НАЦІОНАЛЬНЕ АГЕНТСТВО ІЗ ЗАБЕЗПЕЧЕННЯ ЯКОСТІ ВИЩОЇ ОСВІТИ

ВІДОМОСТІ
про самооцінювання освітньої програми

Заклад вищої освіти	**Національний технічний університет "Харківський політехнічний інститут"**
Освітня програма	**54114 Кібербезпека**
Рівень вищої освіти	**Магістр**
Спеціальність	**125 Кібербезпека**

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

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

Використані скорочення:

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

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	**54114**
Назва ОП	**Кібербезпека**
Галузь знань	**12 Інформаційні технології**
Спеціальність	**125 Кібербезпека**
Спеціалізація (за наявності)	*відсутня*
Рівень вищої освіти	**Магістр**
Тип освітньої програми	**Освітньо-професійна**
Вступ на освітню програму здійснюється на основі ступеня (рівня)	**Бакалавр**
Структурний підрозділ (кафедра або інший підрозділ), відповідальний за реалізацію ОП	**кафедра кібербезпеки**
Інші навчальні структурні підрозділи (кафедра або інші підрозділи), залучені до реалізації ОП	**-**
Місце (адреса) провадження освітньої діяльності за ОП	**60002 м. Харків вул. Кирпичова 2**
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	**410239**
ПІБ гаранта ОП	**Мілов Олександр Володимирович**
Посада гаранта ОП	**Професор**
Корпоративна електронна адреса гаранта ОП	**Oleksandr.Milov@khpi.edu.ua**
Контактний телефон гаранта ОП	**+38(066)-431-35-36**
Додатковий телефон гаранта ОП	**+38(066)-431-35-36**

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

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

Загальні відомості про ОП, історію її розроблення та впровадження (довге поле)
Виходячи з освітніх потреб Харківського регіону, наявності відповідних ресурсів університет здатний гарантувати якісну підготовку висококваліфікованих фахівців за спеціальністю 125 "Кібербезпека", що забезпечить ефективну роботу з удосконалення освіти у галузі безпеки інформаційних ресурсів, та дозволить задовольнити попит у кваліфікованих кадрах у бізнес-середовищі.
Освітньо-професійна програма "Кібербезпека" (далі – ОПП "Кібербезпека") була розроблена в 2022 році (затверджено Вченою радою від 04.02.2022 року, протокол № 2) та розроблена відповідно до Стандарту вищої освіти за спеціальністю 125 "Кібербезпека" (https://cybersecurity.kpi.kharkov.ua/)
До розробки програми були залучені викладачі за фахом, з яких була утворена група забезпечення, фахівці навчального відділу, керівний склад університету, представники роботодавців, органи студентського самоврядування. На основі Договору з університетом у Бєльсько-Бялій (м. Бельсько-Бяла, Польща) освітня програма підготовки студентів другого (магістерського) рівня забезпечує можливість отримання спільного (двох дипломів) для підготовки магістрів за спеціальністю "Кібербезпека".
Кафедра кібербезпеки в НТУ "ХПІ" організована з 1.01.2022 року, але кафедра приймаэ активну участь у гранті з United States Agency for International Development "Cybersecurity of Critical Infrastructure of Ukraine", організує 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/), приймає активну участь у підготовкці та проведенні міжнародної науково-практичної конференції IEEE "International Congress on Human-Computer Interaction, Optimization and Robotic Applications"(https://www.horacongress.com/index.php?go=supporters) (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), міжнародної науково-практичної конференції "Modern information, measurement and control systems: problems, applications and perspectives 2022 (MIMCS'2022)" (http://mimcs.net/) (Азербайджан). На кафедрі постійно займаються дослідними роботами, що підтверджується отриманими патентами на корисну модель викладачами кафедри (https://cybersecurity.kpi.kharkov.ua/patenty-kafedry-kiberbezpeka/). У підготовці проекту змін ОПП "Кібербезпека" у 2023 р. брали участь: завідувач кафедри кібербезпеки Євсеєв Сергій Петрович, професор кафедри Мілов Олександр Володимирович, доцент кафедри Король Ольга Григорівна, а також представники академічної спільноти та роботодавці: комерційний директор ТОВ "Сайфер", к.т.н. Ковтун Владислав Юрійович; співзасновник компанії "Distributed Lab", к.т.н. Кравченко Павло Олександрович; директор ТОВ "Мікрокрипт Технолоджіс", к.т.н., доцент Головашич Сергій Олександрович; керівник навчально-наукового центру інформаційних технологій Поліського національного університету, д.т.н., професор Молодецька Катерина Валеріївна.

5. Інформація про контингент здобувачів вищої освіти на ОП станом на 1 жовтня поточного навчального року у розрізі форм здобуття освіти та набір на ОП (кількість здобувачів, зарахованих на навчання у відповідному навчальному році сумарно за усіма формами здобуття освіти)

Рік навчання	Навчальний рік, у якому відбувся набір здобувачів відповідного року навчання	Обсяг набору на ОП у відповідному навчальному році	Контингент студентів на відповідному році навчання станом на 1 жовтня поточного навчального року	У тому числі іноземців
			ОД	*ОД*
1 курс	2023 - 2024	19	19	0
2 курс	2022 - 2023	54	54	0

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

6. Інформація про інші ОП ЗВО за відповідною спеціальністю

Рівень вищої освіти	Інформація про освітні програми
початковий рівень (короткий цикл)	*програми відсутні*
перший (бакалаврський) рівень	**25278 Кібербезпека**
другий (магістерський) рівень	**54114 Кібербезпека** **30579 Кібербезпека**
третій (освітньо-науковий/освітньо-творчий) рівень	**56363 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	*08_2023_НП_Магистры_125_дневное2023_2024_СО_СКАНАМИ.pdf*	ewVfi0ze3PF4Bu74nhZBhnrSfZZB2GkeHsoGEjQpwNk=
Навчальний план за ОП	*август_2023_ОПП_Магістр_125_Кібербезпека_та_захист_інформації_БЕЗ.pdf*	Y6Wp3kC4adycQmwZ1c5Hemf2UvoiZ95rRTmP6Fpz7yM=
Рецензії та відгуки роботодавців	*Рецензія_відгук_магістри_Головашич.pdf*	JCIkqYA5aOqop+qewHC1yMSUSQKAJ2i6oGUsusrvvMo=
Рецензії та відгуки роботодавців	*Рецензія_відгук_магістри_Волощук.pdf*	jBuFbl65krhNbk4FRUWMLfpTS/PBCEyWxKBXsrz2xQY=
Рецензії та відгуки роботодавців	*Рецензія_відгук_магістри_Ковтун.pdf*	nAzp214BU04g0U9LQpJ+L5uASgChcdAp4G5+H/obQsI=
Рецензії та відгуки роботодавців	*Рецензія-відгук_магістри_Молодецька.pdf*	uCB+Y5c9dBa0uyTJcG7Ue2Ze88jxkQJZrHctcVMihJw=

1. Проектування та цілі освітньої програми

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

Цілі ОП – Підготовка фахівців, здатних розв'язувати задачі дослідницького та/або інноваційного характеру у сфері інформаційної та/або кібербезпеки, використовувати і впроваджувати технології та застосовувати засоби захисту в системах безпеки контуру бізнес-процесів.
Особливостями програми є формування у здобувачів навичок побудови комплексних систем захисту інформації для забезпечення безпеки контуру бізнес-процесів на основі сучасних технологій та програмних застосунків, в умовах розвитку цифрової економіки.
Орієнтація на партнерство із вітчизняними та закордонними закладами освіти та науки, приватним сектором, науковцями та практиками, участь в міжнародних програмах спільних дипломів.
За допомогою ТОВ "Сайфер БІС" розгортається ЦСК, який дозволяє використовувати власні розробки компанії у формуванні електронного документообігу університету. Під час навчання здобувачі можуть отримати сертифікати академії CISCO (https://cybersecurity.kpi.kharkov.ua). Це дозволяє здобувачу вищої освіти в рамках неформальної освіти отримувати додаткові знання за відповідними освітніми компонентами та сертифікати академії CISCO, що підвищує конкурентоспроможність випускників на ринку праці.

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

Освітньо-професійна програма створена у відповідності до місії та стратегії 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 ОП 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.

Опишіть, яким чином інтереси та пропозиції таких груп заінтересованих сторін (стейкхолдерів) були враховані під час формулювання цілей та програмних результатів навчання ОП:
- здобувачі вищої освіти та випускники програми

Студент 1 року навчання (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. 9 (https://cybersecurity.kpi.kharkov.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 (зв допомогою ЦСК), та провести тренінги із здобувачами.

- академічна спільнота

ОПП "Кібербезпека" отримала позитивну рецензію-відгук від Катерини Молодецької, д.т.н., професора, керівника навчально-наукового центру інформаційних технологій Поліського національного університету.
Завідувач кафедри комп'ютерних наук та автоматики університету Більсько-Бяла (Польща) проф., д.т.н. Карпінський М.П., які погодились включити в навчальний план дисципліни: "Інформаційна безпека телекомунікаційних та хмарних технологій", "Тестування на проникнення та етичний хакінг", "Безпека бездротових та мобільних мереж", "Безпека Web-ресурсів", "Цифрова криміналістика", "Безпека Інтернет-речей".

- інші стейкхолдери

Випускником магістерської програми за спеціальністю 122 "Комп'ютерні науки" Циганенко Олексієм, який працює в компанії Jabil Circuit Inc., виходячи з задач, що виникають під час трудової діяльності, та його професійного досвіду, було запропоновано розширити програму 125-ї спеціальності, додавши до неї вивчення основ та засобів безпеки інформаційно-комунікаційних систем. Після обговорення, в вибіркову складову введена навчальна дисципліна "Інженерія безпеки інформаційно-комунікаційних систем".

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

Ринок праці ІТ-галузі України розвивається доволі стрімко, при цьому все більшу популярність набувають вакансії за категорією програміст-аналітик. Понад 47 % замовлень в ІТ-компаніях пов'язані з розробленням програмних застосунків, які забезпечують інформаційну безпеку та захист інформації. За результатами 2020-2021 рр. індустрія працівників ІТ зросла на 20% (https://bit.ly/2Gcq9ux), серед мов програмування найбільш затребуваними 2020–2021 рр. були Python, Java і PHP. ОП дає можливість набуття компетентностей з використання зазначених мов програмування, що дозволить здобувачам вищої освіти на основі компетентностей з програмування та забезпечення безпеки підвищити свою конкурентоспроможність на ринку праці. Робоча група регулярно проводить аналіз рекомендацій стейкхолдерів (всіх груп) під час оновлення програми на наступний рік. А саме в рамках освітніх компонентів, які пов'язані з програмуванням, особлива увага приділяється формуванню практичних навичок з розробки програмних застосунків з забезпеченням безпеки в умовах сучасних загроз.

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

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 ІТ-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.
Згідно з результатами дослідження, галузь регіону налічує майже 480 сервісних та продуктових компаній, а кількість фахівців подолала позначку у 31 000 осіб. Загалом, порівнюючи з минулим роком, у кількісному вимірі індустрія в Харкові зросла на 24%. Сумарний об'єм індустрії досяг 962 млн. USD у 2020 році, забезпечивши зростання на рівні 20%. Попит на експертів у галузі інформаційних технологій перевищує пропозицію – потреба компаній у спеціалістах у півтора рази перевищує кількість випускників (харківські університети щороку випускають понад 2 000 молодих спеціалістів тільки за профільними спеціальностями). Зростання вимог до забезпечення безпеки програмних застосунків складає понад 47% від загальної кількості замовлень ІТ-індустрії, тому підготовка спеціалістів з кібербезпеки та програмування є актуальною.

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

Під час формування ОПП "Кібербезпека" проаналізовані освітні програми з підготовки здобувачів другого

(магістерського) рівня вищої освіти за спеціальністю 125 “Кібербезпека” 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/), освітні програми з підготовки здобувачів зі спеціальності “Кібербезпека” у закладах США (https://www.cyberdegrees.org/listings/bachelors-degrees/), а також освітні компоненти погоджені в рамках Польсько-української програми обміну та двох дипломів для підготовки магістрів за спеціальністю “Кібербезпека” з Університетом у Бєльсько-Бялій (м. Бельсько-Бяла, Польща), до якої приєднались кафедра Безпеки інформаційних технологій (Національний авіаційний університет), кафедра кібербезпеки та математичного моделювання (Чернігівський національний технологічний університет), а також університеті Казахстану та Йорданії.
На основі аналізу були визначені основні фахові компетенції та результати навчання, дисципліни, форми та методи навчання, які також враховують пропозиції стейкхолдерів.

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

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:
Технології управління безпекою бізнес-процесів
Розширена мережева та хмарна безпека
Веб-безпека
Цифрова криміналістика
Тестування на проникнення та етичний хакінг
Захист інтелектуальної власності
Інноваційне підприємництво та управління стартап проєктами
Англійська мова
Презентація та обробка знань
Господарське право

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.

2. Структура та зміст освітньої програми

Яким є обсяг ОП (у кредитах ЄКТС)?

90

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

65

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

25

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

Обов’язкові ОК, які включені до ОП 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 ОПП “Кібербезпека”. Зміст ОП “Кібербезпека” забезпечує поглиблене вивчення проведення, як зовнішнього, так й 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 мировими методиками.
Дисципліни навчального плану ОП потребують спеціалізованого програмного та апаратного забезпечення, яке використовується у кіберполігоні. Дисципліни ОП в повній мірі забезпечені ліцензованим та open source програмним забезпеченням, що дозволяє досягти поставленої мети та завдань. Таким чином, ОПП “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 навчальних дисциплін 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 дисциплін в НТУ “ХПІ” здійснюється згідно Положення про порядок реалізації студентами права на вільний вибір навчальних дисциплін (http://blogs.kpi.kharkov.ua/v2/nv/dokumenti-ntu-hpi-2/). В рамках формування індивідуальної складової студентам пропонуються вибіркові дисципліни (https://cybersecurity.kpi.kharkov.ua/vybirkova-skladova-osvitnikh-program-125-magistr/), а також в рамках неформальної освіти студентам пропонуються курси Cisco, які дозволяють додатково в рамках ОПП формувати індивідуальну освітню траєкторію з особливою підготовкою.

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

Вибір студентом навчальних дисциплін 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 компентностями. На сайті кафедри (https://cybersecurity.kpi.kharkov.ua/vybirkova-skladova-osvitnikh-program-125-magistr/) міститься перелік дисциплін вільного вибору.
Кафедра ознайомлює студентів з переліком вибіркових дисциплін та інформує про особливості формування груп для вивчення вибіркових дисциплін на наступний навчальний рік згідно з Положенням про порядок реалізації студентами права на вільний вибір навчальних дисциплін.
(http://blogs.kpi.kharkov.ua/v2/nv/dokumenti-ntu-hpi-2/) Вибір дисциплін студентами здійснюється шляхом подачі письмової заяви на ім’я директора інституту. Заява зберігається в директораті протягом усього терміну навчання студента. На підставі поданих заяв директоратом формується індивідуальний навчальний план для кожного студента та розподіляє академічні групи за обраними дисциплінами та подає до навчальної частини. 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: Технології управління безпекою бізнес-процесів, Розширена мережева та хмарна безпека, Веб-безпека, Цифрова криміналістика, Тестування на проникнення та етичний хакінг, Захист інтелектуальної власності, Інноваційне підприємництво та управління стартап проектами, Англійська мова, Презентація та обробка знань, Господарське право. Відповідно до навчального плану ОП передбачає практику (3сем., 15 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, які відповідають цілям та результатам навчання ОП результатам навчання ОП

ОП передбачає набуття здобувачами вищої освіти soft skills. ОК ОП 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. ОП 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: Господарське право, Презентація та обробка знань, Інноваційне підприємництво та управління стартап проектами, Англійська мова, Захист інтелектуальної власності 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.

Яким чином зміст ОП ураховує вимоги відповідного професійного стандарту?

Професійний стандарт за спеціальністю відсутній.
Фахівці з кібербезпеки можуть працювати, згідно з чинною редакцією Національного класифікатора України: Класифікатор професій (Зміна № 10 до ДК 003:2010):
2139.2 Аналітик загроз безпеки;
2139.2 Аналітик систем захисту інформації та оцінки вразливостей;
2139.2 Аналітик з безпеки інформаційно-телекомунікаційних систем;
2139.2 Дізнавач (сфера кібербезпеки та захисту інформації);
2139.2 Експерт-криміналіст (сфера кібербезпеки та захисту інформації);
2139.2 Експерт-криміналіст судової експертизи (сфера кібербезпеки та захисту інформації);
2139.2 Слідчий з кіберзлочінів.

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 ОП 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 (http://blogs.kpi.kharkov.ua/v2/nv/zaviduvacham-kafedr). Розподіл навчальних годин на аудиторну роботу за навчальними тижнями та видами
навчальної роботи бакалавра відображено в силабусах та РПНД.
Навчальний час, відведений для самостійної роботи студента, визначається гарантом освітньої програми.
Співвідношення обсягу окремих освітніх компонент ОП з фактичним навантаженням здобувачів вищої освіти у навчальному плані складає:
1. Загальна підготовка – 16 кредити, 17,8 %.
2. Спеціальна (фахова) підготовка – 49 кредитів, 59,4 %.
3. Вибіркові освітні компоненти – 25 кредитів, 27,8 % .

Якщо за ОП здійснюється підготовка здобувачів вищої освіти за дуальною формою освіти, продемонструйте, яким чином структура освітньої програми та навчальний план зумовлюються завданнями та особливостями цієї форми здобуття освіти

Підготовки здобувачів за дуальною формою навчання немає.

3. Доступ до освітньої програми та визнання результатів навчання

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

Веб-сайт НТУ ХПІ
http://vstup.kpi.kharkov.ua/edprogram-cat/125-kiberbezpeka/
Веб-сайт інституту
http://web.kpi.kharkov.ua/if/uk/specialties_ua/
Веб-сайт кафедри
https://cybersecurity.kpi.kharkov.ua/osvitno-profesijna-programa-125-magistr/

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
1. http://vstup.kpi.kharkov.ua/edprogram/kiberbezpeka-magistr/, 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, отриманих в інших ЗВО? Яким чином забезпечується його доступність для учасників освітнього процесу?

Результати навчання, отриманих в інших ЗВО, визнаються та зараховуються відповідно до таких документів: Положення про організацію освітнього процесу в НТУ «ХПІ», підрозділи 1.4, 10.2, тощо (Затверджено Вченою радою НТУ «ХПІ», Протокол № 1 від 27 січня 2017 р. http://blogs.kpi.kharkov.ua/v2/nv/dokumenti-ntu-hpi-2/).

Положення про академічну мобільність студентів, аспірантів, докторантів, науково-педагогічних та наукових працівників університету (зі змінами та доповненнями) (Затверджено Вченою радою НТУ «ХПІ», Протокол № 2 від 23.02.2018 р., http://blogs.kpi.kharkov.ua/v2/nv/dokumenti-ntu-hpi-2/)
Положення про порядок реалізації студентами права на вільний вибір навчальних дисциплін у НТУ «ХПІ» (Затверджено Вченою радою НТУ «ХПІ», Протокол № 2 від «23» лютого 2018 р., http://blogs.kpi.kharkov.ua/v2/nv/dokumenti-ntu-hpi-2/)

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

Здобувачі вищої освіти за ОПП "Кібербезпека" не мали академічної мобільності, але відповідно до програми "ПРОГРАМА СПІЛЬНИЙ ДИПЛОМ Університету у Бєльсько-Бялій (УББ), Польща для студентів другого ступеня навчання (другого (магістерського) рівня вищої освіти) на напрямі/в галузі знань Інформатика/Інформаційні технології (ІТ), віднесеної до наукової дисципліни/спеціальності "Технічна інформатика та телекомунікація"/"Кібербезпека" студенти набору 2023 р. мають право отримати другий диплом Університету у Бєльсько-Бялій (Польща).

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

Проект Положення про порядок визнання результатів неформальної та інформальної освіти у Національному технічному університеті «Харківський політехнічний інститут» Затверджено Вченою Радою НТУ «ХПІ» «30» квітня 2021 р. Протокол № 4. Введено в дію наказом ректора «30» квітня 2021 р. № 206 ОД (http://blogs.kpi.kharkov.ua/v2/nv/dokumenti-ntu-hpi-2/).

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

Відповідно до пропозицій робочої групи та викладачів кафедри на ОП 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.kpi.kharkov.ua/cisco-networking-academy/) розміщено перелік курсів академії CISCO Інституту. Після проходження курсів на засіданнях кафедри затверджується кількість балів, які отримують студенти після проходження відповідних курсів академії CISCO Інституту.

4. Навчання і викладання за освітньою програмою

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

Основними формами навчання відповідно до Положення про організацію освітнього процесу в НТУ «ХПІ» (затверджено Вченою радою НТУ «ХПІ», Протокол № 1 від 27 січня 2017 р (п.8), (http://blogs.kpi.kharkov.ua/v2/nv/dokumenti-ntu-hpi-2/), силабусів (https://cybersecurity.kpi.kharkov.ua/sylabusy-osvitnikh-komponentiv-125-magistr/) є лекційні, практичні заняття, лабораторні заняття, індивідуальні заняття, командна та самостійна робота студента. Основними методами навчання на ОП 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://bit.ly/3w5adQfhttp://blogs.kpi.kharkov.ua/v2/metododel/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 форми і методи навчання і викладання відповідають вимогам студентоцентрованого підходу? Яким є рівень задоволеності здобувачів вищої освіти методами навчання і викладання відповідно до результатів опитувань?

Студенти здійснюють вибір дисциплін після ознайомлення зі змістом силабусів навчальних дисциплін, 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 дисципліни ОП студентам пропонується взяти участь в опитуванні щодо якості викладання дисципліни, 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 ОП 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 освітньою програмою – 89,6 % (https://drive.google.com/drive/folders/1VFuFrTMVMBViHsS1D9pIWTl7H6gK5XUz)

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

Відповідно до Положення про академічну мобільність студентів університету здобувачі вищої освіти мають право здійснювати навчання в закладі-партері. НТУ «ХПІ» має велику чисельність міжнародних партнерів серед закордонних закладів вищої освіти (http://web.kpi.kharkov.ua/asu/universiteti-partneri/) та компаній (http://web.kpi.kharkov.ua/asu/kompaniyi-partneri/), 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 ОП. 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 відповідає 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 ОПП, силабуси (https://cybersecurity.kpi.kharkov.ua/sylabusy-osvitnikh-komponentiv-125-magistr/), які містять інформацію щодо змісту, цілей, критеріїв та процедур оцінювання знань, компетентностей та очікуваних результатів навчання за дисциплінами.
Здобувач вищої освіти після ознайомлення з документами до початку навчального року має можливість отримати кваліфіковану консультацію викладачів навчальних дисциплін. В ЗВО в рамках виконання стратегії диджиталізації 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://bit.ly/3w5adQf). Графік організації освітнього процесу та розклади атестаційних тижнів (сесій) наведено за посиланням (http://blogs.kpi.kharkov.ua/v2/nv/zaviduvacham-kafedr/). 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 проектів 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;
- Захист 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 підтримкою кафедри у лютому 2023 року 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/), який дозволяє здобувачам отримати 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 дисципліни 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 навчальних дисциплін 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:
У 2022–2023 роках викладачами кафедри надруковано статей у НМБ Scopus – 15, з них 1 монографія (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.), які відповідають за тематикою спеціальності "Кібербезпека". Викладачі кафедри використовують науково-практичні досягнення у стартапах (https://www.calltools.ua/) та "Розумний будинок", де пропонується нова технологія захисту на основі двоконтурних (багатоконтурних) систем захисту інформації соціокіберфізичних систем на основі постквантових алгоритмів – крипто-кодових конструкцій Мак-Еліса та Нідеррайтера на алгеброгеометричних та збиткових кодах, що також використовується в ОК Моделювання кіберфізичних дій. 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".

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

В НТУ «ХПІ» здобувачі вищої освіти мають право доступу до електронних наукових баз даних SCOPUS та Web of Science.
Згідно зі стратегією інтернаціоналізації НТУ «ХПІ» (https://www.kpi.kharkov.ua/ukr/mizhnarodni-zv-yazki/strategiyainternatsionalizatsiyi/)
здобувачі вищої освіти мають право на мовну підготовку, участь у спільних освітніх програмах, залучення до науково-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/), а також приймає активну участь у проведенні МНПК IEEE "International Congress on Human-Computer Interaction, Optimization and Robotic Applications" (https://www.horacongress.com/index.php?go=supporters) (Туреччина), а також МНПК "International Congress on 3D Printing (Additive Manufacturing) Technologies and Digital Industry 2023 (HYBRID)" (https://3dprintturkey.org/#scope.html) (Туреччина), а також МНПК "Modern information, measurement and control systems: problems, applications and perspectives 2022 (MIMCS'2022)" (http://mimcs.net/) (Азербайджан).

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

Опишіть, яким чином форми контрольних заходів у межах навчальних дисциплін ОП дозволяють перевірити досягнення програмних результатів навчання?

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/dokumenti-ntu-hpi-2/
Критерії оцінювання навчальних досягнень здобувачів вищої освіти здійснюються відповідно до Положення про критерії та систему оцінювання знань та вмінь і про рейтинг студентів (https://blogs.kpi.kharkov.ua/v2/nv/dokumenti-ntu-hpi-2/).
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.kpi.kharkov.ua/program-bachelor/) 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» (http://blogs.kpi.kharkov.ua/v2/nv/dokumenti-ntu-hpi-2/).

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

Форми атестації здобувачів ОПП 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 репозиторії) 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 студентів (http://blogs.kpi.kharkov.ua/v2/nv/dokumenti-ntu-hpi-2/) 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., http://blogs.kpi.kharkov.ua/v2/nv/dokumenti-ntu-hpi-2/) зазначено порядок створення екзаменаційної комісії, організацію роботи екзаменаційної комісії, порядок проведення атестації. Ознайомитись з порядком проведення атестації можна на зазначених сайтах.

Яким чином ці процедури 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 студентів (http://blogs.kpi.kharkov.ua/v2/nv/dokumenti-ntu-hpi-2/) та Положення про екзаменаційну комісію у Національному технічному університеті «Харківський політехнічний інститут» (затверджено Вченою радою НТУ «ХПІ» Протокол №1 від 27 січня 2017р. (http://blogs.kpi.kharkov.ua/v2/nv/dokumenti-ntu-hpi-2/)
та Порядок подання апеляцій (іспити, заліки, атестація) (http://blogs.kpi.kharkov.ua/v2/nv/dokumenti-ntu-hpi-2/). 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 освітній 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 № 1 від 27 січня 2017 р. (http://blogs.kpi.kharkov.ua/v2/nv/dokumenti-ntu-hpi-2/), Положення про критерії та систему оцінювання знань та вмінь і про рейтинг студентів (http://blogs.kpi.kharkov.ua/v2/nv/dokumenti-ntu-hpi-2/).
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 (п.п.10.10http://blogs.kpi.kharkov.ua/v2/nv/dokumenti-ntu-hpi-2/ та до Положення про екзаменаційну комісію (п.8 http://blogs.kpi.kharkov.ua/v2/nv/dokumenti-ntu-hpi-2/).
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?

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 репозиторіїв НТУ «ХПІ» (наукових публікацій та кваліфікаційних випускних робіт здобувачів вищої освіти); технологічної співпраці з Unicheck Україна (ТОВ “Антиплагіат”) 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 ОП інформаційних семінарів, он-лайн 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» (http://blogs.kpi.kharkov.ua/v2/nv/wp-content/uploads/sites/17/2019/11/04_code_ethics.pdf) та положення про систему запобігання та виявлення академічного плагіату у випускних кваліфікаційних роботах здобувачів вищої освіти НТУ «ХПІ» (http://library.kpi.kharkov.ua/files/documents/polozhennya-proekt-plagyat.pdf).
Серед здобувачів вищої освіти за ОП подібних прикладів не було.

6. Людські ресурси

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

професіоналізму?

Види порушень та відповідальність за них прописані в кодексі етики академічних взаємовідносин та доброчесності НТУ «ХПІ» (http://blogs.kpi.kharkov.ua/v2/nv/wp-content/uploads/sites/17/2019/11/04_code_ethics.pdf) та положення про систему запобігання та виявлення академічного плагіату у випускних кваліфікаційних роботах здобувачів вищої освіти НТУ «ХПІ» (http://library.kpi.kharkov.ua/files/documents/polozhennya-proekt-plagyat.pdf). Серед здобувачів вищої освіти за ОП подібних прикладів не було.

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

Під час розробки ОП 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”, кан.тех.наук Ковтун Владислав Юрійович; Богдан Скрябін, науковий дослідник компанії “Distributed Lab” запропонував 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).

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

Під час розробки ОП 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”, кан.тех.наук Ковтун Владислав Юрійович; Богдан Скрябін, науковий дослідник компанії “Distributed Lab” запропонував 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).

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

Професійному розвитку викладачів ОП 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 (схвалено Вченою радою Університету протокол №5 від 30.05.2014 р., із змінами внесеними згідно протоколу №4 від 29.03.2019 р., http://blogs.kpi.kharkov.ua/v2/nv/dokumenti-ntu-hpi-2/).
Викладачі НТУ ХПІ отримали дипломи рівня В2 з англійської мови (Мілевський С.В., Погасій С.С., Євсеєев С.П., Мілов О.В., Корольов Р.В., Ткачов А.В., Воропай Н.І.), прохойшли стажування за кордоном (Король О.Г., Мілов О.В., Ткачов А.М., Корольов Р.В., Гаврилова А.А., Хвостенко В.С., Воропай Н.І. в Університеті м. Бельска-Бяла, Польща), Євсеєв С.П., Король О.Г., Мілов О.В., Ткачов А.М., Корольов Р.В. є сертифікованими спеціалістами з курсу CCNA CyberSecurity, а также Євсеєв С.П. має сертифікати з курсів CCNA Introduction to Networks, Routing and Switching Essentials, Scaling Networks, Connecting Networks (стали інструкторами з курсу).

Продемонструйте, що ЗВО стимулює розвиток 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 (http://science.kpi.kharkov.ua/polozhennya-ntu-khpi/).
Станом на 01.09.2023р. доступні такі зовнішні ресурси: аналітичні – Scopus, SciVal та платформа Web of Science (з можливістю віддаленого доступу); повнотекстові – Springer Nature (доступні книги 2017 року 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 No1 від 31.01.2020р. 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 фінансові та матеріально-технічні ресурси (бібліотека, інша інфраструктура, обладнання тощо), а також навчально-методичне забезпечення ОП забезпечують досягнення визначених ОП цілей та програмних результатів навчання?

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 http://public.kpi.kharkov.ua/zvitrektora/.
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 репозиторій 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://bit.ly/3F0p0yV.
Станом на 01.09.2023р. доступні зовнішні ресурси: аналітичні – Scopus, SciVal та платформа Web of Science (з можливістю віддаленого доступу); повнотекстові – Springer Nature (доступні книги 2017р. видання); ScienceDirect (книжкові видання та книжкові розділи, віддалений доступ для користувачів корпоративної пошти); Bentham Science (доступні книги та журнали).

Продемонструйте, яким чином освітнє середовище, створене у ЗВО, дозволяє задовольнити потреби та інтереси здобувачів вищої освіти ОП? Які заходи вживаються ЗВО задля виявлення і врахування цих потреб та інтересів?

Потреби та інтереси здобувачів вищої освіти належним образом виявляються під час співпраці ЗВО з органами студентського самоврядування. На базі НТУ «ХПІ» працює СтудАльянс (https://bit.ly/2ZLNA7G).
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://bit.ly/3BAXRRh).
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 ЗВО забезпечує безпечність освітнього середовища для життя та здоров'я здобувачів вищої освіти (включаючи психічне здоров'я)?

Оздоровчий пункт розташований у зручному для відвідувачів місці у приміщенні гуртожитку «Гігант» НТУ «ХПІ», що дозволяє досягнути вільного та зручного відвідування закладу охорони здоров'я студентами. В медичному пункті працюють 11 лікарів. Задачі центру: надання кваліфікованої лікувально - діагностичної допомоги в повному обсязі в центрі та вдома, надання невідкладної медичної допомоги при раптових захворюваннях та нещасних випадках, направлення хворих здобувачів вищої освіти на консультування до лікарів інших спеціальностей поліклінічного відділення та у стаціонарні відділення студентської лікарні, санітарно - протиепідемічних заходів, навчання жінок фертильного віку питанням планування сім'ї, проведення комплексних профілактичних медичних оглядів, флюорографічного обстеження, імунізація студентів проти керованих інфекцій, проведення санітарно - освітньої роботи серед здобувачів вищої освіти. 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 (http://blogs.kpi.kharkov.ua/v2/nv/dokumenti-ntu-hpi-2/).

Опишіть механізми освітньої, організаційної, інформаційної, консультативної та соціальної підтримки здобувачів вищої освіти? Яким є рівень задоволеності здобувачів вищої освіти цією підтримкою відповідно до результатів опитувань?

Права та обов'язки здобувачів освіти регламентують Правила поведінки здобувачів освіти НТУ «ХПІ» http://blogs.kpi.kharkov.ua/v2/nv/wp-content/uploads/sites/17/2021/07/PRAVILA-POVEDINKI-ZDOBUVACHIVOSVITI-NTU-HPI.pdf.
Навчально-методичне забезпечення дисциплін ОП доступно на внутрішньому репозитарії електронних документів кафедри. Методичні рекомендації та учбові посібники розміщені в електронному репозитарії. НТУ «ХПІ» (http://repository.kpi.kharkov.ua/handle/KhPI-Press/1665). 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 репозиторії електронних документів кафедр. Методичні рекомендації та навчальні посібники розміщені в електронному репозиторії НТУ «ХПІ» http://library.kpi.kharkov.ua/scripts/irbis64r_01/cgiirbis_64.exe?C21COM=F&I21DBN=BOOK&P21DBN=BOOK&LNG=uk. 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://profkom-khpi.org/ 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.

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 осіб з обмеженими фізичними можливостями та інших маломобільних груп населення на території Національного технічного університету «Харківський політехнічний інститут» здійснюється згідно наказу №354 ОД від 27 липня 2018р. про порядок супроводу (надання допомоги) осіб з інвалідністю та інших маломобільних груп населення в НТУ «ХПІ» (http://blogs.kpi.kharkov.ua/v2/nv/wp-content/uploads/sites/17/2020/02/2020_PORYADOK-suprovodu-nadannya-dopomogi-osib-z-invalidnistyu.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 ОП таких студентів не навчалось.
Документи, які регулюють перебування особами з особливими освітніми потребами в ЗВО Інформація на сайті:
1) http://vstup.kpi.kharkov.ua/korisni-posilannya-dlya-abituriientiv/normatygni-dokumenty/?fbclid=IwAR38EDcauCcXp4S7Ls4MNesrklEZAwetVjRq8xmeLZc8hLecpxLrtLmerQ
2) http://blogs.kpi.kharkov.ua/v2/nv/wp-content/uploads/sites/17/2020/02/2020_PORYADOK-suprovodu-nadannya-dopomogi-osib-z-invalidnistyu.pdf (наказ № 129 Од від 24 лютого 2020р.).

Яким чином у ЗВО визначено політику та процедури врегулювання конфліктних ситуацій (включаючи пов'язаних із сексуальними домаганнями, дискримінацією та корупцією)? Яким чином забезпечується їх доступність політики та процедур врегулювання для учасників освітнього процесу? Якою є практика їх застосування під час реалізації ОП?

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 затверджено наказом НТУ «ХПІ» № 501 ОД від «28» жовтня 2019р. http://blogs.kpi.kharkov.ua/v2/nv/wpcontent/uploads/sites/17/2019/10/PORYADOK-rozgglyadu-skarg-zdobuvachiv-osviti-_28_10_2019_1.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». (http://blogs.kpi.kharkov.ua/v2/nv/wpcontent/uploads/sites/17/2021/07/PORYADOK-PODANNYA-TA-ROZGLYADU-REAGUVANNYA-NA-DOVEDENIVIPADKI-BULINGU-NTU-HPI.pdf, http://blogs.kpi.kharkov.ua/v2/nv/wp-content/uploads/sites/17/2021/07/PLANZAHODIV-IZ-ZAPOBIGANNYA-TA-PROTIDIYI-BULINGU-NTU-HPI.pdf) .
У разі ситуацій пов'язаних із сексуальними домаганнями, дискримінацією з потерпілим працює соціально-психологічна служба НТУ «ХПІ».
http://blogs.kpi.kharkov.ua/v2/nv/wpcontent/uploads/sites/17/2019/10/POLOZHENNYA-pro-sotsialno-psihologichnu-sluzhbu-NTU-HPI-27_09_2019.doc.
Практики застосування таких процедур на даній ОП не було.

8. Внутрішнє забезпечення якості освітньої програми

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

Процедури розроблення, затвердження, моніторингу та періодичного перегляду 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" http://blogs.kpi.kharkov.ua/v2/nv/dokumenti-ntu-hpi-2/

Опишіть, 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 університет» http://blogs.kpi.kharkov.ua/v2/nv/dokumenti-ntu-hpi-2/ перегляд освітніх програм відбувається щорічно. Перегляд ОПП здійснює група забезпечення спеціальності, завдання та функції якої визначені у зазначених «Методичних рекомендаціях щодо розроблення, затвердження та оновлення освітніх програм».
Перегляд та оновлення ОПП відбувається кожен навчальний рік з урахуванням результатів моніторингу ОПП http://blogs.kpi.kharkov.ua/v2/nv/dokumenti-ntu-hpi-2/, зауважень, результатів, відображених у звітах про забезпечення якості освіти в Університеті http://blogs.kpi.kharkov.ua/v2/quality/pidsumky/, висновків та пропозицій роботодавців та здобувачів вищої освіти; стратегії (програми) розвитку університету тощо.
Були прийняті до уваги пропозиції компаній стейкхолдерів (учасників розробки ОПП) 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 позиція береться до уваги під час перегляду ОП

Здобувачі мають постійний доступ до змісту та складових ОПП на сайті НТУ «ХПІ». До процесу періодичного перегляду ОПП 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.kpi.kharkov.ua/onovlennya-osvitnikh-program-125-magistr/), або пропозиції здобувачів щодо удосконалення ОПП 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 щодо змісту ОПП на відповідних засіданнях вченої ради інституту, науково-методичних семінарах.

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

До процесу періодичного перегляду ОПП 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 процесу періодичного перегляду ОП та інших процедур забезпечення її якості

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

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

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://www.kpi.kharkov.ua/rus/tag/tsentr-karera-ntu-hpi/, 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).

Які недоліки в ОП та/або освітній діяльності з реалізації ОП були виявлені у ході здійснення

процедур внутрішнього забезпечення якості за час її реалізації? Яким чином система забезпечення якості ЗВО відреагувала на ці недоліки?

За результатами співбесід зі здобувачами вступу 2022 р. другого (магістерського) рівня вищих освіти було виявлено, що недостатня увага приділяється набуттю компетентностей щодо практичної роботи з розробки програмних застосунків та забезпечення їх безпеки. З метою покращення в рамках дисципліни Веб-безпека пропонуються практичні заняття з цих питань. З метою покращення якості проведення практичних занять навчальних дисциплін, 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.

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

Акредитація уперше

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

Учасники академічної спільноти змістовно залучаються до процедур внутрішнього забезпечення якості ОП 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., Керівник навчально-наукового центру інформаційних технологій Поліського національного університету Молодецька К.В. (м. Житомир).
З метою своєчасного врахування зауважень та пропозицій від академічної спільноти на сайті кафедри створена сторінка, яка дозволяє своєчасно ознайомитись з пропозиціями внесення змін до ОПП "Кібербезпека". Крім цього, є можливість відправити свої пропозиції та зауваження з використання веб-застосунку (https://cybersecurity.kpi.kharkov.ua/onovlennya-osvitnikh-program-125-magistr/)

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

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 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 ОПП.
Структурні підрозділи співпрацюють на забезпечення якості освіти.

9. Прозорість і публічність

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

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://bit.ly/3apTJa1;
Правила внутрішнього розпорядку НТУ «ХПІ» https://bit.ly/2ygtGUt;
Положення про організацію освітнього процесу https://bit.ly/2UqlsBV;
Положення про підготовку здобувачів вищої освіти ступеня доктора філософії в аспірантурі https://drive.google.com/file/d/1TP1zmObzR1pymt-YjlT_alsOF8uloLW_/view;
Положення про забезпечення якості освітньої діяльності та якості вищої освіти в НТУ «ХПІ» https://bit.ly/2QToMjF;
Положення про академічну мобільність студентів, аспірантів, докторантів, науково-педагогічних та наукових працівників університету https://bit.ly/2UqlsBV;
Положення про критерії та систему оцінювання знань та вмінь і про рейтинг студентів https://bit.ly/2UqlsBV;
Положення про ректорат, Положення про Вчену раду, Положення про раду з якості, Положення по Наглядову раду, Положення про кафедру https://bit.ly/2QToMjF.
На розгляді проект Положення про проектні групи освітньої діяльності, робочі групи освітніх програм, групи забезпечення спеціальностей https://bit.ly/39LnBfP.

Наведіть посилання на веб-сторінку, яка містить інформацію про оприлюднення на офіційному веб-сайті ЗВО відповідного проекту з метою отримання зауважень та пропозиції заінтересованих сторін (стейкхолдерів). Адреса веб-сторінки

https://cybersecurity.kpi.kharkov.ua/osvitno-profesijna-programa-125-magistr/

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

https://cybersecurity.kpi.kharkov.ua/osvitno-profesijna-programa-125-magistr/

11. Перспективи подальшого розвитку ОП

Якими загалом є сильні та слабкі сторони ОП?

Сильними сторонами ОП 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, аналітиком систем захисту інформації та оцінки вразливостей, аналітиком з безпеки інформаційно-телекомунікаційних систем та інш. 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.
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 ОП 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?

Сильними сторонами ОП 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, аналітиком систем захисту інформації та оцінки вразливостей, аналітиком з безпеки інформаційно-телекомунікаційних систем та інш. 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.
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 ОП є відсутність створення CIRT на базі кіберполігону, приєднання до мережі CERT України.

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: Сокол Євген Іванович

Дата: 05.09.2023 р.

Таблиця 1. Інформація про обов'язкові освітні компоненти ОП

Назва освітнього компонента	**Вид компонента**	**Силабус або інші навчально-методичні матеріали**		**Якщо освітній компонент потребує спеціального матеріально-технічного та/або інформаційного забезпечення, наведіть відомості щодо нього***
		Назва файла	**Хеш файла**	
Англійська мова	навчальна дисципліна	*Силабус_Англійська мова.pdf*	yYKsyDDzybUfhy0IUAGFyw/4jB5A9Su7T9Io4JogWEw=	*Обладнання:* *Комп'ютерний клас:* *1. ПК Intel Celeron G1610T 2.30GHz, Ram 4 Gb, HDD 160 Gb, monitor Philips 170S – 14 шт* *Література:* *1. Словник термінів із кібербезпеки / За заг. ред. О. В. Копана, Є. Д. Скулиша - К.: ВБ «Аванпост-Прим», 2012.-214 с.* *2. Borova T. English for Business Analysts: textbook: in 3 parts, Part 3. Business Intelligent Tools / T. Borova, O. Milov. – Kharkiv: S. Kuznets KhNUE, 2019. – 179 P.* *3. Journal of Information Security [Електронний ресурс].- Режим доступу: https://www.scirp.org/journa/home.aspx?issueid=l4294#103116*
Веб-безпека	навчальна дисципліна	*Силабус_Веб-безпека.pdf*	uSFfl9yq16OfgBlwQwqO4anF+xvMvgK6mbShFSU7Cl4=	*Обладнання:* *Кіберполігон:* *1. ПК Intel I3-2100/4Gb/150GB - 6 шт* *2. ПК Intel I3-530/4Gb/150GB - 19 шт* *3. Системний блок R-LINE серверний у складі: процесор Intel Xeon Silver 4210R*2шт/ материнська плата Supermicro MBDX11DDW-L/ оперативна пам'ять Samsung 32GB DDR4-3200 ECC Registered *4шт/ накопичувач 3840GB Samsung PM983 NVMe M.2*2шт/ RAID контролер Supermicro AOC-SLG3-2H8M2/ мережева плата Supermicro AOC-SGP-I2/ корпус Supermicro 1U, 4 x 3.5" hot-swap SAS/SATA, Redundant 700/750W/ ДБЖ APC Smart-UPS RM 3000VA LCD (SMC3000RMI2U) 4. FortiSwitch-148F 1 Year 24x7 FortiCare Contract FC-10-148FN247-02-12* *5. USB адаптер модуль Zigbee CC2531 Sniffer сніфер.* *6. Радіоприймач аналізатор спектру зібраний portapack h2+i hackrf one.* *Література:* *1. CCNA Cybersecurity Operations [Електронний ресурс]. – Режим доступу: https://www.netacad.com/ru/courses/cybersecurity/cyberops-associate* *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: *5. https://www.checkpoint.com/solutions/google-cloud-platform-security/* *6. Kali Linux [Електронний ресурс]. – Режим доступу : https://www.kali.org/*
Господарське право	навчальна дисципліна	*Силабус_Господарське право.pdf*	QQScJUrffPDipCFtDeC+BBhrRuKfHcV52eUPu7sp28k=	*Обладнання:* *Комп'ютерний клас:* *1. ПК Intel Celeron G1610T 2.30GHz, Ram 4 Gb, HDD 160 Gb, monitor Philips 170S – 14 шт* *Література:* *1. Андрєєва О. Б., Жорнокуй Ю. М., Гетманець О. П. та ін. Господарське право України. Частина 1 Навчальний посібник. – Х.: Харк. нац. ун-т внутр. справ, 2014. – 340 с.* *2. Гетманець О.П. (ред). Господарське право України. Частина 2 Навчальний посібник. – Х.: Харк. нац. ун-т внутр. справ, 2014. – 368 с.* *3. Господарський кодекс України : Закон України від 16.01.2003 р. № 436-IV // Відом. Верхов. Ради України. – 2003. – № 18. – Ст. 144.* *4. Господарський процесуальний кодекс України : Закон України від 06.11.1991 № 1798-XII // ВВР України. – 2001. – № 36. – Ст. 188.* *5. Кодекс України про адміністративні правопорушення : Закон України від 07.12.1984 р. № 8073-X // Відомості Верхов-ної Ради УРСР. – 1984. – № 51. – Ст. 1122.* *6. Конституція України : прийнята на п'ятій сес. Верхов. Ради України 28 черв. 1996 р. – К. : Преса України, 1997. – 80 с.* *7. Податковий кодекс України : Закон України від 02.12.2010 р. № 2755-VI // ВВР України. – 2011. – № 13. – Ст. 112.* *8. Понікаров В. Д. Господарське законодавство : навч. посібн. / В. Д. Понікаров, Ж. О. Андрійченко. □ Х. : ВД "ІНЖЕК", 2004. □ 232 с.* *9. Про акціонерні товариства : Закон України від від 17 вересня 2008 року № 514-VI // ВВР України*
Захист інтелектуальної власності	навчальна дисципліна	*Силабус_Захист інтелектуальної власності.pdf*	1R1shD8NwoPxcGGLoQqAhnQbnLpjFypJU1XoIKh10Cg=	*Обладнання:* *Комп'ютерний клас:* *1. ПК Intel Celeron G1610T 2.30GHz, Ram 4 Gb, HDD 160 Gb, monitor Philips 170S – 14 шт* *Література:* *1. Доріс Лонг, Патриція Рей, Жаров В.О., Шевелева Т.М., Василенко І.Е., Дроб'язко В.С. Захист прав інтелектуальної власності: норми міжнародного і національного законодавства та їх правозастосування. Практичний посібник. – К.: "К.І.С. ", 2007.– 448 с.* *2. Драпак Г. Основи інтелектуальної власності : навчальний посібник / Г. Драпак, М. Скиба. – Хмельницький : ТУП, 2003. – 135 с.*

				3. Кожарська І. Ю. Патентне право: конспект лекцій навчального курсу / І. Ю. Кожарська. – К. : ЗАТ "Інст. інтелектуальної власн. та права", 2003. – 140 с. *4. Кузнецов Ю. М. Патентознавство та авторське право : підручник / Ю. М. Кузнецов. – К. : Кондор, 2005. – 428 с.* *5. Конституція України. Прийнята Верховною Радою України 28 червня 1996 р. // Відомості Верховної Ради України. – 1996. – № 30. – С. 141.* *6. Цивільний кодекс України від 16.01.03 № 435-IVЗакон України від 23 грудня 1993 р. № 3793-XII «Про авторське право і суміжні права».*
Інноваційне підприємництво та управління стартап проектами	навчальна дисципліна	*Силабус_Інноваційне підприємництво та управління стартап проєктами.pdf*	sHCymigCt3eLPAYoYwovxvdwUsMclpvRW105gSVDaeU=	*Обладнання:* *Комп'ютерний клас:* *1. ПК Intel Celeron G1610T 2.30GHz, Ram 4 Gb, HDD 160 Gb, monitor Philips 170S – 14 шт* *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.* *2. Ден Сенор, Сол Сінґер. Країна стартапів. Історія ізраїльського економічного дива. Yakaboo Publishing. 2016. – 368 с.* *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.* *4. Шаповал В.А. Опорний конспект лекцій «Стартап міжнародних проектів» для студентів спеціальності «076 19 Підприємництво, торгівля та біржова діяльність». Дніпро: ДВНЗ «НГУ», 2017. – 29 с.* *5. Тимур Ворона. Стартап на мільйон: як українці за-робляють статки на технологіях. – К. : Видавництво «ВІВАТ», 2017. – 224 с.* *6. Лей Галлагер. Історія Airbnb: Як троє звичайних хло-пців підірвали готельну індустрію. – К. : Видавництво: "Book Chef", 2018.*
Презентація та обробка знань	навчальна дисципліна	*Силабус_Презентація та обробка знань.pdf*	PiDiND4yaygTmH6SdIv1vLsQDZAaj3sCq9XVVnEv734=	*Обладнання:* *Комп'ютерний клас:* *1. ПК Intel Celeron G1610T 2.30GHz, Ram 4 Gb, HDD 160 Gb, monitor Philips 170S – 14 шт* *Література:* *1. Аналіз даних та знань : навчальний посібник / Литвин В. В., Пасічник В. В., Нікольський Ю. В. – Львів : Магнолія-2006 , 2021. – 276 с.*

				2. Data Mining : пошук знань в даних / Гладун А. Я., Рогушина Ю. В. – К. : ТОВ «ВД «АДЕФ-Україна», 2016. – 452 с. *3. Черняк О. І. Інтелектуальний аналіз даних : підручник / О. І. Черняк, П. В. Захарченко. – К. : Знання, 2014. – 599 с.*
Розширена мережева та хмарна безпека	навчальна дисципліна	*Силабус_Розширена мережева та хмарна безпека.pdf*	Csm1XLwMpipQ/1BqssScjvvjqzyvQLphrPxkORm77FY=	*Обладнання:* *Комп'ютерний клас Cisco:* *Laptop (Ноутбук) Dell Inspiron 3584 15.6 FHD (1920 xl 080), Intel Core i3-7020U (2.3 GH7), RAM 4GB DDR4, HDD I TB – 1 шт.* *MFD (багатофункціональний пристрій) Canon i-SENSYS MF42 Idw – 1 шт.* *ПК: i3- 9100 3.6GHz / H310 /4Gb /500GB/Wi-Fi/ – 12 шт.* *Interactive panel (Інтерактивна панель) Prestigio 55" (i5-8400/8Gb/256Gb/ Windows 10 Pro) з мобільною стійкою – 1 шт.* *Conference system (система проведення конференцій) LOGITECH Conference Cam GROUP – 1 шт.* *CISCO обладнання:* *Cisco Комутатор Catalyst 2960 – 6 шт.* *Cisco Маршрутизатор-2801 – 6 шт.* *Cisco ASA 5510 – 1 шт.,* *Cisco ASA 5506 – 1 шт.* *Cisco комутатор Catalyst 3750 – 4 шт.* *Cisco Маршрутизатор 2911 з IPS – 2 шт.* *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 :* *5. https://www.checkpoint.com/solutions/google-cloud-platform-security/* *6. Kali Linux [Електронний ресурс]. – Режим доступу : https://www.kali.org/* *7. Ronald L. Krutz and Russell Dean Vines. 2010. Cloud Security: A Comprehensive Guide to Secure Cloud Computing. Wiley Publishing.* *8. Abdulsalam YS, Hedabou M. Security and Privacy in Cloud Computing: Technical Review. Future Internet. 2022; 14(1):11. https://doi.org/10.3390/fi14010011*
Тестування на проникнення та етичний хакінг	навчальна дисципліна	*Силабус_Тестування на проникнення та етичний хакінг.pdf*	tBrVIrEeYgoYod8+n4fG+2l4aCai/w1/2C57GXBucTU=	*Обладнання:* *Комп'ютерний клас Cisco:* *Laptop (Ноутбук) Dell Inspiron 3584 15.6 FHD (1920 xl 080), Intel Core i3-7020U (2.3 GH7), RAM 4GB DDR4, HDD I TB – 1 шт.*

				MFD (багатофункціональний пристрій) Canon i-SENSYS MF42 Idw – 1 шт. *ПК: i3- 9100 3.6GHz / H310 /4Gb /500GB/Wi-Fi/ – 12 шт.* *Interactive panel (Інтерактивна панель) Prestigio 55" (i5-8400/8Gb/256Gb/ Windows 10 Pro) з мобільною стійкою – 1 шт.* *Conference system (система проведення конференцій) LOGITECH Conference Cam GROUP – 1 шт.* *CISCO обладнання:* *Cisco Комутатор Catalyst 2960 – 6 шт.* *Cisco Маршрутизатор-2801 – 6 шт.* *Cisco ASA 5510 – 1 шт.,* *Cisco ASA 5506 – 1 шт.* *Cisco комутатор Catalyst 3750 – 4 шт.* *Cisco Маршрутизатор 2911 з IPS – 2 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.* *2. Євсеєв С.П. Кібербезпека: Лабораторний практикум з основ криптографічного захисту. – Львів "Новий світ-2000", 2020ю – 241 с.* *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.*
Технології управління безпекою бізнес-процесів	навчальна дисципліна	*Силабус_Технології управління безпекою бізнес-процесів.pdf*	JCq3dsQ8LxYgpviTHn78fn8w7SG+FDGYS/QSzQjhJq8=	*Обладнання:* *Комп'ютерний клас:* *1. ПК Intel Celeron G1610T 2.30GHz, Ram 4 Gb, HDD 160 Gb, monitor Philips 170S – 14 шт* *Література:* *1. Інформаційна безпека та інформаційні технології. – Х.; ТОВ "ДІСА ПЛЮС", 2019. - 322 с.* *2. Кібербезпека та інформаційні технології. – Х.; ТОВ "ДІСА ПЛЮС", 2020. -380 с.* *3. Управління бізнес-процесами: Навч. посібник. – Рівне: НУВГП, 2014. – 158 с.*
Цифрова криміналістика	навчальна дисципліна	*Силабус_Цифрова криміналістика.pdf*	osLMt+anOxCe5UDeEMiXNWGC82zAUMtW9HZu/uTuwjM=	*Обладнання:* *Кіберполігон:* *1. ПК Intel I3-2100/4Gb/150GB - 6 шт* *2. ПК Intel I3-530/4Gb/150GB - 19 шт* *3. Системний блок R-LINE серверний у складі: процесор Intel Xeon Silver 4210R*2шт/ материнська плата Supermicro MBDX11DDW-L/ оперативна пам'ять Samsung 32GB DDR4-3200 ECC Registered *4шт/ накопичувач 3840GB Samsung PM983 NVMe M.2*2шт/ RAID контролер Supermicro AOC-SLG3-2H8M2/ мережева плата Supermicro AOC-SGP-I2/ корпус Supermicro 1U, 4 x 3.5" hot-swap SAS/SATA, Redundant 700/750W/ ДБЖ APC Smart-UPS RM 3000VA LCD*

				(SMC3000RMI2U) 4. FortiSwitch-148F 1 Year 24x7 FortiCare Contract FC-10-148FN247-02-12 *5. USB адаптер модуль Zigbee CC2531 Sniffer сніфер.* *6. Радіоприймач аналізатор спектру зібраний portapack h2+i hackrf one.* *Література:* *1. Davidoff, Sherri. Network forensics: tracking hackers through cyberspace / Sherri Davidoff, Jonathan Ham. Pearson Education, Inc. 2012.* *2. Євсеєв С.П. Кібербезпека: Лабораторний практикум з основ криптографічного захисту. – Львів "Новий світ-2000", 2020р – 241 с.* *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.* *4. Маркусь В. О. Криміналістика. Навчальний посібник – К.: Кондор, 2007. – 558 с.* *5. Цифрова криміналістика : консп. лекцій / уклад. І. З. Яки-менко. - Тернопіль : ТНЕУ, 2019. - 109 с.* *6. Вертузаєв М. С., Голубаєв В. О., Котляревський О. І., Юр-ченко О. М. Безпека комп'ютерних систем. Комп'ютерна зло-чинність та її попередження / Під ред. Снігірьова О. П.. – Запоріжжя: ПВКФ «Навел», 1998.* *7. Полотай О.І. «Роль комп'ютерної криміналістики у забез-печенні інформаційної безпеки. Інформаційне суспільство: тех-нологічні, економічні та технічні аспекти становлення» : матері-али Міжнародної наукової інтернетконференції. – Тернопіль. вип. 67. 2022. – с. 41-43* *8. Brian Carrier. File Systems Forensic Analysis / Addison Wesley Professional, 2005. – 382 p.* *9. Jason T. Luttgens, Matthew Pepe, Kevin Mandia. Incident Response & Computer Forensics / McGraw-Hill, 2014. 706 p.* *10. Harlan Carvey. Investigating Windows Systems / Elsevier Inc., 2018. – 128 p.* *11. Oleg Skulkin, Scar de Courcier. Windows Forensics Cookbook / Packt Publishing, 2017. – 456 p.* *12. Michael Hale Ligh. The Art of Memory Forensics: Detecting Malware and Threats in Windows, Linux, and Mac Memory / John Wiley & Sons, Inc., 2014. – 914 p.* *13. Davidoff, Sherri. Network forensics: tracking hackers through cyberspace / Sherri Davidoff, Jonathan Ham. 2012. 916 p.* *14. Ric Messier. Network Forensics. John Wiley & Sons, Inc., 2017. – 344 p.*

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

Таблиця 2. Зведена інформація про викладачів ОП

ID викладача	ПІБ	Посада	Структурний підрозділ	Кваліфікація викладача	Стаж	Навчальні дисципліни, що їх викладає викладач на ОП	Обґрунтування
410253	Ткачов Андрій Михайлович	Доцент, Основне місце роботи	Навчально-науковий інститут комп'ютерних наук та інформаційних технологій	Диплом спеціаліста, Харківський військовий університет, рік закінчення: 1996, спеціальність: 7.080403 Програмне забезпечення обчислювальної техніки і автоматизованих систем, Диплом кандидата наук ДК 025982, виданий 13.10.2004, Атестат старшого наукового співробітника (старшого дослідника) АС 000423, виданий 26.09.2012	32	Розширена мережева та хмарна безпека	Підвищення кваліфікації: 1) Центр підтримки академій Cisco Національний технічний університет "Харківський політехнічний інститут". Сертифікат від "30" червня 2021 р. 6 кредитів. Тема: "CCNA CyberOps" та "Network Security". 2) Міжнародний проект USAID "Кібербезпека критичної інфраструктури України" Сертифікат від "23" липня 2021 р. 3 кредити. Тема: "Аналіз шкідливих програм". Пункти відповідності ліцензійних умов: П. 1, 2, 4, 10, 12, 13,14,19 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. Д.А. Гриб, Б.О. Демідов, Ю.Ф. Кучеренко, А.М. Ткачов, Т.В. Кулєшова Принципи, методи і технології ведення збройної боротьби, управління силами і засобами в умовах активного інформаційного протиборства конфліктуючих сторін // Наука і техніка Повітряних Сил Збройних Сил України, 2019, - Вип. 1 (34). -С. 13-22. –Укр. http://www.hups.mil.gov.ua/periodic-app/article/19192 (0,5 ум. др. арк. / 0,1 ум. др. арк. власного внеску) вільний (дата звернення 11.10.2021). (фахове, категорія Б) 2. О.В. Турінський, Д.А. Гриб, Б.О. Демідов, Ю.Ф. Кучеренко, А.М. Ткачов, О.О.

							Хмелевська Науково-методичні основи і засоби дослідження процесів управління структурною динамікою складних багатоструктурних систем військового призначення у їх змістовному висвітленні // Наука і техніка Повітряних Сил Збройних Сил України. — 2019. — № 3(36). С. 60-72. Режим доступу: http://www.hups.mil.gov.ua/periodic-app/article/19226 вільний, (дата звернення 11.10.2021). (фахове, категорія Б) 3. S.Yevseiev, R. Korolyov, A. Tkachov, O. Laptiev, I. Opirskyy, O. Soloviova // Modification of the algorithm (OFM) S-box, which provides increasing crypto resistance in the post-quantum period / International Journal of Advanced Trends in Computer Science and Engineering, 9(5), September-October 2020, pp. 8725 - 8729 http://repository.hneu.edu.ua/jspui/bitstream/123456789/24831/1/India_Scopus_9.pdf (0,252 ум. др. арк. / 0,042 ум. др. арк. власного внеску) вільний (дата звернення 11.10.2021). (Scopus) 4. Yevseiev S., Korolyov R., Tkachov A., Nimchenko A. // Development of procedures for modifying the cipher GOST 28147 / Advanced Information Systems. 2021. Vol. 5, No. 2. P. 125-129. http://ais.khpi.edu.ua/article/view/235002 (0,16 ум. др. арк. / 0,04 ум. др. арк. власного внеску)вільний (дата звернення 11.10.2021). (фахове, категорія Б) 5. Voitko O., Solonnikov S., Poliakova O., Tkachov A. // Equations of periodic modes, which take into account features of the dynamics of their course in nonlinear automatic systems with computers in control system / Системи обробки інформації. 2021. №1(164). С. 12-20. http://repository.hneu.

							edu.ua/handle/123456789/25624 (0,1 ум. др. арк. / 0,25 ум. др. арк. власного внеску) вільний (дата звернення 11.10.2021). (фахове, категорія Б) 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. (12,25 ум. др. арк. / 0,4 ум. др. арк. власного внеску) вільний (дата звернення 30.08.2023). (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. Патент на винахід (корисну модель) СПОСІБ КРИПТОГРАФІЧНОГО ПЕРЕТВОРЕННЯ ІНФОРМАЦІЇ З ВИКОРИСТАННЯМ ПОДОВЖЕНИХ КОДІВ З НАНЕСЕННЯМ ЗБИТКУ G09C 1/00. № 143963, Україна, МПК (2020.01). - № u 2020 00756; Заяв. 07.02.2020; опубл. 25.08.2020, Бюл. № 22. – 6 с. 2. Патент на винахід (корисну модель) u 2021 03726 від 30.06.2021 СПОСІБ КРИПТОГРАФІЧНОГО ПЕРЕТВОРЕННЯ ІНФОРМАЦІЇ. 3. Патент на винахід (корисну модель) u 2021 03704 від 29.06.2021 СПОСІБ КРИПТОГРАФІЧНОГО ПЕРЕТВОРЕННЯ ІНФОРМАЦІЇ 4. Патент на винахід (корисну модель) u 2021 03665 від 25.06.2021 СПОСІБ КРИПТОГРАФІЧНОГО ПЕРЕТВОРЕННЯ ІНФОРМАЦІЇ. Патент на винахід (корисну модель) u 2021 03683 від 23.07.2021 СПОСІБ КРИПТОГРАФІЧНОГО ПЕРЕТВОРЕННЯ ІНФОРМАЦІЇ. 5. Патент на винахід (корисну модель) u

							2021 03680 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. Технології програмування: робоча програма навчальної дисципліни для студентів спеціальності 125 “Кібербезпека” першого (бакалаврського) рівня [Електронне видання] / укл. О. В. Шматко, А. М. Ткачов – Харків : Вид. ХНЕУ ім. С. Кузнеця, 2020. (Укр. мов.) Режим доступу: https://pns.hneu.edu.ua/course/view.php?id=5397 2. Передові методики програмування: робоча програма навчальної дисципліни для студентів спеціальності 125 Кібербезпека другого (магістерського) рівня [Електронне видання] / укл. А. М. Ткачов – Харків : Вид. ХНЕУ ім. С. Кузнеця, 2020. (Укр. мов.) Режим доступу: https://pns.hneu.edu.ua/course/view.php?id=7224 3. Адміністрування UNIX подібних систем: робоча програма навчальної дисципліни для студентів спеціальності 125 «Кібербезпека» першого (бакалаврського) рівня / укл. А. М. Ткачов, С. С. Погасій. – Харків : ХНЕУ ім. С. Кузнеця, 2020. (Укр. мовою). Режим доступу:

							https://pns.hneu.edu.ua/course/view.php?id=7554 4. Веб-програмування: робоча програма навчальної дисципліни для студентів спеціальності 122 “Комп`ютерні науки” першого (бакалаврського) рівня [Електронне видання] / укл. А. М. Ткачов. – Харків: ХНЕУ ім. С. Кузнеця, 2020. Режим доступу: https://pns.hneu.edu.ua/course/view.php?id=4931 5. Веб-технології та веб-дизайн: робоча програма навчальної дисципліни для студентів спеціальності 121 “Інженерія програмного забезпечення”, 122 “Комп`ютерні науки” першого (бакалаврського) рівня [Електронне видання] / укл. А. М. Ткачов. – Харків : ХНЕУ ім. С. Кузнеця, 2020. Режим доступу: https://pns.hneu.edu.ua/course/view.php?id=5381 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», у рамках літньої програми підготовки з Кібербезпеки 2021, 14 червня – 23 липня 2021, успішно закінчив навчання на курсі “Аналіз зловнамірних програм” сертифікат про виконання, що підписаний Тимоті Дубель - Голова відділу Заходів з Кібербезпеки USAID сертификат 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. Ткачов А. Аналіз технологій боротьби у інформаційному просторі // Збірник наукових праць Харківського університету Повітряних Сил. - Харків, 2010. Вип. 4(26), С.28-31. (0,28 ум. др. арк. / 0,055 ум. друк. арк. власного внеску). Режим доступу: http://www.hups.mil.gov.ua/periodic-app/article/2728 (дата звернення 11.10.2021). 2. Ткачов А. Оцінка захищеності інформаційно-управляючих систем // Системи обробки інформації. - Харьків: ХУПС. -2010. - Вип. 9 (90). -С. 104-106. – Укр. (0,18 ум. др. арк. / 0,18 ум. друк. арк. власного внеску). Режим доступу: http://nbuv.gov.ua/UJRN/soi_2010_9_33 вільний, (дата звернення 11.10.2021). 3. Aloshyn, H. V., Kolomiitsev, O. V., Kulieshov, O. V., Kulahin, K. K. and Tkachov, A. M. // The method of parameters optimization of the multifunctional laser information-measuring system on the multiplicity of signals, structures and technical parameters. Science and Technology of the Air Force of Ukraine, No. 1(30), 2018. pp. 73-79. (0,43 ум. др. арк. / 0,07 ум. друк. арк. власного внеску). Режим доступу: http://www.hups.mil.gov.ua/periodic-app/article/18332 вільний, (дата звернення 11.10.2021). 4. Д.А. Гриб, Б.О. Демідов, Ю.Ф. Кучеренко, А.М. Ткачов, Т.В. Кулєшова Принципи, методи і технології ведення збройної боротьби, управління силами і засобами в умовах активного інформаційного протиборства конфліктуючих сторін // Наука і техніка Повітряних Сил Збройних Сил України, 2019, - Вип. 1 (34). -С. 13-22. –Укр. (0,52 ум. др. арк. / 0,08 ум. друк. арк. власного внеску). Режим доступу:

							http://www.hups.mil.gov.ua/periodic-app/article/19192 вільний, (дата звернення 11.10.2021). 5. Д.А. Гриб, Б.О. Демідов, О.В. Довбня, Ю.Ф. Кучеренко, А.М. Ткачов Управління структурною динамікою складних систем військового призначення у оперативно-тактичній обстановці, що динамічно змінюється // Наука і техніка Повітряних Сил Збройних Сил України./ — 2019. — № 2(35). С. 16-26. Режим доступу: http://www.hups.mil.gov.ua/periodic-app/article/19272 вільний, (дата звернення 11.10.2021). 6. Ю.Ф. Кучеренко, А.М. Носик, А.М. Ткачов, Є.В. Шубін Визначення ефективності функціонування системи управління військового призначення з врахуванням вагомості, своєчасності та якості виконання завдань у її підсистемах військового призначення // Збірник наукових праць Харківського університету Повітряних Сил. - Харків, 2019. Вип. 4(62), С.53-60. (0,5 ум. др. арк. / 0,12 ум. друк. арк. власного внеску). Режим доступу: http://www.hups.mil.gov.ua/periodic-app/article/19567 вільний, (дата звернення 11.10.2021). 7. Д.А. Гриб, Б.О. Демідов, Ю.Ф. Кучеренко, А.М. Ткачов, Є.В. Шубін // Принципи, методи і технології моделювання і дослідження процесів функціонування складних багатоструктурних систем військового призначення і управління їх структурною динамікою Системи обробки інформації. — 2019. — № 1(156). С. 64-73. Режим доступу: http://www.hups.mil.gov.ua/periodic-app/article/19192 вільний, (дата

							звернення 11.10.2021). 8. Tkachov A. /Tomashevsky B. Yevseiev S. Tkachov A. PERSPECTIVE NATIONAL COMMUNICATION SYSTEM FOR CYBER MANAGEMENT OF CRITICAL FACILITIES // Scientific Collection «InterConf», (39): with the Proceedings of the 8th International Scientific and Practical Conference «Science and Practice: Implementation to Modern Society» (December 26-28, 2020) in Manchester, Great Britain; pp. 1834-1840. Available at: https://www.interconf.top/documents/2020.12.26-28.pdf П. 13 проведення навчальних занять із спеціальних дисциплін іноземною мовою (крім дисциплін мовної підготовки) в обсязі не менше 50 аудиторних годин на навчальний рік 2019-2020 н. р.: 1.КОМП'ЮТЕРНІ СИСТЕМИ ТА АРХІТЕКТУРА КОМП'ЮТЕРІВ 121.010-А, ЕІ, лекцій - 48, лаб. роб. - 26. 2020-2021 н. р. : 1.ПРОГРАМУВАННЯ 121 ЕІ (анг) лекції -48, лаб. роб. 48; 2.ОБ'ЄКТНО-ОРІЄНТОВАНЕ ПРОГРАМУВАННЯ 121 ПІГ (англ.) Лекції - 24, лаб. роб. 24. П. 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, Паралімпійських 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 1. Керівництво студентом переможцем 1 етапу Всеукраїнського конкурсу студентських наукових робіт за напрямом Кібербезпека (шифр "Безпека ключів", Назарько О.М.) П. 19 діяльність за спеціальністю у формі участі у професійних та/або громадських об'єднаннях член Громадської організації

							“СХІДНОЄВРОПЕЙСЬКЕ НАУКОВЕ ТОВАРИСТВО” посвідчення №ES 062 від 20.05.2022р.
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	16	Інноваційне підприємництво та управління стартап проектами	Підвищення кваліфікації : Центр підтримки академій Cisco Національний технічний університет “Харківський політехнічний інститут”. Сертифікат від “30” червня 2021 р. 6 кредитів. Тема: “CCNA CyberOps” та “Network Security” Пункти відповідності ліцензійних умов: П 1, 2, 4, 8, 12, 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. Khvostenko V. S. Financial and commercial aspect of the technology transfer process / V. S. Khvostenko, M. A. Kipa, I. I. Aleksieienko // Financial and credit activity: problems of theory and practice. – 2019. – № 1(28). – Vol. 1. – P. 430-440. Режим доступу: http://fkd1.ubs.edu.ua/article/view/163934 (фахове, категорія А) (Web of Science Core Collection) 0,9 ум.друк.арк./власний внесок 0,3 авторських аркушів. 2. Khvostenko V. S. Development of methodological foundations for designing a classifier of threats to cyberphysical systems / O. Shmatko, S. Balakireva, A. Vlasov, N. Zagorodna, O. Korol, O. Milov, O. Petrov, S. Pohasii, Kh. Rzayev, V. Khvostenko// Eastern-European Journal of Enterprise Technologies – 2020. - № 3/9 (105). – P. 6 – 19. Режим доступу: http://journals.uran.ua/eejet/article/view/205702/206727 (фахове, категорія А) (Scopus). 0,87 ум.друк.арк./власний внесок 0,08 авторських аркушів. 3. Khvostenko V. S.

							Development of the classification of the cyber security agents bounded rationality/ O. Milov, O. Korol/ Системи управління, навігації та зв'язку, 2019, випуск 4(56), С. 82 – 86. Режим доступу: http://www.repository.hneu.edu.ua/jspui/bitstream/123456789/22709/1/Milov%20O.%20A%20Development%20of%20the%20classification%20of%20the%20cyber%20security%20agents%20bounded%20rationality.pdf (фахове, категорія Б) 0,625 ум.друк.арк./власний внесок 0,208 авторських аркушів. 4.Хвостенко В. С. Розробка комплексного показника якості обслуговування на основі постквантових алгоритмів/ Євсеєв С. П., Хвостенко В. С., Бондаренко К. О.// Системи управління, навігації та зв'язку. Вип. 3(65). Полтава : НУ "ПП", 2021. С 82-88. (фахове, категорія Б). 0,8 ум.друк.арк./власний внесок 0,3 авторських аркушів. 5. Khvostenko V. DEVELOPMENT OF A PROTOCOL FOR A CLOSED MOBILE INTERNET CHANNEL BASED ON POST-QUANTUM ALGORITHMS/ Serhii Yevseiev, Serhii Pohasii, Vladyslav Khvostenko// Системи обробки інформації №3(166), стор. 35-41, DOI:10.30748/soi.2021.166.03. (фахове, категорія Б) 0,7 ум.друк.арк./власний внесок 0,2 авторських аркушів. 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 Свідоцтва про реєстрацію авторського права на твір: 1. Фундаментальне наукове дослідження «Technology transfer»

							№ 77581 від 14.03.2018. 2. Теоретико методичні підходи до визначення поняття "трансфер технологій" № 81831 від 27.09.2018 (співавтор - Литовченко І.В.). 3. Internet trading market in Ukraine: stock exchanges, brokers and brokerage trading systems № 85208 від 01.02.2019. 4. Організаційні аспекти інтеграції локального підприємства у франчайзингову мережу №80214 від 12.07.2018. Патенти на корисну модель: 1. Патент на винахід (корисну модель) u 2021 03726 від 30.06.2021 СПОСІБ КРИПТОГРАФІЧНОГО ПЕРЕТВОРЕННЯ ІНФОРМАЦІЇ 2. Патент на винахід (корисну модель) u 2021 03704 від 29.06.2021 СПОСІБ КРИПТОГРАФІЧНОГО ПЕРЕТВОРЕННЯ ІНФОРМАЦІЇ 3. Патент на винахід (корисну модель) u 2021 03665 від 25.06.2021 СПОСІБ КРИПТОГРАФІЧНОГО ПЕРЕТВОРЕННЯ ІНФОРМАЦІЇ 4. Патент на винахід (корисну модель) u 2021 03617 від 23.06.2021 СПОСІБ КРИПТОГРАФІЧНОГО ПЕРЕТВОРЕННЯ ІНФОРМАЦІЇ 5. Патент на винахід (корисну модель) u 2021 03615 від 23.06.2021 СПОСІБ КРИПТОГРАФІЧНОГО ПЕРЕТВОРЕННЯ ІНФОРМАЦІЇ 6. Патент на винахід (корисну модель) u 2021 03683 від 23.07.2021 СПОСІБ КРИПТОГРАФІЧНОГО ПЕРЕТВОРЕННЯ ІНФОРМАЦІЇ 7. Патент на винахід (корисну модель) u 2021 03680 від 25.06.2021 СПОСІБ КРИПТОГРАФІЧНОГО ПЕРЕТВОРЕННЯ ІНФОРМАЦІЇ П. 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. Інтелектуальна власність: робоча програма навчальної дисципліни для студентів усіх спеціальностей першого (бакалаврського) рівня [Електронне видання] / укл. В. С. Хвостенко – Харків : Вид. ХНЕУ ім. С. Кузнеця, 2020. (Укр. мов.) Режим доступу: https://pns.hneu.edu.ua/course/view.php?id=5616. 2. Інтелектуальна власність: робоча програма навчальної дисципліни для студентів спеціальності 186 Видавництво та поліграфія першого (бакалаврського) рівня [Електронне видання] / укл. В. С. Хвостенко – Харків : Вид. ХНЕУ ім. С. Кузнеця, 2020. (Укр. мов.) Режим доступу: https://pns.hneu.edu.ua/course/view.php?id=5616 3. Господарське право: робоча програма навчальної дисципліни для студентів спеціальності 125 Кібербезпека другого (магістерського) рівня [Електронне видання] / укл. В. С. Хвостенко – Харків : Вид. ХНЕУ ім. С. Кузнеця, 2020. (Укр. мов.) Режим доступу: https://pns.hneu.edu.ua/course/view.php?id=7222 4. Захист інтелектуальної власності: робоча програма навчальної дисципліни для студентів спеціальності 125 Кібербезпека другого (магістерського) рівня [Електронне видання] / укл. В. С. Хвостенко – Харків : Вид. ХНЕУ ім. С. Кузнеця, 2020. – (Укр. мов.) Режим доступу:

							https://pns.hneu.edu.ua/course/view.php?id=7211 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 №376-46 від 18.11.2021 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. Хвостенко В.С. Європейська реформа, як засіб Балансу суб'єктів авторського права /В.В. Воліков, В. С. Хвостенко //Матеріали міжнародної науково-практичної інтернет-конференції «Управляння проектами. Ефективне використання результатів наукових досліджень та об'єктів інтелектуальної власності»): збірник матеріалів (м. Київ, 21 березня 2019 р.) / НДІ інтелектуальної власності НАПрН України. – К.: ФО-П Кравченко Я.О., 2019. – С.36-38. Власний внесок 0,1 авторських аркушів. Режим доступу: https://bit.ly/3mKqt5h Дата звернення 05.10.2021 2. Khvostenko V. S. Leaders in the on-line trading market in Ukraine: stock exchanges, brokers, and brokerage trading systems/ V. Khvostenko, Y. Tkachenko, S.

							Kuzmenko // Advances in Social Science, Education and Humanities Research, volume 318. - May 2019. с. 410-415. Власний внесок 0,1 авторських аркушів. Режим доступу: https://www.atlantis-press.com/proceedings/icseal-19/125909068 Дата звернення 05.10.2021 3. Хвостенко В.С. Моделювання інтегральної оцінки ефективності формування фінансової стратегії підприємства / В. С. Хвостенко, Чуйко Б. В. // Науково-практичний журнал «Регіональна економіка та управління» 4 (17), жовтень 2017. С. 105-108. Власний внесок 0,1 авторських аркушів. Режим доступу: http://ir.nusta.edu.ua/jspui/bitstream/123456789/2383/1/2549_IR.pdf Дата звернення 05.10.2021 4. Хвостенко В.С. Фірмове найменування, відоме в Україні / В. С. Хвостенко, Д. А. Григорова // «International Scientific Conference From the Baltic to the Black Sea: the Formation of Modern Economic Area» – Conference Proceedings, August 19th, 2017.Riga, Latvia. – Baltija Publishing, 2017. – С. 185-187. Власний внесок 0,075 авторських аркушів. Режим доступу: https://bit.ly/3BsKhzS Дата звернення 05.10.2021 5. Хвостенко В.С. Державне регулювання процесу комерціалізації об'єктів інтелектуальної власності. /В.В. Воліков, В. С. Хвостенко // Всеукраїнський семінар з проблем економіки інтелектуальної власності»: збірник наукових праць II Всеукраїнської науково-практичної конференції, м. Київ, 24 травня 2019 р. - К.: ФОП Кравченко Я.О.,

							2019. – С.96-102. Власний внесок 0,175 авторських аркушів. Режим доступу: https://bit.ly/3mKqt5h Дата звернення 05.10.2021 6. Khvostenko V. Synergy of building cybersecurity systems: monograph / 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. – Kharkiv: PC TECHNOLOGY CENTER, 2021. – 188 p. Режим доступу : http://www.repository.hneu.edu.ua/jspui/handle/123456789/25623. – Назва з тит. екрана. – ISBN 978-617-7319-31-2 (on-line); ISBN 978-617-7319-32-9 (print). Власний внесок 0,47 авторських аркушів. 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", свідотство ES № 063 П. 20 досвід практичної роботи за спеціальністю не менше п'яти років (крім педагогічної, науково-педагогічної, наукової діяльності) – Спеціаліст I категорії розрахункової палати УДКУ у Харківській обл. 13 ранг 6 категорії державного службовця 12.01.2005-18.09.2009. – директор, ТОВ АТІЛОГ (ЄДРПОУ: 35974114) з 2008, ІТ

							компанія. https://youcontrol.com.ua/catalog/company_details/35974114/
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	16	Господарське право	Підвищення кваліфікації : Центр підтримки академій Cisco Національний технічний університет "Харківський політехнічний інститут". Сертифікат від "30" червня 2021 р. 6 кредитів. Тема: "CCNA CyberOps" та "Network Security" Пункти відповідності ліцензійних умов: П 1, 2, 4, 8, 12, 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. Khvostenko V. S. Financial and commercial aspect of the technology transfer process / V. S. Khvostenko, M. A. Kipa, I. I. Aleksieienko // Financial and credit activity: problems of theory and practice. – 2019. – № 1(28). – Vol. 1. – P. 430-440. Режим доступу: http://fkd1.ubs.edu.ua/article/view/163934 (фахове, категорія А) (Web of Science Core Collection) 0,9 ум.друк.арк./власний внесок 0,3 авторських аркушів. 2. Khvostenko V. S. Development of methodological foundations for designing a classifier of threats to cyberphysical systems / O. Shmatko, S. Balakireva, A. Vlasov, N. Zagorodna, O. Korol, O. Milov, O. Petrov, S. Pohasii, Kh. Rzayev, V. Khvostenko// Eastern-European Journal of Enterprise Technologies – 2020. - № 3/9 (105). – P. 6 – 19. Режим доступу: http://journals.uran.ua/eejet/article/view/205702/206727 (фахове, категорія А) (Scopus). 0,87 ум.друк.арк./власний внесок 0,08 авторських аркушів. 3. Khvostenko V. S. Development of the classification of the

							cyber security agents bounded rationality/ O. Milov, O. Korol/ Системи управління, навігації та зв'язку, 2019, випуск 4(56), С. 82 – 86. Режим доступу: http://www.repository.hneu.edu.ua/jspui/bitstream/123456789/22709/1/Milov%20O.%20A%20Development%20of%20the%20classification%20of%20the%20cyber%20security%20agents%20bounded%20rationality.pdf (фахове, категорія Б) 0,625 ум.друк.арк./власний внесок 0,208 авторських аркушів. 4.Хвостенко В. С. Розробка комплексного показника якості обслуговування на основі постквантових алгоритмів/ Євсеєв С. П., Хвостенко В. С., Бондаренко К. О.// Системи управління, навігації та зв'язку. Вип. 3(65). Полтава : НУ "ПП", 2021. С 82-88. (фахове, категорія Б). 0,8 ум.друк.арк./власний внесок 0,3 авторських аркушів. 5. Khvostenko V. DEVELOPMENT OF A PROTOCOL FOR A CLOSED MOBILE INTERNET CHANNEL BASED ON POST-QUANTUM ALGORITHMS/ Serhii Yevseiev, Serhii Pohasii, Vladyslav Khvostenko// Системи обробки інформації №3(166), стор. 35-41, DOI:10.30748/soi.2021.166.03. (фахове, категорія Б) 0,7 ум.друк.арк./власний внесок 0,2 авторських аркушів. 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 Свідоцтва про реєстрацію авторського права на твір: 1. Фундаментальне наукове дослідження «Technology transfer» № 77581 від 14.03.2018.

							2. Теоретико методичні підходи до визначення поняття "трансфер технологій" № 81831 від 27.09.2018 (співавтор - Литовченко І.В.). 3. Internet trading market in Ukraine: stock exchanges, brokers and brokerage trading systems № 85208 від 01.02.2019. 4. Організаційні аспекти інтеграції локального підприємства у франчайзингову мережу №80214 від 12.07.2018. Патенти на корисну модель: 1. Патент на винахід (корисну модель) u 2021 03726 від 30.06.2021 СПОСІБ КРИПТОГРАФІЧНОГО ПЕРЕТВОРЕННЯ ІНФОРМАЦІЇ 2. Патент на винахід (корисну модель) u 2021 03704 від 29.06.2021 СПОСІБ КРИПТОГРАФІЧНОГО ПЕРЕТВОРЕННЯ ІНФОРМАЦІЇ 3. Патент на винахід (корисну модель) u 2021 03665 від 25.06.2021 СПОСІБ КРИПТОГРАФІЧНОГО ПЕРЕТВОРЕННЯ ІНФОРМАЦІЇ 4. Патент на винахід (корисну модель) u 2021 03617 від 23.06.2021 СПОСІБ КРИПТОГРАФІЧНОГО ПЕРЕТВОРЕННЯ ІНФОРМАЦІЇ 5. Патент на винахід (корисну модель) u 2021 03615 від 23.06.2021 СПОСІБ КРИПТОГРАФІЧНОГО ПЕРЕТВОРЕННЯ ІНФОРМАЦІЇ 6. Патент на винахід (корисну модель) u 2021 03683 від 23.07.2021 СПОСІБ КРИПТОГРАФІЧНОГО ПЕРЕТВОРЕННЯ ІНФОРМАЦІЇ 7. Патент на винахід (корисну модель) u 2021 03680 від 25.06.2021 СПОСІБ КРИПТОГРАФІЧНОГО ПЕРЕТВОРЕННЯ ІНФОРМАЦІЇ П. 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. Інтелектуальна власність: робоча програма навчальної дисципліни для студентів усіх спеціальностей першого (бакалаврського) рівня [Електронне видання] / укл. В. С. Хвостенко – Харків : Вид. ХНЕУ ім. С. Кузнеця, 2020. (Укр. мов.) Режим доступу: https://pns.hneu.edu.ua/course/view.php?id=5616. 2. Інтелектуальна власність: робоча програма навчальної дисципліни для студентів спеціальності 186 Видавництво та поліграфія першого (бакалаврського) рівня [Електронне видання] / укл. В. С. Хвостенко – Харків : Вид. ХНЕУ ім. С. Кузнеця, 2020. (Укр. мов.) Режим доступу: https://pns.hneu.edu.ua/course/view.php?id=5616 3. Господарське право: робоча програма навчальної дисципліни для студентів спеціальності 125 Кібербезпека другого (магістерського) рівня [Електронне видання] / укл. В. С. Хвостенко – Харків : Вид. ХНЕУ ім. С. Кузнеця, 2020. (Укр. мов.) Режим доступу: https://pns.hneu.edu.ua/course/view.php?id=7222 4. Захист інтелектуальної власності: робоча програма навчальної дисципліни для студентів спеціальності 125 Кібербезпека другого (магістерського) рівня [Електронне видання] / укл. В. С. Хвостенко – Харків : Вид. ХНЕУ ім. С. Кузнеця, 2020. – (Укр. мов.) Режим доступу: https://pns.hneu.edu.ua/course/view.php?

							id=7211 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 №376-46 від 18.11.2021 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. Хвостенко В.С. Європейська реформа, як засіб Балансу суб'єктів авторського права /В.В. Воліков, В. С. Хвостенко //Матеріали міжнародної науково-практичної інтернет-конференції «Управляння проектами. Ефективне використання результатів наукових досліджень та об'єктів інтелектуальної власності»): збірник матеріалів (м. Київ, 21 березня 2019 р.) / НДІ інтелектуальної власності НАПрН України. – К.: ФО-П Кравченко Я.О., 2019. – С.36-38. Власний внесок 0,1 авторських аркушів. Режим доступу: https://bit.ly/3mKqt5h Дата звернення 05.10.2021 2. Khvostenko V. S. Leaders in the on-line trading market in Ukraine: stock exchanges, brokers, and brokerage trading systems/ V. Khvostenko, Y. Tkachenko, S. Kuzmenko // Advances in Social Science,

							Education and Humanities Research, volume 318. - May 2019. с. 410-415. Власний внесок 0,1 авторських аркушів. Режим доступу: https://www.atlantis-press.com/proceedings/icseal-19/125909068 Дата звернення 05.10.2021 3. Хвостенко В.С. Моделювання інтегральної оцінки ефективності формування фінансової стратегії підприємства / В. С. Хвостенко, Чуйко Б. В. // Науково-практичний журнал «Регіональна економіка та управління» 4 (17), жовтень 2017. С. 105-108. Власний внесок 0,1 авторських аркушів. Режим доступу: http://ir.nusta.edu.ua/jspui/bitstream/123456789/2383/1/2549_IR.pdf Дата звернення 05.10.2021 4. Хвостенко В.С. Фірмове найменування, відоме в Україні / В. С. Хвостенко, Д. А. Григорова // «International Scientific Conference From the Baltic to the Black Sea: the Formation of Modern Economic Area» – Conference Proceedings, August 19th, 2017.Riga, Latvia. – Baltija Publishing, 2017. – С. 185-187. Власний внесок 0,075 авторських аркушів. Режим доступу: https://bit.ly/3BsKhzS Дата звернення 05.10.2021 5. Хвостенко В.С. Державне регулювання процесу комерціалізації об'єктів інтелектуальної власності. /В.В. Воліков, В. С. Хвостенко // Всеукраїнський семінар з проблем економіки інтелектуальної власності»: збірник наукових праць II Всеукраїнської науково-практичної конференції, м. Київ, 24 травня 2019 р. - К.: ФОП Кравченко Я.О., 2019. – С.96-102. Власний внесок 0,175

							авторських аркушів. Режим доступу: https://bit.ly/3mKqt5h Дата звернення 05.10.2021 6. Khvostenko V. Synergy of building cybersecurity systems: monograph / 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. – Kharkiv: PC TECHNOLOGY CENTER, 2021. – 188 p. Режим доступу : http://www.repository.hneu.edu.ua/jspui/handle/123456789/25623. – Назва з тит. екрана. – ISBN 978-617-7319-31-2 (on-line); ISBN 978-617-7319-32-9 (print). Власний внесок 0,47 авторських аркушів. 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", свідотство ES № 063 П. 20 досвід практичної роботи за спеціальністю не менше п'яти років (крім педагогічної, науково-педагогічної, наукової діяльності) – Спеціаліст I категорії розрахункової палати УДКУ у Харківській обл. 13 ранг 6 категорії державного службовця 12.01.2005-18.09.2009. – директор, ТОВ АТІЛОГ (ЄДРПОУ: 35974114) з 2008, IT компанія. https://youcontrol.com.

							ua/catalog/company_details/35974114/
410245	Погасій Сергій Сергійович	Доцент, 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 кандидата наук ДК 051003, виданий 28.04.2009, Атестат доцента АД 006046, виданий 26.11.2020	19	Веб-безпека	Підвищення кваліфікації: 1). МОН України НТУ "ХПІ" (Свідоцтво ПК 36627007/100008-20 від 28.01.2020 р.) 6 кредитів. Тема: "Комп'ютерні системи та мережі". 2) магістр з кібербезпеки. 31.12.2021 р. диплом М21 №089409. Пункти відповідності ліцензійних умов: П. 1, 2, 4, 8, 10, 12, 14, 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. S. Pohasii. Development and analysis of game-theoretical models of security systems agents interaction / S. Yevseiev, O. Milov, S. Milevskyi, O. Voitko, M. Kasianenko, Y. Melenti, S. Pohasii, H. Stepanov, O. Turinskyi, S. Faraon./ Eastern-European Journal of Enterprise Technologies ISSN 1729-3774 2/4 (104) 2020 (p. 15–29) Режим доступу: http://journals.uran.ua/eejet/article/view/201418/201883 (фахове, категорія А) (Scopus) 0.8 ум.друк.арк./власний внесок 0.08 авторських аркушів. 2. S. Pohasii. Development of methodological foundations for designing a classifier of threats to cyberphysical systems / O. Shmatko, S. Balakireva, A. Vlasov, N. Zagorodna, O. Korol, O. Milov, O. Petrov, S. Pohasii, Kh. Rzayev, V. Khvostenko/ Eastern-European Journal of Enterprise Technologies ISSN 1729-3774 3/9 (105) 2020 (p. 6–19) Режим доступу: http://journals.uran.ua/eejet/article/view/205702/206727 (фахове, категорія А) (Scopus) 0.65

							ум.друк.арк./власний внесок 0.06 авторських аркушів. 3. S. Pohasii. Procedural basis of cybersecurity systems. / Milov O., Milevskyi S., Pohasii S., Rzayev K. /Системи управління, навігації та зв'язку. Полтава : ПНТУ, 2019. Вип. 5(57). С. 81-86. Режим доступу: 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=suntz_2019_5_18 (фахове, категорія Б) 0.26 ум.друк.арк./власний внесок 0.06 авторських аркушів. 4. S. Pohasii. Verification of the security systems antagonistic agents behavior model./ O. Milov, L. Parkhuts, S. Milevskyi, S. Pohasii/ Системи обробки інформації. — 2019. — № 4(159). – С. 65-81. Режим доступу: https://www.researchgate.net/publication/338510968_Verification_of_the_security_systems_antagonistic_agents_behavior_model (фахове, категорія Б) 0.8 ум.друк.арк./власний внесок 0.2 авторських аркушів. 5. S. Pohasii. JS Security Using Cryptographic Hash Functions./I. R. Ragimova, F. A. Gubadova, B. A. Asker-zade, S. S. Pohasii./ Сучасні інформаційні системи. 2019. Т. 3, № 4 р 105-108. Режим доступу: http://repository.kpi.kharkov.ua/handle/KhPI-Press/43617 (фахове, категорія Б) 0.15 ум.друк.арк./власний внесок 0.04 авторських аркушів. 6. Edited by Serhii Yevseiev, Volodymir Ponomarenko, Oleksandr Laptiev, Oleksandr Milov. Synergy of building cybersecurity systems: monograph / S. Yevseiev, V. Ponomarenko, O. Laptiev, O. Milov and others. – Kharkiv: PC

							TECHNOLOGY CENTER, 2021. – 188 p. (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. Патент на винахід (корисну модель) u 2021 03726 від 30.06.2021 СПОСІБ КРИПТОГРАФІЧНОГО ПЕРЕТВОРЕННЯ ІНФОРМАЦІЇ 2. Патент на винахід (корисну модель) u 2021 03704 від 29.06.2021 СПОСІБ КРИПТОГРАФІЧНОГО ПЕРЕТВОРЕННЯ ІНФОРМАЦІЇ 3. Патент на винахід (корисну модель) u 2021 03665 від 25.06.2021 СПОСІБ КРИПТОГРАФІЧНОГО ПЕРЕТВОРЕННЯ ІНФОРМАЦІЇ 4. Патент на винахід (корисну модель) u 2021 03683 від 23.07.2021 СПОСІБ КРИПТОГРАФІЧНОГО ПЕРЕТВОРЕННЯ ІНФОРМАЦІЇ 5. Патент на винахід (корисну модель) u 2021 03680 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. Основи ІТ: робоча програма навчальної дисципліни для студентів усіх спеціальностей першого (бакалаврського) рівня [Електронне видання] / укл. Р. В. Корольов, С. С.

							Погасій. – Харків : ХНЕУ ім. С. Кузнеця, 2020. – 11 с. Режим доступу http://www.repository.hneu.edu.ua/handle/123456789/24055 2. Безпека інтернет-речей: робоча програма навчальної дисципліни для студентів спеціальності 125 “Кібербезпека” першого (бакалаврського) рівня [Електронне видання] / укл. С. С. Погасій. – Х. : Вид. ХНЕУ ім. С. Кузнеця, 2019. – 11 с. (Укр. мов.). Режим доступу http://www.repository.hneu.edu.ua/handle/123456789/23322 3.Основи побудови та функціонування мікропроцесорних систем: робоча програма навчальної дисципліни для студентів спеціальності 125 “Кібербезпека” першого (бакалаврського) рівня [Електронне видання] / укл. С. С. Погасій. – Х. : Вид. ХНЕУ ім. С. Кузнеця, 2019. – 10 с. (Укр. мов.) Режим доступу http://www.repository.hneu.edu.ua/handle/123456789/23314 4.Системи виявлення та протидія атакам: робоча програма навчальної дисципліни для студентів спеціальності 125 “Кібербезпека” першого (бакалаврського) рівня [Електронне видання] / укл. С. С. Погасій. – Х. : Вид. ХНЕУ ім. С. Кузнеця, 2019. – 9 с. (Укр. мов.) Режим доступу http://www.repository.hneu.edu.ua/handle/123456789/23313 5. Захист систем електронної комерції та мультисервісних систем: робоча програма навчальної дисципліни для студентів спеціальності 125 “Кібербезпека” першого (бакалаврського) рівня [Електронне видання] / укл. С. С. Погасій. – Х. : Вид. ХНЕУ ім. С. Кузнеця, 2019. – 8 с. (Укр. мов.). Режим доступу

							http://www.repository.hneu.edu.ua/handle/123456789/23312 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 Керівник госпдоговірної НДР №376-46 від 18.11.2021 р. 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. Pohasii S., Milov O., Milevskyi S., Rzayev K. Procedural basis of cybersecurity systems. Системи управління, навігації та зв'язку. Полтава : ПНТУ, 2019. Вип. 5(57). С. 81-86. (0,25 ум. др. арк. / 0,06 ум. друк. арк. власного внеску) 2. S. Pohasii., O. Milov, L. Parkhuts, S. Milevskyi. Verification of the security systems antagonistic agents behavior model. Системи обробки інформації. — 2019. — № 4(159). – С. 65-81.

							(0,8 ум. др. арк. / 0,2 ум. друк. арк. власного внеску) 3. S. S. Pohasii.,I. R. Ragimova, F. A. Gubadova, B. A. Asker-zade, JS Security Using Cryptographic Hash Functions. Сучасні інформаційні системи. 2019. Т. 3, № 4 р 105-108. (0,16 ум. др. арк. / 0,04 ум. друк. арк. власного внеску) 4. S. Pohasii, S. Yevseiev, O. Milov, S. Milevskyi, O. Voitko, M. Kasianenko, Y. Melenti, H. Stepanov, O. Turinskyi, S. Faraon. Development and analysis of game-theoretical models of security systems agents interaction Eastern-European Journal of Enterprise Technologies ISSN 1729-3774 2/4 (104) 2020(p. 15–29) (0,8 ум. др. арк. / 0,07 ум. друк. арк. власного внеску) 5. S. Pohasii . Synergy of building cybersecurity systems: monograph / S.Yevseiev, V. Ponomarenko, O. Laptiev, O. Milov, O. Korol, S. Milevskyi, 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.Khvostenko, V. Sobchuk, G. Shuklin, V. Khvostenko, O. Tymochko, M. Pavlenko, A.Trystan, S.Florov. – Kharkiv: PC TECHNOLOGY CENTER, 2021. – 188 p. Режим доступу : http://www.repository.hneu.edu.ua/jspui/handle/123456789/25623. – Назва з тит. екрана. – ISBN 978-617-7319-31-2 (on-line); ISBN 978-617-7319-32-9 (print). Власний внесок 0,47 авторських аркушів. П. 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, Паралімпійських 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 Суддя у складі журі з компетенції «Мобільна робототехніка» (Junior):I (відбіркового) етапу Всеукраїнського конкурсу професійної майстерності «WorldSkills Ukraine» у 2021 році. Наказ Департаменту Науки і освіти від 28 серпня 2021 року № 112 «Про організацію та проведення І етапу Всеукраїнського конкурсу професійної майстерності «WorldSkills Ukraine» у 2021 році» Режим доступу https://drive.google.com/file/d/1bjtYbubJoVA66EhjL8JYSrtFlN-Nw2FB/view?usp=sharing П. 19 діяльність за спеціальністю у формі участі у професійних та/або громадських об'єднаннях Засновник Громадської організації "Association of STEM researchers and inventors" Член громадської організації "Східноєвропейське наукове товариство", свідотство ES № 061 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.
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	16	Захист інтелектуальної власності	Підвищення кваліфікації : Центр підтримки академій Cisco Національний технічний університет "Харківський політехнічний інститут". Сертифікат від "30" червня 2021 р.

				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			6 кредитів. Тема: “CCNA CyberOps” та “Network Security” Пункти відповідності ліцензійних умов: П 1, 2, 4, 8, 12, 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. Khvostenko V. S. Financial and commercial aspect of the technology transfer process / V. S. Khvostenko, M. A. Kipa, I. I. Aleksieienko // Financial and credit activity: problems of theory and practice. – 2019. – № 1(28). – Vol. 1. – P. 430-440. Режим доступу: http://fkd1.ubs.edu.ua/article/view/163934 (фахове, категорія А) (Web of Science Core Collection) 0,9 ум.друк.арк./власний внесок 0,3 авторських аркушів. 2. Khvostenko V. S. Development of methodological foundations for designing a classifier of threats to cyberphysical systems / O. Shmatko, S. Balakireva, A. Vlasov, N. Zagorodna, O. Korol, O. Milov, O. Petrov, S. Pohasii, Kh. Rzayev, V. Khvostenko// Eastern-European Journal of Enterprise Technologies – 2020. - № 3/9 (105). – P. 6 – 19. Режим доступу: http://journals.uran.ua/eejet/article/view/205702/206727 (фахове, категорія А) (Scopus). 0,87 ум.друк.арк./власний внесок 0,08 авторських аркушів. 3. Khvostenko V. S. Development of the classification of the cyber security agents bounded rationality/ O. Milov, O. Korol/ Системи управління, навігації та зв'язку, 2019, випуск 4(56), С. 82 – 86. Режим доступу: http://www.repository.hneu.edu.ua/jspui/bitstream/123456789/22709/1/Milov%20O.%20A%20Development%20of%20the%20classification%

							20of%20the%20cyber%20security%20agents%20bounded%20rationality.pdf (фахове, категорія Б) 0,625 ум.друк.арк./власний внесок 0,208 авторських аркушів. 4.Хвостенко В. С. Розробка комплексного показника якості обслуговування на основі постквантових алгоритмів/ Євсеєв С. П., Хвостенко В. С., Бондаренко К. О.// Системи управління, навігації та зв'язку. Вип. 3(65). Полтава : НУ "ПП", 2021. С 82-88. (фахове, категорія Б). 0,8 ум.друк.арк./власний внесок 0,3 авторських аркушів. 5. Khvostenko V. DEVELOPMENT OF A PROTOCOL FOR A CLOSED MOBILE INTERNET CHANNEL BASED ON POST-QUANTUM ALGORITHMS/ Serhii Yevseiev, Serhii Pohasii, Vladyslav Khvostenko// Системи обробки інформації №3(166), стор. 35-41, DOI:10.30748/soi.2021.166.03. (фахове, категорія Б) 0,7 ум.друк.арк./власний внесок 0,2 авторських аркушів. 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 Свідоцтва про реєстрацію авторського права на твір: 1. Фундаментальне наукове дослідження «Technology transfer» № 77581 від 14.03.2018. 2. Теоретико методичні підходи до визначення поняття "трансфер технологій" № 81831 від 27.09.2018 (співавтор - Литовченко І.В.). 3. Internet trading market in Ukraine: stock exchanges, brokers and brokerage trading systems № 85208 від 01.02.2019. 4. Організаційні

							аспекти інтеграції локального підприємства у франчайзингову мережу №80214 від 12.07.2018. Патенти на корисну модель: 1. Патент на винахід (корисну модель) u 2021 03726 від 30.06.2021 СПОСІБ КРИПТОГРАФІЧНОГО ПЕРЕТВОРЕННЯ ІНФОРМАЦІЇ 2. Патент на винахід (корисну модель) u 2021 03704 від 29.06.2021 СПОСІБ КРИПТОГРАФІЧНОГО ПЕРЕТВОРЕННЯ ІНФОРМАЦІЇ 3. Патент на винахід (корисну модель) u 2021 03665 від 25.06.2021 СПОСІБ КРИПТОГРАФІЧНОГО ПЕРЕТВОРЕННЯ ІНФОРМАЦІЇ 4. Патент на винахід (корисну модель) u 2021 03617 від 23.06.2021 СПОСІБ КРИПТОГРАФІЧНОГО ПЕРЕТВОРЕННЯ ІНФОРМАЦІЇ 5. Патент на винахід (корисну модель) u 2021 03615 від 23.06.2021 СПОСІБ КРИПТОГРАФІЧНОГО ПЕРЕТВОРЕННЯ ІНФОРМАЦІЇ 6. Патент на винахід (корисну модель) u 2021 03683 від 23.07.2021 СПОСІБ КРИПТОГРАФІЧНОГО ПЕРЕТВОРЕННЯ ІНФОРМАЦІЇ 7. Патент на винахід (корисну модель) u 2021 03680 від 25.06.2021 СПОСІБ КРИПТОГРАФІЧНОГО ПЕРЕТВОРЕННЯ ІНФОРМАЦІЇ П. 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. Інтелектуальна власність: робоча

							програма навчальної дисципліни для студентів усіх спеціальностей першого (бакалаврського) рівня [Електронне видання] / укл. В. С. Хвостенко – Харків : Вид. ХНЕУ ім. С. Кузнеця, 2020. (Укр. мов.) Режим доступу: https://pns.hneu.edu.ua/course/view.php?id=5616. 2. Інтелектуальна власність: робоча програма навчальної дисципліни для студентів спеціальності 186 Видавництво та поліграфія першого (бакалаврського) рівня [Електронне видання] / укл. В. С. Хвостенко – Харків : Вид. ХНЕУ ім. С. Кузнеця, 2020. (Укр. мов.) Режим доступу: https://pns.hneu.edu.ua/course/view.php?id=5616 3. Господарське право: робоча програма навчальної дисципліни для студентів спеціальності 125 Кібербезпека другого (магістерського) рівня [Електронне видання] / укл. В. С. Хвостенко – Харків : Вид. ХНЕУ ім. С. Кузнеця, 2020. (Укр. мов.) Режим доступу: https://pns.hneu.edu.ua/course/view.php?id=7222 4. Захист інтелектуальної власності: робоча програма навчальної дисципліни для студентів спеціальності 125 Кібербезпека другого (магістерського) рівня [Електронне видання] / укл. В. С. Хвостенко – Харків : Вид. ХНЕУ ім. С. Кузнеця, 2020. – (Укр. мов.) Режим доступу: https://pns.hneu.edu.ua/course/view.php?id=7211 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 №376-46 від 18.11.2021 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. Хвостенко В.С. Європейська реформа, як засіб Балансу суб'єктів авторського права /В.В. Воліков, В. С. Хвостенко //Матеріали міжнародної науково-практичної інтернет-конференції «Управляння проектами. Ефективне використання результатів наукових досліджень та об'єктів інтелектуальної власності»): збірник матеріалів (м. Київ, 21 березня 2019 р.) / НДІ інтелектуальної власності НАПрН України. – К.: ФО-П Кравченко Я.О., 2019. – С.36-38. Власний внесок 0,1 авторських аркушів. Режим доступу: https://bit.ly/3mKqt5h Дата звернення 05.10.2021 2. Khvostenko V. S. Leaders in the on-line trading market in Ukraine: stock exchanges, brokers, and brokerage trading systems/ V. Khvostenko, Y. Tkachenko, S. Kuzmenko // Advances in Social Science, Education and Humanities Research, volume 318. - May 2019. c. 410-415. Власний внесок 0,1 авторських аркушів. Режим доступу: https://www.atlantis-press.com/proceedings/icseal-19/125909068 Дата звернення 05.10.2021 3. Хвостенко В.С. Моделювання

							інтегральної оцінки ефективності формування фінансової стратегії підприємства / В. С. Хвостенко, Чуйко Б. В. // Науково-практичний журнал «Регіональна економіка та управління» 4 (17), жовтень 2017. С. 105-108. Власний внесок 0,1 авторських аркушів. Режим доступу: http://ir.nusta.edu.ua/jspui/bitstream/123456789/2383/1/2549_IR.pdf Дата звернення 05.10.2021 4. Хвостенко В.С. Фірмове найменування, відоме в Україні / В. С. Хвостенко, Д. А. Григорова // «International Scientific Conference From the Baltic to the Black Sea: the Formation of Modern Economic Area» – Conference Proceedings, August 19th, 2017.Riga, Latvia. – Baltija Publishing, 2017. – С. 185-187. Власний внесок 0,075 авторських аркушів. Режим доступу: https://bit.ly/3BsKhzS Дата звернення 05.10.2021 5. Хвостенко В.С. Державне регулювання процесу комерціалізації об'єктів інтелектуальної власності. /В.В. Воліков, В. С. Хвостенко // Всеукраїнський семінар з проблем економіки інтелектуальної власності»: збірник наукових праць II Всеукраїнської науково-практичної конференції, м. Київ, 24 травня 2019 р. - К.: ФОП Кравченко Я.О., 2019. – С.96-102. Власний внесок 0,175 авторських аркушів. Режим доступу: https://bit.ly/3mKqt5h Дата звернення 05.10.2021 6. Khvostenko V. Synergy of building cybersecurity systems: monograph / 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. – Kharkiv: PC TECHNOLOGY CENTER, 2021. – 188 p. Режим доступу : http://www.repository.hneu.edu.ua/jspui/handle/123456789/25623. – Назва з тит. екрана. – ISBN 978-617-7319-31-2 (on-line); ISBN 978-617-7319-32-9 (print). Власний внесок 0,47 авторських аркушів. 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", свідотство ES № 063 П. 20 досвід практичної роботи за спеціальністю не менше п'яти років (крім педагогічної, науково-педагогічної, наукової діяльності) – Спеціаліст І категорії розрахункової палати УДКУ у Харківській обл. 13 ранг 6 категорії державного службовця 12.01.2005-18.09.2009. – директор, ТОВ АТІЛОГ (ЄДРПОУ: 35974114) з 2008, ІТ компанія. https://youcontrol.com.ua/catalog/company_details/35974114/
410244	Мілевський Станіслав Валерійович	Доцент, Основне місце роботи	Навчально-науковий інститут комп'ютерних наук та інформаційних технологій	Диплом спеціаліста, Харківський державний економічний університет, рік закінчення: 2001, спеціальність: 0501 Економіка	21	Англійська мова	Підвищення кваліфікації: Міжнародний проект USAID "Кібербезпека критичної інфраструктури України" Сертифікат від "23" липня 2021 р. 3 кредити. Тема: "Аудит та ризик-менеджмент".

				підприємства, Диплом магістра, Національний авіаційний університет, рік закінчення: 2021, спеціальність: 125 Кібербезпека, 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			Пункти відповідності ліцензійних умов: П. 1, 2, 4, 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. Milov O. Development of the model of the antagonistic agents behavior under a cyber conflict / O. Milov, S. Yevseiev, Y. Ivanchenko, S. Milevskyi, O. Nesterov, O. Puchkov, A. Salii, O. Timochko, V. Tiurin, A. Yarovyi // Eastern-Europe Journal of Enterprise Technologies, 2019, v.4, № 9(100). P.6-19. - Access mode: http://journals.uran.ua/eejet/article/view/175978. (2.5 ум.друк.арк./власний внесок 0,25 авторських аркушів). 2. Havrylova A. Mathematical model of authentication of a transmitted message based on a McEliece scheme on shorted and extended modified elliptic codes using UMAC modified algorithm / Alla A. Havrylova, Olha H. Korol, Stanyslav V. Milevskyi, Lala R. Bakirova // "Кібербезпека: освіта, наука, техніка", 2019. – No 1(5). – P. 40 – 51. Acces mode: https://webcache.googleusercontent.com/search?q=cache:diuoPNu4g-cJ:https://www.csecurity.kubg.edu.ua/index.php/journal/article/download/102/105/+&cd=1&hl=ru&ct=clnk&gl=ua (0,6 ум. др. арк. / 0,15 ум. друк. арк. власного внеску). 3. Milov O. Development of the interacting agents behavior scenario in the cyber security system / O. Milov, S. Yevseiev, V. Aleksiyev, P. Berdnik, O. Voitko, V. Dyptan, Y. Ivanchenko, M. Pavlenko, A. Salii, S. Yarovyy // Eastern-European Journal of Enterprise

							Technologies. – 2019. – Vol. 5. – No. 9 (105). – P. 46–57. – Режим доступу: http://journals.uran.ua/eejet/article/view/181047 (Scopus). 1 ум. друк. арк. / 0,1 ум. др. арк. власного внеску. 4. Guryanova L. Modeling of the enterprise functioning stability using the automatic control theory apparatus / L. Guryanova, I. Nikolaiev, R. Zhovnovach at al. // Eastern-European Journal of Enterprise Technologies. – 2017. - № 3(88), Vol. 4 - С. 45-55. Режим доступу: http://journals.uran.ua/eejet/article/view/108936 (фахове видання, Scopus) (2.5 ум. друк. арк./0.25 ум. др. арк. власного внеску) 5. Developing an advanced classifier of threat for security agent behavior models / Milov O., Korol O., Milevskyi S. // Наука і техніка Повітряних Сил Збройних Сил України, 2019, № 4(37). С. 105-112. DOI: 10.30748/nitps.2019.37.15. Режим доступу: http://www.hups.mil.gov.ua/periodic-app/article/19554 (фахове, категорія Б) 1 ум. друк. арк. / 0,33 ум. др. арк. власного внеску. 6. Євсеєв С. Development and analysis of game-theoretical models of security systems agents interaction / Євсеєв С.П., Мілов О.В., Войтко О.В., Кас'яненко М.В., Меленті Є. О., Мілевський С. В., Погасій С.С., Степанов Г.С., Туринский А.В., Фараон С.І. // Eastern-European Journal of Enterprise Technologies. – Харьков. – 2020. 2/4(104). С. 15-29 Режим доступу: http://journals.uran.ua/eejet/article/view/201418 (фахове видання, Scopus) 2 ум. друк. арк. / 0,2 ум. др. арк. власного внеску. 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. (12,25 ум. др. арк. / 0,4 ум. др. арк. власного внеску) вільний (дата звернення 30.08.2023). (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. Патент на винахід (корисну модель) u 2021 03726 від 30.06.2021 СПОСІБ КРИПТОГРАФІЧНОГО ПЕРЕТВОРЕННЯ ІНФОРМАЦІЇ 2. Патент на винахід (корисну модель) u 2021 03704 від 29.06.2021 СПОСІБ КРИПТОГРАФІЧНОГО ПЕРЕТВОРЕННЯ ІНФОРМАЦІЇ 3. Патент на винахід (корисну модель) u 2021 03665 від 25.06.2021 СПОСІБ КРИПТОГРАФІЧНОГО ПЕРЕТВОРЕННЯ ІНФОРМАЦІЇ 4. Патент на винахід (корисну модель) u 2021 03617 від 23.06.2021 СПОСІБ КРИПТОГРАФІЧНОГО ПЕРЕТВОРЕННЯ ІНФОРМАЦІЇ 5. Патент на винахід (корисну модель) u 2021 03615 від 23.06.2021 СПОСІБ КРИПТОГРАФІЧНОГО ПЕРЕТВОРЕННЯ ІНФОРМАЦІЇ 6. Патент на винахід (корисну модель) u 2021 03683 від 23.07.2021 СПОСІБ КРИПТОГРАФІЧНОГО ПЕРЕТВОРЕННЯ ІНФОРМАЦІЇ 7. Патент на винахід (корисну модель) u 2021 03680 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. Організація і збереження баз даних: робоча програма навчальної дисципліни для студентів спеціальності 125 “Кібербезпека” першого (бакалаврського) рівня [Електронне видання] / укл. С. В. Мілевський. – Харків : ХНЕУ ім. С. Кузнеця, 2020. – 12 с. Режим доступу: http://www.repository.hneu.edu.ua/handle/123456789/24047 2. Експертні системи: робоча програма навчальної дисципліни для студентів спеціальності 125 «Кібербезпека» першого (бакалаврського) рівня / укл. О. В. Мілов, С. В. Мілевський. – Харків : ХНЕУ ім. С. Кузнеця, 2020. – 16 с. (Укр. мовою). Режим доступу: http://www.repository.hneu.edu.ua/handle/123456789/24689 3. Комп’ютерні мережі: робоча програма навчальної дисципліни для студентів спеціальності 121 “Інженерія програмного забезпечення” першого (бакалаврського) рівня [Електронне видання] / укл. С. В. Мілевський. – Х. : Вид. ХНЕУ ім. С. Кузнеця, 2019. – 9 с. (Укр. мов.) Режим доступу: http://www.repository.hneu.edu.ua/handle/123456789/23304 4. Менеджмент інформаційної безпеки: робоча програма навчальної дисципліни для студентів спеціальності 125 “Кібербезпека” першого (бакалаврського) рівня [Електронне видання] / укл. С. В.

							Мілевський. – Х. : Вид. ХНЕУ ім. С. Кузнеця, 2019. – 9 с. (Укр. мов.) Режим доступу: http://www.repository.hneu.edu.ua/handle/123456789/23305 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 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. 1. Lydia Guryanova, Stanislav Milevskyi, Sergey Razumovskyi Econometric models for evaluating the effectiveness of the financial decentralization mechanisms development // Econometric Research in Finance Workshop 2019, Warsaw School of Economics, Warsaw, Poland, 13.09.2019, pp. 13-14 Режим доступу: https://www.conference.erfin.org/program2019/booklet.pdf (10.10.2021) 2. 2. Milevskyi S.V., Pohasii S.S. Cybersecurity issues in the internet of things // 1st International Conference: Modern Information, Measurement and Control Systems: Problems and Perspectives (MIMCS’2019), 01-02 July, Baku, AZERBAIJAN. – P. 33-34 Режим доступу:

							https://zenodo.org/record/3783978#.YWP01dpByUk (10.10.2021) 3. 3. Milevskyi S.V., Milov O.V. Requirements for the properties of agents and multi-agent systems in the models of cybersecurity // 1st International Conference: Modern Information, Measurement and Control Systems: Problems and Perspectives (MIMCS'2019), 01-02 July, Baku, AZERBAIJAN. – P. 258-259 Режим доступу: https://zenodo.org/record/3783978#.YWP01dpByUk (10.10.2021) 4. 4. O. Ivahnenko, S. Milevskyi Average Wage Dynamics Modeling In View Of Threshold Effects // Матеріали Міжнародної науково-практичної конференції "Економічний розвиток і спадщина Семена Кузнеця": тези доповідей, 30 – 31 травня 2019 р. – Х.: ХНЕУ імені Семена Кузнеця, 2019. – С. 228-229 Режим доступу: http://repository.hneu.edu.ua/handle/123456789/22165 (10.10.2021) 5. S. Milevskyi, S. Pohasii Internet Security Problems Caused By Artificial Intelligence // Матеріали Міжнародної науково-практичної конференції "Економічний розвиток і спадщина Семена Кузнеця": тези доповідей, 30 – 31 травня 2019 р. – Х.: ХНЕУ імені Семена Кузнеця, 2019. – С. 248-249 Режим доступу: http://repository.hneu.edu.ua/handle/123456789/22165 (10.10.2021) П. 13 проведення навчальних занять із спеціальних дисциплін іноземною мовою (крім дисциплін мовної підготовки) в обсязі не менше 50 аудиторних годин на навчальний рік Комп'ютерні системи та архітектура комп'ютерів – 48 годин, освітня

							програма «Інженерія програмного забезпечення», 2 курс Комп'ютерні мережі – 48 годин, освітня програма «Інженерія програмного забезпечення», 2 курс Організація і збереження баз даних – 72 години, освітня програма «Кібербезпека», 3 курс Табличний процесор MS Excel: просунутий рівень – 90 годин, всі освітні програми, 1 курс 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", свідотство ES № 059
410247	Гаврилова Алла Андріївна	Старший викладач, 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	18	Презентація та обробка знань	Підвищення кваліфікації: магістр з кібербезпеки. 31.12.2021 р. диплом М21 №089064 2) 2022 IEEE KhPI Week on Advanced Technology, October 03-07, 2022 Kharkiv, Ukraine. Cerfies professional development (30 hours - 1 ECTS credit) Пункти відповідності ліцензійних умов: П. 1, 2, 4, 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. 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. (12,25 ум. др. арк. / 0,4 ум. др. арк. власного внеску) вільний (дата звернення 30.08.2023). (Scopus)

							2. Development of an improved SSL/TLS protocol using post-quantum algorithms / S. Yevseiev, A. Havrylova, S. Milevskyi, I. Sinitsyn, V. Chalapko, H. Dukin, V. Hrebeniuk, M. Diedov, L. Bekirova, O. Shpak. // Eastern-European Journal of Enterprise Technologies. – 2023. – № 3(9 (123). – P. 33–48. (1,8 ум. др. арк. / 0,2 ум. др. арк. власного внеску) вільний (дата звернення 30.08.2023). (Scopus) 3. Gavrilova A. Development of a modified UMAC Algorithm based on crypto-code constructions / A. Gavrilova, I. Volkov, Yu. Kozhedub, R. Korolev, O. Lezik, V. Medvediev, O. Milov, B. Tomashevsky, A. Trystan, O. Chekunova // Eastern-European Journal of Enterprise Technologies. – 2020. – № 4/9 (106). – C. 45 – 63. – Acces mode: http://webcache.googleusercontent.com/search?q=cache:k22GaB786vAJ:journals.uran.ua/eejet/article/download/210683/210958+&cd=3&hl=ru&ct=clnk&gl=ua (Scopus) (0,95 ум. др. арк. / 0,095 ум. друк. арк. власного внеску). 4. Gavrilova A. Development of Niederreiter hybrid crypto-code structure on flawed codes / S. Yevseiev, O. Tsyhaneko, A. Gavrilova, V. Guzhva, O. Milov, V. Moskalenko, I. Opirskyy, O. Roma, B. Tomashevsky, O. Shmatko // Eastern-European Journal of Enterprise Technologies. – 2019. – № 1/9 (97). – P. 27 – 38. – Acces mode: http://webcache.googleusercontent.com/search?q=cache:E9OE7avPTyoJ:journals.uran.ua/eejet/article/view/210683+&cd=2&hl=ru&ct=clnk&gl=ua (Scopus) (0,7 ум. др. арк. / 0,07 ум. друк. арк. власного внеску). 5. Havrylova Alla A. Mathematical model of authentication of a transmitted message

							based on a McEliece scheme on shorted and extended modified elliptic codes using UMAC modified algorithm / Alla A. Havrylova, Olha H. Korol, Stanyslav V. Milevskyi, Lala R. Bakirova // "Кібербезпека: освіта, наука, техніка", 2019. – No 1(5). – P. 40 – 51. Acces mode: https://webcache.googleusercontent.com/search?q=cache:diuoPNu4g-cJ:https://www.csecurity.kubg.edu.ua/index.php/journal/article/download/102/105/+&cd=1&hl=ru&ct=clnk&gl=ua (0,6 ум. др. арк. / 0,15 ум. друк. арк. власного внеску). 6. Havrylova A.. A NEW FRAMEWORK DESIGNED FOR KNOWLEDGE MANAGEMENT IN DISTRIBUTED SOFTWARE DEVELOPMENT / A. Havrylova, O. Shmatko, Liang Dong, V. Aleksiyev // Щоквартальний науково-технічний журнал "Сучасні інформаційні системи", Том 3, № 1. - Х. : Національний технічний університет “Харківський політехнічний інститут”.2019. – С. 109 – 115. – Acces mode: http://webcache.googleusercontent.com/search?q=cache:p8Fk-AseLYMJ:ais.khpi.edu.ua/issue/download/10065/6794+&cd=1&hl=ru&ct=clnk&gl=ua (0,35 ум. др. арк. / 0,088 ум. друк. арк. власного внеску).
							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. Патент на винахід (корисну модель) u 2021 03726 від 30.06.2021 СПОСІБ КРИПТОГРАФІЧНОГО ПЕРЕТВОРЕННЯ ІНФОРМАЦІЇ. 2. Патент на винахід (корисну модель) u 2021 03704 від

							29.06.2021 СПОСІБ КРИПТОГРАФІЧНОГО ПЕРЕТВОРЕННЯ ІНФОРМАЦІЇ. 3. Патент на винахід (корисну модель) u 2021 03665 від 25.06.2021 СПОСІБ КРИПТОГРАФІЧНОГО ПЕРЕТВОРЕННЯ ІНФОРМАЦІЇ. 4. Патент на винахід (корисну модель) u 2021 03683 від 23.07.2021 СПОСІБ КРИПТОГРАФІЧНОГО ПЕРЕТВОРЕННЯ ІНФОРМАЦІЇ. 5. Патент на винахід (корисну модель) u 2021 03680 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. Гаврилова А. А. Методичні рекомендації щодо написання курсових проєктів для студентів зі спеціальності 125 "Кібербезпека" першого (бакалаврського) рівня / укл. С. П. Євсеєв, А. А. Гаврилова, О. Г. Король, Г. П. Коц. – Харків : ХНЕУ ім. С. Кузнеця, 2020. – 85 с. – Режим доступу: http://repository.hneu.edu.ua/handle/123456789/23326?locale=uk (4,25 ум. др. арк. / 1,063 ум. друк. арк. власного внеску) 2. Гаврилова А. А. Методичні рекомендації до виконання кваліфікаційних проєктів для студентів спеціальності 125 “Кібербезпека” першого (бакалаврського) рівня / уклад. С. П. Євсеєв, О. Г. Король,

							А. А. Гаврилова, Г. П. Коц. – Харків : ХНЕУ ім. С. Кузнеця, 2020. – 51 с. – Режим доступу: http://webcache.googleusercontent.com/search?q=cache:k5xuE3LmIGMJ:repository.hneu.edu.ua/bitstream/123456789/25448/1/2021-%25D0%2584%25D0%25B2%25D1%2581%25D0%25B5%25D1%2594%25D0%25B2%2520%25D0%25A1%25D0%259F%252C%2520%25D0%259A%25D0%25BE%25D1%2580%25D0%25BE%25D0%25BB%25D1%258C%2520%25D0%259E%25D0%2593%252C%2520%25D0%2593%25D0%25B0%25D0%25B2%25D1%2580%25D0%25B8%25D0%25BB%25D0%25BE%25D0%25B2%25D0%25B0%2520%25D0%2590%25D0%2590%252C%2520%25D0%259A%25D0%25BE%25D1%2586%2520%25D0%2593%25D0%259F.pdf+&cd=1&hl=ru&ct=clnk&gl=ua (2,55 ум. др. арк. / 0,638 ум. друк. арк. власного внеску) 3. Гаврилова А. А. Наскрізна програма практики для студентів спеціальності 125 "Кібербезпека" першого (бакалаврського) рівня / уклад. С. П. Євсеєв, А. А. Гаврилова, Г. П. Коц. – Харків : ХНЕУ ім. С. Кузнеця, 2020. – 35 с. – Режим доступу: http://webcache.googleusercontent.com/search?q=cache:UUCvWjoCQVUJ:www.kafcbit.hneu.edu.ua/wp-content/uploads/sites/13/2020/01/1401%25D0%2593%25D0%25B0%25D0%25B2%25D1%2580%25D0%25B8%25D0%25BB%25D0%25BE%25D0%25B2%25D0%25B0%25D0%259A%25D0%2591%25D0%2598%25D0%25A2%25D0%25BC%25D0%25B5%25D1%2582%25D0%25BE%25D0%25B4%25D0%25B8%25D1%2587%25D0%25BA%25D0%25B0-%25D0%25BF%25D1%2580%25D0%25B0%25D0%25BA%25D1%2582%25D0%25B8%25D0%25BA%25D0%25B0_2020.pdf+&cd=1&hl=ru&ct=clnk&gl=ua (1,75 ум. др. арк. / 0,875 ум.

							друк. арк. власного внеску) 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. Формирование модели оценки показателей развития ИТ-отрасли в регионах Украины / Н. А. Брынза, А. А. Гаврилова // Системи обробки інформації. – 2019. – № 2 (157). – С. 13-21. – URL: http://webcache.googleusercontent.com/search?q=cache:CaCFYQUSjL8J:www.hups.mil.gov.ua/periodic-app/article/19322/soi_2019_2_4.pdf+&cd=3&hl=ru&ct=clnk&gl=ua (0,9 ум. др. арк. / 0,45 ум. друк. арк. власного внеску) (дата звернення 1.03.2019). 2. Гаврилова А. А. Побудова крипто-кодових конструкцій для використання в постквантовій криптографії / А. А. Гаврилова, О.Г. Король, К. Четінкайя. Глава 1: Інформаційна безпека держави, суспільства та особистості Інформаційна безпека та інформаційні технології: монографія / за заг. ред. В.С. Пономаренка. – Х.: ТОВ "ДІСА ПЛЮС", 2019. – 322 с. укр. мов. (С.15-30) – URL: http://www.itconf.hneu.edu.ua/wp-content/uploads/2019/04/%D0%9C%D0%BE%D0%BD%D0%BE%D0%B3%D1%80%D0%B0%D1%84%D0%B8%D1%8F_%D0%BA%D0%BE%D0%BD%D1%84%D0%B5%D1%80%D0%B5%D0%BD%D1%86%D0%B8%D1%8F_2019-%D0%B8%D1%82%D0%BE%D0%B3.pdf (0,3 ум. др. арк. / 0,1 ум. друк. арк. власного внеску) (дата звернення 16.04.2019). 3. Gavrilova Alla. BLOCKCHAIN AS THE BASIS OF THE

							DIGITAL ECONOMY. WORLD EXPERIENCE OF CRYPTOCURRENCY FINANCIAL REGULATION / Alexander Shmatko, Alla Gavrilova //4th International Congress on 3D Printing (Additive Manufacturing) Technologies and Digital Industry 2019, 11-14 APRIL 2019. – Antalya / TÜRKİYE. P. 785-790. URL: // https://scholar.google.com/citations?view_0=view_citation&hl=ru&user=Vj8UnS4AAAAJ&sortby=pubdate&citation_for_view=Vj8UnS4AAAAJ:M3ejUd6NZC8C (0,6 ум. др. арк. / 0,3 ум. друк. арк. власного внеску) (дата звернення 16.04.2019). 4. Havrylova Alla. Development of authentication codes of messages on the basis of UMAC with crypto-code McEliece's scheme on elliptical codes / Alla Havrylova, Serhii Yevseiev, Olha Korol // Materials of VIIth International Scientific and Technical Conference "Information protection and information systems security": report theses, May 30–31, 2019. – Lviv: Lviv Polytechnic Publishing House, 2019. – 1 electron. opt. disk (DVD). – С. 86 – 87. – URL: //https://scholar.google.com/scholar?hl=ru&as_sdt=0,5&cluster=9407398346914807026 (0,3 ум. др. арк. / 0,1 ум. друк. арк. власного внеску) (дата звернення 16.04.2019). 5. Гаврилова А. А. Анализ состояния блокчейн-проектов на рынке украинских сервисов / А. А. Гаврилова // Material of International Conference, Modern Information, Measurement and Control Systems: Problems and Perspectives (MIMCS'2019), 01-02 July, Baku, Azerbaijan. – С. 76.– URL: //http://repository.hneu.edu.ua/handle/123456789/22704 (0,1 ум. др. арк. / 0,1 ум. друк. арк. власного внеску)

							(дата звернення 16.07.2019). 6. Гаврилова А. А. Применение алгоритма UMAC на крипто-кодовых конструкциях в блокчейн-технологиях / А. А. Гаврилова // Науковий журнал «ScienceRise», 2019. – Серія “Технічні науки”. – №12(65). – С. 20 – 23. URL: //http://webcache.googleusercontent.com/search?q=cache:BCPmofoM5hwJ:journals.uran.ua/sciencerise/article/view/189617+&cd=1&hl=ru&ct=clnk&gl=ua (0,4 ум. др. арк. / 0,4 ум. друк. арк. власного внеску) (дата звернення 12.12.2019). 7. Havrylova Alla Practical UMAC algorithms based on crypto code designs/ Olha Korol, Alla Havrylova, Serhii Yevseiev // Przetwarzanie, transmisja I bezpieczenstwo informacji, 2019, Tom 2. – Bielsko-Biala: Wydawnitwo naukowe Akademii Techniczno-Humanistycznej w Bielsku-Bialej, 2019. – 130 p. eng. lang. (P. 221-232) – URL: //http://webcache.googleusercontent.com/search?q=cache:9SakRzEO9OwJ:www.engineerxxi.ath.eu/wp-content/uploads/2019/11/ATH_tc_2019_vol2.pdf+&cd=1&hl=ru&ct=clnk&gl=ua (6,5 ум. др. арк. / 2,17 ум. друк. арк. власного внеску) (дата звернення 21.12.2019). 8. Гаврилова А. А. Використання геш-кодів, створених за допомогою алгоритма UMAC на крипто-кодових конструкціях, для забезпечення необхідного рівня стійкості до зломів / С. С. Погасій, А. А. Гаврилова // Матеріали регіон. круг. столу «Актуальні питання забезпечення службово-бойової діяльності сил сектору безпеки і оборони» (м. Харків, 24 квіт. 2020 р.) Вип. 4. / редкол.: Є. О. Меленті, І. В. Євтушенко, О. А. Гарбузов, В. О. Пономарьов. – Х. :

							ФОП Бровін О. В., 2020. – С. 290 – 294. http://webcache.googleusercontent.com/search?q=cache:pSrozgeYDDIJ:repository.hneu.edu.ua/bitstream/123456789/23492/1/_%25D0%259A%25D1%2580%25D1%2583%25D0%25B3%25D0%25BB%25D0%25B8%25D0%25B9_%25D1%2581%25D1%2582i%25D0%25BB_I%25D0%259F%25D0%25AE%25D0%259A_%25D0%25A1%25D0%2591%25D0%25A3_24.04.2020.pdf+&cd=4&hl=ru&ct=clnk&gl=ua (0,313 ум. др. арк. / 0,156 ум. друк. арк. власного внеску) (дата звернення 24.04.2021). 9. Havrylova Alla Improved UMAC algorithm with crypto-code mceliece's scheme / Yevseiev Serhii, Havrylova Alla // Modern Problems Of Computer Science And IT-Education: collective monograph / [editorial board K. Melnyk, O. Shmatko].– Vienna : Premier Publishing s.r.o., 2020.– 236 p. eng. lang. (P. 79 – 92). – URL: http://ppublishing.org/upload/iblock/431/Mono_Shmatko.pdf (0,25 ум. др. арк. / 0,125 ум. друк. арк. власного внеску) (дата звернення 15.06.2020). 10. Гаврилова А. А. Оценка показателей динамики сетевой активности блокчейн-кошельков на рынке биткоина / Н. А. Брынза, А. А. Гаврилова // Безпека ресурсів інформаційних систем: збірник тез І Міжнародної науково-практичної конференції (м. Чернігів 16-17 квітня 2020 р.). – Чернігів : НУЧП, 2020. – С. 59 – 64. – URL: //https://stu.cn.ua/wp-content/uploads/2021/04/bris-t.pdf (0,3 ум. др. арк. / 0,15 ум. друк. арк. власного внеску) (дата звернення 06.10.2021). 11. Гаврилова Алла. Реализация алгоритма UMAC на крипто-кодовых конструкциях / Ольга Король, Алла

							Гаврилова // ITSec: Безпека інформаційних технологій: X міжнародна науково-технічна конференція, 19-24 березня 2020 р. – К.: НАУ, 2019. – С. 12 – 13. – URL: //http://bit.nau.edu.ua/wp-content/uploads/2020/05/ITSec-2020_Zbirnyk.pdf (0,1 ум. др. арк. / 0,05 ум. друк. арк. власного внеску) (дата звернення 06.10.2021). 12. Havrylova Alla. Practical UMAC algorithm on hybrid crypto-code constructions of McElise on shortened MEC / Alla Havrylova // International Journal of 3D Printing Technologies and Digital Industry 5 (1), Araştırma Makalesi/Research Articles, 2020. – 1 electron. opt. disk (DVD). – P. 143 – 154. – URL: //https://webcache.googleusercontent.com/search?q=cache:6OTFMy3Qmj4J:https://asosindex.com.tr/index.jsp%3Fmodul%3Darticles-page%26journal-id%3D183%26article-id%3D419827+&cd=2&hl=ru&ct=clnk&gl=ua (0,6 ум. др. арк. / 0,6 ум. друк. арк. власного внеску) (дата звернення 21.05.2020). 13. Гаврилова А. А. Анализ уязвимостей технологии блокчейн при работе с криптовалютами [Електронний ресурс] / А. А. Гаврилова, Р. В. Корольов // Матеріали II Міжнародної науково-практичної конференції “Інформаційна безпека та інформаційні технології” “Information Security and Information Technologies” 2 – 3 квітня 2020 р. – Електрон.текст. дані. Кропивницький, 2020. С. 4. – URL: //http://kbpz.kntu.kr.ua/wp-content/uploads/2020/04/%D0%97%D0%91%D0%86%D0%A0%D0%9D

							%D0%98%D0%9A-%D0%A2%D0%95%D0%97-%D0%BA%D0%BE%D0%BD% D1%84-2-3-%D0%BA%D0%B2%D1%96%D1%82%D0%BD%D1%8F.pdf#page=4, вільний (0,1 ум. др. арк. / 0,05 ум. друк. арк. власного внеску) (дата звернення 3.04.2020). 14. Гаврилова А. А. Формування кортежу показників оцінки блокчейн-гаманців / Н. О. Бринза, А. А. Гаврилова // Матеріали Міжнародної науково-практичної конференції "Інформаційні технології та системи": тези доповідей, 9-10 квітня 2020 р. – Х.: ХНЕУ імені Семена Кузнеця, 2020. – С. 39. – URL: //http://www.repository.hneu.edu.ua /jspui/bitstream/123456789/23038/1/%D0%A1%D0%91%D0%9E%D0%A0%D0%9D%D0%98%D0%9A_%D0%BA%D0%BE%D0%BD%D1%84._9.04.2020.pdf (0,1 ум. др. арк. / 0,05 ум. друк. арк. власного внеску) (дата звернення 23.05.2020). 15. Гаврилова А. А. Аналіз шифрів у бездротових мережах / Ю. Е. Куля, А. А. Гаврилова // Стан, досягнення та перспективи інформаційних систем і технологій / Матеріали XXI Всеукраїнської науково-технічної конференції молодих вчених, аспірантів та студентів. Одеса, 22-23 квітня 2021 р. – Одеса, Видавництво ОНАХТ, 2021 р. – С. 40 – 41. – URL: //http: Stan_dosyagnennya_inform_system_2021.pdf. (0,1 ум. др. арк. / 0,05 ум. друк. арк. власного внеску) (дата звернення 23.04.2021). 16. 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: http://repository.hneu.edu.ua/handle/123456789/25621 (0,25 ум. др. арк. / 0,25 ум. друк. арк. власного внеску) (дата звернення 23.05.2021). 17. Гаврилова А. А. Визначення стану захищеності кіберпростору / А. А. Гаврилова // "Інформаційні технології та комп'ютерне моделювання"; матеріали статей Міжнародної науково-практичної конференції, м. Івано-Франківськ, 5-10 липня 2021 року. – Івано-Франківськ: п. Голіней О.М., 2021. – С. 11 – 12. URL: https://itcm.comp-sc.if.ua/2021/zbirnyk_2021.pdf (0,1 ум. др. арк. / 0,1 ум. друк. арк. власного внеску) (дата звернення 28.08.2021). 18. 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). Acces mode: http://webcache.googleusercontent.com/search?q=cache:Ii4pGrNeP2QJ:www.repository.hneu.edu.ua/jspui/handle/123456789/25623+&cd=1&hl=ru&ct=clnk&gl=ua (9,4 ум. др. арк. / 0,077 ум.

							друк. арк. власного внеску) 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 №1 від 7.10.2021р. Член громадської організації "Східноєвропейське наукове товариство", свідотство ES № 055
410239	Мілов Олександр Володимирович	Професор, Основне місце роботи	Навчально-науковий інститут комп'ютерних наук та інформаційних технологій	Диплом спеціаліста, Московский ордена Ленина энергетический институт, рік закінчення: 1978, спеціальність: Промышленная электроника, Диплом доктора наук ДД 010482, виданий 26.11.2020, Диплом кандидата наук ТН 094834, виданий 12.11.1986, Атестат доцента ДЦ 039210, виданий 04.07.1991, Атестат професора АП 001430, виданий 16.12.2019	41	Тестування на проникнення та етичний хакінг	Підвищення кваліфікації: Центр підтримки академій Cisco Національний технічний університет "Харківський політехнічний інститут". Сертифікат від "30" червня 2021 р. 6 кредитів, Тема: "CCNA CyberOps" та "Network Security". Пункти відповідності ліцензійних умов: п. 1-5, 7, 8, 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. 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. (12,25 ум. др. арк. / 0,7 ум. др. арк. власного внеску) вільний (дата звернення 30.08.2023). (Scopus) 2. Milov O. Development of Niederreiter hybrid crypto-code structure on flawed codes / Yevseiev S., Milov O., Tsyhanenko O., Gavrilova A., Tomashevsky B., Shmatko O. et al.// Eastern-Europe Journal of Enterprise Technologies, 2019, 1(9-97), p. 27-38. - Access mode: http://journals.uran.ua/eejet/article/view/1566

							20 Scopus (1,5 ум.друк.арк./власний внесок 0,15 авторських аркушів). 3. Milov O. Development of scenario modeling of conflict tools in a security system based on formal grammars / Milov O., Yevseiev S., Vlasov A., Herasimov S., Dmitriiev O., Kasianenko M., Pievtsov H., Peleshok Y., Tkach Y., Faraon S. // Eastern-European Journal of Enterprise Technologies, 2019, v.9, N 6, p. 53-64. - Access mode: http://journals.uran.ua/eejet/article/view/184274 Scopus (2,5 ум.друк.арк./власний внесок 0,25 авторських аркушів). 4. Milov O.V. Development of methodology for modeling the interaction of antagonistic agents in cybersecurity systems / Milov O., Voitko A., Husarova I., Domaskin O., Ivanchenko E., Ivanchenko I., Korol O., Kots H, Opirskyy I., Fraze-Frazenko O.// Eastern-European Journal of Enterprise Technologies, 2019, v.9, N 2, p. 56-66. - Access mode: http://journals.uran.ua/eejet/article/view/164730. Scopus (2,5 ум.друк.арк./власний внесок 0,25 авторських аркушів). 5. Milov O. Development of a methodology for building an information security system in the corporate research and education system in the context of university autonomy / Yevseiev S., Milov O., Aleksiyev V., Balakireva S., Tyshyk I., Shmatko O. et. al. // Eastern-Europe Journal of Enterprise Technologies, 2019, v. 3, №9 (99), p. 49-63. - Access mode: http://journals.uran.ua/eejet/article/view/169527. Scopus (2,5 ум.друк.арк./власний внесок 0,25 авторських аркушів). 6. Milov O. Development of the model of the antagonistic agents behavior under a cyber conflict / O. Milov, S.

							Yevseiev, Y. Ivanchenko, S. Milevskyi, O. Nesterov, O. Puchkov, A. Salii, O. Timochko, V. Tiurin, A. Yarovyi // Eastern-Europe Journal of Enterprise Technologies, 2019, v.4, № 9(100). P.6-19. - Access mode: http://journals.uran.ua/eejet/article/view/175978. Scopus (2.5 ум.друк.арк./власний внесок 0,25 авторських аркушів). 7. Milov O. Development of the interacting agents behavior scenario in the cyber security system / Milov, O., Yevseiev, S., Aleksiyev, V., Berdnik, P., Voitko, O., Dyptan, V., Ivanchenko, Y., Pavlenko, M., Salii, A., & Yarovyy, S. // Eastern-Europe Journal of Enterprise Technologies, 2019, v.5, № 9(101). P.46-57. - Access mode: http://journals.uran.ua/eejet/article/view/181047. Scopus (2,5 ум.друк.арк./власний внесок 0,25 авторських аркушів). 8 Milov O. Development of a hardware cryptosystem based on a random number generator with two types of entropy sources Yevseiev, S., Rzayev, K., Laptiev, O., ...Camalova, J., Pohasii, S. Eastern-European Journal of Enterprise Technologiesthis link is disabled, 2022, 5(9-119), pp. 6–16 9 Milov O. Development of a concept for cybersecurity metrics classificatioN Yevseiev, S., Milov, O., Opirskyy, I., ...Melenti, Y., Tomashevsky, B. Eastern-European Journal of Enterprise Technologiesthis link is disabled, 2022, 4(4-118), pp. 6-18 10 Milov O. Development of crypto-code constructs based on LDPC codes / Pohasii, S., Yevseiev, S., Zhuchenko, O., ...Lezik, A., Susukailo, V. Eastern-European Journal of Enterprise Technologiesthis link is disabled, 2022, 2(9-116), pp. 44–59 11 Milov O.

							Development of a modification of the method for constructing energy-efficient sensor networks using static and dynamic sensors / Petrivskyi, V., Shevchenko, V., Yevseiev, S., ...Kurchenko, O., Opirskyy, I. Eastern-European Journal of Enterprise Technologiesthis link is disabled, 2022, 1(9-115), pp. 15–23 12 Milov O. Situational Control of Cyber Security in Socio-Cyber-Physical Systems / Milov, O., Khvostenko, V., Natalia, V., Korol, O., Zviertseva, N. HORA 2022 - 4th International Congress on Human-Computer Interaction, Optimization and Robotic Applications, Proceedings, 2022 13 Milov O., Yevseiev, S., Zviertseva, N., Zviertsev, H., Motalyhin, Y. Pseudo-Physical Logics in Control of Cyber Security Systems. ISMSIT 2022 - 6th International Symposium on Multidisciplinary Studies and Innovative Technologies, Proceedings, 2022, pp. 1038–1042 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. Патент на винахід (корисну модель) u 2021 03726 від 30.06.2021 СПОСІБ КРИПТОГРАФІЧНОГО ПЕРЕТВОРЕННЯ ІНФОРМАЦІЇ 2. Патент на винахід (корисну модель) u 2021 03704 від 29.06.2021 СПОСІБ КРИПТОГРАФІЧНОГО ПЕРЕТВОРЕННЯ ІНФОРМАЦІЇ 3. Патент на винахід (корисну модель) u 2021 03665 від 25.06.2021 СПОСІБ КРИПТОГРАФІЧНОГО ПЕРЕТВОРЕННЯ ІНФОРМАЦІЇ 4. Патент на винахід (корисну модель) u 2021 03617 від

							23.06.2021 СПОСІБ КРИПТОГРАФІЧНОГО ПЕРЕТВОРЕННЯ ІНФОРМАЦІЇ 5. Патент на винахід (корисну модель) u 2021 03615 від 23.06.2021 СПОСІБ КРИПТОГРАФІЧНОГО ПЕРЕТВОРЕННЯ ІНФОРМАЦІЇ 6. Патент на винахід (корисну модель) u 2021 03683 від 23.07.2021 СПОСІБ КРИПТОГРАФІЧНОГО ПЕРЕТВОРЕННЯ ІНФОРМАЦІЇ 7. Патент на винахід (корисну модель) u 2021 03680 від 25.06.2021 СПОСІБ КРИПТОГРАФІЧНОГО ПЕРЕТВОРЕННЯ ІНФОРМАЦІЇ 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) Лабораторний практикум з основ криптографічного захисту [Електронний ресурс] : навч. посіб. / С. П. Євсеєв, О. В. Мілов, О. Г. Король ; Харківський національний економічний університет ім. С. Кузнеця. - Електрон. текстові дан. (221 с. / 12,3 МБ). - Харків : ХНЕУ ім. С. Кузнеця, 2020. Режим доступу: http://repository.hneu.edu.ua/handle/123456789/24508. 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. Лабораторний

							практикум з основ криптографічного захисту [Електронний ресурс] : навч. посіб. / С. П. Євсеєв, О. В. Мілов, О. Г. Король ; Харківський національний економічний університет ім. С. Кузнеця. - Електрон. текстові дан. (221 с. / 12,3 МБ). - Харків : ХНЕУ ім. С. Кузнеця, 2020. Режим доступу: http://repository.hneu.edu.ua/handle/123456789/24508. РПНД: 1. Математичні основи криптології: робоча програма навчальної дисципліни для студентів спеціальності 125 “Кібербезпека” першого (бакалаврського) рівня [Електронне видання] / укл. О. В. Мілов. – Х. : Вид. ХНЕУ ім. С. Кузнеця, 2019. (Укр. мов.) http://www.repository.hneu.edu.ua/handle/123456789/23311 2. Інтелектуальний аналіз даних: робоча програма навчальної дисципліни для студентів спеціальності 125 “Кібербезпека” другого (магістерського) рівня [Електронне видання] / укл. О. В. Мілов – Х. : Вид. ХНЕУ ім. С. Кузнеця, 2019. (Укр. мов.) http://www.repository.hneu.edu.ua/handle/123456789/22419 3. Ризик-менеджмент: робоча програма навчальної дисципліни для студентів спеціальності 125 “Кібербезпека” другого (магістерського) рівня [Електронне видання] / укл. О. В. Мілов. – Х. : Вид. ХНЕУ ім. С. Кузнеця, 2019. (Укр. мов.) http://www.repository.hneu.edu.ua/handle/123456789/22423 4. Тестування на проникнення та етичний хакінг: робоча програма навчальної дисципліни для студентів спеціальності 125 Кібербезпека другого (магістерського) рівня [Електронне видання]

							/ укл. О. В. Мілов. – Харків : ХНЕУ ім. С. Кузнеця, 2020. http://www.repository.hneu.edu.ua/handle/123456789/24051 5. Основи криптографічного захисту: робоча програма навчальної дисципліни для студентів спеціальності 125 “Кібербезпека” першого (бакалаврського) рівня [Електронне видання] / укл. О. В. Мілов – Харків : ХНЕУ ім. С. Кузнеця, 2020. http://www.repository.hneu.edu.ua/handle/123456789/24048 П. 5 захист дисертації на здобуття наукового ступеня. Доктор технічних наук, 05.13.21. Системи захисту інформації, тема дисертації: Методологія моделювання процесів поведінки антагоністичних агентів в системах безпеки. Диплом ДД №010482 від 26 листопада 2020 року, Міністерство Освіти та 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 Член спеціалізованої вченої ради Д 26.861.06 з присудження наукового ступеня доктора наук за спеціальністю 05.13.21 «Системи захисту інформації» 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 Керівник НДР ХНЕУ ім. С.Кузнеця «Методологія моделювання взаємодії агентів в системах безпеки» за номер державної реєстрації № 0119U103117. П. 10 участь у міжнародних наукових та/або освітніх проектах, залучення до міжнародної експертизи, наявність звання “суддя міжнародної категорії” Участь у Cybersecurity Summer Training Program under the USAID Project “Cybersecurity for Critical Infrastructure in Ukraine” 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. Milov O. Self-organizing organizational structures of cybersecurity systems // Modern Problems Of Computer Science And IT-Education : collective monograph / [editorial board K. Melnyk, O. Shmatko]. – Vienna : Premier Publishing s.r.o., 2020. – 236 p. – URL: http://repository.hneu.edu.ua/bitstream/123456789/23495/1/%d0%90%d0%b2%d1%81%d1%82%d1%80%d0%b8%d1%8f_%d0%9c%d0%b8%d0%bb%d0%be%d0%b2_%d0%a0%d0%b5%d0%bf%d0%be%d0%b7%d0%b8%d1%82%d0%b0%d1%80%d0%b8%d0%b9.pdf (дата звернення 12.10.2021 р.) 2. Milov O. Adaptive decision support systems for cyber security / O. Milov // Сучасні інформаційні системи. - 2019. - Т. 3, № 1. - С. 131-135. - –

							URL: http://nbuv.gov.ua/UJRN/adinsys_2019_3_1_24. (дата звернення 12.10.2021 р.) 3. Milov O. V. Development of basic principles for corporate planning / Milevsky S. V., Korol O. H. // Системи обробки інформації. – 2019, випуск 1 (156). С. 28-36. - – URL: https://doi.org/10.30748/soi.2019.156.04. (дата звернення 12.10.2021 р.) 4. Milov O. Mechanisms of cyber security: The Problem of Conceptualization / Milov O., Kazakova N., Milczarski P., Korol O. // Безпека інформації. – 2019, vol. 25, issue 3. – P. 110–116. DOI: 10.18372/2225-5036.25.13841. – URL: https://www.researchgate.net/publication/337114411_Mechanisms_of_cyber_security_the_problem_of_conceptualization. (дата звернення 12.10.2021 р.) 5. Milov O. Simulation of a distributed decision-making system in cyber security / Milov O., Milevskyi S., Aleksiyev V. // International Journal of 3D Printing Technologies and Digital Industry. – 2019, 3:2(2019), – P. 147-152. – URL: https://dergipark.org.tr/tr/download/article-file/797288. (дата звернення 12.10.2021 р.) 6. Yevseiev, S., Hryshchuk, R., Molodetska, K., Nazarkevych, M., Hrytsyk, V., Milov, O. et. al.; (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 7. Synergy of building cybersecurity systems / Yevseiev, S., Ponomarenko, V., Laptiev, O., MilovO., ..., Florov, S. Synergy of building cybersecurity systems, 2021, pp. 1–175 П. 13 проведення навчальних занять із спеціальних дисциплін іноземною

							мовою (крім дисциплін мовної підготовки) в обсязі не менше 50 аудиторних годин на навчальний рік. 2019-2020 н. р.: 1.Програмування (121.017-А (БЕР.2019). лекції - 32, лаб. роб. - 32; 2.КОМП'ЮТЕРНІ СИСТЕМИ ТА АРХІТЕКТУРА КОМП'ЮТЕРІВ (121.010-А) лаб. роб. - 22; 3.ДАНІ ТА ПРИЙНЯТТЯ РІШЕНЬ (122.010-БАІСП (Словацька програма) лекції -20, лаб. роб. - 20. П. 19 діяльність за спеціальністю у формі участі у професійних та/або громадських об'єднаннях Член громадської організації "Східноєвропейське наукове товариство", свідотство ES № 060
410244	Мілевський Станіслав Валерійович	Доцент, 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 кандидата наук ДК 033701, виданий 13.04.2006, Атестат доцента 12ДЦ 023152, виданий 17.06.2010, Атестат доцента АД 006043, виданий 26.11.2020	21	Технології управління безпекою бізнес-процесів	Підвищення кваліфікації: Міжнародний проект USAID "Кібербезпека критичної інфраструктури України" Сертифікат від "23" липня 2021 р. 3 кредити. Тема: "Аудит та ризик-менеджмент". Пункти відповідності ліцензійних умов: П. 1, 2, 4, 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. Milov O. Development of the model of the antagonistic agents behavior under a cyber conflict / O. Milov, S. Yevseiev, Y. Ivanchenko, S. Milevskyi, O. Nesterov, O. Puchkov, A. Salii, O. Timochko, V. Tiurin, A. Yarovyi // Eastern-Europe Journal of Enterprise Technologies, 2019, v.4, № 9(100). P.6-19. - Access mode: http://journals.uran.ua/eejet/article/view/175978. (2.5 ум.друк.арк./власний

							внесок 0,25 авторських аркушів). 2. Havrylova A. Mathematical model of authentication of a transmitted message based on a McEliece scheme on shorted and extended modified elliptic codes using UMAC modified algorithm / Alla A. Havrylova, Olha H. Korol, Stanyslav V. Milevskyi, Lala R. Bakirova // "Кібербезпека: освіта, наука, техніка", 2019. – No 1(5). – P. 40 – 51. Acces mode: https://webcache.googleusercontent.com/search?q=cache:diuoPNu4g-cJ:https://www.csecurity.kubg.edu.ua/index.php/journal/article/download/102/105/+&cd=1&hl=ru&ct=clnk&gl=ua (0,6 ум. др. арк. / 0,15 ум. друк. арк. власного внеску). 3. Milov O. Development of the interacting agents behavior scenario in the cyber security system / O. Milov, S. Yevseiev, V. Aleksiyev, P. Berdnik, O. Voitko, V. Dyptan, Y. Ivanchenko, M. Pavlenko, A. Salii, S. Yarovyy // Eastern-European Journal of Enterprise Technologies. – 2019. – Vol. 5. – No. 9 (105). – P. 46–57. – Режим доступу: http://journals.uran.ua/eejet/article/view/181047 (Scopus). 1 ум. друк. арк. / 0,1 ум. др. арк. власного внеску. 4. Guryanova L. Modeling of the enterprise functioning stability using the automatic control theory apparatus / L. Guryanova, I. Nikolaiev, R. Zhovnovach at al. // Eastern-European Journal of Enterprise Technologies. – 2017. - № 3(88), Vol. 4 - C. 45-55. Режим доступу: http://journals.uran.ua/eejet/article/view/108936 (фахове видання, Scopus) (2.5 ум. друк. арк./0.25 ум. др. арк. власного внеску) 5. Developing an advanced classifier of threat for security agent behavior models / Milov O., Korol O., Milevskyi S. // Наука і техніка Повітряних

							Сил Збройних Сил України, 2019, № 4(37). С. 105-112. DOI: 10.30748/nitps.2019.37.15. Режим доступу: http://www.hups.mil.gov.ua/periodic-app/article/19554 (фахове, категорія Б) 1 ум. друк. арк. / 0,33 ум. др. арк. власного внеску. 6. Євсеєв С. Development and analysis of game-theoretical models of security systems agents interaction / Євсеєв С.П., Мілов О.В., Войтко О.В., Кас'яненко М.В., Меленті Є. О., Мілевський С. В., Погасій С.С., Степанов Г.С., Туринский А.В., Фараон С.І. // Eastern-European Journal of Enterprise Technologies. – Харьков. – 2020. 2/4(104). С. 15-29 Режим доступу: http://journals.uran.ua/eejet/article/view/201418 (фахове видання, Scopus) 2 ум. друк. арк. / 0,2 ум. др. арк. власного внеску. 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. (12,25 ум. др. арк. / 0,4 ум. др. арк. власного внеску) вільний (дата звернення 30.08.2023). (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. Патент на винахід (корисну модель) u 2021 03726 від 30.06.2021 СПОСІБ КРИПТОГРАФІЧНОГО ПЕРЕТВОРЕННЯ ІНФОРМАЦІЇ 2. Патент на винахід (корисну модель) u 2021 03704 від 29.06.2021 СПОСІБ КРИПТОГРАФІЧНОГО ПЕРЕТВОРЕННЯ ІНФОРМАЦІЇ 3. Патент на винахід (корисну модель) u

							2021 03665 від 25.06.2021 СПОСІБ КРИПТОГРАФІЧНОГО ПЕРЕТВОРЕННЯ ІНФОРМАЦІЇ 4. Патент на винахід (корисну модель) u 2021 03617 від 23.06.2021 СПОСІБ КРИПТОГРАФІЧНОГО ПЕРЕТВОРЕННЯ ІНФОРМАЦІЇ 5. Патент на винахід (корисну модель) u 2021 03615 від 23.06.2021 СПОСІБ КРИПТОГРАФІЧНОГО ПЕРЕТВОРЕННЯ ІНФОРМАЦІЇ 6. Патент на винахід (корисну модель) u 2021 03683 від 23.07.2021 СПОСІБ КРИПТОГРАФІЧНОГО ПЕРЕТВОРЕННЯ ІНФОРМАЦІЇ 7. Патент на винахід (корисну модель) u 2021 03680 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. Організація і збереження баз даних: робоча програма навчальної дисципліни для студентів спеціальності 125 “Кібербезпека” першого (бакалаврського) рівня [Електронне видання] / укл. С. В. Мілевський. – Харків : ХНЕУ ім. С. Кузнеця, 2020. – 12 с. Режим доступу: http://www.repository.hneu.edu.ua/handle/123456789/24047 2. Експертні системи: робоча програма навчальної дисципліни для студентів спеціальності 125 «Кібербезпека»

							першого (бакалаврського) рівня / укл. О. В. Мілов, С. В. Мілевський. – Харків : ХНЕУ ім. С. Кузнеця, 2020. – 16 с. (Укр. мовою). Режим доступу: http://www.repository.hneu.edu.ua/handle/123456789/24689 3. Комп'ютерні мережі: робоча програма навчальної дисципліни для студентів спеціальності 121 "Інженерія програмного забезпечення" першого (бакалаврського) рівня [Електронне видання] / укл. С. В. Мілевський. – Х. : Вид. ХНЕУ ім. С. Кузнеця, 2019. – 9 с. (Укр. мов.) Режим доступу: http://www.repository.hneu.edu.ua/handle/123456789/23304 4. Менеджмент інформаційної безпеки: робоча програма навчальної дисципліни для студентів спеціальності 125 "Кібербезпека" першого (бакалаврського) рівня [Електронне видання] / укл. С. В. Мілевський. – Х. : Вид. ХНЕУ ім. С. Кузнеця, 2019. – 9 с. (Укр. мов.) Режим доступу: http://www.repository.hneu.edu.ua/handle/123456789/23305 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 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. 1. Lydia Guryanova, Stanislav Milevskyi, Sergey Razumovskyi Econometric models for evaluating the effectiveness of the financial decentralization mechanisms development // Econometric Research in Finance Workshop 2019, Warsaw School of Economics, Warsaw, Poland, 13.09.2019, pp. 13-14 Режим доступу: https://www.conference.erfin.org/program2019/booklet.pdf (10.10.2021) 2. 2. Milevskyi S.V., Pohasii S.S. Cybersecurity issues in the internet of things // 1st International Conference: Modern Information, Measurement and Control Systems: Problems and Perspectives (MIMCS’2019), 01-02 July, Baku, AZERBAIJAN. – P. 33-34 Режим доступу: https://zenodo.org/record/3783978#.YWP01dpByUk (10.10.2021) 3. 3. Milevskyi S.V., Milov O.V. Requirements for the properties of agents and multi-agent systems in the models of cybersecurity // 1st International Conference: Modern Information, Measurement and Control Systems: Problems and Perspectives (MIMCS’2019), 01-02 July, Baku, AZERBAIJAN. – P. 258-259 Режим доступу: https://zenodo.org/record/3783978#.YWP01dpByUk (10.10.2021) 4. 4. O. Ivahnenko, S. Milevskyi Average Wage Dynamics Modeling In View Of Threshold Effects // Матеріали Міжнародної науково-практичної конференції “Економічний розвиток і спадщина

							Семена Кузнеця": тези доповідей, 30 – 31 травня 2019 р. – Х.: ХНЕУ імені Семена Кузнеця, 2019. – С. 228-229 Режим доступу: http://repository.hneu.edu.ua/handle/123456789/22165 (10.10.2021) 5. S. Milevskyi, S. Pohasii Internet Security Problems Caused By Artificial Intelligence // Матеріали Міжнародної науково-практичної конференції "Економічний розвиток і спадщина Семена Кузнеця": тези доповідей, 30 – 31 травня 2019 р. – Х.: ХНЕУ імені Семена Кузнеця, 2019. – С. 248-249 Режим доступу: http://repository.hneu.edu.ua/handle/123456789/22165 (10.10.2021) П. 13 проведення навчальних занять із спеціальних дисциплін іноземною мовою (крім дисциплін мовної підготовки) в обсязі не менше 50 аудиторних годин на навчальний рік Комп'ютерні системи та архітектура комп'ютерів – 48 годин, освітня програма «Інженерія програмного забезпечення», 2 курс Комп'ютерні мережі – 48 годин, освітня програма «Інженерія програмного забезпечення», 2 курс Організація і збереження баз даних – 72 години, освітня програма «Кібербезпека», 3 курс Табличний процесор MS Excel: просунутий рівень – 90 годин, всі освітні програми, 1 курс 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", свідотство ES № 059

410239	Мілов Олександр Володимирович	Професор, Основне місце роботи	Навчально-науковий інститут комп'ютерних наук та інформаційних технологій	Диплом спеціаліста, Московский ордена Ленина энергетический институт, рік закінчення: 1978, спеціальність: Промышленная электроника, Диплом доктора наук ДД 010482, виданий 26.11.2020, Диплом кандидата наук ТН 094834, виданий 12.11.1986, Атестат доцента ДЦ 039210, виданий 04.07.1991, Атестат професора АП 001430, виданий 16.12.2019	41	Цифрова криміналістика	Підвищення кваліфікації: Центр підтримки академій Cisco Національний технічний університет "Харківський політехнічний інститут". Сертифікат від "30" червня 2021 р. 6 кредитів, Тема: "CCNA CyberOps" та "Network Security". Пункти відповідності ліцензійних умов: п. 1-5, 7, 8, 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. 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. (12,25 ум. др. арк. / 0,7 ум. др. арк. власного внеску) вільний (дата звернення 30.08.2023). (Scopus) 2. Milov O. Development of Niederreiter hybrid crypto-code structure on flawed codes / Yevseiev S., Milov O., Tsyhanenko O., Gavrilova A., Tomashevsky B., Shmatko O. et al.// Eastern-Europe Journal of Enterprise Technologies, 2019, 1(9-97), p. 27-38. - Access mode: http://journals.uran.ua/eejet/article/view/156620 Scopus (1,5 ум.друк.арк./власний внесок 0,15 авторських аркушів). 3. Milov O. Development of scenario modeling of conflict tools in a security system based on formal grammars / Milov O., Yevseiev S., Vlasov A., Herasimov S., Dmitriiev O., Kasianenko M., Pievtsov H., Peleshok Y., Tkach Y., Faraon S. // Eastern-European Journal of Enterprise

							Technologies, 2019, v.9, N 6, p. 53-64. - Access mode: http://journals.uran.ua/eejet/article/view/184274 Scopus (2,5 ум.друк.арк./власний внесок 0,25 авторських аркушів). 4. Milov O.V. Development of methodology for modeling the interaction of antagonistic agents in cybersecurity systems / Milov O., Voitko A., Husarova I., Domaskin O., Ivanchenko E., Ivanchenko I., Korol O., Kots H, Opirskyy I., Fraze-Frazenko O.// Eastern-European Journal of Enterprise Technologies, 2019, v.9, N 2, p. 56-66. - Access mode: http://journals.uran.ua/eejet/article/view/164730. Scopus (2,5 ум.друк.арк./власний внесок 0,25 авторських аркушів). 5. Milov O. Development of a methodology for building an information security system in the corporate research and education system in the context of university autonomy / Yevseiev S., Milov O., Aleksiyev V., Balakireva S., Tyshyk I., Shmatko O. et. al. // Eastern-Europe Journal of Enterprise Technologies, 2019, v. 3, №9 (99), p. 49-63. - Access mode: http://journals.uran.ua/eejet/article/view/169527. Scopus (2,5 ум.друк.арк./власний внесок 0,25 авторських аркушів). 6. Milov O. Development of the model of the antagonistic agents behavior under a cyber conflict / O. Milov, S. Yevseiev, Y. Ivanchenko, S. Milevskyi, O. Nesterov, O. Puchkov, A. Salii, O. Timochko, V. Tiurin, A. Yarovyi // Eastern-Europe Journal of Enterprise Technologies, 2019, v.4, № 9(100). P.6-19. - Access mode: http://journals.uran.ua/eejet/article/view/175978. Scopus (2.5 ум.друк.арк./власний внесок 0,25 авторських аркушів). 7. Milov O.

							Development of the interacting agents behavior scenario in the cyber security system / Milov, O., Yevseiev, S., Aleksiyev, V., Berdnik, P., Voitko, O., Dyptan, V., Ivanchenko, Y., Pavlenko, M., Salii, A., & Yarovyy, S. // Eastern-Europe Journal of Enterprise Technologies, 2019, v.5, № 9(101). P.46-57. - Access mode: http://journals.uran.ua/eejet/article/view/181047. Scopus (2,5 ум.друк.арк./власний внесок 0,25 авторських аркушів).
							8 Milov O. Development of a hardware cryptosystem based on a random number generator with two types of entropy sources Yevseiev, S., Rzayev, K., Laptiev, O., ...Camalova, J., Pohasii, S. Eastern-European Journal of Enterprise Technologiesthis link is disabled, 2022, 5(9-119), pp. 6–16
							9 Milov O. Development of a concept for cybersecurity metrics classificatioN Yevseiev, S., Milov, O., Opirskyy, I., ...Melenti, Y., Tomashevsky, B. Eastern-European Journal of Enterprise Technologiesthis link is disabled, 2022, 4(4-118), pp. 6-18
							10 Milov O. Development of crypto-code constructs based on LDPC codes / Pohasii, S., Yevseiev, S., Zhuchenko, O., ...Lezik, A., Susukailo, V. Eastern-European Journal of Enterprise Technologiesthis link is disabled, 2022, 2(9-116), pp. 44–59
							11 Milov O. Development of a modification of the method for constructing energy-efficient sensor networks using static and dynamic sensors / Petrivskyi, V., Shevchenko, V., Yevseiev, S., ...Kurchenko, O., Opirskyy, I. Eastern-European Journal of Enterprise Technologiesthis link is disabled, 2022, 1(9-115), pp. 15–23
							12 Milov O. Situational

							Control of Cyber Security in Socio-Cyber-Physical Systems / Milov, O., Khvostenko, V., Natalia, V., Korol, O., Zviertseva, N. HORA 2022 - 4th International Congress on Human-Computer Interaction, Optimization and Robotic Applications, Proceedings, 2022 13 Milov O., Yevseiev, S., Zviertseva, N., Zviertsev, H., Motalyhin, Y. Pseudo-Physical Logics in Control of Cyber Security Systems. ISMSIT 2022 - 6th International Symposium on Multidisciplinary Studies and Innovative Technologies, Proceedings, 2022, pp. 1038–1042 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. Патент на винахід (корисну модель) u 2021 03726 від 30.06.2021 СПОСІБ КРИПТОГРАФІЧНОГО ПЕРЕТВОРЕННЯ ІНФОРМАЦІЇ 2. Патент на винахід (корисну модель) u 2021 03704 від 29.06.2021 СПОСІБ КРИПТОГРАФІЧНОГО ПЕРЕТВОРЕННЯ ІНФОРМАЦІЇ 3. Патент на винахід (корисну модель) u 2021 03665 від 25.06.2021 СПОСІБ КРИПТОГРАФІЧНОГО ПЕРЕТВОРЕННЯ ІНФОРМАЦІЇ 4. Патент на винахід (корисну модель) u 2021 03617 від 23.06.2021 СПОСІБ КРИПТОГРАФІЧНОГО ПЕРЕТВОРЕННЯ ІНФОРМАЦІЇ 5. Патент на винахід (корисну модель) u 2021 03615 від 23.06.2021 СПОСІБ КРИПТОГРАФІЧНОГО ПЕРЕТВОРЕННЯ ІНФОРМАЦІЇ 6. Патент на винахід (корисну модель) u 2021 03683 від 23.07.2021 СПОСІБ КРИПТОГРАФІЧНОГО ПЕРЕТВОРЕННЯ ІНФОРМАЦІЇ

							7. Патент на винахід (корисну модель) u 2021 03680 від 25.06.2021 СПОСІБ КРИПТОГРАФІЧНОГО ПЕРЕТВОРЕННЯ ІНФОРМАЦІЇ 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) Лабораторний практикум з основ криптографічного захисту [Електронний ресурс] : навч. посіб. / С. П. Євсеєв, О. В. Мілов, О. Г. Король ; Харківський національний економічний університет ім. С. Кузнеця. - Електрон. текстові дан. (221 с. / 12,3 МБ). - Харків : ХНЕУ ім. С. Кузнеця, 2020. Режим доступу: http://repository.hneu.edu.ua/handle/123456789/24508. 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. Лабораторний практикум з основ криптографічного захисту [Електронний ресурс] : навч. посіб. / С. П. Євсеєв, О. В. Мілов, О. Г. Король ; Харківський національний економічний університет ім. С. Кузнеця. - Електрон. текстові дан. (221 с. / 12,3 МБ). - Харків : ХНЕУ ім. С. Кузнеця, 2020. Режим доступу: http://repository.hneu.edu.ua/handle/123456789/24508.

							РПНД: 1. Математичні основи криптології: робоча програма навчальної дисципліни для студентів спеціальності 125 “Кібербезпека” першого (бакалаврського) рівня [Електронне видання] / укл. О. В. Мілов. – Х. : Вид. ХНЕУ ім. С. Кузнеця, 2019. (Укр. мов.) http://www.repository.hneu.edu.ua/handle/123456789/23311 2. Інтелектуальний аналіз даних: робоча програма навчальної дисципліни для студентів спеціальності 125 “Кібербезпека” другого (магістерського) рівня [Електронне видання] / укл. О. В. Мілов – Х. : Вид. ХНЕУ ім. С. Кузнеця, 2019. (Укр. мов.) http://www.repository.hneu.edu.ua/handle/123456789/22419 3. Ризик-менеджмент: робоча програма навчальної дисципліни для студентів спеціальності 125 “Кібербезпека” другого (магістерського) рівня [Електронне видання] / укл. О. В. Мілов. – Х. : Вид. ХНЕУ ім. С. Кузнеця, 2019. (Укр. мов.) http://www.repository.hneu.edu.ua/handle/123456789/22423 4. Тестування на проникнення та етичний хакінг: робоча програма навчальної дисципліни для студентів спеціальності 125 Кібербезпека другого (магістерського) рівня [Електронне видання] / укл. О. В. Мілов. – Харків : ХНЕУ ім. С. Кузнеця, 2020. http://www.repository.hneu.edu.ua/handle/123456789/24051 5. Основи криптографічного захисту: робоча програма навчальної дисципліни для студентів спеціальності 125 “Кібербезпека” першого (бакалаврського) рівня [Електронне видання] / укл. О. В.

							Мілов – Харків : ХНЕУ ім. С. Кузнеця, 2020. http://www.repository.hneu.edu.ua/handle/123456789/24048 П. 5 захист дисертації на здобуття наукового ступеня. Доктор технічних наук, 05.13.21. Системи захисту інформації, тема дисертації: Методологія моделювання процесів поведінки антагоністичних агентів в системах безпеки. Диплом ДД №010482 від 26 листопада 2020 року, Міністерство Освіти та 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 Член спеціалізованої вченої ради Д 26.861.06 з присудження наукового ступеня доктора наук за спеціальністю 05.13.21 «Системи захисту інформації» 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 Керівник НДР ХНЕУ ім. С.Кузнеця «Методологія моделювання взаємодії агентів в системах безпеки» за номер державної реєстрації № 0119U103117. П. 10 участь у міжнародних

							наукових та/або освітніх проектах, залучення до міжнародної експертизи, наявність звання “суддя міжнародної категорії” Участь у Cybersecurity Summer Training Program under the USAID Project “Cybersecurity for Critical Infrastructure in Ukraine” 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. Milov O. Self-organizing organizational structures of cybersecurity systems // Modern Problems Of Computer Science And IT-Education : collective monograph / [editorial board K. Melnyk, O. Shmatko]. – Vienna : Premier Publishing s.r.o., 2020. – 236 p. – URL: http://repository.hneu.edu.ua/bitstream/123456789/23495/1/%d0%90%d0%b2%d1%81%d1%82%d1%80%d0%b8%d1%8f_%d0%9c%d0%b8%d0%bb%d0%be%d0%b2_%d0%a0%d0%b5%d0%bf%d0%be%d0%b7%d0%b8%d1%82%d0%b0%d1%80%d0%b8%d0%b9.pdf (дата звернення 12.10.2021 р.) 2. Milov O. Adaptive decision support systems for cyber security / O. Milov // Сучасні інформаційні системи. - 2019. - Т. 3, № 1. - С. 131-135. - – URL: http://nbuv.gov.ua/UJRN/adinsys_2019_3_1_24. (дата звернення 12.10.2021 р.) 3. Milov O. V. Development of basic principles for corporate planning / Milevsky S. V., Korol O. H. // Системи обробки інформації. – 2019, випуск 1 (156). С. 28-36. - – URL: https://doi.org/10.30748/soi.2019.156.04. (дата звернення 12.10.2021 р.)

							4. Milov O. Mechanisms of cyber security: The Problem of Conceptualization / Milov O., Kazakova N., Milczarski P., Korol O. // Безпека інформації. – 2019, vol. 25, issue 3. – P. 110–116. DOI: 10.18372/2225-5036.25.13841. – URL: https://www.researchgate.net/publication/337114411_Mechanisms_of_cyber_security_the_problem_of_conceptualization. (дата звернення 12.10.2021 р.) 5. Milov O. Simulation of a distributed decision-making system in cyber security / Milov O., Milevskyi S., Aleksiyev V. // International Journal of 3D Printing Technologies and Digital Industry. – 2019, 3:2(2019), – P. 147-152. – URL: https://dergipark.org.tr/tr/download/article-file/797288. (дата звернення 12.10.2021 р.) 6. Yevseiev, S., Hryshchuk, R., Molodetska, K., Nazarkevych, M., Hrytsyk, V., Milov, O. et. al.; (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 7. Synergy of building cybersecurity systems / Yevseiev, S., Ponomarenko, V., Laptiev, O., MilovO., ..., Florov, S. Synergy of building cybersecurity systems, 2021, pp. 1–175 П. 13 проведення навчальних занять із спеціальних дисциплін іноземною мовою (крім дисциплін мовної підготовки) в обсязі не менше 50 аудиторних годин на навчальний рік. 2019-2020 н. р.: 1.Програмування (121.017-А (БЕР.2019). лекції - 32, лаб. роб. - 32; 2.КОМП'ЮТЕРНІ СИСТЕМИ ТА АРХІТЕКТУРА КОМП'ЮТЕРІВ (121.010-А) лаб. роб. - 22; 3.ДАНІ ТА

							ПРИЙНЯТТЯ РІШЕНЬ (122.010-БАІСП (Словацька програма) лекції -20, лаб. роб. - 20. П. 19 діяльність за спеціальністю у формі участі у професійних та/або громадських об'єднаннях Член громадської організації "Східноєвропейське наукове товариство", свідотство ES № 060

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**
РН1. Вільно спілкуватись державною та іноземною мовами, усно і письмово для представлення і обговорення результатів досліджень та інновацій, забезпечення бізнес\операційних процесів та питань професійної діяльності в галузі інформаційної безпеки та/або кібербезпеки. *РН2. Інтегрувати фундаментальні та спеціальні знання для розв'язування складних задач інформаційної безпеки та/або кібербезпеки у широких або мультидисциплінарних контекстах.* *РН3. Провадити дослідницьку та/або інноваційну діяльність в сфері інформаційної безпеки та/або кібербезпеки, а також в сфері технічного та криптографічного захисту інформації у кіберпросторі.* *РН4. Застосовувати, інтегрувати,*	☒	Презентація та обробка знань	Пояснювально-ілюстративний (інформаційно-рецептивний) та репродуктивний	Опитування на лекційних заняттях, тестування, презентації докладів за темами лекційних занять, захист лабораторних робіт, проведення контрольних робіт, залік

розробляти, впроваджувати та удосконалювати сучасні інформаційні технології, фізичні та математичні методи і моделі в сфері інформаційної безпеки та/або кібербезпеки. *РН6. Аналізувати та оцінювати захищеність систем, комплексів та засобів кіберзахисту, технології створення та використання спеціалізованого програмного забезпечення.* *РН10. Забезпечувати безперервність бізнес/операційних процесів, а також виявляти уразливості інформаційних систем та ресурсів, аналізувати та оцінювати ризики для інформаційної безпеки та/або кібербезпеки організації.* *РН11. Аналізувати, контролювати та забезпечувати ефективне функціонування системи управління доступом до інформаційних ресурсів відповідно до встановлених стратегії і політики інформаційної безпеки та/або кібербезпеки організації.* *РН16. Приймати обґрунтовані рішення з організаційно-технічних питань інформаційної безпеки та/або кібербезпеки у складних і непередбачуваних умовах, у тому числі із застосуванням сучасних методів та засобів оптимізації, прогнозування та прийняття рішень.* *РН19. Обирати, аналізувати і розробляти придатні типові аналітичні, розрахункові та*					

експериментальні методи кіберзахисту, розробляти, реалізовувати та супроводжувати проекти з захисту інформації у кіберпросторі, інноваційної діяльності та захисту інтелектуальної власності. *РН20. Ставити та вирішувати складні інженерно-прикладні та наукові задачі інформаційної безпеки та/або кібербезпеки з урахуванням вимог вітчизняних та світових стандартів та кращих практик.* *РН21. Використовувати методи натурного, фізичного і комп'ютерного моделювання для дослідження процесів, які стосуються інформаційної безпеки та/або кібербезпеки.* *РН22. Планувати та виконувати експериментальні і теоретичні дослідження, висувати і перевіряти гіпотези, обирати для цього придатні методи та інструменти, здійснювати статистичну обробку даних, оцінювати достовірність результатів досліджень, аргументувати висновки.* *РН23. Обґрунтовувати вибір програмного забезпечення, устаткування та інструментів, інженерних технологій і процесів, а також обмежень щодо них в галузі інформаційної безпеки та/або кібербезпеки на основі сучасних знань у суміжних галузях, наукової, технічної та довідкової літератури та іншої доступної інформації.*				

РН-1 Вільно спілкуватись державною та іноземною мовами, усно і письмово для представлення і обговорення результатів досліджень та інновацій, забезпечення бізнес\операційних процесів та питань професійної діяльності в галузі інформаційної безпеки та/або кібербезпеки. *РН-3 Провадити дослідницьку та/або інноваційну діяльність в сфері інформаційної безпеки та/або кібербезпеки, а також в сфері технічного та криптографічного захисту інформації у кіберпросторі.* *РН-4 Застосовувати, інтегрувати, розробляти, впроваджувати та удосконалювати сучасні інформаційні технології, фізичні та математичні методи і моделі в сфері інформаційної безпеки та/або кібербезпеки.* *РН-6 Аналізувати та оцінювати захищеність систем, комплексів та засобів кіберзахисту, технології створення та використання спеціалізованого програмного забезпечення.* *РН-7 Обґрунтовувати використання, впроваджувати та аналізувати кращі світові стандарти, практики з метою розв'язання складних задач професійної діяльності в галузі інформаційної безпеки та/або кібербезпеки.* *РН-8 Досліджувати, розробляти і супроводжувати системи та засоби інформаційної безпеки та/або кібербезпеки на об'єктах інформаційної*	☒	Господарське право	Пояснювально-ілюстративний (інформаційно-рецептивний) та репродуктивний	Опитування на лекційних заняттях, тестування, презентації докладів за темами лекційних занять, перевірка практичних завдань, проведення контрольних робіт, залік

діяльності та критичної інфраструктури. *РН-9 Аналізувати, розробляти і супроводжувати систему управління інформаційною безпекою та/або кібербезпекою організації на базі стратегії і політики інформаційної безпеки.* *РН-10 Забезпечувати безперервність бізнес/операційних процесів, а також виявляти уразливості інформаційних систем та ресурсів, аналізувати та оцінювати ризики для інформаційної безпеки та/або кібербезпеки організації.* *РН-11 Аналізувати, контролювати та забезпечувати ефективне функціонування системи управління доступом до інформаційних ресурсів відповідно до встановлених стратегії і політики інформаційної безпеки та/або кібербезпеки організації* *РН-12 Досліджувати, розробляти та впроваджувати методи і заходи протидії кіберінцидентам, здійснювати процедури управління, контролю та розслідування, а також надавати рекомендації щодо попередження та аналізу кіберінцидентів в цілому* *РН-13 Досліджувати, розробляти, впроваджувати та використовувати методи та засоби криптографічного та технічного захисту інформації бізнес/операційних процесів, а також аналізувати і надавати оцінку ефективності їх*					

використання в інформаційних системах, на об'єктах інформаційної діяльності та критичної інфраструктури. *РН-14 Аналізувати, розробляти і супроводжувати систему аудиту та моніторингу ефективності функціонування інформаційних систем і технологій, бізнес\операційних процесів у сфері інформаційної та\або кібербезпеки в цілому.* *РН-16 Приймати обґрунтовані рішення з організаційно-технічних питань інформаційної безпеки та/або кібербезпеки у складних і непередбачуваних умовах, у тому числі із застосуванням сучасних методів та засобів оптимізації, прогнозування та прийняття рішень.* *РН-18 Планувати навчання, а також супроводжувати та контролювати роботу з персоналом у напряму інформаційної безпеки та/або кібербезпеки.* *РН-19 Обирати, аналізувати і розробляти придатні типові аналітичні, розрахункові та експериментальні методи кіберзахисту, розробляти, реалізовувати та супроводжувати проекти з захисту інформації у кіберпросторі, інноваційної діяльності та захисту інтелектуальної власності.* *РН-20 Ставити та вирішувати складні інженерно-прикладні та наукові задачі інформаційної безпеки та/або кібербезпеки з урахуванням вимог*					

вітчизняних та світових стандартів та кращих практик *РН-21 Використовувати методи натурного, фізичного і комп'ютерного моделювання для дослідження процесів, які стосуються інформаційної безпеки та/або кібербезпеки.* *РН-23 Обґрунтовувати вибір програмного забезпечення, устаткування та інструментів, інженерних технологій і процесів, а також обмежень щодо них в галузі інформаційної безпеки та/або кібербезпеки на основі сучасних знань у суміжних галузях, наукової, технічної та довідкової літератури та іншої доступної інформації.*				
РН-1 Вільно спілкуватись державною та іноземною мовами, усно і письмово для представлення і обговорення результатів досліджень та інновацій, забезпечення бізнес\операційних процесів та питань професійної діяльності в галузі інформаційної безпеки та/або кібербезпеки. *РН-3 Провадити дослідницьку та/або інноваційну діяльність в сфері інформаційної безпеки та/або кібербезпеки, а також в сфері технічного та криптографічного захисту інформації у кіберпросторі.* *РН-4 Застосовувати, інтегрувати, розробляти, впроваджувати та удосконалювати сучасні інформаційні технології, фізичні та математичні методи і моделі в*	☒	Інноваційне підприємництво та управління стартап проектами	Пояснювально-ілюстративний (інформаційно-рецептивний) та репродуктивний	Опитування на лекційних заняттях, тестування, презентації докладів за темами лекційних занять, перевірка практичних завдань, проведення контрольних робіт, іспит

сфері інформаційної безпеки та/або кібербезпеки. *РН-6 Аналізувати та оцінювати захищеність систем, комплексів та засобів кіберзахисту, технології створення та використання спеціалізованого програмного забезпечення.* *РН-7 Обґрунтовувати використання, впроваджувати та аналізувати кращі світові стандарти, практики з метою розв'язання складних задач професійної діяльності в галузі інформаційної безпеки та/або кібербезпеки.* *РН-8 Досліджувати, розробляти і супроводжувати системи та засоби інформаційної безпеки та/або кібербезпеки на об'єктах інформаційної діяльності та критичної інфраструктури.* *РН-9 Аналізувати, розробляти і супроводжувати систему управління інформаційною безпекою та/або кібербезпекою організації на базі стратегії і політики інформаційної безпеки.* *РН-10 Забезпечувати безперервність бізнес/операційних процесів, а також виявляти уразливості інформаційних систем та ресурсів, аналізувати та оцінювати ризики для інформаційної безпеки та/або кібербезпеки організації.* *РН-11 Аналізувати, контролювати та забезпечувати ефективне функціонування системи управління доступом до інформаційних*					

ресурсів відповідно до встановлених стратегії і політики інформаційної безпеки та/або кібербезпеки організації *РН-12 Досліджувати, розробляти та впроваджувати методи і заходи протидії кіберінцидентам, здійснювати процедури управління, контролю та розслідування, а також надавати рекомендації щодо попередження та аналізу кіберінцидентів в цілому* *РН-13 Досліджувати, розробляти, впроваджувати та використовувати методи та засоби криптографічного та технічного захисту інформації бізнес/операційних процесів, а також аналізувати і надавати оцінку ефективності їх використання в інформаційних системах, на об'єктах інформаційної діяльності та критичної інфраструктури.* *РН-14 Аналізувати, розробляти і супроводжувати систему аудиту та моніторингу ефективності функціонування інформаційних систем і технологій, бізнес\операційних процесів у сфері інформаційної та\або кібербезпеки в цілому.* *РН-16 Приймати обґрунтовані рішення з організаційно-технічних питань інформаційної безпеки та/або кібербезпеки у складних і непередбачуваних умовах, у тому числі із застосуванням сучасних методів та засобів оптимізації, прогнозування та*					

прийняття рішень. *РН-18 Планувати навчання, а також супроводжувати та контролювати роботу з персоналом у напряму інформаційної безпеки та/або кібербезпеки.* *РН-19 Обирати, аналізувати і розробляти придатні типові аналітичні, розрахункові та експериментальні методи кіберзахисту, розробляти, реалізовувати та супроводжувати проекти з захисту інформації у кіберпросторі, інноваційної діяльності та захисту інтелектуальної власності.* *РН-20 Ставити та вирішувати складні інженерно-прикладні та наукові задачі інформаційної безпеки та/або кібербезпеки з урахуванням вимог вітчизняних та світових стандартів та кращих практик* *РН-21 Використовувати методи натурного, фізичного і комп'ютерного моделювання для дослідження процесів, які стосуються інформаційної безпеки та/або кібербезпеки.* *РН-23 Обґрунтовувати вибір програмного забезпечення, устаткування та інструментів, інженерних технологій і процесів, а також обмежень щодо них в галузі інформаційної безпеки та/або кібербезпеки на основі сучасних знань у суміжних галузях, наукової, технічної та довідкової літератури та іншої доступної інформації.*				
РН1. Вільно спілкуватись	☒	Англійська мова	Пояснювально-ілюстративний	Тестування, презентації докладів за темами занять,

державною та іноземною мовами, усно і письмово для представлення і обговорення результатів досліджень та інновацій, забезпечення бізнес\операційних процесів та питань професійної діяльності в галузі інформаційної безпеки та/або кібербезпеки. *РН2. Інтегрувати фундаментальні та спеціальні знання для розв'язування складних задач інформаційної безпеки та/або кібербезпеки у широких або мультидисциплінарних контекстах.* *РН3. Провадити дослідницьку та/або інноваційну діяльність в сфері інформаційної безпеки та/або кібербезпеки, а також в сфері технічного та криптографічного захисту інформації у кіберпросторі.* *РН4. Застосовувати, інтегрувати, розробляти, впроваджувати та удосконалювати сучасні інформаційні технології, фізичні та математичні методи і моделі в сфері інформаційної безпеки та/або кібербезпеки.* *РН5. Критично осмислювати проблеми інформаційної безпеки та/або кібербезпеки, у тому числі на міжгалузевому та міждисциплінарному рівні, зокрема на основі розуміння нових результатів інженерних і фізико-математичних наук, а також розвитку технологій створення та використання спеціалізованого програмного забезпечення.* *РН6. Аналізувати та оцінювати захищеність*			(інформаційно-рецептивний) та репродуктивний	перевірка практичних завдань, проведення контрольних робіт, іспит

систем, комплексів та засобів кіберзахисту, технології створення та використання спеціалізованого програмного забезпечення. *РН7. Обґрунтовувати використання, впроваджувати та аналізувати кращі світові стандарти, практики з метою розв'язання складних задач професійної діяльності в галузі інформаційної безпеки та/або кібербезпеки.* *РН8. Досліджувати, розробляти і супроводжувати системи та засоби інформаційної безпеки та/або кібербезпеки на об'єктах інформаційної діяльності та критичної інфраструктури.* *РН9. Аналізувати, розробляти і супроводжувати систему управління інформаційною безпекою та/або кібербезпекою організації на базі стратегії і політики інформаційної безпеки.* *РН10. Забезпечувати безперервність бізнес/операційних процесів, а також виявляти уразливості інформаційних систем та ресурсів, аналізувати та оцінювати ризики для інформаційної безпеки та/або кібербезпеки організації.* *РН11. Аналізувати, контролювати та забезпечувати ефективне функціонування системи управління доступом до інформаційних ресурсів відповідно до встановлених стратегії і політики інформаційної безпеки та/або кібербезпеки*					

організації. *РН12. Досліджувати, розробляти та впроваджувати методи і заходи протидії кіберінцидентам, здійснювати процедури управління, контролю та розслідування, а також надавати рекомендації щодо попередження та аналізу кіберінцидентів в цілому.* *РН13. Досліджувати, розробляти, впроваджувати та використовувати методи та засоби криптографічного та технічного захисту інформації бізнес/операційних процесів, а також аналізувати і надавати оцінку ефективності їх використання в інформаційних системах, на об'єктах інформаційної діяльності та критичної інфраструктури.* *РН14. Аналізувати, розробляти і супроводжувати систему аудиту та моніторингу ефективності функціонування інформаційних систем і технологій, бізнес\операційних процесів у сфері інформаційної та\або кібербезпеки в цілому.* *РН15. Зрозуміло і недвозначно доносити власні висновки з проблем інформаційної безпеки та/або кібербезпеки, а також знання та пояснення, що їх обґрунтовують до персоналу, партнерів та інших осіб.* *РН16. Приймати обґрунтовані рішення з організаційно-технічних питань інформаційної безпеки та/або кібербезпеки у складних і непередбачуваних умовах, у тому*					

числі із застосуванням сучасних методів та засобів оптимізації, прогнозування та прийняття рішень. *РН17. Мати навички автономного і самостійного навчання у сфері інформаційної безпеки та/або кібербезпеки і дотичних галузей знань, аналізувати власні освітні потреби та об'єктивно оцінювати результати навчання.* *РН18. Планувати навчання, а також супроводжувати та контролювати роботу з персоналом у напряму інформаційної безпеки та/або кібербезпеки.* *РН19. Обирати, аналізувати і розробляти придатні типові аналітичні, розрахункові та експериментальні методи кіберзахисту, розробляти, реалізовувати та супроводжувати проекти з захисту інформації у кіберпросторі, інноваційної діяльності та захисту інтелектуальної власності.* *РН20. Ставити та вирішувати складні інженерно-прикладні та наукові задачі інформаційної безпеки та/або кібербезпеки з урахуванням вимог вітчизняних та світових стандартів та кращих практик.* *РН21. Використовувати методи натурного, фізичного і комп'ютерного моделювання для дослідження процесів, які стосуються інформаційної безпеки та/або кібербезпеки.* *РН22. Планувати та виконувати експериментальні і*					

теоретичні дослідження, висувати і перевіряти гіпотези, обирати для цього придатні методи та інструменти, здійснювати статистичну обробку даних, оцінювати достовірність результатів досліджень, аргументувати висновки. *РН23. Обґрунтовувати вибір програмного забезпечення, устаткування та інструментів, інженерних технологій і процесів, а також обмежень щодо них в галузі інформаційної безпеки та/або кібербезпеки на основі сучасних знань у суміжних галузях, наукової, технічної та довідкової літератури та іншої доступної інформації.*				
РН2. Інтегрувати фундаментальні та спеціальні знання для розв'язування складних задач інформаційної безпеки та/або кібербезпеки у широких або мультидисциплінарних контекстах. *РН4. Застосовувати, інтегрувати, розробляти, впроваджувати та удосконалювати сучасні інформаційні технології, фізичні та математичні методи і моделі в сфері інформаційної безпеки та/або кібербезпеки.* *РН5. Критично осмислювати проблеми інформаційної безпеки та/або кібербезпеки, у тому числі на міжгалузевому та міждисциплінарному рівні, зокрема на основі розуміння нових результатів інженерних і фізико-*	☒	Захист інтелектуальної власності	Пояснювально-ілюстративний (інформаційно-рецептивний) та репродуктивний	Опитування на лекційних заняттях, тестування, презентації докладів за темами лекційних занять, перевірка практичних завдань, проведення контрольних робіт, виконання курсового проєкту, залік

математичних наук, а також розвитку технологій створення та використання спеціалізованого програмного забезпечення. *РН7. Обґрунтовувати використання, впроваджувати та аналізувати кращі світові стандарти, практики з метою розв'язання складних задач професійної діяльності в галузі інформаційної безпеки та/або кібербезпеки.* *РН8. Досліджувати, розробляти і супроводжувати системи та засоби інформаційної безпеки та/або кібербезпеки на об'єктах інформаційної діяльності та критичної інфраструктури.* *РН9. Аналізувати, розробляти і супроводжувати систему управління інформаційною безпекою та/або кібербезпекою організації на базі стратегії і політики інформаційної безпеки.* *РН12. Досліджувати, розробляти та впроваджувати методи і заходи протидії кіберінцидентам, здійснювати процедури управління, контролю та розслідування, а також надавати рекомендації щодо попередження та аналізу кіберінцидентів в цілому.* *РН14. Аналізувати, розробляти і супроводжувати систему аудиту та моніторингу ефективності функціонування інформаційних систем і технологій, бізнес\операційних процесів у сфері інформаційної та\або*					

кібербезпеки в цілому. *РН15. Зрозуміло і недвозначно доносити власні висновки з проблем інформаційної безпеки та/або кібербезпеки, а також знання та пояснення, що їх обґрунтовують до персоналу, партнерів та інших осіб.* *РН16. Приймати обґрунтовані рішення з організаційно-технічних питань інформаційної безпеки та/або кібербезпеки у складних і непередбачуваних умовах, у тому числі із застосуванням сучасних методів та засобів оптимізації, прогнозування та прийняття рішень.* *РН18. Планувати навчання, а також супроводжувати та контролювати роботу з персоналом у напряму інформаційної безпеки та/або кібербезпеки.* *РН19. Обирати, аналізувати і розробляти придатні типові аналітичні, розрахункові та експериментальні методи кіберзахисту, розробляти, реалізовувати та супроводжувати проекти з захисту інформації у кіберпросторі, інноваційної діяльності та захисту інтелектуальної власності.* *РН20. Ставити та вирішувати складні інженерно-прикладні та наукові задачі інформаційної безпеки та/або кібербезпеки з урахуванням вимог вітчизняних та світових стандартів та кращих практик.* *РН23. Обґрунтовувати вибір програмного забезпечення, устаткування та*					

інструментів, інженерних технологій і процесів, а також обмежень щодо них в галузі інформаційної безпеки та/або кібербезпеки на основі сучасних знань у суміжних галузях, наукової, технічної та довідкової літератури та іншої доступної інформації.				
РН1. Вільно спілкуватись державною та іноземною мовами, усно і письмово для представлення і обговорення результатів досліджень та інновацій, забезпечення бізнес\операційних процесів та питань професійної діяльності в галузі інформаційної безпеки та/або кібербезпеки. *РН2. Інтегрувати фундаментальні та спеціальні знання для розв'язування складних задач інформаційної безпеки та/або кібербезпеки у широких або мультидисциплінарних контекстах.* *РН3. Провадити дослідницьку та/або інноваційну діяльність в сфері інформаційної безпеки та/або кібербезпеки, а також в сфері технічного та криптографічного захисту інформації у кіберпросторі.* *РН4. Застосовувати, інтегрувати, розробляти, впроваджувати та удосконалювати сучасні інформаційні технології, фізичні та математичні методи і моделі в сфері інформаційної безпеки та/або кібербезпеки.* *РН5. Критично осмислювати проблеми інформаційної безпеки та/або кібербезпеки, у*	☒	Технології управління безпекою бізнес-процесів	Пояснювально-ілюстративний (інформаційно-рецептивний) та репродуктивний	Опитування на лекційних заняттях, тестування, презентації докладів за темами лекційних занять, захист лабораторних робіт, проведення контрольних робіт, залік

тому числі на міжгалузевому та міждисциплінарному рівні, зокрема на основі розуміння нових результатів інженерних і фізико-математичних наук, а також розвитку технологій створення та використання спеціалізованого програмного забезпечення. *РН6. Аналізувати та оцінювати захищеність систем, комплексів та засобів кіберзахисту, технології створення та використання спеціалізованого програмного забезпечення.* *РН7. Обґрунтовувати використання, впроваджувати та аналізувати кращі світові стандарти, практики з метою розв'язання складних задач професійної діяльності в галузі інформаційної безпеки та/або кібербезпеки.* *РН8. Досліджувати, розробляти і супроводжувати системи та засоби інформаційної безпеки та/або кібербезпеки на об'єктах інформаційної діяльності та критичної інфраструктури.* *РН9. Аналізувати, розробляти і супроводжувати систему управління інформаційною безпекою та/або кібербезпекою організації на базі стратегії і політики інформаційної безпеки.* *РН10. Забезпечувати безперервність бізнес/операційних процесів, а також виявляти уразливості інформаційних систем та ресурсів, аналізувати та оцінювати ризики*					

для інформаційної безпеки та/або кібербезпеки організації. *РН11. Аналізувати, контролювати та забезпечувати ефективне функціонування системи управління доступом до інформаційних ресурсів відповідно до встановлених стратегії і політики інформаційної безпеки та/або кібербезпеки організації.* *РН12. Досліджувати, розробляти та впроваджувати методи і заходи протидії кіберінцидентам, здійснювати процедури управління, контролю та розслідування, а також надавати рекомендації щодо попередження та аналізу кіберінцидентів в цілому.* *РН13. Досліджувати, розробляти, впроваджувати та використовувати методи та засоби криптографічного та технічного захисту інформації бізнес/операційних процесів, а також аналізувати і надавати оцінку ефективності їх використання в інформаційних системах, на об'єктах інформаційної діяльності та критичної інфраструктури.* *РН14. Аналізувати, розробляти і супроводжувати систему аудиту та моніторингу ефективності функціонування інформаційних систем і технологій, бізнес\операційних процесів у сфері інформаційної та\або кібербезпеки в цілому.* *РН15. Зрозуміло і недвозначно доносити власні висновки з проблем*					

інформаційної безпеки та/або кібербезпеки, а також знання та пояснення, що їх обґрунтовують до персоналу, партнерів та інших осіб. *РН16. Приймати обґрунтовані рішення з організаційно-технічних питань інформаційної безпеки та/або кібербезпеки у складних і непередбачуваних умовах, у тому числі із застосуванням сучасних методів та засобів оптимізації, прогнозування та прийняття рішень.* *РН17. Мати навички автономного і самостійного навчання у сфері інформаційної безпеки та/або кібербезпеки і дотичних галузей знань, аналізувати власні освітні потреби та об'єктивно оцінювати результати навчання.* *РН18. Планувати навчання, а також супроводжувати та контролювати роботу з персоналом у напряму інформаційної безпеки та/або кібербезпеки.* *РН19. Обирати, аналізувати і розробляти придатні типові аналітичні, розрахункові та експериментальні методи кіберзахисту, розробляти, реалізовувати та супроводжувати проекти з захисту інформації у кіберпросторі, інноваційної діяльності та захисту інтелектуальної власності.* *РН20. Ставити та вирішувати складні інженерно-прикладні та наукові задачі інформаційної безпеки та/або кібербезпеки з*					

урахуванням вимог вітчизняних та світових стандартів та кращих практик. *РН21. Використовувати методи натурного, фізичного і комп'ютерного моделювання для дослідження процесів, які стосуються інформаційної безпеки та/або кібербезпеки.* *РН22. Планувати та виконувати експериментальні і теоретичні дослідження, висувати і перевіряти гіпотези, обирати для цього придатні методи та інструменти, здійснювати статистичну обробку даних, оцінювати достовірність результатів досліджень, аргументувати висновки.* *РН23. Обґрунтовувати вибір програмного забезпечення, устаткування та інструментів, інженерних технологій і процесів, а також обмежень щодо них в галузі інформаційної безпеки та/або кібербезпеки на основі сучасних знань у суміжних галузях, наукової, технічної та довідкової літератури та іншої доступної інформації.*				
РН1. Вільно спілкуватись державною та іноземною мовами, усно і письмово для представлення і обговорення результатів досліджень та інновацій, забезпечення бізнес\операційних процесів та питань професійної діяльності в галузі інформаційної безпеки та/або кібербезпеки. *РН2. Інтегрувати фундаментальні та спеціальні знання для*	☒	Розширена мережева та хмарна безпека	Пояснювально-ілюстративний (інформаційно-рецептивний) та репродуктивний	Опитування на лекційних заняттях, тестування, презентації докладів за темами лекційних занять, захист лабораторних робіт, проведення контрольних робіт, іспит

розв'язування складних задач інформаційної безпеки та/або кібербезпеки у широких або мультидисциплінарних контекстах. *РН3. Провадити дослідницьку та/або інноваційну діяльність в сфері інформаційної безпеки та/або кібербезпеки, а також в сфері технічного та криптографічного захисту інформації у кіберпросторі.* *РН4. Застосовувати, інтегрувати, розробляти, впроваджувати та удосконалювати сучасні інформаційні технології, фізичні та математичні методи і моделі в сфері інформаційної безпеки та/або кібербезпеки.* *РН5. Критично осмислювати проблеми інформаційної безпеки та/або кібербезпеки, у тому числі на міжгалузевому та міждисциплінарному рівні, зокрема на основі розуміння нових результатів інженерних і фізико-математичних наук, а також розвитку технологій створення та використання спеціалізованого програмного забезпечення.* *РН6. Аналізувати та оцінювати захищеність систем, комплексів та засобів кіберзахисту, технології створення та використання спеціалізованого програмного забезпечення.* *РН7. Обґрунтовувати використання, впроваджувати та аналізувати кращі світові стандарти, практики з метою розв'язання складних задач професійної діяльності в галузі*					

інформаційної безпеки та/або кібербезпеки. *РН8. Досліджувати, розробляти і супроводжувати системи та засоби інформаційної безпеки та/або кібербезпеки на об'єктах інформаційної діяльності та критичної інфраструктури.* *РН9. Аналізувати, розробляти і супроводжувати систему управління інформаційною безпекою та/або кібербезпекою організації на базі стратегії і політики інформаційної безпеки.* *РН10. Забезпечувати безперервність бізнес/операційних процесів, а також виявляти уразливості інформаційних систем та ресурсів, аналізувати та оцінювати ризики для інформаційної безпеки та/або кібербезпеки організації.* *РН11. Аналізувати, контролювати та забезпечувати ефективне функціонування системи управління доступом до інформаційних ресурсів відповідно до встановлених стратегії і політики інформаційної безпеки та/або кібербезпеки організації.* *РН12. Досліджувати, розробляти та впроваджувати методи і заходи протидії кіберінцидентам, здійснювати процедури управління, контролю та розслідування, а також надавати рекомендації щодо попередження та аналізу кіберінцидентів в цілому.* *РН13.*					

Досліджувати, розробляти, впроваджувати та використовувати методи та засоби криптографічного та технічного захисту інформації бізнес/операційних процесів, а також аналізувати і надавати оцінку ефективності їх використання в інформаційних системах, на об'єктах інформаційної діяльності та критичної інфраструктури. *РН14. Аналізувати, розробляти і супроводжувати систему аудиту та моніторингу ефективності функціонування інформаційних систем і технологій, бізнес\операційних процесів у сфері інформаційної та\або кібербезпеки в цілому.* *РН15. Зрозуміло і недвозначно доносити власні висновки з проблем інформаційної безпеки та/або кібербезпеки, а також знання та пояснення, що їх обґрунтовують до персоналу, партнерів та інших осіб.* *РН16. Приймати обґрунтовані рішення з організаційно-технічних питань інформаційної безпеки та/або кібербезпеки у складних і непередбачуваних умовах, у тому числі із застосуванням сучасних методів та засобів оптимізації, прогнозування та прийняття рішень.* *РН17. Мати навички автономного і самостійного навчання у сфері інформаційної безпеки та/або кібербезпеки і дотичних галузей знань, аналізувати власні освітні потреби та об'єктивно*					

оцінювати результати навчання. *РН18. Планувати навчання, а також супроводжувати та контролювати роботу з персоналом у напряму інформаційної безпеки та/або кібербезпеки.* *РН19. Обирати, аналізувати і розробляти придатні типові аналітичні, розрахункові та експериментальні методи кіберзахисту, розробляти, реалізовувати та супроводжувати проекти з захисту інформації у кіберпросторі, інноваційної діяльності та захисту інтелектуальної власності.* *РН20. Ставити та вирішувати складні інженерно-прикладні та наукові задачі інформаційної безпеки та/або кібербезпеки з урахуванням вимог вітчизняних та світових стандартів та кращих практик.* *РН21. Використовувати методи натурного, фізичного і комп'ютерного моделювання для дослідження процесів, які стосуються інформаційної безпеки та/або кібербезпеки.* *РН22. Планувати та виконувати експериментальні і теоретичні дослідження, висувати і перевіряти гіпотези, обирати для цього придатні методи та інструменти, здійснювати статистичну обробку даних, оцінювати достовірність результатів досліджень, аргументувати висновки.* *РН23. Обґрунтовувати вибір програмного*					

забезпечення, устаткування та інструментів, інженерних технологій і процесів, а також обмежень щодо них в галузі інформаційної безпеки та/або кібербезпеки на основі сучасних знань у суміжних галузях, наукової, технічної та довідкової літератури та іншої доступної інформації.				
РН1. Вільно спілкуватись державною та іноземною мовами, усно і письмово для представлення і обговорення результатів досліджень та інновацій, забезпечення бізнес\операційних процесів та питань професійної діяльності в галузі інформаційної безпеки та/або кібербезпеки. *РН2. Інтегрувати фундаментальні та спеціальні знання для розв'язування складних задач інформаційної безпеки та/або кібербезпеки у широких або мультидисципліна рних контекстах.* *РН3. Провадити дослідницьку та/або інноваційну діяльність в сфері інформаційної безпеки та/або кібербезпеки, а також в сфері технічного та криптографічного захисту інформації у кіберпросторі.* *РН4. Застосовувати, інтегрувати, розробляти, впроваджувати та удосконалювати сучасні інформаційні технології, фізичні та математичні методи і моделі в сфері інформаційної безпеки та/або кібербезпеки.* *РН5. Критично осмислювати проблеми інформаційної*	☒	Веб-безпека	Пояснювально-ілюстративний (інформаційно-рецептивний) та репродуктивний	Опитування на лекційних заняттях, тестування, презентації докладів за темами лекційних занять, захист лабораторних робіт, проведення контрольних робіт, іспит

безпеки та/або кібербезпеки, у тому числі на міжгалузевому та міждисциплінарному рівні, зокрема на основі розуміння нових результатів інженерних і фізико-математичних наук, а також розвитку технологій створення та використання спеціалізованого програмного забезпечення. *РН6. Аналізувати та оцінювати захищеність систем, комплексів та засобів кіберзахисту, технології створення та використання спеціалізованого програмного забезпечення.* *РН7. Обґрунтовувати використання, впроваджувати та аналізувати кращі світові стандарти, практики з метою розв'язання складних задач професійної діяльності в галузі інформаційної безпеки та/або кібербезпеки.* *РН8. Досліджувати, розробляти і супроводжувати системи та засоби інформаційної безпеки та/або кібербезпеки на об'єктах інформаційної діяльності та критичної інфраструктури.* *РН9. Аналізувати, розробляти і супроводжувати систему управління інформаційною безпекою та/або кібербезпекою організації на базі стратегії і політики інформаційної безпеки.* *РН10. Забезпечувати безперервність бізнес/операційних процесів, а також виявляти уразливості інформаційних систем та ресурсів,*					

аналізувати та оцінювати ризики для інформаційної безпеки та/або кібербезпеки організації. *РН11. Аналізувати, контролювати та забезпечувати ефективне функціонування системи управління доступом до інформаційних ресурсів відповідно до встановлених стратегії і політики інформаційної безпеки та/або кібербезпеки організації.* *РН12. Досліджувати, розробляти та впроваджувати методи і заходи протидії кіберінцидентам, здійснювати процедури управління, контролю та розслідування, а також надавати рекомендації щодо попередження та аналізу кіберінцидентів в цілому.* *РН13. Досліджувати, розробляти, впроваджувати та використовувати методи та засоби криптографічного та технічного захисту інформації бізнес/операційних процесів, а також аналізувати і надавати оцінку ефективності їх використання в інформаційних системах, на об'єктах інформаційної діяльності та критичної інфраструктури.* *РН14. Аналізувати, розробляти і супроводжувати систему аудиту та моніторингу ефективності функціонування інформаційних систем і технологій, бізнес\операційних процесів у сфері інформаційної та\або кібербезпеки в цілому.* *РН15. Зрозуміло і недвозначно*					

доносити власні висновки з проблем інформаційної безпеки та/або кібербезпеки, а також знання та пояснення, що їх обґрунтовують до персоналу, партнерів та інших осіб. *РН16. Приймати обґрунтовані рішення з організаційно-технічних питань інформаційної безпеки та/або кібербезпеки у складних і непередбачуваних умовах, у тому числі із застосуванням сучасних методів та засобів оптимізації, прогнозування та прийняття рішень.* *РН17. Мати навички автономного і самостійного навчання у сфері інформаційної безпеки та/або кібербезпеки і дотичних галузей знань, аналізувати власні освітні потреби та об'єктивно оцінювати результати навчання.* *РН18. Планувати навчання, а також супроводжувати та контролювати роботу з персоналом у напряму інформаційної безпеки та/або кібербезпеки.* *РН19. Обирати, аналізувати і розробляти придатні типові аналітичні, розрахункові та експериментальні методи кіберзахисту, розробляти, реалізовувати та супроводжувати проекти з захисту інформації у кіберпросторі, інноваційної діяльності та захисту інтелектуальної власності.* *РН20. Ставити та вирішувати складні інженерно-прикладні та наукові задачі інформаційної*					

безпеки та/або кібербезпеки з урахуванням вимог вітчизняних та світових стандартів та кращих практик. *РН21. Використовувати методи натурного, фізичного і комп'ютерного моделювання для дослідження процесів, які стосуються інформаційної безпеки та/або кібербезпеки.* *РН22. Планувати та виконувати експериментальні і теоретичні дослідження, висувати і перевіряти гіпотези, обирати для цього придатні методи та інструменти, здійснювати статистичну обробку даних, оцінювати достовірність результатів досліджень, аргументувати висновки.* *РН23. Обґрунтовувати вибір програмного забезпечення, устаткування та інструментів, інженерних технологій і процесів, а також обмежень щодо них в галузі інформаційної безпеки та/або кібербезпеки на основі сучасних знань у суміжних галузях, наукової, технічної та довідкової літератури та іншої доступної інформації.*				
РН2. Інтегрувати фундаментальні та спеціальні знання для розв'язування складних задач інформаційної безпеки та/або кібербезпеки у широких або мультидисциплінарних контекстах. *РН6. Аналізувати та оцінювати захищеність систем, комплексів та засобів кіберзахисту, технології*	☒	Цифрова криміналістика	Пояснювально-ілюстративний (інформаційно-рецептивний) та репродуктивний	Опитування на лекційних заняттях, тестування, презентації докладів за темами лекційних занять, захист лабораторних робіт, проведення контрольних робіт, виконання курсового проєкту, іспит

створення та використання спеціалізованого програмного забезпечення. *РН8. Досліджувати, розробляти і супроводжувати системи та засоби інформаційної безпеки та/або кібербезпеки на об'єктах інформаційної діяльності та критичної інфраструктури.* *РН10. Забезпечувати безперервність бізнес/операційних процесів, а також виявляти уразливості інформаційних систем та ресурсів, аналізувати та оцінювати ризики для інформаційної безпеки та/або кібербезпеки організації.* *РН12. Досліджувати, розробляти та впроваджувати методи і заходи протидії кіберінцидентам, здійснювати процедури управління, контролю та розслідування, а також надавати рекомендації щодо попередження та аналізу кіберінцидентів в цілому.* *РН16. Приймати обґрунтовані рішення з організаційно-технічних питань інформаційної безпеки та/або кібербезпеки у складних і непередбачуваних умовах, у тому числі із застосуванням сучасних методів та засобів оптимізації, прогнозування та прийняття рішень.* *РН17. Мати навички автономного і самостійного навчання у сфері інформаційної безпеки та/або кібербезпеки і дотичних галузей знань, аналізувати власні освітні*					

потреби та об'єктивно оцінювати результати навчання. *РН19. Обирати, аналізувати і розробляти придатні типові аналітичні, розрахункові та експериментальні методи кіберзахисту, розробляти, реалізовувати та супроводжувати проекти з захисту інформації у кіберпросторі, інноваційної діяльності та захисту інтелектуальної власності.* *РН20. Ставити та вирішувати складні інженерно-прикладні та наукові задачі інформаційної безпеки та/або кібербезпеки з урахуванням вимог вітчизняних та світових стандартів та кращих практик.* *РН21. Використовувати методи натурного, фізичного і комп'ютерного моделювання для дослідження процесів, які стосуються інформаційної безпеки та/або кібербезпеки.* *РН22. Планувати та виконувати експериментальні і теоретичні дослідження, висувати і перевіряти гіпотези, обирати для цього придатні методи та інструменти, здійснювати статистичну обробку даних, оцінювати достовірність результатів досліджень, аргументувати висновки.* *РН23. Обґрунтовувати вибір програмного забезпечення, устаткування та інструментів, інженерних технологій і процесів, а також обмежень щодо них в галузі*					

інформаційної безпеки та/або кібербезпеки на основі сучасних знань у суміжних галузях, наукової, технічної та довідкової літератури та іншої доступної інформації.				
РН2. Інтегрувати фундаментальні та спеціальні знання для розв'язування складних задач інформаційної безпеки та/або кібербезпеки у широких або мультидисциплінарних контекстах. *РН6. Аналізувати та оцінювати захищеність систем, комплексів та засобів кіберзахисту, технології створення та використання спеціалізованого програмного забезпечення.* *РН8. Досліджувати, розробляти і супроводжувати системи та засоби інформаційної безпеки та/або кібербезпеки на об'єктах інформаційної діяльності та критичної інфраструктури.* *РН10. Забезпечувати безперервність бізнес/операційних процесів, а також виявляти уразливості інформаційних систем та ресурсів, аналізувати та оцінювати ризики для інформаційної безпеки та/або кібербезпеки організації.* *РН12. Досліджувати, розробляти та впроваджувати методи і заходи протидії кіберінцидентам, здійснювати процедури управління, контролю та розслідування, а також надавати рекомендації щодо попередження та аналізу кіберінцидентів в*	☒	Тестування на проникнення та етичний хакінг	Пояснювально-ілюстративний (інформаційно-рецептивний) та репродуктивний	Опитування на лекційних заняттях, тестування, презентації докладів за темами лекційних занять, захист лабораторних робіт, проведення контрольних робіт, виконання курсового проєкту, іспит

цілому. *РН16. Приймати обґрунтовані рішення з організаційно-технічних питань інформаційної безпеки та/або кібербезпеки у складних і непередбачуваних умовах, у тому числі із застосуванням сучасних методів та засобів оптимізації, прогнозування та прийняття рішень.* *РН17. Мати навички автономного і самостійного навчання у сфері інформаційної безпеки та/або кібербезпеки і дотичних галузей знань, аналізувати власні освітні потреби та об'єктивно оцінювати результати навчання.* *РН19. Обирати, аналізувати і розробляти придатні типові аналітичні, розрахункові та експериментальні методи кіберзахисту, розробляти, реалізовувати та супроводжувати проекти з захисту інформації у кіберпросторі, інноваційної діяльності та захисту інтелектуальної власності.* *РН20. Ставити та вирішувати складні інженерно-прикладні та наукові задачі інформаційної безпеки та/або кібербезпеки з урахуванням вимог вітчизняних та світових стандартів та кращих практик.* *РН21. Використовувати методи натурного, фізичного і комп'ютерного моделювання для дослідження процесів, які стосуються інформаційної безпеки та/або кібербезпеки.* *РН22. Планувати*					

та виконувати експериментальні і теоретичні дослідження, висувати і перевіряти гіпотези, обирати для цього придатні методи та інструменти, здійснювати статистичну обробку даних, оцінювати достовірність результатів досліджень, аргументувати висновки. *РН23. Обґрунтовувати вибір програмного забезпечення, устаткування та інструментів, інженерних технологій і процесів, а також обмежень щодо них в галузі інформаційної безпеки та/або кібербезпеки на основі сучасних знань у суміжних галузях, наукової, технічної та довідкової літератури та іншої доступної інформації.*				