НАЦІОНАЛЬНЕ АГЕНТСТВО ІЗ ЗАБЕЗПЕЧЕННЯ ЯКОСТІ ВИЩОЇ ОСВІТИ

ВІДОМОСТІ
про самооцінювання освітньої програми

Заклад вищої освіти	**Національний технічний університет "Харківський політехнічний інститут"**
Освітня програма	**63504 Кібербезпека**
Рівень вищої освіти	**Магістр**
Спеціальність	**125 Кібербезпека та захист інформації**

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

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

Використані скорочення:

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

Загальні відомості

1. Інформація про ЗВО (ВСП ЗВО)

Реєстраційний номер ЗВО у ЄДЕБО	**104**
Повна назва ЗВО	**Національний технічний університет "Харківський політехнічний інститут"**
Ідентифікаційний код ЗВО	**02071180**
ПІБ керівника ЗВО	**Сокол Євген Іванович**
Посилання на офіційний веб-сайт ЗВО	**www.kpi.kharkov.ua**

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

https://registry.edbo.gov.ua/university/104

3. Загальна інформація про ОП, яка подається на акредитацію

ID освітньої програми в ЄДЕБО	**63504**
Назва ОП	**Кібербезпека**
Галузь знань	**12 Інформаційні технології**
Спеціальність	**125 Кібербезпека та захист інформації**
Спеціалізація (за наявності)	*відсутня*
Рівень вищої освіти	**Магістр**
Тип освітньої програми	**Освітньо-наукова**
Вступ на освітню програму здійснюється на основі ступеня (рівня)	**Бакалавр**
Структурний підрозділ (кафедра або інший підрозділ), відповідальний за реалізацію ОП	**кафедра кфбербезпеки**
Інші навчальні структурні підрозділи (кафедра або інші підрозділи), залучені до реалізації ОП	**кафедра філософії**
Місце (адреса) провадження освітньої діяльності за ОП	**Національний технічний університет "Харківський політехнічний інститут" вул. Кирпичова, 2, Харків, 61002**
Освітня програма передбачає присвоєння професійної кваліфікації	*не передбачає*
Професійна кваліфікація, яка присвоюється за ОП (за наявності)	***відсутня***
Мова (мови) викладання	**Українська**
ID гаранта ОП у ЄДЕБО	**410244**
ПІБ гаранта ОП	**Мілевський Станіслав Валерійович**
Посада гаранта ОП	**Професор**
Корпоративна електронна адреса гаранта ОП	**Stanislav.Milevskyi@khpi.edu.ua**
Контактний телефон гаранта ОП	**+38(066)-716-59-73**
Додатковий телефон гаранта ОП	*відсутній*

Форми здобуття освіти на ОП	Термін навчання
очна денна	1 р. 9 міс.

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

Виходячи із освітніх потреб Харківського регіону й наявності відповідних ресурсів, університет здатний гарантувати якісну підготовку висококваліфікованих фахівців за спеціальністю F5 "Кібербезпека та захист інформації", що забезпечить ефективну роботу з удосконалення освіти в галузі безпеки інформаційних ресурсів та дозволить задовольнити попит у кваліфікованих кадрах для бізнес-середовища.
ОНП "Кібербезпека" розроблена у 2024 р. (затверджено Вченою радою від 26.04.2024 р., протокол № 4) відповідно до Стандарту вищої освіти другого (магістерського) рівня, галузі знань 12 "Інформаційні технології", спеціальності 125 "Кібербезпека та захист інформації", який затверджено наказом Міністерства освіти і науки України від 18.03.2021 р. № 332 (https://drive.google.com/drive/u/1/folders/1KTRfwT329b4ZypCxk70g69QJpLhp0MY0).
До розробки освітньо-наукової програми "Кібербезпека" були залучені викладачі за фахом, з яких була утворена група забезпечення, фахівці навчального відділу, керівний склад університету, представники роботодавців, органи студентського самоврядування.
Кафедра кібербезпеки в НТУ "ХПІ" організована з 1.01.2022 р. Кафедра приймає активну участь у гранті з United States Agency for International Development "Cybersecurity of Critical Infrastructure of Ukraine", організовує неформальну освіту студентів другого (магістерського) рівня в рамках академії Cisco. На кафедрі відбувається щорічна міжнародна конференція Інформаційна безпека та інформаційні технології", яка проводиться в рамках форуму "Digital Reality Forum" (https://drforum.science/en/home/). Кафедра приймає активну участь у підготовці та проведенні міжнародних науково-практичних конференцій IEEE "International Congress on Human-Computer Interaction, Optimization and Robotic Applications" (https://ichoracongress.com/) (Туреччина), IEEE "International Symposium on Multidisciplinary Studies and Innovative Technologies (ISMSIT)" (https://www.ismsitconf.org/) (Туреччина), IEEE "Cognitive Models and Artificial Intelligence Conference (AICCONF)" (https://ai-conf.com/) (Чеська Республіка), IEEE "International Symposium on Innovative Approaches in Smart Technologies (ISAS)" (https://www.isassymposium.org/) (Туреччина) а також міжнародної науково-практичної конференції "International Congress on 3D Printing (Additive Manufacturing) Technologies and Digital Industry 2023 (HYBRID)" (https://3dprintturkey.org/#scope.html) (Туреччина).
У лютому 2025 р. на кафедрі було засновано науково-технічний журнал "Територія безпеки", в якому публікуються наукові праці за спеціальностями F5 "Кібербезпека та захист інформації" та F7 "Комп'ютерна інженерія". Журнал реферується в 5 базах даних. На сьогоднішній момент опубліковано три номера журналу.
З моменту заснування кафедри захищено 2 доктора технічних наук (Мілевський С. В., Погасій С. С.), та 4 аспіранта кафедри (Бондаренко К. О., Лаптєва Т. О., Дженюк Н. В., Толкачов М. Ю.) за спеціальністю "Кіберезпека та захист інформації".
На кафедрі постійно займаються дослідними роботами, що підтверджується отриманими патентами на корисну модель викладачами кафедри (https://cybersecurity.khpi.edu.ua/patenty-kafedry-kiberbezpeka/).

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

Рік навчання	Навчальний рік, у якому відбувся набір здобувачів відповідного року навчання	Обсяг набору на ОП у відповідному навчальному році	Контингент студентів на відповідному році навчання станом на 1 жовтня поточного навчального року	У тому числі іноземців
			ОД	*ОД*
1 курс	2025 - 2026	8	8	8
2 курс	2024 - 2025	10	8	8

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	**59032 Кібербезпека**
другий (магістерський) рівень	**59033 Кібербезпека** **63504 Кібербезпека**
третій (освітньо-науковий/освітньо-творчий) рівень	**58837 Кібербезпека**

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

самооцінювання, кв. м.

	Загальна площа	Навчальна площа
Усі приміщення ЗВО	282386	91582
Власні приміщення ЗВО (на праві власності, господарського відання або оперативного управління)	282386	91582
Приміщення, які використовуються на іншому праві, аніж право власності, господарського відання або оперативного управління (оренда, безоплатне користування тощо)	0	0
Приміщення, здані в оренду	0	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	*ОНП_1.9_125_Магістр_2024.pdf*	u7w6qMNg88Niv0UelTNqor+AOT+5FMItC5uPkD8gZXk=
Навчальний план за ОП	*НП_2024_2025_Магістр_Денне_125_1.9.pdf*	bMhwojwgbkTCV2HKHX607f6Tq851VsjFCACYumNwv18=

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?

Відповідно до наказу МОН України № 332 від 18.03.2021 р. введений Стандарт вищої освіти за спеціальністю 125 “Кібербезпека” для другого (магістерського) рівня вищої освіти. Освітня програма “Кібербезпека” дозволяє досягти результатів навчання шляхом впровадження в освітній процес таких навчальних дисциплін:
Аналіз шкідливих програм;
Цифрова криміналістика;
Етичний хакінг;
Основи управління в проєктах галузі кібербезпеки та захисту інформації;
Математичні моделі управління ІТ-проєктами;
Основи наукових досліджень;
Філософські проблеми сучасного наукового пізнання;
Сучасні проблеми постквантової криптографії;
Аналіз шкідливих програм;
Авторське право у цифровому суспільстві;
Виявлення вторгнень у комп’ютерні мережі (мережеві аномалії);
Технології управління безпекою бізнес-процесів;
Безпека та анонімність роботи в інтернеті;
Мережева та хмарна безпека;
Англійська мова в академічних застосунках;
Інноваційне підприємництво та управління стартап проєктами.

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

Професійний стандарт за спеціальністю 125 Кібербезпека та захист інформації відсутній.

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

Випускник другого (магістерського) рівня вищої освіти (Олександр Кушнерьов) запропонував в рамках освітньої компоненти “Тестування на проникнення та етичний хакінг проходження на платформі EC-Council курсу “Ethical Hacker”. Протокол засідання кафедри кібербезпеки № 1 від 28.08.23 р. (https://cybersecurity.khpi.edu.ua/dokumenty-kafedry-kiberbezpeka/)
Студент другого (магістерського) рівня вищої освіти (Максим Рогозін) запропонував в рамках освітньої компоненти

“Мережева та хмарна безпека”, “Технології управління безпекою бізнес-процесів”(FortiSASE 25 Core Administrator Self-Paced, https://training.fortinet.com/course/view.php?id=72311) проходження на платформі перечень курсов Fortinet (https://training.fortinet.com/local/library/), Протокол засідання кафедри кібербезпеки № 7 від 01.12.25 р. (https://cybersecurity.khpi.edu.ua/dokumenty-kafedry-kiberbezpeka/)

- роботодавці

Технічний директор ТОВ “Сайфер БІС” Ковтун Владислав запропонував включити в освітній процес підготовки здобувачів другого (магістерського) рівня питання, які пов’язані з забезпеченням протидії корупції в університеті, впровадження елементів е-послуг на рівні інститутів, кафедр за допомогою технології PKI (за допомогою ЦСК), та провести тренінги із здобувачами.

- академічна спільнота

ОНП “Кібербезпека” отримала позитивну рецензію-відгук від:
1. Молодецької Катерини Валеріївни, доктора технічних наук, професорки кафедри менеджменту організацій Києво-Могилянської бізнес школи Національного університету “Києво-Могилянська академія”;
2. Ковтуна Владислава Юрійовича, кандидата технічних наук, доцента, директора ТОВ “Сайфер”;
3. Головашича Сергія Олександровича, кандидата технічних наук, доцента директора ТОВ “Мікрокрипт Текнолоджіс”;
4. Волощук Олени Борисівни, кандидата технічних наук, керівника освітніх програм ТОВ “Distributed Lab”.

- інші стейкхолдери

Випускником магістерської програми за спеціальністю 125 “Кібербезпека” Дунаєвим Сергієм, який працює в компанії Holbi Group LTD, виходячи із задач, що виникають під час трудової діяльності, та його професійного досвіду, було запропоновано розширити програму спеціальності F5 “Кібербезпека та захист інформації”, додавши до неї вивчення основ та засобів безпеки інформаційно-комунікаційних систем. Після обговорення, у вибіркову складову введені навчальні дисципліни “WEB-аналітика” та “WEB-безпека”.

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

Освітньо-наукова програма створена у відповідності до місії та стратегічного плану розвитку НТУ “ХПІ” (http://www.kpi.kharkov.ua/ukr/ntu-hpi/mission/, http://www.kpi.kharkov.ua/ukr/ntu-hpi/strategichnyj-plan-rozvytku-ntu-hpi-na-2019-2025-roky/). Цілі ОНП відповідають місії та стратегії НТУ “ХПІ”, а саме: реалізації широкого спектру освітніх послуг; проведенню фундаментальних і прикладних досліджень, формуванню та реалізації в університеті повного інноваційного циклу в освітній та науковій діяльності.

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

Мета освітньої програми та програмні результати навчання відповідають Стратегічному плану розвитку НТУ “ХПІ” на 2019–2025 роки (http://www.kpi.kharkov.ua/ukr/ntu-hpi/strategichnyj-plan-rozvytku-ntu-hpi-na-2019-2025-roky/). Сучасні тенденції розвитку спеціальності та ринку праці пов’язані із застосуванням сучасних інформаційних технологій, що знайшло відображення у результатах навчання за освітньою програмою. Тенденції розвитку спеціальності постійно корегуються в ході проведення наукових семінарів та конференцій, де учасники ОНП представляють свої дослідження і обмінюються досвідом з іншими вченими.

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

Дослідження Європейської Бізнес Асоціації показало, що 71 % компаній відчувають дефіцит кваліфікованих кадрів. За результатами звіту DUO, попит на аналітиків у 2024 р. збільшився на 60 %, а протягом другого півріччя 2025 р. спостерігалося значне зростання заробітних плат фахівців з обробки даних – аналітиків, інженерів даних, фахівців з обробки даних, машинного навчання та штучного інтелекту (https://tech.liga.net/en/technology/novosti/salaries-of-it-analysts-in-ukraine-have-increased---from-1500-for-beginners-to-6000-for-seniors?utm_source=chatgpt.com).
Освітні цілі та програмні результати ОП враховують вимоги:
Стратегії сталого розвитку “Україна – 2020” (п. 2. Мета реалізації Стратегії та вектори руху, п.4. Стратегічні індикатори реалізації Стратегії п.п.19 - https://zakon.rada.gov.ua/laws/show/5/2015#Text)
Стратегія розвитку Харківської області на період з 2021 – 2027 роки (https://kharkivoda.gov.ua/oblasna-derzhavna-administratsiya/struktura-administratsiyi/strukturni-pidrozdili/717/102538)
Враховано аналіз ринку праці у IT-індустрії спираючись на звіт IT-cluster (https://www.slideshare.net/ITcluster/kharkivitresearchreport-118970190), з якого видно, що у Харківській області є затребуваними спеціалісти з інформаційних систем та технологій.
У 2024 р., на українському ринку переважали кіберрішення з часткою 57 %.

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

Під час формування ОНП “Кібербезпека” проаналізовані освітні програми з підготовки здобувачів другого (магістерського) рівня вищої освіти за спеціальністю 125“Кібербезпека та захист інформації” провідних технічних університетів м. Києва (Київський політехнічний інститут імені Ігоря Сікорського (https://osvita.kpi.ua/125), Національний авіаційний університет (https://pk.nau.edu.ua/125-kiberbezpeka-2/), м. Харкова (Харківський національний університет радіоелектроніки (https://nure.ua/abituriyentam/spetsialnosti-ta-spetsializatsiyi/spetsialnist-125-kiberbezpeka-ta-zakhyst-informatsii), (Харківський національний університет ім. В.Н. Каразіна (http://www-csd.univer.kharkov.ua/navchannya/standarti-osviti/osviti-programi/)

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

Під час формування ОНП “Кібербезпека” проаналізовані освітні програми з підготовки здобувачів зі спеціальності “Кібербезпека” у закладах США:
1. Гарвард (https://extension.harvard.edu/academics/programs/cybersecurity-graduate-program/)
2. Іллінойський технологічний інститут (https://www.iit.edu/academics/programs/cybersecurity-mas)
3. Х’юстонський університет (https://www.ist.uh.edu/programs/graduate/cybersecurity)
4. Університет Західної Флориди (https://info.onlinedegrees.uwf.edu/ms-cybersecurity-af/)
5. Університет Тафтса (https://asegrad.tufts.edu/program/cybersecurity-and-public-policy-masters)
6. Університет Джорджа Мейсона (https://info.masononline.gmu.edu/msait-af/)

2. Структура та зміст освітньої програми

Яким є обсяг ОП (у кредитах ЄКТС)?

120

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)?

90

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

30

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

Обов’язкові ОК, які включені до ОНП забезпечують досягнення програмних результатів навчання. ОК, які передбачені навчальним планом, розглядають наступні питання: формування безпеки на об’єктах інформаційної діяльності та критичних інфраструктур сфери інформаційної безпеки та / або кібербезпеки; інформаційні системи (інформаційно-комунікаційні, інформаційно-телекомунікаційні, автоматизовані) та технології; інфраструктуру об’єктів інформаційної діяльності та критичних інфраструктур; системи та комплекси створення, обробки, передачі, зберігання, знищення, захисту та відображення даних (інформаційних потоків); інформаційні ресурси різних класів (в т.ч. державні інформаційні ресурси); програмне та програмно-апаратне забезпечення (засоби) кіберзахисту; системи управління інформаційною безпекою та / або кібербезпекою; технології, методи, моделі та засоби інформаційної безпеки та / або кібербезпеки.
Ці питання відповідають теоретичному змісту предметної області, методам, методикам та технологіям формування компетентностей за ОНП “Кібербезпека”. Зміст ОНП “Кібербезпека” забезпечує поглиблене вивчення проведення, як зовнішнього, так і внутрішнього аудиту з метою забезпечення безпеки контуру бізнес-процесів. Отримання сертифікатів курсів академії Cisco, сприяє підвищенню конкурентоспроможності на ринку праці, удосконаленню механізмів аудиту та захисту за світовими методиками.
Дисципліни навчального плану ОНП потребують спеціалізованого програмного та апаратного забезпечення, яке використовується на кіберполігоні. Дисципліни ОНП в повній мірі забезпечені ліцензованим та open source програмним забезпеченням, що дозволяє досягти поставленої мети та завдань. Таким чином, ОНП “Кібербезпека”, що спрямована на підготовку фахівців з інформаційної та кібербезпеки, програмістів-аналітиків, за своїм змістом відповідає предметній області заявленої спеціальності.

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

Згідно пункту 15 статті 62 Закону України “Про вищу освіту” особи, які навчаються у закладах вищої освіти, мають право на вибір освітніх компонентів у межах, передбачених відповідною освітньою програмою та навчальним планом, в обсязі, що становить не менш як 25 відсотків загальної кількості кредитів ЄКТС, передбачених для даного рівня вищої освіти. Вибір освітніх компонентів в НТУ “ХПІ” здійснюється згідно Положення про порядок реалізації здобувачами вищої освіти права на вільний вибір освітніх компонентів (https://blogs.kpi.kharkov.ua/v2/nv/dokumenty/normatyvni-dokumenty).

В рамках формування індивідуальної складової здобувачам пропонуються вибіркові освітні компоненти (https://drive.google.com/drive/u/1/folders/1IcZuU2ywVyCOQvfRucs1rYsgBSsg6wxJ), а також в рамках неформальної освіти здобувачам пропонуються курси Cisco, які дозволяють додатково в рамках ОНП формувати індивідуальну освітню траєкторію з особливою підготовкою.

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

Вибір здобувачем освітніх компонентів в обсязі, що складає не менш як 25 % загальної кількості кредитів ЄКТС, створює умови для досягнення ним таких цілей: поглибити професійні знання в межах обраної освітньої програми та здобути додаткові спеціальні професійні компетентності, у тому числі із здобуттям професійної кваліфікації; поглибити свої знання та здобути додаткові загальні та професійні компетентності в межах спеціальності або споріднених спеціальностей у тієї ж самої галузі знань; ознайомитись із сучасним рівнем наукових досліджень у інших галузях знань та розширити або поглибити результати навчання за загальними компетентностями. На сайті кафедри (https://cybersecurity.khpi.edu.ua/vybirkova-skladova-osvitno-naukovoi-prohramy-kiberbezpeka-magistr/) міститься перелік освітніх компонентів вільного вибору.
Кафедра ознайомлює здобувачів із переліком вибіркових освітніх компонентів та інформує про особливості формування груп для вивчення вибіркових освітніх компонентів на наступний навчальний рік згідно з Положенням про порядок реалізації здобувачами вищої освіти права на вільний вибір освітніх компонентів. (https://blogs.kpi.kharkov.ua/v2/nv/dokumenty/normatyvni-dokumenty) Вибір освітніх компонентів здобувачами здійснюється шляхом подачі письмової заяви на ім'я директора інституту. Заява зберігається в директораті протягом усього терміну навчання студента. На підставі поданих заяв протягом двох тижнів з моменту завершення процедури їх отримання від здобувачів вищої освіти директор інституту сумісно з гарантами освітніх програм формує академічні групи відповідно до обраних освітніх компонентів. Після ознайомлення з переліком дисциплін здобувач має можливість зробити свій вибір.

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

У відповідності до навчального плану практична підготовка здійснюється під час проведення лабораторних занять за освітніми компонентами базової складової: Аналіз шкідливих програм, Цифрова криміналістика, Етичний хакінг, Основи управління в проєктах галузі кібербезпеки та захисту інформації, Математичні моделі управління ІТ-проєктами, Сучасні проблеми постквантової криптографії, Аналіз шкідливих програм, Виявлення вторгнень у комп'ютерні мережі (мережеві аномалії), Технології управління безпекою бізнес-процесів, Безпека та анонімність роботи в інтернеті, Мережева та хмарна безпека, Англійська мова в академічних застосунках, Інноваційне підприємництво та управління стартап проєктами, Комплексний тренінг "Безпека веб-застосунків", Комплексний тренінг "Блокчейн: математичні проблеми та застосунки", Комплексний тренінг "Криптографія та криптоаналіз". Відповідно до навчального плану ОНП передбачає практику (4 сем., 19 кредитів ЄКТС), метою якої є формування професійних умінь і навичок щодо прийняття самостійних рішень під час професійної діяльності в сфері кібербезпеки та захисту інформації. Обговорення з роботодавцями змісту програм практик дало змогу визначити відповідні компоненти для того, щоб отримані здобувачами під час практик компетентності стали корисними в їх подальшій професійній діяльності.

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

ОНП передбачає набуття здобувачами вищої освіти soft skills. ОК ОНП сприяють формуванню соціальних навичок у студентів, опануванню знань, умінь, здатності до комунікації, засвоєнню критичного мислення, правил поведінки в команді, комунікабельності, призвичаюють до етичних норм поведінки та дотримання принципів академічної доброчесності, побудови комунікаційних зав'язків і вміння ведення переговорів на професійному рівні. ОНП дозволяє набути здобувачам соціальних навичок, які відповідають перелікам компетентностей випускника: здатність працювати в команді, виявляти ініціативу, здатність організовувати та проводити переговори, здатність до самонавчання, підтримки належного рівня знань, готовність до опанування знань нового рівня, підвищення своєї фаховості та рівня кваліфікації. Набуттю таких універсальних компетентностей сприяють наступні ОК: Безпека та анонімність роботи в інтернеті, Основи наукових досліджень, Інноваційне підприємництво та управління стартап проектами, Англійська мова в академічних застосунках, Авторське право у цифровому суспільстві, які забезпечують наступні компетентності щодо формування соціальних навичок: КЗ-1, 5, КФ-1, 2, 4, 5, 6, 10. Запропоновані ОК дозволяють сформувати у студентів навички комунікації, лідерства, відповідальності, цілеспрямованості та вміння діяти в критичній ситуації.

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

Зміст освітньо-наукової програми «Кібербезпека» має чітку, логічно вибудувану структуру та реалізується через взаємопов'язану систему обов'язкових і вибіркових освітніх компонентів. Послідовність їх вивчення забезпечує поетапне формування загальних, фахових і дослідницьких компетентностей відповідно до вимог Стандарту вищої освіти за спеціальністю 125 «Кібербезпека та захист інформації» для другого (магістерського) рівня вищої освіти, затвердженого наказом МОН України від 18.03.2021 № 332.

Обов'язкові освітні компоненти спрямовані на формування фундаментальних знань, аналітичного мислення, розуміння сучасних соціально-економічних і технологічних процесів, а також на здобуття здатності до критичного осмислення явищ інформаційного суспільства. Дисципліни гуманітарного та управлінського спрямування (філософські проблеми сучасного наукового пізнання, основи наукових досліджень, авторське право у цифровому суспільстві, інноваційне підприємництво) забезпечують формування загальнокультурних і громадянських компетентностей, зокрема відповідальності, академічної доброчесності, правосвідомості та розуміння суспільної значущості професійної діяльності.
Фахові та дослідницькі компоненти логічно інтегруються з гуманітарною складовою, що в сукупності забезпечує досягнення програмних результатів навчання, пов'язаних із готовністю здобувача самостійно аналізувати суспільні та професійні процеси, виявляти закономірності їх розвитку, приймати обґрунтовані рішення та застосовувати наукові методи у сфері кібербезпеки.

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

Співвіднесення обсягу освітніх компонентів ОНП із фактичним навантаженням здобувачів здійснюється у кредитах ЄКТС. Обсяг 1 кредиту ЄКТС становить 30 год. Розподіл аудиторних занять між лекційними та лабораторними (практичними) заняттями, а також між тижнями теоретичного навчання є прерогативою гаранта освітньої програми та робочої групи. Навчальні дні, їх тривалість визначені графіком навчального процесу та розкладом занять з урахуванням перенесень робочих днів, затвердженим у порядку і у терміни, встановлені в Університеті (https://blogs.kpi.kharkov.ua/v2/nv/navchalnyj-protses).
Розподіл навчальних годин на аудиторну роботу за навчальними тижнями та видами навчальної роботи бакалавра відображено в силабусах освітніх компонентів.
Навчальний час, відведений для самостійної роботи студента, визначається гарантом освітньої програми.
Співвідношення обсягу окремих освітніх компонент ОНП з фактичним навантаженням здобувачів вищої освіти у навчальному плані складає:
1. Загальна підготовка – 7 кредитів, 6 %.
2. Спеціальна (фахова) підготовка – 23 кредити, 19 %.
3. Наукова підготовка – 30 кредитів, 25 %.
4. Вибіркові освітні компоненти – 30 кредитів, 25 % .
5. Практична підготовка – 19 кредитів, 16 %.
6. Атестація – 11 кредитів, 9 %

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

З метою покращення в рамках освітнього компоненту Веб-безпека пропонуються практичні заняття з цих питань. З метою покращення якості проведення практичних занять освітніх компонентів, які пов'язані з відпрацюванням практичних питань кібернападу (захисту від кібернападу) сформований спеціалізований клас "Кіберполігон". Кіберполігон забезпечує доступ до ресурсів не тільки внутрішніх, а і зовнішніх, що дозволяє в повному обсязі відпрацьовувати практичні завдання в умовах дистанційного навчання.
Підготовки здобувачів за дуальною формою навчання немає.

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

Освітні цілі та програмні результати ОНП враховують вимоги:
Указу Президента України №722/2019 Про Цілі сталого розвитку України на період до 2030 року
https://www.president.gov.ua/documents/7222019-29825
Освітні цілі та програмні результати ОНП враховують вимоги:
Стратегії сталого розвитку "Україна – 2020" (п. 2. Мета реалізації Стратегії та вектори руху, п.4. Стратегічні індикатори реалізації Стратегії п.п.19 - https://zakon.rada.gov.ua/laws/show/5/2015#Text)
Стратегія розвитку Харківської області на період з 2021–2027 роки (https://kharkivoda.gov.ua/oblasna-derzhavna-administratsiya/struktura-administratsiyi/strukturni-pidrozdili/717/102538)
У межах ОНП здобувачі набувають здатності застосовувати сучасні технології кіберзахисту для мінімізації соціальних, економічних і екологічних ризиків, пов'язаних із цифровізацією, а також формують готовність до прийняття професійних рішень з урахуванням принципів сталого розвитку, національних стратегій та глобальних викликів безпеки.

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

Веб-сайт Національного технічного університету “Харківський політехнічний інститут” (НТУ “ХПІ”)
https://vstup.kpi.kharkov.ua/admission/
Веб-сайт Навчально-наукового інституту комп’ютерних наук та інформаційних технологій (ННІ КНІТ)
https://web.kpi.kharkov.ua/if/uk/specialties_ua/master_ua/master_125_ua/
Веб-сайт кафедри кібербезпеки
https://cybersecurity.khpi.edu.ua/prohrama-vstupnoho-vyprobuvannia-mahistr/

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

Правила прийому є чіткими та зрозумілими для абітурієнта, не містять дискримінаційних положень, оприлюднені на офіційному веб-сайті ЗВО
https://vstup.kpi.kharkov.ua/admission/admission_rules/, що відповідає вимогам частини п’ятої статті 44 Закону України “Про вищу освіту”. Вступник повинен продемонструвати здатність вирішувати типові професійні завдання, передбачені для відповідного рівня. Згідно з вимогами, затвердженим Міністерством освіти і науки України, прийом відбувається на конкурсній основі. Набір за спеціальністю освітнього рівня “магістр” здійснюється за результатами зовнішнього незалежного оцінювання (іноземна мова) та вступного фахового випробування. Загальний конкурсний бал для вступу на основі освіти бакалавра не може бути менше 100 балів.

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?

Результати навчання, отриманих в інших ЗВО, визнаються та зараховуються відповідно до таких документів:
Положення про організацію освітнього процесу в Національному технічному університеті “Харківський політехнічний інститут” (четверта редакція), (Затверджено Вченою радою НТУ “ХПІ”, Протокол № 1 від 24 січня 2025 р. https://blogs.kpi.kharkov.ua/v2/nv/dokumenty/normatyvni-dokumenty).
Положення про порядок реалізації права на академічну мобільність здобувачів вищої освіти, аспірантів, докторантів, науково-педагогічних, наукових та інших працівників Національного технічного університету «Харківський політехнічний інститут» (Затверджено Вченою радою НТУ “ХПІ”, Протокол № 9 від 29.11.2024 р., https://blogs.kpi.kharkov.ua/v2/nv/dokumenty/normatyvni-dokumenty)
Положення про порядок реалізації здобувачами вищої освіти права на вільний вибір освітніх компонентів (Затверджено Вченою радою НТУ “ХПІ”, Протокол № 11 від 26 грудня 2023 р., https://blogs.kpi.kharkov.ua/v2/nv/dokumenty/normatyvni-dokumenty).

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

Практики застосування вказаних правил на відповідній ОНП 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?

Положення про порядок визнання результатів неформальної та інформальної освіти у Національному технічному університеті “Харківський політехнічний інститут” (Затверджено Вченою Радою НТУ “ХПІ”, Протокол № 1 від 19 січня 2024 р., введено в дію наказом ректора 25 січня 2024 р. № 38 ОД (https://blogs.kpi.kharkov.ua/v2/nv/dokumenty/normatyvni-dokumenty).

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

Відповідно до пропозицій робочої групи та викладачів кафедри на ОНП здобувачам вищої освіти пропонується проходження курсів академії Cisco Інституту комп’ютерних наук та інформаційних технологій. (Керівник академії – завідувач кафедри кібербезпеки, проф. Євсеєв С. П.). За відповідними ОК на сайті кафедри (https://cybersecurity.khpi.edu.ua/cisco-networking-academy/) розміщено перелік курсів академії Cisco. Після проходження курсів на засіданнях кафедри затверджується кількість балів, які отримують студенти після проходження відповідних курсів академії Cisco.

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?

Основними формами навчання відповідно до Положення про організацію освітнього процесу в Національному технічному університеті “Харківський політехнічний інститут” (затверджено Вченою радою НТУ “ХПІ”, Протокол № 1 від 24 січня 2025 р. (п.8), (https://blogs.kpi.kharkov.ua/v2/nv/dokumenty/normatyvni-dokumenty) силабусів освітніх компонентів (https://cybersecurity.khpi.edu.ua/sylabusy-onp-mahistry/) є лекційні, практичні заняття, лабораторні

заняття, індивідуальні заняття, командна та самостійна робота студента. Основними методами навчання на ОНП є комунікативний, пояснювально-ілюстративний (інформаційно-рецептивний), стимулюючо-пошуковий, репродуктивний, проблемного викладу. Використовуються як традиційні форми і методи навчання, так і інноваційні методи (метод кейс-стаді, ділові ігри, тренінги), інтерактивні методи під час дистанційного навчання студентів (проведення дистанційних лекцій, практичних та лабораторних занять з використанням засобів Microsoft Teams відповідно до Положення про систему корпоративної комунікації Національного технічного університету "Харківський політехнічний інститут", https://blogs.kpi.kharkov.ua/v2/metodotdel/wp-content/uploads/sites/28/2020/10/Polozhennya-pro-sistemu-korporativnoyi-komunikatsiyi-NTU-HPI-.pdf. Вказані методи та форми сприяють досягненню програмних результатів навчання за рахунок поєднання теоретичних та практичних знань.

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?

Здобувачі здійснюють вибір освітніх компонентів після ознайомлення зі змістом силабусів освітніх компонентів, що пропонуються. З метою визначення набутих компетентностей кожен викладач самостійно обирає методи оцінювання, що формуються на засадах поопераційного контролю та накопичення рейтингових балів за різноманітну навчальну діяльність студента за певний період навчання. Після засвоєння певної освітньої компоненти ОНП здобувачам пропонується взяти участь в опитуванні щодо якості викладання освітніх компонентів, використаних методів навчання та оцінювання. Результати опитування використовують з метою запровадження заходів щодо покращення, оптимізації освітнього процесу. За результатами опитування здобувачів вищої освіти другого (магістерського) рівня вищої освіти за ОНП отримані наступні результати: задоволеність освітньою програмою – 88,4 % (середнє значення); застосування викладачами форм, методів, технологій навчання, що сприяють формуванню професійних компетентностей – 87,4 %, якість викладання – 88,6 %, якість оцінювання – 91,0 %, академічна доброчесність – 88,4 %, академічна підтримка – 89,3 %, індивідуальна траєкторія навчання – 87,9 %, практична підготовка – 82,7 %, самостійна робота (навантаження) – 88,6 %, можливості навчання – 87,7 %, загальна задоволеність навчанням за освітньо-науковою програмою – 89,6 % (https://drive.google.com/file/d/14Z2gH6KARjrvUFewJt2CemR4oNpUn8H/view?usp=sharing)

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

Відповідно до Положення про порядок реалізації права на академічну мобільність здобувачів вищої освіти, аспірантів, докторантів, науково-педагогічних, наукових та інших працівників Національного технічного університету "Харківський політехнічний інститут" здобувачі вищої освіти мають право здійснювати навчання в закладі-партнері. НТУ "ХПІ" має велику чисельність міжнародних партнерів серед закордонних закладів вищої освіти (https://www.kpi.kharkov.ua/ukr/mizhnarodni-zv-yazki/mizhnarodni-partneri-ntu-hpi) та компаній (https://www.kpi.kharkov.ua/ukr/mizhnarodni-zv-yazki/mizhnarodne-spivrobitnytstvo/), бере активну участь в міжнародних організаціях та програмах: є членом Альянсу університетів за демократію (AUDEM), Ради Європейської асоціації університетів, Чорноморської Мережі університетів (BSUN), Євразійської асоціації університетів (https://www.kpi.kharkov.ua/ukr/mizhnarodni-zv-yazki/uchast-v-mizhnarodnih-organizatsiyah-i-programah/). Кожен викладач вільний обирати ті форми та методи навчання, які вважає доцільними для забезпечення формування результатів навчання здобувача освіти, відповідно до дисциплін, загальної мети та задач ОНП. При цьому основною задачею викладача є підбір таких форм та методів навчання, які дозволяють максимально ефективно сформувати компетентності здобувача освіти. Таким чином завдання викладача повністю відповідають інтересам здобувача вищої освіти.

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

Здобувачам вищої освіти під час реалізації освітнього процесу забезпечено вільний доступ до сайту випускаючої кафедри, на якому розміщена ОНП, силабуси (https://cybersecurity.khpi.edu.ua/osvitno-naukova-prohrama-mahistr/, https://drive.google.com/drive/u/1/folders/12MZNzwXIYJA5VsWoiyQxsN7iWeUkxcEL), які містять інформацію щодо змісту, цілей, критеріїв та процедур оцінювання знань, компетентностей та очікуваних результатів навчання за освітніми компонентами.
Здобувач вищої освіти після ознайомлення з документами до початку навчального року має можливість отримати кваліфіковану консультацію викладачів освітніх компонентів. У ЗВО в рамках виконання стратегії діджиталізації впроваджено електронні кабінети студентів, в яких студент може ознайомитись з електронними заліковими книжками, що містять поточні оцінки за дисциплінами семестру, що є передовою практикою впровадження сучасних цифрових технологій в освітній процес (Положення про систему корпоративної комунікації Національного технічного університету "Харківський політехнічний інститут", https://blogs.kpi.kharkov.ua/v2/vr/wp-content/uploads/sites/27/2020/11/Polozhennya-pro-sistemu-korporativnoyi-komunikatsiyi.pdf). Графік організації освітнього процесу та розклади атестаційних тижнів (сесій) наведено за посиланням (https://blogs.kpi.kharkov.ua/v2/nv/navchalnyj-protses). Результати опитування студентів щодо надання інформації про цілі, зміст та очікувані результати навчання, порядок та критерії оцінювання у межах окремих ОК зберігаються в директораті інституту.

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

Поєднання навчання і досліджень відбувається шляхом активної участі студентів у науково-дослідній роботі кафедри під час розробки проєктів та науково-дослідних тем. Поєднання навчання і досліджень відбувається шляхом активної участі студентів в науково-дослідній тематиці НТУ "ХПІ" та кафедри кібербезпеки за наступними напрямками:
– Моделювання соціокіберфізичних систем;
– Розробка симетричної криптосистеми на основі використання згорткової штучної нейронної мережі;
– Побудова інтелектуальних багатоконтурних систем захисту інформації.
Поєднання навчання та наукових досліджень також відбувається шляхом участі студентів в щорічних міжнародних конференціях.
Оприлюднити результати своїх наукових досліджень здобувачі вищої освіти можуть в рамках проведення Міжнародної науково-практичної конференції "Інформаційна безпека та інформаційні технології", яка проводиться за підтримки кафедри в рамках форуму "Digital Reality Forum" (https://drforum.science/en/home/)
З метою практичної реалізації результатів наукових досліджень на кафедрі сформовано лабораторію блокчейн (https://cybersecurity.kpi.kharkov.ua/%d0%b1%d0%bb%d0%be%d0%ba%d1%87%d0%b5%d0%b9%d0%bd-%d0%bb%d0%b0%d0%b1%d0%be%d1%80%d0%b0%d1%82%d0%be%d1%80%d1%96%d1%8f/), яка дозволяє здобувачам отримувати додаткові навчальні матеріали, відпрацьовувати питання забезпечення безпеки в програмних застосунках з використанням технології блокчейн, на основі мови Python, та виконувати індивідуальні наукові дослідження.
З боку викладачів результати дослідження, отримані при виконанні наукової роботи, використовуються при викладанні таких дисциплін: Моделювання кіберфізичних дій – розглядаються процедури використання крипто-кодових конструкцій Мак-Еліса та Нідеррайтера на алгеброгеометричних та збиткових кодах, Бездротова та мобільна безпека – розглядаються власні бібліотеки створення алгоритмів несиметричної криптографії мовою Python.

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

Викладачі оновлюють зміст освітніх компонентів на основі наукових досягнень і сучасних практик у галузі кібербезпеки наступним чином. Викладачі кафедри приймають активну участь у міжнародних конференціях, а також публікують результати досліджень в науково-метричної базі Scopus. Так за 2022–2025 рр. викладачами кафедри надруковано статей у НМБ Scopus – 34, з них 2 монографії. Викладачі кафедри використовують науково-практичні досягнення у стартапах (https://www.calltools.ua/), а також фреймворк "Класифікатор загроз" (https://skl.khpi.edu.ua/en), де пропонується нова технологія захисту на основі багатоконтурних систем захисту інформації на основі постквантових алгоритмів – ККК Мак-Еліса, Нідеррайтера та Рао-Нама, а також аналіз можливих атак на ОКІ. В навчальних дисциплінах, які пов'язані з блокчейн-технологією використовується матеріал навчальних курсів платформи Coursera, а також навчальні матеріали компаній Сайфер і DisnhsbutedLab, а саме: "Новітні технології забезпечення кібербезпеки на основі технології блокчейн". В дисциплінах "Технології управління безпекою бізнес-процесів", "Моделі і аналіз мультиагентних систем" розглядаються питання побудови багатоконтурних систем захисту на основі досліджень Лауреатів Національної Премії імені Бориса Патона у 2024 р. проф. Євсеєва С. П. та Мілова О. В.

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

В НТУ "ХПІ" здобувачі вищої освіти мають право доступу до наукових баз Scopus та Web of Science. Згідно зі стратегією інтернаціоналізації Національного технічного університету "Харківський політехнічний інститут" (https://www.kpi.kharkov.ua/ukr/mizhnarodni-zv-yazki/strategiya-internatsionalizatsiyi/) здобувачі вищої освіти мають право на мовну підготовку, участь у спільних освітніх програмах, залучення до науко-дослідної роботи з міжнародної тематики та ін. Щороку на базі Університету проводиться понад 30 міжнародних науково-технічних конференцій, низка крупних міжнародних форумів, презентацій та виставок.
Університет постійно бере участь у міжнародних виставках за кордоном. При цьому за підтримкою кафедри щорічна МНПК "Інформаційна безпека та інформаційні технології" в рамках форуму "Digital Reality Forum" (https://drforum.science/en/home/), IEEE "International Congress on Human-Computer Interaction, Optimization and Robotic Applications"(https://ichoracongress.com/) (Туреччина), IEEE "International Symposium on Multidisciplinary Studies and Innovative Technologies (ISMSIT)" (https://www.ismsitconf.org/) (Туреччина), IEEE "Cognitive Models and Artificial Intelligence Conference (AICCONF)" (https://ai-conf.com/) (Чеська Республіка), IEEE "International Symposium on Innovative Approaches in Smart Technologies (ISAS)" (https://www.isassymposium.org/) (Туреччина), "International Congress on 3D Printing (Additive Manufacturing) Technologies and Digital Industry 2023 (HYBRID)" (https://3dprintturkey.org/#scope.html) (Туреччина).

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?

Контрольні заходи – це форма організації освітнього процесу, що визначає відповідність рівня набутих здобувачами вищої освіти знань, умінь та компетентностей вимогам нормативних документів. Головне завдання контрольних заходів полягає у виявленні справжнього стану здобутків студентів на відповідному етапі опанування освітньої

програми з метою раціональної організації освітнього процесу та управління якістю освітньої діяльності Університету.
Вхідний контроль застосовується для реалізації індивідуального підходу в процесі викладання дисципліни.
Поточний контроль проводиться під час практичних / лабораторних занять та за результатами виконання завдань самостійної роботи. Форму проведення поточного контролю і систему оцінювання визначає викладач.
Підсумковий контроль проводиться у формах іспиту або диференційованого заліку, в обсязі навчального матеріалу, визначеного робочою програмою навчальної дисципліни.
Атестація – це встановлення відповідності засвоєних здобувачами вищої освіти рівня та обсягу знань, умінь, інших компетентностей вимогам стандартів вищої школи. Заклад вищої освіти на підставі рішення екзаменаційної комісії присуджує особі, яка успішно виконала освітню програму на певному рівні вищої освіти, відповідний ступінь вищої освіти та присвоює відповідну кваліфікацію.
Перелік контрольних заходів встановлюється силабусами. Результати контролю оформлюються у відповідних відомостях, та є підґрунтям для прийняття рішення щодо виконання здобувачами індивідуального навчального плану здобувача вищої освіти.

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

Чіткість та зрозумілість форм контрольних заходів забезпечується згідно Положення про організацію освітнього процесу в НТУ "ХПІ" https://blogs.kpi.kharkov.ua/v2/nv/dokumenty/normatyvni-dokumenty
Критерії оцінювання навчальних досягнень здобувачів вищої освіти здійснюються відповідно до Положення про критерії та систему оцінювання знань та вмінь і про рейтинг здобувачів вищої освіти (https://blogs.kpi.kharkov.ua/v2/nv/dokumenty/normatyvni-dokumenty).
В силабусі є розділ, в якому описуються методи контролю, що передбачені даною дисципліною та відповідають програмним результатам навчання.
Формами контрольних заходів є контрольна робота, екзамен та залік, а також апробації на конференціях та публікації.
Вибір форми контрольних заходів відбувається на етапі підготовки навчального плану: освітні компоненти, результати яких передбачають більш практичне наповнення, завершуються заліком, освітні компоненти більш теоретичного або теоретико-практичного наповнення – екзаменом.

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

На початку навчального року викладачі дисциплін доводять до здобувачів вищої освіти, що на сайті кафедри (https://cybersecurity.khpi.edu.ua/sylabusy-onp-mahistry/) розміщуються силабуси, де міститься опис технологій оцінювання знань студентів під час проведення поточного контролю у формі опитування, захисту лабораторних робіт, тестів, контрольних робіт та семестрового контролю у формі заліку або іспиту у терміни, передбачені навчальним планом. Контроль відбувається згідно приведеної шкали оцінювання знань та умінь: національної та ЄКТС. Крім того, на передекзаменаційній консультації лектор доводить зміст екзаменаційного білету та критерії оцінювання кожного питання у білеті з детальним описом нарахування кожного балу. Все це забезпечує доведення до здобувачів вищої освіти інформації про форми контрольних заходів та критерії оцінювання. Основні засади застосування правил ECTS визначені у "Положенні про критерії та систему оцінювання знань та вмінь і про рейтинг студентів" НТУ "ХПІ" (https://blogs.kpi.kharkov.ua/v2/nv/dokumenty/normatyvni-dokumenty).

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

Форми атестації здобувачів ОНП відповідають стандарту вищої освіти зі спеціальності 125 "Кібербезпека та захист інформації" (Стандарт вищої освіти України: другий (магістерський) рівень, галузь знань 12 – Інформаційні технології, спеціальність 125 – Кібербезпека та захист інформації. Затверджено і введено в дію наказом Міністерства освіти і науки України № 332 від 18.03.2021 р. Атестація здійснюється у формі публічного захисту кваліфікаційної роботи. Кваліфікаційна робота має розв'язувати складну задачу інформаційної безпеки та / або кібербезпеки і передбачати проведення досліджень та / або здійснення інновацій. Кваліфікаційна робота не повинна містити академічного плагіату, фабрикації, фальсифікації. Кваліфікаційна робота має бути розміщена на офіційному сайті (або у репозитарії) закладу вищої освіти або його підрозділу. Оприлюднення кваліфікаційних робіт з обмеженим доступом здійснюється відповідно до вимог законодавства.

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

Відповідно до Положення про критерії та систему оцінювання знань та вмінь і про рейтинг здобувачів вищої освіти (https://blogs.kpi.kharkov.ua/v2/nv/dokumenty/normatyvni-dokumenty) визначені процедури проведення контрольних заходів.
Крім цього у Положенні про екзаменаційну комісію у Національному технічному університеті "Харківський політехнічний інститут" (зі змінами) (Розглянуто та затверджено Вченою радою НТУ "ХПІ" Протокол № 7 від 02 липня 2021р., https://blogs.kpi.kharkov.ua/v2/nv/dokumenty/normatyvni-dokumenty) зазначено порядок створення екзаменаційної комісії, організацію роботи екзаменаційної комісії, порядок проведення атестації. Ознайомитись з порядком проведення атестації можна на зазначених сайтах.

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

Відповідно до Положення про критерії та систему оцінювання знань та вмінь і про рейтинг здобувачів вищої освіти (https://blogs.kpi.kharkov.ua/v2/nv/dokumenty/normatyvni-dokumenty) та Положення про екзаменаційну комісію у Національному технічному університеті "Харківський політехнічний інститут" (затверджено Вченою радою НТУ "ХПІ" Протокол № 7 від 02 липня 2021 р. (https://blogs.kpi.kharkov.ua/v2/nv/dokumenty/normatyvni-dokumenty) та Порядок подання апеляцій (іспити, заліки, атестація) (https://blogs.kpi.kharkov.ua/v2/nv/dokumenty/normatyvni-dokumenty) згідно яких у випадку незгоди з оцінкою студент має право на апеляцію. Апеляція має бути розглянута на засіданні апеляційної комісії не пізніше наступного дня після її подання. Здобувач, який подав апеляцію, має право бути присутнім при розгляді своєї заяви. У випадках конфліктної ситуації за мотивованою заявою здобувача чи викладача, розпорядженням директора інституту створюється комісія для проведення підсумкового контролю, до якої входять завідувач кафедри і викладачі відповідної кафедри, представники дирекції, профспілкового комітету студентів та органів студентського самоврядування. Прикладів застосування відповідних процедур на освітньо-науковій програмі немає.

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

Графік ліквідації академічної заборгованості складається в Інституті та затверджується ректором університету (проректором з науково-педагогічної роботи) та доводиться до відома здобувачів вищої освіти у паперовому вигляді та на сайті Інституту та кафедри. Відповідно до Положення про екзаменаційну комісію у Національному технічному університеті "Харківський політехнічний інститут" (п. 6, затверджено Вченою радою НТУ "ХПІ" Протокол № 7 від 02 липня 2021 р. (https://blogs.kpi.kharkov.ua/v2/nv/dokumenty/normatyvni-dokumenty), Положення про критерії та систему оцінювання знань та вмінь і про рейтинг здобувачів вищої освіти (https://blogs.kpi.kharkov.ua/v2/nv/dokumenty/normatyvni-dokumenty).
Прикладів застосування відповідних правил на освітній програмі немає.

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

У випадку незгоди з оцінкою здобувач вищої освіти має право на апеляцію. Заява про апеляцію з візою директору інституту подається Ректору або проректору з науково-педагогічної роботи Університету в день після оголошення результатів атестації відповідно до Положення про організацію освітнього процесу в Національному технічному університеті "Харківський політехнічний інститут" (п. 9.10) https://blogs.kpi.kharkov.ua/v2/nv/dokumenty/normatyvni-dokumenty та до Положення про екзаменаційну комісію у Національному технічному університеті "Харківський політехнічний інститут" (п.8) https://blogs.kpi.kharkov.ua/v2/nv/dokumenty/normatyvni-dokumenty.
Прикладів застосування відповідних правил на освітній програмі немає.

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

НТУ "ХПІ" в процесі впровадження принципів академічної доброчесності в освітній та науковий процес керується Законами України, нормативними актами Кабінету Міністрів України, центральних органів виконавчої влади та внутрішніми нормативними документами (http://blogs.kpi.kharkov.ua/v2/nv/akademichna-dobrochesnist/): Статут Національного технічного університету "Харківський політехнічний інститут"; Правила внутрішнього розпорядку НТУ "ХПІ"; Опис системи внутрішнього забезпечення якості освітньої діяльності та якості вищої освіти НТУ "ХПІ"; Кодекс етики академічних взаємовідносин та доброчесності НТУ "ХПІ"; Положення про систему запобігання та виявлення академічного плагіату у випускних кваліфікаційних роботах здобувачів вищої освіти НТУ "ХПІ"; Положення про репозитарій Електронний архів НТУ "ХПІ"; Положення про Електронний репозитарій кваліфікаційних випускних робіт здобувачів вищої освіти у НТУ "ХПІ".

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

Технологічні рішення мають на меті створення середовища, в якому учасники свідомо дотримуються принципів академічної доброчесності, мотивовані до навчання, розуміють, що шахрайство є невигідним та може бути викрите шляхом: підтримки електронних репозитаріїв НТУ "ХПІ" (наукових публікацій та кваліфікаційних випускних робіт здобувачів вищої освіти); технологічної співпраці з StrikePlagiarism (компанія "Plagiat.pl") щодо захисту інтелектуальної власності і впровадження в НТУ "ХПІ" передового міжнародного досвіду у сфері академічної доброчесності та антиплагіатної експертизи наукових праць; створення умов для самостійного виконання навчальних завдань (НТБ), у тому числі забезпечення віддаленого доступу до зовнішніх та власних інформаційних освітніх та наукових ресурсів; запровадження процедур моніторингу дотримання академічної доброчесності (анкетування); поєднання сучасних педагогічних технологій, інноваційних підходів до навчання та оцінювання; дослідження перспективних технологій виявлення можливого плагіату та аналіз ефективності використання існуючого антиплагіатного ПЗ для робіт за спеціальностями, які крім тексту, містять схеми, рисунки, формули, діаграми, фрагменти програмного коду.

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

Академічна доброчесність популяризується в НТУ "ХПІ" через проведення на постійній основі співробітниками відділу забезпечення якості освітньої діяльності, науково-технічної бібліотеки (http://library.kpi.kharkov.ua/uk/Academic_Goodness) та групи забезпечення ОНП інформаційних семінарів, онлайн курсів, круглих столів, презентацій з висвітлення питань академічної доброчесності, проведення моніторингу курсових та випускних кваліфікаційних робіт здобувачів вищої освіти та наявність плагіату, вивчення кращих практик вітчизняних та закордонних закладів вищої освіти.
Основні напрями з популяризації принципів академічної доброчесності:
– розміщення та демонстрація візуальних мотиваційних матеріалів у приміщеннях та на сайтах підрозділів;
– проведення на базі НТУ "ХПІ" науково-практичних семінарів (http://library.kpi.kharkov.ua/uk/conference) за темою "Академічна доброчесність" та темами, дотичними до них із залученням представників авторитетних компаній Unichek, Plagiat.pl, Clarivate Analytics, Elsevier Ukraine.
– формування мотивації здобувачів до дотримання академічної доброчесності шляхом проведення заходів, що популяризують потенційні можливості відомих вчених та демонструють пріоритет знань;
– активна участь у зовнішніх заходах за темою "Академічна доброчесність" (НАЗЯВО, Academic IQ, Elsevier Ukraine, Unichek, Plagiat.pl, Clarivate Analytics)

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

Види порушень та відповідальність за них прописані в кодексі етики академічних взаємовідносин та доброчесності НТУ "ХПІ" (https://blogs.kpi.kharkov.ua/v2/nv/wp-content/uploads/sites/43/2023/12/Kodeks-etyky-akademichnyh-vzayemovidnosyn-ta-dobrochesnosti-NTU-HPI.pdf) та положення про систему запобігання та виявлення академічного плагіату у випускних кваліфікаційних роботах здобувачів вищої освіти НТУ "ХПІ" (https://blogs.kpi.kharkov.ua/v2/quality/wp-content/uploads/sites/44/2024/06/polozhennya-proekt-plagyat.pdf).
Серед здобувачів вищої освіти за ОНП подібних прикладів не було.

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

Серед професорсько-викладацького складу, що викладає на ОНП "Кібербезпека":
Завідувач кафедри Євсеєв С. П. захистив дисертацію на здобуття наукового ступеня доктора технічних наук за спеціальністю 21.05.01 – Інформаційна безпека держави; професор Мілевський С. В. захистив дисертацію на здобуття наукового ступеня доктора технічних наук за спеціальністю 05.13.21 – Системи захисту інформації; професор Погасій С. С. захистив дисертацію на здобуття наукового ступеня доктора технічних наук за спеціальністю 05.13.21 – Системи захисту інформації;
доцент Гаврилова А.А. захистила дисертацію на здобуття наукового ступеня доктора філософії з кібербезпеки;
доцент Аксьонова І.В. має профільну освіту з кібербезпеки та має вчене звання старшого дослідника зі спеціальності F5 "Кібербезпека та захист інформації";
доцент Король О.Г. захистила дисертацію на здобуття наукового ступеня кандидата технічних наук за спеціальністю 05.13.21 – Системи захисту інформації.

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

Конкурсний добір викладачів ОНП регламентується Положенням про обрання та прийняття на роботу науково-педагогічних працівників НТУ "ХПІ", затвердженого на засіданні Вченої Ради НТУ "ХПІ" протокол 11 від 26.11.2021 р. (http://blogs.kpi.kharkov.ua/v2/staff/polozhennya-pro-obrannya-ta-prijnyattya-na-robotu-naukovo-pedagogichnih-pratsivnikiv-ntu-hpi-2/).
Конкурсний відбір проводиться на засадах: відкритості, гласності, законності, рівності прав членів конкурсної комісії, колегіальності прийняття рішень конкурсною комісією, незалежності, об'єктивності та обґрунтованості рішень конкурсної комісії, неупередженого ставлення до кандидатів на зайняття вакантних посад науково-педагогічних працівників (НПП).
Під час конкурсного добору враховується рівень фахової підготовки, наукова та професійна діяльність згідно пп. 37, 38 Ліцензійних умов провадження освітньої діяльності (https://zakon.rada.gov.ua/laws/show/1187-2015-%D0%BF#Text).
Також враховується їх наукова та професійна діяльність, а саме: публікації в науково-метричних базах Scopus, Web of Science, наявність сертифікатів неформальних курсів за напрямами викладання, наявність сертифікатів на знання іноземних мов, наявність сертифікатів підвищення кваліфікації в галузі "Кібербезпеки та захисту інформації".

Опишіть, із посиланням на конкретні приклади, яким чином заклад вищої освіти залучає

роботодавців, їх організації, професіоналів-практиків та експертів галузі до реалізації освітнього процесу

Під час розробки ОНП для погодження переліку компетентностей здобувачів вищої освіти другого (магістерського) рівня та на їх основі вибору дисциплін навчального плану, які повинні забезпечити формування відповідних результатів навчання були залучені комерційний директор ТОВ "Сайфер БІС", к.т.н., доцент, Ковтун Владислав Юрійович; к.т.н. доцент Олена Волощук, керівник освітньо-наукового департаменту компанії "Distributed Lab", директор ТОВ "МікрокриптТехнолоджис" к.т.н, доцент Сергій Головашіч запропонували спільну підготовку дисертаційних досліджень, які пов'язані з науковою діяльністю компанії.
В навчальній процес компанія ТОВ "Сайфер БІС" запропонувала використовувати ЦСК. Компанія "Distributed Lab" запропонувала провести курс лекцій з Блокчейн-технології, а саме "Криптографія в децентралізованих системах"(https://distributed.education/cryptography-course).

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

Професійному розвитку викладачів ОНП сприяє система післядипломної освіти НТУ "ХПІ" (https://www.kpi.kharkov.ua/ukr/osvita/pislyadiploplomna-osvita/), у межах якої пропонуються програми з підвищення кваліфікації та тренінги з розвитку загальних і професійних компетентностей, актуальних навичок викладача.
В НТУ "ХПІ" передбачено гранти та стажування у зарубіжних ВНЗ http://www.ec.kharkiv.edu/gsk.html та http://www.ec.kharkiv.edu/mp.html. Положення про підвищення кваліфікації педагогічних і науково-педагогічних працівників Національного технічного університету "Харківський політехнічний інститут" (затверджено Вченою радою Університету протокол № 8 від 01.11.2024 р., введено в дію наказом ректора 14.11.2024 р. № 472 ОД https://blogs.kpi.kharkov.ua/v2/nv/dokumenty/normatyvni-dokumenty).
Викладачі кафедри кібербезпеки отримали дипломи рівня В2 з англійської мови: Мілевський С. В., Погасій С. С., Євсеєев С. П., Гаврилова А. А., Корольов Р. В., Ткачов А. В., Воропай Н. І., Аксьонова І. В., Севрюкова Є. О.
Пройшли стажування в Університеті національного комітету освіти у Кракові (Польща) на кафедрі інженерії програмного забезпечення за напрямом "Методи та технічні засоби захисту інформації" тривалістю 180 годин (6 кредитів), Євсеєв С. П., Мілевський С. В., Погасій С. С., Король О. Г., Корольов Р. В., Аксьонова І. В., Гаврилова А. А., Мілевська Т. С., Ткачов А. М., Хвостенко В. С.
Євсеєв С. П., Король О. Г., Ткачов А. М., Корольов Р. В. є сертифікованими спеціалістами з курсів CCNA Cisco.

Наведіть конкретні приклади заохочення розвитку викладацької майстерності

Матеріальне стимулювання діяльності викладачів регулюється Колективним договором між адміністрацією НТУ "ХПІ" та комітетом первинної профспілкової організації працівників (https://public.kpi.kharkov.ua/profspilkova-organizatsiya/).
Матеріальне стимулювання наукової діяльності викладачів за публікацію Scopus та Web Of Science (https://ndch.kpi.kharkov.ua/polozhennya/).
Станом на 01.11.2025 р. доступні такі зовнішні ресурси: аналітичні – Scopus, SciVal та платформа Web of Science (з можливістю віддаленого доступу); повнотекстові – Springer Nature (доступні книги 2017 р. видання); ScienceDirect (книжкові видання та книжкові розділи, віддалений доступ для користувачів корпоративної пошти); Bentham Science (доступні книги та журнали). Вченою радою університету запроваджено додаткове диференційоване матеріальне стимулювання за викладання англійською мовою (протокол Вченої ради № 1 від 31.01.2020 р. http://blogs.kpi.kharkov.ua/v2/vr/archives/1820).
Динаміка обсягів мотиваційних доплат до заробітної плати (надбавок, премій, матеріальної допомоги) щорічно висвітлюється у Звітах ректора (приклад, ЗВІТ РЕКТОРА НТУ "ХПІ" (http://public.kpi.kharkov.ua/zvit-rektora/).
Протягом року за досягнення у фаховій сфері науково-педагогічні працівники кафедр та інститутів нагороджуються почесними грамотами від ректора університету, органів місцевого самоврядування, Міністерства освіти України, що дозволяє формувати систему заохочень викладачів нематеріального характеру.

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

Фінансово-бюджетну звітність, штатний розпис та кошториси наведено на сайті НТУ "ХПІ" https://bit.ly/3kiO2l9.
Детальна інформація про оновлення матеріально-технічної бази є у звітах ректора https://public.kpi.kharkov.ua/administrativna-diyalnist/zvit-rektora/.
Здобувачі вищої освіти мають доступ до таких матеріально-технічних ресурсів НТУ "ХПІ" (безоплатно): навчальних приміщень заг. площею 91582 м2 в т.ч.: лекційні, аудиторні приміщення, кабінети, лабораторії – 78994 м2, Комп'ютерні лабораторії – 4901 м2, спортивні зали – 7687 м2 https://bit.ly/2YxvFRP; комп'ютерної мережі з Wi-Fi (94 точки доступу), під'єднаної до мережі Eduroam. На сьогодні в університеті є 3187 комп'ютерів та 93 мультимедійних проектори.
Доступ до інформаційних ресурсів та фондів бібліотеки надається на 6 абонементах, 7 читальних залах бібліотеки та в 32 читальних залах при кафедрах.
Вільний доступ – електронний репозитарій НТУ "ХПІ" (eNTUKhPIIR) http://repository.kpi.kharkov.ua/; ресурси

авторизованого доступу – повнотекстова база “Навчальні видання” та повнотекстова база “Праці вчених НТУ “ХПІ” електронного каталогу науково-технічної бібліотеки НТУ “ХПІ” https://library.kpi.kharkov.ua/uk/resursu.
Станом на 30.12.2025р. доступні зовнішні ресурси: аналітичні – Scopus, SciVal та платформа Web of Science (з можливістю віддаленого доступу); повнотекстові – Springer Nature (доступні книги 2017 р. видання); ScienceDirect (книжкові видання та книжкові розділи, віддалений доступ для користувачів корпоративної пошти); Bentham Science (доступні книги та журнали).

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

Доступ здобувачів вищої освіти до інфраструктури та інформаційних ресурсів, необхідних для навчання, наукової діяльності в межах ОНП є безкоштовним. Університет надає навчальні приміщення, лабораторії та комп'ютерні класи, оснащені необхідним обладнанням і програмним забезпеченням, що відповідає Ліцензійним умовам провадження освітньої діяльності https://public.kpi.kharkov.ua/administrativna-diyalnist/materialno-tehnichne-zabezpechennya/. Науково-технічна бібліотека НТУ “ХПІ”, крім вільного доступу до Інтернету, Wi-Fi, забезпечує вільний доступ до національних і світових інформаційних ресурсів https://library.kpi.kharkov.ua/uk/resursu який надається на абонементах та читальних залах. Здобувачі мають також вільний доступ до електронного репозиторію НТУ “ХПІ” (eNTUKhPIIR) (http://repository.kpi.kharkov.ua/)
та ресурсу авторизованого доступу до Повнотекстової бази “Навчальні видання” електронного каталогу науково-технічної бібліотеки НТУ “ХПІ” та Повнотекстової бази
“Праці вчених НТУ “ХПІ” електронного каталогу науково-технічної бібліотеки НТУ “ХПІ”.

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

Потреби та інтереси здобувачів вищої освіти належним чином виявляються під час співпраці ЗВО з органами студентського самоврядування. На базі НТУ “ХПІ” працює СтудАльянс (https://web.kpi.kharkov.ua/studalliance/).
У житті студентів і співробітників НТУ “ХПІ” велику роль відіграє учбово-спортивний комплекс “ПОЛІТЕХ”. Він є фундаментальною базою, де створені умови для проведення учбових занять, реалізації потенціалу студентів у самостійних заняттях фізичною культурою та спортом. Саме тут проводяться тренування збірних команд України з баскетболу, бадмінтону, легкої атлетиці та іншим видам спорту, чисельні спортивно-масові та фізкультурно-оздоровчі заходи (https://www.kpi.kharkov.ua/ukr/studentske-zhittya/cportivnij-kompleks/).
На базі Палацу студентів НТУ “ХПІ” працюють 18 творчих колективів, 8 з яких мають почесне звання “Народний художній колектив України”. Колективи Палацу студентів беруть активну участь у проведенні різних міських, обласних, всеукраїнських та міжнародних конкурсів і фестивалів.
Здобувачі вищої освіти та викладачі мають вільний безкоштовний доступ до сучасної науково-технічної бібліотеки з можливістю: вільного доступу до Інтернету, Wi-Fi, попереднього дистанційного замовлення видань з фонду, електронного каталогу повнотекстові бази та багато інших послуг (http://library.kpi.kharkov.ua/uk).

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.

Права та обов’язки здобувачів освіти регламентують Правила поведінки здобувачів освіти НТУ “ХПІ” https://blogs.kpi.kharkov.ua/v2/nv/wp-content/uploads/sites/43/2023/12/Pravyla-povedinky-zdobuvachiv-osvity.pdf
Навчально-методичне забезпечення дисциплін ОНП доступно на внутрішньому репозитарії електронних документів кафедри. Методичні рекомендації та учбові посібники розміщені в електронному репозитарії. НТУ “ХПІ” (https://repository.kpi.kharkov.ua/collections/76947913-5200-482f-9bce-6a54c2ab31da). На території університету доступна наукометрична БД Scopus. Зареєстрованим читачам бібліотеки також надається і можливість віддаленої роботи (http://library.kpi.kharkov.ua/uk/node/4572).
Навчально-методичне забезпечення дисциплін ОНП доступно на внутрішньому репозитарії електронних документів кафедр. Методичні рекомендації та навчальні посібники розміщені в електронному репозитарії НТУ “ХПІ” (https://repository.kpi.kharkov.ua/collections/76947913-5200-482f-9bce-6a54c2ab31da). Консультативна підтримка здобувачів, надання допомоги та інформування здійснюється через наукових керівників та завідувачів кафедр, за якими закріплені здобувачі.
Комунікація викладачів із здобувачами здійснюється безпосередньо під час занять, консультацій тощо.
Соціальною підтримкою здобувачів вищої освіти є академічна стипендія, соціальна стипендія та інші стипендії за результатами навчання. Профспілка студентів НТУ “ХПІ” (https://www.kpi.kharkov.ua/ukr/studentske-zhittya/profspilkova-organizatsiya-studentiv/) надає: соціальну підтримку у вигляді матеріальної допомоги студентам з малозабезпечених сімей та при тимчасовій втраті здоров’я, організовує відпочинок та дозвілля студентів, надає правовий захист, контролює роботу підприємства громадського харчування університету, підтримує ініціативи студентів, допомагає віршувати побутові проблеми студентів в гуртожитках.
В медичному пункті НТУ«ХПІ» працюють 11 лікарів. Мета роботи оздоровчого пункту забезпечення доступної якісної та кваліфікованої медичної допомоги здобувача третього рівня вищої освіти. На базі НТУ “ХПІ” створена соціально-психологічна служба. Метою діяльності якої є соціально-психологічне забезпечення навчально-виховного процесу, підвищення ефективності навчального, наукового процесу, особистісний розвиток, захист психічного здоров'я, соціального благополуччя студентів, викладачів та працівників (https://blogs.kpi.kharkov.ua/v2/nv/dokumenty/normatyvni-dokumenty).

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)

Порядок супроводу (надання допомоги) осіб з інвалідністю та інших мало мобільних груп населення в Національному технічному університеті "Харківський політехнічний інститут" здійснюється згідно наказу № 129 ОД від 24 лютого 2020 р. про порядок супроводу (надання допомоги) осіб з інвалідністю та інших маломобільних груп населення в НТУ "ХПІ" (https://public.kpi.kharkov.ua/wp-content/uploads/2020/03/Poryadok-suprovodu-NOVA-REDAKTSIYA-v-red.yur.otd.pdf), також ці процедури прописані в правилах прийому до НТУ "ХПІ" (http://vstup.kpi.kharkov.ua/admission/admission_rules/).
Корпуси обладнані пандусами та ліфтами, що дає можливість студентам з обмеженими можливостями навчитися. На даній ОНП такі студенти не навчались.
Документи, які регулюють перебування осіб з особливими освітніми потребами в ЗВО:
1) http://vstup.kpi.kharkov.ua/korisni-posilannya-dlya-abituriientiv/normatygni-dokumenty/?fbclid=IwAR38EDcauCcXp4S7Ls4MNesrklEZAwetVjRq8xmeLZc8hLecpxLrtLmerQ
2) https://public.kpi.kharkov.ua/wp-content/uploads/2020/03/Poryadok-suprovodu-NOVA-REDAKTSIYA-v-red.yur.otd.pdf (наказ № 129 Од від 24 лютого 2020 р.).
Серед здобувачів вищої освіти за ОНП подібних прикладів не було.

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

Процедури врегулювання конфліктних ситуацій (включаючи пов'язаних із сексуальними домаганнями, дискримінацією та корупцією) в Університеті прописані в кодексі етики академічних взаємовідносин та доброчесності НТУ "ХПІ", який погоджено та підтримано на Конференції трудового колективу НТУ "ХПІ". Здобувач вищої освіти має право звернутися до ректора, проректора, директора інституту зі скаргою стосовно питань конфліктних ситуацій.
Процедура звернення регулюється Порядком розгляду скарг здобувачів вищої освіти у НТУ "ХПІ", який введено в дію наказом ректора НТУ "ХПІ" № 68 ОД від 26 лютого 2025 р. https://blogs.kpi.kharkov.ua/v2/nv/wp-content/uploads/sites/43/2025/04/Poryadok-rozglyadu-skarg-zdobuvachiv.pdf
Діяльність щодо запобігання та протидії булінгу (цькуванню) в університеті є системним процесом та регулюється Планом заходів із запобігання та протидії булінгу (цькування) у НТУ "ХПІ", конфліктні ситуації розглядаються згідно до Порядку подання та розгляду заяв про випадки булінгу (цькування), реагування на доведені випадки булінгу (цькування) у НТУ "ХПІ" (https://blogs.kpi.kharkov.ua/v2/nv/wp-content/uploads/sites/43/2023/12/Poryadok-podannya-ta-rozglyadu-reaguvannya-na-dovedeni-vypadky-boulingu.pdf, https://blogs.kpi.kharkov.ua/v2/nv/wp-content/uploads/sites/43/2023/12/Plan-zahodiv-iz-zapobigannya-ta-protydiyi-boulingu.pdf).
У разі ситуацій пов'язаних із сексуальними домаганнями, дискримінацією з потерпілим працює соціально-психологічна служба НТУ "ХПІ". https://web.kpi.kharkov.ua/ppuss/uk/sotsialno-psihologichna-sluzhba-ntu-hpi/.
Практики застосування таких процедур на даній ОНП не було.

8. Внутрішнє забезпечення якості освітньої програми

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

Процедури розроблення, затвердження, моніторингу та періодичного перегляду ОНП регулюються "Методичними рекомендаціями щодо порядку розроблення, затвердження, моніторингу та періодичного перегляду освітніх програм в НТУ "ХПІ" та "Методичними рекомендаціями щодо розроблення, затвердження та оновлення освітніх програм"
https://blogs.kpi.kharkov.ua/v2/nv/wp-content/uploads/sites/43/2025/07/Metodychni-rekomendatsiyi-OP-2025-2026n.r.-Versiya-5-1.pdf
2) Положення про гаранта освітньої програми https://blogs.kpi.kharkov.ua/v2/nv/wp-content/uploads/sites/43/2024/07/Polozhennya-pro-garanta-osvitnoyi-programy.pdf;
3) Положення про внутрішню систему забезпечення якості вищої освіти в Національному університеті https://blogs.kpi.kharkov.ua/v2/quality/wp-content/uploads/sites/44/2025/11/Polozhennya-pro-zabezpechennya-yakosti-osvitnoyi-diyalnosti-ta-yakosti-vyshhoyi-osvity-v-NTU-HPI.pdf;
4) Положення про раду із забезпечення якості вищої освіти https://blogs.kpi.kharkov.ua/v2/quality/yakist-osvity/rada-z-yakosti/
5) Моніторинг освітніх програм https://blogs.kpi.kharkov.ua/v2/quality/yakist-osvity/monitoryng-op/
6) Моніторинг якості в університеті https://blogs.kpi.kharkov.ua/v2/quality/yakist-osvity/monitoryng-yakosti /

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

Згідно з Методичними рекомендаціями щодо порядку розроблення, затвердження, моніторингу та періодичного перегляду освітніх програм в Національному технічному університеті "Харківський політехнічний інститут"

https://blogs.kpi.kharkov.ua/v2/nv/wp-content/uploads/sites/43/2025/07/Metodychni-rekomendatsiyi-OP-2025-2026n.r.-Versiya-5-1.pdf перегляд освітніх програм відбувається щорічно.
При цьому враховується: прийняття чи коригування стандарту вищої освіти; висновки акредитаційної експертизи; відгуки стейкхолдерів; перегляд місії та стратегії Університету; результати наукових досліджень; результати вступної кампанії та інше. У випадку необхідності внесення змін гарант освітньої програми здійснює коригування потрібних елементів освітньої програми, узгоджує її з навчальним та навчально-методичними відділами, виносить на затвердження Вченою радою Університету. Зміни вводяться в дію наказом ректора та мають бути оприлюднені на офіційних веб ресурсах Університету.
Перегляд ОНП здійснює група забезпечення спеціальності, завдання та функції якої визначені у зазначених "Методичних рекомендаціях щодо розроблення, затвердження та оновлення освітніх програм".
Перегляд та оновлення ОНП відбувається кожен навчальний рік з урахуванням результатів моніторингу ОНП https://blogs.kpi.kharkov.ua/v2/nv/dokumenty/normatyvni-dokumenty, зауважень, результатів, відображених у звітах про забезпечення якості освіти в Університеті https://blogs.kpi.kharkov.ua/v2/quality/yakist-osvity/rezultaty-opytuvan/, висновків та пропозицій роботодавців та здобувачів вищої освіти; стратегії (програми) розвитку університету тощо.
Були прийняті до уваги пропозиції компаній стейкхолдерів (учасників розробки ОНП) а саме: технічний директор компанії Сайфер Владислав Ковтун запропонував розгортання ЦСК, який дозволить сформувати електронний документообіг та формування елементі корпоративної інформаційно-освітньої системи, а також проводити дослідження моделей: синергічної моделі загроз, моделі порушника на об'єкти критичної інфраструктури, а також формування універсального класифікатора загроз соціокіберфізичної системи.

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

Здобувачі мають постійний доступ до змісту та складових ОНП на сайті НТУ "ХПІ". До процесу періодичного перегляду ОНП та інших процедур забезпечення її якості їх залучають для проведення опитувань щодо змісту усієї програми та конкретних дисциплін, формування набору дисциплін вільного вибору. Думка здобувачів щодо якості викладання на ОНП збирається шляхом проведення анонімного анкетування (https://cybersecurity.khpi.edu.ua/onovlennya-osvitnikh-program-125-magistr/), або пропозиції здобувачів щодо удосконалення ОНП збираються також безпосередньо під час освітнього процесу шляхом спілкування з гарантом програми, НПП випускових кафедр. Окрім цього здобувачі, мають змогу поставити свої питання та надати пропозиції на офіційний e-mail кафедри.

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

До процесу періодичного перегляду ОНП та інших процедур внутрішнього забезпечення якості освіти в Університеті активно залучаються органи студентського самоврядування та Рада молодих вчених http://blogs.kpi.kharkov.ua/v2/rmv/.
В НТУ "ХПІ" органи студентського самоврядування беруть участь в обговоренні та вирішенні питань удосконалення освітнього процесу, науково-дослідної роботи, призначення стипендій, організації дозвілля, оздоровлення, побуту та харчування; беруть участь у заходах (процесах) щодо забезпечення якості вищої освіти; делегують своїх представників до робочих, консультативно-дорадчих органів (Конференція трудового колективу Університету, Вчена рада Університету, Вчені ради інститутів); вносять пропозиції щодо змісту навчальних планів і програм. На сторінці інституту (https://web.kpi.kharkov.ua/if/uk/category/uastud/) викладені події, які відображають діяльність Студентської ради інституту. Також студенти можуть оцінити якість викладання дисциплін через анонімне анкетування, що проводиться впродовж всього терміну навчання (https://docs.google.com/forms/d/e/1FAIpQLSeO8H958E--31eITdamcoUImdRacn6BoxGrmZCreVaNbJ_6ZQ/viewform)

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

Роботодавці (стейкхолдери) мають можливість безпосередньо подати пропозиції щодо ОНП "Кібербезпека" через відповідну сторінку сайту кафедри (https://cybersecurity.khpi.edu.ua/onovlennya-osvitnikh-program-125-magistr/). Відповідно до співпраці Проєкт наступної ОНП погоджується з членами робочої групи, компанією ТОВ "Сайфер БІС" та компанією "Distributed Lab", а також з генеральним директором ТОВ "Микрокрипт Текнолоджис".

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

НТУ "ХПІ", і зокрема на сайті Інституту комп'ютерних наук та інформаційних технологій сформовано систему збирання інформації щодо кар'єрного шляху випускників університету https://web.kpi.kharkov.ua/asu/istoriyi-uspihu/. Цим займається Навчально-методичний відділ договірної та практичної підготовки, Центр "Кар'єра" https://web.kpi.kharkov.ua/career/, Асоціація випускників НТУ "ХПІ" https://alumni.kpi.kharkov.ua/. Працівники відділів та структур у тісної взаємодії з представниками випускових кафедр здійснюють збір інформації щодо працевлаштування випускників, зокрема випускників аспірантури минулих років, яка аналізується на засіданнях Вченої ради університету). Кафедра проводить аналіз конкурентоспроможності майбутніх випускників шляхом дослідження ринку праці. У якості прикладу можна навести аналітичний звіт "Розвиток української IT-індустрії" (https://bit.ly/2S6wdr1), (https://bit.ly/2Gcq9ux).

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

Під час реалізації ОП згідно документів здійснення процесів і процедур внутрішнього забезпечення якості освіти в НТУ "ХПІ" (https://surl.li/ksjats) були здійснені наступні процедури: анкетування здобувачів вищої освіти; контроль підвищення кваліфікації співробітників НТУ "ХПІ" (https://cybersecurity.khpi.edu.ua/wp-content/uploads/2025/12/%D0%A0%D0%B5%D0%B7%D1%83%D0%BB%D1%8C%D1%82%D0%B0%D1%82%D0%B8_%D0%BE%D0%BF%D0%B8%D1%82%D1%83%D0%B2%D0%B0%D0%BD%D0%BD%D1%8F_%D0%BC%D0%B0%D0%B3%D1%96%D1%81%D1%82%D1%80_%D0%BD%D0%B0%D1%83%D0%BA%D0%BE%D0%B2%D1%86%D1%96.pdf); підвищення педагогічної майстерності науково-педагогічних працівників шляхом організації семінарів, конференцій, круглих столів та форумів (http://blogs.kpi.kharkov.ua/v2/metodotdel/konferentsiyi/) проведення заходів із виявлення та запобігання академічному плагіату (https://blogs.kpi.kharkov.ua/v2/quality/wp-content/uploads/sites/44/2024/06/polozhennya-proekt-plagyat.pdf).
Система забезпечення якості НТУ "ХПІ" постійно моніторить якість освітніх послуг (відповідно до «Положення про моніторинг результатів навчання здобувачів вищої освіти НТУ "ХПІ" https://blogs.kpi.kharkov.ua/v2/quality/dokumenty/normatyvni-dokumenty/) і оперативно реагує на результати моніторингу, впроваджуючи механізми для швидкого коригування освітніх процесів відповідно до потреб і очікувань заінтересованих сторін. В університеті на постійній основі проводиться моніторинг якості, який базується на "Положенні про моніторинг результатів навчання здобувачів вищої освіти Національного технічного університету "Харківський політехнічний інститут" та включає перевірку залишкових знань студентів. Результати наведені за посиланням: https://blogs.kpi.kharkov.ua/v2/quality/yakist-osvity/monitoryng-yakosti/. Ключовим інструментом моніторингу ОП та освітньої діяльності в цілому є регулярні опитування зацікавлених сторін та моніторинг якості освітніх послуг, які регламентовані: "Положення про порядок організації та проведення опитування учасників освітнього процесу" (https://blogs.kpi.kharkov.ua/v2/quality/dokumenty/normatyvnidokumenty) та "Положення про моніторинг результатів навчання здобувачів вищої освіти НТУ "ХПІ" (https://blogs.kpi.kharkov.ua/v2/quality/dokumenty/normatyvnidokumenty). Результати опитування враховуються при вдосконаленні організації освітнього процесу, щорічному (згідно з "Методичними рекомендаціями щодо порядку розроблення, затвердження, моніторингу та періодичного перегляду ОП в НТУ "ХПІ" https://blogs.kpi.kharkov.ua/v2/nv/wpcontent/uploads/sites/43/2024/09/METODYCHKA-OP-2024-zminy-vid-23.09.2024-2.pdf) перегляді змісту ОП і силабусів, виборі технологій і методів викладання, виборі тем підвищення кваліфікації викладачів, оновленні фонду Науково-технічної бібліотеки та удосконаленні інформаційної політики Університету. Для отримання зауважень та пропозицій на сайті кафедри розміщено оголошення про запрошення усіх зацікавлених осіб до перегляду ОНП та надання рекомендацій, зауважень, відгуків.

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

Акредитація уперше. Під час удосконалення освітньо-наукової програми «Кібербезпека» системно враховуються результати зовнішнього забезпечення якості вищої освіти, зокрема висновки та рекомендації експертних груп і галузевих експертних рад, отримані в межах акредитаційних процедур інших освітніх програм закладу вищої освіти, а також загальні рекомендації НАЗЯВО. Аналіз матеріалів попередніх акредитацій дозволив ідентифікувати напрями для посилення практикоорієнтованості, студентоцентрованого підходу, інтеграції наукових досліджень в освітній процес та розширення можливостей формування індивідуальних освітніх траєкторій.
Досвід акредитацій інших освітніх програм ЗВО також був використаний для вдосконалення внутрішньої системи забезпечення якості, що сприяло підвищенню узгодженості цілей ОП, освітніх компонентів і очікуваних результатів навчання та забезпечило сталий розвиток освітньої програми відповідно до національних і європейських стандартів якості вищої освіти.
Висновки та рекомендації щодо якості освітніх програм за результатами акредитаційних експертиз 2024-2025 н.р. (Магістр ОНП)
https://blogs.kpi.kharkov.ua/v2/quality/wp-content/uploads/sites/44/2025/06/Vysnovky-ta-rekomendatsiyi-shhodo-yakosti-osvitnih-program-za-rezultatamy-akredytatsijnyh-ekspertyz-2024-2025-n.r.-Magistr-ONP.pdf
Перелік рекомендованих заходів до усунення зауважень щодо якості освітньої програми у постакредитаційний період
https://blogs.kpi.kharkov.ua/v2/quality/wp-content/uploads/sites/44/2024/10/Perelik-rekomendovanyh-zahodiv.pdf

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

Учасники академічної спільноти змістовно залучаються до процедур внутрішнього забезпечення якості ОНП наступним чином. В обговорені освітніх компонентів приймали участь завідувач кафедри кібербезпеки та математичного моделювання Чернігівського державного технологічного університету (м. Чернігів) д.пед.н., доц. Ткач Ю.М., професор кафедри менеджменту організацій Києво-Могилянської бізнес школи Національного університету "Києво-Могилянська академія", д.т.н., професор Молодецька Катерина Валеріївна (м. Київ), завідувач кафедри кібербезпеки та програмного забезпечення Центрально-українського національного технічного університету, д.т.н., професор, Смірнов Олексій Анатолійович (м. Кропивницький), завідувачка кафедри інформаційних технологій Одеського національного університету ім. І. І. Мечникова, д.т.н., професор Казакова Надія Феліксівна (м. Одеса).
З метою своєчасного врахування зауважень та пропозицій від академічної спільноти на сайті кафедри створена

сторінка, яка дозволяє своєчасно ознайомитись з пропозиціями внесення змін до ОНП “Кібербезпека”. Крім цього, є можливість відправити свої пропозиції та зауваження з використання веб-застосунку (https://cybersecurity.khpi.edu.ua/onovlennya-osvitnikh-program-125-magistr/).

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

З метою своєчасного врахування зауважень та пропозицій від академічної спільноти на сайті кафедри створена сторінка, яка дозволяє своєчасно ознайомитись з пропозиціями внесення змін до ОНП “Кібербезпека”. Крім цього, є можливість відправити свої пропозиції та зауваження з використання веб-застосунку (https://cybersecurity.khpi.edu.ua/onovlennya-osvitnikh-program-125-magistr/).
Розподіл відповідальності між структурними підрозділами НТУ “ХПІ”:
– відділ забезпечення якості освітньої діяльності забезпечує моніторинг якості освіти НТУ “ХПІ”, згідно з вимогами Закону України “Про вищу освіту” та нормативно-правових документів МОН України (http://blogs.kpi.kharkov.ua/v2/quality/pro-viddil/).
– навчальний відділ (https://blogs.kpi.kharkov.ua/v2/nv/) забезпечує організацію та контроль освітнього процесу, організує підвищення професійного розвитку викладачів;
– методичний відділ НТУ “ХПІ” розробляє форми нормативних документів, які регламентують певні види методичної діяльності, організує проведення Методичної ради НТУ “ХПІ”, на якій обговорюються питання методичної діяльності (http://blogs.kpi.kharkov.ua/v2/metodotdel/);
– відповідальними за впровадження та виконання моніторингу і перегляду відповідних освітніх програм є випускаюча кафедра, робоча група та гарант ОНП.
Структурні підрозділи співпрацюють на забезпечення якості освіти.

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?

В НТУ “ХПІ” розроблені нормативні документи, в яких визначені права та обов’язки усіх учасників освітнього процесу, які знаходяться у відкритому доступі, розміщенні на офіційному веб-сайті НТУ “ХПІ” і доступні для аналізу та висловлення зауважень аспірантами.
До них відносяться:
Статут НТУ “ХПІ” https://public.kpi.kharkov.ua/administrativna-diyalnist/statut/;
Правила внутрішнього розпорядку НТУ “ХПІ” https://library.kpi.kharkov.ua/files/documents/pravila-vnutr-rozporyadku-2018.pdf;
Положення про організацію освітнього процесу в НТУ “ХПІ” https://bit.ly/3McqkrC;
Положення про підготовку здобувачів вищої освіти ступеня доктора філософії в аспірантурі https://bit.ly/3MfMwRx;
Положення про забезпечення якості освітньої діяльності та якості вищої освіти у НТУ “ХПІ” https://bit.ly/445dVvG;
Положення про порядок реалізації на академічну мобільність здобувачів, аспірантів, докторантів, науково-педагогічних, наукових та інших працівників НТУ “ХПІ” https://bit.ly/3KEzVa7;
Положення про критерії та систему оцінювання знань та вмінь і про рейтинг здобувачів вищої освіти НТУ “ХПІ” https://surl.li/lsvrdt;
Положення про Вчену раду, Положення про Наглядову раду НТУ “ХПІ” https://surl.lu/bjcyfu
Положення про раду з якості НТУ “ХПІ” https://surl.li/qcmcyv
Положення про кафедру НТУ “ХПІ” https://surl.li/gytrqj.

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

https://cybersecurity.khpi.edu.ua/onovlennya-osvitnikh-program-125-magistr/

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

https://cybersecurity.khpi.edu.ua/osvitno-naukova-prohrama-mahistr/

11. Перспективи подальшого розвитку ОП

Якими загалом є сильні та слабкі сторони ОП?

Сильними сторонами ОНП є впровадження сучасного підходу до підготовки магістрів з кібербезпеки, а саме

поєднання набуття компетентностей з елементами науково-дослідницької роботи, що дозволяє працевлаштовуватись аналітиками загроз безпеки, аналітиками систем захисту інформації та оцінки вразливостей, аналітиками з безпеки інформаційно-телекомунікаційних систем та ін. в кіберполіцію, у державні органи та СБУ, а також подальше навчання на третьому рівні вищої освіти. Проведення майстер класів спеціалістами компанії DistributedLab в рамках ОК, які пов'язані з технологією блокчейн, що дозволить здобувачам вищої освіти отримувати знання в сучасних новітніх технологіях.
Використання навчальних курсів академії Cisco, що дозволяє здобувачам вищої освіти отримувати знання на рівні міжнародної освіти. Удосконалення практичних занять з технології PKI на основі ЦСК дозволяє здобувачам вищої освіти отримувати відповідні компетенції щодо їх застосування в сфері електронного документообігу.
Можливість студентів публікувати результати досліджень в науковому журналі кафедри "Територія безпеки/Terra Security", а також апробувати на міжнародній науково-практичній конференції кафедри "Інформаційна безпека та інформаційні технології".
Удосконалення ОК, які пов'язані з набуттям компетентностей з захисту об'єктів критичної інфраструктури.
Подальше нарощування програмно-апаратних засобів для кіберполігону, що дозволить посилити практичну складову результатів навчання за сучасними технологіями.
Слабкими сторонами ОНП є відсутність створення CIRT на базі кіберполігону, приєднання до мережі CERT України.

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

Перспективами розвитку ОНП є:
– вдосконалення практичних проектів на базі лабораторії блокчейн-технології завдяки розширенню кількості серверів віртуалізації і розробки розподіленої мережі віртуальних машин для програмування задач, що містять блокчейн-рішення;
– розширити залученість студентів до співпраці з міжнародною академічною спільнотою;
– розширити роботу з компаніями-стейкхолдерами та залучити професіоналів-практиків до аудиторних занять на ОНП;
– ввести науковий журнал кафедри "Територія безпеки/Terra Security" в категорію "Б";
– забезпечити можливість вивчення навчальних дисциплін дистанційно.

Запевнення

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

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

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

Додатки:

Таблиця 1. Інформація про обов'язкові освітні компоненти ОП

Таблиця 2. Зведена інформація про викладачів ОП

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

***

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

Документ підписаний кваліфікованим електронним підписом/кваліфікованою електронною печаткою.

Інформація про КЕП

ПІБ:

Дата:

Таблиця 1. Інформація про 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**	
Філософські проблеми сучасного наукового пізнання	навчальна дисципліна	*НП 2_Магістр_1.9_Філософські проблеми сучасного наукового пізнання.pdf*	hgT6XlpYlicuf+ouHCPY89IEw3pqCDi2xTQbI6MKJmE=	*Обладнання:* *Мультимедійні аудиторії, ПК з доступом до Інтернету* *ПЗ: Packet Tracer* *Література:* *1.Кодекс етики академічних взаємовідносин та доброчесності Національного Технічного Університету «Харківський Політехнічний Інститут» СУЯ ХПІ-ВЗЯОД-МР/10.1:2023. https://blogs.kpi.kharkov.ua/v2/nv/wp-content/uploads/sites/43/2024/04/Kodeks-etyky-akademichnyh-vzayemovidnosyn-ta-dobrochesnosti-Natsionalnogo-tehnichnogo-universytetu-Harkivskyj-politehnichnyj-instytut-.pdf* *2.Система стандартів з організації навчального процесу. ТЕКСТОВІ ДОКУМЕНТИ У СФЕРІНАВЧАЛЬНОГО ПРОЦЕСУ. Загальні вимоги до виконання. СТЗВО-ХПІ-3.01-2025. https://blogs.kpi.kharkov.ua/v2/metodotdel/wp-content/uploads/sites/28/2025/06/STZVO-HPI-3.01-2025-2.pdf* *3.Філософські проблеми сучасно наукового пізнання: підручник для студентів-магістрівусіх спеціальностей і форм навчання. / Я.В. Тараоєв; О.О. Дольська; Т.М. Дишкант та ін.Харків: Видавець Іванченко І. С., 2023. – 350 с. https://repository.kpi.kharkov.ua/server/api/core/bitstreams/ec570172-dc88-4ef3-90b1-17adb2605928/content* *4.Заремський М.Й. Філософія науки: навчально-методичний посібник для аспірантів.Глухів, 2022. – 211 с. http://46.201.250.252:8080/handle/123456789/1796* *5.Стежко, З. В. Філософські проблеми наукового пізнання: навч. посіб. / З. В. Стежко,С. П. Римар ; М-во освіти і науки України, Центральноукраїн. нац. техн. ун-т. –Кропивницький : ЦНТУ, 2022. – 141 с. https://dspace.kntu.kr.ua/handle/123456789/12347* *6.Житарюк І.В. Філософія освіти, науки та окремих її галузей. Конспект лекцій: Навч.посібник. – 2-ге вид., стереотипне. Київ: Видавництво «Людмила», 2022. – 620 с. https://archer.chnu.edu.ua/xmlui/bitstream/handle/123456789/5000/%d0%a4%d0%9e%d0%9d.pdf* *7.Філософія науки : підручник/ О. П. Дзьобань; ДНУ «Ін-т інформації, безпеки і права*

				Нац.академії прав. наук України». – Київ; Одеса : Фенікс, 2024. – 516 с. https://ippi.org.ua/sites/default/files/filosofiya_nauki_2024.pdf 8.Кіпенський А. В., Тараоев Я. В. Техніка, наука і духовність у XXI сторіччі: філософськийаналіз / Вісник Національного технічного університету "Харківський політехнічнийінститут". Серія: Актуальні проблеми розвитку українського суспільства, 2023, № 1, с. 6–14. https://doi.org/10.20998/2227-6890.2023.1.01
Технології управління безпекою бізнес - процесів	навчальна дисципліна	*НП 7_Магістр_1.9_Технології управління безпекою бізнес-процесів.pdf*	aahrGR5uGVcfGVaioXkrcGOF5PvkRFdUJjuS8xYUoSg=	*Обладнання: Мультимедійні аудиторії ПК: Intel Pentium G4560/ОЗУ 4 GB DDR3-1600/Монітор 20" Dell P2017H/HDD 500 GB, 7200 об/хв, SATA 3.0 – 15шт. QlikView, QlikSense, Microsoft Power BI Література: 1 Інформаційна безпека та інформаційні технології. – Х.; ТОВ "ДІСА ПЛЮС", 2019. - 322 с. http://library.kpi.kharkov.ua/files/new_postupleniya/ibtait.pdf 2. Кібербезпека та інформаційні технології. – Х.; ТОВ "ДІСА ПЛЮС", 2020. -380 с. 3. Управління бізнес-процесами: Навч. посібник. – Рівне: НУВГП, 2014. – 158 с. https://ep3.nuwm.edu.ua/8812/1/%D0%A3%D0%BF%D1%80%D0%B0%D0%B2%D0%BB%D1%96%D0%BD%D0%BD%D1%8F%20%20%D0%B1%D1%96%D0%B7%D0%BD%D0%B5%D1%81-%D0%BF%D1%80%D0%BE%D1%86%D0%B5%D1%81%D0%B0%D0%BC%D0%B8.pdf 4. WEB-технології [Електронний ресурс]: Навчально-довідковий посібник / С.П. Євсеєв, А.М. Ткачов, В.О. Алексіев, Ю.М. Рябуха – Харків : ХНЕУ ім. С. Кузнеця, – Львів: Видавництво «Новий Світ –2000», 2021. – 390 с. https://drive.google.com/drive/u/1/folders/1wOTN8N-GBGOo6AnvjQHU1SdBl3xCaUju. 5. Synergy of building cybersecurity systems: monograph / S. Yevseiev, V. Ponomarenko, O. Laptiev, O. Milov and others. – Kharkiv: PC TECHNOLOGY CENTER, 2021. – 188 p. URL: https://drive.google.com/drive/u/1/folders/1wOTN8N-GBGOo6AnvjQHU1SdBl3xCaUju 6. Models of socio-cyber-physical systems security: monograph / S. Yevseiev, Yu. Khokhlachova, S. Ostapov, O. Laptiev and others. – Kharkiv: PC TECHNOLOGY CENTER, 2023. – 168 p. URL: https://drive.google.com/drive/u/1/folders/1wOTN8N-GBGOo6AnvjQHU1SdBl3xCaUju 7. Modeling of security systems for critical infrastructure facilities: monograph / S. Yevseiev, R. Hryshchuk, K. Molodetska, M. Nazarkevych and others. – Kharkiv: PC TECHNOLOGY CENTER, 2022.*

				– 196 p. URL: https://drive.google.com/drive/u/1/folders/1wOTN8N-GBGOo6AnvjQHU1SdBl3xCaUju.
Сучасні проблеми постквантової криптографії	навчальна дисципліна	*НП 3_Магістр_1.9_Сучасні проблеми постквантової криптографії_Євсеєв.pdf*	F+HB3sZHb+q5OFk74TbWh2vQcpTiTCOizjmjdysVFJo=	*Обладнання: Мультимедійні аудиторії ПК: Intel Pentium G4560/ОЗУ 4 GB DDR3-1600/Монітор 20" Dell P2017H/HDD 500 GB, 7200 об/хв, SATA 3.0 – 15шт. QlikView, QlikSense, Microsoft Power BI Література: 1. A RIDDLE WRAPPED IN AN ENIGMA. NEAL KOBLITZ AND ALFRED J. MENEZES Department of Mathematics, Box 354350, University of Washington, Seattle, WA 98195 U.S.A URL: https://eprint.iacr.org/2015/1018.pdf 2. Lili Chen, Stephen Jordan, Yi-Kai-Liu, Dustin Moody, Rene Peralta, Ray Perlner, Daniel Smith-Tone. Report on Post – Quatum Cryptography. NISTIR 8105 (DRAFT). URL: https://www.google.com.ua/search? 3. Shor, P. W. Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer / P. W. Shor // SIAM J. Comput. – 1997. – 26 (5). – P. 1484–1509. URL: https://fab.cba.mit.edu/classes/862.19/notes/computation/Shor-1999.pdf 4. Аналіз можливостей квантових комп'ютерів та квантових обчислень для криптоаналізу сучасних криптосистем / Ю. І. Горбенко, Р. С. Ганзя // Восточно-Европейский журнал передовых технологий. - 2014. - № 1(9). - С. 8-16. - Режим доступу: http://nbuv.gov.ua/UJRN/Vejpte_2014_1%289%29__3 5. М. Рябий // Безпека інформації. - 2014. - Т. 20, № 3. - С. 236-241. - Режим доступу: http://nbuv.gov.ua/UJRN/bezin_2014_20_3_6*
Основи управління в проєктах галузі кібербезпеки та захисту інформації	навчальна дисципліна	*5__19_~1.PDF*	pCz4//eub9mPOVmoRycQAvhv+Qb4dGdu7Ob2/W4lZZ4=	*Обладнання: Мультимедійні аудиторії ПК: Intel Pentium G4560/ОЗУ 4 GB DDR3-1600/Монітор 20" Dell P2017H/HDD 500 GB, 7200 об/хв, SATA 3.0 – 15шт. QlikView, QlikSense, Microsoft Power BI Література: 1. Гвоздь М. Я., Злидник Ю. О. AGILE – нова методологія менеджменту: теоретичні аспекти. Електронний журнал «Інфраструктура ринку», 2018. № 25. С 230-234. URL: https://er.nau.edu.ua/bitstream/NAU/61366/1/%d0%a3%d0%bf%d1%80%d0%b0%d0%b2%d0%bb%d1%96%d0%bd%d0%bd%d1%8f%20%d0%86%d0%a2-%d0%bf%d1%80%d0%be%d1%94%d0%ba%d1%82%d0%b0%d0%bc%d0%b8_%d0%a4%d0%b5%d0%bd%d0%b4%d1%8c%d0%be%20%d0%9e.%20%d0%9c..pdf*

				2. Демиденко М. А. Управління проектами інформатизації за методологією SCRUM : навч. посіб., 2016. – Дніпро. : Нац. гірн. ун-т. – 80 с. URL: https://ir.nmu.org.ua/jspui/bitstream/123456789/151152/1/scrum%20Demydenko%20Mykhailo.pdf *3. Довгань Л. Є., Мохонько Г. А., Малик І. П. Управління проектами: навч. посіб. до вивчення дисципліни для магістрів галузі знань 07 «Управління та адміністрування» спеціальності 073 «Менеджмент», 2017. – Київ : КПІ ім. Ігоря Сікорського. – 420 с URL: https://ela.kpi.ua/server/api/core/bitstreams/cf735d19-339f-44c8-8b5a-42f40468edf4/content* *4. Мартін Р. Чистий Agile: назад до основ / пер. з англ. В. Луненко, 2021. Харків : Вид-во «Ранок». 224 с.* *5. Моделі та засоби управління ІТ-проєктами: навч. посіб. / уклад.: В. О. Кузьмінних, О. В. Коваль, Р. А. Тараненко, 2023. Київ: КПІ ім. Ігоря Сікорського. 222 с. URL: https://ela.kpi.ua/server/api/core/bitstreams/057779d8-d88f-4cef-b2d5-67086a013516/content* *6. Моделювання бізнес-процесів та управління ІТ-проектами : навч. посібн. / Є. М. Крижановський, А. Р. Ящолт, С. О. Жуков, О. М. Козачко, 2018. Вінниця: ВНТУ. 91 с. URL: https://ecopy.posibnyky.vntu.edu.ua/txt/2018/Kryzanovsk_yascholt_modelyuvanna_np_p024.pdf* *7. Перит І. О. Перспективи впровадження Kanban в управління бізнесом вітчизняних суб'єктів господарювання. Бізнес Інформ, 2019. № 8. С. 218-228. URL: http://www.irbis-nbuv.gov.ua/cgi-bin/irbis_nbuv/cgiirbis_64.exe?I21DBN=LINK&P21DBN=UJRN&Z21ID=&S21REF=10&S21CNR=20&S21STN=1&S21FMT=ASP_meta&C21COM=S&2_S21P03=FILA=&2_S21STR=binf_2019_8_31*
Основи наукових досліджень	навчальна дисципліна	*НП 1_Магістр_1.9_Основи наукових досліджень_Євсеєв.pdf*	jI3hoSu58skVyo3gmF6G3osILGQ/lQQQ7LzPcFtXOOc=	*Обладнання:* *Мультимедійні аудиторії, ПК з доступом до Інтернету* *ПЗ: Packet Tracer 9.0* *Література:* *1. Мазур О.В. Основи наукових досліджень : навч. посіб. Для студ. вищих навч. заклад. філол. спец. /О. В. Мазур, О.В. Подвойська, С. В. Радецька. – Вінниця : Нова Книга, 2013. – 120с.https://www.google.com.ua/books/edition/_/jl3XCQAAQBAJ?hl=ru&gbpv=1&pg=PP1&dq=inauthor:%22%D0%9C%D0%B0%D0%B7%D1%83%D1%80+%D0%9E.+%D0%92.+%D1%82%D0%B0+%D1%96%D0%BD.%22* *2. Данильян О. Г. Методологія наукових досліджень : підручник / О. Г. Данильян, О. П. Дзьобань. – Харків : Право, 2019. – 368 с. https://library.nlu.edu.ua/POLN_TEXT/SENMK/OMND.pdf*

				3. Методологія та організація наукових досліджень : навч. посіб. / І. С. Добронравова, О. В. Руденко, Л. І. Сидоренко та ін. ; за ред. І. С. Добронравової (ч. 1), О. В. Руденко (ч. 2). – К. : ВПЦ "Київський університет", 2018. – 607 с. http://www.philsci.univ.kiev.ua/biblio/Methodol.pdf *4. Synergy of building cybersecurity systems: monograph / S. Yevseiev, V. Ponomarenko, O. Laptiev, O. Milov and others. – Kharkiv: PC TECHNOLOGY CENTER, 2021. – 188 p. https://drive.google.com/drive/u/1/folders/1wOTN8N-GBGO06AnvjQHU1SdBl3xCaUju* *5. Models of socio-cyber-physical systems security: monograph / S. Yevseiev, Yu. Khokhlachova, S. Ostapov, O. Laptiev and others. – Kharkiv: PC TECHNOLOGY CENTER, 2023. – 168 p. https://drive.google.com/drive/u/1/folders/1wOTN8N-GBGO06AnvjQHU1SdBl3xCaUju* *6. Modeling of security systems for critical infrastructure facilities: monograph / S. Yevseiev, R. Hryshchuk, K. Molodetska, M. Nazarkevych and others. – Kharkiv: PC TECHNOLOGY CENTER, 2022. – 196 p. https://drive.google.com/drive/u/1/folders/1wOTN8N-GBGO06AnvjQHU1SdBl3xCaUju*
Науково – дослідницька практика	практика	*ПП 1_Магістр_1.9_Науково-дослідницька практика_Гаврилова.pdf*	sIS3AJAwdHaqJhNYVbuGwSNaHz+v7mtboonPc9qvVNo=	*Обладнання:* *Кіберполігон* *Персональний комп'ютер 2E Integer Intel i5-11400/H510/16/480F/int/FreeDos/2E-S616/400W- 25 шт.* *Монітор HP P24 G5 FHD Monitor – 25 шт.* *Гарнітура для ПК 2E CH11, On-Ear, 3.5mm/2*3.5mm – 25 шт.* *Комплект 2E MK410 WL Black – 25 шт.* *Міжмережевий екран Fortinet FG-40F 5*GE RJ45 ports (including 4* internal Ports 1* WAN Ports – 1 шт.* *Ноутбук/Notebook Del Vostro 3510/Core i3-1115G4/8GB/256GB SSD/15.6`` FHD/Intel UHD/Cam& Mic/WLAN + BT/Backlit Kb/3 Cell/W11Pro/3Yr – 2 шт.* *Багатофункціональний пристрій А4 ч/б Multifuntional device A4 b/w Xerox B235 (WI-FI) – 1 шт.* *Проєктор короткофокусний Epson EB-536Wi WXGA, 3400 lm, 0.65 інтерактивний – 1 шт.* *Проектор/ Projector Epson EB-X49 (3LCD, XGA,3600 ANSI lm) – 1 шт.* *Екран 2E на тринозі,1:1, 112, (2.0*2.0) – 1 шт.* *Сервер IBM BladeCenter /BladeCenter-H shassis, HS23 (Type 7875), HS22 (Type 7870) - 1 шт.* *Сервер R- LINE на базі Xeon Silver 421 OR – 1 шт.* *Точка доступу Ubiguiti UniFi 6 LR Access Point U6-LR – 1 шт.* *Маршрутизатор Mikro Tik RB4011iGS+5HacQ2HnD-IN – 1 шт.*

				Комутатор D-Link DGS-1210-28X/ME – 1 шт. *Сервер HPE ML350 Gen10 Hot Plug LFF CTO – 1 шт.* *ДБЖ HPE T1000 Gen5 INTL UPS with Management Card Slot – 1шт.* *Комутатор Aruba 6000 48G 4SFP Switch – 1 шт.* *Aruba 1G SFP LC LX 10km SMF Transceiver – 2 шт.* *Aruba 1G SFP RJ45T 100m Cat5e Transceiver – 2 шт.* *Кількість переданих ліцензій на програмне забезпечення – 110* *Примірник ПЗ Microsoft Windows 11 Pro укр. OEM на DVD носії – 25 шт.* *Примірник ПЗ Microsoft Visio Professional SLng LSA OLV NL 1Y Aq Y1 Acad AP – 27 шт.* *Примірник ПЗ Microsoft Visual Studio Test Pro MSDN ALng LSAvOLV NL 1Y Aq Y1 Acad AP – 25 шт.* *Програмний продукт Microsoft Visual Studio Professional 2022– 27 шт.* *Програмний продукт Microsoft Skype for Business Server Plus 2019 User CAL – 2 шт.* *Програмний продукт Microsoft Windows Server 2022 Standard – 2 Core License Pack – 1 шт.* *Примірник ПЗ Microsoft Azure DevOps Server SLng LSA OLV NL 1Y Aq Y1 Acad AP – 1 шт.* *Примірник ПЗ Microsoft SQL Server Enterprise Core SLng LSA OLV 2L NL 1Y Aq Y1 Acad AP – 1 шт.* *Примірник ПЗ Microsoft Win Server Essentials SLng LSA OLV NL 1Y Aq Y1 Acad AP – 1 шт.* *Література:* *1. Інформаційна безпека. Менеджмент інформаційної безпеки держави [Електронний ресурс]: курс лекцій: навч. посіб. для здобувачів ступеня магістра за освітніми програми Комп'ютерні системи і технології спеціального зв'язку та Спеціальні системи електронних комунікацій спец. 122 Комп'ютерні науки 172 Електронні комунікації та радіотехніка / В. О. Ананьїн, В. В. Горлинський, А. В. Гангал. ІСЗЗІ КПІ ім. Ігоря Сікорського. – Електронні текстові дані (1 файл: 2,73 Мбайт). – Київ : ІСЗЗІ КПІ ім. Ігоря Сікорського 2025. – 140 с. https://ela.kpi.ua/server/api/core/bitstreams/c4ad5148-9e04-4979-9ef7-0fec3a385650/content* *2. Чунарьова А., Чунарьов А. Система управління інформаційною безпекоюна базі міжнародних стандартів серії ISO. Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні, 2(24) вип., 2012 р. С. 48 - 52.* *3. Бурячок В. Л. Основи інформаційної та кібернетичної безпеки. [Навчальний посібник]. / В. Л. Бурячок , Р. В. Киричок, П. М. Складанний – К. , 2018. – 320 с. https://elibrary.kubg.edu.ua/id/epr*

				int/27370/1/V_Buriachok_Posibnik_2019_FITU.pdf 4. Григор'єв В. І. Інформаційні загрози в державному управлінні // Наукові записки Львів. ун-ту бізнесу та права. 2013. Вип. 11. С. 93. URL: http://irbis-nbuv.gov.ua/UJRN/Nzlubp_2013_11_26 5. Терещенко, Л. (2021). Управління ризиками інформаційних систем: етапи процесу управління ризиками. Економіка та суспільство, (31). https://doi.org/10.32782/2524-0072/2021-31-12 6. Кіберризики критичної інфраструктури: від аналізу загроз до впровадження рішень [Текст] : наук.- практ. посіб. / Олександр Довгань, Тарас Ткачук ; Держ. наук. установа "Ін-т інформації, безпеки і права Нац. акад. прав. наук України". - Київ ; Одеса : Фенікс, 2024. - 70 с. URL: https://irbis-nbuv.gov.ua/cgi-bin/irbis_nbuv/cgiirbis_64.exe?C21COM=S&I21DBN=EC&P21DBN=EC&S21FMT=JwU_B&S21ALL=%28%3C.%3EI%3D%21NBUV$%3C.%3E%29%2A%28%3C.%3EU%3D%D0%A5849%284%D0%A3%D0%9A%D0%A0%2904:%D0%9797%3C.%3E%29&Z21ID=&S21SRW=TIPVID&S21SRD=DOWN&S21STN=1&S21REF=10&S21CNR=20 7. Кібербезпека та кіберзахист: питання порядку денного в українському суспільстві [Електронний ресурс] / З. Свердлик // Український журнал з бібліотекознавства та інформаційних наук. - 2022. - Вип. 10. - С. 175-188. - URL: http://nbuv.gov.ua/UJRN/ujlis_2022_10_17 8. Дорошенко А. Захист персональних даних у сфері Data Science: імплементація GDPR в Україні [Текст] : [монографія] ; "Erasmus+" Programme of the European Union ; [Нац. ун-т "Львів. політехніка"]. Львів : Вид-во Тараса Сороки, 2022. С. 80-88. URL:https://irbis-nbuv.gov.ua/cgi-bin/irbis_nbuv/cgiirbis_64.exe?C21COM=S&I21DBN=EC&P21DBN=EC&S21FMT=JwU_B&S21ALL=%28%3C.%3EI%3D%21NBUV$%3C.%3E%29%2A%28%3C.%3EU%3D%D0%A5849%284%D0%A3%D0%9A%D0%A0%2904:%D0%9797%3C.%3E%29&Z21ID=&S21SRW=TIPVID&S21SRD=DOWN&S21STN=1&S21REF=10&S21CNR=20 9. ДСТУ ISO/IEC 27001:2015. Інформаційні технології. Методи та засоби убезпечення. Системи управління інформаційною безпекою. Вимоги. Київ : Держстандарт України, 2015. 48 с. URL:https://www.assistem.kiev.ua/doc/dstu_ISO-IEC_27001_2015.pdf 10. Загальний регламент про захист даних (GDPR) : Регламент (ЄС) 2016/679 Європейського Парламенту та Ради від 27 квітня 2016 р. – URL: https://eur-lex.europa.eu/legal-

				content/EN/TXT/?uri=CELEX%3A32016R0679 (дата звернення: 13.07.2025). *11. Закон України "Про основні засади забезпечення кібербезпеки України" від 05.10.2017 № 2163-VIII. Відомості Верховної Ради України. 2017. № 45. С. 138–150. URL: https://zakon.rada.gov.ua/laws/main/2163-19#Text* *12. Закон України "Про захист інформації в інформаційно-телекомунікаційних системах": [Електронний ресурс]. URL: https://zakon.rada.gov.ua/laws/show/80/94-вр (дата звернення: 18.08.2025).* *13. Закон України "Про захист персональних даних" від 01.06.2010 № 2297-VI. URL: https://zakon.rada.gov.ua/laws/show/2297-17 (дата звернення: 13.07.2025).* *14. Зубенко С. В., Ракша О. В. Мережева безпека : навч. посіб. Київ: ІТНВУ, 2019. 256 с. URL: https://elartu.tntu.edu.ua/bitstream/lib/42625/1/%D0%9A%D0%91%D0%86%D0%9C%D0%A1_%28%D0%BF%D0%BE%D1%81%D1%96%D0%B1%D0%BD%D0%B8%D0%BA%29.pdf* *15. Ігнатенко Р. С. Захист вебдодатків від DDoS-атак: сучасні підходи. Наукові праці Інституту кібербезпеки. 2023. Вип. 1 (45). С. 112-120. https://dspace.onua.edu.ua/server/api/core/bitstreams/cf6c1f9c-b1d7-4c35-9b35-2e8901b23fdd/content* *16. Кіберзахист в умовах гібридної війни: монографія. / за заг. ред. О. В. Довгаля. Харків : ТОВ "Видавництво "Нове слово", 2021. 288 с. https://dnuvs.ukr.education/wp-content/uploads/2025/06/zbirnyk_materialiv_17_kvitnya_2025_compressed.pdf* *17. Когут О. В. Міжнародна кібербезпека: виклики та співпраця : навч. посіб. Львів : ЛНУ ім. І. Франка, 2021. 250 с. https://nashformat.ua/pdf-preview/kiberbezpeka-ta-ryzyky-tsyfrovoi-transformatsii-kompanij-928039?srsltid=AfmBOooeyaQ8Rvb_BP4tDNenSGt8YafubMbe5FXGCCJgljORK3kdewOk* *18. Козаченко Ю. М., Мельник О. М. Застосування машинного навчання для виявлення аномалій у мережевому трафіку. Вісник кібербезпеки. 2023. № 2. С. 45–56. URL: https://indico.ldubgd.edu.ua/event/55/attachments/662/975/%D0%97%D0%B1%D1%96%D1%80%D0%BD%D0%B8%D0%BA%20%D0%BD%D0%B0%D1%83%D0%BA%D0%BE%D0%B2%D0%B8%D1%85%20%D0%BF%D1%80%D0%B0%D1%86%D1%8C%20%D0%BA%D0%BE%D0%BD%D1%84.%20%D0%86%D0%91%D0%86%D0%A2_2024%20%E2%80%93%20%D0%B7%20%D0%BE%D0%B1%D0%BA%D0%BB%D0%B0%D0%B4%D0%B8%D0%BD%D0%BA%D0%BE%D1%8E.pdf*

19. Кривогуз І. М. Криптографічні методи захисту інформації. Львів : Видавництво Львівської політехніки, 2019. 250 с. https://vaodesa.mil.gov.ua/wp-content/uploads/2024/10/Zbirnyk-tez-dop.-Nats.-bezpeka-Ukrainy-aktualny-problemy-ta-shliakhy-ikh-vyrishennia-1.pdf
20. Ліщук В. В. Аналіз сучасних кіберзагроз в умовах гібридної війни. Інформаційна безпека. 2024. Т. 1, № 1. С. 110–125. https://hups.mil.gov.ua/assets/doc/science/conference/20/xx-conf-hnups_01.pdf
21. Павленко О. В. Аналіз сучасних методів кіберрозвідки та протидія цілеспрямованим атакам. Проблеми кібербезпеки. 2024. № 1 (25). С. 45-53. https://archer.chnu.edu.ua/bitstream/handle/123456789/12135/%D0%BA%D0%BE%D0%BD%D1%84%D0%B5%D1%80%D0%B5%D0%BD%D1%86%D1%96%D1%8F%202024%20%D0%A8%D1%82%D1%83%D1%82%D0%B3%D0%B0%D1%80%D1%82.pdf?sequence=1&isAllowed=y
22. Сілін Є.С., Кадубовський О.А. Основи кібербезпеки : навчальний посібник [електронний ресурс]. Дніпро, 2023. – 200 с.URL: https://ddpu.edu.ua/fmk/publications/manuals/manual_18.pdf
23. Потопальський В. В., Лисенко О. А., Семенов І. Г. Захист інформації: криптографічні методи. Київ : Центр навчальної літератури, 2022. 356 с. https://kingu.edu.ua/wp-content/uploads/2024/07/%D0%97%D0%91%D0%86%D0%A0%D0%9D%D0%98%D0%9A-%D1%82%D0%B5%D0%B7-%D0%B4%D0%BE%D0%BF%D0%BE%D0%B2%D1%96%D0%B4%D0%B5%D0%B9-%D0%9D%D0%9F%D0%9A-%D0%A4%D0%A1%D0%91%D0%94-%D0%9D%D0%93%D0%A3.pdf
24. Скляров В. А. Безпека програмного забезпечення та даних : навч. посіб. Харків : Ранок, 2023. 360 с.
25. Адамов О. С. Моделі і методи захисту кіберпростору на основі аналізу великих даних з використанням машинного навчання [Текст] : автореф. дис. ... канд. техн. наук : 05.13.05 /; Харк. нац. ун-т радіоел. Харків, 2019. 31 с. : рис., табл. URL: https://openarchive.nure.ua/server/api/core/bitstreams/529a9e7c-069c-4bd3-99ea-7398e7a33fef/content
26. Щеголенкова Н. М. Аудит інформаційної безпеки: навч. посіб. Львів: Магнолія Плюс, 2022. 280 с. URL: https://www.google.com/aclk?sa=L&pf=1&ai=DChsSEwjqzrft2bCPAxUrCqIDHbEjPIwYACICCAEQABoCbGU&co=1&ase=2&gclid=EAIaIQobChMI6s637dmwjwMVKwqiAx2xIzyMEAAYASAAEgI5ofD_BwE&cid=CAASJeRo3OkjayRwsRDY_jpGtCfajHPsEogvNn3awsbidorNbK9lv8k&ce=2&category=acrcp_v1_32&sig=AOD64_1uxFNtInYWktpiHObyogU

gj-DKAg&q&nis=4&adurl=https://xray-sec.com/ua/?utm_source%3Dgoogle%26utm_medium%3Dcpc%26utm_campaign%3Dsearch-ua-ukr%26utm_term%3Daudit-ib%26gad_source%3D1%26gad_campaignid%3D21032544132%26gbraid%3D0AAAAAqc6yf5THnodBnvDeIZ2_FWNWLB4U%26gclid%3DEAIaIQobChMI6s637dmwjwMVKwqiAx2xIzyMEAAYASAAEgI5ofD_BwE&ved=2ahUKEwjXmLDt2bCPAxW5QVUIHXpFAIoQoQx6BAgYEAE

27. Кузьменко О., Маклюк О., Чернишова О. Кібербезпека бізнесу під час війни. Економіка та суспільство. 2022. Вип. 44. DOI: https://doi.org/10.32782/2524-0072/2022-44-21.
28. CERT-UA. Річний звіт про кіберінциденти у 2023 році. Державний центр кіберзахисту CERT-UA. 2024. URL: https://cert.gov.ua/article/11223 (дата звернення: 17.08.2025).
29. CERT-UA. Звіт про кіберінциденти та кібератаки на об'єкти критичної інфраструктури України. Державний центр кіберзахисту CERT-UA. 2024. URL: https://cert.gov.ua/report (дата звернення: 18.08.2025).
30. ENISA Threat Landscape Report 2023. European Union Agency for Cybersecurity (ENISA). 2023. URL: https://www.enisa.europa.eu/publications/enisa-threat-landscape-2023 (дата звернення: 18.08.2025).
31. ISO/IEC 27001:2022. Information security, cybersecurity and privacy protection. Information security management systems. URL: https://www.iso.org/standard/82875.html (access on: 18.08.2025).
32. Kaspersky Security Bulletin. Statistics 2024. Kaspersky. 2024. URL: https://www.kaspersky.com/about/security-bulletin (access on: 18.08.2025).
33. Microsoft. Digital Defense Report 2024. URL: https://www.microsoft.com/en-us/security/business/reports/digital-defense-report-2024 (acces on: 17.08.2025).
34. Modeling of security systems for critical infrastructure facilities [Text] : monograph / [R. Korolev et al.] ; ed. by Serhii Yevseiev [et al.]. Kharkiv : PC Technology Center, 2022. XIV, P. 169-181. https://doi.org/10.15587/978-617-7319-57-2
35. NIST Cybersecurity Framework (National Institute of Standards and Technology Cybersecurity Framework). URL: https://www.nist.gov/cyberframework (acces on: 13.07.2025).
36. Simpson Michael T., Antill Nicholas, Backman Kent. Hands-On

				Ethical Hacking and Network Defense. Boston: Cengage Learning, 2022. 720 p. URL: https://books.google.com.ua/books/about/Hands_On_Ethical_Hacking_and_Network_Def.html?id=S1RbzgEACAAJ&redir_esc=y
Мережева та хмарна безпека	навчальна дисципліна	*СП 1_Магістр_1.9_Мережева та хмарна безпека.pdf*	orf9Xu/xXITemklCt45H86xoErIp+xoSG7Hwi4SgFzw=	*Обладнання: Мультимедійні аудиторії ПК: Intel Pentium G4560/ОЗУ 4 GB DDR3-1600/Монітор 20" Dell P2017H/HDD 500 GB, 7200 об/хв, SATA 3.0 – 15шт. Packet Tracer 9.0 Література: 1. Безпека хмарного середовища [Електронний ресурс]. – Режим доступу : https://www.netacad.com/ru/courses/cybersecurity/cloud-security. 2. Amazon Web Services (AWS) [Електронний ресурс]. – Режим доступу : https://www.checkpoint.com/solutions/amazon-aws-security/. 3. Microsoft Azure (Azure) [Електронний ресурс]. – Режим доступу : https://www.checkpoint.com/solutions/microsoft-azure-security/. 4. Google Cloud Platform (GCP) [Електронний ресурс]. – Режим доступу : https://www.checkpoint.com/solutions/google-cloud-platform-security/. 5. Kali Linux [Електронний ресурс]. – Режим доступу : https://www.kali.org/*
Цифрова криміналістика	навчальна дисципліна	*СП 3_Магістр_1.9_Цифрова криміналістика.pdf*	/reo+iOvxSOwLbxMTFypPYX7pqh3NOdhdOMXLkASZHI=	*Обладнання: Мультимедійні аудиторії ПК: Intel Pentium G4560/ОЗУ 4 GB DDR3-1600/Монітор 20" Dell P2017H/HDD 500 GB, 7200 об/хв, SATA 3.0 – 15шт. QlikView, QlikSense, Microsoft Power BI Література: 1. Davidoff, Sherri. Network forensics: tracking hackers through cyberspace / Sherri Davidoff, Jonathan Ham. Pearson Education, Inc. 2012. https://ptgmedia.pearsoncmg.com/images/9780132564717/samplepages/0132564718.pdf 2 Євсеєв С.П. КІБЕРБЕЗПЕКА: ЛАБОРАТОРНИЙ ПРАКТИКУМ З ОСНОВ КРИПОГРАФІЧНОГО ЗАХИСТУ / С.П. Євсеєв, О.В. Мілов, О.Г. Король – Львів: «Новий Світ- 2000», 2020 . – 241 с. http://library.hneu.edu.ua/storage/new-arrivals-books/December2020/Yevseiev.pdf*
Математичні моделі управління ІТ проєктами	навчальна дисципліна	*СП 6_Магістр_1.9_Математичні_моделі_управління_ІТ_проєктами_Мілевський.pdf*	P/v/DRoARbo8txi1KLWPobS4t/VMfFWyOoPlC5rX1t4=	*Обладнання: Мультимедійні аудиторії ПК: Intel Pentium G4560/ОЗУ 4 GB DDR3-1600/Монітор 20" Dell P2017H/HDD 500 GB, 7200 об/хв, SATA 3.0 – 15шт. Packet Tracer 9.0 Література: 1. Kerzner, Harold. Project Management: A Systems Approach to Planning, Scheduling, and*

				Controlling. Wiley, 2017. URL: https://books.google.com.ua/books/about/Project_Management.html?id=xlASDgAAQBAJ&redir_esc=y *2. Meredith, Jack R., and Samuel J. Mantel. Project Management: A Managerial Approach. Wiley, 2018. URL: https://books.google.com.ua/books/about/Project_Management.html?id=xGRtQetWjNsC&redir_esc=y* *3. Verzuh, Eric. The Fast Forward MBA in Project Management. Wiley, 2015. URL: https://books.google.com.ua/books/about/The_Fast_Forward_MBA_in_Project_Manageme.html?id=AgCJjwEACAAJ&redir_esc=y*
Етичний хакінг	навчальна дисципліна	*СП 4_Магістр_1.9_Етичний хакінг.pdf*	TxftejlLWaJWQmdbTWEYKKFokJqs8U/hqgtpbJ+oIco=	*Обладнання:* *Кіберполігон* *Персональний комп'ютер 2E Integer Intel i5-11400/H510/16/480F/int/FreeDos/2E-S616/400W- 25 шт.* *Монітор HP P24 G5 FHD Monitor – 25 шт.* *Гарнітура для ПК 2E CH11, On-Ear, 3.5mm/2*3.5mm – 25 шт.* *Комплект 2E MK410 WL Black – 25 шт.* *Міжмережевий екран Fortinet FG-40F 5*GE RJ45 ports (including 4* internal Ports 1* WAN Ports – 1 шт.* *Ноутбук/Notebook Del Vostro 3510/Core i3-1115G4/8GB/256GB SSD/15.6`` FHD/Intel UHD/Cam&Mic/WLAN + BT/Backlit Kb/3Cell/W11Pro/3Yr – 2 шт.* *Багатофункціональний пристрій A4 ч/б Multifuntional device A4 b/w Xerox B235 (WI-FI) – 1 шт.* *Проєктор короткофокусний Epson EB-536Wi WXGA, 3400 lm, 0.65 інтерактивний – 1 шт.* *Проектор/ Projector Epson EB-X49 (3LCD, XGA,3600 ANSI lm) – 1 шт.* *Екран 2E на тринозі,1:1, 112, (2.0*2.0) – 1 шт.* *Сервер IBM BladeCenter /BladeCenter-H shassis, HS23 (Type 7875), HS22 (Type 7870) - 1 шт.* *Сервер R- LINE на базі Xeon Silver 421 OR – 1 шт.* *Точка доступу Ubiguiti UniFi 6 LR Access Point U6-LR – 1 шт.* *Маршрутизатор Mikro Tik RB4011iGS+5HacQ2HnD-IN – 1 шт.* *Комутатор D-Link DGS-1210-28X/ME – 1 шт.* *Сервер HPE ML350 Gen10 Hot Plug LFF CTO – 1 шт.* *ДБЖ HPE T1000 Gen5 INTL UPS with Management Card Slot – 1шт.* *Комутатор Aruba 6000 48G 4SFP Switch – 1 шт.* *Aruba 1G SFP LC LX 10km SMF Transceiver – 2 шт.* *Aruba 1G SFP RJ45T 100m Cat5e Transceiver – 2 шт.* *Кількість переданих ліцензій на програмне забезпечення – 110* *Примірник ПЗ Microsoft Windows 11 Pro укр. OEM на DVD носії – 25 шт.* *Примірник ПЗ Microsoft Visio Professional SLng LSA OLV NL 1Y Aq Y1 Acad AP – 27 шт.* *Примірник ПЗ Microsoft Visual*

				Studio Test Pro MSDN ALng LSAvOLV NL 1Y Aq Y1 Acad AP – 25 шт. *Програмний продукт Microsoft Visual Studio Professional 2022– 27 шт.* *Програмний продукт Microsoft Skype for Business Server Plus 2019 User CAL – 2 шт.* *Програмний продукт Microsoft Windows Server 2022 Standard – 2 Core License Pack – 1 шт.* *Примірник П3 Microsoft Azure DevOps Server SLng LSA OLV NL 1Y Aq Y1 Acad AP – 1 шт.* *Примірник П3 Microsoft SQL Server Enterprise Core SLng LSA OLV 2L NL 1Y Aq Y1 Acad AP – 1 шт.* *Примірник П3 Microsoft Win Server Essentials SLng LSA OLV NL 1Y Aq Y1 Acad AP – 1 шт.* *Література:* *1. Oriyano Sean-Philip. Penetration Testing Essentials. Sybex, a Wiley brand, 2017, 363 p. 2. Baloch Rafay. Ethical hacking and penetration testing guide. Auerbach Publications, 2017, 523 p. https://www.tsoungui.fr/ebooks/Ethickal-haking-postexploitation.pdf* *2. Євсеєв С.П. Кібербезпека: Лабораторний практикум з основ криптографічного захисту. – Львів "Новий світ-2000", 2020. – 241 с. https://drive.google.com/drive/u/1/folders/1wOTN8N-GBGO06AnvjQHU1SdBl3xCaUju* *3. Бобало Ю.Я., Горбатий І.В. (ред.) Інформаційна безпека. Навчальний посібник. — Львів : Видавництво Львівської політехніки, 2019. — 580 с. — ISBN 978-966-941-339-0. https://pdf.lib.vntu.edu.ua/books/2021/Bobalo_2019_580.pdf.* *4. Етичний хакінг : навчально-практичний посібник / уклад. О. В. Мілов, О. В. Шматко, С. В. Мілевський, О. Г. Король ; за заг. ред. С. П. Євсеєва. – Харків : НТУ «ХПІ», – Львів : «Новий Світ-2000», 2025. – 100 с. – (Серія «Кібербезпека та штучний інтелект»). https://drive.google.com/file/d/1AHYbnhItLvuyRnjZzVqmXskkXZ6KSjRJ/view?usp=sharing*
Виявлення вторгнень у компьютерні мережі (мережеві аномалії)	навчальна дисципліна	*НП 6_Магістр_1.9_Виявлення_вторгнень_у_комп'ютерні_мережі_мережеві_1.9_Мілов.pdf*	rQpzJXnHVR/Vr4d/VBUXX/RtL6aFMeYsgJ44V4JZokI=	*Обладнання:* *Кіберполігон:* *Персональний комп'ютер 2E Integer Intel i5-11400/H510/16/480F/int/FreeDos/2E-S616/400W- 25 шт.* *Монітор HP P24 G5 FHD Monitor – 25 шт.* *Гарнітура для ПК 2E CH11, On-Ear, 3.5mm/2*3.5mm – 25 шт.* *Комплект 2E MK410 WL Black – 25 шт.* *Міжмережевий екран Fortinet FG-40F 5*GE RJ45 ports (including 4* internal Ports 1* WAN Ports – 1 шт.* *Ноутбук/Notebook Del Vostro 3510/Core i3-1115G4/8GB/256GB SSD/15.6`` FHD/Intel UHD/Cam&Mic/WLAN + BT/Backlit Kb/3 Cell/W11Pro/3Yr – 2 шт.*

				Багатофункціональний пристрій А4 ч/б Multifuntional device A4 b/w Xerox B235 (WI-FI) – 1 шт. *Проєктор короткофокусний Epson EB-536Wi WXGA, 3400 lm, 0.65 інтерактивний – 1 шт.* *Проектор/ Projector Epson EB-X49 (3LCD, XGA,3600 ANSI lm) – 1 шт.* *Екран 2E на тринозі,1:1, 112, (2.0*2.0) – 1 шт.* *Сервер IBM BladeCenter /BladeCenter-H shassis, HS23 (Type 7875), HS22 (Type 7870) - 1 шт.* *Сервер R- LINE на базі Xeon Silver 421 OR – 1 шт.* *Точка доступу Ubiguiti UniFi 6 LR Access Point U6-LR – 1 шт.* *Маршрутизатор Mikro Tik RB4011iGS+5HacQ2HnD-IN – 1 шт.* *Комутатор D-Link DGS-1210-28X/ME – 1 шт.* *Сервер HPE ML350 Gen10 Hot Plug LFF CTO – 1 шт.* *ДБЖ HPE T1000 Gen5 INTL UPS with Management Card Slot – 1шт.* *Комутатор Aruba 6000 48G 4SFP Switch – 1 шт.* *Aruba 1G SFP LC LX 10km SMF Transceiver – 2 шт.* *Aruba 1G SFP RJ45T 100m Cat5e Transceiver – 2 шт.* *Кількість переданих ліцензій на програмне забезпечення – 110* *Примірник ПЗ Microsoft Windows 11 Pro укр. OEM на DVD носії – 25 шт.* *Примірник ПЗ Microsoft Visio Professional SLng LSA OLV NL 1Y Aq Y1 Acad AP – 27 шт.* *Примірник ПЗ Microsoft Visual Studio Test Pro MSDN ALng LSAvOLV NL 1Y Aq Y1 Acad AP – 25 шт.* *Програмний продукт Microsoft Visual Studio Professional 2022– 27 шт.* *Програмний продукт Microsoft Skype for Business Server Plus 2019 User CAL – 2 шт.* *Програмний продукт Microsoft Windows Server 2022 Standard – 2 Core License Pack – 1 шт.* *Примірник ПЗ Microsoft Azure DevOps Server SLng LSA OLV NL 1Y Aq Y1 Acad AP – 1 шт.* *Примірник ПЗ Microsoft SQL Server Enterprise Core SLng LSA OLV 2L NL 1Y Aq Y1 Acad AP – 1 шт.* *Примірник ПЗ Microsoft Win Server Essentials SLng LSA OLV NL 1Y Aq Y1 Acad AP – 1 шт.* *Література:* *1. Cybersecurity Fundamentals/ ISACA/ www/isaca/org/cyber? Cybersecurity Fundamentals Study Guide/ 2003.- 156 p.* *2. Sankar R. Burpsuite – A Beginner's Guide For Web Application Security or Penetration Testing [Електронний ресурс] / Ravi Sankar. – 2018. – Режим доступу до ресурсу: https://kalilinuxtutorials.com/burp suite/.* *3. Ganore P. What Is A Web Server And How Does It Function? [Електронний ресурс] / Pravin*

				Ganore. – 2017. – Режим доступу до ресурсу: https://www.milesweb.com/blog/hosting/web-server-function/. *4. How a Web server functions? [Електронний ресурс]. – 2006. – Режим доступу до ресурсу: https://www.eukhost.com/blog/webhosting/how-aweb-server-functions/.* *5. Державна служба спеціального зв'язку та захисту інформації України. www.dsszzi.gov.ua* *6. Learn Ethical Hacking from Scratch: Your Stepping Stone to Penetration Testing* *7. Mastering Modern Web Penetration Testing Prakhar Prasad* *8. Common Vulnerability Scoring System Calculator Version 3/ https://nvd.nist.gov/vuln-metrics/cvss/v3-calculator*
Безпека та анонімність роботи в інтернеті	навчальна дисципліна	*СП 2_Магістр_1.9_Безпека та анонімність роботи в Інтернеті_Гаврилова.pdf*	wGJBhiOQAy8KfMSISxVJFIc+SKgzkXM7Ah10Sd4bNCA=	*Обладнання:* *Мультимедійні аудиторії* *ПК: Intel Pentium G4560/ОЗУ 4 GB DDR3-1600/Монітор 20" Dell P2017H/HDD 500 GB, 7200 об/хв, SATA 3.0 – 15шт.* *QlikView, QlikSense, Microsoft Power BI* *Література:* *1. Виховання культури користувача Інтернету. Безпека у всесвітній мережі: навчально-методичний посібник / А. Кочарян, Н. Гущина. – К., 2011. – 100 с. URL: https://elibrary.kubg.edu.ua/id/eprint/1547/1/Internet.pdf* *2. Сухорольський П. М. Право на анонімність як суттєвий елемент прав людини // "Правова інформатика", № 1(37). 2013. С. 39 – 48. URL: https://ippi.org.ua/sites/default/files/13sptmepl.pdf* *3. Pariser E. The Filter Bubble: What the Internet Is Hiding from You. – New York : The Penguin Press, 2011. – 203 p. URL: https://books.google.com.ua/books?id=-FWOoрuw3nYC&printsec=frontcover&hl=ru&source=gbs_ge_summary_r&cad=0#v=onepage&q&f=false* *4. Безпечне користування сучасними інформаційно-комунікативними технологіями / О. Удалова, О. Швед, О. Кузнєцова [та ін.]. – К.: Україна, 2010. – 72 с. URL: https://rescentre.org.ua/images/Uploads/Files/internet_safety_dl/bezpechne_koristuvannya_ikt.pdf* *5. Model Inter-American Law on Access to Public Information. – Organization of American States. – Режим доступу : http://www.oas.org/dil/AG-RES_2607-2010_eng.pdf.*
Атестація	підсумкова атестація	*СП_Атестація_125_Магістр_1.9_(Публічний захист кваліфікаційної роботи).pdf*	iBkW4IgdhEGIUxZi5Org1Six6mQrWDjFyxShpRNPV7A=	*Обладнання:* *Мультимедійні аудиторії* *ПК: Intel Pentium G4560/ОЗУ 4 GB DDR3-1600/Монітор 20" Dell P2017H/HDD 500 GB, 7200 об/хв, SATA 3.0 – 15шт.* *Packet Tracer 9.0* *Література:* *1. Методичні вказівки до*

				виконання магістерських робіт для студентів спеціальності 125 "Кібербезпека та захист інформації" / уклад. О. В. Мілов, О. Г. Король, Н. І. Воропай. – Харків: НТУ "ХПІ". – 51 с. URL: https://repository.kpi.kharkov.ua/server/api/core/bitstreams/e02b0d47-b1f7-4417-8f45-2fb38e98ad7c/content *2. Про вищу освіту: Закон України (Відомості Верховної Ради (ВВР), 2014, № 37-38, ст.2004). URL: https://zakon.rada.gov.ua/laws/show/1556-18#Text* *3. Про освіту: Закон України (Відомості Верховної Ради (ВВР), 2017, № 38-39, ст.380). URL: https://zakon.rada.gov.ua/laws/show/2145-19#Text* *4. СТЗВО – ХПІ – 2.01-2021 ССОНП. Дипломні проекти та дипломні роботи. Загальні вимоги до виконання (зі змінами) URL: https://blogs.kpi.kharkov.ua/v2/metodotdel/wp-content/uploads/sites/28/2022/12/STZVO-HPI-2.01-2021-SSONP.-Diplomni-proekti-ta-diplomni-roboti.-Zagalni-vimogi-do-vikonannya-zi-zminami.pdf* *5. СТЗВО-ХПІ-3.01-2021 ССОНП. Текстові документи у сфері навчального процесу. Загальні вимоги до виконання (зі змінами) URL: https://blogs.kpi.kharkov.ua/v2/metodotdel/wp-content/uploads/sites/28/2022/12/STZVO-HPI-3.01-2021-SSONP.-Tekstovi-dokumenti-u-sferi-navchalnogo-protsesu.-Zagalni-vimogi-do-vikonannya-zi-zminami.pdf*
Англійська мова в академічних застосунках	навчальна дисципліна	*ЗП 1_Магістр_1.9_Англійська мова в академічних застосунках.pdf*	CN8+3zb+cY2BKfjcr9J4OBoKsNoevU1Y8KydMn2rCeQ=	*Обладнання:* *Мультимедійні аудиторії, ПК з доступом до Інтернету* *Література:* *1. Словник термінів із кібербезпеки / За заг. ред. О. В. Копана, Є. Д. Скулиша - К.: ВБ «Аванпост-Прим», 2012.-214 с. [Електронний ресурс].- Режим доступу: https://www.nas.gov.ua/siaz/Ways_of_development_of_Ukrainian_science/article/12058.016.pdf* *2. Borova T. English for Business Analysts: textbook: in 3 parts, Part 3. Business Intelligent Tools / T. Borova, O. Milov. – Kharkiv: S. Kuznets KhNUE, 2018. – 179 P. [Електронний ресурс].- Режим доступу: http://repository.hneu.edu.ua/bitstream/123456789/21467/1/2018-%D0%91%D0%BE%D1%80%D0%BE%D0%B2%D0%B0%20%D0%A2%20%D0%90%2C%20%D0%9C%D1%96%D0%BB%D0%BE%D0%B2%20%D0%9E%20%D0%92.pdf* *3. Journal of Information Security [Електронний ресурс].- Режим доступу: https://www.scirp.org/journa/home.aspx?issueid=l4294#103116.*
Аналіз шкідливих програм	навчальна дисципліна	*НП 4_Магістр_1.9_Ан*	X91hUolLCHt85WEN4cyA5U4MRYDodL	*Обладнання:* *Мультимедійні аудиторії, ПК з*

		аліз шкідливих програм.pdf	g8MjdvrTtIR3s=	*доступом до Інтернету* *ПЗ: Packet Tracer 9.0* *Література:* *1 Sharp, R. Malware. Technical University of Denmark, 2017. 72 p. [Електронний ресурс]. – Режим доступу: https://orbit.dtu.dk/files/139067614/malware.pdf* *2 Mundie, D. A. The MAL: A Malware Analysis Lexicon. Carnegie Mellon University, 2013. 39 p. [Електронний ресурс]. – Режим доступу: https://www.sei.cmu.edu/documents/2247/2013_004_001_40250.pdf* *3 Kara, I. A basic malware analysis method. ResearchGate, 2019. 11 p. [Електронний ресурс]. – Режим доступу: https://www.researchgate.net/publication/333834813_A_basic_malware_analysis_method* *4 Zhang, H., Wu, J., & Xu, H. Analyzing PDFs like Binaries: Adversarially Robust PDF Malware Analysis via Intermediate Representation and Language Model. arXiv preprint, 2025. 18 p. [Електронний ресурс]. – Режим доступу: https://arxiv.org/abs/2506.17162* *5 Egele, M., Scholte, T., Kirda, E., & Kruegel, C. A Survey of Stealth Malware: Attacks, Mitigation Measures, and Steps Toward Autonomous Open World Solutions. arXiv preprint, 2016. 27 p. [Електронний ресурс]. – Режим доступу: https://arxiv.org/abs/1603.06028*
Авторське право у цифровому суспільстві	навчальна дисципліна	*НП 5_Магістр_1.9_Авторське право у цифровому суспільстві.pdf*	nzPXOK8sCnsxcL1GtQHOVgWeGnKUt10//FgFk+v9AkA=	*Обладнання:* *Мультимедійні аудиторії, ПК з доступом до Інтернету* *ПЗ: Packet Tracer 9.0* *Література:* *1 Про авторське право і суміжні права: Закон України від 15 квітня 2023 р. № 2811-IX. URL: https://zakon.rada.gov.ua/laws/show/2811-20#n855* *2 Цивільний кодекс України: Кодекс України від 16.01.2003 №435-IV. URL: https://ips.ligazakon.net/document/T030435* *3 Бернська конвенція про охорону літературних і художніх творів від 24.07.1971 р. Bernska konventsiia pro okhoronu literaturnykh i khudozhnikh tvoriv vid 24.07.1971 r. URL: https://zakon.rada.gov.ua/laws/show/995_051#Text* *4 WIPO Copyright Treaty (WCT), WIPO Performances and Phonograms Treaty (WPPT).* *5 Directive (EU) 2001/29/EC on the harmonisation of certain aspects of copyright and related rights in the information society (InfoSoc Directive).* *6 Directive (EU) 2019/790 on copyright and related rights in the Digital Single Market (DSM Directive).* *7 Gervais, D. The TRIPS*

				Agreement: Drafting History and Analysis. – London: Sweet & Maxwell, 2020. *8 Hugenholtz, P. B. Copyright in the Digital Age. – Amsterdam: IViR, 2018.* *9 Сопільник Л. В. Право інтелектуальної власності: авторське право і суміжні права : навч. посіб. – Львів : ЛьвДУВС, 2021.* *10 Войціховський А. Цифрові права в Україні: авторське право у мережі. – Київ : Юстініан, 2020.*
Інноваційне підприємництво та управління стартап - проєктами	навчальна дисципліна	*ЗП 2_Магістр_1.9_Інноваційне підприємництво та управління стартап проєктами.pdf*	kvMgrkMJ9g25xLiDgTnXOYTbasqNwm9uQCDYyKo3zKY=	*Обладнання:* *Мультимедійні аудиторії, ПК з доступом до Інтернету* *ПЗ: Packet Tracer 9.0* *Література:* *1. Котлубай В. О. Інноваційне підприємництво та управління стартап проектами. Economic evaluation of innovative solution : практикум / В. О. Котлубай, Г. А. Отливанська. – Одеса : НУ "ОЮА", 2021. – 131 с. [Електронний ресурс]. – Режим доступу: https://dspace.onua.edu.ua/server/api/core/bitstreams/dbd21a89-cc80-479b-9f28-17b4d8998767/content* *2. Ден Сенор, Сол Синґер. Країна стартапів. Історія ізраїльського економічного дива. Yakaboo Publishing. 2016. – 368 с. [Електронний ресурс]. – Режим доступу: https://findbook.in.ua/books/krayina-startapiv-istoriia-izrayil-s-kogho-iekonomichnogho-diva* *3. Гавриш О. А., Бояринова К. О., Копішинська К. О. Розробка стартап-проектів: практикум [Електронний ресурс]: навч. посіб. для студ. спеціальностей 151 – «Автоматизація та комп'ютерно-інтегровані технології» та 152 – «Метрологія та інформаційно-вимірювальна техніка». Електронні текстові данні (1 файл: X,XX Мбайт). Київ : КПІ ім. Ігоря Сікорського, 2019. 116 с. [Електронний ресурс]. – Режим доступу: https://ela.kpi.ua/server/api/core/bitstreams/a1ad390a-6a4b-40b2-944f-e82dc7f8e3db/content* *4. Гавриш О. А., Бояринова К. О., Копішинська К. О. Розробка стартап-проектів: Конспект лекцій [Електронний ресурс]: навч. посіб. для студ. спеціальностей 151 – «Автоматизація та комп'ютерно-інтегровані технології» та 152 – «Метрологія та інформаційно-вимірювальна техніка». Електронні текстові данні (1 файл: X,XX Мбайт). Київ: КПІ ім. Ігоря Сікорського, 2019. – 188 с. [Електронний ресурс]. – Режим доступу: https://ela.kpi.ua/server/api/core/bitstreams/63391483-0014-435b-866f-ab3188b5a372/content* *5. Шаповал В.А. Опорний конспект лекцій «Стартап*

				міжнародних проектів» для студентів спеціальності «07б 19 Підприємництво, торгівля та біржова діяльність». Дніпро: ДВНЗ «НГУ», 2017. – 29 с. [Електронний ресурс]. – Режим доступу: https://pe.nmu.org.ua/ua/studentam/magistr/076/mb/%D0%9A%D0%9B_%D0%A1%D0%90%D0%9C%D0%9F.pdf *6. Тимур Ворона. Стартап на мільйон: як українці заробляють статки на технологіях. – К. : Видавництво «ВІВАТ», 2017. – 224 с.* *7. Ли Галлахер. Історія Airbnb: Як троє звичайних хлопців підірвали готельну індустрію. – К. : Видавництво: "Book Chef", 2018. [Електронний ресурс]. – Режим доступу: https://www.google.com.ua/books/edition/Airbnb_%D0%9A%D0%B0%D0%BA_%D1%82%D1%80%D0%B8_%D0%BF%D1%80%D0%BE%D1%81%D1%82%D1%8B%D1%85_%D0%BF%D0%B0/AK5VDwAAQBAJ?hl=ru&gbpv=1&dq=%D0%86%D1%81%D1%82%D0%BE%D1%80%D1%96%D1%8F+Airbnb:+%D0%AF%D0%BA+%D1%82%D1%80%D0%BE%D1%94+%D0%B7%D0%B2%D0%B8%D1%87%D0%B0%D0%B9%D0%BD%D0%B8%D1%85+%D1%85%D0%BB%D0%BE%D0%BF%D1%86%D1%96%D0%B2+%D0%BF%D1%96%D0%B4%D1%96%D1%80%D0%B2%D0%B0%D0%BB%D0%B8+%D0%B3%D0%BE%D1%82%D0%B5%D0%BB%D1%8C%D0%BD%D1%83+%D1%96%D0%BD%D0%B4%D1%83%D1%81%D1%82%D1%80%D1%96%D1%8E.&printsec=frontcover*

* 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)
14477	Тараpоєв Яків Володимирович	Професор, Основне місце роботи	Навчально-науковий інститут соціально-гуманітарних технологій	Диплом спеціаліста, Харківський державний університет, рік закінчення: 1996, спеціальність: астрономія, Диплом доктора наук ДД 008640, виданий 06.10.2010, Диплом кандидата наук ДК 016948,	27	Філософські проблеми сучасного наукового пізнання	Підвищення кваліфікації: Харківський Національний педагогічний університет імені Г.С. Сковороди з «17» березня 2025 р. по «17» травня 2025 р. Посвідчення про стажування № 07/23-132. Тема: «Новітні тенденції вивчення та викладання дисциплін в галузі філософських наук для магістрів та

				виданий 11.12.2002, Атестат доцента 02ДЦ 011220, виданий 15.12.2005, Атестат професора 12ПР 008298, виданий 13.11.2012			аспірантів.». Термін: 2 місяці. Наказ НТУ «ХПІ» № 1082 С від 18.06.2025 6 кредитів/180 годин Пункти відповідності ліцензійних умов: 1, 3, 6, 8, 11, 12. П. 1. наявність не менше п'яти публікацій у періодичних наукових виданнях, що включені до переліку фахових видань України, до наукометричних баз, зокрема Scopus, Web of Science Core Collection; 1. Tararoev Jakov, Olga Horodyska and Olga Dolska Ontological Prerequisites for the Emergence of Scientific Cosmology in the Context of the Emergence and Development of the Scientific Thinking.// Philosophy and Cosmology, Volume (2024), 32, 60-73. https://repository.kpi.kharkov.ua/handle/KhPI-Press/73734 2. Яків Тараоєв, Вікторія Горева. Вплив глобальних тенденцій на розвиток політичних еліт. Humanities Studies. 2024. Випуск 19 (96). С. 83-89. http://humstudies.com.ua/article/view/307061 https://doi.org/10.32782/hst-2024-19-96-09 3. Я. В. Тараоєв, Є. В. Захаров, В. А. Захаров. Філософське розуміння економіки сучасного світу крізь інтелектуальний спадок Аристотеля. Вісник Національного технічного університету "ХПІ". Серія : Актуальні проблеми розвитку українського суспільства : зб. наук. пр. – Харків : НТУ "ХПІ", 2024. – № 1. – С. 25-31. https://repository.kpi.kharkov.ua/handle/KhPI-Press/788022. 4. Tararoev Jakov, Olga Horodyska and Olga Dolska From Universe to Society: Developing a Methodological Approach Philosophy and Cosmology, Volume 34, 2025 Philosophy and Cosmology, Volume (2025), 34, 93-108. https://ispcjournal.org/journals/2025/34/PhC_vol_34.pdf

							5.Я. В. Тараоєв, Горбань Р.І. Етика штучного інтелекту: історія становлення та сучасний стан.// Вісник Національного технічного університету «ХПІ». Серія : Актуальні проблеми розвитку українського суспільства : зб. наук. пр. – Харків : НТУ «ХПІ», 2025. – № 1. – С. 11-15. http://aprus.khpi.edu.ua/article/view/336792 П. 3. наявність виданого підручника чи навчального посібника (включаючи електронні) або монографії (загальним обсягом не менше 5 авторських аркушів), в тому числі видані у співавторстві (обсягом не менше 1,5 авторського аркуша на кожного співавтора); 1. Філософські проблеми сучасно наукового пізнання: підручник для студентів-магістрів усіх спеціальностей і форм навчання. / Я.В. Тараоєв; О.О. Дольська; Т.М. Дишкант та ін. Харків: Видавець Іванченко І. С., 2023. 550 с. 20.3 автторськх аркуша http://repository.kpi.kharkov.ua/bitstream/KhPI-Press/61484/1/Book_2023_Tararoiev_Filosofski_problemy.pdf 2. Tararoev J. Industrial civilization is unique. True or false? // Are we alone in the Universe? Collective monograph / Vil Bakirov, Massimo Capaccioli and Vadym Kaydash, Ed. – Kharkiv: V. N. Karazin Kharkiv National University, 2022. С.47–66. Колективна монографія 10 авторських аркушів П. 6. наукове керівництво (консультування) здобувача, який одержав документ про присудження наукового ступеня; Фідровська М.Г. «Християнський концепт любові в сучасній культурі: філософсько-антропологічний аналіз», дис. доктора філософії; науковий керівник - док. філос. н., проф. Тараоєв

							Я.В. 07.02.2024 р., спеціалізована рада ДФ 64.050.110, Національний технічний університет «Харківський політехнічний інститут» диплом Н24 № 001255 від 26.02.2024 р. П. 8. виконання функцій (повноважень, обов'язків) наукового керівника або відповідального виконавця наукової теми (проекту), або головного редактора/члена редакційної колегії/експерта (рецензента) наукового видання, включеного до переліку фахових видань України, або іноземного наукового видання, що індексується в бібліографічних базах; 1. Член редакційної колегії наукового видання: Вісник ХНУ імені В. Н. Каразіна. Серія «Філософія. Філософські перипетії». З 2015р. до теперішнього часу. Журнал є фаховий, група В. 2. Член редакційної колегії наукового видання: Вісник Національного технічного університету «ХПІ». Серія: Актуальні проблеми розвитку українського суспільства. ISSN 2227-6890 З 2016 р. по теперішній час. Журнал є фаховий з 2019 р., група В. 3. Член редакційної колегії наукового видання: «Philosophy and Cosmology». Philosophy and Cosmology (ISSN 2518-1866 (Online), ISSN 2307-3705 (Print)) is an international, double-blind, peer-reviewed, open-access journal, published semiannually by the International Society of Philosophy and Cosmology (ISPC). Журнал входить до бібліографічної бази Web of Science. З 2024 р. до теперішнього часу. П. 11. наукове консультування підприємств, установ, організацій не менше трьох років, що

							здійснювалося на підставі договору із закладом вищої освіти (науковою установою); Наукове консультування та співпраця з Науково-дослідним інститутом українознавства та козацтва, Українською асоціацією суспільствознавців та педагогів та Академією військово-історичних наук і козацтва (на підставі договору № 300/39-2024, терміном 2024-2029 р.р.). П. 12. наявність апробаційних та/або науково-популярних, та/або консультаційних (дорадчих), та/або науково-експертних публікацій з наукової або професійної тематики загальною кількістю не менше п'яти публікацій 1. Тараоєв Я. В. Світ-система, «метаекономіка обміну» та технології// Філософія в сучасному світі : Матеріали III Міжнародної науково-практичної конференції, 18–19 листопада 2022 р. // Ред. кол. Я. В. Тараоєв, А. В. Кіпенський, О. О. Дольська [та ін.]. – Харків, 2022. – с. 225, С.16-20 https://web.kpi.kharkov.ua/philosophy/wp-content/uploads/sites/124/2023/01/zbirka_2022.pdf 2. Тараоєв Я. В. Матеріалістичне розуміння суспільства. Соціальні структури як нерівноважні системи та оцінка перспектив їх розвитку і функціонування за допомогою параметра EROI [Електронний ресурс] / Я. В. Тараоєв // Філософія в сучасному світі : матеріали 4-ї Міжнар. наук.-практ. конф., 17-19 листопада 2023 р. / гол. ред. Я. В. Тараоєв ; Нац. техн. ун-т "Харків. політехн. ін-т" [та ін.]. – Електрон. текст. дані. – Харків, 2023. – С. 13-19. https://repository.kpi.kharkov.ua/server/api/core/bitstreams/fc6c5c0

							2-35ac-49e5-9474-512d831bf882/content 3. Тараоєв Я. В. Економіка капіталізму та науково-технічний прогрес / Я. В. Тараоєв // Людина/світ на роздоріжжі: технології, ресурси, соціальні інституції. Практичні студії : матеріали 3-го міжнар. наук.-метод. семінару, 4-6 травня 2023 р. / Нац. техн. ун-т "Харків. політехн. ін-т". – Харків : НТУ "ХПІ", 2023. – С. 64-69. https://repository.kpi.kharkov.ua/handle/KhPI-Press/64770 4.Тараоєв Я. В. Енергетичний баланс у суспільстві та соціальні інститути: певні оцінки та методологічні підходи // Людина/світ на роздоріжжі: технології, ресурси, соціальні інституції. Практичні студії : матеріали 4-го міжнар. наук.-метод. семінару, 15–17 травня 2024 р. / Нац. техн. ун-т "Харків. політехн. ін-т". – Харків : НТУ "ХПІ", 2023. С. 42–46. https://repository.kpi.kharkov.ua/server/api/core/bitstreams/31a63f0f-c4a6-4710-ab67-4d079ba67301/content#page=42 5. Тараоєв Я. В. Категорія «часу» як фактор розвитку технологій та соціальні інституції економічної діяльності у сучасному суспільстві // Філософія в сучасному світі [Електронний ресурс] : матеріали 5-ї Міжнар. наук.-практ. конф., 22-24 листопада 2024 р. / ред. кол. О. О. Дольська, Я. В. Тараоєв, А. В. Кіпенський, [та ін.] ; Нац. техн. ун-т "Харків. політехн. ін-т" [та ін.]. – Електрон. текст. дані. – Харків, 2024. – 254 с. – Укр. та англ. мовами. https://repository.kpi.kharkov.ua/server/api/core/bitstreams/a7ad0904-a529-431d-94c8-86332aeab41e/content 6. Тараоєв Я. В. Капіталізм та проблема ресурсів, енергії та соціальних інституцій // Людина,

							суспільство, комунікативні технології: матеріали XII Міжнар. наук.-практ. конф. 25 жовтня 2024 р. / відп. за випуск І. В. Толстов. — Харків: УкрДУЗТ, 2024. –С. 86-88 https://kart.edu.ua/wp-content/uploads/2023/04/ljudina_suspilstvo_komunikativni_tehnologii_2024.pdf
410246	Хвостенко Владислав Сергійович	Доцент, Основне місце роботи	Навчально-науковий інститут комп'ютерних наук та інформаційних технологій	Диплом бакалавра, Харківський національний економічний університет, рік закінчення: 2005, спеціальність: 0501 Економіка і підприємництво, Диплом спеціаліста, Харківський національний економічний університет, рік закінчення: 2007, спеціальність: 050107 Економічна статистика, Диплом магістра, Харківський національний економічний університет, рік закінчення: 2006, спеціальність: 050104 Фінанси, Диплом магістра, Відокремлений структурний підрозділ "Інститут інтелектуальної власності Національного університету "Одеська юридична академія" в м. Києві, рік закінчення: 2014, спеціальність: Інтелектуальна власність, Диплом кандидата наук ДК 008014, виданий 26.09.2012, Атестат доцента АД 003303, виданий 15.10.2019, Атестат	18	Інноваційне підприємництво та управління стартап - проєктами	Підвищення кваліфікації Стажування в Університеті національного комітету освіти у Кракові (Польща) на кафедрі інженерії програмного забезпечення за напрямом «Методи та технічні засоби захисту інформації» тривалістю 180 годин (6 кредитів), сертифікат №КІО/23-04-18/2025 від 23.04.2025 р., затверджено наказом №2186С від 21.11.2025р. Пункти відповідності ліцензійних умов: П. 1, 2, 4, 8, 12, 13, 19 20 П. 1 наявність не менше п'яти публікацій у періодичних наукових виданнях, що включені до переліку фахових видань України, до наукометричних баз, зокрема Scopus, Web of Science Core Collection 1. Alla Havrylova, Yuliia Khokhlachova, Andrii Tkachov, Natalia Voropay, Vladyslav Khvostenko. Justification of directions for improving authentication protocols in information and communication systems. Ukrainian Information Security Research Journal. 2023. № 1 (25). P. 6-19. https://jrnl.nau.edu.ua/index.php/ZI/article/view/17593 2. Khvostenko V., Havrylova A., Milevskyi S. Development of an Advanced SSL/TLS Protocol for Transferring Requests to a 3D-Printer // Springer Tracts in

				доцента АД 006909, виданий 09.02.2021			Additive Manufacturing. – 2025. – Part F641. – P. 489–503. – DOI: [SpringerLink] – Індексується в Scopus. – 0,94 авт. арк. https://link.springer.com/chapter/10.1007/978-3-031-84873-5_383. Khvostenko V., Milevskyi S., Bukatych I., Yevseiev D., Iegrashyn O., Kyryk V. Smart Contracts: Classification Problems // Proc. 7th International Congress on Human-Computer Interaction, Optimization and Robotic Applications (ICHORA 2025). – IEEE, 2025. – DOI: https://www.ichoracongress.com/ichora2025/ICHORA2025_Congress_Information.pdf – 0,04 авт. арк. 4. Androshchuk H., Khvostenko V. Digital tools for determining intellectual property object notoriety (on the example of character and work notoriety) // Information and Law. – 2024. – № 3(50). – P. 54–64. – DOI: https://doi.org/10.37750/2616-6798.2024.3(50).311635 – Категорія Б (фахове видання України, індексується в Index Copernicus). – 0,7 ум. друк. арк. / внесок 0,35 авт. арк. 5. Dunayev S., Milevska T., Voropay N., Murr P., Khvostenko V., Sevriukova Y. Research of Technologies and Methods of Web Application Protection in the Infrastructure of a Higher Education Institution with the Assistance of Specialized Systems // Proc. International Congress on Human-Computer Interaction, Optimization and Robotic Applications (HORA 2024). – IEEE, 2024. – 0,25 авт. арк. https://jglobal.jst.go.jp/en/detail?JGLOBAL_ID=202402257602422312&utm_source=chatgpt.com 6. Melenti Y., Yevseiev S., Korol O., Milevskyi S., Khvostenko V. Application of the innovative approach in the modernization of higher education

							institutions of the Security Service of Ukraine // Ukrainian Scientific Journal of Information Security. – 2024. – Vol. 30, No. 1. – P. 179–189. – DOI: https://doi.org/10.18372/2225-5036.30.18619 7. Розумний С. М., Воліков В. В., Хвостенко В. С. The influence of the methodology functions on the quality of solving an expert task // Науковий журнал судових експертів Міністерства юстиції України. – 2024. – № 1(9). – С. 28–35. – DOI: https://doi.org/10.32782/2708-1834/2024-09.2 8. Molodetska K., Veretiuk S., Rahimova I., Milevskyi S., Khvostenko V. Information Influence on the Virtual Community: Implementation Features and Method of Detection in Social Internet Services // Proc. 7th International Symposium on Multidisciplinary Studies and Innovative Technologies (ISMSIT 2023). – IEEE, 2023. – Індексується в Scopus. https://www.scopus.com/pages/publications/85179132580 9. Kondratenko Y., Korobkin D., Dunayev S., Khvostenko V. Design and Evaluation of an AIOT-Based Medical Information System // Ukrainian Information Security Research Journal. – 2023. – (Категорія Б, фахове видання України, входить до баз Index Copernicus). https://jrnl.nau.edu.ua/index.php/ZI/article/view/17594 10. Havrylova Alla, Khvostenko V., et al. Justification of Directions for Improving Authentication Protocols in Information and Communication Systems // Ukrainian Information Security Research Journal. – 2023. – (Категорія Б, індексується у фахових базах, Index Copernicus). DOI: 10.18372/2410-7840.25.17593

							П. 2 наявність одного патенту на винахід або п'яти деклараційних патентів на винахід чи корисну модель, включаючи секретні, або наявність не менше п'яти свідоцтв про реєстрацію авторського права на твір Патенти на корисну модель: 1. Патент u202103704 від 29.06.2021 СПОСІБ КРИПТОГРАФІЧНОГО ПЕРЕТВОРЕННЯ ІНФОРМАЦІЇ 2. Патент u202103665 від 25.06.2021 СПОСІБ КРИПТОГРАФІЧНОГО ПЕРЕТВОРЕННЯ ІНФОРМАЦІЇ 3. Патент u202103617 від 23.06.2021 СПОСІБ КРИПТОГРАФІЧНОГО ПЕРЕТВОРЕННЯ ІНФОРМАЦІЇ 4. Патент u202103615 від 23.06.2021 СПОСІБ КРИПТОГРАФІЧНОГО ПЕРЕТВОРЕННЯ ІНФОРМАЦІЇ 5. Патент u202103683 від 23.07.2021 СПОСІБ КРИПТОГРАФІЧНОГО ПЕРЕТВОРЕННЯ ІНФОРМАЦІЇ 6. Патент u202103680 від 25.06.2021 СПОСІБ КРИПТОГРАФІЧНОГО ПЕРЕТВОРЕННЯ ІНФОРМАЦІЇ П. 4 наявність виданих навчально-методичних посібників/посібників для самостійної роботи здобувачів вищої освіти та дистанційного навчання, електронних курсів на освітніх платформах ліцензіатів, конспектів лекцій/практикумів/методичних вказівок/рекомендацій/ робочих програм, інших друкованих навчально-методичних праць загальною кількістю три найменування 1. Intellectual Property: syllabus for students of specialty 113, Master's level [Електронне видання] / comp. V. S. Khvostenko. – Kharkiv: NTU «KhPI», 2024. – (Eng. lang.). – Режим

							доступу: https://web.kpi.kharkov.ua/kmmm/wp-content/uploads/sites/110/2024/12/GS-3_Intellectual_Property_Syllabus_Master_113_Khvostenko-V.S._ENG_2024.pdf 2. Господарське право: робоча програма навчальної дисципліни для здобувачів другого (магістерського) рівня спеціальності 125 «Кібербезпека» [Електронне видання] / уклад. В. С. Хвостенко. – Харків: НТУ «ХПІ», 2022. – (Укр. мов.). – Режим доступу: http://repository.kpi.kharkov.ua/handle/KhPI-Press/63734 3. Захист інтелектуальної власності: робоча програма навчальної дисципліни для здобувачів другого (магістерського) рівня спеціальності 125 «Кібербезпека» [Електронне видання] / уклад. В. С. Хвостенко. – Харків: НТУ «ХПІ», 2022. – 17 с. – (Укр. мов.). – Режим доступу: http://repository.kpi.kharkov.ua/handle/KhPI-Press/63733 4. Правове забезпечення діяльності у сфері безпеки: робоча програма навчальної дисципліни для здобувачів другого (магістерського) рівня спеціальності 125 «Кібербезпека» [Електронне видання] / уклад. В. С. Хвостенко, А. А. Гаврилова. – Харків: НТУ «ХПІ», 2022. – (Укр. мов.). – Режим доступу: http://repository.kpi.kharkov.ua/handle/KhPI-Press/63735 5. Правове регулювання інформаційної безпеки: робоча програма навчальної дисципліни для здобувачів другого (магістерського) рівня спеціальності 125 «Кібербезпека» [Електронне видання] / уклад. В. С. Хвостенко. – Харків: НТУ «ХПІ», 2022. – (Укр. мов.). – Режим

							доступу: https://web.kpi.kharkov.ua/kmmm/wp-content/uploads/sites/110/2024/04/VP-3.2.1_Pravove_regulyuvannya_informatsijnoyi_bezpeky_Sylabus_113_Bakalavr_Hvostenko-V.S._UKR_2023-24.pdf 6. Технології баз даних : навчально-практичний посібник / уклад. А. А. Гаврилова, С. С. Погасій, Р. В. Корольов, В. С. Хвостенко, Т. С. Мілевська ; за заг. ред. С. П. Євсеєва. – Харків : НТУ «ХПІ», – Львів : «Новий Світ-2000», 2025. – 222 с. Технології баз даних : навчально-практичний посібник – Новий Світ 2000 П. 8 виконання функцій (повноважень, обов'язків) наукового керівника або відповідального виконавця наукової теми (проекту), або головного редактора/члена редакційної колегії/експерта (рецензента) наукового видання, включеного до переліку фахових видань України, або іноземного наукового видання, що індексується в бібліографічних базах Виконання функцій рецензента міжнародного наукового видання Asian Journal of Research in Computer Science https://journalajrcos.com/ (Certificate of Excellence in Reviewing, 2025). Іноземне наукове видання, що індексується у міжнародних бібліографічних базах П. 12 наявність апробаційних та/або науково-популярних, та/або консультаційних (дорадчих), та/або науково-експертних публікацій з наукової або професійної тематики загальною кількістю не менше п'яти публікацій Хвостенко В.С., Мілевський С., Букатич І., Євсеєв Д.,

							Єграшин О., Кирик В. Smart Contracts: Classification Problems // Матеріали 7th International Congress on Human-Computer Interaction, Optimization and Robotic Applications (ICHORA 2025): збірник матеріалів. – IEEE, 2025. – [Електронний ресурс]. – Режим доступу: https://set-science.com/org/ichora2025/news/ICHORA2025_news_1.pdf Дунаєв С., Мілевська Т., Воропай Н., Murr P., Хвостенко В., Севрюкова Є. Research of Technologies and Methods of Web Application Protection in the Infrastructure of a Higher Education Institution with the Assistance of Specialized Systems // Матеріали International Congress on Human-Computer Interaction, Optimization and Robotic Applications (HORA 2024): збірник матеріалів. – IEEE, 2024. – [Електронний ресурс]. – DOI: 10.1109/HORA61326.2024.10550503 Molodetska K., Veretiuk S., Rahimova I., Milevskyi S., Khvostenko V. Information Influence on the Virtual Community: Implementation Features and Method of Detection in Social Internet Services // Proc. 7th International Symposium on Multidisciplinary Studies and Innovative Technologies (ISMSIT 2023). – IEEE, 2023. – Індексується в Scopus. https://www.scopus.com/pages/publications/85179132580 9. Kondratenko Y., Korobkin D., Dunayev S., Khvostenko V. Design and Evaluation of an AIOT-Based Medical Information System // Ukrainian Information Security Research Journal. – 2023. – (Категорія Б, фахове видання України, входить до баз Index Copernicus). https://jrnl.nau.edu.ua/index.php/ZI/article/view/17594 10. Havrylova Alla, Khvostenko V., et al.

							Justification of Directions for Improving Authentication Protocols in Information and Communication Systems // Ukrainian Information Security Research Journal. – 2023. – (Категорія Б, індексується у фахових базах, Index Copernicus). DOI: 10.18372/2410-7840.25.17593 Synergy of building cybersecurity systems / S. Yevseiev, V. Ponomarenko, O. Laptiev, O. Milov, O. Korol, S. Milevskyi, S. Pohasii, A. Tkachov, O. Shmatko, Y. Melenti, O. Sievierinov, S. Ostapov, A. Gavrilova, O. Tsyhanenko, S. Herasimov, E. Nyemkova, B. Tomashevsky, I. Hrod, I. Opirskyy, V. Zvieriev, O. Prokopenko, V. Savchenko, O. Barabash, V. Sobchuk, G. Shuklin, V. Khvostenko, O. Tymochko, M. Pavlenko, A. Trystan, S. Florov // monograph. – Kharkiv: PC TECHNOLOGY CENTER, 2021. – 188 p.(P. 102 – 147). Acces mode: https://www.scopus.com/pages/publications/85119654284 П.13. проведення навчальних занять із спеціальних дисциплін іноземною мовою (крім дисциплін мовної підготовки) в обсязі не менше 50 аудиторних годин на навчальний рік 1. Legal regulation of cybersecurity, (50 ауд. год) КН-1125і.е. П. 19 діяльність за спеціальністю у формі участі у професійних та/або громадських об'єднаннях Учасник Громадської організації "Національна асоціація патентних повірених" https://www.napa.org.ua член громадської організації "Східноєвропейське наукове товариство", посвідчення ES № 063 П. 20 досвід практичної роботи за спеціальністю не

							менше п’яти років (крім педагогічної, науково-педагогічної, наукової діяльності) – директор, ТОВ АТІЛОГ (ЄДРПОУ: 35974114) з 2008, ІТ компанія. https://youcontrol.com.ua/catalog/company_details/35974114/
410245	Погасій Сергій Сергійович	Професор, Основне місце роботи	Навчально-науковий інститут комп’ютерних наук та інформаційних технологій	Диплом бакалавра, ХДЕУ, рік закінчення: 1998, спеціальність: Економіка, Диплом спеціаліста, Харківський державний економічний університет, рік закінчення: 1999, спеціальність: 050104 Фінанси і кредит, Диплом магістра, Харківський національний університет радіоелектроніки, рік закінчення: 2021, спеціальність: 125 Кібербезпека, Диплом доктора наук ДД 013762, виданий 18.02.2025, Диплом кандидата наук ДК 051003, виданий 28.04.2009, Атестат доцента АД 006046, виданий 26.11.2020	21	Виявлення вторгнень у компьютерні мережі (мережеві аномалії)	Підвищення кваліфікації Стажування в Університеті національного комітету освіти у Кракові (Польща) на кафедрі інженерії програмного забезпечення за напрямом «Методи та технічні засоби захисту інформації» тривалістю 180 годин (6 кредитів), сертифікат №КІО/23-04-18/2025 від 23.04.2025 р., затверджено наказом №2186С від 21.11.2025р. Пункти відповідності ліцензійних умов: П. 1, 2, 4, 5, 10, 12,13, 15, 19, 20. П. 1 наявність не менше п’яти публікацій у періодичних наукових виданнях, що включені до переліку фахових видань України, до наукометричних баз, зокрема Scopus, Web of Science Core Collection 1. Shmatko, O., Herasymov, S., Milevskyi, S., Balitskyi, N., Pohasii, S., Aleksieiev, M., Vlasov, I., Melenti, Y., Kovalenko, Y., & Peleshok, Y. (2025). Development of a method for assessing the efficiency of technical systems’ computer dynamic simulators. Eastern-European Journal of Enterprise Technologies, 2(9 (134), 50–61. ISSN (print) 1729-3774, ISSN (online) 1729-406 https://doi.org/10.15587/1729-4061.2025.327558 2. Pohasii, S., Milevskyi, S., Yevseiev, S., Korol, O. (2025). Development of a Method for Comprehensive Evaluation of the Service Provision Quality. In: Durakbasa, N.M., Cetinkaya, K.,

Demircioglu, P., Bogrekci, I. (eds) Digitalization in Additive Manufacturing. ICPTDI 2024. Springer Tracts in Additive Manufacturing. Springer, Cham. (459 – 473), ISSN (on-line) 27309576 https://doi.org/10.1007/978-3-031-84873-5_36
3. Pohasii, S., Milevskyi, S., Brynza, N., Vilkhivska, O. (2025). Prospects for the Development of UAVs Using CFRP and 3D Printing. In: Durakbasa, N.M., Cetinkaya, K., Demircioglu, P., Bogrekci, I. (eds) Digitalization in Additive Manufacturing. ICPTDI 2024. Springer Tracts in Additive Manufacturing. Springer, Cham. (323 – 333), ISSN (on-line) 27309576 https://doi.org/10.1007/978-3-031-84873-5_26
4. Погасій С. (2023). «Застосування збиткових LDPC кодів в стандарті LORAWAN». Ukrainian Scientific Journal of Information Security. № 29. С.73–79. https://jrnl.nau.edu.ua/index.php/Infosecurity/article/view/17871
5. Погасій С. (2022). «Моделі і методи захисту інформації в кіберфізичних системах». Безпека інформації. Том 28 № 2, С. 67– 79. https://jrnl.nau.edu.ua/index.php/Infosecurity/article/view/16951
6. Погасій С. (2022). «Оцінка рівня безпеки в кіберфізичних системах. Захист інформації». Том 24 № 2, С. 81– 94. https://jrnl.nau.edu.ua/index.php/ZI/article/view/16933
7. Yevseiev S., Pohasii S., Zhuchenko O., Milov O., Lysechko V., Kovalenko O., Kostiak M., Volkov A., Lezik A., & Susukailo V. (2022). «Development of crypto-code constructs based on LDPC codes. Eastern-European Journal of Enterprise Technologies», 2(9 (116), pp.44–59.

							(Scopus) https://journals.uran.ua/eejet/article/view/254545 П. 2 наявність одного патенту на винахід або п'яти деклараційних патентів на винахід чи корисну модель, включаючи секретні, або наявність не менше п'яти свідоцтв про реєстрацію авторського права на твір 1. Назва винаходу (корисної моделі) № 150292 від 26.01.2022 Спосіб криптографічного перетворення інформації https://sis.nipo.gov.ua/uk/search/detail/1675026/ 2. Назва винаходу (корисної моделі) № 143963 від 25.08.2020 Спосіб криптографічного перетворення інформації з використанням подовжених кодів з нанесенням збитку https://sis.nipo.gov.ua/uk/search/detail/1449467/ 3. Назва винаходу (корисної моделі) № 149715 від 01.12.2021 Спосіб криптографічного перетворення інформації https://sis.nipo.gov.ua/uk/search/detail/1664381/ 4. Назва винаходу (корисної моделі) № 150235 від 19.01.2022 Спосіб криптографічного перетворення інформації https://sis.nipo.gov.ua/uk/search/detail/1674091/ 5. Назва винаходу (корисної моделі) № 151040 від 01.06.2022 Спосіб криптографічного перетворення інформації https://sis.nipo.gov.ua/uk/search/detail/1690711/ П. 4 наявність виданих навчально-методичних посібників/посібників для самостійної роботи здобувачів вищої освіти та дистанційного навчання, електронних курсів на освітніх платформах ліцензіатів, конспектів

							лекцій/практикумів/методичних вказівок/рекомендацій/ робочих програм, інших друкованих навчально-методичних праць загальною кількістю три найменування 1. Сучасні методи захисту соціо-кіберфізичних систем робоча програма навчальної дисципліни [Електронний ресурс] : [для здобувачів] третього (доктор філософії) рівня вищої освіти очної та заочної форми навчання спец. 125 " Кібербезпека"/ розроб. С. С. Погасій ; Нац. техн. ун-т "Харків. політехн. ін-т". – Електрон. текст. дані. – Харків, 2022. – 11 с. – URI: http://repository.kpi.kharkov.ua/handle/KhPI-Press/63666. 2. Основи побудови та захисту мікропроцесорних систем робоча програма навчальної дисципліни [Електронний ресурс] : [для здобувачів] першого (бакалаврський) рівня вищої освіти денної форми навчання спец. 125 "Кібербезпека"/ розроб. С. С. Погасій, А. А. Гаврилова; Нац. техн. ун-т "Харків. політехн. ін-т". – Електрон. текст. дані. – Харків, 2022. – 31 с. – URI: http://repository.kpi.kharkov.ua/handle/KhPI-Press/63777.3. Методичні вказівки до виконання магістерських робіт для студентів спеціальності F5 “Кібербезпека та захист інформації” / уклад. С.П. Євсеєв, С.С. Погасій, С.В. Мілевський, О. Г. Король. – Харків: НТУ “ХПІ”. – 52 с. 3. Моделювання механізмів кібербезпеки робоча програма навчальної дисципліни [Електронний ресурс] : [для здобувачів] третього (доктор філософії) рівня вищої освіти очної та заочної форми навчання спец. 125 " Кібербезпека"/

							розроб. С. С. Погасій ; Нац. техн. ун-т "Харків. політехн. ін-т". – Електрон. текст. дані. – Харків, 2022. – 11 с. – URI: http://repository.kpi.kharkov.ua/handle/KhPI-Press/63700. 4. Технології баз даних. Навчально-практичний посібник / уклад. А. А. Гаврилова, С. С. Погасій, Р. В. Корольов, В. С. Хвостенко, Т. С. Мілевська ; за заг. ред. С. П. Євсеєва. – Харків : НТУ «ХПІ», – Львів : «Новий Світ-2000», 2025. – 222 с. – (Серія «Кібербезпека та штучний інтелект»). ISBN 978-966-418-516-2. П. 5 захист дисертації на здобуття наукового ступеня (*за останні 5 років) Доктор технічних наук, 05.13.21 - Системи захисту інформації, тема дисертації: . Моделі і методи захисту інформації в кіберфізичних системах. Диплом ДД № 013762 від 18 лютого 2025 року, Міністерство освіти і науки України, Державний університет інформаційно-комунікаційних технологій. П. 10 участь у міжнародних наукових та/або освітніх проектах, залучення до міжнародної експертизи, наявність звання “суддя міжнародної категорії” United States Department of State Global Innovation through Science and Technology Initiative (GIST) GIST Innovates Ukraine 2021,CERTIFICATE OF COMPLETION GIST Innovates Ukraine 2021, 4 AUGUST 2021 П. 12 наявність апробаційних та/або науково-популярних, та/або консультаційних (дорадчих), та/або науково-експертних публікацій з наукової або професійної тематики загальною кількістю не менше п’яти публікацій :

1. S. Pohasii, M. Tkach, A. Salii, T. Kurtseitov, D. Pecherytsia and V. Hrunovych, "Secure Data Exchange Technologies in Mobile and IoT Devices," 2025 7th International Congress on Human-Computer Interaction, Optimization and Robotic Applications (ICHORA), Ankara, Turkiye, 2025, pp. 1-6, doi: 10.1109/ICHORA65333.2025.11016977.
2. S. Pohasii, S. Holdobin, N. Brynza, O. Vilkhivska, O. Bilotserkivskyi and B. Samorodov, "Management Models for Wireless Communication Channel Interference Monitoring," 2024 8th International Symposium on Multidisciplinary Studies and Innovative Technologies (ISMSIT), Ankara, Turkiye, 2024, pp. 1-7, doi: 10.1109/ISMSIT63511.2024.10757190.
3. O. Sitchenko, S. Milevskyi, S. Pohasii, V. Kotsiuba, A. Krepko and S. Vladimir, "A Combination of Steganography Methods to Increase the Degree of Information Concealment," 2025 3rd Cognitive Models and Artificial Intelligence Conference (AICCONF), Prague, Czech Republic, 2025, pp. 1-4, https://ieeexplore.ieee.org/document/11064251
4. S. Pohasii, M. Mashchenko, O. Serhiienko, O. Klimenko, T. Andriushchenko and T. Milevska, "Assessing the Economic and Technical Effectiveness of Intercepting UAVs Using Alternative Methods," 2023 7th International Symposium on Multidisciplinary Studies and Innovative Technologies (ISMSIT), Ankara, Turkiye, 2023, pp. 1-5, https://ieeexplore.ieee.org/document/10304959
5. Pohasii, S., Milevskyi, S., Yevseiev, S., Korol, O. (2025). Development of a Method for Comprehensive Evaluation of the

							Service Provision Quality. In: Durakbasa, N.M., Cetinkaya, K., Demircioglu, P., Bogrekci, I. (eds) Digitalization in Additive Manufacturing. ICPTDI 2024. Springer Tracts in Additive Manufacturing. Springer, Cham. https://doi.org/10.1007/978-3-031-84873-5_36 6. S. Pohasii, R. Korolov, N. Dzheniuk, A. Jammine, T. Andriushchenko and T. Milevska, "Decision Making in Managing the Choice of UAV Threat Detection Systems in the Protection of Critical Infrastructure Facilities," 2023 5th International Congress on Human-Computer Interaction, Optimization and Robotic Applications (HORA), Istanbul, Turkiye, 2023, pp. 1-6, doi: 10.1109/HORA58378.2023.10155776. П.13. проведення навчальних занять із спеціальних дисциплін іноземною мовою (крім дисциплін мовної підготовки) в обсязі не менше 50 аудиторних годин на навчальний рік 2025-2026: 1. Internet of Things security, (48 ауд. год) КН-1122ia.e 2. Fundamentals of steganographic information protection, (48 ауд. год) КН-1122ia.e https://cybersecurity.kpi.kharkov.ua/sylabusy-osvitnikh-komponentiv-125-bakalavr/ П. 15 керівництво школярем, який зайняв призове місце III-IV етапу Всеукраїнських учнівських олімпіад з базових навчальних предметів, II-III етапу Всеукраїнських конкурсів-захистів науково-дослідницьких робіт учнів - членів Національного центру “Мала академія наук України”; участь у журі III-IV етапу Всеукраїнських учнівських олімпіад з базових навчальних

							предметів чи II-III етапу Всеукраїнських конкурсів-захистів науково-дослідницьких робіт учнів - членів Національного центру “Мала академія наук України” (крім третього (освітньо-наукового/освітньо-творчого рівня) (*надати лінки чи документи, що підтверджують наявність цього досягнення)II етап Всеукраїнського конкурсу-захисту науково-дослідницьких робіт учнів – членів МАН України у 2024/2025 навчальному році 1. Наукове відділення Інформаційних технологій Секція: «Комп’ютерна інженерія» Магомедов Карім Магомедназірович http://khom.org.ua/wp-content/uploads/2025/01/%D0%9A%D0%BE%D0%BC%D0%BF%D1%8E%D1%82%D0%B5%D1%80%D0%BD%D0%B0-%D1%96%D0%BD%D0%B6%D0%B5%D0%BD%D0%B5%D1%80%D1%96%D1%8F.doc 2. Наукове відділення Інформаційних технологій Секція: «Інтернет-технології та вебдизайн» Пархоменко Яна Русланівна http://khom.org.ua/wp-content/uploads/2025/01/%D0%86%D0%BD%D1%82%D0%B5%D1%80%D0%BD%D0%B5%D1%82-%D1%82%D0%B5%D1%85%D0%BD%D0%BE%D0%BB%D0%BE%D0%B3%D1%96%D1%97-%D1%82%D0%B0-%D0%B2%D0%B5%D0%B1%D0%B4%D0%B8%D0%B7%D0%B0%D0%B9%D0%BD.doc П. 19 діяльність за спеціальністю у формі участі у професійних та/або громадських об’єднаннях Засновник Громадської організації “Association of STEM researchers and inventors” П. 20 досвід практичної роботи за спеціальністю не

							менше п’яти років (крім педагогічної, науково-педагогічної, наукової діяльності) 1. Керівник виробничо-комерційної фірми, ПП ХАРКІВ ІНТЕЛКОМ, (Діяльність із керування комп’ютерним устаткованням, ремонт комп’ютерів і периферійного устаткування). З 2003р- по теперішній час.
410244	Мілевський Станіслав Валерійович	Професор, Основне місце роботи	Навчально-науковий інститут комп’ютерних наук та інформаційних технологій	Диплом спеціаліста, Харківський державний економічний університет, рік закінчення: 2001, спеціальність: 0501 Економіка підприємства, Диплом магістра, Національний авіаційний університет, рік закінчення: 2021, спеціальність: 125 Кібербезпека, Диплом доктора наук ДД 013771, виданий 18.02.2025, Диплом кандидата наук ДК 033701, виданий 13.04.2006, Атестат доцента 12ДЦ 023152, виданий 17.06.2010, Атестат доцента АД 006043, виданий 26.11.2020	19	Англійська мова в академічних застосунках	Підвищення кваліфікації Стажування в Університеті національного комітету освіти у Кракові (Польща) на кафедрі інженерії програмного забезпечення за напрямом «Методи та технічні засоби захисту інформації» тривалістю 180 годин (6 кредитів), сертифікат №KIO/23-04-17/2025 від 23.04.2025 р., затверджено наказом №2186С від 21.11.2025р. Пункти відповідності ліцензійних умов: П. 1, 3, 4, 5, 10, 12, 13, 19 П. 1 наявність не менше п’яти публікацій у періодичних наукових виданнях, що включені до переліку фахових видань України, до наукометричних баз, зокрема Scopus, Web of Science Core Collection 1. Yevseiev, S., Milevskyi, S., Melenti, Y., Voitko, O., Aleksieiev, M., Morklyanyk, B., Povaliaiev, S., Shvorak, R., Sevriukova, Y., & Rykov, D. (2025). Development of a method for assessing the society national security level based on the triple helix concept. Eastern-European Journal of Enterprise Technologies, 4(4 (136), 32–45. https://doi.org/10.15587/1729-4061.2025.337398 2. Melenti, Y., Korol, O., Shulha, V., Milevskyi, S., Sievierinov O., Voitko, O., Rzayev, K., Husarova, I.,

Kravchenko, S., & Pashayeva, S. (2025). Development of post-quantum cryptosystems based on the Rao-Nam scheme. Eastern-European Journal of Enterprise Technologies, 1(9 (133), 35–48. ISSN (print) 1729-3774, ISSN (on-line) 1729-406 https://doi.org/10.15587/1729-4061.2025.323195

3. Shmatko, O., Herasymov, S., Milevskyi, S., Balitskyi, N., Pohasii, S., Aleksieiev, M., Vlasov, I., Melenti, Y., Kovalenko, Y., & Peleshok, Y. (2025). Development of a method for assessing the efficiency of technical systems' computer dynamic simulators. Eastern-European Journal of Enterprise Technologies, 2(9 (134), 50–61. ISSN (print) 1729-3774, ISSN (on-line) 1729-406 https://doi.org/10.15587/1729-4061.2025.327558

4. Yevseiev, S., Milevskyi, S., Pribyliev, Y., Melenti, Y., Nalivayko, A., Bazarnyi, S., Morozov, O., Kazak, I., Hrebeniuk, A., & Ivashchenko, O. (2025). Development of a method of psychological impact on target audiences of gamers using modern information technologies. Eastern-European Journal of Enterprise Technologies, 3(9 (135), 55–64. ISSN (print) 1729-3774, ISSN (on-line) 1729-406 https://doi.org/10.15587/1729-4061.2025.332271

5. Yevseiev, S., Milevskyi, S., Sokol, V., Yemanov, V., Volobuiev, A., Dakova, L., Brailovskyi, M., Rahimova, I., Kravchenko, V., & Cherniavskiy, O. (2024). Development of functionality principles for the automated data transmission system through wireless communication channels to ensure information protection .

Eastern-European Journal of Enterprise Technologies, 4(9 (130), 18–33. https://doi.org/10.15587/1729-4061.2024.310547

6. Shmatko, O., Yevseiev, S., Dudykevych, V., Milevskyi, S., Solnyshkova, S., Havrylova, A., Shestak, Y., Oriekhov, S., Korsunov, S., & Kravchenko, S. (2024). Development of a method for synthesizing an information-analytical system for assessing the level of information transmission channels protection. Eastern-European Journal of Enterprise Technologies, 2(9 (128), 36–43. https://doi.org/10.15587/1729-4061.2024.302495

7. Milevskyi, S., Korol, O., Mykytyn, G., Lozova, I., Solnyshkova, S., Husarova, I., Hrebeniuk, A., Vlasov, A., Sukhoteplyi, V., & Balagura, D. (2024). Development of the sociocyberphysical systems` multi-contour security methodology. Eastern-European Journal of Enterprise Technologies, 1(9 (127), 34–51. https://doi.org/10.15587/1729-4061.2024.298844

8. Murr, P., Yevseiev, S., Milevskyi, S., Melnyk, M., Katsalap, V., Pribyliev, Y., Rzayev, K., Bryla, A., Shpak, O., & Fedorka, P. (2023). Development of an error correction method using perfect binary arrays. Eastern-European Journal of Enterprise Technologies, 4(9 (124), 45–53. https://doi.org/10.15587/1729-4061.2023.285540

9. Yevseiev, S., Havrylova, A., Milevskyi, S., Sinitsyn, I., Chalapko, V., Dukin, H., Hrebeniuk, V., Diedov, M., Bekirova, L., & Shpak, O. (2023). Development of an improved SSL/TLS

							protocol using post-quantum algorithms. Eastern-European Journal of Enterprise Technologies, 3(9 (123), 33–48. https://doi.org/10.15587/1729-4061.2023.281795 П. 3 наявність виданого підручника чи навчального посібника (включаючи електронні) або монографії (загальним обсягом не менше 5 авторських аркушів), в тому числі видані у співавторстві (обсягом не менше 1,5 авторського аркуша на кожного співавтора) (*за наявності надати лінк або бібліографічний опис) 1. Yevseiev, S., Khokhlachova, Yu., Ostapov, S., Laptiev, O., Korol, O., Milevskyi, S. et. al.; Yevseiev, S., Khokhlachova, Yu., Ostapov, S., Laptiev, O. (Eds.) (2023). Models of socio-cyber-physical systems security. Kharkiv: PC TECHNOLOGY CENTER, 184. doi: http://doi.org/10.15587/978-617-7319-72-5 Власний внесок 2,4 авторських аркушів. 2. Yevseiev, S., Hryshchuk, R., Molodetska, K., Nazarkevych, M., Hrytsyk, V., Milov, O. et. al.; Yevseiev, S., Hryshchuk, R., Molodetska, K., Nazarkevych, M. (Eds.) (2022). Modeling of security systems for critical infrastructure facilities. Kharkiv: PC TECHNOLOGY CENTER, 196. doi: http://doi.org/10.15587/978-617-7319-57-2 Власний внесок 2,2 авторських аркушів. П. 4 наявність виданих навчально-методичних посібників/посібників для самостійної роботи здобувачів вищої освіти та дистанційного навчання, електронних курсів на освітніх платформах ліцензіатів, конспектів лекцій/практикумів/методичних вказівок/рекомендацій/ робочих програм, інших друкованих

							навчально-методичних праць загальною кількістю три найменування 1. Основи математичного моделювання систем безпеки: робоча програма навчальної дисципліни [Електронний ресурс] : [для здобувачів] першого (бакалаврський) рівня вищої освіти денної форми навчання спец. 125 "Кібербезпека"/ розроб. С. В. Мілевський; Нац. техн. ун-т "Харків. політехн. ін-т". – Електрон. текст. дані. – Харків, 2022. – 34 с. – URI: http://repository.kpi.kharkov.ua/handle/KhPI-Press/63765 2. Технології управління безпекою бізнес-процесів: робоча програма навчальної дисципліни [Електронний ресурс] : [для здобувачів] другого (магістер.) рівня вищої освіти денної форми навчання спец. 125 "Кібербезпека" / розроб.: С. В. Мілевський ; Нац. техн. ун-т "Харків. політехн. ін-т". – Електрон. текст. дані. – Харків, 2022. – 21 с. – URI: http://repository.kpi.kharkov.ua/handle/KhPI-Press/63832. 3. Робоча програма навчальної дисципліни Математичні методи, моделі та інформаційні технології у наукових дослідженнях: [Електронний ресурс] : [для здобувачів] третього (доктор філософії) рівня вищої освіти очної та заочної форми навчання спец. 125 " Кібербезпека"/ розроб. С. В. Мілевський ; Нац. техн. ун-т "Харків. політехн. ін-т". – Електрон. текст. дані. – Харків, 2022. – 11 с. – URI: http://repository.kpi.kharkov.ua/handle/KhPI-Press/63700 4. Методичні вказівки до виконання магістерських робіт

							для студентів спеціальності F5 “Кібербезпека та захист інформації” / уклад. С. В. Мілевський, С. С. Погасій, О. Г. Король, І. В. Аксьонова, Т. С. Мілевська. – Харків: НТУ “ХПІ”. – 54 с. https://repository.kpi.kharkov.ua/items/4e23f899-8c3e-4990-b723-f56e40bb349a 5. Етичний хакінг : навчально-практичний посібник / уклад. О. В. Мілов, О. В. Шматко, С. В. Мілевський, О. Г. Король ; за заг. ред. С. П. Євсеєва. – Харків : НТУ «ХПІ», – Львів : «Новий Світ-2000», 2025. – 100 с. – (Серія «Кібербезпека та штучний інтелект»). ISBN 978-966-418-513-1 https://repository.kpi.kharkov.ua/items/5d29e96b-7457-4832-a886-fc952fcce7a5 П. 5 захист дисертації на здобуття наукового ступеня (*за останні 5 років) Доктор технічних наук, 05.13.21 – Системи захисту інформації, диплом ДД №013771 від 18.02.2025 р. Тема: “Методологія побудови систем безпеки мультимедійних ресурсів в інтернет-сервісах”. П. 10 участь у міжнародних наукових та/або освітніх проектах, залучення до міжнародної експертизи, наявність звання “суддя міжнародної категорії” Проект USAID «Кібербезпека критично важливої інфраструктури України», Security Audit and Risk Management, 15 June 2021 - 19 August 2021 United States Department of State Global Innovation through Science and Technology Initiative (GIST) GIST Innovates Ukraine 2021, June-August 2021 CRDF Global «Інтеграція курсів з кібербезпеки в навчальні плани українських університетів»

							07.02.2023-31.08.2023 П. 12 наявність апробаційних та/або науково-популярних, та/або консультаційних (дорадчих), та/або науково-експертних публікацій з наукової або професійної тематики загальною кількістю не менше п’яти публікацій 1. S. Yevseiev, S. Milevskyi, V. Sokol, Y. Melenti, O. Akhiiezer and K. Petrenko, "Methodological Foundations for Constructing Intelligent Information Security Systems," 2025 7th International Congress on Human-Computer Interaction, Optimization and Robotic Applications (ICHORA), Ankara, Turkiye, 2025, pp. 1-6, doi: 10.1109/ICHORA65333.2025.11017207 https://ieeexplore.ieee.org/document/11017207 2. R. Korolov, S. Milevskyi, L. Shcherbyna, Y. Lutsenko, S. Dunaiev and V. Stetsenko, "Authentication and Authorization Method Based on McEliece Crypto-Code Construction," 2024 8th International Symposium on Multidisciplinary Studies and Innovative Technologies (ISMSIT), Ankara, Turkiye, 2024, pp. 1-5, doi: 10.1109/ISMSIT63511.2024.10757296 https://ieeexplore.ieee.org/document/10757296 3. R. Korolov, D. Yevseiev, S. Milevskyi, O. Umanskiy, I. Shyian and Z. Sydorenko, "Development of a Lightweight Encryption Algorithm Based on Extended Galois Fields," 2024 International Congress on Human-Computer Interaction, Optimization and Robotic Applications (HORA), Istanbul, Turkiye, 2024, pp. 1-6, doi: 10.1109/HORA61326.2024.10550599 https://ieeexplore.ieee.org/document/10550599 4. S. Yevseiev, P. Murr, S. Milevskyi, O. Korol

							and M. Melnyk, "Development of a Sociocyberphysical Systems Cyber Threats Classifier," 2023 7th International Symposium on Multidisciplinary Studies and Innovative Technologies (ISMSIT), Ankara, Turkiye, 2023, pp. 1-7, doi: 10.1109/ISMSIT58785.2023.10304895 5. S. Herasymov, V. Soroka, S. Yevseiev, S. Milevskyi and S. Pohasii, "Phase-Modulated Signals Synthesis Method to Control Information Transmission Channels," 2023 IEEE 4th KhPI Week on Advanced Technology (KhPIWeek), Kharkiv, Ukraine, 2023, pp. 1-5, doi: 10.1109/KhPIWeek61412.2023.10312859 https://ieeexplore.ieee.org/document/10312859 6. N. Dzheniuk, S. Milevskyi, B. Lazurenko, A. Serkov and A. Zakharzhevskyi, "Sociocyberphysical Security Systems Synthesis Models," 2023 7th International Symposium on Multidisciplinary Studies and Innovative Technologies (ISMSIT), Ankara, Turkiye, 2023, pp. 1-5, doi: 10.1109/ISMSIT58785.2023.10304965 https://ieeexplore.ieee.org/document/10304965 7. S. Herasymov, V. Soroka, S. Milevskyi, N. Voropay, H. Zviertsev and Y. Motalyhin, "Development of a Method for Digital Synthesis of Electrical Signals with a Normalized Harmonic Coefficient," 2023 5th International Congress on Human-Computer Interaction, Optimization and Robotic Applications (HORA), Istanbul, Turkiye, 2023, pp. 1-5, doi: 10.1109/HORA58378.2023.10156678 https://ieeexplore.ieee.org/document/10156678 П. 13 проведення навчальних занять із спеціальних дисциплін іноземною мовою (крім дисциплін мовної

							підготовки) в обсязі не менше 50 аудиторних годин на навчальний рік Computer networks – 64 години (2 курс сп. F5, група КН-1124ia.e), Fundamentals of social engineering – 16 годин (2 курс сп. F5, група КН-1124ia.e) П. 19 діяльність за спеціальністю у формі участі у професійних та/або громадських об'єднаннях асоційований член Громадської організації "Association of STEM researchers and inventors" довідка №3 від 7.10.2021р. Член громадської організації "Східноєвропейське наукове товариство", свідоцтво ES № 059
410244	Мілевський Станіслав Валерійович	Професор, Основне місце роботи	Навчально-науковий інститут комп'ютерних наук та інформаційних технологій	Диплом спеціаліста, Харківський державний економічний університет, рік закінчення: 2001, спеціальність: 0501 Економіка підприємства, Диплом магістра, Національний авіаційний університет, рік закінчення: 2021, спеціальність: 125 Кібербезпека, Диплом доктора наук ДД 013771, виданий 18.02.2025, Диплом кандидата наук ДК 033701, виданий 13.04.2006, Атестат доцента 12ДЦ 023152, виданий 17.06.2010, Атестат доцента АД 006043, виданий 26.11.2020	19	Математичні моделі управління ІТ проєктами	Підвищення кваліфікації Стажування в Університеті національного комітету освіти у Кракові (Польща) на кафедрі інженерії програмного забезпечення за напрямом «Методи та технічні засоби захисту інформації» тривалістю 180 годин (6 кредитів), сертифікат №КІО/23-04-17/2025 від 23.04.2025 р., затверджено наказом №2186С від 21.11.2025р. Пункти відповідності ліцензійних умов: П. 1, 3, 4, 5, 10, 12, 13, 19 П. 1 наявність не менше п'яти публікацій у періодичних наукових виданнях, що включені до переліку фахових видань України, до наукометричних баз, зокрема Scopus, Web of Science Core Collection 1. Yevseiev, S., Milevskyi, S., Melenti, Y., Voitko, O., Aleksieiev, M., Morklyanyk, B., Povaliaiev, S., Shvorak, R., Sevriukova, Y., & Rykov, D. (2025). Development of a method for assessing the society national security level based on the triple helix concept. Eastern-European Journal of Enterprise

Technologies, 4(4 (136), 32–45. https://doi.org/10.15587/1729-4061.2025.337398

2. Melenti, Y., Korol, O., Shulha, V., Milevskyi, S., Sievierinov O., Voitko, O., Rzayev, K., Husarova, I., Kravchenko, S., & Pashayeva, S. (2025). Development of post-quantum cryptosystems based on the Rao-Nam scheme. Eastern-European Journal of Enterprise Technologies, 1(9 (133), 35–48. ISSN (print) 1729-3774, ISSN (on-line) 1729-406 https://doi.org/10.15587/1729-4061.2025.323195

3. Shmatko, O., Herasymov, S., Milevskyi, S., Balitskyi, N., Pohasii, S., Aleksieiev, M., Vlasov, I., Melenti, Y., Kovalenko, Y., & Peleshok, Y. (2025). Development of a method for assessing the efficiency of technical systems' computer dynamic simulators. Eastern-European Journal of Enterprise Technologies, 2(9 (134), 50–61. ISSN (print) 1729-3774, ISSN (on-line) 1729-406 https://doi.org/10.15587/1729-4061.2025.327558

4. Yevseiev, S., Milevskyi, S., Pribyliev, Y., Melenti, Y., Nalivayko, A., Bazarnyi, S., Morozov, O., Kazak, I., Hrebeniuk, A., & Ivashchenko, O. (2025). Development of a method of psychological impact on target audiences of gamers using modern information technologies. Eastern-European Journal of Enterprise Technologies, 3(9 (135), 55–64. ISSN (print) 1729-3774, ISSN (on-line) 1729-406 https://doi.org/10.15587/1729-4061.2025.332271

5. Yevseiev, S., Milevskyi, S., Sokol, V., Yemanov, V., Volobuiev, A., Dakova, L., Brailovskyi, M.,

Rahimova, I., Kravchenko, V., & Cherniavskiy, O. (2024). Development of functionality principles for the automated data transmission system through wireless communication channels to ensure information protection . Eastern-European Journal of Enterprise Technologies, 4(9 (130), 18–33. https://doi.org/10.15587/1729-4061.2024.310547

6. Shmatko, O., Yevseiev, S., Dudykevych, V., Milevskyi, S., Solnyshkova, S., Havrylova, A., Shestak, Y., Oriekhov, S., Korsunov, S., & Kravchenko, S. (2024). Development of a method for synthesizing an information-analytical system for assessing the level of information transmission channels protection. Eastern-European Journal of Enterprise Technologies, 2(9 (128), 36–43. https://doi.org/10.15587/1729-4061.2024.302495

7. Milevskyi, S., Korol, O., Mykytyn, G., Lozova, I., Solnyshkova, S., Husarova, I., Hrebeniuk, A., Vlasov, A., Sukhoteplyi, V., & Balagura, D. (2024). Development of the sociocyberphysical systems` multi-contour security methodology. Eastern-European Journal of Enterprise Technologies, 1(9 (127), 34–51. https://doi.org/10.15587/1729-4061.2024.298844

8. Murr, P., Yevseiev, S., Milevskyi, S., Melnyk, M., Katsalap, V., Pribyliev, Y., Rzayev, K., Bryla, A., Shpak, O., & Fedorka, P. (2023). Development of an error correction method using perfect binary arrays. Eastern-European Journal of Enterprise Technologies, 4(9 (124), 45–53. https://doi.org/10.15587/1729-4061.2023.285540

							9. Yevseiev, S., Havrylova, A., Milevskyi, S., Sinitsyn, I., Chalapko, V., Dukin, H., Hrebeniuk, V., Diedov, M., Bekirova, L., & Shpak, O. (2023). Development of an improved SSL/TLS protocol using post-quantum algorithms. Eastern-European Journal of Enterprise Technologies, 3(9 (123), 33–48. https://doi.org/10.15587/1729-4061.2023.281795 П. 3 наявність виданого підручника чи навчального посібника (включаючи електронні) або монографії (загальним обсягом не менше 5 авторських аркушів), в тому числі видані у співавторстві (обсягом не менше 1,5 авторського аркуша на кожного співавтора) (*за наявності надати лінк або бібліографічний опис) 1. Yevseiev, S., Khokhlachova, Yu., Ostapov, S., Laptiev, O., Korol, O., Milevskyi, S. et. al.; Yevseiev, S., Khokhlachova, Yu., Ostapov, S., Laptiev, O. (Eds.) (2023). Models of socio-cyber-physical systems security. Kharkiv: PC TECHNOLOGY CENTER, 184. doi: http://doi.org/10.15587/978-617-7319-72-5 Власний внесок 2,4 авторських аркушів. 2. Yevseiev, S., Hryshchuk, R., Molodetska, K., Nazarkevych, M., Hrytsyk, V., Milov, O. et. al.; Yevseiev, S., Hryshchuk, R., Molodetska, K., Nazarkevych, M. (Eds.) (2022). Modeling of security systems for critical infrastructure facilities. Kharkiv: PC TECHNOLOGY CENTER, 196. doi: http://doi.org/10.15587/978-617-7319-57-2 Власний внесок 2,2 авторських аркушів. П. 4 наявність виданих навчально-методичних посібників/посібників для самостійної роботи здобувачів вищої освіти та

							дистанційного навчання, електронних курсів на освітніх платформах ліцензіатів, конспектів лекцій/практикумів/методичних вказівок/рекомендацій/ робочих програм, інших друкованих навчально-методичних праць загальною кількістю три найменування 1. Основи математичного моделювання систем безпеки: робоча програма навчальної дисципліни [Електронний ресурс] : [для здобувачів] першого (бакалаврський) рівня вищої освіти денної форми навчання спец. 125 "Кібербезпека"/ розроб. С. В. Мілевський; Нац. техн. ун-т "Харків. політехн. ін-т". – Електрон. текст. дані. – Харків, 2022. – 34 с. – URI: http://repository.kpi.kharkov.ua/handle/KhPI-Press/63765 2. Технології управління безпекою бізнес-процесів: робоча програма навчальної дисципліни [Електронний ресурс] : [для здобувачів] другого (магістер.) рівня вищої освіти денної форми навчання спец. 125 "Кібербезпека" / розроб.: С. В. Мілевський ; Нац. техн. ун-т "Харків. політехн. ін-т". – Електрон. текст. дані. – Харків, 2022. – 21 с. – URI: http://repository.kpi.kharkov.ua/handle/KhPI-Press/63832. 3. Робоча програма навчальної дисципліни Математичні методи, моделі та інформаційні технології у наукових дослідженнях: [Електронний ресурс] : [для здобувачів] третього (доктор філософії) рівня вищої освіти очної та заочної форми навчання спец. 125 " Кібербезпека"/ розроб. С. В. Мілевський ; Нац. техн. ун-т "Харків.

							політехн. ін-т". – Електрон. текст. дані. – Харків, 2022. – 11 с. – URI: http://repository.kpi.kharkov.ua/handle/KhPI-Press/63700 4. Методичні вказівки до виконання магістерських робіт для студентів спеціальності F5 “Кібербезпека та захист інформації” / уклад. С. В. Мілевський, С. С. Погасій, О. Г. Король, І. В. Аксьонова, Т. С. Мілевська. – Харків: НТУ “ХПІ”. – 54 с. https://repository.kpi.kharkov.ua/items/4e23f899-8c3e-4990-b723-f56e40bb349a 5. Етичний хакінг : навчально-практичний посібник / уклад. О. В. Мілов, О. В. Шматко, С. В. Мілевський, О. Г. Король ; за заг. ред. С. П. Євсеєва. – Харків : НТУ «ХПІ», – Львів : «Новий Світ-2000», 2025. – 100 с. – (Серія «Кібербезпека та штучний інтелект»). ISBN 978-966-418-513-1 https://repository.kpi.kharkov.ua/items/5d29e96b-7457-4832-a886-fc952fcce7a5 П. 5 захист дисертації на здобуття наукового ступеня (*за останні 5 років) Доктор технічних наук, 05.13.21 – Системи захисту інформації, диплом ДД №013771 від 18.02.2025 р. Тема: “Методологія побудови систем безпеки мультимедійних ресурсів в інтернет-сервісах”. П. 10 участь у міжнародних наукових та/або освітніх проектах, залучення до міжнародної експертизи, наявність звання “суддя міжнародної категорії” Проект USAID «Кібербезпека критично важливої інфраструктури України», Security Audit and Risk Management, 15 June 2021 - 19 August 2021 United States Department of State Global Innovation

							through Science and Technology Initiative (GIST) GIST Innovates Ukraine 2021, June-August 2021 CRDF Global «Інтеграція курсів з кібербезпеки в навчальні плани українських університетів» 07.02.2023-31.08.2023 П. 12 наявність апробаційних та/або науково-популярних, та/або консультаційних (дорадчих), та/або науково-експертних публікацій з наукової або професійної тематики загальною кількістю не менше п’яти публікацій 1. S. Yevseiev, S. Milevskyi, V. Sokol, Y. Melenti, O. Akhiiezer and K. Petrenko, "Methodological Foundations for Constructing Intelligent Information Security Systems," 2025 7th International Congress on Human-Computer Interaction, Optimization and Robotic Applications (ICHORA), Ankara, Turkiye, 2025, pp. 1-6, doi: 10.1109/ICHORA65333.2025.11017207 https://ieeexplore.ieee.org/document/11017207 2. R. Korolov, S. Milevskyi, L. Shcherbyna, Y. Lutsenko, S. Dunaiev and V. Stetsenko, "Authentication and Authorization Method Based on McEliece Crypto-Code Construction," 2024 8th International Symposium on Multidisciplinary Studies and Innovative Technologies (ISMSIT), Ankara, Turkiye, 2024, pp. 1-5, doi: 10.1109/ISMSIT63511.2024.10757296 https://ieeexplore.ieee.org/document/10757296 3. R. Korolov, D. Yevseiev, S. Milevskyi, O. Umanskiy, I. Shyian and Z. Sydorenko, "Development of a Lightweight Encryption Algorithm Based on Extended Galois Fields," 2024 International Congress on Human-Computer Interaction, Optimization and

Robotic Applications (HORA), Istanbul, Turkiye, 2024, pp. 1-6, doi: 10.1109/HORA61326.2024.10550599 https://ieeexplore.ieee.org/document/10550599
4. S. Yevseiev, P. Murr, S. Milevskyi, O. Korol and M. Melnyk, "Development of a Sociocyberphysical Systems Cyber Threats Classifier," 2023 7th International Symposium on Multidisciplinary Studies and Innovative Technologies (ISMSIT), Ankara, Turkiye, 2023, pp. 1-7, doi: 10.1109/ISMSIT58785.2023.10304895
5. S. Herasymov, V. Soroka, S. Yevseiev, S. Milevskyi and S. Pohasii, "Phase-Modulated Signals Synthesis Method to Control Information Transmission Channels," 2023 IEEE 4th KhPI Week on Advanced Technology (KhPIWeek), Kharkiv, Ukraine, 2023, pp. 1-5, doi: 10.1109/KhPIWeek61412.2023.10312859 https://ieeexplore.ieee.org/document/10312859
6. N. Dzheniuk, S. Milevskyi, B. Lazurenko, A. Serkov and A. Zakharzhevskyi, "Sociocyberphysical Security Systems Synthesis Models," 2023 7th International Symposium on Multidisciplinary Studies and Innovative Technologies (ISMSIT), Ankara, Turkiye, 2023, pp. 1-5, doi: 10.1109/ISMSIT58785.2023.10304965 https://ieeexplore.ieee.org/document/10304965
7. S. Herasymov, V. Soroka, S. Milevskyi, N. Voropay, H. Zviertsev and Y. Motalyhin, "Development of a Method for Digital Synthesis of Electrical Signals with a Normalized Harmonic Coefficient," 2023 5th International Congress on Human-Computer Interaction, Optimization and Robotic Applications (HORA), Istanbul, Turkiye, 2023, pp. 1-5, doi:

							10.1109/HORA58378.2023.10156678 https://ieeexplore.ieee.org/document/10156678 П. 13 проведення навчальних занять із спеціальних дисциплін іноземною мовою (крім дисциплін мовної підготовки) в обсязі не менше 50 аудиторних годин на навчальний рік Computer networks – 64 години (2 курс сп. F5, група КН-1124ia.e), Fundamentals of social engineering – 16 годин (2 курс сп. F5, група КН-1124ia.e) П. 19 діяльність за спеціальністю у формі участі у професійних та/або громадських об'єднаннях асоційований член Громадської організації "Association of STEM researchers and inventors" довідка №3 від 7.10.2021р. Член громадської організації "Східноєвропейське наукове товариство", свідоцтво ES № 059
409404	Король Ольга Григорівна	Доцент, Основне місце роботи	Навчально-науковий інститут комп'ютерних наук та інформаційних технологій	Диплом молодшого спеціаліста, Харківський патентно-комп'ютерний коледж, рік закінчення: 2001, спеціальність: 080405 Програмування для електронно-обчислювальної техніки і автоматизованих систем, Диплом спеціаліста, Харківський національний економічний університет, рік закінчення: 2005, спеціальність: 080401 Інформаційні управляючі системи та технології, Диплом кандидата наук ДК 020725, виданий 03.04.2014, Атестат доцента 12ДЦ 045523, виданий	19	Аналіз шкідливих програм	Підвищення кваліфікації Certificate of Completion №KIO/23-04-01/2025 "Methods and technical means of information protection" (Krakow, Poland) (from 20 february, 2025 to 20 april 2025, затверджено наказом ректора НТУ ХПІ №2186С від 21.11.2025р) (6 ects-credits – 180 hours) Пункти відповідності ліцензійних умов: п. 1-4,6, 8, 12,19 П. 1. наявність не менше п'яти публікацій у періодичних наукових виданнях, що включені до переліку фахових видань України, до наукометричних баз, зокрема Scopus, Web of Science Core Collection. 1. Korol O. and other. Research of collision propeties of the modified UMAC algorithm on crypto-code constructions. "EUREKA: Physical Sciences and Engineering", № 1. – 2022. P. 34–44. (Scopus) – Режим

				15.12.2015			доступу: https://journal.eu-jr.eu/engineering/article/view/2213. 2. Korol O. and other. Development of post-quantum cryptosystems based on the Rao-Nam scheme. Eastern-European Journal of Enterprise Technologies. 1/9 (133) 2025. p. 35–48. (Scopus) – Режим доступу: https://journals.uran.ua/eejet/article/view/323195 3. Havrylova A., Korol O., Voropay N., Sevriukova Y., Bondarenko K. Analysis of cryptographic authentication and manipulation detection methods for big data // Сучасний захист інформації, 2024, №1(57) P. 97 – 102. DOI: 10.31673/2409-7292.2024.010011 (фахове видання) https://repository.kpi.kharkov.ua/handle/KhPI-Press/88594 4. MODELS OF SOCIO-CYBER-PHYSICAL SYSTEMS SECURITY Yevseiev, S., Khokhlachova, Y., Ostapov, S., ... Milov O., Tolkachov, M. // Models of Socio-Cyber-Physical Systems Security, 2023, pp. 1–168 (Scopus) https://monograph.com.ua/catalog/book/978-617-7319-72-5 5. Milevskyi, S., Korol, O., Mykytyn, G., Lozova, I., Solnyshkova, S., Husarova, I., Hrebeniuk, A., Vlasov, A., Sukhoteplyi, V., & Balagura, D. (2024). Development of the sociocyberphysical systems` multi-contour security methodology. Eastern-European Journal of Enterprise Technologies, 1(9 (127), 34–51. https://doi.org/10.15587/1729-4061.2024.298844. https://journals.uran.ua/eejet/article/view/298844 П. 2 наявність одного патенту на винахід або п’яти деклараційних патентів на винахід чи корисну модель, включаючи секретні, або наявність не менше п’яти свідоцтв про реєстрацію авторського права на твір.

							1. Пат. u202103665, МПК (51) G009C 1/00;Спосіб криптографічного перетворення інформації. Заявл. 23.06.2021; Опубл. 01.12.2021 р 2. Пат. u202103680, МПК (51) G009C 1/00;Спосіб криптографічного перетворення інформації. Заявл. 23.06.2021; Опубл. 01.12.2021 р 3. Пат. u202103683, МПК (51) G009C 1/00; Спосіб криптографічного перетворення інформації. Заявл. 23.06.2021; Опубл. 01.12.2021 р. 4. Пат. u202103704, МПК (51) G009C 1/00; Спосіб криптографічного перетворення інформації. Заявл. 23.06.2021; Опубл. 01.12.2021 р. 5. Пат. u202103617, МПК (51) G009C 1/00; Спосіб криптографічного перетворення інформації. Заявл. 23.06.2021; Опубл. 01.12.2021 р. П. 3 наявність виданого підручника чи навчального посібника (включаючи електронні) або монографії (загальним обсягом не менше 5 авторських аркушів), в тому числі видані у співавторстві (обсягом не менше 1,5 авторського аркуша на кожного співавтора). 1. Євсеєв С.П., Дженюк Н.В., Толкачов М.Ю., Во-ропай Н.І. Технології комп'ютерних мереж. Харків – Львів: Вид-во ПП "Новий Світ – 2000", 2023. Власний внесок 5,9 авторських аркушів. 2. Євсеєв С.П., Дженюк Н.В., Толкачов М.Ю., Касілов О.В., Король О.Г., Кудій Д.А. Комп'ютерні мережі. Книга 2. Архітектура комп'ютерів. Навч. посібник Харків, – Львів: Видавництво ПП «Новий Світ – 2000», 2025. – 320 с Власний внесок 4,3 авторських аркушів. П.4 наявність виданих навчально-

							методичних посібників/посібників для самостійної роботи здобувачів вищої освіти та дистанційного навчання, електронних курсів на освітніх платформах ліцензіатів, конспектів лекцій/практикумів/методичних вказівок/рекомендацій/ робочих програм, інших друкованих навчально-методичних праць загальною кількістю три найменування. 1. Етичний хакінг. навчально-практичний посібник / уклад. О. В. Мілов, О. В. Шматко, С. В. Мілевський, О. Г. Король ; за заг. ред. С. П. Євсеєва. – Харків : НТУ «ХПІ», – Львів : «Новий Світ-2000», 2025. – 100 с. ISBN 978-966-418-513-1 2. Погасій С.С., КорольО.Г., Аксьонова І.В., Мілевська Т.С., Мілевський С.В. Методичні вказівки до виконання магістерських дипломних робіт: для студентів спец. F5 “Кібербезпека та захист інформації” денної та заочної форм навчання. Харків: НТУ «ХПІ», 2025.
							П. 6 наукове керівництво (консультування) здобувача, який одержав документ про присудження наукового ступеня 1. Лаптєва Тетяна Олександрівна, доктор філософії, 125 – Кібербезпека та захист інформації, тема дисертації: Методи виявлення дезінформації на основі експертних оцінок, 2025 рік. Диплом Н25 №001079 від 30 травня 2025 року, Міністерство освіти і науки України. Національний технічний університет “Харківський політехнічний інститут”. 2. Дженюк Наталія Володимирівна, доктор філософії, 125 – Кібербезпека, тема дисертації: Моделі синтезу систем безпеки

							соціокіберфізичних систем, 2025 рік, Диплом Н25 №003259 від 18.09.2025 року, Міністерство освіти і науки України. Національний технічний університет “Харківський політехнічний інститут”. 3. Толкачов Максим Юрійович, доктор філософії, 125 – Кібербезпека тема дисертації: Моделювання безпеки інтернет-трафіку як семіотичної системи, 2025 рік, Диплом Н25№003260 від 18.09.2025 року, Міністерство освіти і науки України. Національний технічний університет “Харківський політехнічний інститут”. П. 8 виконання функцій (повноважень, обов’язків) наукового керівника або відповідального виконавця наукової теми (проекту), або головного редактора/члена редакційної колегії/експерта (рецензента) наукового видання, включеного до переліку фахових видань України, або іноземного наукового видання, що індексується в бібліографічних базах Відповідальний виконавець госпдоговірної НДР №403-46 від 29.11.2021 р. П. 12 наявність апробаційних та/або науково-популярних, та/або консультаційних (дорадчих), та/або науково-експертних публікацій з наукової або професійної тематики загальною кількістю не менше п’яти публікацій 1. Євсеєв С., Король О. Багатоконтурні системи безпеки об’єктів критичної інфраструктури/ XIV наукова конференція «Наукові підсумки 2025 року». С.40. https://entc.com.ua/uk/konferentsii/610-naukovi-pidsumky-roku. 2.Yevseiev S., Pohasii

							S., Milevskyi S., Korol O. Development of a Method for Comprehensive Evaluation of the Service Provision Quality/ International Congress Digitalization in Additive Manufacturing (Included in the following conference series: International Congress on 3D Printing (Additive Manufac-turing) Technologies and Digital Industry, 2025. https://link.springer.com/book/10.1007/978-3-031-84873-5 3. S. Herasymov, V. Soroka, S. Milevskyi, O. Korol, I. Aksonova and V. Stetsenko, "Method for Reducing the Frequency Spectrum Overlaying Error in Digital Narrow-Band Filtration," 2024 International Congress on Human-Computer Interaction, Optimization and Robotic Applications (HORA), Istanbul, Turkiye, 2024, pp. 1-5, doi: 10.1109/HORA61326.2024.10550889// https://ieeexplore.ieee.org/abstract/document/10550889 4. Yevseiev S., Murr P., Milevskyi S., Korol O., Melnyk M. Development of a Sociocyberphysical Systems Cyber Threats Classifier. 2023 7th International Symposium on Multidisci-plinary Studies and Innovative Technologies (ISMSIT), 2023. https://ieeexplore.ieee.org/document/10304895 5. Crypto Code Constructions in Post-Quantum Cryptography A Tkachov, O Korol, N Voropay, S Dunaiev... - 2025, 7th International Congress on Human-Computer ..., 2025 (P. 1-6). // https://ieeexplore.ieee.org/abstract/document/11016982 П. 19 діяльність за спеціальністю у формі участі у професійних та/або громадських об'єднаннях Членкиня Громадської організації "СХІДНО-ЄВРОПЕЙСЬКЕ

							НАУКОВЕ ТОВАРИСТВО” з 20.05.2022 р. посвідчення № ES 057
410246	Хвостенко Владислав Сергійович	Доцент, Основне місце роботи	Навчально-науковий інститут комп’ютерних наук та інформаційних технологій	Диплом бакалавра, Харківський національний економічний університет, рік закінчення: 2005, спеціальність: 0501 Економіка і підприємництво, Диплом спеціаліста, Харківський національний економічний університет, рік закінчення: 2007, спеціальність: 050107 Економічна статистика, Диплом магістра, Харківський національний економічний університет, рік закінчення: 2006, спеціальність: 050104 Фінанси, Диплом магістра, Відокремлений структурний підрозділ "Інститут інтелектуальної власності Національного університету "Одеська юридична академія" в м. Києві, рік закінчення: 2014, спеціальність: Інтелектуальна власність, Диплом кандидата наук ДК 008014, виданий 26.09.2012, Атестат доцента АД 003303, виданий 15.10.2019, Атестат доцента АД 006909, виданий 09.02.2021	18	Авторське право у цифровому суспільстві	Підвищення кваліфікації Стажування в Університеті національного комітету освіти у Кракові (Польща) на кафедрі інженерії програмного забезпечення за напрямом «Методи та технічні засоби захисту інформації» тривалістю 180 годин (6 кредитів), сертифікат №KIO/23-04-18/2025 від 23.04.2025 р., затверджено наказом №2186С від 21.11.2025р. Пункти відповідності ліцензійних умов: П. 1, 2, 4, 8, 12, 13, 19 20 П. 1 наявність не менше п’яти публікацій у періодичних наукових виданнях, що включені до переліку фахових видань України, до наукометричних баз, зокрема Scopus, Web of Science Core Collection 1. Alla Havrylova, Yuliia Khokhlachova, Andrii Tkachov, Natalia Voropay, Vladyslav Khvostenko. Justification of directions for improving authentication protocols in information and communication systems. Ukrainian Information Security Research Journal. 2023. № 1 (25). P. 6-19. https://jrnl.nau.edu.ua/index.php/ZI/article/view/17593 2. Khvostenko V., Havrylova A., Milevskyi S. Development of an Advanced SSL/TLS Protocol for Transferring Requests to a 3D-Printer // Springer Tracts in Additive Manufacturing. – 2025. – Part F641. – P. 489–503. – DOI: [SpringerLink] – Індексується в Scopus. – 0,94 авт. арк. https://link.springer.com/chapter/10.1007/978-3-031-84873-5_38 3. Khvostenko V., Milevskyi S., Bukatych

							I., Yevseiev D., Iegrashyn O., Kyryk V. Smart Contracts: Classification Problems // Proc. 7th International Congress on Human-Computer Interaction, Optimization and Robotic Applications (ICHORA 2025). – IEEE, 2025. – DOI: https://www.ichoracongress.com/ichora2025/ICHORA2025_Congress_Information.pdf – 0,04 авт. арк. 4. Androshchuk H., Khvostenko V. Digital tools for determining intellectual property object notoriety (on the example of character and work notoriety) // Information and Law. – 2024. – № 3(50). – P. 54–64. – DOI: https://doi.org/10.37750/2616-6798.2024.3(50).311635 – Категорія Б (фахове видання України, індексується в Index Copernicus). – 0,7 ум. друк. арк. / внесок 0,35 авт. арк. 5. Dunayev S., Milevska T., Voropay N., Murr P., Khvostenko V., Sevriukova Y. Research of Technologies and Methods of Web Application Protection in the Infrastructure of a Higher Education Institution with the Assistance of Specialized Systems // Proc. International Congress on Human-Computer Interaction, Optimization and Robotic Applications (HORA 2024). – IEEE, 2024. – 0,25 авт. арк. https://jglobal.jst.go.jp/en/detail?JGLOBAL_ID=202402257602422312&utm_source=chatgpt.com 6. Melenti Y., Yevseiev S., Korol O., Milevskyi S., Khvostenko V. Application of the innovative approach in the modernization of higher education institutions of the Security Service of Ukraine // Ukrainian Scientific Journal of Information Security. – 2024. – Vol. 30, No. 1. – P. 179–189. – DOI: https://doi.org/10.18372/2225-5036.30.18619 7. Розумний С. М., Воліков В. В.,

							Хвостенко В. С. The influence of the methodology functions on the quality of solving an expert task // Науковий журнал судових експертів Міністерства юстиції України. – 2024. – № 1(9). – С. 28–35. – DOI: https://doi.org/10.32782/2708-1834/2024-09.2 8. Molodetska K., Veretiuk S., Rahimova I., Milevskyi S., Khvostenko V. Information Influence on the Virtual Community: Implementation Features and Method of Detection in Social Internet Services // Proc. 7th International Symposium on Multidisciplinary Studies and Innovative Technologies (ISMSIT 2023). – IEEE, 2023. – Індексується в Scopus. https://www.scopus.com/pages/publications/85179132580 9. Kondratenko Y., Korobkin D., Dunayev S., Khvostenko V. Design and Evaluation of an AIOT-Based Medical Information System // Ukrainian Information Security Research Journal. – 2023. – (Категорія Б, фахове видання України, входить до баз Index Copernicus). https://jrnl.nau.edu.ua/index.php/ZI/article/view/17594 10. Havrylova Alla, Khvostenko V., et al. Justification of Directions for Improving Authentication Protocols in Information and Communication Systems // Ukrainian Information Security Research Journal. – 2023. – (Категорія Б, індексується у фахових базах, Index Copernicus). DOI: 10.18372/2410-7840.25.17593 П. 2 наявність одного патенту на винахід або п’яти деклараційних патентів на винахід чи корисну модель, включаючи секретні, або наявність не менше п’яти свідоцтв про реєстрацію авторського права на твір

							Патенти на корисну модель: 1. Патент u202103704 від 29.06.2021 СПОСІБ КРИПТОГРАФІЧНОГО ПЕРЕТВОРЕННЯ ІНФОРМАЦІЇ 2. Патент u202103665 від 25.06.2021 СПОСІБ КРИПТОГРАФІЧНОГО ПЕРЕТВОРЕННЯ ІНФОРМАЦІЇ 3. Патент u202103617 від 23.06.2021 СПОСІБ КРИПТОГРАФІЧНОГО ПЕРЕТВОРЕННЯ ІНФОРМАЦІЇ 4. Патент u202103615 від 23.06.2021 СПОСІБ КРИПТОГРАФІЧНОГО ПЕРЕТВОРЕННЯ ІНФОРМАЦІЇ 5. Патент u202103683 від 23.07.2021 СПОСІБ КРИПТОГРАФІЧНОГО ПЕРЕТВОРЕННЯ ІНФОРМАЦІЇ 6. Патент u202103680 від 25.06.2021 СПОСІБ КРИПТОГРАФІЧНОГО ПЕРЕТВОРЕННЯ ІНФОРМАЦІЇ П. 4 наявність виданих навчально-методичних посібників/посібників для самостійної роботи здобувачів вищої освіти та дистанційного навчання, електронних курсів на освітніх платформах ліцензіатів, конспектів лекцій/практикумів/методичних вказівок/рекомендацій/ робочих програм, інших друкованих навчально-методичних праць загальною кількістю три найменування 1. Intellectual Property: syllabus for students of specialty 113, Master's level [Електронне видання] / comp. V. S. Khvostenko. – Kharkiv: NTU «KhPI», 2024. – (Eng. lang.). – Режим доступу: https://web.kpi.kharkov.ua/kmmm/wp-content/uploads/sites/110/2024/12/GS-3_Intellectual_Property_Syllabus_Master_113_Khvostenko-V.S._ENG_2024.pdf 2. Господарське право: робоча програма навчальної

							дисципліни для здобувачів другого (магістерського) рівня спеціальності 125 «Кібербезпека» [Електронне видання] / уклад. В. С. Хвостенко. – Харків: НТУ «ХПІ», 2022. – (Укр. мов.). – Режим доступу: http://repository.kpi.kharkov.ua/handle/KhPI-Press/63734 3. Захист інтелектуальної власності: робоча програма навчальної дисципліни для здобувачів другого (магістерського) рівня спеціальності 125 «Кібербезпека» [Електронне видання] / уклад. В. С. Хвостенко. – Харків: НТУ «ХПІ», 2022. – 17 с. – (Укр. мов.). – Режим доступу: http://repository.kpi.kharkov.ua/handle/KhPI-Press/63733 4. Правове забезпечення діяльності у сфері безпеки: робоча програма навчальної дисципліни для здобувачів другого (магістерського) рівня спеціальності 125 «Кібербезпека» [Електронне видання] / уклад. В. С. Хвостенко, А. А. Гаврилова. – Харків: НТУ «ХПІ», 2022. – (Укр. мов.). – Режим доступу: http://repository.kpi.kharkov.ua/handle/KhPI-Press/63735 5. Правове регулювання інформаційної безпеки: робоча програма навчальної дисципліни для здобувачів другого (магістерського) рівня спеціальності 125 «Кібербезпека» [Електронне видання] / уклад. В. С. Хвостенко. – Харків: НТУ «ХПІ», 2022. – (Укр. мов.). – Режим доступу: https://web.kpi.kharkov.ua/kmmm/wp-content/uploads/sites/110/2024/04/VP-3.2.1_Pravove_regulyuvannya_informatsijnoyi_bezpeky_Sylabus_113_Bakalavr_Hvostenko-V.S._UKR_2023-24.pdf

							6. Технології баз даних : навчально-практичний посібник / уклад. А. А. Гаврилова, С. С. Погасій, Р. В. Корольов, В. С. Хвостенко, Т. С. Мілевська ; за заг. ред. С. П. Євсеєва. – Харків : НТУ «ХПІ», – Львів : «Новий Світ-2000», 2025. – 222 с. Технології баз даних : навчально-практичний посібник – Новий Світ 2000 П. 8 виконання функцій (повноважень, обов'язків) наукового керівника або відповідального виконавця наукової теми (проекту), або головного редактора/члена редакційної колегії/експерта (рецензента) наукового видання, включеного до переліку фахових видань України, або іноземного наукового видання, що індексується в бібліографічних базах Виконання функцій рецензента міжнародного наукового видання Asian Journal of Research in Computer Science https://journalajrcos.com/ (Certificate of Excellence in Reviewing, 2025). Іноземне наукове видання, що індексується у міжнародних бібліографічних базах П. 12 наявність апробаційних та/або науково-популярних, та/або консультаційних (дорадчих), та/або науково-експертних публікацій з наукової або професійної тематики загальною кількістю не менше п'яти публікацій Хвостенко В.С., Мілевський С., Букатич І., Євсеєв Д., Єграшин О., Кирик В. Smart Contracts: Classification Problems // Матеріали 7th International Congress on Human-Computer Interaction, Optimization and Robotic Applications (ICHORA 2025): збірник матеріалів. – IEEE, 2025. –

							[Електронний ресурс]. – Режим доступу: https://set-science.com/org/ichora2025/news/ICHORA2025_news_1.pdf Дунаєв С., Мілевська Т., Воропай Н., Murr P., Хвостенко В., Севрюкова Є. Research of Technologies and Methods of Web Application Protection in the Infrastructure of a Higher Education Institution with the Assistance of Specialized Systems // Матеріали International Congress on Human-Computer Interaction, Optimization and Robotic Applications (HORA 2024): збірник матеріалів. – IEEE, 2024. – [Електронний ресурс]. – DOI: 10.1109/HORA61326.2024.10550503 Molodetska K., Veretiuk S., Rahimova I., Milevskyi S., Khvostenko V. Information Influence on the Virtual Community: Implementation Features and Method of Detection in Social Internet Services // Proc. 7th International Symposium on Multidisciplinary Studies and Innovative Technologies (ISMSIT 2023). – IEEE, 2023. – Індексується в Scopus. https://www.scopus.com/pages/publications/85179132580 9. Kondratenko Y., Korobkin D., Dunayev S., Khvostenko V. Design and Evaluation of an AIOT-Based Medical Information System // Ukrainian Information Security Research Journal. – 2023. – (Категорія Б, фахове видання України, входить до баз Index Copernicus). https://jrnl.nau.edu.ua/index.php/ZI/article/view/17594 10. Havrylova Alla, Khvostenko V., et al. Justification of Directions for Improving Authentication Protocols in Information and Communication Systems // Ukrainian Information Security Research Journal. – 2023. – (Категорія Б, індексується у

							фахових базах, Index Copernicus). DOI: 10.18372/2410-7840.25.17593 Synergy of building cybersecurity systems / S. Yevseiev, V. Ponomarenko, O. Laptiev, O. Milov, O. Korol, S. Milevskyi, S. Pohasii, A. Tkachov, O. Shmatko, Y. Melenti, O. Sievierinov, S. Ostapov, A. Gavrilova, O. Tsyhanenko, S. Herasimov, E. Nyemkova, B. Tomashevsky, I. Hrod, I. Opirskyy, V. Zvieriev, O. Prokopenko, V. Savchenko, O. Barabash, V. Sobchuk, G. Shuklin, V. Khvostenko, O. Tymochko, M. Pavlenko, A. Trystan, S. Florov // monograph. – Kharkiv: PC TECHNOLOGY CENTER, 2021. – 188 p.(P. 102 – 147). Acces mode: https://www.scopus.com/pages/publications/85119654284 П.13. проведення навчальних занять із спеціальних дисциплін іноземною мовою (крім дисциплін мовної підготовки) в обсязі не менше 50 аудиторних годин на навчальний рік 1. Legal regulation of cybersecurity, (50 ауд. год) КН-1125і.е. П. 19 діяльність за спеціальністю у формі участі у професійних та/або громадських об'єднаннях Учасник Громадської організації "Національна асоціація патентних повірених" https://www.napa.org.ua член громадської організації "Східноєвропейське наукове товариство", посвідчення ES № 063 П. 20 досвід практичної роботи за спеціальністю не менше п'яти років (крім педагогічної, науково-педагогічної, наукової діяльності) – директор, ТОВ АТІЛОГ (ЄДРПОУ: 35974114) з 2008, ІТ компанія. https://youcontrol.com.ua/catalog/company_details/35974114/

107555	Євсеєв Сергій Петрович	Завідувач кафедри, Основне місце роботи	Навчально-науковий інститут комп'ютерних наук та інформаційних технологій	Диплом спеціаліста, Пермське вище військове командно-інженерне Червонопрапорне училище ракетних військ імені Маршала Радянського Союзу Чуйкова В.І., рік закінчення: 1991, спеціальність: Автоматизовані системи управління, Диплом магістра, Харківський військовий університет, рік закінчення: 2002, спеціальність: Організація технічного забезпечення військ (за видами та родами військ і сил), Диплом доктора наук ДД 007606, виданий 05.07.2018, Диплом кандидата наук ДК 035254, виданий 04.07.2006, Атестат доцента 12ДЦ 034106, виданий 25.01.2013, Атестат професора АП 001633, виданий 26.02.2020, Атестат старшого наукового співробітника (старшого дослідника) АС 007292, виданий 14.04.2010	39	Сучасні проблеми постквантової криптографії	Підвищення кваліфікації: 1. Certificate of Completion №KIO/23-04-01/2025 "Methods and technical means of information protection" (Krakow, Poland) (from 20 february, 2025 to 20 april 2025, затверджено наказом ректора НТУ ХПІ №2186С від 21.11.2025р) (6 ects-credits – 180 hours) Пункти відповідності ліцензійних умов: П. 1-4, 6-10, 12, 13, 19 П. 1 наявність не менше п'яти публікацій у періодичних наукових виданнях, що включені до переліку фахових видань України, до наукометричних баз, зокрема Scopus, Web of Science Core Collection 1. Serhii Yevseiev and other. Development of an improved SSL/TLS protocol using post-quantum algorithms. Eastern-European Journal of Enterprise Technologies. 2023. 3/9 (123). P. 34–45. https://repository.kpi.kharkov.ua/items/203ec4f5-7cd2-4c92-ad6f-a4039cfb25e7 2. Yevseiev and other. Development of a method for synthesizing an information-analytical system for assessing the level of information transmission channels protection. Eastern-European Journal of Enterprise Technologies. 2024. 2/9 (128). P. 36–43. https://journals.uran.ua/eejet/article/view/302495 3. Renata Danieliene1, Sergiy Bronin, Oleksandr Milov, Serhii Yevseiev. Model basis for cybersecurity of socio-cyberphysical systems. Baltic journal of modern computing. – 2024. – Т. 12. – №. 2. – С. 125-149. https://www.bjmc.lu.lv/fileadmin/user_upload/lu_portal/projekti/bjmc/Contents/12_2_01_Danieliene.pdf 4. Bazarnyi, S., Husak, Y., Voitko, T., Aliew, F., & Yevseiev, S. Mathematical model of multi-domain interaction based on game theory. Advanced

							Information Systems, 9(3), p. 22–31 https://repository.kpi.kharkov.ua/items/bbf7c1a8-69ee-4497-abab-cec65d0f6683 5. Yevseiev and other. Development of a method for protecting information resources in a corporate network by segmenting traffic. Eastern-European Journal of Enterprise Technologies, 2024, 5(9(131)), pp. 63–78. https://journals.uran.ua/eejet/article/view/313158 П. 2 наявність одного патенту на винахід або п'яти деклараційних патентів на винахід чи корисну модель, включаючи секретні, або наявність не менше п'яти свідоцтв про реєстрацію авторського права на твір 1. Пат. u202103665, МПК (51) G009C 1/00;Спосіб криптографічного перетворення інформації. Заяв. 25.06.2021; Опубл. 01.12.2021 р 2. Пат. u202103680, МПК (51) G009C 1/00;Спосіб криптографічного перетворення інформації. Заяв. 25.06.2021; Опубл. 01.12.2021 р 3. Пат. u202103683, МПК (51) G009C 1/00; Спосіб криптографічного перетворення інформації. Заяв. 23.06.2021; Опубл. 01.12.2021 р. 4. Пат. u202103704, МПК (51) G009C 1/00; Спосіб криптографічного перетворення інформації. Заяв. 23.06.2021; Опубл. 01.12.2021 р. 5. Пат. u202103617, МПК (51) G009C 1/00; Спосіб криптографічного перетворення інформації. Заявл. 23.06.2021; Опубл. 01.12.2021 р. П. 3 наявність виданого підручника чи навчального посібника (включаючи електронні) або монографії (загальним обсягом не менше 5 авторських аркушів), в тому числі

							видані у співавторстві (обсягом не менше 1,5 авторського аркуша на кожного співавтора) 1. Євсеєв С.П., Дженюк Н.В., Толкачов М.Ю., Касілов О.В., Король О.Г., Кудій Д.А. Комп'ютерні мережі. Книга 2. Архітектура комп'ютерів. Навч. посібник Харків, – Львів: Видавництво ПП «Новий Світ – 2000», 2023. – 320 с Власний внесок 4,3 авторських аркушів. 2. Євсеєв С. П., Мілов О.В., Остапов С.Е., Северінов О.В. Кібербезпека: Основи кодування та криптографії. Навчальний посібник. Львів: "Новий Світ– 2000", 2025. – 658 3. В.Ю. Ковтун, С.П. Євсеєв, І. В. Аксьонова. Новітні технології захисту інформації. навчальний посібник. – Харків, – Львів: Видавництво ПП «Новий Світ – 2000», 2024. – 285 с.
							П. 4 наявність виданих навчально-методичних посібників/посібників для самостійної роботи здобувачів вищої освіти та дистанційного навчання, електронних курсів на освітніх платформах ліцензіатів, конспектів лекцій/практикумів/методичних вказівок/рекомендацій/ робочих програм, інших друкованих навчально-методичних праць загальною кількістю три найменування 1.Основи кібербезпеки. навчально-практичний посібник / уклад. С. П. Євсеєв, О. В. Шматко, О. Б. Ахієзер, Т. В. Горбач ; за заг. ред. С. П. Євсеєва. – Харків : НТУ «ХПІ», – Львів : «Новий Світ-2000», 2025. – 95 с. – (Серія «Кібербезпека та штучний інтелект»). ISBN 978-966-418-514-8. 2. Атаки на системи штучного інтелекту. навчально-практичний посібник / уклад. С. П. Євсеєв, О. В. Шматко, О. Б. Ахієзер, В. Є. Сокол, Н.

							Л. Чернова, Харків : НТУ «ХПІ», – Львів : «Новий Світ-2000», 2025. – 108 с. – (Серія «Кібербезпека та штучний інтелект»). ISBN 978-966-418-515-5 3. Штучний інтелект. Нейромережева обробка інформації : архітектури, навчання, застосування : навчальний посібник у 2-х ч. : Ч. 1 / О. Г. Руденко, О. О. Безсонов, С. П. Євсеєв, О. Б. Ахієзер, Ю. І. Зайцев. ; за заг. ред. С. П. Євсеєва. – Харків : НТУ «ХПІ», – Львів : «Новий Світ-2000», 2025. – 426 с. – (Серія «Кібербезпека та штучний інтелект»). ISBN 978-966-418-517-9 4. Штучний інтелект. Нейромережева обробка інформації : архітектури, навчання, застосування : навчальний посібник у 2-х ч. : Ч. 2 / О. Г. Руденко, О. О. Безсонов, С. П. Євсеєв, О. Б. Ахієзер, Ю. І. Зайцев. ; за заг. ред. С. П. Євсеєва. – Харків : НТУ «ХПІ», – Львів : «Новий Світ-2000», 2025. – 376 с. – (Серія «Кібербезпека та штучний інтелект»). Руденко О. Г. та ін. ISBN 978-966-418-518-6 П. 6 наукове керівництво (консультування) здобувача, який одержав документ про присудження наукового ступеня Циганенко Олексій Сергійович, доктор філософії зі спеціальності 122 – комп'ютерні науки, тема дисертації: "Моделі та методи підвищення якості обслуговування інформаційних систем", 2022 р., Диплом ДР №003787 від 1 лютого 2022 року, Міністерство освіти і науки України. Одеський державний екологічний університет. Погасій Сергій Сергійович, доктор технічних наук, 05.13.21. Системи захисту інформації, тема дисертації:

							Моделі і методи захисту інформації в кіберфізичних системах, 2024 рік. Диплом ДД № 013762 від 18 лютого 2025 року. Міністерство освіти і науки України. Державний університет інформаційно-комунікаційних технологій. Мілевський Станіслав Валерійович, доктор технічних наук, 05.13.21. Системи захисту інформації, тема дисертації: Методологія побудови систем безпеки мультимедійних ресурсів в інтернет-сервісах, 2024 рік. Диплом ДД №013771 від 18 лютого 2025 року, Міністерство освіти і науки України. Національний університет “Львівська політехніка”. П.7 участь в атестації наукових кадрів як офіційного опонента або члена постійної спеціалізованої вченої ради, або члена не менше трьох разових спеціалізованих вчених рад Улічев Олександр Сергійович, здобуття наукового ступеня кандидата технічних наук за спеціальністю 21.05.01 – “Інформаційна безпека держави”, “Модель та методи поширення інформаційних впливів у соціальних мережах в умовах інформаційного протиборства”, 13.05. 2021 р., Національний авіаційний університет. Костяк Марина Юріївна, здобуття наукового ступеня кандидата технічних наук за спеціальністю 05.13.21 – системи захисту інформації, “Підвищення ефективності функціонування захищених інформаційних мереж спеціального призначення”, 2021 р., Національний університет “Львівська політехника”. Ляшенко Галина Євгеніївна здобуття наукового ступеня

							доктора філософії за спеціальністю 172 – Електронні комунікації та радіотехніка, 2025, Харківський національний університет радіоелектроніки Кирсанов Олександр Олександрович, здобуття наукового ступеня доктора філософії за спеціальністю 172 Телекомунікації та радіотехніка галузь знань 17 Електроніка та телекомунікації, 2025, Харківський національний університет радіоелектроніки П 8. виконання функцій (повноважень, обов'язків) наукового керівника або відповідального виконавця наукової теми (проекту), або головного редактора/члена редакційної колегії/експерта (рецензента) наукового видання, включеного до переліку фахових видань України, або іноземного наукового видання, що індексується в бібліографічних базах Заступник головного редактора наукового видання «Територія безпеки», «Terra Security». https://ts.khpi.edu.ua/about/editorialTeam П.9 робота у складі експертної ради з питань проведення експертизи дисертацій МОН або у складі галузевої експертної ради як експерта Національного агентства із забезпечення якості вищої освіти, або у складі Акредитаційної комісії, або міжгалузевої експертної ради з вищої освіти Акредитаційної комісії, або трьох експертних комісій МОН/зазначеного Агентства, або Науково-методичної ради/науково-методичних комісій (підкомісій) з вищої або фахової передвищої освіти МОН,

							наукових/науково-методичних/експертних рад органів державної влади та органів місцевого самоврядування, або у складі комісій Державної служби якості освіти із здійснення планових (позапланових) заходів державного нагляду (контролю) Робота у складі НМК 6 “З інформаційних технологій ”, підкомісія F5 “Кібербезпека та захист інформації” Наказ Міністерства освіти і науки України від 02 квітня 2025 р. № 535 «Про затвердження персонального складу Науково-методичних комісій (підкомісій) сектору вищої освіти науково-методичної ради МОН») Експерт Національного фонду досліджень України (2020–2024 рр) Експерт МОН України Секція: 2. Інформатика та кібернетика (2024 р.) П. 10 участь у міжнародних наукових та/або освітніх проектах, залучення до міжнародної експертизи, наявність звання “суддя міжнародної категорії” Євсеєв Сергій Петрович – координатор робочої групи з реалізації міжнародного гранту “Conducting e-learning cyberhygiene” П. 12 наявність апробаційних та/або науково-популярних, та/або консультаційних (дорадчих), та/або науково-експертних публікацій з наукової або професійної тематики загальною кількістю не менше п’яти публікацій. 1. Yevseiev Serhii. Socio-Cyber-Physical Systems Security Concept / Serhii Yevseiev, Stanislav Milevskyi, Leonid Bortnik, Voropay Alexey, Kyrylo Bondarenko, Serhii Pohasii / 4th International Congress on Human-Computer Interaction, Optimization and

							Robotic Applications. June 9-11, 2022, Ankara, Turkey. URL: https://www.aconf.org/conf_181999.html 2. Yevseiev Serhii. Measuring Signals Synthesis Method on the Basis of Triangular Time-Pulse Modulation for Control of Radiotechnic Systems Technical Condition. Concept / Sergiy Tymchenko, Volodymyr Kutsenko, Serhii Yevseiev, Stanislav Milevskyi, Serhii Pohasii / 4th International Congress on Human-Computer Interaction, Optimization and Robotic Applications. June 9-11, 2022, Ankara, Turkey URL: https://www.aconf.org/conf_181999.html 3. Serhii Yevseiev, Pierre Murr, Stanislav Milevskyi, Olha Korol, Marharyta Melnyk. Development of a Sociocyberphysical Systems Cyber Threats Classifier. 2023 7th International Symposium on Multidisciplinary Studies and Innovative Technologies (ISMSIT). https://ieeexplore.ieee.org/document/10304895 4. Serhii Yevseiev, Stanislav Milevskyi, Vladyslav Sokol, Yevhen Melenti, Olena Akhiiezer, Kyrylo Petrenko. Methodological Foundations for Constructing Intelligent Information Security Systems. 7th International Congress on Human-Computer Interaction, Optimization and Robotic Applications, Proceedings Conference Paper 2025. https://ieeexplore.ieee.org/document/11017207 5. Serhii Yevseiev, Stanislav Milevskyi, Vladyslav Sokol, Yevhen Melenti, Olena Akhiiezer. Multi-Contour Intellectual Cyber Protection System Methodology. 9th International Symposium on Multidisciplinary Studies and Innovative Technologies. https://ieeexplore.ieee.org/document/11267930

							П.13. проведення навчальних занять із спеціальних дисциплін іноземною мовою (крім дисциплін мовної підготовки) в обсязі не менше 50 аудиторних годин на навчальний рік 1. Information security of the state, кредитів 4,0 (64 години), КН-1122іа.е, 2022 р. П. 19 . Діяльність за спеціальністю у формі участі у професійних та/або громадських об'єднаннях член громадської організації "Східноєвропейське наукове товариство", посвідчення ES № 053.
107555	Євсеєв Сергій Петрович	Завідувач кафедри, Основне місце роботи	Навчально-науковий інститут комп'ютерних наук та інформаційних технологій	Диплом спеціаліста, Пермське вище військове командно-інженерне Червонопрапорне училище ракетних військ імені Маршала Радянського Союзу Чуйкова В.І., рік закінчення: 1991, спеціальність: Автоматизовані системи управління, Диплом магістра, Харківський військовий університет, рік закінчення: 2002, спеціальність: Організація технічного забезпечення військ (за видами та родами військ і сил), Диплом доктора наук ДД 007606, виданий 05.07.2018, Диплом кандидата наук ДК 035254, виданий 04.07.2006, Атестат доцента 12ДЦ 034106, виданий 25.01.2013, Атестат професора АП 001633, виданий 26.02.2020,	39	Основи наукових досліджень	Підвищення кваліфікації: 1. Certificate of Completion №KIO/23-04-01/2025 "Methods and technical means of information protection" (Krakow, Poland) (from 20 february, 2025 to 20 april 2025, затверджено наказом ректора НТУ ХПІ №2186С від 21.11.2025р) (6 ects-credits – 180 hours) Пункти відповідності ліцензійних умов: П. 1-4, 6-10, 12, 13, 19 П. 1 наявність не менше п'яти публікацій у періодичних наукових виданнях, що включені до переліку фахових видань України, до наукометричних баз, зокрема Scopus, Web of Science Core Collection 1. Serhii Yevseiev and other. Development of an improved SSL/TLS protocol using post-quantum algorithms. Eastern-European Journal of Enterprise Technologies. 2023. 3/9 (123). P. 34–45. https://repository.kpi.kharkov.ua/items/203ec4f5-7cd2-4c92-ad6f-a4039cfb25e7 2. Yevseiev and other. Development of a method for synthesizing an information-analytical system for assessing the level of information transmission channels protection. Eastern-European Journal of Enterprise

				Атестат старшого наукового співробітника (старшого дослідника) АС 007292, виданий 14.04.2010			Technologies. 2024. 2/9 (128). P. 36–43. https://journals.uran.ua/eejet/article/view/302495 3. Renata Danieliene1, Sergiy Bronin, Oleksandr Milov, Serhii Yevseiev. Model basis for cybersecurity of socio-cyberphysical systems. Baltic journal of modern computing. – 2024. – Т. 12. – №. 2. – С. 125-149. https://www.bjmc.lu.lv/fileadmin/user_upload/lu_portal/projekti/bjmc/Contents/12_2_01_Danieliene.pdf 4. Bazarnyi, S., Husak, Y., Voitko, T., Aliew, F., & Yevseiev, S. Mathematical model of multi-domain interaction based on game theory. Advanced Information Systems, 9(3), p. 22–31 https://repository.kpi.kharkov.ua/items/bbf7c1a8-69ee-4497-abab-cec65d0f6683 5. Yevseiev and other. Development of a method for protecting information resources in a corporate network by segmenting traffic. Eastern-European Journal of Enterprise Technologies, 2024, 5(9(131)), pp. 63–78. https://journals.uran.ua/eejet/article/view/313158 П. 2 наявність одного патенту на винахід або п’яти деклараційних патентів на винахід чи корисну модель, включаючи секретні, або наявність не менше п’яти свідоцтв про реєстрацію авторського права на твір 1. Пат. u202103665, МПК (51) G009C 1/00;Спосіб криптографічного перетворення інформації. Заяв. 25.06.2021; Опубл. 01.12.2021 р 2. Пат. u202103680, МПК (51) G009C 1/00;Спосіб криптографічного перетворення інформації. Заяв. 25.06.2021; Опубл. 01.12.2021 р 3. Пат. u202103683, МПК (51) G009C 1/00; Спосіб криптографічного перетворення інформації. Заяв. 23.06.2021; Опубл.

							01.12.2021 р. 4. Пат. u202103704, МПК (51) G009C 1/00; Спосіб криптографічного перетворення інформації. Заяв. 23.06.2021; Опубл. 01.12.2021 р. 5. Пат. u202103617, МПК (51) G009C 1/00; Спосіб криптографічного перетворення інформації. Заявл. 23.06.2021; Опубл. 01.12.2021 р. П. 3 наявність виданого підручника чи навчального посібника (включаючи електронні) або монографії (загальним обсягом не менше 5 авторських аркушів), в тому числі видані у співавторстві (обсягом не менше 1,5 авторського аркуша на кожного співавтора) 1. Євсеєв С.П., Дженюк Н.В., Толкачов М.Ю., Касілов О.В., Король О.Г., Кудій Д.А. Комп'ютерні мережі. Книга 2. Архітектура комп'ютерів. Навч. посібник Харків, – Львів: Видавництво ПП «Новий Світ – 2000», 2023. – 320 с Власний внесок 4,3 авторських аркушів. 2. Євсеєв С. П., Мілов О.В., Остапов С.Е., Северінов О.В. Кібербезпека: Основи кодування та криптографії. Навчальний посібник. Львів: "Новий Світ– 2000", 2025. – 658 3. В.Ю. Ковтун, С.П. Євсеєв, І. В. Аксьонова. Новітні технології захисту інформації. навчальний посібник. – Харків, – Львів: Видавництво ПП «Новий Світ – 2000», 2024. – 285 с. П. 4 наявність виданих навчально-методичних посібників/посібників для самостійної роботи здобувачів вищої освіти та дистанційного навчання, електронних курсів на освітніх платформах ліцензіатів, конспектів лекцій/практикумів/методичних вказівок/рекомендацій/ робочих програм, інших друкованих

							навчально-методичних праць загальною кількістю три найменування 1.Основи кібербезпеки. навчально-практичний посібник / уклад. С. П. Євсеєв, О. В. Шматко, О. Б. Ахієзер, Т. В. Горбач ; за заг. ред. С. П. Євсеєва. – Харків : НТУ «ХПІ», – Львів : «Новий Світ-2000», 2025. – 95 с. – (Серія «Кібербезпека та штучний інтелект»). ISBN 978-966-418-514-8. 2. Атаки на системи штучного інтелекту. навчально-практичний посібник / уклад. С. П. Євсеєв, О. В. Шматко, О. Б. Ахієзер, В. Є. Сокол, Н. Л. Чернова, Харків : НТУ «ХПІ», – Львів : «Новий Світ-2000», 2025. – 108 с. – (Серія «Кібербезпека та штучний інтелект»). ISBN 978-966-418-515-5 3. Штучний інтелект. Нейромережева обробка інформації : архітектури, навчання, застосування : навчальний посібник у 2-х ч. : Ч. 1 / О. Г. Руденко, О. О. Безсонов, С. П. Євсеєв, О. Б. Ахієзер, Ю. І. Зайцев. ; за заг. ред. С. П. Євсеєва. – Харків : НТУ «ХПІ», – Львів : «Новий Світ-2000», 2025. – 426 с. – (Серія «Кібербезпека та штучний інтелект»). ISBN 978-966-418-517-9 4. Штучний інтелект. Нейромережева обробка інформації : архітектури, навчання, застосування : навчальний посібник у 2-х ч. : Ч. 2 / О. Г. Руденко, О. О. Безсонов, С. П. Євсеєв, О. Б. Ахієзер, Ю. І. Зайцев. ; за заг. ред. С. П. Євсеєва. – Харків : НТУ «ХПІ», – Львів : «Новий Світ-2000», 2025. – 376 с. – (Серія «Кібербезпека та штучний інтелект»). Руденко О. Г. та ін. ISBN 978-966-418-518-6 П. 6 наукове керівництво (консультування) здобувача, який одержав документ про

							присудження наукового ступеня Циганенко Олексій Сергійович, доктор філософії зі спеціальності 122 – комп'ютерні науки, тема дисертації: "Моделі та методи підвищення якості обслуговування інформаційних систем", 2022 р., Диплом ДР №003787 від 1 лютого 2022 року, Міністерство освіти і науки України. Одеський державний екологічний університет. Погасій Сергій Сергійович, доктор технічних наук, 05.13.21. Системи захисту інформації, тема дисертації: Моделі і методи захисту інформації в кіберфізичних системах, 2024 рік. Диплом ДД № 013762 від 18 лютого 2025 року. Міністерство освіти і науки України. Державний університет інформаційно-комунікаційних технологій. Мілевський Станіслав Валерійович, доктор технічних наук, 05.13.21. Системи захисту інформації, тема дисертації: Методологія побудови систем безпеки мультимедійних ресурсів в інтернет-сервісах, 2024 рік. Диплом ДД №013771 від 18 лютого 2025 року, Міністерство освіти і науки України. Національний університет "Львівська політехніка". П.7 участь в атестації наукових кадрів як офіційного опонента або члена постійної спеціалізованої вченої ради, або члена не менше трьох разових спеціалізованих вчених рад Улічев Олександр Сергійович, здобуття наукового ступеня кандидата технічних наук за спеціальністю 21.05.01 – "Інформаційна безпека держави", "Модель та методи поширення інформаційних впливів у соціальних

							мережах в умовах інформаційного протиборства", 13.05. 2021 р., Національний авіаційний університет. Костяк Марина Юріївна, здобуття наукового ступеня кандидата технічних наук за спеціальністю 05.13.21 – системи захисту інформації, "Підвищення ефективності функціонування захищених інформаційних мереж спеціального призначення", 2021 р., Національний університет "Львівська політехника". Ляшенко Галина Євгеніївна здобуття наукового ступеня доктора філософії за спеціальністю 172 – Електронні комунікації та радіотехніка, 2025, Харківський національний університет радіоелектроніки Кирсанов Олександр Олександрович, здобуття наукового ступеня доктора філософії за спеціальністю 172 Телекомунікації та радіотехніка галузь знань 17 Електроніка та телекомунікації, 2025, Харківський національний університет радіоелектроніки П 8. виконання функцій (повноважень, обов'язків) наукового керівника або відповідального виконавця наукової теми (проекту), або головного редактора/члена редакційної колегії/експерта (рецензента) наукового видання, включеного до переліку фахових видань України, або іноземного наукового видання, що індексується в бібліографічних базах Заступник головного редактора наукового видання «Територія безпеки», «Terra Security». https://ts.khpi.edu.ua/about/editorialTeam П.9 робота у складі експертної ради з

							питань проведення експертизи дисертацій МОН або у складі галузевої експертної ради як експерта Національного агентства із забезпечення якості вищої освіти, або у складі Акредитаційної комісії, або міжгалузевої експертної ради з вищої освіти Акредитаційної комісії, або трьох експертних комісій МОН/зазначеного Агентства, або Науково-методичної ради/науково-методичних комісій (підкомісій) з вищої або фахової передвищої освіти МОН, наукових/науково-методичних/експертних рад органів державної влади та органів місцевого самоврядування, або у складі комісій Державної служби якості освіти із здійснення планових (позапланових) заходів державного нагляду (контролю) Робота у складі НМК 6 “З інформаційних технологій ”, підкомісія F5 “Кібербезпека та захист інформації” Наказ Міністерства освіти і науки України від 02 квітня 2025 р. № 535 «Про затвердження персонального складу Науково-методичних комісій (підкомісій) сектору вищої освіти науково-методичної ради МОН») Експерт Національного фонду досліджень України (2020–2024 рр) Експерт МОН України Секція: 2. Інформатика та кібернетика (2024 р.) П. 10 участь у міжнародних наукових та/або освітніх проектах, залучення до міжнародної експертизи, наявність звання “суддя міжнародної категорії” Євсеєв Сергій Петрович – координатор робочої групи з реалізації міжнародного гранту “Conducting e-learning

							cyberhygiene” П. 12 наявність апробаційних та/або науково-популярних, та/або консультаційних (дорадчих), та/або науково-експертних публікацій з наукової або професійної тематики загальною кількістю не менше п’яти публікацій. 1. Yevseiev Serhii. Socio-Cyber-Physical Systems Security Concept / Serhii Yevseiev, Stanislav Milevskyi, Leonid Bortnik, Voropay Alexey, Kyrylo Bondarenko, Serhii Pohasii / 4th International Congress on Human-Computer Interaction, Optimization and Robotic Applications. June 9-11, 2022, Ankara, Turkey. URL: https://www.aconf.org/conf_181999.html 2. Yevseiev Serhii. Measuring Signals Synthesis Method on the Basis of Triangular Time-Pulse Modulation for Control of Radiotechnic Systems Technical Condition. Concept / Sergiy Tymchenko, Volodymyr Kutsenko, Serhii Yevseiev, Stanislav Milevskyi, Serhii Pohasii / 4th International Congress on Human-Computer Interaction, Optimization and Robotic Applications. June 9-11, 2022, Ankara, Turkey URL: https://www.aconf.org/conf_181999.html 3. Serhii Yevseiev, Pierre Murr, Stanislav Milevskyi, Olha Korol, Marharyta Melnyk. Development of a Sociocyberphysical Systems Cyber Threats Classifier. 2023 7th International Symposium on Multidisciplinary Studies and Innovative Technologies (ISMSIT). https://ieeexplore.ieee.org/document/10304895 4. Serhii Yevseiev, Stanislav Milevskyi, Vladyslav Sokol, Yevhen Melenti, Olena Akhiiezer, Kyrylo Petrenko. Methodological Foundations for Constructing Intelligent Information Security

							Systems. 7th International Congress on Human-Computer Interaction, Optimization and Robotic Applications, Proceedings Conference Paper 2025. https://ieeexplore.ieee.org/document/11017207 5. Serhii Yevseiev, Stanislav Milevskyi, Vladyslav Sokol, Yevhen Melenti, Olena Akhiiezer. Multi-Contour Intellectual Cyber Protection System Methodology. 9th International Symposium on Multidisciplinary Studies and Innovative Technologies. https://ieeexplore.ieee.org/document/11267930 П.13. проведення навчальних занять із спеціальних дисциплін іноземною мовою (крім дисциплін мовної підготовки) в обсязі не менше 50 аудиторних годин на навчальний рік 1. Information security of the state, кредитів 4,0 (64 години), КН-1122ia.e, 2022 р. П. 19 . Діяльність за спеціальністю у формі участі у професійних та/або громадських об'єднаннях член громадської організації "Східноєвропейське наукове товариство", посвідчення ES № 053.
107555	Євсеєв Сергій Петрович	Завідувач кафедри, Основне місце роботи	Навчально-науковий інститут комп'ютерних наук та інформаційних технологій	Диплом спеціаліста, Пермське вище військове командно-інженерне Червонопрапорне училище ракетних військ імені Маршала Радянського Союзу Чуйкова В.І., рік закінчення: 1991, спеціальність: Автоматизовані системи управління, Диплом магістра, Харківський військовий університет, рік закінчення: 2002, спеціальність:	39	Етичний хакінг	Підвищення кваліфікації: 1. Certificate of Completion №KIO/23-04-01/2025 "Methods and technical means of information protection" (Krakow, Poland) (from 20 february, 2025 to 20 april 2025, затверджено наказом ректора НТУ ХПІ №2186С від 21.11.2025р) (6 ects-credits – 180 hours) Пункти відповідності ліцензійних умов: П. 1-4, 6-10, 12, 13, 19 П. 1 наявність не менше п'яти публікацій у періодичних наукових виданнях, що включені до переліку фахових видань України, до наукометричних баз, зокрема Scopus, Web

				Організація технічного забезпечення військ (за видами та родами військ і сил), Диплом доктора наук ДД 007606, виданий 05.07.2018, Диплом кандидата наук ДК 035254, виданий 04.07.2006, Атестат доцента 12ДЦ 034106, виданий 25.01.2013, Атестат професора АП 001633, виданий 26.02.2020, Атестат старшого наукового співробітника (старшого дослідника) АС 007292, виданий 14.04.2010			of Science Core Collection 1. Serhii Yevseiev and other. Development of an improved SSL/TLS protocol using post-quantum algorithms. Eastern-European Journal of Enterprise Technologies. 2023. 3/9 (123). P. 34–45. https://repository.kpi.kharkov.ua/items/203ec4f5-7cd2-4c92-ad6f-a4039cfb25e7 2. Yevseiev and other. Development of a method for synthesizing an information-analytical system for assessing the level of information transmission channels protection. Eastern-European Journal of Enterprise Technologies. 2024. 2/9 (128). P. 36–43. https://journals.uran.ua/eejet/article/view/302495 3. Renata Danieliene1, Sergiy Bronin, Oleksandr Milov, Serhii Yevseiev. Model basis for cybersecurity of socio-cyberphysical systems. Baltic journal of modern computing. – 2024. – Т. 12. – №. 2. – С. 125-149. https://www.bjmc.lu.lv/fileadmin/user_upload/lu_portal/projekti/bjmc/Contents/12_2_01_Danieliene.pdf 4. Bazarnyi, S., Husak, Y., Voitko, T., Aliew, F., & Yevseiev, S. Mathematical model of multi-domain interaction based on game theory. Advanced Information Systems, 9(3), p. 22–31 https://repository.kpi.kharkov.ua/items/bbf7c1a8-69ee-4497-abab-cec65d0f6683 5. Yevseiev and other. Development of a method for protecting information resources in a corporate network by segmenting traffic. Eastern-European Journal of Enterprise Technologies, 2024, 5(9(131)), pp. 63–78. https://journals.uran.ua/eejet/article/view/313158 П. 2 наявність одного патенту на винахід або п’яти деклараційних патентів на винахід чи корисну модель, включаючи секретні, або наявність не менше п’яти свідоцтв

							про реєстрацію авторського права на твір 1. Пат. u202103665, МПК (51) G009C 1/00;Спосіб криптографічного перетворення інформації. Заяв. 25.06.2021; Опубл. 01.12.2021 р 2. Пат. u202103680, МПК (51) G009C 1/00;Спосіб криптографічного перетворення інформації. Заяв. 25.06.2021; Опубл. 01.12.2021 р 3. Пат. u202103683, МПК (51) G009C 1/00; Спосіб криптографічного перетворення інформації. Заяв. 23.06.2021; Опубл. 01.12.2021 р. 4. Пат. u202103704, МПК (51) G009C 1/00; Спосіб криптографічного перетворення інформації. Заяв. 23.06.2021; Опубл. 01.12.2021 р. 5. Пат. u202103617, МПК (51) G009C 1/00; Спосіб криптографічного перетворення інформації. Заявл. 23.06.2021; Опубл. 01.12.2021 р. П. 3 наявність виданого підручника чи навчального посібника (включаючи електронні) або монографії (загальним обсягом не менше 5 авторських аркушів), в тому числі видані у співавторстві (обсягом не менше 1,5 авторського аркуша на кожного співавтора) 1. Євсеєв С.П., Дженюк Н.В., Толкачов М.Ю., Касілов О.В., Король О.Г., Кудій Д.А. Комп'ютерні мережі. Книга 2. Архітектура комп’ютерів. Навч. посібник Харків, – Львів: Видавництво ПП «Новий Світ – 2000», 2023. – 320 с Власний внесок 4,3 авторських аркушів. 2. Євсеєв С. П., Мілов О.В., Остапов С.Е., Северінов О.В. Кібербезпека: Основи кодування та криптографії. Навчальний посібник. Львів: “Новий Світ– 2000”, 2025. – 658 3. В.Ю. Ковтун, С.П. Євсеєв, І. В.

							Аксьонова. Новітні технології захисту інформації. навчальний посібник. – Харків, – Львів: Видавництво ПП «Новий Світ – 2000», 2024. – 285 с. П. 4 наявність виданих навчально-методичних посібників/посібників для самостійної роботи здобувачів вищої освіти та дистанційного навчання, електронних курсів на освітніх платформах ліцензіатів, конспектів лекцій/практикумів/методичних вказівок/рекомендацій/ робочих програм, інших друкованих навчально-методичних праць загальною кількістю три найменування 1.Основи кібербезпеки. навчально-практичний посібник / уклад. С. П. Євсеєв, О. В. Шматко, О. Б. Ахієзер, Т. В. Горбач ; за заг. ред. С. П. Євсеєва. – Харків : НТУ «ХПІ», – Львів : «Новий Світ-2000», 2025. – 95 с. – (Серія «Кібербезпека та штучний інтелект»). ISBN 978-966-418-514-8. 2. Атаки на системи штучного інтелекту. навчально-практичний посібник / уклад. С. П. Євсеєв, О. В. Шматко, О. Б. Ахієзер, В. Є. Сокол, Н. Л. Чернова, Харків : НТУ «ХПІ», – Львів : «Новий Світ-2000», 2025. – 108 с. – (Серія «Кібербезпека та штучний інтелект»). ISBN 978-966-418-515-5 3. Штучний інтелект. Нейромережева обробка інформації : архітектури, навчання, застосування : навчальний посібник у 2-х ч. : Ч. 1 / О. Г. Руденко, О. О. Безсонов, С. П. Євсеєв, О. Б. Ахієзер, Ю. І. Зайцев. ; за заг. ред. С. П. Євсеєва. – Харків : НТУ «ХПІ», – Львів : «Новий Світ-2000», 2025. – 426 с. – (Серія «Кібербезпека та штучний інтелект»). ISBN 978-966-418-517-9

							4. Штучний інтелект. Нейромережева обробка інформації : архітектури, навчання, застосування : навчальний посібник у 2-х ч. : Ч. 2 / О. Г. Руденко, О. О. Безсонов, С. П. Євсеєв, О. Б. Ахієзер, Ю. І. Зайцев. ; за заг. ред. С. П. Євсеєва. – Харків : НТУ «ХПІ», – Львів : «Новий Світ-2000», 2025. – 376 с. – (Серія «Кібербезпека та штучний інтелект»). Руденко О. Г. та ін. ISBN 978-966-418-518-6 П. 6 наукове керівництво (консультування) здобувача, який одержав документ про присудження наукового ступеня Циганенко Олексій Сергійович, доктор філософії зі спеціальності 122 – комп'ютерні науки, тема дисертації: "Моделі та методи підвищення якості обслуговування інформаційних систем", 2022 р., Диплом ДР №003787 від 1 лютого 2022 року, Міністерство освіти і науки України. Одеський державний екологічний університет. Погасій Сергій Сергійович, доктор технічних наук, 05.13.21. Системи захисту інформації, тема дисертації: Моделі і методи захисту інформації в кіберфізичних системах, 2024 рік. Диплом ДД № 013762 від 18 лютого 2025 року. Міністерство освіти і науки України. Державний університет інформаційно-комунікаційних технологій. Мілевський Станіслав Валерійович, доктор технічних наук, 05.13.21. Системи захисту інформації, тема дисертації: Методологія побудови систем безпеки мультимедійних ресурсів в інтернет-сервісах, 2024 рік. Диплом ДД №013771 від 18 лютого 2025 року, Міністерство освіти і науки

							України. Національний університет “Львівська політехніка”. П.7 участь в атестації наукових кадрів як офіційного опонента або члена постійної спеціалізованої вченої ради, або члена не менше трьох разових спеціалізованих вчених рад Улічев Олександр Сергійович, здобуття наукового ступеня кандидата технічних наук за спеціальністю 21.05.01 – “Інформаційна безпека держави”, “Модель та методи поширення інформаційних впливів у соціальних мережах в умовах інформаційного протиборства”, 13.05. 2021 р., Національний авіаційний університет. Костяк Марина Юріївна, здобуття наукового ступеня кандидата технічних наук за спеціальністю 05.13.21 – системи захисту інформації, “Підвищення ефективності функціонування захищених інформаційних мереж спеціального призначення”, 2021 р., Національний університет “Львівська політехника”. Ляшенко Галина Євгеніївна здобуття наукового ступеня доктора філософії за спеціальністю 172 – Електронні комунікації та радіотехніка, 2025, Харківський національний університет радіоелектроніки Кирсанов Олександр Олександрович, здобуття наукового ступеня доктора філософії за спеціальністю 172 Телекомунікації та радіотехніка галузь знань 17 Електроніка та телекомунікації, 2025, Харківський національний університет радіоелектроніки П 8. виконання функцій (повноважень, обов’язків) наукового

							керівника або відповідального виконавця наукової теми (проекту), або головного редактора/члена редакційної колегії/експерта (рецензента) наукового видання, включеного до переліку фахових видань України, або іноземного наукового видання, що індексується в бібліографічних базах Заступник головного редактора наукового видання «Територія безпеки», «Terra Security». https://ts.khpi.edu.ua/about/editorialTeam П.9 робота у складі експертної ради з питань проведення експертизи дисертацій МОН або у складі галузевої експертної ради як експерта Національного агентства із забезпечення якості вищої освіти, або у складі Акредитаційної комісії, або міжгалузевої експертної ради з вищої освіти Акредитаційної комісії, або трьох експертних комісій МОН/зазначеного Агентства, або Науково-методичної ради/науково-методичних комісій (підкомісій) з вищої або фахової передвищої освіти МОН, наукових/науково-методичних/експертних рад органів державної влади та органів місцевого самоврядування, або у складі комісій Державної служби якості освіти із здійснення планових (позапланових) заходів державного нагляду (контролю) Робота у складі НМК 6 “З інформаційних технологій ”, підкомісія F5 “Кібербезпека та захист інформації” Наказ Міністерства освіти і науки України від 02 квітня 2025 р. № 535 «Про затвердження персонального складу Науково-методичних комісій (підкомісій) сектору вищої освіти

							науково-методичної ради МОН») Експерт Національного фонду досліджень України (2020–2024 рр) Експерт МОН України Секція: 2. Інформатика та кібернетика (2024 р.) П. 10 участь у міжнародних наукових та/або освітніх проектах, залучення до міжнародної експертизи, наявність звання “суддя міжнародної категорії” Євсеєв Сергій Петрович – координатор робочої групи з реалізації міжнародного гранту “Conducting e-learning cyberhygiene” П. 12 наявність апробаційних та/або науково-популярних, та/або консультаційних (дорадчих), та/або науково-експертних публікацій з наукової або професійної тематики загальною кількістю не менше п’яти публікацій. 1. Yevseiev Serhii. Socio-Cyber-Physical Systems Security Concept / Serhii Yevseiev, Stanislav Milevskyi, Leonid Bortnik, Voropay Alexey, Kyrylo Bondarenko, Serhii Pohasii / 4th International Congress on Human-Computer Interaction, Optimization and Robotic Applications. June 9-11, 2022, Ankara, Turkey. URL: https://www.aconf.org/conf_181999.html 2. Yevseiev Serhii. Measuring Signals Synthesis Method on the Basis of Triangular Time-Pulse Modulation for Control of Radiotechnic Systems Technical Condition. Concept / Sergiy Tymchenko, Volodymyr Kutsenko, Serhii Yevseiev, Stanislav Milevskyi, Serhii Pohasii / 4th International Congress on Human-Computer Interaction, Optimization and Robotic Applications. June 9-11, 2022, Ankara, Turkey URL: https://www.aconf.org/conf_181999.html

							3. Serhii Yevseiev, Pierre Murr, Stanislav Milevskyi, Olha Korol, Marharyta Melnyk. Development of a Sociocyberphysical Systems Cyber Threats Classifier. 2023 7th International Symposium on Multidisciplinary Studies and Innovative Technologies (ISMSIT). https://ieeexplore.ieee.org/document/10304895 4. Serhii Yevseiev, Stanislav Milevskyi, Vladyslav Sokol, Yevhen Melenti, Olena Akhiiezer, Kyrylo Petrenko. Methodological Foundations for Constructing Intelligent Information Security Systems. 7th International Congress on Human-Computer Interaction, Optimization and Robotic Applications, Proceedings Conference Paper 2025. https://ieeexplore.ieee.org/document/11017207 5. Serhii Yevseiev, Stanislav Milevskyi, Vladyslav Sokol, Yevhen Melenti, Olena Akhiiezer. Multi-Contour Intellectual Cyber Protection System Methodology. 9th International Symposium on Multidisciplinary Studies and Innovative Technologies. https://ieeexplore.ieee.org/document/11267930 П.13. проведення навчальних занять із спеціальних дисциплін іноземною мовою (крім дисциплін мовної підготовки) в обсязі не менше 50 аудиторних годин на навчальний рік 1. Information security of the state, кредитів 4,0 (64 години), КН-1122ia.e, 2022 р. П. 19 . Діяльність за спеціальністю у формі участі у професійних та/або громадських об'єднаннях член громадської організації "Східноєвропейське наукове товариство", посвідчення ES № 053.
107555	Євсеєв Сергій	Завідувач кафедри,	Навчально-науковий	Диплом спеціаліста,	39	Цифрова криміналістик	Підвищення кваліфікації:

	Петрович	Основне місце роботи	інститут комп'ютерних наук та інформаційних технологій	Пермське вище військове командно-інженерне Червонопрапорне училище ракетних військ імені Маршала Радянського Союзу Чуйкова В.І., рік закінчення: 1991, спеціальність: Автоматизовані системи управління, Диплом магістра, Харківський військовий університет, рік закінчення: 2002, спеціальність: Організація технічного забезпечення військ (за видами та родами військ і сил), Диплом доктора наук ДД 007606, виданий 05.07.2018, Диплом кандидата наук ДК 035254, виданий 04.07.2006, Атестат доцента 12ДЦ 034106, виданий 25.01.2013, Атестат професора АП 001633, виданий 26.02.2020, Атестат старшого наукового співробітника (старшого дослідника) АС 007292, виданий 14.04.2010		а	1. Certificate of Completion №КІО/23-04-01/2025 "Methods and technical means of information protection" (Krakow, Poland) (from 20 february, 2025 to 20 april 2025, затверджено наказом ректора НТУ ХПІ №2186С від 21.11.2025р) (6 ects-credits – 180 hours) Пункти відповідності ліцензійних умов: П. 1-4, 6-10, 12, 13, 19 П. 1 наявність не менше п'яти публікацій у періодичних наукових виданнях, що включені до переліку фахових видань України, до наукометричних баз, зокрема Scopus, Web of Science Core Collection 1. Serhii Yevseiev and other. Development of an improved SSL/TLS protocol using post-quantum algorithms. Eastern-European Journal of Enterprise Technologies. 2023. 3/9 (123). P. 34–45. https://repository.kpi.kharkov.ua/items/203ec4f5-7cd2-4c92-ad6f-a4039cfb25e7 2. Yevseiev and other. Development of a method for synthesizing an information-analytical system for assessing the level of information transmission channels protection. Eastern-European Journal of Enterprise Technologies. 2024. 2/9 (128). P. 36–43. https://journals.uran.ua/eejet/article/view/302495 3. Renata Danieliene1, Sergiy Bronin, Oleksandr Milov, Serhii Yevseiev. Model basis for cybersecurity of socio-cyberphysical systems. Baltic journal of modern computing. – 2024. – Т. 12. – №. 2. – С. 125-149. https://www.bjmc.lu.lv/fileadmin/user_upload/lu_portal/projekti/bjmc/Contents/12_2_01_Danieliene.pdf 4. Bazarnyi, S., Husak, Y., Voitko, T., Aliew, F., & Yevseiev, S. Mathematical model of multi-domain interaction based on game theory. Advanced Information Systems, 9(3), p. 22–31

							https://repository.kpi.kharkov.ua/items/bbf7c1a8-69ee-4497-abab-cec65d0f6683 5. Yevseiev and other. Development of a method for protecting information resources in a corporate network by segmenting traffic. Eastern-European Journal of Enterprise Technologies, 2024, 5(9(131)), pp. 63–78. https://journals.uran.ua/eejet/article/view/313158 П. 2 наявність одного патенту на винахід або п'яти деклараційних патентів на винахід чи корисну модель, включаючи секретні, або наявність не менше п'яти свідоцтв про реєстрацію авторського права на твір 1. Пат. u202103665, МПК (51) G009C 1/00;Спосіб криптографічного перетворення інформації. Заяв. 25.06.2021; Опубл. 01.12.2021 р 2. Пат. u202103680, МПК (51) G009C 1/00;Спосіб криптографічного перетворення інформації. Заяв. 25.06.2021; Опубл. 01.12.2021 р 3. Пат. u202103683, МПК (51) G009C 1/00; Спосіб криптографічного перетворення інформації. Заяв. 23.06.2021; Опубл. 01.12.2021 р. 4. Пат. u202103704, МПК (51) G009C 1/00; Спосіб криптографічного перетворення інформації. Заяв. 23.06.2021; Опубл. 01.12.2021 р. 5. Пат. u202103617, МПК (51) G009C 1/00; Спосіб криптографічного перетворення інформації. Заявл. 23.06.2021; Опубл. 01.12.2021 р. П. 3 наявність виданого підручника чи навчального посібника (включаючи електронні) або монографії (загальним обсягом не менше 5 авторських аркушів), в тому числі видані у співавторстві (обсягом не менше 1,5

							авторського аркуша на кожного співавтора) 1. Євсеєв С.П., Дженюк Н.В., Толкачов М.Ю., Касілов О.В., Король О.Г., Кудій Д.А. Комп'ютерні мережі. Книга 2. Архітектура комп'ютерів. Навч. посібник Харків, – Львів: Видавництво ПП «Новий Світ – 2000», 2023. – 320 с Власний внесок 4,3 авторських аркушів. 2. Євсеєв С. П., Мілов О.В., Остапов С.Е., Северінов О.В. Кібербезпека: Основи кодування та криптографії. Навчальний посібник. Львів: "Новий Світ– 2000", 2025. – 658 3. В.Ю. Ковтун, С.П. Євсеєв, І. В. Аксьонова. Новітні технології захисту інформації. навчальний посібник. – Харків, – Львів: Видавництво ПП «Новий Світ – 2000», 2024. – 285 с. П. 4 наявність виданих навчально-методичних посібників/посібників для самостійної роботи здобувачів вищої освіти та дистанційного навчання, електронних курсів на освітніх платформах ліцензіатів, конспектів лекцій/практикумів/методичних вказівок/рекомендацій/ робочих програм, інших друкованих навчально-методичних праць загальною кількістю три найменування 1.Основи кібербезпеки. навчально-практичний посібник / уклад. С. П. Євсеєв, О. В. Шматко, О. Б. Ахієзер, Т. В. Горбач ; за заг. ред. С. П. Євсеєва. – Харків : НТУ «ХПІ», – Львів : «Новий Світ-2000», 2025. – 95 с. – (Серія «Кібербезпека та штучний інтелект»). ISBN 978-966-418-514-8. 2. Атаки на системи штучного інтелекту. навчально-практичний посібник / уклад. С. П. Євсеєв, О. В. Шматко, О. Б. Ахієзер, В. Є. Сокол, Н. Л. Чернова, Харків : НТУ «ХПІ», – Львів :

							«Новий Світ-2000», 2025. – 108 с. – (Серія «Кібербезпека та штучний інтелект»). ISBN 978-966-418-515-5 3. Штучний інтелект. Нейромережева обробка інформації : архітектури, навчання, застосування : навчальний посібник у 2-х ч. : Ч. 1 / О. Г. Руденко, О. О. Безсонов, С. П. Євсеєв, О. Б. Ахієзер, Ю. І. Зайцев. ; за заг. ред. С. П. Євсеєва. – Харків : НТУ «ХПІ», – Львів : «Новий Світ-2000», 2025. – 426 с. – (Серія «Кібербезпека та штучний інтелект»). ISBN 978-966-418-517-9 4. Штучний інтелект. Нейромережева обробка інформації : архітектури, навчання, застосування : навчальний посібник у 2-х ч. : Ч. 2 / О. Г. Руденко, О. О. Безсонов, С. П. Євсеєв, О. Б. Ахієзер, Ю. І. Зайцев. ; за заг. ред. С. П. Євсеєва. – Харків : НТУ «ХПІ», – Львів : «Новий Світ-2000», 2025. – 376 с. – (Серія «Кібербезпека та штучний інтелект»). Руденко О. Г. та ін. ISBN 978-966-418-518-6 П. 6 наукове керівництво (консультування) здобувача, який одержав документ про присудження наукового ступеня Циганенко Олексій Сергійович, доктор філософії зі спеціальності 122 – комп'ютерні науки, тема дисертації: "Моделі та методи підвищення якості обслуговування інформаційних систем", 2022 р., Диплом ДР №003787 від 1 лютого 2022 року, Міністерство освіти і науки України. Одеський державний екологічний університет. Погасій Сергій Сергійович, доктор технічних наук, 05.13.21. Системи захисту інформації, тема дисертації: Моделі і методи захисту інформації в

							кіберфізичних системах, 2024 рік. Диплом ДД № 013762 від 18 лютого 2025 року. Міністерство освіти і науки України. Державний університет інформаційно-комунікаційних технологій. Мілевський Станіслав Валерійович, доктор технічних наук, 05.13.21. Системи захисту інформації, тема дисертації: Методологія побудови систем безпеки мультимедійних ресурсів в інтернет-сервісах, 2024 рік. Диплом ДД №013771 від 18 лютого 2025 року, Міністерство освіти і науки України. Національний університет "Львівська політехніка". П.7 участь в атестації наукових кадрів як офіційного опонента або члена постійної спеціалізованої вченої ради, або члена не менше трьох разових спеціалізованих вчених рад Улічев Олександр Сергійович, здобуття наукового ступеня кандидата технічних наук за спеціальністю 21.05.01 – "Інформаційна безпека держави", "Модель та методи поширення інформаційних впливів у соціальних мережах в умовах інформаційного протиборства", 13.05. 2021 р., Національний авіаційний університет. Костяк Марина Юріївна, здобуття наукового ступеня кандидата технічних наук за спеціальністю 05.13.21 – системи захисту інформації, "Підвищення ефективності функціонування захищених інформаційних мереж спеціального призначення", 2021 р., Національний університет "Львівська політехника". Ляшенко Галина Євгеніївна здобуття наукового ступеня доктора філософії за спеціальністю 172 –

							Електронні комунікації та радіотехніка, 2025, Харківський національний університет радіоелектроніки Кирсанов Олександр Олександрович, здобуття наукового ступеня доктора філософії за спеціальністю 172 Телекомунікації та радіотехніка галузь знань 17 Електроніка та телекомунікації, 2025, Харківський національний університет радіоелектроніки П 8. виконання функцій (повноважень, обов'язків) наукового керівника або відповідального виконавця наукової теми (проекту), або головного редактора/члена редакційної колегії/експерта (рецензента) наукового видання, включеного до переліку фахових видань України, або іноземного наукового видання, що індексується в бібліографічних базах Заступник головного редактора наукового видання «Територія безпеки», «Terra Security». https://ts.khpi.edu.ua/about/editorialTeam П.9 робота у складі експертної ради з питань проведення експертизи дисертацій МОН або у складі галузевої експертної ради як експерта Національного агентства із забезпечення якості вищої освіти, або у складі Акредитаційної комісії, або міжгалузевої експертної ради з вищої освіти Акредитаційної комісії, або трьох експертних комісій МОН/зазначеного Агентства, або Науково-методичної ради/науково-методичних комісій (підкомісій) з вищої або фахової передвищої освіти МОН, наукових/науково-методичних/експертн

							их рад органів державної влади та органів місцевого самоврядування, або у складі комісій Державної служби якості освіти із здійснення планових (позапланових) заходів державного нагляду (контролю) Робота у складі НМК 6 “З інформаційних технологій ”, підкомісія F5 “Кібербезпека та захист інформації” Наказ Міністерства освіти і науки України від 02 квітня 2025 р. № 535 «Про затвердження персонального складу Науково-методичних комісій (підкомісій) сектору вищої освіти науково-методичної ради МОН») Експерт Національного фонду досліджень України (2020–2024 рр) Експерт МОН України Секція: 2. Інформатика та кібернетика (2024 р.) П. 10 участь у міжнародних наукових та/або освітніх проектах, залучення до міжнародної експертизи, наявність звання “суддя міжнародної категорії” Євсеєв Сергій Петрович – координатор робочої групи з реалізації міжнародного гранту “Conducting e-learning cyberhygiene” П. 12 наявність апробаційних та/або науково-популярних, та/або консультаційних (дорадчих), та/або науково-експертних публікацій з наукової або професійної тематики загальною кількістю не менше п’яти публікацій. 1. Yevseiev Serhii. Socio-Cyber-Physical Systems Security Concept / Serhii Yevseiev, Stanislav Milevskyi, Leonid Bortnik, Voropay Alexey, Kyrylo Bondarenko, Serhii Pohasii / 4th International Congress on Human-Computer Interaction, Optimization and Robotic Applications. June 9-11, 2022,

							Ankara, Turkey. URL: https://www.aconf.org/conf_181999.html 2. Yevseiev Serhii. Measuring Signals Synthesis Method on the Basis of Triangular Time-Pulse Modulation for Control of Radiotechnic Systems Technical Condition. Concept / Sergiy Tymchenko, Volodymyr Kutsenko, Serhii Yevseiev, Stanislav Milevskyi, Serhii Pohasii / 4th International Congress on Human-Computer Interaction, Optimization and Robotic Applications. June 9-11, 2022, Ankara, Turkey URL: https://www.aconf.org/conf_181999.html 3. Serhii Yevseiev, Pierre Murr, Stanislav Milevskyi, Olha Korol, Marharyta Melnyk. Development of a Sociocyberphysical Systems Cyber Threats Classifier. 2023 7th International Symposium on Multidisciplinary Studies and Innovative Technologies (ISMSIT). https://ieeexplore.ieee.org/document/10304895 4. Serhii Yevseiev, Stanislav Milevskyi, Vladyslav Sokol, Yevhen Melenti, Olena Akhiiezer, Kyrylo Petrenko. Methodological Foundations for Constructing Intelligent Information Security Systems. 7th International Congress on Human-Computer Interaction, Optimization and Robotic Applications, Proceedings Conference Paper 2025. https://ieeexplore.ieee.org/document/11017207 5. Serhii Yevseiev, Stanislav Milevskyi, Vladyslav Sokol, Yevhen Melenti, Olena Akhiiezer. Multi-Contour Intellectual Cyber Protection System Methodology. 9th International Symposium on Multidisciplinary Studies and Innovative Technologies. https://ieeexplore.ieee.org/document/11267930 П.13. проведення навчальних занять із

							спеціальних дисциплін іноземною мовою (крім дисциплін мовної підготовки) в обсязі не менше 50 аудиторних годин на навчальний рік 1. Information security of the state, кредитів 4,0 (64 години), КН-1122іа.е, 2022 р. П. 19 . Діяльність за спеціальністю у формі участі у професійних та/або громадських об'єднаннях член громадської організації "Східноєвропейське наукове товариство", посвідчення ES № 053.
107555	Євсеєв Сергій Петрович	Завідувач кафедри, Основне місце роботи	Навчально-науковий інститут комп'ютерних наук та інформаційних технологій	Диплом спеціаліста, Пермське вище військове командно-інженерне Червонопрапорне училище ракетних військ імені Маршала Радянського Союзу Чуйкова В.І., рік закінчення: 1991, спеціальність: Автоматизовані системи управління, Диплом магістра, Харківський військовий університет, рік закінчення: 2002, спеціальність: Організація технічного забезпечення військ (за видами та родами військ і сил), Диплом доктора наук ДД 007606, виданий 05.07.2018, Диплом кандидата наук ДК 035254, виданий 04.07.2006, Атестат доцента 12ДЦ 034106, виданий 25.01.2013, Атестат професора АП 001633, виданий 26.02.2020, Атестат старшого наукового співробітника	39	Мережева та хмарна безпека	Підвищення кваліфікації: 1. Certificate of Completion №KIO/23-04-01/2025 "Methods and technical means of information protection" (Krakow, Poland) (from 20 february, 2025 to 20 april 2025, затверджено наказом ректора НТУ ХПІ №2186С від 21.11.2025р) (6 ects-credits – 180 hours) Пункти відповідності ліцензійних умов: П. 1-4, 6-10, 12, 13, 19 П. 1 наявність не менше п'яти публікацій у періодичних наукових виданнях, що включені до переліку фахових видань України, до наукометричних баз, зокрема Scopus, Web of Science Core Collection 1. Serhii Yevseiev and other. Development of an improved SSL/TLS protocol using post-quantum algorithms. Eastern-European Journal of Enterprise Technologies. 2023. 3/9 (123). P. 34–45. https://repository.kpi.kharkov.ua/items/203ec4f5-7cd2-4c92-ad6f-a4039cfb25e7 2. Yevseiev and other. Development of a method for synthesizing an information-analytical system for assessing the level of information transmission channels protection. Eastern-European Journal of Enterprise Technologies. 2024. 2/9 (128). P. 36–43. https://journals.uran.ua/eejet/article/view/30

				(старшого дослідника) АС 007292, виданий 14.04.2010			2495 3. Renata Danieliene1, Sergiy Bronin, Oleksandr Milov, Serhii Yevseiev. Model basis for cybersecurity of socio-cyberphysical systems. Baltic journal of modern computing. – 2024. – Т. 12. – №. 2. – С. 125-149. https://www.bjmc.lu.lv/fileadmin/user_upload/lu_portal/projekti/bjmc/Contents/12_2_01_Danieliene.pdf 4. Bazarnyi, S., Husak, Y., Voitko, T., Aliew, F., & Yevseiev, S. Mathematical model of multi-domain interaction based on game theory. Advanced Information Systems, 9(3), p. 22–31 https://repository.kpi.kharkov.ua/items/bbf7c1a8-69ee-4497-abab-cec65d0f6683 5. Yevseiev and other. Development of a method for protecting information resources in a corporate network by segmenting traffic. Eastern-European Journal of Enterprise Technologies, 2024, 5(9(131)), pp. 63–78. https://journals.uran.ua/eejet/article/view/313158 П. 2 наявність одного патенту на винахід або п’яти деклараційних патентів на винахід чи корисну модель, включаючи секретні, або наявність не менше п’яти свідоцтв про реєстрацію авторського права на твір 1. Пат. u202103665, МПК (51) G009C 1/00;Спосіб криптографічного перетворення інформації. Заяв. 25.06.2021; Опубл. 01.12.2021 р 2. Пат. u202103680, МПК (51) G009C 1/00;Спосіб криптографічного перетворення інформації. Заяв. 25.06.2021; Опубл. 01.12.2021 р 3. Пат. u202103683, МПК (51) G009C 1/00; Спосіб криптографічного перетворення інформації. Заяв. 23.06.2021; Опубл. 01.12.2021 р. 4. Пат. u202103704, МПК (51) G009C 1/00; Спосіб

							криптографічного перетворення інформації. Заяв. 23.06.2021; Опубл. 01.12.2021 р. 5. Пат. u202103617, МПК (51) G009C 1/00; Спосіб криптографічного перетворення інформації. Заявл. 23.06.2021; Опубл. 01.12.2021 р. П. 3 наявність виданого підручника чи навчального посібника (включаючи електронні) або монографії (загальним обсягом не менше 5 авторських аркушів), в тому числі видані у співавторстві (обсягом не менше 1,5 авторського аркуша на кожного співавтора) 1. Євсеєв С.П., Дженюк Н.В., Толкачов М.Ю., Касілов О.В., Король О.Г., Кудій Д.А. Комп'ютерні мережі. Книга 2. Архітектура комп'ютерів. Навч. посібник Харків, – Львів: Видавництво ПП «Новий Світ – 2000», 2023. – 320 с Власний внесок 4,3 авторських аркушів. 2. Євсеєв С. П., Мілов О.В., Остапов С.Е., Северінов О.В. Кібербезпека: Основи кодування та криптографії. Навчальний посібник. Львів: "Новий Світ– 2000", 2025. – 658 3. В.Ю. Ковтун, С.П. Євсеєв, І. В. Аксьонова. Новітні технології захисту інформації. навчальний посібник. – Харків, – Львів: Видавництво ПП «Новий Світ – 2000», 2024. – 285 с. П. 4 наявність виданих навчально-методичних посібників/посібників для самостійної роботи здобувачів вищої освіти та дистанційного навчання, електронних курсів на освітніх платформах ліцензіатів, конспектів лекцій/практикумів/методичних вказівок/рекомендацій/ робочих програм, інших друкованих навчально-методичних праць загальною кількістю три найменування

							1.Основи кібербезпеки. навчально-практичний посібник / уклад. С. П. Євсеєв, О. В. Шматко, О. Б. Ахієзер, Т. В. Горбач ; за заг. ред. С. П. Євсеєва. – Харків : НТУ «ХПІ», – Львів : «Новий Світ-2000», 2025. – 95 с. – (Серія «Кібербезпека та штучний інтелект»). ISBN 978-966-418-514-8. 2. Атаки на системи штучного інтелекту. навчально-практичний посібник / уклад. С. П. Євсеєв, О. В. Шматко, О. Б. Ахієзер, В. Є. Сокол, Н. Л. Чернова, Харків : НТУ «ХПІ», – Львів : «Новий Світ-2000», 2025. – 108 с. – (Серія «Кібербезпека та штучний інтелект»). ISBN 978-966-418-515-5 3. Штучний інтелект. Нейромережева обробка інформації : архітектури, навчання, застосування : навчальний посібник у 2-х ч. : Ч. 1 / О. Г. Руденко, О. О. Безсонов, С. П. Євсеєв, О. Б. Ахієзер, Ю. І. Зайцев. ; за заг. ред. С. П. Євсеєва. – Харків : НТУ «ХПІ», – Львів : «Новий Світ-2000», 2025. – 426 с. – (Серія «Кібербезпека та штучний інтелект»). ISBN 978-966-418-517-9 4. Штучний інтелект. Нейромережева обробка інформації : архітектури, навчання, застосування : навчальний посібник у 2-х ч. : Ч. 2 / О. Г. Руденко, О. О. Безсонов, С. П. Євсеєв, О. Б. Ахієзер, Ю. І. Зайцев. ; за заг. ред. С. П. Євсеєва. – Харків : НТУ «ХПІ», – Львів : «Новий Світ-2000», 2025. – 376 с. – (Серія «Кібербезпека та штучний інтелект»). Руденко О. Г. та ін. ISBN 978-966-418-518-6 П. 6 наукове керівництво (консультування) здобувача, який одержав документ про присудження наукового ступеня Циганенко Олексій Сергійович, доктор

							філософії зі спеціальності 122 – комп'ютерні науки, тема дисертації: "Моделі та методи підвищення якості обслуговування інформаційних систем", 2022 р., Диплом ДР №003787 від 1 лютого 2022 року, Міністерство освіти і науки України. Одеський державний екологічний університет. Погасій Сергій Сергійович, доктор технічних наук, 05.13.21. Системи захисту інформації, тема дисертації: Моделі і методи захисту інформації в кіберфізичних системах, 2024 рік. Диплом ДД № 013762 від 18 лютого 2025 року. Міністерство освіти і науки України. Державний університет інформаційно-комунікаційних технологій. Мілевський Станіслав Валерійович, доктор технічних наук, 05.13.21. Системи захисту інформації, тема дисертації: Методологія побудови систем безпеки мультимедійних ресурсів в інтернет-сервісах, 2024 рік. Диплом ДД №013771 від 18 лютого 2025 року, Міністерство освіти і науки України. Національний університет "Львівська політехніка". П.7 участь в атестації наукових кадрів як офіційного опонента або члена постійної спеціалізованої вченої ради, або члена не менше трьох разових спеціалізованих вчених рад Улічев Олександр Сергійович, здобуття наукового ступеня кандидата технічних наук за спеціальністю 21.05.01 – "Інформаційна безпека держави", "Модель та методи поширення інформаційних впливів у соціальних мережах в умовах інформаційного протиборства", 13.05. 2021 р., Національний

							авіаційний університет. Костяк Марина Юріївна, здобуття наукового ступеня кандидата технічних наук за спеціальністю 05.13.21 – системи захисту інформації, “Підвищення ефективності функціонування захищених інформаційних мереж спеціального призначення”, 2021 р., Національний університет “Львівська політехника”. Ляшенко Галина Євгеніївна здобуття наукового ступеня доктора філософії за спеціальністю 172 – Електронні комунікації та радіотехніка, 2025, Харківський національний університет радіоелектроніки Кирсанов Олександр Олександрович, здобуття наукового ступеня доктора філософії за спеціальністю 172 Телекомунікації та радіотехніка галузь знань 17 Електроніка та телекомунікації, 2025, Харківський національний університет радіоелектроніки П 8. виконання функцій (повноважень, обов’язків) наукового керівника або відповідального виконавця наукової теми (проекту), або головного редактора/члена редакційної колегії/експерта (рецензента) наукового видання, включеного до переліку фахових видань України, або іноземного наукового видання, що індексується в бібліографічних базах Заступник головного редактора наукового видання «Територія безпеки», «Terra Security». https://ts.khpi.edu.ua/about/editorialTeam П.9 робота у складі експертної ради з питань проведення експертизи дисертацій МОН або у складі галузевої

							експертної ради як експерта Національного агентства із забезпечення якості вищої освіти, або у складі Акредитаційної комісії, або міжгалузевої експертної ради з вищої освіти Акредитаційної комісії, або трьох експертних комісій МОН/зазначеного Агентства, або Науково-методичної ради/науково-методичних комісій (підкомісій) з вищої або фахової передвищої освіти МОН, наукових/науково-методичних/експертних рад органів державної влади та органів місцевого самоврядування, або у складі комісій Державної служби якості освіти із здійснення планових (позапланових) заходів державного нагляду (контролю) Робота у складі НМК 6 “З інформаційних технологій ”, підкомісія F5 “Кібербезпека та захист інформації” Наказ Міністерства освіти і науки України від 02 квітня 2025 р. № 535 «Про затвердження персонального складу Науково-методичних комісій (підкомісій) сектору вищої освіти науково-методичної ради МОН») Експерт Національного фонду досліджень України (2020–2024 рр) Експерт МОН України Секція: 2. Інформатика та кібернетика (2024 р.) П. 10 участь у міжнародних наукових та/або освітніх проектах, залучення до міжнародної експертизи, наявність звання “суддя міжнародної категорії” Євсеєв Сергій Петрович – координатор робочої групи з реалізації міжнародного гранту “Conducting e-learning cyberhygiene” П. 12 наявність апробаційних та/або науково-популярних,

							та/або консультаційних (дорадчих), та/або науково-експертних публікацій з наукової або професійної тематики загальною кількістю не менше п’яти публікацій. 1. Yevseiev Serhii. Socio-Cyber-Physical Systems Security Concept / Serhii Yevseiev, Stanislav Milevskyi, Leonid Bortnik, Voropay Alexey, Kyrylo Bondarenko, Serhii Pohasii / 4th International Congress on Human-Computer Interaction, Optimization and Robotic Applications. June 9-11, 2022, Ankara, Turkey. URL: https://www.aconf.org/conf_181999.html 2. Yevseiev Serhii. Measuring Signals Synthesis Method on the Basis of Triangular Time-Pulse Modulation for Control of Radiotechnic Systems Technical Condition. Concept / Sergiy Tymchenko, Volodymyr Kutsenko, Serhii Yevseiev, Stanislav Milevskyi, Serhii Pohasii / 4th International Congress on Human-Computer Interaction, Optimization and Robotic Applications. June 9-11, 2022, Ankara, Turkey URL: https://www.aconf.org/conf_181999.html 3. Serhii Yevseiev, Pierre Murr, Stanislav Milevskyi, Olha Korol, Marharyta Melnyk. Development of a Sociocyberphysical Systems Cyber Threats Classifier. 2023 7th International Symposium on Multidisciplinary Studies and Innovative Technologies (ISMSIT). https://ieeexplore.ieee.org/document/10304895 4. Serhii Yevseiev, Stanislav Milevskyi, Vladyslav Sokol, Yevhen Melenti, Olena Akhiiezer, Kyrylo Petrenko. Methodological Foundations for Constructing Intelligent Information Security Systems. 7th International Congress on Human-Computer Interaction,

							Optimization and Robotic Applications, Proceedings Conference Paper 2025. https://ieeexplore.ieee.org/document/11017207 5. Serhii Yevseiev, Stanislav Milevskyi, Vladyslav Sokol, Yevhen Melenti, Olena Akhiiezer. Multi-Contour Intellectual Cyber Protection System Methodology. 9th International Symposium on Multidisciplinary Studies and Innovative Technologies. https://ieeexplore.ieee.org/document/11267930 П.13. проведення навчальних занять із спеціальних дисциплін іноземною мовою (крім дисциплін мовної підготовки) в обсязі не менше 50 аудиторних годин на навчальний рік 1. Information security of the state, кредитів 4,0 (64 години), КН-1122ia.e, 2022 р. П. 19 . Діяльність за спеціальністю у формі участі у професійних та/або громадських об'єднаннях член громадської організації "Східноєвропейське наукове товариство", посвідчення ES № 053.
410247	Гаврилова Алла Андріївна	Доцент, Основне місце роботи	Навчально-науковий інститут комп'ютерних наук та інформаційних технологій	Диплом спеціаліста, Харківський державний економічний університет, рік закінчення: 1994, спеціальність: Економічної інформатики і автоматизованих систем управління, Диплом магістра, Харківський національний університет радіоелектроніки, рік закінчення: 2021, спеціальність: 125 Кібербезпека, Диплом доктора філософії Н23 001755, виданий 06.12.2023,	20	Безпека та анонімність роботи в інтернеті	Підвищення кваліфікації 1) Сертифікат з курсу "Інформаційна безпека" ПК-ЦК № Р0824-0145 від 15.06.2024 р. (3 кр. – 90 год.) затверджено наказом ПК № 1729 С від 04.10.2024 2) Сертифікат з курсу "ІКТ в освіті" ПК-ЦК № Р0824-0146 від 30.06.2024 р. (3 кр. – 90 год.) затверджено наказом ПК № 1729 С від 04.10.2024 3) UNIVERSITY OF THE NATIONAL EDUCATION COMMISSION (KRAKOW, POLAND). TOPIC: METHODS AND TECHNICAL MEANS OF INFORMATION PROTECTION. Сертифікат № KIO/23 - 04 - 12/2025 (180 ГОДИН (6 КРЕДИТІВ ECTS, з 20.02.2025 р. по 20.04.2025 р.,

				Атестат доцента АД 016983, виданий 18.02.2025			затверджено наказом №2186С від 21.11.2025р.) Пункти відповідності ліцензійних умов: П. 1, 3, 4, 5, 7, 8, 12, 13, 19. П. 1 наявність не менше п'яти публікацій у періодичних наукових виданнях, що включені до переліку фахових видань України, до наукометричних баз, зокрема Scopus, Web of Science Core Collection 1. Havrylova A., Aksonova I., Khokhlachova Yu., Milevska T., Dunaiev S. Rationale for improving authentication protocols in the conditions of postquantum cryptography // Безпека інформації. – Київ, 2024. – Vol. 30. – issue 1. pp. 130-139 (DOI: 10.31673/2409-7292.2024.010011) URL: https://repository.kpi.kharkov.ua/items/b7b88fa3-41e7-4c25-9bbb-7578e6a2bc5d. 2. Havrylova A., Korol O., Voropay N., Sevriukova Y., Bondarenko K. Analysis of cryptographic authentication and manipulation detection methods for big data // Сучасний захист інформації, 2024, №1(57) P. 97 – 102. (DOI: 10.31673/2409-7292.2024.010011) URL: https://repository.kpi.kharkov.ua/items/b7b88fa3-41e7-4c25-9bbb-7578e6a2bc5d. 3. Shmatko O., Yevseiev S., Dudykevych V., Milevskyi S., Solnyshkova S., Havrylova A., Shestak Ya., Oriekhov S., Korsunov S., & Kravchenko S. (2024). Development of a method for synthesizing an information-analytical system for assessing the level of information transmission channels protection. Eastern-European Journal of Enterprise Technologies, 2/9 (128), 36–43. DOI: 10.15587/1729-4061.2024.302495 URL: https://repository.kpi.k

							harkov.ua/items/b1de9005-f882-44a1-85f6-5feac9bb3674 (Scopus) 4. Yevseiev, S., Havrylova, A., Milevskyi, S., Sinitsyn, I., Chalapko, V., Dukin, H., Hrebeniuk, V., Diedov, M., Bekirova, L., & Shpak, O. (2023). Development of an improved SSL/TLS protocol using post-quantum algorithms. Eastern-European Journal of Enterprise Technologies, 3(9 (123), 33–48. (DOI:10.15587/1729-4061.2023.281795/) URL: https://journals.uran.ua/eejet/article/view/281795 (Scopus) (5. Havrylova, A., Khokhlachova, Y., Tkachov, A., Voropay, N., & Khvostenko V. (2023). Justification of directions for improving authentication protocols in information and communication systems. Ukrainian Information Security Research Journal, Vol. 25 No. 1, 6–19. https://doi.org/10.18372/2410-7840.25.17593 6. Гаврилова Алла, Хохлачова Юлія, Погорелов Володимир. Аналіз застосування гібридних крипто-кодових конструкцій для підвищення рівня стійкості геш-кодів до зламу / Алла Гаврилова, Юлія Хохлачова, Володимир Погорелов // «Безпека інформації», 2022. – Том 28. – № 2. URL:https://www.researchgate.net/publication/370823626_ANALIZ_ZASTOSUVANNA_GIBRIDNIH_KRIPTO-KODOVIH_KONSTRUKCIJ_DLA_PIDVISENNA_RIVNA_STIJKOSTI_GES-KODIV_DO_ZLOMU (DOI: 10.18372/2225-5036.28.16953) П.3 наявність виданого підручника чи навчального посібника (включаючи електронні) або монографії (загальним обсягом не менше 5 авторських аркушів), в тому числі видані у співавторстві

							(обсягом не менше 1,5 авторського аркуша на кожного співавтора); 1. Технології баз даних : навчально-практичний посібник / уклад. А. А. Гаврилова, С. С. Погасій, Р. В. Корольов, В. С. Хвостенко, Т. С. Мілевська ; за заг. ред. С. П. Євсеєва. – Харків : НТУ «ХПІ», – Львів : «Новий Світ-2000», 2025. – 222 с. – (Серія «Кібербезпека та штучний інтелект»). ISBN 978-966-418-516-2 URL: https://library.kpi.kharkov.ua/files/files/documents/tebada.pdf. (9,25 ум. др. арк. / 1,85 ум. друк. арк. власного внеску) П. 4 наявність виданих навчально-методичних посібників/посібників для самостійної роботи здобувачів вищої освіти та дистанційного навчання, електронних курсів на освітніх платформах ліцензіатів, конспектів лекцій/практикумів/методичних вказівок/рекомендацій/ робочих програм, інших друкованих навчально-методичних праць загальною кількістю три найменування 1. Методичні вказівки до проведення виробничої практики [Електронний ресурс] : для студентів ден. та заочн. форм навчання першого (бакалаврського) рівня вищої освіти за спец. 125 (F5) "Кібербезпека та захист інформації", 256 (К3) "Національна безпека (за окремими сферами забезпечення і видами діяльності)" та 257 (К4) "Управління інформаційною безпекою" / уклад.: Р. В. Корольов, А. М. Ткачов, А. А. Гаврилова ; Нац. техн. ун-т "Харків. політехн. ін-т". – Електрон. текст. дані. – Харків : НТУ "ХПІ", 2025. – 35 с. URI: https://repository.kpi.kharkov.ua/handle/KhPI-Press/95152 (1,45 ум. др. арк. / 0,486 ум.

							друк. арк. власного внеску) 2. Методичні вказівки до проведення технологічної практики [Електронний ресурс] : для студентів ден. та заочн. форм навчання першого (бакалаврського) рівня вищої освіти за спец. 125 (F5) "Кібербезпека та захист інформації" / уклад.: А. А. Гаврилова ; Нац. техн. ун-т "Харків. політехн. ін-т". – Електрон. текст. дані. – Харків : НТУ "ХПІ", 2025. – 25 с. URI: https://repository.kpi.kharkov.ua/handle/KhPI-Press/95153 (1,04 ум. др. арк. / 1,04 ум. друк. арк. власного внеску) 3. Методичні вказівки до виконання бакалаврських кваліфікаційних робіт [Електронний ресурс] : для студентів ден. форми навчання першого (бакалаврського) рівня вищої освіти за спец. 256 (К3) "Національна безпека (за окремими сферами забезпечення і видами діяльності)" та 257 (К4) "Управління інформаційною безпекою" / уклад.: Р. В. Корольов, А. М. Ткачов, А. А. Гаврилова ; Нац. техн. ун-т "Харків. політехн. ін-т". – Електрон. текст. дані. – Харків : НТУ "ХПІ", 2025. – 64 с. URI: https://repository.kpi.kharkov.ua/handle/KhPI-Press/95155 (2,67 ум. др. арк. / 0,889 ум. друк. арк. власного внеску) 4. Методичні вказівки до проведення науково-дослідницької практики [Електронний ресурс] : для студентів ден. форми навчання другого (магістерського) рівня вищої освіти за спец. 125 (F5) "Кібербезпека та захист інформації" / уклад.: Р. В. Корольов, А. М. Ткачов, А. А. Гаврилова ; Нац. техн. ун-т "Харків. політехн. ін-т". – Електрон. текст. дані. – Харків :

							НТУ "ХПІ", 2025. – 36 с. URI: https://repository.kpi.kharkov.ua/handle/KhPI-Press/95157 (1,5 ум. др. арк. / 0,5 ум. друк. арк. власного внеску) 5. Методичні вказівки до проведення переддипломної практики [Електронний ресурс] : для студентів ден. та заочн. форм навчання другого (магістерського) рівня вищої освіти за спец. 125 (F5) "Кібербезпека та захист інформації" / уклад.: Р. В. Корольов, С. В. Мілевський, А. А. Гаврилова ; Нац. техн. ун-т "Харків. політехн. ін-т". – Електрон. текст. дані. – Харків : НТУ "ХПІ", 2025. – 32 с. URI: https://repository.kpi.kharkov.ua/handle/KhPI-Press/95159 (1,33 ум. др. арк. / 0,44 ум. друк. арк. власного внеску) 6. Методичні вказівки до проведення переддипломної практики [Електронний ресурс] : для студентів ден. форми навчання першого (бакалаврського) рівня вищої освіти за спец. 256 (К3) "Національна безпека (за окремими сферами забезпечення і видами діяльності)" та 257 (К4) "Управління інформаційною безпекою" / уклад.: Р. В. Корольов, А. М. Ткачов, А. А. Гаврилова ; Нац. техн. ун-т "Харків. політехн. ін-т". – Електрон. текст. дані. – Харків : НТУ "ХПІ", 2025. – 35 с. URI: https://repository.kpi.kharkov.ua/handle/KhPI-Press/95160 (1,458 ум. др. арк. / 0,486 ум. друк. арк. власного внеску) 7. Методичні вказівки до виконання лабораторних робіт з дисципліни "Управління ІТ-проєктами та їх безпека" [Електронний ресурс] : для студентів ден. та заочн. форм навчання першого (бакалаврського) рівня вищої освіти за спец. F5 "Кібербезпека

							та захист інформації", К3 "Національна безпека (за окремими сферами забезпечення і видами діяльності)" та К4 "Управління інформаційною безпекою" / уклад.: А. А. Гаврилова, І. В. Аксьонова ; Нац. техн. ун-т "Харків. політехн. ін-т". – Електрон. текст. дані. – Харків : НТУ "ХПІ", 2025. – 56 с. URI: https://repository.kpi.kharkov.ua/handle/KhPI-Press/95162 (2,33 ум. др. арк. / 1,17 ум. друк. арк. власного внеску) 8. Інформаційні системи електронної комерції: навчальний посібник / С.Е. Остапов, С.П. Євсеєв, К.П. Газдюк, О.Ю. Тарновецька, Л.М. Шумиляк, І.В. Аксьонова, А.А. Гаврилова. Чернівецький національний університет ім. Ю. Федьковича, Національний технічний університет “Харківський Політехнічний Інститут”, – Львів: Видавництво “Новий Світ-2000”, 2024. 282 с. (11,75 ум. др. арк. / 1,68 ум. друк. арк. власного внеску) 9. Методичні вказівки до проведення виробничої практики [Електронний ресурс] : для студентів першого (бакалаврського) рівня вищої освіти за спец. 125 “Кібербезпека та захист інформації" / уклад.: С. П. Євсеєв, О. Г. Король, А. А. Гаврилова ; Нац. техн. ун-т “Харків. політехн. ін-т”. – Електрон. текст. дані. – Харків : НТУ “ХПІ”, 2024. – 22 с. (1,375 ум. др. арк. / 0,458 ум. друк. арк. власного внеску) URI: https://repository.kpi.kharkov.ua/handle/KhPI-Press/81233. 10. Методичні вказівки до виконання лабораторних робіт з дисципліни “Управління ІТ-проєктами та їх безпека” [Електронний ресурс] : для студентів першого (бакалаврського) рівня вищої освіти за спец. 125

							“Кібербезпека та захист інформації” / уклад.: А. А. Гаврилова, І. В. Аксьонова ; Нац. техн. ун-т “Харків. політехн. ін-т”. – Електрон. текст. дані. – Харків : НТУ “ХПІ”, 2024. – 55 с. URI: https://repository.kpi.kharkov.ua/handle/KhPI-Press/81234 (3,44 ум. др. арк. / 1,72 ум. друк. арк. власного внеску) П. 5 захист дисертації на здобуття наукового ступеня Диплом доктора філософії, 125 – Кібербезпека та захист інформації, тема дисертації: Моделі та методи контролю цілісності та автентичності на основі каскадного алгоритму UMAC. Диплом Н23 № 001755, від 6 грудня 2023 року, Міністерство освіти і науки України, Національний авіаційний університет. П. 7. участь в атестації наукових кадрів як офіційного опонента або члена постійної спеціалізованої вченої ради, або члена не менше трьох разових спеціалізованих вчених рад Вчений секретар спеціалізованої вченої ради Д 64.050.21 – Технічні науки, Національний технічний університет "Харківський політехнічний інститут" (Наказ МОН України №986 від 08.07.2025 р.) https://blogs.kpi.kharkov.ua/v2/vr/spetsializovani-rady/d-64-050-21 П. 8 виконання функцій (повноважень, обов’язків) наукового керівника або відповідального виконавця наукової теми (проекту), або головного редактора/члена редакційної колегії/експерта (рецензента) наукового видання, включеного до переліку фахових видань України, або іноземного наукового видання, що

							індексується в бібліографічних базах 1. Відповідальний виконавець в госпдоговірній науково-дослідній роботі за темою: “Моделі і методи контролю цілісності та автентичності на основі каскадного алгоритму UMAC” (№ ДР 87-2023/09.01.08 від 01.05.2023 р.) (Національний авіаційний університет, м. Київ). 2. Відповідальний виконавець в ініціативній науко-дослідній роботі за темою: “Моделювання соціо-кіберфізичних систем” (№ ДР 0123U101018 від 12.02.23) (Національний технічний університет “Харківський політехнічний інститут”, м. Харків). П. 12 наявність апробаційних та/або науково-популярних, та/або консультаційних (дорадчих), та/або науково-експертних публікацій з наукової або професійної тематики загальною кількістю не менше п’яти публікацій 1. Гаврилова А. А. Аналіз криптографічних алгоритмів поданих до третього туру конкурсу NIST / А. А. Гаврилова // Актуальні питання забезпечення службово-бойової діяльності сил сектору безпеки і оборони : матеріали всеукр. круг. столу (м. Харків, 23 квіт. 2021 р.) / редкол.: Є. О. Меленті, І. В. Євтушенко, О. А. Гарбузов, В. О. Пономарьов – Х.: ФОП Бровін О. В., 2021. – Вип. 5. – С. 361 – 365. URL: https://repository.hneu.edu.ua/bitstream/123456789/25621/1/%D0%93%D0%B0%D0%B2%D1%80%D0%B8%D0%BB%D0%BE%D0%B2%D0%B0%D0%A5%D0%B0%D1%80_%D0%BA%D0%BE%D0%B2%D0%A1%D0%91%D0%A3.pdf 2. Gavrilova A. Synergy of building cybersecurity systems / S. Yevseiev, V.

							Ponomarenko, O. Laptiev, O. Milov, O. Korol, S. Milevskyi, S. Pohasii, A. Tkachov, O. Shmatko, Y. Melenti, O. Sievierinov, S. Ostapov, A. Gavrilova, O. Tsyhanenko, S. Herasimov, E. Nyemkova, B. Tomashevsky, I. Hrod, I. Opirskyy, V. Zvieriev, O. Prokopenko, V. Savchenko, O. Barabash, V. Sobchuk, G. Shuklin, V. Khvostenko, O. Tymochko, M. Pavlenko, A. Trystan, S. Florov // monograph. – Kharkiv: PC TECHNOLOGY CENTER, 2021. – 188 p. (P. 102 – 147). – https://doi.org/10.15587/978-617-7319-31-2 3. Havrylova Alla. Research of collision properties of the modified UMAC algorithm on crypto-code constructions / Serhii Yevseiev, Alla Havrylova, Olha Korol, Oleh Dmitriiev, Oleksii Nesmiian, Yevhen Yufa, Asadi Hrebennikov // "EUREKA: Physics and Engineering". – 2022. – Number 1 (38), P. 34 – 43. https://journal.eu-jr.eu/engineering/article/view/2213 (https://doi.org/10.21303/2461-4262.2022.002213) 4. Гаврилова А. А. Перевірка на колізійність геш-кодів які сформовано за допомогою алгоритму UMAC на крипто-кодових конструкціях / С. П. Євсеєв, А. А. Гаврилова // "Математика. Інформаційні технології. Освіта"; тези доповідей на XI Міжнародній науково-практичній конференції, Луцьк-Світязь, 3 – 5 червня 2022 р. – Луцьк, 2022. – С. 66 – 68. https://repository.kpi.kharkov.ua/handle/KhPI-Press/89797 5. Havrylova Alla. Estimating the Efficiency of Using the Modified UMAC Algorithm / Alla Havrylova, Andrii Tkachov, Irada Rahim qizi Rahimova // 2022 IEEE 3rd KhPI Week on Advanced Technology (KhPIWeek) 03-07 October 2022 .– 2022.

							Kharkiv, Ukraine: Publisher: IEEE, P. 1 – 5 URL: https://ieeexplore.ieee.org/document/9916425 (Scopus) 6. Havrylova A. Models of socio-cyber-physical systems security: monograph / Yevseiev S., Khokhlachova Yu., Ostapov S., Laptiev O., Korol O., Milevskyi S., Milov O., Pohasii S., Melenti Y., Hrebeniuk V., Havrylova A., Herasymov S., Korolev R., Barabash O., Sobchuk V., Kyrychok R., Shuklin G., Akhramovych V., Savchenko V., Golovashych S., Lezik O., Opirskyy I., Voitko O., Yerhidzei K., Mykus S., Pribyliev Y., Prokopenko O., Vlasov A., Dzheniuk N., Tolkachov M. – Kharkiv: PC TECHNOLOGY CENTER, 2023. – 168 p. (DOI: 10.15587/978-617-7319-72-5) (SCOPUS) . 7. Гаврилов А. В., Гаврилова А. А. Оцінка рівня захищеності повідом лень електронної пошти на транспортному рівні передачі комунікаційними каналами зв'язку // Актуальні питання забезпечення службово-бойової діяльності сил сектору безпеки і оборони: матеріали III Всеукраїнської конференції, м. Харків, 25 квітня 2024 року. – Харків: ФОП Бровін О.В., 2024., С. 219 – 224 https://dspace.nlu.edu.ua/jspui/bitstream/123456789/20100/1/konf_APZSBDSBO-2024.pdf 8. Алла Гаврилова, Ірина Аксьонова. Використання алгоритмів CCC/UMAC для вдосконалення протоколу SSL/TLS. Матерали XIII міжнародної науково-технічної конференції "ITSec: Безпека інформаційних технологій". м. Львів, 9-11 травня 2024 р. Л.: ЛНУ ім. І. Франка, 2024, 265 с. (С. 69 – 70). https://sci.ldubgd.edu.ua/bitstream/123456789/13509/1/2024-

							ITSec_%D0%BA%D1%96%D0%B1%D0%B5%D1%80%D0%B1%D0%B5%D0%B7%D0%BF%D0%B5%D0%BA%D0%B0.pdf 9. Havrylova A., Milov O., Rahimova I., Golovashych S., Aksonova I., Pecherytsia D. Cybersecurity of SMART Technologies Using Deep Learning Methods. ISMSIT 2024 – 8th International Symposium on Multidisciplinary Studies and Innovative Technologies, Proceedings, 2024. – Ankara, Turkiye. DOI: 10.1109/ISMSIT63511.2024.10757295. URL: https://ieeexplore.ieee.org/document/10757295. (SCOPUS) 10. Havrylova A., Tkachov A., Hapon A., Balagura D., Sievierinov O., Bukatych I. Analysis of the Software Security Protection. ISMSIT 2024 – 8th International Symposium on Multidisciplinary Studies and Innovative Technologies, Proceedings, 2024. – Ankara, Turkiye. DOI: 10.1109/ISMSIT63511.2024. 10757202 URL: https://ieeexplore.ieee.org/document/10757202. (SCOPUS) 11. Гаврилова А.А., Сосновий В.В. Аналіз загроз інформаційної безпеки за об'єктовим принципом. Проблеми та шляхи захисту інформаційно-психологічної і духовної безпеки особи, суспільства, держави: матеріали п'ятої Міжнародної науково- практичної конференції. – м. Київ, 28 червня 2024 р. – К., 2025. – С. 24 – 25. https://dspace.kntu.kr.ua/server/api/core/bitstreams/8683d444-de7e-442e-bcec-83596a5969e6/content 12. Гаврилова А.А., Сіпко Д.С. Аналіз загроз соціальної інженерії на теренах кіберпростору. Проблеми та шляхи захисту інформаційно-психологічної і духовної безпеки особи, суспільства, держави: матеріали

							п’ятої Міжнародної науково- практичної конференції. – м. Київ, 28 червня 2024 р. – К., 2025. – С. 26 – 27. https://dspace.kntu.kr.ua/server/api/core/bitstreams/8683d444-de7e-442e-bcec-83596a5969e6/content 13. Гаврилова А.А., Коваленко Д.С. Аналіз впливу інформаційної війни на національну безпеку. Проблеми та шляхи захисту інформаційно-психологічної і духовної безпеки особи, суспільства, держави: матеріали п’ятої Міжнародної науково- практичної конференції. – м. Київ, 28 червня 2024 р. – К., 2025. – С. 28 – 29. https://dspace.kntu.kr.ua/server/api/core/bitstreams/8683d444-de7e-442e-bcec-83596a5969e6/content 14. Havrylova A.A., Tkachov A.M., Hapon A.O. Approaches to detecting vulnerabilities in software to ensure code protection. Матеріали V Міжнародної науково-практичної конференції «Інформаційна безпека та інформаційні технології», Харків, Одеса, Луцьк, 9–11 червня 2025 року. P. 59 – 60 URL: https://essuir.sumdu.edu.ua/server/api/core/bitstreams/a3082f67-b8fe-4b39-a74d-c3591992efd3/content 15. Гаврилова А. А., Аксьонова І. В. Фреймворк аналізу кіберзагроз як інструмент управління корпоративною безпекою. Актуальні питання забезпечення кібербезпеки та захисту інформації: матеріали XI Міжнародної науково-практичної конференції, 24 квітня 2025 р., Київ / редкол.: О. І. Тимошенко [та ін.]. – Київ: Вид-во Європейського університету, 2025. – С. 10 – 12. https://files.znu.edu.ua/files/Bibliobooks/Inshi84/0063968.pdf 16. Havrylova A., Tolkachov M.,

							Dzheniuk N., Chechui O., Hapon A., Tiutiunyk V. Cognitive Approach to Cybersecurity: Causality Analysis and Situational Learning. 2025 7th International Congress on Human-Computer Interaction, Optimization and Robotic Applications (ICHORA), May 23-24, 2025 Ankara-Türkiye (Hybrid), 2025. Pp. 1 – 4. DOI: 10.1109/ICHORA65333.2025.11017107 (SCOPUS) 17. Havrylova A., Khvostenko V., Milevskyi S. Development of an Advanced SSL/TLS Protocol for Transferring Requests to a 3D-Printer: monograf In: Durakbasa, N. M., Cetinkaya, K., Demircioglu, P., Bogrekci, I. (eds) Digitalization in Additive Manufacturing. ICPTDI 2025. Springer Tracts in Additive Manufacturing. Springer, Cham. Part F641, P. 489–503. https://link.springer.com/chapter/10.1007/978-3-031-84873-5_38 П 13. проведення навчальних занять із спеціальних дисциплін іноземною мовою (крім дисциплін мовної підготовки) в обсязі не менше 50 аудиторних годин на навчальний рік 1. Introduction to the specialty. Introductory practice (3 кр.):Всього 32 год.: лекцій – 16 год., практик – 16 год. (КН-1125ia.e) 2. Decentralized systems (4 кр.) Всього 50 год.: лекцій – 32 год., практик – 16 год., консультації – 2 год. (КН-1122ia.e) П. 19 діяльність за спеціальністю у формі участі у професійних та/або громадських об'єднаннях член Громадської організації "СХІДНО-ЄВРОПЕЙСЬКЕ НАУКОВЕ ТОВАРИСТВО" з 20.05.2022р. посвідчення № ES 055
410247	Гаврилова Алла	Доцент, Основне	Навчально-науковий	Диплом спеціаліста,	20	Основи управління в	Підвищення кваліфікації

	Андріївна	місце роботи	інститут комп'ютерних наук та інформаційних технологій	Харківський державний економічний університет, рік закінчення: 1994, спеціальність: Економічної інформатики і автоматизованих систем управління, Диплом магістра, Харківський національний університет радіоелектроніки, рік закінчення: 2021, спеціальність: 125 Кібербезпека, Диплом доктора філософії Н23 001755, виданий 06.12.2023, Атестат доцента АД 016983, виданий 18.02.2025		проєктах галузі кібербезпеки та захисту інформації	1) Сертифікат з курсу "Інформаційна безпека" ПК-ЦК № Р0824-0145 від 15.06.2024 р. (3 кр. – 90 год.) затверджено наказом ПК № 1729 С від 04.10.2024 2) Сертифікат з курсу "ІКТ в освіті" ПК-ЦК № Р0824-0146 від 30.06.2024 р. (3 кр. – 90 год.) затверджено наказом ПК № 1729 С від 04.10.2024 3) UNIVERSITY OF THE NATIONAL EDUCATION COMMISSION (KRAKOW, POLAND). TOPIC: METHODS AND TECHNICAL MEANS OF INFORMATION PROTECTION. Сертифікат № KIO/23 - 04 - 12/2025 (180 ГОДИН (6 КРЕДИТІВ ECTS, з 20.02.2025 р. по 20.04.2025 р., затверджено наказом №2186С від 21.11.2025р.) Пункти відповідності ліцензійних умов: П. 1, 3, 4, 5, 7, 8, 12, 13, 19. П. 1 наявність не менше п'яти публікацій у періодичних наукових виданнях, що включені до переліку фахових видань України, до наукометричних баз, зокрема Scopus, Web of Science Core Collection 1. Havrylova A., Aksonova I., Khokhlachova Yu., Milevska T., Dunaiev S. Rationale for improving authentication protocols in the conditions of postquantum cryptography // Безпека інформації. – Київ, 2024. – Vol. 30. – issue 1. pp. 130-139 (DOI: 10.31673/2409-7292.2024.010011) URL: https://repository.kpi.kharkov.ua/items/b7b88fa3-41e7-4c25-9bbb-7578e6a2bc5d. 2. Havrylova A., Korol O., Voropay N., Sevriukova Y., Bondarenko K. Analysis of cryptographic authentication and manipulation detection methods for big data // Сучасний захист інформації, 2024, №1(57) P. 97 – 102. (DOI: 10.31673/2409-

							7292.2024.010011) URL: https://repository.kpi.kharkov.ua/items/b7b88fa3-41e7-4c25-9bbb-7578e6a2bc5d. 3. Shmatko O., Yevseiev S., Dudykevych V., Milevskyi S., Solnyshkova S., Havrylova A., Shestak Ya., Oriekhov S., Korsunov S., & Kravchenko S. (2024). Development of a method for synthesizing an information-analytical system for assessing the level of information transmission channels protection. Eastern-European Journal of Enterprise Technologies, 2/9 (128), 36–43. DOI: 10.15587/1729-4061.2024.302495 URL: https://repository.kpi.kharkov.ua/items/b1de9005-f882-44a1-85f6-5feac9bb3674 (Scopus) 4. Yevseiev, S., Havrylova, A., Milevskyi, S., Sinitsyn, I., Chalapko, V., Dukin, H., Hrebeniuk, V., Diedov, M., Bekirova, L., & Shpak, O. (2023). Development of an improved SSL/TLS protocol using post-quantum algorithms. Eastern-European Journal of Enterprise Technologies, 3(9 (123), 33–48. (DOI:10.15587/1729-4061.2023.281795/) URL: https://journals.uran.ua/eejet/article/view/281795 (Scopus) (5. Havrylova, A., Khokhlachova, Y., Tkachov, A., Voropay, N., & Khvostenko V. (2023). Justification of directions for improving authentication protocols in information and communication systems. Ukrainian Information Security Research Journal, Vol. 25 No. 1, 6–19. https://doi.org/10.18372/2410-7840.25.17593 6. Гаврилова Алла, Хохлачова Юлія, Погорелов Володимир. Аналіз застосування гібридних крипто-кодових конструкцій для підвищення рівня стійкості геш-кодів до зламу / Алла

							Гаврилова, Юлія Хохлачова, Володимир Погорелов // «Безпека інформації», 2022. – Том 28. – № 2. URL:https://www.researchgate.net/publication/370823626_ANALIZ_ZASTOSUVANNA_GIBRIDNIH_KRIPTO-KODOVIH_KONSTRUKCIJ_DLA_PIDVISENNA_RIVNA_STIJKOSTI_GES-KODIV_DO_ZLOMU (DOI: 10.18372/2225-5036.28.16953) П.3 наявність виданого підручника чи навчального посібника (включаючи електронні) або монографії (загальним обсягом не менше 5 авторських аркушів), в тому числі видані у співавторстві (обсягом не менше 1,5 авторського аркуша на кожного співавтора); 1. Технології баз даних : навчально-практичний посібник / уклад. А. А. Гаврилова, С. С. Погасій, Р. В. Корольов, В. С. Хвостенко, Т. С. Мілевська ; за заг. ред. С. П. Євсеєва. – Харків : НТУ «ХПІ», – Львів : «Новий Світ-2000», 2025. – 222 с. – (Серія «Кібербезпека та штучний інтелект»). ISBN 978-966-418-516-2 URL: https://library.kpi.kharkov.ua/files/files/documents/tebada.pdf. (9,25 ум. др. арк. / 1,85 ум. друк. арк. власного внеску) П. 4 наявність виданих навчально-методичних посібників/посібників для самостійної роботи здобувачів вищої освіти та дистанційного навчання, електронних курсів на освітніх платформах ліцензіатів, конспектів лекцій/практикумів/методичних вказівок/рекомендацій/ робочих програм, інших друкованих навчально-методичних праць загальною кількістю три найменування 1. Методичні вказівки до проведення

							виробничої практики [Електронний ресурс] : для студентів ден. та заочн. форм навчання першого (бакалаврського) рівня вищої освіти за спец. 125 (F5) "Кібербезпека та захист інформації", 256 (K3) "Національна безпека (за окремими сферами забезпечення і видами діяльності)" та 257 (K4) "Управління інформаційною безпекою" / уклад.: Р. В. Корольов, А. М. Ткачов, А. А. Гаврилова ; Нац. техн. ун-т "Харків. політехн. ін-т". – Електрон. текст. дані. – Харків : НТУ "ХПІ", 2025. – 35 с. URI: https://repository.kpi.kharkov.ua/handle/KhPI-Press/95152 (1,45 ум. др. арк. / 0,486 ум. друк. арк. власного внеску) 2. Методичні вказівки до проведення технологічної практики [Електронний ресурс] : для студентів ден. та заочн. форм навчання першого (бакалаврського) рівня вищої освіти за спец. 125 (F5) "Кібербезпека та захист інформації" / уклад.: А. А. Гаврилова ; Нац. техн. ун-т "Харків. політехн. ін-т". – Електрон. текст. дані. – Харків : НТУ "ХПІ", 2025. – 25 с. URI: https://repository.kpi.kharkov.ua/handle/KhPI-Press/95153 (1,04 ум. др. арк. / 1,04 ум. друк. арк. власного внеску) 3. Методичні вказівки до виконання бакалаврських кваліфікаційних робіт [Електронний ресурс] : для студентів ден. форми навчання першого (бакалаврського) рівня вищої освіти за спец. 256 (K3) "Національна безпека (за окремими сферами забезпечення і видами діяльності)" та 257 (K4) "Управління інформаційною безпекою" / уклад.: Р. В. Корольов, А. М. Ткачов, А. А. Гаврилова ; Нац. техн. ун-т "Харків. політехн.

							ін-т". – Електрон. текст. дані. – Харків : НТУ "ХПІ", 2025. – 64 с. URI: https://repository.kpi.kharkov.ua/handle/KhPI-Press/95155 (2,67 ум. др. арк. / 0,889 ум. друк. арк. власного внеску) 4. Методичні вказівки до проведення науково-дослідницької практики [Електронний ресурс] : для студентів ден. форми навчання другого (магістерського) рівня вищої освіти за спец. 125 (F5) "Кібербезпека та захист інформації" / уклад.: Р. В. Корольов, А. М. Ткачов, А. А. Гаврилова ; Нац. техн. ун-т "Харків. політехн. ін-т". – Електрон. текст. дані. – Харків : НТУ "ХПІ", 2025. – 36 с. URI: https://repository.kpi.kharkov.ua/handle/KhPI-Press/95157 (1,5 ум. др. арк. / 0,5 ум. друк. арк. власного внеску) 5. Методичні вказівки до проведення переддипломної практики [Електронний ресурс] : для студентів ден. та заочн. форм навчання другого (магістерського) рівня вищої освіти за спец. 125 (F5) "Кібербезпека та захист інформації" / уклад.: Р. В. Корольов, С. В. Мілевський, А. А. Гаврилова ; Нац. техн. ун-т "Харків. політехн. ін-т". – Електрон. текст. дані. – Харків : НТУ "ХПІ", 2025. – 32 с. URI: https://repository.kpi.kharkov.ua/handle/KhPI-Press/95159 (1,33 ум. др. арк. / 0,44 ум. друк. арк. власного внеску) 6. Методичні вказівки до проведення переддипломної практики [Електронний ресурс] : для студентів ден. форми навчання першого (бакалаврського) рівня вищої освіти за спец. 256 (К3) "Національна безпека (за окремими сферами забезпечення і видами діяльності)" та 257 (К4) "Управління

							інформаційною безпекою" / уклад.: Р. В. Корольов, А. М. Ткачов, А. А. Гаврилова ; Нац. техн. ун-т "Харків. політехн. ін-т". – Електрон. текст. дані. – Харків : НТУ "ХПІ", 2025. – 35 с. URI: https://repository.kpi.kharkov.ua/handle/KhPI-Press/95160 (1,458 ум. др. арк. / 0,486 ум. друк. арк. власного внеску) 7. Методичні вказівки до виконання лабораторних робіт з дисципліни "Управління ІТ-проєктами та їх безпека" [Електронний ресурс] : для студентів ден. та заочн. форм навчання першого (бакалаврського) рівня вищої освіти за спец. F5 "Кібербезпека та захист інформації", К3 "Національна безпека (за окремими сферами забезпечення і видами діяльності)" та К4 "Управління інформаційною безпекою" / уклад.: А. А. Гаврилова, І. В. Аксьонова ; Нац. техн. ун-т "Харків. політехн. ін-т". – Електрон. текст. дані. – Харків : НТУ "ХПІ", 2025. – 56 с. URI: https://repository.kpi.kharkov.ua/handle/KhPI-Press/95162 (2,33 ум. др. арк. / 1,17 ум. друк. арк. власного внеску) 8. Інформаційні системи електронної комерції: навчальний посібник / С.Е. Остапов, С.П. Євсеєв, К.П. Газдюк, О.Ю. Тарновецька, Л.М. Шумиляк, І.В. Аксьонова, А.А. Гаврилова. Чернівецький національний університет ім. Ю. Федьковича, Національний технічний університет “Харківський Політехнічний Інститут”, – Львів: Видавництво “Новий Світ-2000”, 2024. 282 с. (11,75 ум. др. арк. / 1,68 ум. друк. арк. власного внеску) 9. Методичні вказівки до проведення виробничої практики [Електронний ресурс] : для студентів першого (бакалаврського)

							рівня вищої освіти за спец. 125 “Кібербезпека та захист інформації" / уклад.: С. П. Євсеєв, О. Г. Король, А. А. Гаврилова ; Нац. техн. ун-т “Харків. політехн. ін-т”. – Електрон. текст. дані. – Харків : НТУ “ХПІ”, 2024. – 22 с. (1,375 ум. др. арк. / 0,458 ум. друк. арк. власного внеску) URI: https://repository.kpi.kharkov.ua/handle/KhPI-Press/81233. 10. Методичні вказівки до виконання лабораторних робіт з дисципліни “Управління ІТ-проєктами та їх безпека” [Електронний ресурс] : для студентів першого (бакалаврського) рівня вищої освіти за спец. 125 “Кібербезпека та захист інформації” / уклад.: А. А. Гаврилова, І. В. Аксьонова ; Нац. техн. ун-т “Харків. політехн. ін-т”. – Електрон. текст. дані. – Харків : НТУ “ХПІ”, 2024. – 55 с. URI: https://repository.kpi.kharkov.ua/handle/KhPI-Press/81234 (3,44 ум. др. арк. / 1,72 ум. друк. арк. власного внеску) П. 5 захист дисертації на здобуття наукового ступеня Диплом доктора філософії, 125 – Кібербезпека та захист інформації, тема дисертації: Моделі та методи контролю цілісності та автентичності на основі каскадного алгоритму UMAC. Диплом Н23 № 001755, від 6 грудня 2023 року, Міністерство освіти і науки України, Національний авіаційний університет. П. 7. участь в атестації наукових кадрів як офіційного опонента або члена постійної спеціалізованої вченої ради, або члена не менше трьох разових спеціалізованих вчених рад Вчений секретар спеціалізованої вченої ради Д 64.050.21 – Технічні науки,

							Національний технічний університет "Харківський політехнічний інститут" (Наказ МОН України №986 від 08.07.2025 р.) https://blogs.kpi.kharkov.ua/v2/vr/spetsializovani-rady/d-64-050-21 П. 8 виконання функцій (повноважень, обов'язків) наукового керівника або відповідального виконавця наукової теми (проекту), або головного редактора/члена редакційної колегії/експерта (рецензента) наукового видання, включеного до переліку фахових видань України, або іноземного наукового видання, що індексується в бібліографічних базах 1. Відповідальний виконавець в госпдоговірній науково-дослідній роботі за темою: "Моделі і методи контролю цілісності та автентичності на основі каскадного алгоритму UMAC" (№ ДР 87-2023/09.01.08 від 01.05.2023 р.) (Національний авіаційний університет, м. Київ). 2. Відповідальний виконавець в ініціативній науко-дослідній роботі за темою: "Моделювання соціо-кіберфізичних систем" (№ ДР 0123U101018 від 12.02.23) (Національний технічний університет "Харківський політехнічний інститут", м. Харків). П. 12 наявність апробаційних та/або науково-популярних, та/або консультаційних (дорадчих), та/або науково-експертних публікацій з наукової або професійної тематики загальною кількістю не менше п'яти публікацій 1. Гаврилова А. А. Аналіз криптографічних алгоритмів поданих до третього туру конкурсу NIST / А. А. Гаврилова //

							Актуальні питання забезпечення службово-бойової діяльності сил сектору безпеки і оборони : матеріали всеукр. круг. столу (м. Харків, 23 квіт. 2021 р.) / редкол.: Є. О. Меленті, І. В. Євтушенко, О. А. Гарбузов, В. О. Пономарьов – Х.: ФОП Бровін О. В., 2021. – Вип. 5. – С. 361 – 365. URL: https://repository.hneu.edu.ua/bitstream/123456789/25621/1/%D0%93%D0%B0%D0%B2%D1%80%D0%B8%D0%BB%D0%BE%D0%B2%D0%B0%D0%A5%D0%B0%D1%80_%D0%BA%D0%BE%D0%B2%D0%A1%D0%91%D0%A3.pdf 2. Gavrilova A. Synergy of building cybersecurity systems / S. Yevseiev, V. Ponomarenko, O. Laptiev, O. Milov, O. Korol, S. Milevskyi, S. Pohasii, A. Tkachov, O. Shmatko, Y. Melenti, O. Sievierinov, S. Ostapov, A. Gavrilova, O. Tsyhanenko, S. Herasimov, E. Nyemkova, B. Tomashevsky, I. Hrod, I. Opirskyy, V. Zvieriev, O. Prokopenko, V. Savchenko, O. Barabash, V. Sobchuk, G. Shuklin, V. Khvostenko, O. Tymochko, M. Pavlenko, A. Trystan, S. Florov // monograph. – Kharkiv: PC TECHNOLOGY CENTER, 2021. – 188 p. (P. 102 – 147). – https://doi.org/10.15587/978-617-7319-31-2 3. Havrylova Alla. Research of collision properties of the modified UMAC algorithm on crypto-code constructions / Serhii Yevseiev, Alla Havrylova, Olha Korol, Oleh Dmitriiev, Oleksii Nesmiian, Yevhen Yufa, Asadi Hrebennikov // "EUREKA: Physics and Engineering". – 2022. – Number 1 (38), P. 34 – 43. https://journal.eu-jr.eu/engineering/article/view/2213 (https://doi.org/10.21303/2461-4262.2022.002213) 4. Гаврилова А. А. Перевірка на колізійність геш-кодів які сформовано за допомогою алгоритму

							UMAC на крипто-кодових конструкціях / С. П. Євсеєв, А. А. Гаврилова // "Математика. Інформаційні технології. Освіта"; тези доповідей на XI Міжнародній науково-практичній конференції, Луцьк-Світязь, 3 – 5 червня 2022 р. – Луцьк, 2022. – С. 66 – 68. https://repository.kpi.kharkov.ua/handle/KhPI-Press/89797 5. Havrylova Alla. Estimating the Efficiency of Using the Modified UMAC Algorithm / Alla Havrylova, Andrii Tkachov, Irada Rahim qizi Rahimova // 2022 IEEE 3rd KhPI Week on Advanced Technology (KhPIWeek) 03-07 October 2022 .– 2022. Kharkiv, Ukraine: Publisher: IEEE, P. 1 – 5 URL: https://ieeexplore.ieee.org/document/9916425 (Scopus) 6. Havrylova A. Models of socio-cyber-physical systems security: monograph / Yevseiev S., Khokhlachova Yu., Ostapov S., Laptiev O., Korol O., Milevskyi S., Milov O., Pohasii S., Melenti Y., Hrebeniuk V., Havrylova A., Herasymov S., Korolev R., Barabash O., Sobchuk V., Kyrychok R., Shuklin G., Akhramovych V., Savchenko V., Golovashych S., Lezik O., Opirskyy I., Voitko O., Yerhidzei K., Mykus S., Pribyliev Y., Prokopenko O., Vlasov A., Dzheniuk N., Tolkachov M. – Kharkiv: PC TECHNOLOGY CENTER, 2023. – 168 p. (DOI: 10.15587/978-617-7319-72-5) (SCOPUS) . 7. Гаврилов А. В., Гаврилова А. А. Оцінка рівня захищеності повідом лень електронної пошти на транспортному рівні передачі комунікаційними каналами зв'язку // Актуальні питання забезпечення службово-бойової діяльності сил сектору безпеки і оборони: матеріали III

							Всеукраїнської конференції, м. Харків, 25 квітня 2024 року. – Харків: ФОП Бровін О.В., 2024., С. 219 – 224 https://dspace.nlu.edu.ua/jspui/bitstream/123456789/20100/1/konf_APZSBDSBO-2024.pdf 8. Алла Гаврилова, Ірина Аксьонова. Використання алгоритмів CCC/UMAC для вдосконалення протоколу SSL/TLS. Матерали XIII міжнародної науково-технічної конференції “ITSec: Безпека інформаційних технологій”. м. Львів, 9-11 травня 2024 р. Л.: ЛНУ ім. І. Франка, 2024, 265 с. (С. 69 – 70). https://sci.ldubgd.edu.ua/bitstream/123456789/13509/1/2024-ITSec_%D0%BA%D1%96%D0%B1%D0%B5%D1%80%D0%B1%D0%B5%D0%B7%D0%BF%D0%B5%D0%BA%D0%B0.pdf 9. Havrylova A., Milov O., Rahimova I., Golovashych S., Aksonova I., Pecherytsia D. Cybersecurity of SMART Technologies Using Deep Learning Methods. ISMSIT 2024 – 8th International Symposium on Multidisciplinary Studies and Innovative Technologies, Proceedings, 2024. – Ankara, Turkiye. DOI: 10.1109/ISMSIT63511.2024.10757295. URL: https://ieeexplore.ieee.org/document/10757295. (SCOPUS) 10. Havrylova A., Tkachov A., Hapon A., Balagura D., Sievierinov O., Bukatych I. Analysis of the Software Security Protection. ISMSIT 2024 – 8th International Symposium on Multidisciplinary Studies and Innovative Technologies, Proceedings, 2024. – Ankara, Turkiye. DOI: 10.1109/ISMSIT63511.2024. 10757202 URL: https://ieeexplore.ieee.org/document/10757202. (SCOPUS) 11. Гаврилова А.А., Сосновий В.В. Аналіз загроз інформаційної безпеки за об’єктовим принципом.

							Проблеми та шляхи захисту інформаційно-психологічної і духовної безпеки особи, суспільства, держави: матеріали п'ятої Міжнародної науково- практичної конференції. – м. Київ, 28 червня 2024 р. – К., 2025. – С. 24 – 25. https://dspace.kntu.kr.ua/server/api/core/bitstreams/8683d444-de7e-442e-bcec-83596a5969e6/content 12. Гаврилова А.А., Сіпко Д.С. Аналіз загроз соціальної інженерії на теренах кіберпростору. Проблеми та шляхи захисту інформаційно-психологічної і духовної безпеки особи, суспільства, держави: матеріали п'ятої Міжнародної науково- практичної конференції. – м. Київ, 28 червня 2024 р. – К., 2025. – С. 26 – 27. https://dspace.kntu.kr.ua/server/api/core/bitstreams/8683d444-de7e-442e-bcec-83596a5969e6/content 13. Гаврилова А.А., Коваленко Д.С. Аналіз впливу інформаційної війни на національну безпеку. Проблеми та шляхи захисту інформаційно-психологічної і духовної безпеки особи, суспільства, держави: матеріали п'ятої Міжнародної науково- практичної конференції. – м. Київ, 28 червня 2024 р. – К., 2025. – С. 28 – 29. https://dspace.kntu.kr.ua/server/api/core/bitstreams/8683d444-de7e-442e-bcec-83596a5969e6/content 14. Havrylova A.A., Tkachov A.M., Hapon A.O. Approaches to detecting vulnerabilities in software to ensure code protection. Матеріали V Міжнародної науково-практичної конференції «Інформаційна безпека та інформаційні технології», Харків, Одеса, Луцьк, 9–11 червня 2025 року. P. 59 – 60 URL: https://essuir.sumdu.e

							du.ua/server/api/core/bitstreams/a3082f67-b8fe-4b39-a74d-c3591992efd3/content 15. Гаврилова А. А., Аксьонова І. В. Фреймворк аналізу кіберзагроз як інструмент управління корпоративною безпекою. Актуальні питання забезпечення кібербезпеки та захисту інформації: матеріали XI Міжнародної науково-практичної конференції, 24 квітня 2025 р., Київ / редкол.: О. І. Тимошенко [та ін.]. – Київ: Вид-во Європейського університету, 2025. – С. 10 – 12. https://files.znu.edu.ua/files/Bibliobooks/Inshi84/0063968.pdf 16. Havrylova A., Tolkachov M., Dzheniuk N., Chechui O., Hapon A., Tiutiunyk V. Cognitive Approach to Cybersecurity: Causality Analysis and Situational Learning. 2025 7th International Congress on Human-Computer Interaction, Optimization and Robotic Applications (ICHORA), May 23-24, 2025 Ankara-Türkiye (Hybrid), 2025. Pp. 1 – 4. DOI: 10.1109/ICHORA65333.2025.11017107 (SCOPUS) 17. Havrylova A., Khvostenko V., Milevskyi S. Development of an Advanced SSL/TLS Protocol for Transferring Requests to a 3D-Printer: monograf In: Durakbasa, N. M., Cetinkaya, K., Demircioglu, P., Bogrekci, I. (eds) Digitalization in Additive Manufacturing. ICPTDI 2025. Springer Tracts in Additive Manufacturing. Springer, Cham. Part F641, P. 489–503. https://link.springer.com/chapter/10.1007/978-3-031-84873-5_38 П 13. проведення навчальних занять із спеціальних дисциплін іноземною мовою (крім дисциплін мовної підготовки) в обсязі не менше 50 аудиторних

							годин на навчальний рік 1. Introduction to the specialty. Introductory practice (3 кр.):Всього 32 год.: лекцій – 16 год., практик – 16 год. (КН-1125ia.e) 2. Decentralized systems (4 кр.) Всього 50 год.: лекцій – 32 год., практик – 16 год., консультації – 2 год. (КН-1122ia.e) П. 19 діяльність за спеціальністю у формі участі у професійних та/або громадських об'єднаннях член Громадської організації "СХІДНО-ЄВРОПЕЙСЬКЕ НАУКОВЕ ТОВАРИСТВО" з 20.05.2022р. посвідчення № ES 055
482108	Аксьонова Ірина Вікторівна	Доцент, Основне місце роботи	Навчально-науковий інститут комп'ютерних наук та інформаційних технологій	Диплом спеціаліста, Харківський державний економічний університет, рік закінчення: 1995, спеціальність: облік і аудіт, Диплом магістра, Національний технічний університет "Харківський політехнічний інститут", рік закінчення: 2024, спеціальність: 125 Кібербезпека та захист інформації, Диплом кандидата наук ДК 003956, виданий 02.07.1999, Атестат доцента ДЦ 006378, виданий 23.12.2002	27	Технології управління безпекою бізнес - процесів	Підвищення кваліфікації 1) UNIVERSITY OF THE NATIONAL EDUCATION COMMISSION (KRAKOW, POLAND). TOPIC: METHODS AND TECHNICAL MEANS OF INFORMATION PROTECTION. Сертифікат № KIO/23 - 04 - 10 / 2025 (180 ГОДИН (6 КРЕДИТІВ ECTS, з 20.02.2025 р. по 20.04.2025 р., затверджено наказом №2186С від 21.11.2025р.) Пункти відповідності ліцензійних умов: П. 1, 2, 3, 4, 12, 14, 19 П. 1 наявність не менше п'яти публікацій у періодичних наукових виданнях, що включені до переліку фахових видань України, до наукометричних баз, зокрема Scopus, Web of Science Core Collection 1. Bukatych I., Aksonova I., Milevska T., Smirnov A., Balagura D., Zhyhalov M. Development of an Advanced Blockchains' Classification // 7th International Congress on Human-Computer Interaction, Optimization and Robotic Applications May 23-24, 2025, Istanbul, Turkey. URL: DOI:10.1109/ICHORA65333.2025.11017298 (Scopus) 2. Milevskyi S., Yevseiev

							S., Aksonova I., Dunaiev S. Development of a Method for Evaluating Data Transmission in Cyber-Physical Systems // Springer Tracts in Additive Manufacturing, 2025. Pp. 475-488. https://doi.org/10.1007/978-3-031-84873-5 (Scopus) 3. Aksonova I. and Milevska T. Information Security and Competitive Intelligence: Development Prospects in the Digital Economy // Springer Tracts in Additive Manufacturing, 2025. Pp. 611-622. https://doi.org/10.1007/978-3-031-84873-5 (Scopus) 4. Tkachov A., Korolov R., Rahimova I., Aksonova I., Sevriukova Y. Cybersecurity challenges and solutions for critical infrastructure protection // Ukrainian Scientific Journal of Information Security, 2024, vol. 30, issue 1, pp. 58-66. URL:https://jrnl.nau.edu.ua/index.php/Infosecurity/article/view/18604 (фахове, категорія Б) 5. Herasymov S., Soroka V., Milevskyi S., Aksonova I., Korol O., Stetsenko V. Method for Reducing the Frequency Spectrum Overlaying Error in Digital Narrow-Band Filtration // 6th International Congress on Human-Computer Interaction, Optimization and Robotic Applications (HORA), May 23-25, 2024, Istanbul, Turkey. URL:https://ieeexplore.ieee.org/abstract/document/10550889; DOI: 10.1109/HORA61326.2024.10550889 (Scopus) 6. Milov O., Rahimova I., Havrylova A., Golovashych S., Aksonova I., Pecherytsia D. Cybersecurity of SMART Technologies Using Deep Learning Methods // 8 th International Symposium on Multidisciplinary Studies and Innovative Technologies (ISMSIT), November 7-10, 2024, pp. 1-6. Ankara, Turkey.

							URL:https://ieeexplore.ieee.org/abstract/document/10757295; DOI: 10.1109/ISMSIT63511.2024.10757295 (Scopus) 7. Havrylova A., Aksonova I., Khokhlachova Yu., Milevska T., Dunaiev S. Rationale for improving authentication protocols in the conditions of postquantum cryptography // Ukrainian Scientific Journal of Information Security, 2024, vol. 30, issue 1, pp. 130-139. URL:https://jrnl.nau.edu.ua/index.php/Infosecurity/article/view/18614 (фахове, категорія Б) 8. Milevskyi S., Voropay N., Korol O., Yevseiev S., Aksonova I. SSL/TLS protocol on post-quantum algorithms // Ukrainian Scientific Journal of Information Security, 2024, vol. 30, issue 1, pp. 150-156. URL:https://jrnl.nau.edu.ua/index.php/Infosecurity/article/view/18616 (фахове, категорія Б) 9. Аксьонова І. В. Статистичний аналіз тенденцій в промислових міжрегіональних диспропорціях // Економіка та суспільство. 2024. № 62. URL:https://economyandsociety.in.ua/index.php/journal/article/view/4002 (фахове, категорія Б) 10. Sierova I., Aksonova I., Shlykova V., Milevska T. Computer-mathematical support for analytical assessment of trends in the Ukrainian grain market development // 5th International Congress on Human-Computer Interaction, Optimization and Robotic Applications June 8-10, 2023, Istanbul, Turkey. URL:https://ieeexplore.ieee.org/document/10155771; DOI: 10.1109/HORA58378.2023.10155771 (Scopus) 11. Аксьонова І.В. Моніторинг як сучасне інформаційне забезпечення аналітики та управління підприємствами // Економіка та суспільство. 2023. № 55. URL:

							https://economyandsociety.in.ua/index.php/journal/article/view/2880 DOI: 10.32782/2524-0072/2023-55-70. (фахове, категорія Б) 12. Rayevnyeva O., Filip S., Brovko O., Aksonova I., Rui S. The impact of sensitivity of economic activities on the economic behaviour of enterprise // Economics of Development. 2022. Vol. 21, No. 3. PP. 27-39. URL: https://doi.org/10.57111/econ.21(3).2022.27-39 (Scopus) 13. Rayevnyeva O., Karpinski M., Brovko O.,Aksonova I., Falat H. The Diagnostic Model for Assessing the State of Stability of an Industrial Enterprise / Wrycza S., Maślankowski J. (eds) Digital Transformation. PLAIS EuroSymposium 2021. Lecture Notes in Business Information Processing, vol 429. Springer, Cham. URL: https://doi.org/10.1007/978-3-030-85893-3_4 (Scopus)
							П. 2 наявність одного патенту на винахід або п’яти деклараційних патентів на винахід чи корисну модель, включаючи секретні, або наявність не менше п’яти свідоцтв про реєстрацію авторського права на твір 1. Свідоцтво про реєстрацію авторського права на твір №123936 від 19.02.2024. Структурно-динамічний аналіз ринку праці України: виклики сьогодення / І.В. Аксьонова (Бюлетень “Авторське право і суміжні права”, №80, 2024 р., стор.536), https://ukrpatent.org/uk/articles/bulletin-copyright 2. Свідоцтво про реєстрацію авторського права на твір № 120457 від 11.07.2023. Статистичне оцінювання вимог ринку праці України: сучасний стан та тенденції майбутнього / І.В. Аксьонова (Бюлетень “Авторське право і суміжні

							права”, №77, 2023 р., стор.94), https://ukrpatent.org/uk/articles/bulletin-copyright 3. Свідоцтво про реєстрацію авторського права на твір № 111477 від 31.01.2022. The Diagnostic Model for Assessing the State of Stability of an Industrial Enterprise / О.В. Раєвнєва, М. Карпінський, О.І. Бровко, П. Фалат, І.В. Аксьонова (Бюлетень “Авторське право і суміжні права”, №69, 2022 р., стор.319), https://ukrpatent.org/uk/articles/bulletin-copyright 4. Свідоцтво про реєстрацію авторського права на твір № 110940 від 12.01.2022. Digitalization as a development factor of innovative-active university / В. С. Пономаренко, О. В. Раєвнєва, В. Є. Єрмаченко, І. В. Аксьонова, О. І.Бровко (Бюлетень “Авторське право і суміжні права”, №69, 2022 р., стор.93), https://ukrpatent.org/uk/articles/bulletin-copyright 5. Свідоцтво про реєстрацію авторського права на твір № 101964 від 22.01.2021. Система вищої освіти України в Європейському освітньому просторі: місце та перспективи розвитку/ Раєвнєва О. В., Аксьонова І. В. (Бюлетень “Авторське право і суміжні права”, №63, 2021 р., стор.169), https://ukrpatent.org/uk/articles/bulletin-copyright П. 3 наявність виданого підручника чи навчального посібника (включаючи електронні) або монографії (загальним обсягом не менше 5 авторських аркушів), в тому числі видані у співавторстві (обсягом не менше 1,5 авторського аркуша на кожного співавтора) (*за наявності надати

							лінк або бібліографічний опис) 1. Інформаційні системи електронної комерції: навчальний посібник / С.Е. Остапов, С.П. Євсеєв, К.П. Газдюк, О.Ю. Тарновецька, Л.М. Шумиляк, І.В. Аксьонова, А.А. Гаврилова. Чернівецький національний університет ім. Ю. Федьковича, Національний технічний університет "Харківський Політехнічний Інститут", – Львів: Видавництво «Новий Світ-2000», 2024. 282 с. (13,8 ум.-друк. арк. / власний внесок 1,97 ум.-друк. арк.) 2. Кібербезпека та новітні технології захисту інформації: навчальний посібник / Ковтун В. Ю., Євсеєв С. П., Аксьонова І. В. Харків, – Львів: «Новий Світ-2000», 2024. 285 с. (17,8 ум.-друк. арк. / власний внесок 5,9 ум.-друк. арк.) 3. Ponomarenko V. Rayevnyeva O., Yermachenko V., Yevseiev S., Poliakova H., Milov O., Labunska S., Aksonova I., Brovko O., Shmatko O. Conceptual and model support for the development of an innovative-active university: monograph / edited by Prof., D.Sc. (Economics) Ponomarenko V., Prof., D.Sc. (Economics), Rayevnyeva O., Prof., Assoc. prof. (Economics) Yermachenko V. - Primedia eLaunch, Boston, USA. 2021. - 377 p. (23,6 ум.-друк. арк. / власний внесок 2,3 ум.-друк. арк.) https://isg-konf.com/wp-content/uploads/2021/12/Conceptual-and-model-support-for-the-development-of-an-innovative-active-university.pdf П. 4 наявність виданих навчально-методичних посібників/посібників для самостійної роботи здобувачів вищої освіти та дистанційного навчання,

							електронних курсів на освітніх платформах ліцензіатів, конспектів лекцій/практикумів/методичних вказівок/рекомендацій/ робочих програм, інших друкованих навчально-методичних праць загальною кількістю три найменування 1. Методичні вказівки до виконання лабораторних робіт з дисципліни «Управління ІТ-проєктами та їх безпека» [Електронний ресурс] : для студентів першого (бакалаврського) рівня вищої освіти за спец. 125 «Кібербезпека та захист інформації» / уклад. Гаврилова А.А., Аксьонова І.В. - Харків: НТУ «ХПІ», 2024.- 55 с. https://repository.kpi.kharkov.ua/items/3464aff9-0b88-471b-844b-5cb3b64f0534 2. Методичні рекомендації до написання дипломної роботи для здобувачів вищої освіти спеціальності 051 «Економіка» освітньої програми «Бізнес-статистика і аналітика» другого (магістерського) рівня / уклад. О. В. Раєвнєва, І. В. Аксьонова, М. І. Койнаш, Т. С. Мілевська. – Харків : ХНЕУ ім. С. Кузнеця, 2024. — 41 с. http://repository.hneu.edu.ua/handle/123456789/31935 3. Аналіз даних та багатовимірна статистика: робоча програма навчальної дисципліни для здобувачів вищої освіти третього (освітньо-наукового) рівня / уклад. Аксьонова І.В. - Харків : ХНЕУ ім. С. Кузнеця, 2024. – 9 с. http://repository.hneu.edu.ua/handle/123456789/32313 4.Web Analytics for Business. Guidelines to laboratory work for Bachelor's (first) degree students of all

							specialities / compiled by I. Sierova, I. Aksonova, V. Shlykova, K. Stryzhychenko. - Kharkiv : S. Kuznets KhNUE, 2023. – 47 p. http://repository.hneu.edu.ua/handle/123456789/33374 П. 12 наявність апробаційних та/або науково-популярних, та/або консультаційних (дорадчих), та/або науково-експертних публікацій з наукової або професійної тематики загальною кількістю не менше п’яти публікацій 1. Дунаєв С., Букатич І., Мілевський С., Аксьонова І. Аналіз адаптивного кодування LT, Raptor і LDPC у мережах нового покоління // SMICS: Безпека сучасних інформаційно-комунікаційних систем: матеріали Міжнар. наук.-техн. конф., м. Львів, 16-18 жовтня 2025 р.: ЛНУ ім. І. Франка, 2025, 468 с. (с. 179-183). URL: https://smics.lnu.edu.ua/uk/zbirnyk/ 2. Аксьонова І., Мілевська Т. Mitre Att&ck: сучасний інструмент виявлення та запобігання кібератакам // Проблеми кібербезпеки інформаційно-комунікаційних систем: Збірник матеріалів доповідей та тез; м. Київ, 11 квітня 2025 року; Київський національний університет імені Тараса Шевченка / Редкол.: В.В. Ільченко, д.ф-м.н., проф., (голова); та ін. – К.: ВПЦ "Київський університет", 2025. – 182 с. (с.155-156). URL: https://drive.google.com/file/d/1R1ywVEyM1XpghS4_6EA_b414LsMbjzHY/view 3. Аксьонова І.В., Гаврилова А. А. Фреймворк аналізу кіберзагроз як інструмент управління корпоративною безпекою // Актуальні питання забезпечення

							кібербезпеки та захисту інформації: матеріали XI Міжнародної науково-практичної конференції, 24 квітня 2025 р., Київ / редкол.: О. І. Тимошенко [та ін.]. – Київ: Вид-во Європейського університету, 2025. – 163 с. (с. 10-12). URL:https://e-u.edu.ua/userfiles/files/135/zbirnik_aktualni_pitannya_zabezpechennya_kiberbezpeki_ta_zahistu_informacii-_24_04_25.pdf 4. Аксьонова І. В. Кластерний аналіз для управління міжрегіональними промисловими диспропорціями / Матеріали V Міжнародної науково-практичної конференції «Бізнес-аналітика: моделі, інструменти та технології». 5-6 бер. 2024. К.: НАУ, 2024. 630 с. URL: https://ir.lib.vntu.edu.ua/bitstream/handle/123456789/41394/148281.pdf?sequence=2&isAllowed=y 5. Аксьонова І. В., Ричкова Л.В. Статистичний моніторинг для розробки ключових показників ефективності підприємств та організацій // Актуальні аспекти сучасної статистичної науки і практики: матеріали Міжнародної науково-практичної конференції пам'яті проф. А.З. Підгорного (Одеса, 31 травня 2023 р.). – Одеса: Одеській національний економічний університет, 2023, с. 88. (С.20-22). URL: https://drive.google.com/file/d/1RoFKnuJAU-sBtEn2XQnMxc71PiGR3Hsq/view 6. Aksonova I. , Milevska T. , Yevseiev S. WEB ANALYTICS: BASIC PRINCIPLES OF USE IN BUSINESS DIGITIZATION CONDITIONS // Матеріали VII Міжнародної науково-

							практичної конференції “Інформаційна безпека та комп’ютерні технології” до 30-ти річчя кафедри кібербезпеки та програмного забезпечення: тези доповідей, 1 листопада 2023 р. – Кропивницький: ЦНТУ, 2023. – 135 с. (с. 49-50), URL: https://kntu.kr.ua/file/content/8108/tezy-dopovidei-vii-vseukrainskoi-naukovo-praktychnoi-internet-konferentsii-informatsiina-bezpeka-ta-komp-yuterni-tekhnolohii-1-lystopada-2023-roku-.pdf ІІ. 14 керівництво студентом, який зайняв призове місце на І або ІІ етапі Всеукраїнської студентської олімпіади (Всеукраїнського конкурсу студентських наукових робіт), або робота у складі організаційного комітету / журі Всеукраїнської студентської олімпіади (Всеукраїнського конкурсу студентських наукових робіт), або керівництво постійно діючим студентським науковим гуртком / проблемною групою; керівництво студентом, який став призером або лауреатом Міжнародних, Всеукраїнських мистецьких конкурсів, фестивалів та проектів, робота у складі організаційного комітету або у складі журі міжнародних, всеукраїнських мистецьких конкурсів, інших культурно-мистецьких проектів (для забезпечення провадження освітньої діяльності на третьому (освітньо-творчому) рівні); керівництво здобувачем, який став призером або лауреатом міжнародних мистецьких конкурсів, фестивалів, віднесених до Європейської або

							Всесвітньої (Світової) асоціації мистецьких конкурсів, фестивалів, робота у складі організаційного комітету або у складі журі зазначених мистецьких конкурсів, фестивалів); керівництво студентом, який брав участь в Олімпійських, Параолімпійських іграх, Всесвітній та Всеукраїнській Універсіаді, чемпіонаті світу, Європи, Європейських іграх, етапах Кубка світу та Європи, чемпіонаті України; виконання обов'язків тренера, помічника тренера національної збірної команди України з видів спорту; виконання обов'язків головного секретаря, головного судді, судді міжнародних та всеукраїнських змагань; керівництво спортивною делегацією; робота у складі організаційного комітету, суддівського корпусу (*надати лінки чи документи, що підтверджують наявність цього досягнення) Керівництво студентом-переможцем І етапу Всеукраїнського конкурсу студентських наукових робіт за напрямом «Економічна аналітика та статистика» у 2021-2022 н.р. – Бочарнікова Д. Р., протокол засідання кафедри статистики і економічного прогнозування ХНЕУ ім. С. Кузнеця, № 6 від 12.01.2022 р. П. 19 діяльність за спеціальністю у формі участі у професійних та/або громадських об'єднаннях (*надати лінки чи документи, що підтверджують наявність цього досягнення) Асоційований член громадської організації «Соціально-економічні ініціативи і проєкти» (СЕІП), свідоцтво № 050-12 від 25.06.2021 р. (з 2021 р. по теперішній час) https://youcontrol.com.

							ua/ru/catalog/company_details/44289364/

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

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