. P. 460–468. <https://doi.org/10.23919/FRUCT64283.2024.10749878>

7. Vasiliu Ye., Okhrimenko T., Fesenko A., Dorozhynskyy S. Passive Eavesdropping Attack of Several Intruders on Deterministic Protocol with Pairs of Entangled Qubits. The 11th IEEE International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications. 22-25

							September, 2021, Cracow, Poland. – V. 1. – P. 1068–1072. https://doi.org/10.1109/IDAACS53288.2021.9660851. 8. Yevhen Vasiliu, Igor Limar, Tomasz Gancarczyk, Mikołaj Karpiński. New Quantum Secret Sharing Protocol Using Entangled Qutrits // 2019 10th IEEE International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications (IDAACS). – Metz, France, 18 – 21 September 2019. – V. 1. – P. 324–329. https://doi.org/10.1109/IDAACS.2019.8924256 9. Zhengbing Hu, Yevhen Vasiliu, Oleksii Smirnov, Viktoriia, Sydorenko, Yuliia Polishchuk. Abstract Model of Eavesdropper and Overview on Attacks in Quantum Cryptography Systems / // 2019 10th IEEE International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications (IDAACS). – Metz, France, 18 – 21 September 2019. – V. 1. – P. 399–405. https://doi.org/10.1109/IDAACS.2019.8924286
414119	Васіліу Євген Вікторович	Професор, Суміщення	Інформаційних технологій та кібербезпеки	Диплом доктора наук ДД 001021, виданий 17.05.2012, Аттестат професора 12ПР 010915, виданий 29.09.2015	31	Криптологія	Підвищення кваліфікації: 1. Erasmus + project Jean Monnet module, сертифікат, EU Best Practices for Trustworthy and Reliable AI, 2026, 40 годин (1,33 кредиту). 2. Mykolas Romeris University, сертифікат, "Social and Technological Transformations in a Changing", 2025, 180 годин (6 кредитів). 3. Universitat Gamburg, сертифікат «Освіта в фокусі сучасних трендів, викликів та технологій», 2025, 30 годин (1 кредит). 4. Erasmus + project Jean Monnet module, сертифікат, “The European experience for enhancement the resilience of critical entities in Ukraine”,

							2025, 120 годин (4 кредити). 5. Агентство США з міжнародного розвитку (USAID), сертифікат, “Foundations of Computer and Network Security”, 2022, 180 годин (6 кредитів). Професійний досвід: 1. Координатор проєкту USAID Cybersecurity for Critical Infrastructure in Ukraine з 2021 по 2024 рр.: 1. Сертифікат про подяку від 28 грудня 2022 року за вірцеву підтримку в узгодженні направлень на навчання інструкторів в Державному університеті інтелектуальних технологій і зв'язку. 2. Сертифікат про визнання від 28 грудня 2021 року за максимальні зусилля та досягнення високих результатів у злагодженості, направлення на навчання вчителів (викладачів) та організацію заходів з Державним університетом інтелектуальних технологій і зв'язку за проектом USAID «Кібербезпека для критичної інфраструктури в Україні». Наукові публікації: 1. Маніпулювання: технології й засоби впливу та шляхи захисту: навчальний посібник / Петрик В. М., Присяжнюк М. М., Черненко О. Є., Карпович О. М., Закаблуківська О. О. та ін. За заг. ред. В. М. Петрика, М. М. Присяжнюка. – К.: Видавничий центр “Кафедра”, 2026. – 336 с. 2. Методи та засоби захисту інформації : навч. посіб. / В. А. Лахно, Є. В. Васіліу, В. М. Гладких, В. М. Домрачев, Н. М. Сивкова. Київ : ЦП «Компринт» О. В., 2021. 444 с. 3. Havel S., Vasiliu Y., Bardis N., Staikutsa S. Eavesdropping Attack of Two Eavesdroppers on the Ping-Pong Protocol with GHZ triplets // 2025 IEEE 13th International
--	--	--	--	--	--	--	--

							Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications (IDAACS), Gliwice, Poland, 2025, pp. 1-5. https://doi.org/10.1109/IDAACS68557.2025.11322111
							4. Vasiliu Y. Modern quantum technologies of cryptographic protection of information. Cybernetics and Systems Analysis. 2025. Vol. 61, No. 4. P. 671–684. https://doi.org/10.1007/s10559-025-00801-y
							5. Васіліу Є. В. Сучасні квантові технології криптографічного захисту інформації. Кібернетика та системний аналіз. 2025. Т. 61, № 4. С. 160–175. https://doi.org/10.34229/KCA2522-9664.25.4.13
							6. Younis M. M., Salim Jamil A., Abdulrazzaq A. H., Ahmed Mawla N., Khudhair R. M., Vasiliu Y. Progress and challenges in quantum computing algorithms for NP-hard problems. Proceedings of the 36th Conference of Open Innovations Association (FRUCT). Lappeenranta, Finland, 2024. P. 460–468. https://doi.org/10.23919/FRUCT64283.2024.10749878
							7. Vasiliu Ye., Okhrimenko T., Fesenko A., Dorozhynskyy S. Passive Eavesdropping Attack of Several Intruders on Deterministic Protocol with Pairs of Entangled Qubits. The 11th IEEE International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications. 22-25 September, 2021, Cracow, Poland. – V. 1. – P. 1068–1072. https://doi.org/10.1109/IDAACS53288.2021.9660851
							8. Yevhen Vasiliu, Igor Limar, Tomasz Gancarczyk, Mikołaj Karpiński. New Quantum Secret Sharing Protocol Using Entangled Qutrits // 2019 10th IEEE

							International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications (IDAACS). – Metz, France, 18 – 21 September 2019. – V. 1. – P. 324–329. https://doi.org/10.1109/IDAACS.2019.8924256 9. Zhengbing Hu, Yevhen Vasiliu, Oleksii Smirnov, Viktoriia, Sydorenko, Yuliia Polishchuk. Abstract Model of Eavesdropper and Overview on Attacks in Quantum Cryptography Systems / // 2019 10th IEEE International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications (IDAACS). – Metz, France, 18 – 21 September 2019. – V. 1. – P. 399–405. https://doi.org/10.1109/IDAACS.2019.8924286
400423	Стайкуца Сергій Володимирович	Доцент, Основне місце роботи	Інформаційних технологій та кібербезпеки	Диплом спеціаліста, Українська державна академія зв'язку імені О.С. Попова, рік закінчення: 2001, спеціальність: 092401 Автоматичний електрозв'язок, Диплом кандидата наук ДК 055529, виданий 14.10.2009, Аттестат доцента 12ДЦ 044266, виданий 29.09.2015	23	Комплексні системи безпеки	Підвищення кваліфікації: 1. As part of the Summer school'2025 under Erasmus + project Jean Monnet module: “The European experience for enhancement the resilience of critical entities in Ukraine”, 21 July – 08 August 2025, 120 год (4 кредити). 2. Mykolas Romeris University (Vilnius, Lithuania), сертифікат No. 5KV-16797, «Social and Technological Transformations in a Changing», 15.04.2025-31.05.2025, University Code 111951726, 180 годин (6 кредитів) 3. USAID Project “Cybersecurity for Critical Infrastructure in Ukraine” Course Security Audit and Risk Management 12 July – 23 August 2022, 90 год (3 кредити); 4. Security Audit and Risk Management Course, 40 (forty) continuing professional education hours, ISACA Kyiv Chapter, Certificate of 29.08.2022, 40 год. (1,3 кредити); Професійний досвід:

						1. З листопада 2016 р. – керівник лабораторії технічних засобів охорони та технічного захисту інформації кафедри КБ та ТЗІ ДУІТЗ (Протокол №3 кафедри ІБ та ПД від 18 листопада 2016 р. 2. З серпня 2025 р. – керівник лабораторії сучасних систем відеоаналітики (проектна лабораторія Kobi Software) (Протокол №1 кафедри ІБ та ПД від 25 серпня 2025 р. 3. З 2015 по 2021 р. – Управитель систем інформаційної безпеки 4. З травня 2018 р. – заступник голови ГО “Технологічний кластер Одеського регіону” Наукові публікації: 1. Петрик В. М., Кононович В. Г., Аль-Файюмі Халед, Музиченко К. М. та ін. Кібергігієна: аналіз у контексті кіберпсихології та соціальної інженерії : навч. посіб. / за заг. ред. В. М. Петрика, С. В. Стайкуци, Аль-Файюмі Халеда. Київ : Видавничий центр «Кафедра», 2026. 360 с. (1,5 автор. стор.) 2. Havel S., Vasiliu Y., Bardis N., Staikutsa S. Eavesdropping attack of two eavesdroppers on the Ping-Pong protocol with GHZ triplets. 2025 IEEE 13th International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications (IDAACS). Gliwice, Poland, 2025. P. 1–5. DOI: 10.1109/IDAACS68557.2025.11322111 3. Соціальна інженерія та кіберпсихологія : монографія / Кононович В. Г., Стайкуца С. В., Тодорова М. М., Воронова С. В., Рябуха О. М. Одеса : ДУІТЗ, 2025. 390 с. (1,5 автор. стор.) 4. Стайкуца С., Похлебін Т., Андрєєв М. Таксономія загроз та ризиків сучасних автотранспортних засобів. 80-та ювілейна Міжнародна науково-технічна
--	--	--	--	--	--	--

							конференція професорсько-викладацького складу, науковців, аспірантів та студентів : зб. матеріалів, м. Одеса, 26 листоп. 2025 р. Одеса : Астропринт, 2025. С. 328–331. ISBN 9786178569–79–5. Стайкуца С., Пастухов Д., Селюкова А. Дослідження інформаційного середовища сучасних компаній методами та інструментами OSINT. Наука, технології, інновації: вектори трансформації : матеріали наук.-практ. конф., м. Ужгород, 24–25 жовт. 2025 р. Одеса : Молодий вчений, 2025. С. 106–110. 6. Kononovych V., Staikutsa S. Integration of cyber-psychological security and cybersecurity. Democratic Governance in the Context of Geopolitical Challenges : Proceedings of the 12th International Scientific and Practical Conference, Vilnius, May 14, 2025. 2025. P. 25–26. 7. Hordiichuk V., Korchynskiy V., Kildishev V., Molodetskiy B., Staikutsa S., Alfaiomi K. Adaptive synthesis of wideband timer signals in the conditions of radio-electronic warfare. 2024 IEEE 17th International Conference on Advanced Trends in Radioelectronics, Telecommunications and Computer Engineering (TCSET). 2024. P. 1–4. 8. Osama O. F., Hussain R. T., Al-Ani A. R. M., Issa S. S., Abdullah I., Staikutsa S., Kanbar A. B. Exploring the security landscape of the Arduino Due in a 6G environment. Proceedings of the 36th Conference of Open Innovations Association (FRUCT). 2024. P. 178–187. 9. Стайкуца С., Гонімар В. Кібергігієна як основа формування безпеки особистості, підприємства та держави. Спільні дії військових формувань і правоохоронних
--	--	--	--	--	--	--	---

							органів держави : матеріали конф. Одеса, 2024. 10. Korchynskyi V., Hordiichuk V., Kildishev V., Riabukha O., Staikutsa S., Alfaiomi K. Method of information protection based on the integration of probabilistic encryption and noise-immune coding. Radioelectronic and Computer Systems. 2023. No. 4. P. 184–195. URL: http://nti.khai.edu/ojs/index.php/reks/article/view/reks.2023.4.13 11. Корчинський В., Стайкуца С. В., Виноградов І., Швець О. В., Белова Ю. В. Методи підвищення якості перетворення мови на текст в системах біометричної аутентифікації. Інфокомунікаційні та комп'ютерні технології. 2023. № 1 (05). С. 114–122. DOI: https://doi.org/10.36994/2788-5518-2023-01-05-13 12. Кононович В. Г., Стайкуца С. В., Бердніков О. М., Севаст'єв Є. О., Швець О. В. Інформаційна безпека інноваційної діяльності в інфокомунікаціях : підручник та дистанційний практикум / за ред. В. В. Корчинського. 2-ге вид., виправл. і доповн. Одеса : ДУІТЗ, 2023. 378 с. (1,5 автор.стор.)
388823	Кільдішев Віталій Йосипович	Доцент, Основне місце роботи	Інформаційні технології та кібербезпеки	Диплом магістра, Українська державна академія зв'язку імені О.С. Попова, рік закінчення: 2001, спеціальність: 092402 Багатоканальний електрозв'язок, Диплом доктора наук ДД 014349, виданий 26.02.2026, Диплом кандидата наук ДК 046943, виданий 21.05.2008, Аттестат доцента 12ДЦ 034732, виданий	24	Кіберфізична безпека об'єктів критичної інфраструктури	Підвищення кваліфікації: 1. Social and Technological Transformations in a Changing, Mykolas Romeris University, 08 April– 31 May 2026, Certificate№5KV-20779of 31.05.2026, 180 год. (6 кредитів). 2. As part of the Summer school'2025 under Erasmus + project Jean Monnet module: “The European experience for enhancement the resilience of critical entities in Ukraine”, Certificate of 08.08.2025, 120 год. (4 кредити). 3. USAID Project “Cybersecurity for Critical Infrastructure in Ukraine” Course Security Audit and Risk

				28.03.2013		Management 12 July – 23 August 2022, Certificate of 23.08.2022, 90 год (3 кредити); 4. Security Audit and Risk Management Course, 40 (forty) continuing professional education hours, ISACA Kyiv Chapter, 12 July – 23 August 2022, Certificate of 29.08.2022, 40 год. (1,3 кредити). Наукові публікації: 1. Stepanov, V., Korchynskyi, V., Kildishev, V., Zarovskiy, R., Havel, S., Slavych, V., & Petrovskiy, R. (2026). Devising a combined spectrum spreading method for timer signal structures to improve covert information transmission. Eastern-European Journal of Enterprise Technologies, 3(9 (141), 16–25. https://doi.org/10.15587/1729-4061.2026.365354 2. Korchynskyi V, Kildishev V., Bektursunov D., Havel S., Stepanov V., Slavych V., Petrovskiy R. (2026). Development of method foundations for generating noise-like signals based on direct sequence spread spectrum of timing signal structures. Technology audit and production reserves. №1(87), C. 18-24. https://doi.org/10.15587/2706-5448.2026.353067 3. V. Hordiichuk, V. Korchynskyi, V. Kildishev, B. Molodetskyi, S. Staikutsa and K. Alfaiomi, "Adaptive Synthesis of Wideband Timer Signals in the Conditions of Radio-Electronic Warfare," 2024 IEEE 17th International Conference on Advanced Trends in Radioelectronics, Telecommunications and Computer Engineering (TCSET), Lviv, Ukraine, 2024, pp. 1-4, doi: 10.1109/TCSET64720.2024.10755658. https://ieeexplore.ieee.org/document/10755658/ 4. Korchynskyi V., Hordiichuk V.,
--	--	--	--	------------	--	--

						Kildishev V., Riabukha O., Staikutsa S., Khaled A. Method of information protection based on the integration of probabilistic encryption and noise immune coding. Radioelectronic and computer systems. 2023.4.13, P.184-185. 5. Onyshchuk Valentyn, Kildishev Vitalii, Korchynskyi Volodymyr and Alfaioni Khaled. Productivity of Modern Homomorphous Cryptosystems in Recommendation Systems of Web Services: Conference Proceedings 16th International Conference on Advanced Trends in Radioelectronics, Telecommunications and Computer Engineering (TCSET) – Lviv-Slavske, Ukraine February 22-26, 2022, P. 331-334. 6. Hordiichuk Valerii, Korchynskyi Volodymyr, Kildishev Vitalii, Zakharchenko Mykola. Timer Signals Transmission Security Increase Based on Spectrum Spreading Methods: 2022 IEEE 2nd Ukrainian Microwave Week (UkrMW) 14-18 November 2022, P. 331-334. Методичне забезпечення: 1. Моніторинг та аудит інформаційно-комунікаційних систем: методичні вказівки до лабораторних робіт [для здобувачів другого (магістерський) рівня вищої освіти за спеціальністю F5 Кібербезпека та захист інформації] / Уклад.: Кільдішев В.Й., Севастєєв Є.О. Одеса: ДУІТЗ, 2026. 38 с. 2. Моніторинг та аудит інформаційно-комунікаційних систем: методичні вказівки до практичних занять [для здобувачів другого (магістерський) рівня вищої освіти за спеціальністю F5 Кібербезпека та захист інформації] / Уклад.: Кільдішев В.Й.. Одеса: ДУІТЗ, 2026. 46 с.
--	--	--	--	--	--	--

388823	Кільдішев Віталій Йосипович	Доцент, Основне місце роботи	Інформаційні технології та кібербезпеки	Диплом магістра, Українська державна академія зв'язку імені О.С. Попова, рік закінчення: 2001, спеціальність: 092402 Багатоканальний електрозв'язок, Диплом доктора наук ДД 014349, виданий 26.02.2026, Диплом кандидата наук ДК 046943, виданий 21.05.2008, Атестат доцента 12/ДЦ 034732, виданий 28.03.2013	24	Моніторинг та аудит інформаційно-комунікаційних систем	Підвищення кваліфікації: 1. Social and Technological Transformations in a Changing, Mykolas Romeris University, 08 April– 31 May 2026, Certificate №5KV-207790 of 31.05.2026, 180 год. (6 кредитів). 2. As part of the Summer school'2025 under Erasmus + project Jean Monnet module: "The European experience for enhancement the resilience of critical entities in Ukraine", Certificate of 08.08.2025, 120 год. (4 кредити). 3. USAID Project "Cybersecurity for Critical Infrastructure in Ukraine" Course Security Audit and Risk Management 12 July – 23 August 2022, Certificate of 23.08.2022, 90 год (3 кредити); 4. Security Audit and Risk Management Course, 40 (forty) continuing professional education hours, ISACA Kyiv Chapter, 12 July – 23 August 2022, Certificate of 29.08.2022, 40 год. (1,3 кредити). Наукові публікації: 1. Stepanov, V., Korchynskyi, V., Kildishev, V., Zarovskiy, R., Havel, S., Slavych, V., & Petrovskiy, R. (2026). Devising a combined spectrum spreading method for timer signal structures to improve covert information transmission. Eastern-European Journal of Enterprise Technologies, 3(9 (141), 16–25. https://doi.org/10.15587/1729-4061.2026.365354 2. Korchynskyi V, Kildishev V., Bektursunov D., Havel S., Stepanov V., Slavych V., Petrovskiy R. (2026). Development of method foundations for generating noise-like signals based on direct sequence spread spectrum of timing signal structures. Technology audit and production reserves. №1(87), C. 18-24. https://doi.org/10.15587/2706-
--------	-----------------------------	------------------------------	---	--	----	--	--

5448.2026.353067
3. V. Hordiichuk, V. Korchynskyi, V. Kildishev, B. Molodetskyi, S. Staikutsa and K. Alfaioni, "Adaptive Synthesis of Wideband Timer Signals in the Conditions of Radio-Electronic Warfare," 2024 IEEE 17th International Conference on Advanced Trends in Radioelectronics, Telecommunications and Computer Engineering (TCSET), Lviv, Ukraine, 2024, pp. 1-4, doi: 10.1109/TCSET64720.2024.10755658. <https://ieeexplore.ieee.org/document/10755658/>
4. Korchynskyi V., Hordiichuk V., Kildishev V., Riabukha O., Staikutsa S., Khaled A. Method of information protection based on the integration of probabilistic encryption and noise immune coding. Radioelectronic and computer systems. 2023.4.13, P.184-185.
5. Onyshchuk Valentyn, Kildishev Vitalii, Korchynskyi Volodymyr and Alfaioni Khaled. Productivity of Modern Homomorphous Cryptosystems in Recommendation Systems of Web Services: Conference Proceedings 16th International Conference on Advanced Trends in Radioelectronics, Telecommunications and Computer Engineering (TCSET) – Lviv-Slavske, Ukraine February 22-26, 2022, P. 331-334.
6. Hordiichuk Valerii, Korchynskyi Volodymyr, Kildishev Vitalii, Zakharchenko Mykola. Timer Signals Transmission Security Increase Based on Spectrum Spreading Methods: 2022 IEEE 2nd Ukrainian Microwave Week (UkrMW) 14-18 November 2022, P. 331-334.

Методичне забезпечення:
1. Моніторинг та аудит інформаційно-комунікаційних систем: методичні

							вказівки до лабораторних робіт [для здобувачів другого (магістерський) рівня вищої освіти за спеціальністю F5 Кібербезпека та захист інформації] / Уклад.: Кільдішев В.Й., Севастєєв Є.О. Одеса: ДУІТЗ, 2026. 38 с. 2. Моніторинг та аудит інформаційно-комунікаційних систем: методичні вказівки до практичних занять [для здобувачів другого (магістерський) рівня вищої освіти за спеціальністю F5 Кібербезпека та захист інформації] / Уклад.: Кільдішев В.Й.. Одеса: ДУІТЗ, 2026. 46 с.
471490	Карпова Олена Олегівна	Доцент, Основне місце роботи	Бізнесу та соціальних комунікацій	Диплом бакалавра, Одеський національний університет імені І. І. Мечникова, рік закінчення: 2023, спеціальність: Філологія, Диплом магістра, Одеський національний університет імені І. І. Мечникова, рік закінчення: 2023, спеціальність: Мова та література (англійська), Диплом кандидата наук ДК 027529, виданий 28.04.2015, Атестат доцента АД 000440, виданий 12.12.2017	19	Ділова іноземна мова	Підвищення кваліфікації: 1. Університет Миколи Ромери (Вільнюс, Литва) Сертифікат №5KV-16786 Програма кваліфікації з теми: "Social and Technological Transformations in a Changing" з 15 квітня по 31 травня 2025, 180 год. (6 кредитів). 2. Магдебурзький університет ім. Отто фон Геріке (Німеччина). Лист-запрошення на умовах академічної мобільності з 01.05.2023 по 30.06.2023. «Особливості та виклики впровадження дуального навчання в університеті», 180 год. (6 кредитів). Наукові публікації: 1. Карпова О., Бублик В. (2025) Стан проблеми використання штучного інтелекту в закладах вищої освіти на практиці та його вплив на якість навчання (на прикладі іноземної мови). Вища освіта України. Вип. №2 (97), 2025. С. 70–78. https://doi.org/10.32782/NPU-VOU.2025.2(97).09 2. Karpova O. Social Media in Academia: Trends, Preferences, and the Implications for Student Privacy and Customization. Університети і лідерство. №1(19).

2025. <https://ul-journal.org/index.php/journal/article/view/278>

3. English for Public Administration : навч. посіб. для 281 спеціальності «Публічне управління та адміністрування» / За заг. ред.: доц. Ю.О. Кузьменко, доц. О.О. Карпова. Одеса: ДУІТЗ, 2024. 128 с.

4. Методичні рекомендації для самостійної роботи студентів з дисципліни «Іноземна мова (англійська)» зі спеціальностей 121 Інженерія програмного забезпечення, 122 Комп'ютерні науки, 123 Комп'ютерна інженерія, 126 Інформаційні системи та технології [методичний посібник] / уклад. О. О. Карпова. Одеса: ДУІТЗ, 2024 р. 36 с.

5. Карпова О.О., Векліч І.В. Innovative teaching methods of English. Матер. ХХІ Міжнар. наук.-практ. конф. «Наукові проблеми господарювання на макро-, мезо- та мікроекономічному рівнях» ОНЕУ 26-27 квіт. 2023 р. Одеса: ОНЕУ. С.7. <https://drive.google.com/file/d/1HnYLRvo3vB2PVbivDWvo8BEq6DA3IWqJ/view>

6. Karpova O. Core approaches to teaching Business English at universities in the era of digitalization. Наука і техніка сьогодні. №6 (6). Вид.: Наукові перспективи. 2022. С.79–88. DOI [https://doi.org/10.52058/2786-6025-2022-6\(6\)-79-88](https://doi.org/10.52058/2786-6025-2022-6(6)-79-88)

7. Карпова О. Теоретичний аналіз проблеми розвитку цифрової грамотності у молоді в умовах безперервного навчання. Актуальні питання гуманітарних наук: міжвуз. зб. наук. праць мол. вчених Дрогоб. держ. пед. ун-ту ім. І. Франка. (Педагогіка). Вип. 47. Т. 2. 2022. С. 256–261. http://www.aphn-journal.in.ua/archive/47_2022/part_2/40.pdf

8. Англійська мова для економістів : навч.

							посіб. 2-е вид. / уклад.: доц. О.О. Карпова. Одеса, 2022. 132 с. 9.Методичні рекомендації для студентів 4-го курсу для підготовки до складання ЄВІ з англійської мови : методичний посібник / уклад. О. О. Карпова. Одеса: ОНЕУ, 2022 р. 37 с.
--	--	--	--	--	--	--	---

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

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