Загальні відомості

Інформація про заклад вищої освіти

*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	https://www.kpi.kharkov.ua/ukr/
*ID освітньої програми в ЄДЕБО	25278
*Назва ОП	“Кібербезпека”
*Реквізити рішення про ліцензування спеціальності на відповідному рівні вищої освіти	
*Цикл (рівень вищої освіти)	бакалавр
*Галузь знань	12 – Інформаційні технології
*Спеціальність	125 – Кібербезпека
Спеціалізація (за наявності)	
*Вид освітньої програми	Освітньо-професійна
*Вступ на освітню програму здійснюється на основі ступеня (рівня)	Повна загальна середня освіта
*Термін навчання на освітній програмі	3 роки 10 місяців
*Форми здобуття освіти на ОП	денна, очна
*Структурний підрозділ (кафедра або інший підрозділ),відповідальний за реалізацію ОП	кафедра кібербезпеки
Інші навчальні структурні підрозділи (кафедра або інші підрозділи), залучені до реалізації ОП	кафедра комп’ютерної математики і аналізу даних, кафедра фізики, кафедра іноземних мов, кафедра українознавства, культурології та історії науки, кафедра філософії, кафедра української мови, кафедра фізичного виховання
*Місце (адреса) провадження освітньої діяльності за ОП	61002 м. Харків вул. Кирпичова 2

*Освітня програма передбачає присвоєння професійної кваліфікації	ні
Професійна кваліфікація, яка присвоюється за ОП (за наявності)	бакалавр з кібербезпеки
*Мова (мови) викладання	українська
*ID гаранта ОП у ЄДЕБО	4460878
*ПІБ гаранта ОП	ЄвсеєвСергійПетрович
*Посада гаранта ОП	завідувач кафедри кібербезпеки
*Корпоративна електронна адреса гаранта ОП	Serhii_Yevseiev@khpi.edu.ua
*Контактний телефон гаранта ОП	+38095-360-6613
Додатковий контактний телефон гаранта ОП	+38068-398-6603

Інформація про контингент здобувачів вищої освіти на ОП станом на 1 жовтня поточного навчального року та набір на ОП

Рік навчання	1 рік навчання	2 рік навчання	3 рік навчання	4 рік навчання
1. Навчальний рік, у якому відбувся набір здобувачів відповідного року навчання	2023	2022	2021	2020
2. Обсяг набору на ОП у відповідному навчальному році	50	47	42	25
3. Контингент студентів:	50	50	34	21
3.1. очна форма навчання	50	50	34	21
3.2. заочна форма навчання	0	0	0	0
4. У т. ч. іноземців:	0	1	0	0
4.1. очна форма навчання	0	1	0	0
4.2. заочна форма навчання	0	0	0	0

Кількість стовпців таблиці змінюється залежно від строку навчання на освітній програмі.

Інформація про інші освітні програми ЗВО за відповідною спеціальністю: *(зазначається ID програм у ЄДЕБО і їх назва)*

Рівень вищої освіти	Інформація про освітні програми
початковий рівень (короткий цикл) вищої освіти	
перший (бакалаврський) рівень	
другий (магістерський) рівень	ID 54114 “Кібербезпека”
третій (освітньо-науковий/освітньо-творчий) рівень	ID 56363 “Кібербезпека”

Інформація про площі 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,	282386	91582
Господарського відання або оперативного управління)	0	0
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

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 та захист інформації”, 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 2023 році (затверджено Вченою радою від 05.05.2023 року, протокол № 4) та розроблена відповідно до Стандарту вищої освіти за спеціальністю 125 “Кібербезпека та захист інформації” (https://cybersecurity.kpi.kharkov.ua/osvitno-profesijna-programa-125-bakalavr/)

Кафедра кібербезпеки в НТУ “ХПІ” організована з 1.01.2022 року, але кафедра відповідно грантів з CRDF Global організовала та провела курс “Базові основи кібергігієни”, впроваджує ОК “Кібербезпека. Правові аспекти”, “Сучасні інформаційні технології”, гранту з United States Agency for International Development “Cybersecurity of Critical Infrastructure of Ukraine” приймає участь в неормальної освіті студентів першого (бакалаврського) рівня, а також 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 підготовці та проведенні міжнародної науково-практичної конференції IEEE “International Congress on Human-Computer Interaction, Optimization and Robotic Applications”(https://ichoracongress.com/index.php).

На кафедрі постійно займаються дослідними роботами, що підтверджується отриманими патентами на корисну модель викладачами кафедри (https://cybersecurity.kpi.kharkov.ua/patenty-kafedry-kiberbezpeka/). У жовтні-грудні 2023 року у рамках проекту “Cybersecurity of Critical Infrastructure of Ukraine” кафедра отримала матеріально-технічну допомогу на суму понад 1 млн. 200 000грн., що дозволяє розгорнути ЦСКуніверситету та кіберполігон. У підготовці проекту змін ОПП “Кібербезпека” у 2022 р. брали участь: завідувач кафедри Євсеєв Сергій Петрович, професор Мілов Олександр, доцент Король Ольга, комерційний директор ТОВ “Сайфер”, к.т.н. Ковтун Владислав; співзасновник компанії “Distributed Lab”, к.т.н. Кравченко Павло; директор ТОВ “Мікрокрипт Текнолоджіс”, к.т.н., доцент Головашич Сергій; керівник ННЦ ІТ Поліського національного університету, д.т.н., професор Молодецька Катерина.

1. Проектування та цілі освітньої програми

Якими є цілі ОП? У чому полягають особливості (унікальність) цієї програми? *коротке поле*
Цілі ОП – підготовка професіоналів, здатних розробляти та використовувати технології програмування та засоби інформаційної та/або кібербезпеки, які володіють сучасними методами та механізмами забезпечення безпеки інформаційних ресурсів інформаційно-комунікаційних систем та технологій. 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. Для цього на кафедрі разом з компанією “Distributed Lab” розгорнута лабораторія Блокчейн, на базі якої представники компанії, виконавці реальних проектів, які пов’язані з децентралізованими системами та смарт-контрактами (https://cybersecurity.kpi.kharkov.ua) проводять майстер-класи, що дозволяє формувати відповідні компетентності. 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 *коротке поле*
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 *коротке поле*
Студенти 3 курсу (Мокин, Муренко, Бельчинская, Радевич, Бобченок, Кузнецов, Ярмош, Азаров, Демяник, Висоцький, Гладков, Шпилька, Васюткин, Запорожец) запропонували приймати участь у неформальної освіті за програмою Проєкту USAID “Кібербезпека критично важливої інфраструктури України”. Від проєкту “USAID Кібербезпека критично важливої інфраструктури України” з квітня 2023 року Проєкт надав доступ до використання навчального полігону RangeForce

студентам спеціальності “Кібербезпека та захист інформації” університету (надано 16 ліцензій RangeForce learner). Нажаль з жовтня 2023 року в рамках проекту припинено фінансування ліцензій на цієї платформі. Після проходження курсів студенти рекомендували в подальшому поширювати таку можливість та направляти здобувачів на навчання.

роботодавці *коротке поле*

Комерційний директор ТОВ “Сайфер ” Ковтун Владислав запропонував включити в навчальний план за ОПП “Кібербезпека” курси з мови програмування Python (з початкового рівня та закінчуючи просунутим рівнем). Після обговорення відповідні зміни включені до навчального плану, а саме в дисципліни “Технології програмування”, “Інформаційні системи та інтернет технології” (https://cybersecurity.kpi.kharkov.ua). А також використовувати ЦСК в підготовці його використання та розгортання електронного документообігу в університеті.

Співзасновник компанії “Distributed Lab” Кравченко Павло, який є членом робочої групи запропонував лабораторні роботи, які розроблені компанією в рамках ОК “Blockchain: основи та приклади застосування”

академічна спільнота *коротке поле*

ОПП “Кібербезпека” отримала позитивну рецензію-відгук від Катерини Молодецької, д.т.н., професора, керівника навчально-наукового центру інформаційних технологій Поліського національного університету.

Академічна спільнота запропонувала включити в ОПП “Кібербезпека” курси академії CISCO (https://cybersecurity.kpi.kharkov.ua), які пов’язані з комп’ютерними мережами та безпекою в них, створення окремих напрямків на кіберполігоні, а саме: лабораторії кіберфізичних систем, лабораторії систем Інтернет-речей та технології блокчейн, лабораторії безпеки об’єктів критичних інфраструктур. Після обговорення було вирішено включити в відповідні дисципліни навчальний матеріал курсів CISCO. Таким чином більша частина пропозицій була врахована. Врахування пропозицій обумовлюється бажанням робочої групи підвищити рівень конкурентоспроможності здобувачів вищої освіти на ринку праці.

інші стейкхолдери *коротке поле*

Випускник магістерської програми за спеціальністю 122 “Комп’ютерні науки” Ігор Леонтієв, який працює в компанії Dvigunity (Chief Technical Officer) запропонував включити в навчальні дисципліни питання, які пов’язані з використанням SIEM-систем, формуванням безпеки на основі DevSecOps, безпеки контейнерів та безпеки K8S. Прийнято рішення включити до ОПП “Кібербезпека” дисципліну “Безпека в DevOps” (профільний пакет).

В рамках проекту USAID “Інтеграція курсів із кібербезпеки в навчальні плани українських університетів” в навчальний план бакалаврського рівня додані дві дисципліни – “Кібербезпека. Правові основи та технології” та “Сучасні інформаційні системи (з елементами кібербезпеки)”

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

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*коротке поле*

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 (http://surl.li/bcurp)
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 *коротке поле*

Під час формулювання цілей та програмних результатів навчання з ОПП "Кібербезпека" були проаналізовані освітні програми з підготовки здобувачів

першого (бакалаврського) рівня вищої освіти за спеціальністю 125 “Кібербезпека” провідних технічних університетів м. Києва (Київський політехнічний інститут імені Ігоря Сікорського (захист комп’ютерних систем, мобільних терміналів, пристроїв інтернету речей) (http://bit.ly/39Cv7dh), Національний авіаційний університет (СП11-СП15, СП18, СП25) (https://pk.nau.edu.ua/125-kiberbezpeka-2/)), м. Харкова (Харківський національний університет радіоелектроніки (https://nure.ua/), Харківський національний університет ім. В.Н. Каразіна (СП4, СП7, СП11, СП13, СП16, СП21) (http://bit.ly/3r4wkn6), освітні програми з підготовки здобувачів зі спеціальності “Кібербезпека” у закладах Великої Британії (http://bit.ly/2SJEiSb). На основі аналізу були розподілені основні фахові компетентності та результати навчання, визначені дисципліни, форми та методи навчання, які також враховують пропозиції стейкхолдерів (здобувачів, роботодавців, академічної спільноти).

Продемонструйте, яким чином ОП дозволяє досягти результатів навчання, визначених стандартом вищої освіти за відповідною спеціальністю та рівнем вищоїосвіти (за наявності) *довге поле*

Стандарт вищої освіти зі спеціальності 125 “Кібербезпека” першого (бакалаврського) рівня вищої освіти затверджено наказом МОН № 1074 від 04.10.2018 року. Освітня програма “Кібербезпека” дозволяє досягти результатів навчання шляхом впровадження в освітній процес таких навчальних дисциплін:
Основи програмування
Кібербезпека. Правові основи та технології
Розробка та аналіз алгоритмів
Фізичні основи технічних засобів розвідки
Інформаційна безпека держави
Структури даних
Математичні основи криптології
Основи побудови та захисту сучасних операційних систем
Введення в мережі
Технології програмування
Основи побудови та захисту мікропроцесорних систем
Менеджмент інформаційної безпеки
Основи математичного моделювання систем безпеки
Основи криптографічного захисту
Безпека в інформаційно-комунікаційних системах
Сучасні інформаційні системи (з елементами кібербезпеки)
Комплексні системи захисту інформації
Організація і безпека баз даних
Комплексні засоби захисту інформації
Основи стеганографічного захисту інформації
Основи соціальної інженерії
Комплексний тренінг
Бізнес інтелідженс
Безпека інтернет-речей

Антивірусний захист інформації
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 відповідногокваліфікаційного рівня? *довге поле*
Відповідно до наказу МОН України № 1074 від 04.10.2018 р. введений Стандарт вищої освіти за спеціальністю 125 “Кібербезпека” для першого (бакалаврського) рівня вищої освіти.

2. Структура та зміст освітньої програми

Яким є обсяг ОП (у кредитах ЄКТС)?	**240**
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)?	**180**
Який обсяг (у кредитах ЄКТС) відводиться на дисципліни за вибором здобувачів вищої освіти?	**60**
Продемонструйте, що зміст ОП відповідає предметній області заявленої для неї спеціальності (спеціальностям, якщо освітня програма є міждисциплінарною)? *довгеполе*	
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 інформатизації, включаючи комп’ютерні, автоматизовані, телекомунікаційні, інформаційні, інформаційно-аналітичні, інформаційно-телекомунікаційні системи, інформаційні ресурси й інформаційні технології; технології забезпечення безпеки інформації об’єктів різного рівня (система, об’єкт системи, компонент об'єкта), що пов'язані з інформаційними, інформаційно-комунікаційними технологіями, які використовуються для забезпечення функціонування цих об’єктів; процеси управління інформаційною і кібербезпекою об’єктів, що підлягають захисту. Такий підхід забезпечує отримання компетентностей та якісну підготовку до ЕДКІ. Ці питання відповідають теоретичному змісту предметної області, методам, методикам та технологіям формування компетентностей за ОПП “Кібербезпека”. Зміст ОП “Кібербезпека” забезпечує поглиблену підготовку здобувачів вищої освіти з програмування та забезпечення на її основі вивчення способів побудови механізмів безпеки, знаходження раціональних методів та засобів розв’язання складних задач з оцінювання поточного стану рівня інформаційної безпеки та кібербезпеки, забезпечення його підвищення. Перелік ОК ОП дозволяє сформувати комплекс знань, навичок та вмінь, які відповідають високому рівню конкурентоспроможності на ринку праці. Дисципліни навчального плану ОП потребують спеціалізованого програмного та апаратного забезпечення, яке використовується в кіберполігоні. Дисципліни ОП в повній мірі забезпечені ліцензованим та open source програмним забезпеченням, що дозволяє досягти поставленої мети та завдань. Таким чином, ОП, 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	

формуванняіндивідуальної освітньої траєкторії? *коротке поле*
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 (https://blogs.kpi.kharkov.ua/v2/nv/dokumenty/normatyvni-dokumenty/). В проект навчального плану підготовки доданий Профільований пакет дисциплін 03 "Innovation Campus", який дозволяє додатково в рамках проекту формувати індивідуальну освітню траєкторію з особливою підготовкою.
Яким чином здобувачі вищої освіти можуть реалізувати своє право на вибір навчальних дисциплін? *довге поле*
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 професійних навичок; 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-bakalavr/, https://bit.ly/36jiMhV) міститься перелік дисциплін вільного вибору та спеціалізовані (профільовані) блоки (пакети) взаємопов'язаних дисциплін з силабусами до кожної дисципліни. Студенту пропонується вибір дисциплін з варіативної складової навчального плану відповідної освітньої програми, на якій студент навчається: спеціалізований (профільований) блок (пакет) дисциплін, який включає переважно фахові дисципліни, що визначають спеціалізовану підготовку студента в межах обраної освітньої програми, і спрямований на поліпшення здатності студента до працевлаштування за обраним фахом. Якщо студент обрав спеціалізований (профільований) блок (пакет), він має прослухати всі дисципліни, що включені до цього блоку (пакета). Студенту також пропонується перелік дисциплін вільного вибору профільної підготовки та можливість вибору дисциплін із загальноуніверситетського каталогу. 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. (https://blogs.kpi.kharkov.ua/v2/nv/dokumenty/normatyvni-dokumenty/) 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 підготовкуздобувачів вищої освіти, яка дозволяє здобути компетентності, необхідні для подальшої професійної діяльності *коротке поле*

У відповідності до навчального плану практична підготовка здійснюється під час проведення лабораторних занять за освітніми компонентами базової складової: Розробка та аналіз алгоритмів, Фізичні основи технічних засобів розвідки, Інформаційна безпека держави, Математичні основи криптології, Теоретичні основи криптографії, Основи побудови та захисту сучасних операційних систем, Технології програмування, Основи побудови та захисту мікропроцесорних систем, Введення в мережі, Інформаційні системи та інтернет технології, Основи криптографічного захисту, Комплексні системи захисту інформації, Комплексні засоби захисту інформації, Безпека в інформаційно-комунікаційних системах, Комплексний, курсовий проект, Основи стеганографічного захисту інформації, Антивірусний захист інформації та ін. Відповідно до навчального плану ОП передбачає виробничу практику (6 сем., 6 кредитів ЄКТС), метою якої є формування професійних умінь і навичок щодо прийняття самостійних рішень під час професійної діяльності в сфері кібербезпеки та захисту інформації. Комплексний тренінг дозволяє узагальнити отримані результати навчання та практичні навички з 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. “Ознайомча практика”, що дозволить посилити практичну підготовку здобувачів вищої освіти ОП.

Продемонструйте, що ОП дозволяє забезпечити набуття здобувачами вищої освітисоціальних навичок (soft skills) упродовж періоду навчання, які відповідають цілямта результатам навчання ОП *коротке поле*

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: Українська мова (за професійним спрямуванням)”, “Історія та культура України”,

“Інформаційна безпека держави”, “Іноземна мова”, які забезпечують наступні компетентності щодо формування соціальних навичок: КЗ-1, КЗ-2, КЗ-3, КЗ-4, КЗ-5, КЗ-6, КЗ-7, КФ-1, КФ-2, КФ-3, КФ-4, КФ-5, КФ-6, КФ-7, КФ-8, КФ-9, КФ-10, КФ-11, КФ-12. 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? *коротке поле*

Професійні стандарти за спеціальністю находяться на затверджені.
Фахівці з кібербезпеки можуть працювати, згідно з чинною редакцією Національного класифікатора України: Класифікатор професій (Зміна № 10 до ДК 003:2010):
2132.2 Розробник систем захисту інформації;
2139.2 Адміністратор мереж і систем;
2139.2 Фахівець з криптографічного захисту інформації;
2139.2 Фахівець з питань безпеки (інформаційно-комунікаційні технології);
2139.2 Фахівець з підтримки інфраструктури кіберзахисту;
2139.2 Фахівець з реагування на інциденти кібербезпеки;
2139.2 Фахівець з тестування систем захисту інформації;
2139.2 Фахівець з технічного захисту інформації;
2139.2 Фахівець сфери захисту інформації.

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

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. При цьому максимальне тижневе аудиторне навантаження здобувачів вищої освіти першого (бакалаврського) рівня не повинно перевищувати максимально допустимі обсяги 30 годин для очної (денної) форми навчання. 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://surl.li/pevcd). Розподіл навчальних годин на аудиторну роботу за навчальними тижнями та видами навчальної роботи бакалавра відображено в сила бусах.
Навчальний час, відведений для самостійної роботи студента, визначається гарантом освітньої програми.
Навантаження також відстежується через опитування студентів (оптимальне навчальне навантаження за ОП – 100%; достатність часу на виконання самостійної роботи – 100% (4курс)).
Співвідношення обсягу окремих освітніх компонент ОП з фактичним

навантаженням здобувачів вищої освіти у навчальному плані складає: 1. Загальна підготовка – 53 кредити, 51% (самостійна). 2. Спеціальна (фахова) підготовка – 127 кредитів, 56% (самостійна). 3. Вибіркові освітні компоненти – 60 кредитів, 55% (самостійна).
Якщо за ОП здійснюється підготовка здобувачів вищої освіти за дуальною формоюосвіти, продемонструйте, яким чином структура освітньої програми та навчальний план зумовлюються завданнями та особливостями цієї форми здобуття освіти *коротке поле*
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 https://vstup.kpi.kharkov.ua/admission/admission_rules/ Веб-сайт інституту http://web.kpi.kharkov.ua/if/uk/abituriyentu/umovi-vstupu/ Веб-сайт кафедри https://cybersecurity.kpi.kharkov.ua/%D0%B0%D0%B1%D1%96%D1%82%D1%83%D1%80%D1%96%D1%94%D0%BD%D1%82%D1%83/	
Поясніть, як правила прийому на навчання та вимоги до вступників ураховуютьособливості ОП? *коротке поле*	
Правила прийому є чіткими та зрозумілими для абітурієнта, не містять дискримінаційних положень, оприлюднені на офіційному веб-сайті ЗВО http://vstup.kpi.kharkov.ua/edprogram/kiberbezpeka-innovatsiinyi-kampus-bakalavr/, 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. Для вступу на 1 курс на освітню програму приймаються абітурієнти, які мають сертифікат МНТ. Підчас вискового стану для вступу на ОП здавався мультитест із Української мови, математики та Історії України.	
Яким документом ЗВО регулюється питання визнання результатів навчання,отриманих в інших ЗВО? Яким чином забезпечується його доступність для учасників освітнього процесу? *коротке поле*	
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 № 10 від 4 грудня 2023 р. https://blogs.kpi.kharkov.ua/v2/nv/dokumenty/normatyvni-dokumenty/). 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., https://blogs.kpi.kharkov.ua/v2/nv/dokumenty/normatyvni-dokumenty/) Положення про порядок реалізації студентами права на вільний вибір навчальних дисциплін у НТУ «ХПІ» (Затверджено Вченою радою НТУ «ХПІ», Протокол № 11 від «26» грудня 2023 р., https://blogs.kpi.kharkov.ua/v2/nv/dokumenty/normatyvni-dokumenty/)	
Опишіть на конкретних прикладах практику застосування вказаних правил навідповідній ОП (якщо такі були)? *коротке поле*	
Відповідно до договору про мобільність з Рейн-Ваальським університетом	

студент 2 курсу Івченко Д.Б. пройшов навчання у першому семестрі та його результати навчання були враховані. Студентка Назаренко Я. С. була зарахована на другий курс після навчання у Харківському національному університеті й також відповідно академічної довідки дисципліни були перезараховані.
Яким документом ЗВО регулюється питання визнання результатів навчання, отриманих у неформальній освіті? Яким чином забезпечується його доступність дляучасників освітнього процесу? *коротке поле*
Положення про порядок визнання результатів неформальної та інформальної освіти у Національному технічному університеті «Харківський політехнічний інститут» (https://blogs.kpi.kharkov.ua/v2/nv/dokumenty/normatyvni-dokumenty/).
Опишіть на конкретних прикладах практику застосування вказаних правил навідповідній ОП (якщо такі були)? *коротке поле*
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 навідповідні документи *коротке поле*
Основними формами навчання відповідно до Положення про організацію освітнього процесу в НТУ «ХПІ» (Затверджено Вченою радою НТУ «ХПІ» «01» грудня 2023 р. Протокол № 10 (п.8), (https://blogs.kpi.kharkov.ua/v2/nv/dokumenty/normatyvni-dokumenty/), Положення про силабус освітнього компонента (програма навчальної дисципліни) в Національному технічному університеті «Харківський політехнічний інститут» (Положення затверджено Вченою радою НТУ «ХПІ» «26» грудня 2023 р. Протокол № 11, https://blogs.kpi.kharkov.ua/v2/nv/dokumenty/normatyvni-dokumenty/) 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» http://surl.li/pevla. 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 відповідаютьвимогам студентоцентрованого підходу? Яким є рівень задоволеності здобувачів вищої освіти методами навчання і викладання відповідно до результатів опитувань?*коротке поле*
Студенти здійснюють вибір дисциплін після ознайомлення зі змістом робочих програм і 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 першого (бакалаврського) рівня вищої освіти за ОП отримані наступні результати: задоволеність освітньою програмою – 80,3 % (середнє значення); застосування викладачами форм, методів, технологій навчання, що сприяють формуванню професійних компетентностей – 77,5 %, якість викладання – 80,0 %, якість оцінювання – 82,7%, академічна доброчесність – 82,5%, академічна підтримка – 81,4%, індивідуальна траєкторія навчання – 80,7%, практична підготовка – 75,4%,

самостійна робота (навантаження) – 80,0 %%, можливості навчання – 78,8%, загальна враження навчанням за освітньою програмою – 80,8% (https://drive.google.com/drive/u/1/folders/1bpN390IgfuNDE6IaKiIYTkk732bMjmJw)

Продемонструйте, яким чином забезпечується відповідність методів навчання івикладання на ОП принципам академічної свободи *коротке поле*

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 такритеріїв оцінювання у межах окремих освітніх компонентів *коротке поле*

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-bakalavr/), 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 (https://blogs.kpi.kharkov.ua/v2/nv/navchalnyj-protses/grafik-navchalnogo-protsesu/). 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 *довге поле*

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/blockchain/), яка 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 дисциплін як Теоретичні основи криптографії (розглядаються процедури використання ККК Мак-Еліса та Нідеррайтера, проф. Євсеєв С.П., докторанти: доц. Погасій С.С., Мілевський С.В., а також побудова генераторів ПВЧ та легковісних блокових шифрів, доц. Корольов Р.В.), Технології програмування, Інформаційні системи та інтернет технології (розглядаються власні бібліотеки створення алгоритмів симетричної та несиметричної криптографії мовою Python, доц. Ткачов А.М.), Основи математичного моделювання системи безпеки, в якій розглядаються моделі та методи побудови системи безпеки на основі наукових досліджень професора Мілова О. В. В дисципліні "Основи криптографічного захисту" розглядаються результати досліджень Гаврилової А.А. побудови модифікованого алгоритму UMAC.

Продемонструйте, із посиланням на конкретні приклади, яким чином викладачіоновлюють зміст освітніх компонентів на основі наукових досягнень і сучаснихпрактик у відповідній галузі *довге поле*

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”. Монографія Models of socio-cyber-physical systems security: monograph / S. Yevseiev, Yu. Khokhlachova, S. Ostapov, O. Laptiev and others. – Kharkiv: PC TECHNOLOGY CENTER, 2023. – 168 p. очікується індексація у наукометричної базі Скопус у лютому2024 року. 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 “Основи криптографічного захисту” та “Математичні основи криптології”. Універсальний класифікатор загроз, та методіка оцінки захищеності об’єктів критичної інфраструктури у рамках докторських досліджень доцентів Погасія С.С., Мілевського С.В. (https://skl.sspu.sumy.ua/login). 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 *коротке поле*

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 науко-дослідної роботи з міжнародної тематики та ін. Щороку на базі Університету проводиться понад 30 міжнародних науково-технічних конференцій, низка крупних міжнародних форумів, презентацій та виставок.
Університет постійно бере участь у міжнародних виставках за кордоном. При цьому за підтримкою кафедри щорічна МНПК “Інформаційна безпека та інформаційні технології” в рамках форуму “Digital Reality Forum” (https://drforum.science/en/home/), а також приймає активну участь у проведенні МНПК IEEE “International Congress on Human-Computer Interaction, Optimization and Robotic Applications” (https://ichoracongress.com/index.php) (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)” (https://web.kpi.kharkov.ua/if/en/international-scienti-c-practical-conference-mimcs-2022/) (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? *довге поле*
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 навчальним планом та ОП та відображається в силабусі. 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? *коротке поле*
Чіткість та зрозумілість форм контрольних заходів забезпечується згідно Положення про організацію освітнього процесу в НТУ «ХПІ» https://blogs.kpi.kharkov.ua/v2/nv/dokumenty/normatyvni-dokumenty/ Критерії оцінювання навчальних досягнень здобувачів вищої освіти здійснюються відповідно до Положення про критерії та систему оцінювання знань та вмінь і про рейтинг студентів (https://blogs.kpi.kharkov.ua/v2/nv/dokumenty/normatyvni-dokumenty/). У силабусі навчальної дисципліни є розділ, в якому описуються методи контролю та перелік запитань для підготовки, що передбачені даною дисципліною та відповідають програмним результатам навчання, також таблиця розподілу балів

для оцінювання поточної успішності студента.
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 критеріїоцінювання доводяться до здобувачів вищої освіти? *коротке поле*

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

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

Форми атестації здобувачів ОПП відповідають стандарту вищої освіти зі спеціальності 125 “Кібербезпека та захист інформації” (Стандарт вищої освіти України: перший (бакалаврський) рівень, галузь знань 12 − Інформаційні технології, спеціальність 125 – Кібербезпека та захист інформації. Затверджено і введено в дію наказом Міністерства освіти і науки України від 04.10.2018 р. № 1074, а також змінами до Стандарту на основі наказу МОН від 13.01.2022 № 26, Атестація здійснюється у формі єдиного державного кваліфікаційного іспиту. Єдиний державний кваліфікаційний іспит передбачає оцінювання досягнень результатів навчання, визначених цим стандартом та освітньою програмою.

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

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

комісії, порядок проведення атестації. Ознайомитись з порядком проведення атестації можна на зазначених сайтах.
Яким чином ці процедури забезпечують об'єктивність екзаменаторів? Якими є процедури запобігання та врегулювання конфлікту інтересів? Наведіть прикладизастосування відповідних процедур на ОП *коротке поле*
Відповідно до Положення про критерії та систему оцінювання знань та вмінь і про рейтинг студентів (https://blogs.kpi.kharkov.ua/v2/nv/dokumenty/normatyvni-dokumenty/) та Положення про екзаменаційну комісію у Національному технічному університеті «Харківський політехнічний інститут» (затверджено Вченою радою НТУ «ХПІ» Протокол №1 від 27 січня 2017р. (https://blogs.kpi.kharkov.ua/v2/nv/dokumenty/normatyvni-dokumenty/) та Порядок подання апеляцій (іспити, заліки, атестація) (https://blogs.kpi.kharkov.ua/v2/nv/dokumenty/normatyvni-dokumenty/). Згідно яких у випадку незгоди з оцінкою студент має право на апеляцію. Апеляція має бути розглянута на засіданні апеляційної комісії не пізніше наступного дня після її подання. Здобувач, який подав апеляцію, має право бути присутнім при розгляді своєї заяви. У випадках конфліктної ситуації за мотивованою заявою здобувача чи викладача, розпорядженням директора інституту створюється комісія для проведення підсумкового контролю, до якої входять завідувач кафедри і викладачі відповідної кафедри, представники дирекції, профспілкового комітету студентів та органів студентського самоврядування. Прикладів застосування відповідних процедур на освітній програмі немає.
Яким чином процедури ЗВО урегульовують порядок повторного проходження контрольних заходів? Наведіть приклади застосування відповідних правил на ОП*коротке поле*
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. https://blogs.kpi.kharkov.ua/v2/nv/dokumenty/normatyvni-dokumenty/), Положення про критерії та систему оцінювання знань та вмінь і про рейтинг студентів (https://blogs.kpi.kharkov.ua/v2/nv/dokumenty/normatyvni-dokumenty/). Прикладів застосування відповідних правил на освітній програмі немає.
Яким чином процедури ЗВО урегульовують порядок оскарження процедури та результатів проведення контрольних заходів? Наведіть приклади застосуваннявідповідних правил на ОП *коротке поле*
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 (https://blogs.kpi.kharkov.ua/v2/nv/dokumenty/normatyvni-dokumenty/ та до Положення про екзаменаційну комісію (п.8

https://blogs.kpi.kharkov.ua/v2/nv/dokumenty/normatyvni-dokumenty/).
Прикладів застосування відповідних правил на освітній програмі немає.

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

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 (https://blogs.kpi.kharkov.ua/v2/nv/akredytatsiya/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? *коротке поле*:

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 вищоїосвіти ОП? *коротке поле*

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
коротке поле

Види порушень та відповідальність за них прописані в кодексі етики академічних взаємовідносин та доброчесності НТУ «ХПІ» та положення про систему запобігання та виявлення академічного плагіату у випускних кваліфікаційних роботах здобувачів вищої освіти НТУ «ХПІ» http://library.kpi.kharkov.ua/uk/Academic_Goodness). Серед здобувачів вищої освіти за ОП подібних прикладів не було.

6. Людські ресурси

Яким чином під час конкурсного добору викладачів ОП забезпечується необхіднийрівень їх професіоналізму? *коротке поле*
Конкурсний добір викладачів ОП регламентується Положенням про обрання та прийняття на роботу науково-педагогічних працівників НТУ «ХПІ», затвердженого на засіданні Вченої Ради НТУ «ХПІ» протокол №8 від 27.09.2019 р. (http://blogs.kpi.kharkov.ua/v2/staff/polozhennya-pro-obrannya-ta-prijnyattya-na-robotu-naukovo-pedagogichnih-pratsivnikiv-ntu-hpi-2/). Конкурсний відбір проводиться на засадах: відкритості, гласності, законності, рівності прав членів конкурсної комісії, колегіальності прийняття рішень конкурсною комісією, незалежності, об'єктивності та обґрунтованості рішень конкурсної комісії, неупередженого ставлення до кандидатів на зайняття вакантних посад науково-педагогічних працівників (НПП). Під час конкурсного добору викладачів ОПП гарант згідно з Положенням про гаранта освітньої програми НТУ «ХПІ» (https://blogs.kpi.kharkov.ua/v2/nv/dokumenty/normatyvni-dokumenty/) враховує рівень їх фахової підготовки, наукову та професійну діяльність згідно пп. 37, 38 Ліцензійних умов провадження освітньої діяльності (https://zakon.rada.gov.ua/laws/show/1187-2015-%D0%BF#Text). Також враховується їх наукова та професійна діяльність, а саме: публікації в науково-метричних базах SCOPUS, Web of Science, наявність сертифікатів неформальних курсів за напрямами викладання, наявність сертифікатів на знання іноземних мов, наявність сертифікатів підвищення кваліфікації в галузі "Кібербезпеки та захисту інформації".
Опишіть, із посиланням на конкретні приклади, яким чином ЗВО залучає роботодавців до організації та реалізації освітнього процесу *коротке поле*
Під час розробки ОП для погодження переліку компетентностей здобувачів вищої освіти першого (бакалаврського) 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 віртуальний ЦСК. Компанія "Distributed Lab" запропонувала провести курс лекцій з Блокчейн-технології, а саме "Криптографія в децентралізованих системах"(https://distributed.education/cryptography-course, https://docs.google.com/forms/d/e/1FAIpQLSekIhSqrJvYN30o9Uuk5SJafLDe5iKQe_gLz7my0KApso9cfw/viewform).
Опишіть, із посиланням на конкретні приклади, яким чином ЗВО залучає до аудиторних занять на ОП професіоналів-практиків, експертів галузі, представників роботодавців *коротке поле*

Доцент кафедри Хвостенко В. С. є патентним повіреним юридичної компанії “ATILOG”, що дозволяє під час проведення занять за ОК “Інтелектуальна власність” забезпечити практичну складову з реєстрації та патентування об'єктів інтелектуальної власності (https://atilog.ua/). Спеціалісти Компанії “Distributed Lab” готови провести лабораторні заняття: 1. Реалізація “baby” blockchain https://docs.google.com/document/d/11sleZufJaXNKGNYQzsO66054BPqLlJEmBNSIzA-gyjo/edit?usp=sharing. 2. Реалізація криптографічного алгоритму https://docs.google.com/document/d/1W_JjmzbS8oibOIsIuVIuDykwhCU6weNXDNKjFKfDKQ8/edit?usp=sharing

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

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 (https://blogs.kpi.kharkov.ua/v2/nv/dokumenty/normatyvni-dokumenty/ .

Викладачі НТУ ХПІ отримали дипломи рівня В2 з англійської мови (Мілевський С.В., Погасій С.С., Євсеєєв 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), а також сертифікати від компанії CRDF GLOBAL INFORMATION в рамках гранту USAID з інтеграції курсів із кіберезпеки в навчальні плани українських університетів (Євсеєв С.П., КорольО.Г., Мілевський С.В.)

Продемонструйте, що ЗВО стимулює розвиток викладацької майстерності *короткеполе*

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 07.04.2023р. 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 (http://public.kpi.kharkov.ua/zvit-rektora/).

Протягом року за досягнення у фаховій сфері науково-педагогічні працівники кафедр та факультетів 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? *коротке поле*
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, у 7 читальних залах бібліотеки та в читальних залах при кафедрах. Вільний доступ – електронний репозиторій НТУ «ХПІ» 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 07.04.2023р. 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).
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? *коротке поле*
Потреби та інтереси здобувачів вищої освіти належним образом виявляються під час співпраці ЗВО з органами студентського самоврядування. На базі НТУ «ХПІ» працює СтудАльянс (https://web.kpi.kharkov.ua/studalliance/). У житті студентів і співробітників НТУ «ХПІ» велику роль відіграє учбово-спортивний комплекс «ПОЛІТЕХ». Він є фундаментальною базою, де створені умови для проведення учбових занять, реалізації потенціалу студентів у самостійних заняттях фізичною культурою та спортом. Саме тут проводяться тренування збірних команд України з баскетболу, бадмінтону, легкої атлетиці та іншим видам спорту, чисельні спортивно-масові та фізкультурно-оздоровчі заходи (https://bit.ly/3BAXRRh).

На базі Палацу студентів НТУ «ХПІ» працюють творчі колективи, 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) *коротке поле*

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. 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 здобувачам вищої освіти. На базі НТУ «ХПІ» створена соціально-психологічна служба. Метою діяльності якої є соціально-психологічне забезпечення навчально-виховного процесу, підвищення ефективності навчального, наукового процесу, особистісний розвиток, захист психічного здоров'я, соціального благополуччя студентів, викладачів та працівників (https://web.kpi.kharkov.ua/ppuss/uk/sotsialno-psihologichna-sluzhba-ntu-hpi/).

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? *довге поле*

Права та обов'язки здобувачів освіти регламентують Правила поведінки здобувачів освіти НТУ «ХПІ» (https://blogs.kpi.kharkov.ua/v2/nv/dokumenty/normatyvni-dokumenty/)
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/). 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 ОП 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://www.kpi.kharkov.ua/ukr/studentske-zhittya/profspilkova-organizatsiya-studentiv/ надає: соціальну підтримку у вигляді матеріальної допомоги студентам з малозабезпечених сімей та при тимчасовій втраті здоров'я, організовує відпочинок та дозвілля студентів, надає правовий захист, контролює роботу підприємства громадського харчування університету, підтримує ініціативи студентів, допомагає віршувати побутові проблеми студентів в гуртожитках.

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

Порядок супроводу осіб з обмеженими фізичними можливостями та інших маломобільних груп населення на території Національного технічного університету «Харківський політехнічний інститут» здійснюється згідно наказу №№129 ОД від 24 лютого 2020р про порядок супроводу (надання допомоги) осіб з інвалідністю та інших маломобільних груп населення в НТУ «ХПІ», 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? *довге поле*
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. https://www.kpi.kharkov.ua/ukr/osvita/rozglyad-skarg-zdobuvachiv-osvity-2/ Діяльність щодо запобігання та протидії булінгу (цькуванню) в університеті є системним процесом та регулюється Планом заходів із запобігання та протидії булінгу (цькування) у НТУ «ХПІ», конфліктні ситуації розглядаються згідно до Порядку подання та розгляду заяв про випадки булінгу (цькування), реагування на доведені випадки булінгу (цькування) у НТУ «ХПІ». (https://blogs.kpi.kharkov.ua/v2/nv/dokumenty/normatyvni-dokumenty/) . У разі ситуацій пов'язаних із сексуальними домаганнями, дискримінацією з потерпілим працює соціально-психологічна служба НТУ «ХПІ». https://web.kpi.kharkov.ua/ppuss/uk/sotsialno-psihologichna-sluzhba-ntu-hpi/ https://blogs.kpi.kharkov.ua/v2/nv/dokumenty/normatyvni-dokumenty/ 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” https://blogs.kpi.kharkov.ua/v2/nv/dokumenty/normatyvni-dokumenty/
Опишіть, яким чином та з якою періодичністю відбувається перегляд ОП? Які зміни були внесені до ОП за результатами останнього перегляду, чим вони були обґрунтовані? *довге поле*
Згідно з Методичними рекомендаціями щодо порядку розроблення, затвердження, моніторингу та періодичного перегляду освітніх програм в Національному технічному університеті «Харківський політехнічний університет» https://blogs.kpi.kharkov.ua/v2/nv/dokumenty/normatyvni-dokumenty/ 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 https://blogs.kpi.kharkov.ua/v2/nv/dokumenty/normatyvni-dokumenty/, 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: генеральний 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.
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 *коротке поле*
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 ОПП збирається шляхом проведення

анонімного анкетування (https://cybersecurity.kpi.kharkov.ua/onovlennya-osvitnikh-program-125-bakalavr/), 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. ОПП була погоджена з студентом КН-1120 Бобченком Дмитром представником від студентів спеціальності.

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

До процесу періодичного перегляду ОПП та інших процедур внутрішнього забезпечення якості освіти в Університеті активно залучаються органи студентського самоврядування. 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://cybersecurity.kpi.kharkov.ua/onovlennya-osvitnikh-program-125-bakalavr/)

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 *коротке поле*

Роботодавці (стейкхолдери) мають можливість безпосередньо подати пропозиції щодо ОПП "Кібербезпека" через відповідну сторінку сайту кафедри (https://cybersecurity.kpi.kharkov.ua/onovlennya-osvitnikh-program-125-bakalavr/).
Відповідно до співпраці Проєкт наступної ОП розглянутий та узгоджений з членами робочої групи – компанії ТОВ "Сайфер БІС" та компанії "Distributed Lab", які надали свої рецензії, а також є позитивна оцінка генерального директора ТОВ "Микрокрипт Текнолоджис".

Опишіть практику збирання та врахування інформації щодо кар'єрного шляху татраєкторій працевлаштування випускників ОП *коротке поле*

НТУ «ХПІ», і зокрема на сайті Інституту комп'ютерних наук та інформаційних технологій сформовано систему збирання інформації щодо кар'єрного шляху випускників університету. Цим займається Навчально-методичний відділ договірної та практичної підготовки https://www.kpi.kharkov.ua/ukr/osvita/navchalno-metodychnyj-viddil-dogovirnoyi-i-praktychnoyi-pidgotovky/, Центр «Кар'єра» http://career.kharkov.ua/, 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. Кафедра проводить аналіз конкурентоспроможності майбутніх випускників шляхом дослідження ринку праці. У якості прикладу можна навести аналітичний звіт “Розвиток української ІТ-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? *довге поле*

За результатами співбесід зі здобувачами вступів 2019, 2020 рр. першого (бакалаврського) рівня вищих освіти було виявлено, що недостатня увага приділяється набуттю компетентностей щодо практичної роботи з розробки програмних застосунків та забезпечення їх безпеки. З урахуванням побажань здобувачів вищої освіти в ОП в рамках дисципліни “Інформаційні системи та Інтернет-технології” пропонується практична реалізація з розробки програмних застосунків, використання вбудованих засобів захисту з використанням мови Python та серверного фреймворку Django.
В блоці дисциплін “Програмування” запропоновано проходження курсів академії Cisco, а саме: ОК “Основи програмування” – курси “Programming Essentials in C”, “Advanced Programming in C”; ОК “Технології програмування” – курси “Programming Essentials in C++”, “CPP: Advanced Programming in C++”, “Programming Essentials In Python”. 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? *довге поле*

Акредитація ОПП умовна без проведення акредитації під час військового стану

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

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-bakalavr/
Опишіть розподіл відповідальності між різними структурними підрозділами ЗВО у контексті здійснення процесів і процедур внутрішнього забезпечення якості освіти*коротке поле*
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 https://blogs.kpi.kharkov.ua/v2/nv/; - 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 освітньогопроцесу? Яким чином забезпечується їх доступність для учасників освітнього процесу? *коротке поле*
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 здобувачів вищої освіти 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://blogs.kpi.kharkov.ua/v2/nv/dokumenty/normatyvni-dokumenty/ Положення про забезпечення якості освітньої діяльності та якості вищої освіти в НТУ «ХПІ» https://blogs.kpi.kharkov.ua/v2/quality/normatyvna-baza/; Положення про академічну мобільність студентів, аспірантів, докторантів, науково-педагогічних та наукових працівників університету; Положення про критерії та систему оцінювання знань та вмінь і про рейтинг студентів; https://blogs.kpi.kharkov.ua/v2/nv/dokumenty/normatyvni-dokumenty/ Положення про ректорат, Положення про Вчену раду, Положення про раду з якості, Положення по Наглядову раду, Положення про кафедру https://bit.ly/2QT0MjF.
Наведіть посилання на веб-сторінку, яка містить інформацію про оприлюднення наофіційному веб-сайті ЗВО відповідного проекту з метою отримання зауважень та пропозиції заінтересованих сторін (стейкхолдерів). Адреса веб-сторінки
https://cybersecurity.kpi.kharkov.ua/onovlennya-osvitnikh-program-125-bakalavr/
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-bakalavr/

11. Перспективи подальшого розвитку ОП

Якими загалом є сильні та слабкі сторони ОП? *довге поле*
Сильними сторонами ОП є впровадження сучасного підходу до підготовки бакалаврів з кібербезпеки, що дозволяє працевлаштовуватись програмістами-аналітиками зі знанням сучасних засобів та програмних застосунків забезпечення безпеки, фахівцями в кіберполіцію, подальше навчання на магістерському рівні у державні органи та СБУ. 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. Можливість організації спільних кібернавчань. В рамках гранту "Кібербезпека критично важливої інфраструктури України" кафедра отримала обладнання та програмного забезпечення на суму понад 1 200 000 грн. від Агентства США з міжнародного розвитку (USAID). 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? *довге поле*
Перспективами розвитку ОП є: - вдосконалення практичних проектів на базі лабораторії блокчейн-технології завдяки розширенню кількості серверів віртуалізації і розробки розподіленої мережі віртуальних машин для програмування задач, що містять блокчейн-рішення; - розширити залученість студентів до співпраці з міжнародною академічною спільнотою; - розширити роботу з компаніями-стейкхолдерами та залучити професіоналів-практиків до аудиторних занять на ОПП; - поширити практику залучення працівників кіберполіції з метою отримання практичного досвіду - забезпечити можливість вивчення навчальних дисциплін дистанційно.

Таблиця 1. *Інформація про обов'язкові освітні компоненти ОП*

Назва освітнього компонента	**Вид компонента**	**Поле для завантаження Силабусу**	**Якщо освітній компонент потребує спеціального матеріально-технічного та/або інформаційного забезпечення, наведіть відомості щодо нього**
Назва дисципліни*	дисципліна	X	Перелік обладнання, яке використовується при вивченні дисципліни. Перелік книжок з зазначенням їх кількості в бібліотеці або з зазначенням електронній ресурс, які використовується при вивченні дисципліни.
Антивірусний захист інформації	дисципліна спеціальна (фахова) підготовка	https://cybersecurity.kpi.kharkov.ua/sylabusy-osvitnikh-komponentiv-125-bakalavr/	**Обладнання:** **Кіберполігон:** Персональний комп` ютер 2E Integer Intel i5-11400/H510/16/480F/int/FreeDos/2E-S616/400W- 25 шт. Монітор HP P24 G5 FHD Monitor – 25 шт. Гарнітура для ПК 2E CH11, On-Ear, 3.5mm/2*3.5mm – 25 шт. Комплект 2E MK410 WL Black – 25 шт. Міжмережевий екран Fortinet FG- 40F 5*GE RJ45 ports (including 4* internal Ports 1* WAN Ports – 1 шт. Ноутбук/Notebook Del Vostro 3510/Core i3-1115G4/8GB/256GB SSD/15.6`` FHD/Intel UHD/Cam& Mic/WLAN + BT/Backlit Kb/3 Cell/W11Pro/3Yr – 2 шт. Багатофункціональний пристрій А4 ч/б Multifuntional device A4 b/w Xerox B235 (WI-FI) – 1 шт. Проєктор короткофокусний Epson EB-536Wi WXGA, 3400 lm, 0.65 інтерактивний – 1 шт. Проектор/ Projector Epson EB-X49 (3LCD, XGA,3600 ANSI lm) – 1 шт. Примірник ПЗ Microsoft Windows 11 Pro укр. OEM на DVD носії – 25 шт. Екран 2E на тринозі,1:1, 112, (2.0*2.0) – 1 шт. Сервер R- LINE на базі Xeon Silver 421 OR – 1 шт. Точка доступу Ubiguiti UniFi 6 LR Access Point U6-LR – 1 шт.

Назва освітнього компонента	Вид компонента	Поле для завантаження Силабусу	Якщо освітній компонент потребує спеціального матеріально-технічного та/або інформаційного забезпечення, наведіть відомості щодо нього
			Маршрутизатор Mikro Tik RB4011iGS+5HacQ2HnD-IN – 1 шт. Комутатор D-Link DGS-1210-28X/ME – 1 шт. Сервер HPE ML350 Gen10 Hot Plug LFF CTO – 1 шт. ДБЖ HPE T1000 Gen5 INTL UPS with Management Card Slot – 1шт. Комутатор Aruba 6000 48G 4SFP Switch – 1 шт. Aruba 1G SFP LC LX 10km SMF Transceiver – 2 шт. Aruba 1G SFP RJ45T 100m Cat5e Transceiver – 2 шт. **Література:** 1.Термінологічний довідник з питань технічного захисту інформації / Коженевський С.Р., Кузнецов Г.В., Хорошко В.О., Чирков Д.В./За ред. проф. В.О. Хорошка. – К.: ДУІКТ, 2007. – 365 с. 2. Дудатьєв А. В., Каплун В. А., Семеренко В. П. Захист програмного забезпечення. Частина 1. Навчальний посібник. – Вінниця: ВНТУ, 2005. – 140 с. Антивірусний захист інформації 3. Каплун В. А. Захист програмного забезпечення. Частина 2 : навчальний посібник. / В. А. Каплун, О. В. Дмитришин, Ю. В. Баришев – Вінниця: ВНТУ, 2014. 4. Synergy of building cybersecurity systems: monograph / S. Yevseiev, V. Ponomarenko, O. Laptiev, O. Milov and others. – Kharkiv: PC TECHNOLOGY CENTER, 2021. – 188 p. 5. Models of socio-cyber-physical systems security: monograph / S. Yevseiev, Yu. Khokhlachova, S. Os- tapov, O. Laptiev and others. – Kharkiv: PC TECHNOLOGY CENTER, 2023. – 168 p. 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.

Назва освітнього компонента	Вид компонента	Поле для завантаження Силабусу	Якщо освітній компонент потребує спеціального матеріально-технічного та/або інформаційного забезпечення, наведіть відомості щодо нього
Безпека в інформаційно-комунікаційних системах	дисципліна спеціальна (фахова) підготовка	https://cybersecurity.kpi.kharkov.ua/sylabusy-osvitnikh-komponentiv-125-bakalavr/	**Обладнання:** **Кіберполігон:** Персональний комп` ютер 2E Integer Intel i5-11400/H510/16/480F/int/FreeDos/2E-S616/400W- 25 шт. Монітор HP P24 G5 FHD Monitor – 25 шт. Гарнітура для ПК 2E CH11, On-Ear, 3.5mm/2*3.5mm – 25 шт. Комплект 2E MK410 WL Black – 25 шт. Міжмережевий екран Fortinet FG- 40F 5*GE RJ45 ports (including 4* internal Ports 1* WAN Ports – 1 шт. Ноутбук/Notebook Del Vostro 3510/Core i3-1115G4/8GB/256GB SSD/15.6`` FHD/Intel UHD/Cam& Mic/WLAN + BT/Backlit Kb/3 Cell/W11Pro/3Yr – 2 шт. Багатофункціональний пристрій А4 ч/б Multifuntional device A4 b/w Xerox B235 (WI-FI) – 1 шт. Проєктор короткофокусний Epson EB-536Wi WXGA, 3400 lm, 0.65 інтерактивний – 1 шт. Проектор/ Projector Epson EB-X49 (3LCD, XGA,3600 ANSI lm) – 1 шт. Примірник ПЗ Microsoft Windows 11 Pro укр. OEM на DVD носії – 25 шт. Екран 2E на тринозі,1:1, 112, (2.0*2.0) – 1 шт. Сервер R- LINE на базі Xeon Silver 421 OR – 1 шт. Точка доступу Ubiguiti UniFi 6 LR Access Point U6-LR – 1 шт. Маршрутизатор Mikro Tik RB4011iGS+5HacQ2HnD-IN – 1 шт. Комутатор D-Link DGS-1210-28X/ME – 1 шт. Сервер HPE ML350 Gen10 Hot Plug LFF CTO – 1 шт. ДБЖ HPE T1000 Gen5 INTL UPS with Management Card Slot – 1шт. Комутатор Aruba 6000 48G 4SFP Switch – 1 шт. Aruba 1G SFP LC LX 10km SMF Transceiver – 2 шт. Aruba 1G SFP RJ45T 100m Cat5e Transceiver – 2 шт. Література:

Назва освітнього компонента	Вид компонента	Поле для завантаження Силабусу	Якщо освітній компонент потребує спеціального матеріально-технічного та/або інформаційного забезпечення, наведіть відомості щодо нього
			1. С. П. Євсеєв. Технології захисту інформації / С. Е. Остапов, С. П. Євсеєв, О. Г. Король. – Чернівці. – Видавничий дом “Родовід”, 2014. – 428 с. 2. М.В. Захарченко, В.Г. Кононович, В.Й. Кільдішев, Д.В. Голев. «Інформаційна безпека інформаційно-комунікаційних систем: навчальний посібник. Лабораторний практикум. Частина 1. Комплекси засобів захисту інформації від НСД.». - 2011. Безпека в інформаційно-комунікаційних системах 3. Кузнецов О. О. Захист інформації в інформаційних системах. Методи традиційної криптографії / О. О. Кузнецов, С. П. Євсеєв, О. Г. Король. – Харків : Вид. ХНЕУ, 2010.– 316 с. 4. Synergy of building cybersecurity systems: monograph / S. Yevseiev, V. Ponomarenko, O. Laptiev, O. Milov and others. – Kharkiv: PC TECHNOLOGY CENTER, 2021. – 188 p. 5. Models of socio-cyber-physical systems security: monograph / S. Yevseiev, Yu. Khokhlachova, S. Os- tapov, O. Laptiev and others. – Kharkiv: PC TECHNOLOGY CENTER, 2023. – 168 p. 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. – 196p.
Безпека інтернет-речей	дисципліна спеціальна (фахова) підготовка	https://cybersecurity.kpi.kharkov.ua/sylabusy-osvitnikh-komponentiv-125-bakalavr/	**Обладнання:** **Кіберполігон:** Персональний комп` ютер 2E Integer Intel i5-11400/H510/16/480F/int/FreeDos/2E-S616/400W- 25 шт. Монітор HP P24 G5 FHD Monitor – 25 шт. Гарнітура для ПК 2E CH11, On-Ear, 3.5mm/2*3.5mm – 25 шт. Комплект 2E MK410 WL Black – 25 шт. Міжмережевий екран Fortinet FG- 40F 5*GE RJ45 ports (including 4* internal Ports 1* WAN Ports – 1 шт. Ноутбук/Notebook Del Vostro 3510/Core i3-1115G4/8GB/256GB

Назва освітнього компонента	Вид компонента	Поле для завантаження Силабусу	Якщо освітній компонент потребує спеціального матеріально-технічного та/або інформаційного забезпечення, наведіть відомості щодо нього
			SSD/15.6`` FHD/Intel UHD/Cam& Mic/WLAN + BT/Backlit Kb/3 Cell/W11Pro/3Yr – 2 шт. Багатофункціональний пристрій А4 ч/б Multifuntional device A4 b/w Xerox B235 (WI-FI) – 1 шт. Проєктор короткофокусний Epson EB-536Wi WXGA, 3400 lm, 0.65 інтерактивний – 1 шт. Проектор/ Projector Epson EB-X49 (3LCD, XGA,3600 ANSI lm) – 1 шт. Примірник П3 Microsoft Windows 11 Pro укр. OEM на DVD носії – 25 шт. Екран 2E на тринозі,1:1, 112, (2.0*2.0) – 1 шт. Сервер R- LINE на базі Xeon Silver 421 OR – 1 шт. Точка доступу Ubiguiti UniFi 6 LR Access Point U6-LR – 1 шт. Маршрутизатор Mikro Tik RB4011iGS+5HacQ2HnD-IN – 1 шт. Комутатор D-Link DGS-1210-28X/ME – 1 шт. Сервер HPE ML350 Gen10 Hot Plug LFF CTO – 1 шт. ДБЖ HPE T1000 Gen5 INTL UPS with Management Card Slot – 1шт. Комутатор Aruba 6000 48G 4SFP Switch – 1 шт. Aruba 1G SFP LC LX 10km SMF Transceiver – 2 шт. Aruba 1G SFP RJ45T 100m Cat5e Transceiver – 2 шт. **Література:** 1. Девід Роуз, Девід Роуз (David Rose), Майбутнє речей. Як казка та фантастика стають реальністю, ISBN: 978-5-91671-394-7, 2015. 2. Баранов А.А., Інтернет речей: теоретико-методологічні засади правового регулювання. Том І. Сфери застосування, ризики та бар'єри, проблеми правового регулювання, ISBN: 978-966-937-513-1, 2018, 344с. 3. Samuel Greengard, The Internet of Things (MIT Press Essential Knowledge series), ASIN: B00VB7I9VS, 2015, 230 P. 4. Cuno Pfister, Getting Started with the Internet of Things: Connecting Sensors and Microcontrollers to the Cloud (Make:

Назва освітнього компонента	Вид компонента	Поле для завантаження Силабусу	Якщо освітній компонент потребує спеціального матеріально-технічного та/або інформаційного забезпечення, наведіть відомості щодо нього
			Projects) 1st Edition, ASIN: B00COVJUGI, 2011, 194 P. 5. Erik Brynjolfsson and Andrew McAfee, The Second Machine Age: Work, Progress, and Prosperity in a Time of Brilliant Technologies 1st Edition, ASIN: B00D97HPQI, 2014, 320 P. 6. Thomas M. Siebel, Digital Transformation: Survive and Thrive in an Era of Mass Extinction, ASIN: B07SPDT74L, 2019, 253P. 7. Технології захисту інформації./ С. Е. Остапов, С. П. Євсєєв, О.Г. Король. – Чернівці : Чернівецький національний університет, 2013. – 471 с. 8. Євсєев С.П. Кібербезпека: основи кодування та криптографії/ С.П. Євсеєв, О.В. Мілов, С.Е. Остапов, О.В. Сєвєрінов. – Харків: Вид. “Новий Світ-2000”, 2023. – 657 с.
Бізнес інтелліджeнс	дисципліна спеціальна (фахова) підготовка	https://cybersecurity.kpi.kharkov.ua/sylabusy-osvitnikh-komponentiv-125-bakalavr/	**Обладнання:** Мультимедійні аудиторії ПК: Intel Pentium G4560/ОЗУ 4 GB DDR3-1600/Монітор 20" Dell P2017H/HDD 500 GB, 7200 об/хв, SATA 3.0 – 15шт. QlikView, QlikSense, Microsoft Power BI **Література:** 1. Савчук В.П. Оцифрований менеджмент: Business Intelligence для ТОПів. К.: "Баланс Бізнес Букс", 2017. - 504 с. 2. Величко О.М Основи системного аналізу і прийняття оптимальних рішень підручник /О.М. Величко, Т.Б. Гордієнко. – К: Олді, 2021. – 672 с. 3. Алексієв В. О. Застосування GRID-технології у транспортному ВНЗ : навч.-метод. посіб. / В. О. Алексієв.– Харків : ХНАДУ, 2008. – 208 с. Бізнес інтелліджeнс 4. Технології захисту інформації./ С. Е. Остапов, С. П. Євсєєв, О.Г. Король. – Чернівці : Чернівецький національний університет, 2013. – 471 с.

Назва освітнього компонента	Вид компонента	Поле для завантаження Силабусу	Якщо освітній компонент потребує спеціального матеріально-технічного та/або інформаційного забезпечення, наведіть відомості щодо нього
			5. WEB-технології [Електронний ресурс]: Навчально-довідковий посібник / С.П. Євсеєв, А.М. Ткачов, В.О. Алексієв, Ю.М. Рябуха – Харків : ХНЕУ ім. С. Кузнеця, – Львів: Видавництво «Новий Світ –2000», 2021. – 390 с. 6. Євсєєв С.П. Кібербезпека: основи кодування та криптографії/ С.П. Євсеєв, О.В. Мілов, С.Е. Остапов, О.В. Сєвєрінов. – Харків: Вид. “Новий Світ-2000”, 2023. – 657 с.
Введення в мережі	дисципліна спеціальна (фахова) підготовка	https://cybersecurity.kpi.kharkov.ua/sylabusy-osvitnikh-komponentiv-125-bakalavr/	**Обладнання:** **Мультимедійні аудиторії** Laptop (Hoyr6YK) 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., ASA 5506 – 1 шт. Cisco комутатор Catalyst 3750 – 4 шт. Cisco Маршрутизатор 2911 з IPS – 2 шт. Packet Tracer **Література:** 1. Технології захисту інформації./ С. Є. Остапов, С. П. Євсєєв, О.Г. Король. – Чернівці: Чернівецький національний університет, 2013. – 471 с. 2. Волосюк Ю.В. Комп'ютерні мережі: курс лекцій / Ю. В. Волосюк. - Миколаїв: МНАУ, 2019. - 203 с.

Назва освітнього компонента	Вид компонента	Поле для завантаження Силабусу	Якщо освітній компонент потребує спеціального матеріально-технічного та/або інформаційного забезпечення, наведіть відомості щодо нього
			3. Kurose James F., Ross Keith W. Computer Networking: A Top-Down Approach. 6th Edition / James F. Kurose, Keith W. Ross. - TX: Pearson, 2012. - 864 p. 4. CCNAv7: Введення в ресурси курсу Networks [Електронний ресурс]. – Режим доступу: https://www.netacad.com/portal/resources/course-resources/ccna-itn. 5. Bonaventure O. Computer Networking: Principls, Protocols and Practice. - Louvain-la-Neuve: Universite catholique de Louvain (Belgium), 2019. - 272 p. 6. Євсеєв С.П., Білова М.О., Жученко О.С., Іванченко С.І., Шматко О.В. Технологія Ethernet: лабораторний практикум з курсу “Комп'ютерні мережі” студентів спеціальностей 121, 122, 126. Львів: “Новий Світ-2000”, 2020. – 196 с. 7. Євсеєв С.П., Остапов С.Є., Король О.Г. Кібербезпека: сучасні технології захисту: навч. посіб. для студ. вищ. навч. закл. Львів: “Новий Світ-2000”, 2019. – 678 с.
Вища математика	дисципліна загальна підготовка	https://cybersecurity.kpi.kharkov.ua/sylabusy-osvitnikh-komponentiv-125-bakalavr/	**Обладнання:** 11 Pentium 4 3.4 GHz1 GB Visual Paradigm 5.1, RAMUS 2.0 **Література:** 1. Вища математика в прикладах і задачах у 2-х томах. За редакцією Курпи Л.В. Том 1. Аналітична геометрія та лінійна алгебра. Диференціальне та інтегральне числення функцій однієї змінної. – Харків: НТУ “ХПІ”, 2009. 2. Вища математика в прикладах і задачах у 2-х томах. За редакцією Курпи Л.В. Том 2. Диференціальне та інтегральне числення функцій багатьох змінних. Диференціальні рівняння та ряди. – Харків: НТУ “ХПІ”, 2009. 3. Тевяшев А.Д., Литвин О.Г. Вища математика у прикладах та задачах. Частина 1. Лінійна алгебра і аналітична геометрія. Диференціальне числення функцій однієї змінної. – Харків:

Назва освітнього компонента	Вид компонента	Поле для завантаження Силабусу	Якщо освітній компонент потребує спеціального матеріально-технічного та/або інформаційного забезпечення, наведіть відомості щодо нього
			ХТУРЕ, 2002. 4. Тевяшев А.Д., Литвин О.Г., Кривошеєва Г.М., Обухова Л.В., Середа О.Г. Вища математика у прикладах та задачах. Частина 2. Інтегральне числення функцій однієї змінної. Диференціальне та інтегральне числення функцій багатьох змінних. – Харків: ХТУРЕ, 2002. 5. Тевяшев А.Д., Литвин О.Г., Кривошеєва Г.М., Обухова Л.В., Середа О.Г., Головко Н.О. Вища математика у прикладах та задачах. Частина 3. Диференціальні рівняння. Ряди. Функції комплексної змінної. Операційне числення. – Харків: ХТУРЕ, 2002. 6. Dummit D.S., Foote R.M. Abstract algebra. 3rd Edition. – John Wiley and Sons, Inc., 2004. 7. Lang S. Algebra. Revised 3rd Edition. – Springer-Verlag, 2002.
Вступ до спеціальності. Ознайомча практика	дисципліна спеціальна (фахова) підготовка	https://cybersecurity.kpi.kharkov.ua/sylabusy-osvitnikh-komponentiv-125-bakalavr/	**Обладнання:** Мультимедійні аудиторії ПК з доступом до Інтернету, MS Word, MS Excel **Література:** 1. 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. 2. Edited by Serhii Yevseiev, Yuliia Khokhlachova, Serhii Ostapov, Oleksandr Laptiev Serhii Yevseiev, Yuliia Khokhlachova, Serhii Ostapov, Oleksandr Laptiev, Olha Korol, Stanislav Milevskyi, Oleksandr Milov, Serhii Pohasii, Yevgen Melenti, Hrebeniuk Vitalii, Alla Havrylova, Serhii Herasymov, Roman Korolev, Oleg Barabash, Valentyn Sobchuk, Roman Kyrychok, German Shuklin, Volodymyr Akhramovych, Vitalii Savchenko, Sergii Golovashych, Oleksandr Lezik, Ivan Opirskyy, Oleksandr Voitko, Kseniia Yerhidzei, Serhii Mykus, Yurii Pribyliev, Oleksandr Prokopenko, Andrii Vlasov, Nataliia

Назва освітнього компонента	Вид компонента	Поле для завантаження Силабусу	Якщо освітній компонент потребує спеціального матеріально-технічного та/або інформаційного забезпечення, наведіть відомості щодо нього
			Dzheniuk, Maksym Tolkachov Models of socio-cyber-physical systems security: monograph / S. Yevseiev, Yu. Khokhlachova, S. Os- tapov, O. Laptiev and others. – Kharkiv: PC TECHNOLOGY CENTER, 2023. – 168 p. 3. Edited by Serhii Yevseiev, Ruslan Hryshchuk, Kateryna Molodetska, Mariia Nazarkevych Serhii Yevseiev, Ruslan Hryshchuk, Kateryna Molodetska, Mariia Nazarkevych, Volodymyr Hrytsyk, Oleksandr Milov, Olha Korol, Stanislav Milevskyi, Roman Korolev, Serhii Pohasii, Andrii Tkachov, Yevgen Melenti, Oleksandr Lavrut, Alla Havrylova, Serhii Herasymov, Halyna Holotaistrova, Dmytro Avramenko, Roman Vozniak, Oleksandr Voitko, Kseniia Yerhidzei, Serhii Mykus, Yurii Pribyliev, Olena Akhiiezer, Mykhailo Shyshkin, Ivan Opirskyy, Oleh Harasymchuk, Olha Mykhaylova, Yuriy Nakonechnyy, Marta Stakhiv, Bogdan Tomashevsky 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. 4. Технології захисту інформації./ С. Е. Остапов, С. П. Євсєєв, О.Г. Король. – Чернівці : Чернівецький національний університет, 2013. – 471 с.
Іноземна мова	дисципліна загальна підготовка	https://cybersecurity.kpi.kharkov.ua/sylabusy-osvitnikh-komponentiv-125-bakalavr/	**Обладнання:** Мультимедійні аудиторії **Література:** 1. Glenda Gay. Oxford Information Technology for CSEC: Third edition/ Glenda Gay, Ronald Blades. - Oxford University Press, 2018. – 320p. 2. Glenda Gay. Oxford Information Technology for CSEC Workbook: Third Edition/ Glenda Gay, Ronald Blades - Oxford University Press, 2019. – 96p. 3. Eric H. Glendinning. Oxford English for Information Technology: Student’s book. / Eric H. Glendinning. – Oxford: Macmillan, Eric H.

Назва освітнього компонента	Вид компонента	Поле для завантаження Силабусу	Якщо освітній компонент потребує спеціального матеріально-технічного та/або інформаційного забезпечення, наведіть відомості щодо нього
			Glendinning 2015. -137p. 4. Frances Eales, Steve Oakes. Speak Out. Intermediate. Students' book. Pearson Education Limited, 2015. – 176p. 5. O'Dell Felicity. Objective Advanced. Student's Book. 4th ed. / O'Dell Felicity, Broadhead Annie. - Cambridge University Press, 2014. - 232p. 6. O'Dell Felicity, Broadhead Annie. Objective IELTS Advanced Workbook / O'Dell Felicity, Broadhead Annie. - Cambridge University Press. 2016. – 101c. 7. Functional structures of academic English. Методичні вказівки до практичних занять з курсу «Англійська мова за професійним спрямуванням» для студентів всіх спеціальностей / уклад. Лазарєва О. Я., Ковтун О.О., Дьомочка Л.В., Харків: НТУ "ХПІ", 2019. – 44с. 8. Allsop J. BEC Vantage Testbuilder / J. Allsop, T. Aspinall. – Oxford: Macmillan, 2015. – 154 p. 9. Pauline Cullen. Common Mistakes at IELTS Intermediate Paperback with IELTS General Training Testbank: And How to Avoid Them. - Cambridge English, 2016. - 64p. 10. Bazin A. Achieve IELTS. Practice Tests / A. Bazin, E. Boyd. – London: Marshal Cavendish Ltd, 2017. – 114 p. 11. Aileen Pincus. Essential Managers: Presenting. / - Aileen Pincus. - Dorling Kindersley, 2015. – 96p. 12. Mark Powell. Presenting in English: How to Give Successful Presentations (Updated Edition). - National Geographic Learning, 2012. - 127p. 13. Gwenn Wilson. 100% Job Search Success (100% Success Series) 3rd Edition. / Gwenn Wilson, Cengage Learning, 2014, - 240p. 14. O.Lazareva, O.Kovtun, L.Dyomochka. Science speaks English. Kharkiv: NTU "KhPI", 2019. – 276p. 15. Jackie Black. Working Virtually International management English. / Jackie Black. - Delta Publishing, 2020. – 119p.

Назва освітнього компонента	Вид компонента	Поле для завантаження Силабусу	Якщо освітній компонент потребує спеціального матеріально-технічного та/або інформаційного забезпечення, наведіть відомості щодо нього
			16. Diana Hopkins, Pauline Cullen. IELTS Grammar for Bands 6.5 and above. Cambridge University Press, 2021. – 268p. 17. Jane Bottomley. Academic Writing for International Students of Science, 2nd edition / Jane Bottomley: Routledge, 2021 – 220p. 18. Brown R. IELTS Advantage. Writing skills / R. Brown, L. Richards. – Cambridge: Cambridge University Press, 2015. – 129 p. Іноземна мова 19. Terry M. Focus on academic skills for IELTS / M.Terry, J. Wilson. – London: Pearson Longman. 2017. – 91 p. 20. Gear J. Cambridge Preparation for the TOEFL Test / J. Gear, R. Gear. – Cambridge: Cambridge University Press, 2017. – 120 p.
Інформаційна безпека держави	дисципліна спеціальна (фахова) підготовка	https://cybersecurity.kpi.kharkov.ua/sylabusy-osvitnikh-komponentiv-125-bakalavr/	**Обладнання:** Мультимедійні аудиторії, ПК з доступом до Інтернету Packet Tracer **Література:** 1. Євсеєв С.П., Остапов С.Є., Король О.Г. Кібербезпека: сучасні технології захисту: навч. посіб. для студ. вищ. навч. закл. Львів: “Новий Світ-2000”, 2019. – 678 с. 2. Богуш В. М., Юдін О. К. Інформаційна безпека держави. - К.: "МК-Прес", 2005. - 432с. 3. Термінологічний довідник з питань технічної захисту інформації / Коженевський С.Р., Кузнєцов Г.В., Хорошко В.О., Чирков Д.В. / За ред. проф. В.О. Хорошка. - К.: ДУІКТ, 2007. - 365 с. 4. Бобало Ю.Я., Горбатій І.В. (ред.) Інформаційна безпека. Навчальний посібник. - Львів: Видавництво Львівської політехніки, 2019. - 580 с. - ISBN 978-966-941-339-0. 5. Інформаційна безпека держави: навч. посіб. для студ. спец. 6.170103 Управління інформаційною безпекою, 125 Кібербезпека / В.І. Гур'єв, Д.Б. Мехед, Ю.М. Ткач, І.В. Фірсова.

Назва освітнього компонента	Вид компонента	Поле для завантаження Силабусу	Якщо освітній компонент потребує спеціального матеріально-технічного та/або інформаційного забезпечення, наведіть відомості щодо нього
			– Ніжин: ФОП Лук'яненко В.В. ТПК "Орхідея", 2018. - 166 с.
Історія та культура України	дисципліна загальна підготовка	https://cybersecurity.kpi.kharkov.ua/sylabusy-osvitnikh-komponentiv-125-bakalavr/	**Обладнання:** не потребує **Література:** 1. Aleksieiev Y. A. History of Ukraine. Third edition / Y. Aleksieiev. Kyiv : Caravela, 2017. 216 p. 2. Shyshkina Y. K. A History of Ukraine: Presentations for English-Speaking Students = Історія України: презентації для англомовних студентів : texts of lectures / Y. K. Shyshkina. Kharkiv : NTU «KhPI», 2016. 176 p. 3. Бойко О. Д. Історія України : підручник / О. Д. Бойко. 7-ме вид., стер. Київ : Академія, 2018. 717 с. 4. Бугрій В. С. Історія та культура України : навч. посіб. / В. С. Бугрій ; М-во освіти і науки України, Сум. держ. пед. ун-т ім. А. С. Макаренка. Суми : Цьома С. П., 2017. 316 с. 5. Греченко В. А. Історія та культура України : підручник / В. А. Греченко ; МВС України, Харків. нац. ун-т внутр. справ. Харків : Харків. нац. ун-т внутр. справ, 2017. 319 с. 6. Грицак Я. Нарис історії України: формування української модерної нації XIX – XX ст. / Я. Грицак. Київ, 2019. 656 с. 7. Грицак Я. Подолати минуле: глобальна історія України / Я. Грицак. Київ : Портал, 2021. 432 с. 8. Історія та культура України : метод. вказівки для студентів заочної форми навчання усіх спеціальностей / Укладачі О. О. Петутіна, Л. П. Савченко. Харків : НТУ «ХПІ», 2019. 30 с. 9. Історія та культура України : підруч. для студентів техн. спец. ВНЗ / М. І. Бушин, О. М. Бут, О. І. Гуржій, С. М. Ховрич ; М-во освіти і науки України, Черкас. держ. технол. ун-т. Черкаси : Гордієнко Є. І., 2018. 1152 с. 10. Історія та культура України : навч. посіб. для студентів неісторич. спец. / [Т. В. Кузнець, О. В. Лісовська, О. В. Скус] ; М-во освіти і науки України, Уман. держ. пед. ун-т ім. П.

Назва освітнього компонента	Вид компонента	Поле для завантаження Силабусу	Якщо освітній компонент потребує спеціального матеріально-технічного та/або інформаційного забезпечення, наведіть відомості щодо нього
			Тичини. Умань : Сочінський М. М., 2017. 175 с. 11. Коршунова І. П. Історія та культура України : навч. посіб. / І. П. Коршунова, Н. А. Лемешева, А. С. Міносян ; М-во освіти і науки України, Харків. держ. ун-т харчування та торгівлі. Харків : Смугаста тип., 2017. 170 с. 12. Михайлуца М. І. Історія України і її державності: осучаснений погляд : навч. посіб. / М. Михайлуца, О. Шипотілова ; М-во освіти і науки України, Одес. нац. мор. ун-т, Навч.-наук. мор. гуманітар. ін-т. Вид. 2-ге, допов. Херсон : Олді-плюс, 2018. 172 с. 13. Плани групових занять та індивідуальні завдання з дисципліни «Історія України та українська культура». Методичні рекомендації для курсантів Військового інститут танкових військ НТУ «ХПІ» / уклад: Дворкін І.В., Телуха С.С., Фрадкіна Н.В. – Харків: НТУ «ХПІ», 2020. 25 с. 14. Плани семінарів та методичні рекомендації з дисципліни «Історія та культура України» : навч.-метод. посібник для студ. усіх спец. / заг. ред. : О. О. Петутіна, Л. П. Савченко ; Нац. техн. ун-т «Харків. політехн. ін-т». Харків : НТУ «ХПІ», 2019. 55 с. 15. Плохій С. Брама Європи : історія України від скіфських воєн до незалежності / Сергій Плохій ; [пер. з англ. Р. Клочка]. 2-ге вид. Харків : Клуб сімейн. дозвілля, 2018. 493 с. 16. Українська культура в іменах. Довідник [для студ. усіх спеціальн.] / О. О. Петутіна, Н. В. Вандишева-Ребро, О. В. Голозубов [та ін.]; за ред. О. О. Петутіної. Харків: НТУ «ХПІ», 2017. 303 с.
Кібербезпека. Правові основи та технології.	дисципліна спеціальна (фахова) підготовка	Х	**Обладнання:** Мультимедійні аудиторії, ПК з доступом до Інтернету **Література:** 1. TI (2015), Corruption: Lessons from the international mission in Afghanistan. p 20. CIDS (2015) Criteria for Good Governance in the

Назва освітнього компонента	Вид компонента	Поле для завантаження Силабусу	Якщо освітній компонент потребує спеціального матеріально-технічного та/або інформаційного забезпечення, наведіть відомості щодо нього
			Defence Sector: International Standards and Principles. p 3. CIDS, Integrity Action Plan, p 10. 2. ДКЗС (2015), Parliamentary Brief: Building integrity in Defence . 3. НАТО-ДКЗС, (2010). Виховання доброчесності і боротьба з корупцією в оборонному секторі. Збірник прикладів (компендіум) позитивного досвіду, стор. 5. 4. НАТО-ДКЗС, (2010). Виховання доброчесності, стор. 151-152. See: Mats R. Berdal and David Malone, eds., Greed and Grievance: Economic Agendas in Civil Wars. (London 2009). 5. ДКЗС (2009), Інформаційний матеріал. Security Sector Governance and Reform. 6. Робоча група ООН з РСБ (2012), Security Sector Reform: Integrated Technical Guidance Notes, p. 92. 7. ДКЗС (2009), Інформаційний матеріал. Security Sector Governance and Reform. Кібербезпека. Правові основи та технології 8. Робоча група ООН з РСБ (2012), Security Sector Reform. Integrated Technical Guidance Notes. p. 95. 9. ЦДОС (2015) Guides to Good Governance: Professionalism and Integrity in the Public Service. No 1. 10. НАТО-ДКЗС, (2010). Виховання доброчесності та боротьба з корупцією в оборонному секторі. 11. Збірник прикладів (компендіум) позитивного досвіду. 12. Гарі Букур-Марку, Оборонний менеджмент: Ознайомлення, ДКЗС (2009) Security and Defence Management Series no 1. стор. 4. 13. Тері Макконвіль, Річард Холмс (ред.), Defence Management in Uncertain Times. Cranfield Defence Management Series Number 3. Routledge 2011. 14. Гарі Букур-Марку, Філіпп Флурі, Тодор Тагарев (ред.), Оборонний менеджмент: Ознайомлення. Security and Defence Management Series No1. ДКЗС(2009) p5.

Назва освітнього компонента	Вид компонента	Поле для завантаження Силабусу	Якщо освітній компонент потребує спеціального матеріально-технічного та/або інформаційного забезпечення, наведіть відомості щодо нього
			15. НАТО-ДКЗС, (2010). Виховання доброчесності та боротьба з корупцією в оборонному секторі. Збірник прикладів (компендіум) позитивного досвіду. “Нормативно-правове забезпечення” стор. 176. 16. Конвенція Організації Об‘єднаних Націй проти корупції ЮНОДК: https://www.unodc.org/unodc/en/treaties/CAC/; Конвенція про відмивання, пошук, арешт та конфіскацію доходів, одержаних злочинним шляхом, Рада Європи: http://conventions.coe.int/Treaty/en/Treaties/Html/141.htm ; Конвенція про відмивання, пошук, арешт та конфіскацію доходів, одержаних злочинним шляхом та фінансування тероризму, Рада Європи: http://conventions.coe.int/Treaty/EN/Treaties/Html/198.htm. 17. Конвенція про кримінальну відповідальність за корупцію, Рада Європи, 1999. Доступно на: http://conventions.coe.int/Treaty/EN/Treaties/Html/173.htm. 18. НАТО-ДКЗС, (2010). Виховання доброчесності та боротьба з корупцією, стор. 175. Available at: https://fba.se/en/how-we-work/research-policy-analysis-and-development/publications/international-support-to-security-sector-reform-in-ukraine/.
Комплексний тренінг	дисципліна спеціальна (фахова) підготовка	https://cybersecurity.kpi.kharkov.ua/sylabusy-osvitnikh-komponentiv-125-bakalavr/	**Обладнання:** **Кіберполігон:** Персональний комп` ютер 2E Integer Intel i5-11400/H510/16/480F/int/FreeDos/2E-S616/400W- 25 шт. Монітор HP P24 G5 FHD Monitor – 25 шт. Гарнітура для ПК 2E CH11, On-Ear, 3.5mm/2*3.5mm – 25 шт. Комплект 2E MK410 WL Black – 25 шт. Міжмережевий екран Fortinet FG- 40F 5*GE RJ45 ports (including 4* internal Ports 1* WAN Ports – 1 шт. Ноутбук/Notebook Del Vostro 3510/Core i3-1115G4/8GB/256GB

Назва освітнього компонента	Вид компонента	Поле для завантаження Силабусу	Якщо освітній компонент потребує спеціального матеріально-технічного та/або інформаційного забезпечення, наведіть відомості щодо нього
			SSD/15.6`` FHD/Intel UHD/Cam& Mic/WLAN + BT/Backlit Kb/3 Cell/W11Pro/3Yr – 2 шт. Багатофункціональний пристрій А4 ч/б Multifuntional device A4 b/w Xerox B235 (WI-FI) – 1 шт. Проєктор короткофокусний Epson EB-536Wi WXGA, 3400 lm, 0.65 інтерактивний – 1 шт. Проектор/ Projector Epson EB-X49 (3LCD, XGA,3600 ANSI lm) – 1 шт. Примірник П3 Microsoft Windows 11 Pro укр. OEM на DVD носії – 25 шт. Екран 2E на тринозі,1:1, 112, (2.0*2.0) – 1 шт. Сервер R- LINE на базі Xeon Silver 421 OR – 1 шт. Точка доступу Ubiguiti UniFi 6 LR Access Point U6-LR – 1 шт. Маршрутизатор Mikro Tik RB4011iGS+5HacQ2HnD-IN – 1 шт. Комутатор D-Link DGS-1210-28X/ME – 1 шт. Сервер HPE ML350 Gen10 Hot Plug LFF CTO – 1 шт. ДБЖ HPE T1000 Gen5 INTL UPS with Management Card Slot – 1шт. Комутатор Aruba 6000 48G 4SFP Switch – 1 шт. Aruba 1G SFP LC LX 10km SMF Transceiver – 2 шт. Aruba 1G SFP RJ45T 100m Cat5e Transceiver – 2 шт. **Література:** 1. Kali Linux Web Penetration Testing Cookbook, Second Edition (Packt Publishing) URL: https://www.packtpub.com/product/kali-linux-web-penetration-testing-cookbook-second-edition/9781788991513. 2. Зразок звіту з тестування на проникнення URL: https://www.offensive-security.com/reports/sample-penetration-testing-report.pdf. 3. Зразок технічного звіту з проникнення URL: https://tbgsecurity. 4. OWASP Top 10: issues in the 10 most critical security risk

Назва освітнього компонента	Вид компонента	Поле для завантаження Силабусу	Якщо освітній компонент потребує спеціального матеріально-технічного та/або інформаційного забезпечення, наведіть відомості щодо нього
			categories in your web applications URL: https://www.sonarqube.org/features/security/owasp/?gads_campaign=Europe-1-Generic&gads_ad_group=OWASP&gads_keyword=owasp%20top%2010&gclid=CjwKCAiAsNKQBhAPEiwAB-I5zQywzTKai6fcrilMphlAn21CRehrI0q9DEjUZNpHUoDt5V_bVpLm4RoClIkQAvD_BwE. 5. Технології захисту інформації./ С. Е. Остапов, С. П. Євсєєв, О.Г. Король. – Чернівці : Чернівецький національний університет, 2013. – 471 с. 6. Євсєев С.П. Кібербезпека: основи кодування та криптографії/ С.П. Євсеєв, О.В. Мілов, С.Е. Остапов, О.В. Сєвєрінов. – Харків: Вид. “Новий Світ-2000”, 2023. – 657 с.
Комплексні засоби захисту інформації	дисципліна спеціальна (фахова) підготовка	https://cybersecurity.kpi.kharkov.ua/sylabusy-osvitnikh-komponentiv-125-bakalavr/	**Обладнання:** **Кіберполігон:** Персональний комп` ютер 2E Integer Intel i5-11400/H510/16/480F/int/FreeDos/2E-S616/400W- 25 шт. Монітор HP P24 G5 FHD Monitor – 25 шт. Гарнітура для ПК 2E CH11, On-Ear, 3.5mm/2*3.5mm – 25 шт. Комплект 2E MK410 WL Black – 25 шт. Міжмережевий екран Fortinet FG- 40F 5*GE RJ45 ports (including 4* internal Ports 1* WAN Ports – 1 шт. Ноутбук/Notebook Del Vostro 3510/Core i3-1115G4/8GB/256GB SSD/15.6`` FHD/Intel UHD/Cam& Mic/WLAN + BT/Backlit Kb/3 Cell/W11Pro/3Yr – 2 шт. Багатофункціональний пристрій А4 ч/б Multifuntional device A4 b/w Xerox B235 (WI-FI) – 1 шт. Проєктор короткофокусний Epson EB-536Wi WXGA, 3400 lm, 0.65 інтерактивний – 1 шт. Проектор/ Projector Epson EB-X49 (3LCD, XGA,3600 ANSI lm) – 1 шт.

Назва освітнього компонента	Вид компонента	Поле для завантаження Силабусу	Якщо освітній компонент потребує спеціального матеріально-технічного та/або інформаційного забезпечення, наведіть відомості щодо нього
			Примірник П3 Microsoft Windows 11 Pro укр. OEM на DVD носії – 25 шт. Екран 2E на тринозі,1:1, 112, (2.0*2.0) – 1 шт. Сервер R- LINE на базі Xeon Silver 421 OR – 1 шт. Точка доступу Ubiguiti UniFi 6 LR Access Point U6-LR – 1 шт. Маршрутизатор Mikro Tik RB4011iGS+5HacQ2HnD-IN – 1 шт. Комутатор D-Link DGS-1210-28X/ME – 1 шт. Сервер HPE ML350 Gen10 Hot Plug LFF CTO – 1 шт. ДБЖ HPE T1000 Gen5 INTL UPS with Management Card Slot – 1шт. Комутатор Aruba 6000 48G 4SFP Switch – 1 шт. Aruba 1G SFP LC LX 10km SMF Transceiver – 2 шт. Aruba 1G SFP RJ45T 100m Cat5e Transceiver – 2 шт. **Література:** 1. Технічний захист інформації в інформаційних та телекомунікаційних системах: Навчальний посібник / укл.: Г. І. Ластівка, П. М. Шпатар – Чернівці: Чернівецький національний університет, 2018. – 252 с. 2. Олейніков А.М., Методи та засоби захисту інформації. Навчальний посібник для студентів вищих навчальних закладів./ – Харків: НТМТ, 2014 – 298с. 3. Технічні канали витоку інформації. Порядок створення комплексів технічного захисту інформації. Навчальний посібник / Іванченко С.О., Гавриленко О.В., Липський О.А., Шевцов А.С. – К.: ІСЗЗІ НТУУ «КПІ», 2016. – 104 с. 4. Стратегія кібербезпеки України" (Введено в дію Указом Президента України від 15 березня 2016 року №96/2016). 5. Закон України "Про захист інформації в інформаційно-телекомунікаційних системах" (1994). 6. ДСТУ 3396.0-96. Захист інформації. Технічний захист інформації. Основні положення. Чинний від 1997-07-01. Київ. Держстандарт України, 1997. – 10 с.

Назва освітнього компонента	Вид компонента	Поле для завантаження Силабусу	Якщо освітній компонент потребує спеціального матеріально-технічного та/або інформаційного забезпечення, наведіть відомості щодо нього
			7. Технології захисту інформації./ С. Е. Остапов, С. П. Євсєєв, О.Г. Король. – Чернівці : Чернівецький національний університет, 2013. – 471 с. 8. Євсєєв С.П. Кібербезпека: основи кодування та криптографії/ С.П. Євсеєв, О.В. Мілов, С.Е. Остапов, О.В. Сєвєрінов. – Харків: Вид. "Новий Світ-2000", 2023. – 657 с.
Комплексні системи захисту інформації	дисципліна спеціальна (фахова) підготовка	https://cybersecurity.kpi.kharkov.ua/sylabusy-osvitnikh-komponentiv-125-bakalavr/	**Обладнання** **Кіберполігон:** Персональний комп` ютер 2E Integer Intel i5-11400/H510/16/480F/int/FreeDos/2E-S616/400W- 25 шт. Монітор HP P24 G5 FHD Monitor – 25 шт. Гарнітура для ПК 2E CH11, On-Ear, 3.5mm/2*3.5mm – 25 шт. Комплект 2E MK410 WL Black – 25 шт. Міжмережевий екран Fortinet FG- 40F 5*GE RJ45 ports (including 4* internal Ports 1* WAN Ports – 1 шт. Ноутбук/Notebook Del Vostro 3510/Core i3-1115G4/8GB/256GB SSD/15.6`` FHD/Intel UHD/Cam& Mic/WLAN + BT/Backlit Kb/3 Cell/W11Pro/3Yr – 2 шт. Багатофункціональний пристрій А4 ч/б Multifuntional device A4 b/w Xerox B235 (WI-FI) – 1 шт. Проєктор короткофокусний Epson EB-536Wi WXGA, 3400 lm, 0.65 інтерактивний – 1 шт. Проектор/ Projector Epson EB-X49 (3LCD, XGA,3600 ANSI lm) – 1 шт. Примірник ПЗ Microsoft Windows 11 Pro укр. OEM на DVD носії – 25 шт. Екран 2E на тринозі,1:1, 112, (2.0*2.0) – 1 шт. Сервер R- LINE на базі Xeon Silver 421 OR – 1 шт. Точка доступу Ubiguiti UniFi 6 LR Access Point U6-LR – 1 шт. Маршрутизатор Mikro Tik RB4011iGS+5HacQ2HnD-IN – 1 шт. Комутатор D-Link DGS-1210-28X/ME – 1 шт.

Назва освітнього компонента	Вид компонента	Поле для завантаження Силабусу	Якщо освітній компонент потребує спеціального матеріально-технічного та/або інформаційного забезпечення, наведіть відомості щодо нього
			Сервер HPE ML350 Gen10 Hot Plug LFF CTO – 1 шт. ДБЖ HPE T1000 Gen5 INTL UPS with Management Card Slot – 1шт. Комутатор Aruba 6000 48G 4SFP Switch – 1 шт. Aruba 1G SFP LC LX 10km SMF Transceiver – 2 шт. Aruba 1G SFP RJ45T 100m Cat5e Transceiver – 2 шт. **Література:** 1. Закон України "Про захист інформації в інформаційно-телекомунікаційних системах" (1994). 2. Закон України "Про захист персональних даних" (2010). 3. СТРАТЕГІЯ національної безпеки України (затверджена Указом Президента України від 26 травня 2015 року № 287/2015). 4. Закон України "Про національну безпеку (2018). 5. Стратегія кібербезпеки України" (Введено в дію Указом Президента України від 15 березня 2016 року №96/2016). 6. Положення про технічний захист інформації в Україні, затверджене Указом Президента України від 27.09.99 № 1229. 7. ДСТУ 3396 0-96 Захист інформації. Технічний захист інформації. Основні положення. 8. 3396 1-96 Захист інформації. Технічний захист інформації. Порядок проведення робіт. 9. НД ТЗІ 2.1-001-2001 Створення комплексів технічного захисту інформації. Атестація комплексів. Основні положення. 10. НД ТЗІ 1.1-003-99: Термінологія в області захисту інформації в комп'ютерних системах від несанкціонованого доступу. НД ТЗІ 2.5-004-99: Критерії оцінки захищеності інформації у комп'ютерних системах від несанкціонованого доступу. Затверджено наказом ДСТСЗІ СБУ № 22 від 28.04.1999. ДСТСЗІ СБУ, К: 1999. – 34с. 11. НД ТЗІ 1.1-002-99. Загальні положення щодо захисту інформації в комп'ютерних системах від несанкціонованого доступу. 12. НД ТЗІ 1.1-003-99. Термінологія в області захисту інформації в

Назва освітнього компонента	Вид компонента	Поле для завантаження Силабусу	Якщо освітній компонент потребує спеціального матеріально-технічного та/або інформаційного забезпечення, наведіть відомості щодо нього
			комп'ютерних системах від несанкціонованого доступу. Комплексні системи захисту інформації 13. НД ТЗІ 1.1-005-07 Захист інформації на об’єктах інформаційної діяльності. Створення комплексу технічного захисту інформації. Основні положення. 14. НД ТЗІ 1.4-001-00. Типове положення про службу захисту інформації в автоматизованій системі. 15. НД ТЗІ 2.5-004-99. Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу. 16. НД ТЗІ 2.5-005-99. Класифікація автоматизованих систем і стандартні функціональні профілі захищеності оброблюваної інформації від несанкціонованого доступу. 17. НД ТЗІ 3.7-003-05. Порядок проведення робіт із створення комплексної системи захисту інформації в інформаційно-телекомунікаційній системі. 18. НД ТЗІ 3.7-001-99. Методичні вказівки щодо розробки технічного завдання на створення комплексної системи захисту інформації в АС. 19. НД ТЗІ 1.6-004-2013 Захист інформації на об’єктах інформаційної діяльності. Положення про категоріювання об’єктів, де циркулює інформація з обмеженим доступом, що становить державну таємницю. 20. Information Security Handbook for Network Beginners. National Center of Incident Readiness and Strategy for Cybersecurity (NISC) ver. 2.11e. 21. Євсєєв С.П. Кібербезпека: основи кодування та криптографії/ С.П. Євсеєв, О.В. Мілов, С.Е. Остапов, О.В. Сєвєрінов. – Харків: Вид. “Новий Світ-2000”, 2023. – 657 с. 22. Технології захисту інформації./ С. Е. Остапов, С. П. Євсєєв, О.Г. Король. – Чернівці : Чернівецький національний університет, 2013. – 471 с.

Назва освітнього компонента	Вид компонента	Поле для завантаження Силабусу	Якщо освітній компонент потребує спеціального матеріально-технічного та/або інформаційного забезпечення, наведіть відомості щодо нього
Математичні основи криптології	дисципліна спеціальна (фахова) підготовка	https://cybersecurity.kpi.kharkov.ua/sylabusy-osvitnikh-komponentiv-125-bakalavr/	**Обладнання:** Мультимедійні аудиторії ПК: Intel Pentium G4560/ОЗУ 4 GB DDR3-1600/Монітор 20" Dell P2017H/HDD 500 GB, 7200 об/хв, SATA 3.0 – 15шт. Лабораторний практикум (ПЗ) **Література:** 1. Євсеєв С.П. Кібербезпека: Криптографія з Python: навчальний посібник. – Львів “Новий світ-2000”, 2021. – 120 с. 2. Євсеєв С.П. Кібербезпека: Лабораторний практикум з основ криптографічного захисту. – Львів “Новий світ-2000”, 2020ю – 241 с. 3. Євсеєв С.П., Остапов С.Е., Король О.Г. Кібербезпека: сучасні тех-нології захисту: навч. посіб. для студ. вищ. навч. закл. Львів : “Новий Світ- 2000”, 2019. – 678 с. 4. Технології захисту інформації./ С. Е. Остапов, С. П. Євсєєв, О.Г. Король. – Чернівці : Чернівецький національний університет, 2013. – 471 с. 5. Yevseiev S.P. Cyber security: basics of coding and cryptography/ S.P. Yevseiev, O.V. Milov, S.E. Ostapov, O.V. Severinov. - Kharkiv: Ed. "New World-2000", 2023. – 657 p.
Менеджмент інформаційної безпеки	дисципліна спеціальна (фахова) підготовка	https://cybersecurity.kpi.kharkov.ua/sylabusy-osvitnikh-komponentiv-125-bakalavr/	**Обладнання:** Laptop (Hoyr6YK) 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:

Назва освітнього компонента	Вид компонента	Поле для завантаження Силабусу	Якщо освітній компонент потребує спеціального матеріально-технічного та/або інформаційного забезпечення, наведіть відомості щодо нього
			Cisco Комутатор Catalyst 2960 – 6 шт. Cisco Маршрутизатор-2801 – 6 шт. Cisco ASA 5510 – 1 шт., ASA 5506 – 1 шт. Cisco комутатор Catalyst 3750 – 4 шт. Cisco Маршрутизатор 2911 з IPS – 2 шт. Packet Tracer, nmap – zenmap, спеціалізовані сканери вразливостей – Nessus, Vega. Maltego, WireShark, Aircrack, Snort. Віртуальна машина робочої станції CyberOps. Kali, Metasploitable, Security Onion. **Література:** 1. Р.В. Грищук, та Ю. Г. Даник. Основи кібернетичної безпеки: Монографія /; за заг. ред. Ю. Г. Данника. Житомир: ЖНАЕУ, 2016. 2. О. Г. Корченко, О. Є. Архипов, та Ю. О. Дрейс, “Оцінювання шкоди національній безпеці України у разі витоку державної таємниці”, монографія, К: наук.-вид.центр НА СБУ України, 2014. 3. Аудит та управління інцидентами інформаційної безпеки: навч. посіб. [Електронний ресурс] / [КорченкоО.Г., Гнатюк С.О., КазмірчукС.В. та ін.]. –К.: Центр навч.-наук. та наук.-пр. видань НАСБ України, 2014. – 190 с. 4. Менеджмент інформаційної безпеки : навчальний посібник для студентів спеціальності 125 "Кібербезпека" / О.Г. Корченко, М.Є. Шелест, С.В. Казмірчук, Ю.М. Ткач, Є.В. Іванченко. – Ніжин: ФОП Лук’яненко В.В. ТПК «Орхідея», 2019. – 408 с. : іл. 5. Synergy of building cybersecurity systems: monograph / S. Yevseiev, V. Ponomarenko, O. Laptiev, O. Milov and others. – Kharkiv: PC TECHNOLOGY CENTER, 2021. – 188 p. 6. Models of socio-cyber-physical systems security: monograph / S. Yevseiev, Yu. Khokhlachova, S. Os- tapov, O. Laptiev and others. – Kharkiv: PC TECHNOLOGY CENTER, 2023. – 168 p. 7. Modeling of security systems for critical infrastructure facilities:

Назва освітнього компонента	Вид компонента	Поле для завантаження Силабусу	Якщо освітній компонент потребує спеціального матеріально-технічного та/або інформаційного забезпечення, наведіть відомості щодо нього
			monograph / S. Yevseiev, R. Hryshchuk, K. Molodetska, M. Nazarkevych and others. – Kharkiv: PC TECHNOLOGY CENTER, 2022. – 196 p.
Організація і безпека баз даних	дисципліна спеціальна (фахова) підготовка	https://cybersecurity.kpi.kharkov.ua/sylabusy-osvitnikh-komponentiv-125-bakalavr/	**Обладнання:** **Мультимедійні аудиторії** Laptop (Hoyr6YK) 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., ASA 5506 – 1 шт. Cisco комутатор Catalyst 3750 – 4 шт. Cisco Маршрутизатор 2911 з IPS – 2 шт. Packet Tracer **Література:** 1. Берко А. Ю., Верес О. М., Пасічник В. В. Системи баз даних та знань. Книга 2. Системи управління базами даних та знань : навч. посіб. Львів : "Магнолія-2006", 2012. 584 с. 2. Завадський І. О. Основи баз даних : навч. посіб. К. : Видавець І. О. Завад-ський, 2011. 192 с. 3. Організація баз даних та знань: лабораторний практикум для студентів напряму 6.050101 “Комп’ютерні науки” ден. та заоч. форм навч. / уклад.: О.М. Мякшило та ін. К.: НУХТ, 2015. 86 с. 4. Сучасні інформаційні та комунікаційні системи і технології: навч.

Назва освітнього компонента	Вид компонента	Поле для завантаження Силабусу	Якщо освітній компонент потребує спеціального матеріально-технічного та/або інформаційного забезпечення, наведіть відомості щодо нього
			посібн. / О. Г. Трофименко, Н. І. Логінова, О. В. Задерейко, О. Б. Козін; Одеса : Фенікс, 2016. 143 с. 5. Тарасов О. В., Федько В. В., Лосєв М. Ю. Проектування баз даних : навч. посіб. Х. : Вид. ХНЕУ, 2011. 200 с. 6. Трофименко О. Г., Буката Л. М., Прокоп Ю. В. Бази даних: створення та опрацювання: навч. посібн. Одеса, 2016. 226 с.
Основи криптографічного захисту	дисципліна спеціальна (фахова) підготовка	https://cybersecurity.kpi.kharkov.ua/sylabusy-osvitnikh-komponentiv-125-bakalavr/	**Обладнання:** Спеціалізований лабораторний практикум. **Кіберполігон:** Персональний комп` ютер 2E Integer Intel i5-11400/H510/16/480F/int/FreeDos/2E-S616/400W- 25 шт. Монітор HP P24 G5 FHD Monitor – 25 шт. Гарнітура для ПК 2E CH11, On-Ear, 3.5mm/2*3.5mm – 25 шт. Комплект 2E MK410 WL Black – 25 шт. Міжмережевий екран Fortinet FG- 40F 5*GE RJ45 ports (including 4* internal Ports 1* WAN Ports – 1 шт. Ноутбук/Notebook Del Vostro 3510/Core i3-1115G4/8GB/256GB SSD/15.6`` FHD/Intel UHD/Cam& Mic/WLAN + BT/Backlit Kb/3 Cell/W11Pro/3Yr – 2 шт. Багатофункціональний пристрій А4 ч/б Multifuntional device A4 b/w Xerox B235 (WI-FI) – 1 шт. Проєктор короткофокусний Epson EB-536Wi WXGA, 3400 lm, 0.65 інтерактивний – 1 шт. Проектор/ Projector Epson EB-X49 (3LCD, XGA,3600 ANSI lm) – 1 шт. Примірник ПЗ Microsoft Windows 11 Pro укр. OEM на DVD носії – 25 шт. Екран 2E на тринозі,1:1, 112, (2.0*2.0) – 1 шт. Сервер R- LINE на базі Xeon Silver 421 OR – 1 шт. Точка доступу Ubiguiti UniFi 6 LR Access Point U6-LR – 1 шт. Маршрутизатор Mikro Tik RB4011iGS+5HacQ2HnD-IN – 1 шт.

Назва освітнього компонента	Вид компонента	Поле для завантаження Силабусу	Якщо освітній компонент потребує спеціального матеріально-технічного та/або інформаційного забезпечення, наведіть відомості щодо нього
			Комутатор D-Link DGS-1210-28X/ME – 1 шт. Сервер HPE ML350 Gen10 Hot Plug LFF CTO – 1 шт. ДБЖ HPE T1000 Gen5 INTL UPS with Management Card Slot – 1шт. Комутатор Aruba 6000 48G 4SFP Switch – 1 шт. Aruba 1G SFP LC LX 10km SMF Transceiver – 2 шт. Aruba 1G SFP RJ45T 100m Cat5e Transceiver – 2 шт. **Література:** 1. Євсеєв С.П. Кібербезпека: сучасні технології захисту. / Євсеєв С.П, Остапов С.Е., Король О.Г. // Навчальний посібник для студентів вищих навчальних закладів. Львів: "Новий Світ- 2000", 2019. – 678. – Режим доступу: http://ns2000.com.ua/wp-content/uploads/2019/11/Kiberbezpeka-suchasni-tekhnolohii-zakhystu.pdf. 2. Євсеєв С.П. Технології захисту інформації. Мультимедійне інтерактивне електронне видання комбінованого використання / уклад. Євсеєв С. П., Король О. Г., Остапов С. Е., Коц Г. П. – Х.: ХНЕУ ім. С. Кузнеця, 2016. – 1013 Мб. ISBN 978-966-676-624-6. 3. Bonaventure O. Computer Networking: Principls, Protocols and Practice. – Louvain-la-Neuve: Universite catholique de Louvain (Belgium), 2019. – 272 p. 4. О. О. Кузнецов, С. П. Євсеєв, С. В. Кавун, та О. Г. Король Сигнали і коди. Алгебраїчні методи синтезу. Монографія. Харків, Україна: Вид. ХНЕУ, 2009. 5. О. О. Кузнецов, С. П. Євсеєв, та С. В. Кавун Захист інформації та економічна безпека підприємства. Монографія. Харків, Україна: Вид. ХНЕУ, 2009. 6. С. П. Євсеєв, О. Ю. Йохов, та О. Г. Король Гешування даних в інформаційних системах. Монографія. Харків, Україна: Вид. ХНЕУ, 2013. 7. Євсєев С.П. Кібербезпека: основи кодування та криптографії/ С.П. Євсеєв, О.В. Мілов, С.Е. Остапов, О.В. Сєвєрінов. – Харків: Вид. "Новий Світ-2000", 2023. – 657 с.

Назва освітнього компонента	Вид компонента	Поле для завантаження Силабусу	Якщо освітній компонент потребує спеціального матеріально-технічного та/або інформаційного забезпечення, наведіть відомості щодо нього
			8. Технології захисту інформації./ С. Е. Остапов, С. П. Євсеєв, О.Г. Король. – Чернівці : Чернівецький національний університет, 2013. – 471 с.
Основи математичного моделювання систем безпеки	дисципліна спеціальна (фахова) підготовка	https://cybersecurity.kpi.kharkov.ua/sylabusy-osvitnikh-komponentiv-125-bakalavr/	**Обладнання:** Мультимедійні аудиторії ПК: Intel Pentium G4560/ОЗУ 4 GB DDR3-1600/Монітор 20" Dell P2017H/HDD 500 GB, 7200 об/хв, SATA 3.0 – 15шт. **Література:** 1. Бахрушин В.Є. Математичне моделювання: навчальний посібник [Текст] – Запоріжжя: ГУ "ЗІДМУ", 2004. – 140 с. 2. Жерновий Ю. В. Імітаційне моделювання систем масового обслуговування : Практикум / Ю. В. Жерновий. — Львів : Вид. центр ЛНУ ім. І. Франка, 2007. — 307 с. 3. Математичне моделювання систем і процесів: навч. посібник / П. М. Павленко, С. Ф. Філоненко, О. М. Чередніков, В. В. Трейтяк. – К. : НАУ, 2017. – 392 с. 4. Математичне моделювання телекомунікаційних систем та мереж: навчальний посібник [Текст] / Є.М. Чернихівський. – Львів: Видавництво Львівської політехніки, 2011. – 272 с. 5. Махней О. В. Математичне моделювання : навчальний посібник / О. В. Махней. — Івано-Франківськ : Супрун В. П., 2015. — 372 с. 6. Томашевський В.М. Моделювання систем / В.М. Томашевський. — К. : Видавнича група BHV, 2005. — 352 с. 7. Synergy of building cybersecurity systems: monograph / S. Yevseiev, V. Ponomarenko, O. Laptiev, O. Milov and others. – Kharkiv: PC TECHNOLOGY CENTER, 2021. – 188 p. 8. Models of socio-cyber-physical systems security: monograph / S. Yevseiev, Yu. Khokhlachova, S. Os- tapov, O. Laptiev and others. – Kharkiv: PC TECHNOLOGY CENTER, 2023. – 168 p. 9. Modeling of security systems for critical infrastructure facilities: monograph / S. Yevseiev, R. Hryshchuk, K. Molodetska, M.

Назва освітнього компонента	Вид компонента	Поле для завантаження Силабусу	Якщо освітній компонент потребує спеціального матеріально-технічного та/або інформаційного забезпечення, наведіть відомості щодо нього
			Nazarkevych and others. – Kharkiv: PC TECHNOLOGY CENTER, 2022. – 196 p.
Основи побудови та захисту мікропроцесорних систем	дисципліна спеціальна (фахова) підготовка	https://cybersecurity.kpi.kharkov.ua/sylabusy-osvitnikh-komponentiv-125-bakalavr/	**Обладнання:** Мультимедійні аудиторії ПК: Intel Pentium G4560/ОЗУ 4 GB DDR3-1600/Монітор 20" Dell P2017H/HDD 500 GB, 7200 об/хв, SATA 3.0 – 15шт. Ai-Thinker Wi-Fi модуль ESP8266 ESP-01S – 10 шт. Bluetooth модуль HC-05 – 10 шт. FC-51 інфрачервоний датчик перешкод для ARDUINO – 10 шт. HC-SR501 Регульований інфрачервоний датчик руху – 10 шт. OV7670 модуль відеокамери – 10 шт. Модуль GPS NEO-7M SMA+IPEX – 10 шт. Модуль GY-30 (BH1750FVI) цифровий датчик освітленості – 10 шт. Модуль HC-SR04 ультразвуковий приймач – 10 шт. Модуль SR602 мініатюрний інфрачервоний датчик руху – 10 шт. Модуль датчика хола A3144 – 10 шт. ARDUINO UNO R3 ATmega328P Rev 3.0 microUSB – 10 шт. Multifunctional Expansion Board Shield Basic Learning Kit for Arduino UNO R3 Модуль XBee 3 Module с UFL роз'ємом антени від Sparkfun – 10 шт. RASPBERRY PI 4 MODEL B 4GB/ – 10 шт. WiFi Плата NodeMCU V2 ESP8266 (CP2102) – 10 шт. GPRS/GSM+GPS Шилд на SIM808 від Elecrow – 10 шт. RFID модуль RC522 з карткою доступу для Arduino – 10 шт. RFID модуль RDM6300 125кГц – 10 шт. **Література:** 1. Жуйков В.Я., Терещенко Т.О., Петергеря Ю.С. і ін «Мікропроцесори і мікроконтролери» - Електронний підручник

Назва освітнього компонента	Вид компонента	Поле для завантаження Силабусу	Якщо освітній компонент потребує спеціального матеріально-технічного та/або інформаційного забезпечення, наведіть відомості щодо нього
			[Електронний ресурс]. – Режим доступу : http://www.kaf-pe.ntu-kpi.kiev.ua/. – Житомир : Вид-во ЖДУ ім. І. Франка, 2015. – 226 с. 2. Мікропроцесорна техніка. Друге видання. Доповнене./ Ю.І. Якименко, Т.О. Терещенко, Є.І. Сокол, В.Я. Жуйков, Ю.С. Петергеря. За ред. Т.О. Терещенко. – Київ, 2004. – 440 с 3. Схемотехніка електронних систем. Том 3. Мікропроцесори та мікроконтролери / Бойко В.І., Гуржій А.М., Жуйков В.Я., Зорі А.А., Петергеря Ю.С., Співак В.М., Терещенко Т.О, Якименко Ю.І. - К.: Вища школа, 2004. – 399 с.:іл. 4. Зубарєв А. А. Асемблер для мікроконтролерів A VR: Навчальний посібник. [Електронний ресурс]. – Режим доступу : bek.sibadi.org/fu11text/ED1S19. 5. Євсеєв С.П., Смірнов О.А., Король О.Г., Коваленко О.В. Архітектура мікропроцесорів та компонентів ЕОМ. Кіровоград: Вид. Лисенко В.Ф., 2015. – 550 с. 6. Цифрова схемотехніка та архітектура мікропроцесорів: навчальний посібник / Євсеєв С. П., Дженюк Н.В., Охріменко М.Ю. та ін. – Харків, – Львів: Видавництво ПП «Новий Світ – 2000», 2023. –513 с.
Основи побудови та захисту сучасних операційних систем	дисципліна спеціальна (фахова) підготовка	https://cybersecurity.kpi.kharkov.ua/sylabusy-osvitnikh-komponentiv-125-bakalavr/	**Обладнання:** Мультимедійні аудиторії ПК: Intel Pentium G4560/ОЗУ 4 GB DDR3-1600/Монітор 20" Dell P2017H/HDD 500 GB, 7200 об/мин, SATA 3.0 – 15шт. OS Windows10, OS Linux, Nmap, Lynis, WPScan, Aircrack-ng, Hydra, Wireshark, Metasploit Framework **Література:** 1. Волосюк Ю .В. Комп'ютерні мережі: курс лекцій / Ю. В. Волосюк. – Миколаїв : МНАУ, 2019. – 203 с. 2. Derrick Rountree, Security for Microsoft Windows System Administrators Introduction to Key Information Security Concepts,

Назва освітнього компонента	Вид компонента	Поле для завантаження Силабусу	Якщо освітній компонент потребує спеціального матеріально-технічного та/або інформаційного забезпечення, наведіть відомості щодо нього
			Syngress, 211 p.,2011. 3. Stallings, William. Operating systems: internals and design principles / William Stallings. – 7 th ed. Prentice Hall, New Jersey, 2012, p.769. ISBN-13:978-0-13-230998-1 4. Kusswurm Daniel. Modern X86 Assembly Language Programming/ Daniel Kusswurm. - Apress, 2019. — 604 p. 5. Russell S. R., Taylor B. W. Operations management : Creating value along the supply chain. 7 ed. N.-Y. : John Wiley & Sons, Inc., 2010. 832 p. 6. Haseman Chris. Android Essentials / Chris Haseman. – Apress, 2008. – 116 p. 7. J.Spealman, K.Hudson, M.Graft, Windows Server 2003: Active Directory Infrastructure. Microsoft Press, pp. 1–8–1–9, 2003 8. Технології захисту інформації./ С. Е. Остапов, С. П. Євсєєв, О.Г. Король. – Чернівці : Чернівецький національний університет, 2013. – 471 с.
Основи програмування	дисципліна спеціальна (фахова) підготовка	https://cybersecurity.kpi.kharkov.ua/sylabusy-osvitnikh-komponentiv-125-bakalavr/	**Обладнання:** **Мультимедійні аудиторії** Laptop (Hoyr6YK) 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., ASA 5506 – 1 шт.

Назва освітнього компонента	Вид компонента	Поле для завантаження Силабусу	Якщо освітній компонент потребує спеціального матеріально-технічного та/або інформаційного забезпечення, наведіть відомості щодо нього
			Cisco комутатор Catalyst 3750 – 4 шт. Cisco Маршрутизатор 2911 з IPS – 2 шт. Packet Tracer **Література:** 1. Євсеєв С.П. КІБЕРБЕЗПЕКА: КРИПТОГРАФІЯ З PYTHON: навч. посібн. / С.П. Євсеєв, О.В. Шматко, О.Г. Король – Харків: Видавництво «Новий Світ – 2000», 2021. –120 с. 1 Python 3.10.2 documentation [Електронний ресурс]. – Режим доступу : https://docs.python.org/3/. 2. Java Platform Standard Edition 8 Documentation [Електронний ресурс]. – Режим доступу : https://docs.oracle.com/javase/8/docs/. 3. Microsoft C++, C, and Assembler documentation [Електронний ресурс]. – Режим доступу : https://docs.microsoft.com/en-us/cpp/?view=msvc-170.
Основи соціальної інженерії	дисципліна спеціальна (фахова) підготовка	https://cybersecurity.kpi.kharkov.ua/sylabusy-osvitnikh-komponentiv-125-bakalavr/	**Обладнання:** **Кіберполігон:** Персональний комп` ютер 2E Integer Intel i5-11400/H510/16/480F/int/FreeDos/2E-S616/400W- 25 шт. Монітор HP P24 G5 FHD Monitor – 25 шт. Гарнітура для ПК 2E CH11, On-Ear, 3.5mm/2*3.5mm – 25 шт. Комплект 2E MK410 WL Black – 25 шт. Міжмережевий екран Fortinet FG- 40F 5*GE RJ45 ports (including 4* internal Ports 1* WAN Ports – 1 шт. Ноутбук/Notebook Del Vostro 3510/Core i3-1115G4/8GB/256GB SSD/15.6`` FHD/Intel UHD/Cam& Mic/WLAN + BT/Backlit Kb/3 Cell/W11Pro/3Yr – 2 шт. Багатофункціональний пристрій А4 ч/б Multifuntional device A4 b/w Xerox B235 (WI-FI) – 1 шт. Проєктор короткофокусний Epson EB-536Wi WXGA, 3400 lm, 0.65 інтерактивний – 1 шт. Проектор/ Projector Epson EB-X49 (3LCD, XGA,3600 ANSI lm) –

Назва освітнього компонента	Вид компонента	Поле для завантаження Силабусу	Якщо освітній компонент потребує спеціального матеріально-технічного та/або інформаційного забезпечення, наведіть відомості щодо нього
			1 шт. Примірник П3 Microsoft Windows 11 Pro укр. OEM на DVD носії – 25 шт. Екран 2E на тринозі,1:1, 112, (2.0*2.0) – 1 шт. Сервер R- LINE на базі Xeon Silver 421 OR – 1 шт. Точка доступу Ubiguiti UniFi 6 LR Access Point U6-LR – 1 шт. Маршрутизатор Mikro Tik RB4011iGS+5HacQ2HnD-IN – 1 шт. Комутатор D-Link DGS-1210-28X/ME – 1 шт. Сервер HPE ML350 Gen10 Hot Plug LFF CTO – 1 шт. ДБЖ HPE T1000 Gen5 INTL UPS with Management Card Slot – 1шт. Комутатор Aruba 6000 48G 4SFP Switch – 1 шт. Aruba 1G SFP LC LX 10km SMF Transceiver – 2 шт. Aruba 1G SFP RJ45T 100m Cat5e Transceiver – 2 шт. **Література:** 1. Ozkaya, Erdal. Learn Social Engineering: Learn the art of human hacking with an internationally renowned expert. Packt Publishing Ltd, 2018.- 557 p. 2. Alexander, Michael; Wanner, R. Methods for understanding and reducing social engineering attacks. SANS Inst., 2016, 1: 1-32. 3. Грищук Р. В., Даник Ю. Г. Основи кібербезпеки: монографія / відп. ред. проф. Ю. Г. Даник, Житомир : ЖНАЕУ, 636 с., 2016. 4. Hadnagy, Christopher. Social engineering: The science of human hacking. John Wiley & Sons, 2018 - 330 p. 5. Michael Bazzell. Open Source Intelligence Techniques: Resources for Searching and Analyzing Online Information Paperback – 2021- 666 p. 6. Ethical Hacking: 3 in 1- Beginner's Guide+ Tips and Tricks+ Advanced and Effective measures of Ethical Hacking Paperback – July 23, 2020 – 456 p. 7. Бурячок В. Л. Інформаційна та кібербезпека: соціотехнічний аспект: підручник / [В. Л. Бурячок, В. Б. Толубко, В. О.

Назва освітнього компонента	Вид компонента	Поле для завантаження Силабусу	Якщо освітній компонент потребує спеціального матеріально-технічного та/або інформаційного забезпечення, наведіть відомості щодо нього
			Хорошко, С. В. Толюпа]; за заг. ред. д-ра техн. наук, професора В. Б. Толубка.– К.: ДУТ, 2015. – 288 с. 8. 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.
Основи стеганографічного захисту інформації	дисципліна спеціальна (фахова) підготовка	https://cybersecurity.kpi.kharkov.ua/sylabusy-osvitnikh-komponentiv-125-bakalavr/	**Обладнання:** Мультимедійні аудиторії ПК: Intel Pentium G4560/ОЗУ 4 GB DDR3-1600/Монітор 20" Dell P2017H/HDD 500 GB, 7200 об/хв, SATA 3.0 – 15шт. Mathcad **Література:** 1. Кузнецов О.О. Стеганографія: навчальний посібник / О.О.Кузнецов, С.П. Євсеєв, О.Г. Король. – Х. : Вид. ХНЕУ, 2015. – 232 с. 2. Хорошко В.О. Комп'ютерна стеганографія: навчальний посібник / В.О. Хорошко, Ю.Є. Яремчук, В.В. Карпінець – Вінниця : ВНТУ, 2017. – 155 с. 3. Козюра В.Д. Захист інформації в комп'ютерних системах :підручник / В.Д.Козюра, В.О.Хорошко, М.Є.Шелест – Ніжин : ФОП Лукяненко В.В., ТПК «Орхідея», 2020. – 236 с. 4. Конахович Г.Ф. Компютерна стеганографічна обробка й аналіз мультимедійних дан6 : підручник /Г.Ф. Конафович, Д.О.Прогонов, О.Ю. Пузиренко. – К. – «Alex Print Centre», 2018/ – 558 с. 5. Технології захисту інформації./ С. Е. Остапов, С. П. Євсєєв, О.Г. Король. – Чернівці : Чернівецький національний університет, 2013. – 471 с.

Назва освітнього компонента	Вид компонента	Поле для завантаження Силабусу	Якщо освітній компонент потребує спеціального матеріально-технічного та/або інформаційного забезпечення, наведіть відомості щодо нього
Розробка та аналіз алгоритмів	дисципліна спеціальна (фахова) підготовка	https://cybersecurity.kpi.kharkov.ua/sylabusy-osvitnikh-komponentiv-125-bakalavr/	**Обладнання:** Мультимедійні аудиторії ПК: Intel Pentium G4560/ОЗУ 4 GB DDR3-1600/Монітор 20" Dell P2017H/HDD 500 GB, 7200 об/мин, SATA 3.0 – 15шт. Visual Studio Code, Tutorialspoint.com **Література:** 1. Marcello La Rocca. Advanced Algorithms and Data Structures. / Marcello La Rocca. – New York: Manning Publications Co., 2021. – 768 p. 2. Креневич А.П. Алгоритми і структури даних. Підручник. / А.П. Креневич. – К.: ВПЦ "Київський Університет", 2021. – 200 с 3. Helmut Knebl. Algorithms and Data Structures: Foundations and Probabilistic Methods for Design and Analysis / Helmut Knebl. – Cham: Springer Nature Switzerland AG, 2020. – 349 p. – Режим доступу: http://repository.kpi.kharkov.ua/handle/KhPI-Press/50239 4. Алгоритми і структури даних: практикум: навч. посіб./ Н.К. Стратієнко, М.Д. Годлевський, І.О. Бородіна.- Харьков: НТУ"ХПИ", 2017. - 224 с. 5. Методичні вказівки до виконання лабораторних робіт з курсу "Алгоритми і структури даних" [Електронний ресурс] / уклад. Н. К. Стратієнко, І. О. Бородіна ; Харківський політехнічний ін-т, нац. техн. ун-т. – Електрон. текстові дані. – Харків, 2017. – 36 с. – Режим доступу: http://repository.kpi.kharkov.ua/handle/KhPI-Press/26426. 6. Євсеєв С.П. КІБЕРБЕЗПЕКА: КРИПТОГРАФІЯ З PYTHON: навч. посібн. / С.П. Євсеєв, О.В. Шматко, О.Г. Король – Харків: Видавництво «Новий Світ – 2000», 2021. –120 с.

Назва освітнього компонента	Вид компонента	Поле для завантаження Силабусу	Якщо освітній компонент потребує спеціального матеріально-технічного та/або інформаційного забезпечення, наведіть відомості щодо нього
Структури даних	дисципліна спеціальна (фахова) підготовка	https://cybersecurity.kpi.kharkov.ua/sylabusy-osvitnikh-komponentiv-125-bakalavr/	**Обладнання:** Мультимедійні аудиторії ПК: Intel Pentium G4560/ОЗУ 4 GB DDR3-1600/Монітор 20" Dell P2017H/HDD 500 GB, 7200 об/хв, SATA 3.0 – 15шт. Лабораторний практикум (ПЗ) **Література:** 1. Marcello La Rocca. Advanced Algorithms and Data Structures. / Marcello La Rocca. - New York: Manning Publications Co., 2021. - 768 p. 2. Креневич А.П. Алгоритми та структури даних. Підручник. / А.П. Креневич. - К.: ВПЦ "Київський Університет", 2021. - 200 с. 3. Helmut Knebl. Algorithms and Data Structures: Foundations and Probabilistic Methods for Design and Analysis / Helmut Knebl. - Cham: Springer Nature Switzerland AG, 2020. - 349 p. – Режим доступу: http://repository.kpi.kharkov.ua/handle/KhPI-Press/50239. 4. Алгоритми та структури даних: практикум: навч. посіб./Н.К. Стратієнко, М.Д. Годлєвський, І.О. Бородіна.- Харків: НТУ "ХПІ", 2017. - 224 с. 5. Методичні вказівки до виконання лабораторних робіт з курсу "Алгоритми та структури даних" [Електронний ресурс] / уклад. Н. К. Стратієнко, І. О. Бородіна; Харківський політехнічний ін-т, нац. техн. ун-т. - Електрон. текстові дані. – Харків, 2017. – 36 с. – Режим доступу: http://repository.kpi.kharkov.ua/handle/KhPI-Press/26426.
Сучасні інформаційні системи (з елементами кібербезпеки)	дисципліна спеціальна (фахова) підготовка	https://cybersecurity.kpi.kharkov.ua/sylabusy-osvitnikh-komponentiv-125-bakalavr/	**Обладнання:** **Кіберполігон:** Персональний комп` ютер 2E Integer Intel i5-11400/H510/16/480F/int/FreeDos/2E-S616/400W- 25 шт. Монітор HP P24 G5 FHD Monitor – 25 шт. Гарнітура для ПК 2E CH11, On-Ear, 3.5mm/2*3.5mm – 25 шт. Комплект 2E MK410 WL Black – 25 шт.

Назва освітнього компонента	Вид компонента	Поле для завантаження Силабусу	Якщо освітній компонент потребує спеціального матеріально-технічного та/або інформаційного забезпечення, наведіть відомості щодо нього
			Міжмережевий екран Fortinet FG- 40F 5*GE RJ45 ports (including 4* internal Ports 1* WAN Ports – 1 шт. Ноутбук/Notebook Del Vostro 3510/Core i3-1115G4/8GB/256GB SSD/15.6`` FHD/Intel UHD/Cam& Mic/WLAN + BT/Backlit Kb/3 Cell/W11Pro/3Yr – 2 шт. Багатофункціональний пристрій А4 ч/б Multifuntional device A4 b/w Xerox B235 (WI-FI) – 1 шт. Проєктор короткофокусний Epson EB-536Wi WXGA, 3400 lm, 0.65 інтерактивний – 1 шт. Проектор/ Projector Epson EB-X49 (3LCD, XGA,3600 ANSI lm) – 1 шт. Примірник П3 Microsoft Windows 11 Pro укр. OEM на DVD носії – 25 шт. Екран 2E на тринозі,1:1, 112, (2.0*2.0) – 1 шт. Сервер R- LINE на базі Xeon Silver 421 OR – 1 шт. Точка доступу Ubiguiti UniFi 6 LR Access Point U6-LR – 1 шт. Маршрутизатор Mikro Tik RB4011iGS+5HacQ2HnD-IN – 1 шт. Комутатор D-Link DGS-1210-28X/ME – 1 шт. Сервер HPE ML350 Gen10 Hot Plug LFF CTO – 1 шт. ДБЖ HPE T1000 Gen5 INTL UPS with Management Card Slot – 1шт. Комутатор Aruba 6000 48G 4SFP Switch – 1 шт. Aruba 1G SFP LC LX 10km SMF Transceiver – 2 шт. Aruba 1G SFP RJ45T 100m Cat5e Transceiver – 2 шт. **Література:** 1. Технології захисту інформації./ С. Е. Остапов, С. П. Євсєєв, О.Г. Король. – Чернівці : Чернівецький національний університет, 2013. – 471 с. 2. WEB-технології [Електронний ресурс]: Навчально-довідковий посібник / С.П. Євсеєв, А.М. Ткачов, В.О. Алексієв, Ю.М. Рябуха – Харків : ХНЕУ ім. С. Кузнеця, – Львів: Видавництво «Новий Світ –2000», 2021. – 390 с.

Назва освітнього компонента	Вид компонента	Поле для завантаження Силабусу	Якщо освітній компонент потребує спеціального матеріально-технічного та/або інформаційного забезпечення, наведіть відомості щодо нього
			3. Академія web розробки MDN [Електронний ресурс]. – Режим доступу: https://developer.mozilla.org/. 4. HTML Tutorial [Електронний ресурс]. – Режим доступу: https://www.tutorialspoint.com/html/index.htm. 5. CSS Tutorial [Електронний ресурс]. – Режим доступу: https://www.tutorialspoint.com/css/index.htm. 6. Javascript Tutorial [Електронний ресурс]. – Режим доступу: https://www.tutorialspoint.com/javascript/index.htm. SQL Tutorial [Електронний ресурс]. – Режим доступу: https://www.tutorialspoint.com/sql/index.htm.
Технології програмування	дисципліна спеціальна (фахова) підготовка	https://cybersecurity.kpi.kharkov.ua/sylabusy-osvitnikh-komponentiv-125-bakalavr/	**Обладнання:** Мультимедійні аудиторії ПК: Intel Pentium G4560/ОЗУ 4 GB DDR3-1600/Монітор 20" Dell P2017H/HDD 500 GB, 7200 об/мин, SATA 3.0 – 15шт. Visual Studio Code **Література:** 1. Python 3.10.2 documentation [Електронний ресурс]. – Режим доступу : https://docs.python.org/3/ 2. Java Platform Standard Edition 8 Documentation [Електронний ресурс]. – Режим доступу : https://docs.oracle.com/javase/8/docs/ 3. Microsoft C++, C, and Assembler documentation [Електронний ресурс]. – Режим доступу : https://docs.microsoft.com/en-us/cpp/?view=msvc-170 4. WEB-технології [Електронний ресурс]: Навчально-довідковий посібник / С.П. Євсеєв, А.М. Ткачов, В.О. Алексієв, Ю.М. Рябуха – Харків : ХНЕУ ім. С. Кузнеця, – Львів: Видавництво «Новий Світ –2000», 2021. – 390 с. 5. Євсеєв С.П. КІБЕРБЕЗПЕКА: КРИПТОГРАФІЯ З PYTHON: навч. посібн. / С.П. Євсеєв, О.В. Шматко, О.Г. Король – Харків:

Назва освітнього компонента	Вид компонента	Поле для завантаження Силабусу	Якщо освітній компонент потребує спеціального матеріально-технічного та/або інформаційного забезпечення, наведіть відомості щодо нього
			Видавництво «Новий Світ – 2000», 2021. –120 с.
Українська мова (за професійним спрямуванням)	дисципліна загальна підготовка	https://cybersecurity.kpi.kharkov.ua/sylabusy-osvitnikh-komponentiv-125-bakalavr/	**Обладнання:** не потребує **Література** 1. Методичні вказівки до практичних занять та самостійних робіт з дисципліни «Українська мова» для студентів усіх спеціальностей «Долаймо суржик!» / уклад. Дяченко О.В., Гомон А.М.− Харків: НТУ «ХПІ», видавництво «Форт», 2019. – 56 с. 2. Заверющенко М.П. Офіційно-діловий стиль: правила укладання документів різних видів»: навч. посібник щодо самостійної роботи / М. П. Заверющенко, О. М. Кримець, С. М. Чернявська, О. В. Шокуров.− Харків: НТУ «ХПІ», 2019.– 140 с. 3. Методичні вказівки для студентів і викладачів з дисциплін «Українська мова» «Метод проектного навчання у контенті комунікативно-інтенційної моделі як нової еволюційної освіти» / уклад. Полянська І.В., Чернявська С.М., Шевченко В.Ф.− Харків: НТУ «ХПІ», 2019. – 27 с. 4. Гомон А.М. Оброблення наукової інформації: навчально-методичний посібник з дисципліни «Українська мова» для студентів І курсу всіх спеціальностей / А.М. Гомон А.М., Кримець О.М.− Харків: НТУ «ХПІ», 2019.− 106 с. 5. Методичні вказівки до практичних занять та самостійних робіт з дисципліни «Українська мова» для студентів усіх спеціальностей «Основні труднощі з орфографії та пунктуації сучасної української мови» / уклад. Гомон А.М. , Дяченко О.В.− Харків: НТУ «ХПІ», 2019. – 36 с. 6. Методичні вказівки до практичних занять та самостійних робіт з дисципліни «Українська мова» для студентів і курсантів 1-го курсу технічних спеціальностей «Культура усного професійно-ділового спілкування» / уклад. Снігурова І.І., Писарська Н.В., Бєлова К.В., Дяченко О.В.− Харків: НТУ «ХПІ», 2020.– 45 с. 7. Методичні вказівки до практичних занять та самостійних робіт з

Назва освітнього компонента	Вид компонента	Поле для завантаження Силабусу	Якщо освітній компонент потребує спеціального матеріально-технічного та/або інформаційного забезпечення, наведіть відомості щодо нього
			навчальної дисципліни «Українська мова для курсантів та студентів 1-го курсу «Наукова комунікація як складник фахової діяльності» / уклад. Бєлова К.В., Писарська Н.В., Снігурова І.І., Дяченко О.В.– Харків: НТУ «ХПІ», 2020. – 30 с. 8. Методичні вказівки до самостійної роботи з навчальної дисципліни «Українська мова» для студентів 1-го курсу нефілологічних спеціальностей та курсантів ВІТВ «Правила укладання ділових паперів» / уклад. Снігурова І.І., Писарська Н.В., Бєлова К.В., Дяченко О.В. – Харків: НТУ «ХПІ», 2020.– 33 с. 9. Бєлова К.В. Українська мова для військовослужбовців: навчальний посібник / К. В. Бєлова, І. І. Снігурова, О. В. Дяченко, Н. В. Писарська .– Харків : НТУ «ХПІ», 2021. – 161 с. 10. Українська мова професійного спрямування : метод. вказівки до самостійної роботи з дисципліни "Українська мова" (професійного спрямування) : для студентів 1-го курсу Навч.-наук. ін-ту механіч. інженерії та транспорту / уклад.: К. В. Бєлова, В. В. Субботіна, Н. В. Писарська ; Нац. техн. ун-т "Харків. політехн. ін-т". – Харків : Форт, 2022. – 45 с. 11. Методичні рекомендації до самостійної роботи з курсу "Українська мова" [Електронний ресурс] : для студентів комп'ютерних спеціальностей / уклад.: С. М. Чернявська [та ін.] ; Нац. техн. ун-т "Харків. політехн. ін-т". – Електрон. текст. дані. – Харків, 2022. – 40 с. 12. Методичні рекомендації до самостійної роботи з курсу "Українська мова" [Електронний ресурс] : для студентів електроенергетичних спеціальностей / уклад.: С. М. Чернявська [та ін.] ; Нац. техн. ун-т "Харків. політехн. ін-т". – Електрон. текст. дані. – Харків, 2022. – 44 с. 13. Методичні вказівки з курсу «Українська мова (професійного спрямування)» для студентів спеціальності 162 «Біотехнології та біоінженерія» / Укл.: С. М. Чернявська, О. М. Кримець, О. Є. Немерцова, О. В. Дяченко, Близнюк О. М., Масалітіна Н. Ю. –

Назва освітнього компонента	Вид компонента	Поле для завантаження Силабусу	Якщо освітній компонент потребує спеціального матеріально-технічного та/або інформаційного забезпечення, наведіть відомості щодо нього
			Харків: НТУ «ХПІ», 2022. – 38 с. 14. Методичні вказівки до самостійної роботи з дисципліни «Українська мова (професійного спрямування)» для студентів комп'ютерних спеціальностей / Укл. : В. А. Сухоруков, О. В. Шокуров, О. В. Дяченко – Х. : НТУ «ХПІ», 2023. – 50 с. 15. Методичні рекомендації до самостійної роботи з дисципліни «Українська мова» для студентів хімічних спеціальностей. Ч. І / Уклад.: Л. Я. Терещенко, С. М. Чернявська, С. А. Лещенко. – Харків: НТУ «ХПІ», 2023. – 23 с. 16. Методичні рекомендації до самостійної роботи з курсу «Українська мова» для студентів економічних спеціальностей / уклад. О.М. Кримець, М.Ю. Лухіна, А.М. Гомон. – Харків : НТУ «ХПІ», 2023. – 40 с. Українська мова (за професійним спрямуванням) 17. Методичні вказівки до самостійної роботи з навчальної дисципліни «Українська мова» (професійного спрямування) для студентів 1-го курсу спеціальності 132 «Матеріалознавство» / Уклад.: В. В. Субботіна, Н. В. Писарська. – Харків: НТУ «ХПІ», 2023. – 44 с.
Фізика	дисципліна загальна підготовка	https://cybersecurity.kpi.kharkov.ua/sylabusy-osvitnikh-komponentiv-125-bakalavr/	**Обладнання:** **1) Практикум з механіки, молекулярної фізики, електрики, магнетизму, коливань та хвиль к.1,2,3,9 У/2, 196 м^2** Установка для визначення періоду коливань та прискорення вільного руху Математичний маятник - 10 Фізичний маятник - 10 Установка для перевірки основного рівняння динаміки обертального руху Обертальний маятник - 6 Установка для вивчення пружного та непружного удару куль - 6 Установка для вивчення законів вільного падіння - 3

Назва освітнього компонента	Вид компонента	Поле для завантаження Силабусу	Якщо освітній компонент потребує спеціального матеріально-технічного та/або інформаційного забезпечення, наведіть відомості щодо нього
			Установка для визначення коефіцієнта в′язкості рідини - 6 Установка для визначення молярних теплоемностей - 2 Установка для визначення довжини вільного вільного пробігу і ефективного діаметра молекул повітря -2 Установка для вивчення розгалужених електричних ланцюгів - 2 Установка для вивчення економічного використання джерела струму - 2 Установка для вивчення градуіровки гальванометра - 2 Установка для вивчення законів земного магнетизму - 4 Установка для вивчення електромагнетизму - 1 Установка для вивчення петлі гістерезису феромагнетиків - 1 Установка для вивчення акустичних параметрів камертона - 2 Установка для визначення швидкості звука в твердих тілах методом резонансу - 2 Установка для визначення швидкості звуку в повітрі методом складання взаємно перпендикулярних коливань – 1 **2) Практикум з оптики та атомної фізики к.11 У/2 58 м^2 к.205,207 Ф/К 132 м^2** Установка для вивчення вимушених електромагнітних коливань - 1 Установка для вивчення дифракції світла - 1 Установка вивчення інтерференційної схеми кілець Ньютона - 1 Установка для вивчення законів теплового випромінювання - 1 Установка для дослідження дискретності енергетичних рівнів атома за допомогою ефекту Франка-Герца - 2 Установка для визначення довжини де Бройля за допомогою електронограм Установка для дослідження спектрів газів і визначення сталої Рідберга - 1 Установка для вивчення флуктуацій потоку природного фону випромінювання - 1 Дослідження резистивно-температурної характеристики

Назва освітнього компонента	Вид компонента	Поле для завантаження Силабусу	Якщо освітній компонент потребує спеціального матеріально-технічного та/або інформаційного забезпечення, наведіть відомості щодо нього
			напівпровідників -1 **3) Практикум фізичного моделювання к.113 Ф/К 45 м^2** Компьютери – 10 (2006-2021 рр), локальна мережа Прикладна програма «Компьютерний практикум з фізики» © Дозволяє моделювати різні фізичні процеси і явища, оброблювати цифрові зображення для вивчення різних фізічних процесів і явищ; перевірка вірності отриманих в експерименті даних і виконання розрахунку **4) Практикум лекційних демонстрацій к.12 У/2 98 м^2** Установки та прилади для проведення лекційних демонстрацій у кількості 160 варіантів Устаткування дозволяє під час проведення лекцій наочно демонструвати закони фізики **5) Лекційна аудиторія 13/105 У/2 291 м^2** Амфітеатр з кількістю посадових місць – 260 Мультимедійна система Стіл для демонстрацій **Література:** 1. Кучерук І.М. Загальний курс фізики : у 3-х т. /Т.1. Механіка, молекулярна фізика і термодинаміка. – І.М. Кучерук, І.Т. Горбачук, П.П. Луцик. – К.: Техніка, 2006, 536 с. Кількіть 150 шт. 2. Кучерук І.М. Загальний курс фізики : у 3-х т. / Т.2. Електрика і магнетизм. – І.М. Кучерук, І.Т. Горбачук, П.П. Луцик. – К.: Техніка, 2006, 452 с. Кількіть 150 шт. 3. Кучерук І.М. Загальний курс фізики : у 3-х т. / Т.3. Оптика. Квантова фізика. – І.М. Кучерук, І.Т. Горбачук, П.П. Луцик. – К.: Техніка, 2006, 520 с. Кількіть 150 шт. 4. Загальна фізика. Лабораторний практикум : навч. посіб. : у 3 ч. Ч. 1 : Класична механіка. Термодинаміка і статистична фізика. Електрика та магнетизм / А.О. Мамалуй, Сук О.П., М.В. Лебедєва, Т.І. Храмова, та ін. ; за заг. ред. А. О. Мамалуя. – Х. : Підручник

Назва освітнього компонента	Вид компонента	Поле для завантаження Силабусу	Якщо освітній компонент потребує спеціального матеріально-технічного та/або інформаційного забезпечення, наведіть відомості щодо нього
			НТУ «ХПІ», 2012. 352 с. Кількіть 300 шт. 5. Загальна фізика. Лабораторний практикум : навч. посіб. : у 3 ч. Ч. 2 : Коливання та хвилі. Оптика. / А.О. Мамалуй, В.В. Пилипенко, К.Т. Лемешевська, та ін. ; за заг. ред. А. О. Мамалуя. – Харків : Підручник НТУ «ХПІ», 2012. с. – 216 с. Кількіть 300 шт. 6. Загальна фізика. Лабораторний практикум : навч. посіб. : у 3 ч. Ч. 3 : Квантова механіка. Фізика атомів і молекул. Фізика твердого тіла. Фізика атомного ядра та елементарних частинок / А. О. Мамалуй, С. Д. Гапоченко, Т. М. Шелест, та ін. ; за заг. ред. А. О. Мамалуя. – Х. : Підручник НТУ «ХПІ», 2013. 172 с. Кількіть 300 шт. 7. Сук О.Ф. Комп'ютерний лабораторний практикум із фізики. / А.Ф. Сук, І.В. Синельник, А.В.Сінельник. - Харків, Точка, 2011. - 247 с. 8. Загальна фізика. Практичні завдання : навч.-метод. посіб. / А. О. Мамалуй, М. В. Лебедєва, В. В. Пилипенко та ін. ; за заг. ред. А. О. Мамалуя – Х. : Вид-во «Підручник НТУ «ХПІ», 2014. – 296 с. 9. Загальний курс фізики : збірник задач / ред. І. П. Гаркуша. - 2-е вид., стер. - Київ : Техніка, 2004. - 560 с. 10. Методичні вказівки до розв’язання задач за темою "Механіка. Частина І. Кінематика" з курсу "Загальна фізика" для студентів усіх спеціальностей та усіх форм навчання / Уклад.: Ветчинкіна З.К., Дзюбенко Н.І., Любченко О.А., Тавріна Т.В. – Харків: НТУ "ХПІ", 2010. – 40 с. http://repository.kpi.kharkov.ua/handle/KhPI-Press/3979 11. Методичні вказівки до розв’язання задач за темою "Механіка. Частина ІІ. Динаміка" з курсу "Загальна фізика" для студентів усіх спеціальностей та усіх форм навчання / Уклад.: Ветчинкіна З.К., Дзюбенко Н.І., Любченко О.А., Тавріна Т.В. – Харків: НТУ "ХПІ", 2010. – 48 с. http://repository.kpi.kharkov.ua/handle/KhPI-Press/3982 12. Методичні вказівки до розв’язання задач за темою "Механіка. Частина ІІІ. Механічні коливання та хвилі" з курсу "Загальна

Назва освітнього компонента	Вид компонента	Поле для завантаження Силабусу	Якщо освітній компонент потребує спеціального матеріально-технічного та/або інформаційного забезпечення, наведіть відомості щодо нього
			фізика" для студентів усіх спеціальностей та усіх форм навчання / Уклад.: Ветчинкіна З.К., Дзюбенко Н.І., Любченко О.А., Тавріна Т.В. – Харків: НТУ "ХПІ", 2010. – 44 с. http://repository.kpi.kharkov.ua/handle/KhPI-Press/3984 13. Методичні вказівки до розв'язання задач за темою "Молекулярна фізика і термодинаміка. Частина І. Молекулярна фізика. Явища переносу" з курсу "Загальна фізика" : для студ. усіх спец. та усіх форм навч. / уклад. М. В. Бурлакова [та ін.]. – Харків : НТУ "ХПІ", 2010. – 36 с. http://repository.kpi.kharkov.ua/handle/KhPI-Press/3987 14. Методичні вказівки до розв'язання задач за темою "Молекулярна фізика і термодинаміка. Частина ІІ. Термодинаміка" з курсу "Загальна фізика" : для студ. усіх спец. та усіх форм навч. / уклад. М. В. Бурлакова [та ін.]. – Харків : НТУ "ХПІ", 2010. – 44 с. http://repository.kpi.kharkov.ua/handle/KhPI-Press/3991 15. Методичні вказівки до розв'язання задач за темою "Електромагнетизм. Частина І. Електрика" з курсу "Загальна фізика" для студентів усіх спеціальностей та усіх форм навчання / Уклад.: Ветчинкіна З.К., Дзюбенко Н.І., Любченко О.А., Тавріна Т.В. – Харків: НТУ "ХПІ", 2010. – 68 с. 16. Методичні вказівки до розв'язання задач за темою "Електромагнетизм. Частина ІІ. Магнетизм" з курсу "Загальна фізика" для студентів усіх спеціальностей та усіх форм навчання / Уклад.: Бурлакова М.В., Ветчинкіна З.К., Дзюбенко Н.І., Лєдєньов В.В., Любченко О.А., Тавріна Т.В. – Харків: НТУ "ХПІ", 2010. – 76 с.
Фізичне виховання	дисципліна загальна підготовка	https://cybersecurity.kpi.kharkov.ua/sylabusy-osvitnikh-komponentiv-125-bakalavr/	**Обладнання:** **Спортивні зали:** Навчально-спортивний комплекс № 1, вул. Алчевських, 50 А: - л/а манеж - ігровий зал

Назва освітнього компонента	Вид компонента	Поле для завантаження Силабусу	Якщо освітній компонент потребує спеціального матеріально-технічного та/або інформаційного забезпечення, наведіть відомості щодо нього
			- тренажерний зал - зал художньої гімнастики № 1 - зал художньої гімнастики № 2 - зал настільного тенісу - зал сухого плавання Навчально-спортивний комплекс № 2, вул. Пушкінська,85: - ігровий зал - тренажерний зал - зал штанги - зал гімнастики - зал боротьби 6. Плавальні басейни 7. Інши споруди: Навчально-спортивний комплекс № 1, вул. Алчевських, 50 А: - Легко-атлетичний стадіон - Площадка для міні-футбола - Гімнастичне містечко - Корти тенісні Навчально-спортивний комплекс № 2, вул. Пушкінська,85: Ігрова площадка У разі переведення проведення навчальних занять у дистанційну форму застосовано корпоративна платформа офіс 365. Навчальні матеріали для дистанційної форми навчання містять завдання, методичні рекомендації, критерії оцінки. **Література:** 1. Бех І.Д. Виховання особистості: у 2 кн. Кн. 2: Особистісно орієнтований підхід: науково-практичні засади. – К.: Либідь, 2003.–344 с. 2. Глазирін І.Д. Основи диференційованого фізичного виховання: Навчальний посібник. – Черкаси: Відлуння-Плюс, 2003. – 351 с. 3. Захлевська Т.В., Волкова Т.В. Методичні вказівки з фізичного

Назва освітнього компонента	Вид компонента	Поле для завантаження Силабусу	Якщо освітній компонент потребує спеціального матеріально-технічного та/або інформаційного забезпечення, наведіть відомості щодо нього
			виховання «Методика розвитку швидкісних якостей (30,60,100 м)» для студентів усіх професійних напрямків. –О.:ОНАХТ, 2010. -18 с. 4. Копа В.М. Соціальна валеологія. Навчальний посібник .- Львів.: «Новий Світ-2000», 2001. -204 с. 5. Раевський Р.Т. Фізичне виховання як дієвий фактор забезпечення здоров'я студентської молоді / Р.Т. Раевський // Спорт для всіх. – Донецьк: ДонНУ. – 2000. - №1. – С.5-10. 6. Раевський Р.Т. Здоров'я, здоровий і оздоровчий образ життя студентів / Р.Т. Раевський, С.М. Канішевський; Під заг. ред. Р.Т. Раевського. – О.: Наука и техника, 2008. – 556 с. 7. Сергєєва Т.П. Методичні вказівки до використання фізичних вправ для профілактики захворювань для студентів усіх напрямків підготовки бакалаврів денної форми навчання-О.:ОНАХТ, 2010.-26 с. 8. Струк Б.І., Копа В.М., Поляков Р.А. Методичні вказівки з фізичного виховання «Організація самостійних занять фізичною культурою і спортом у спеціальних медичних групах» для студентів, які навчаються по навчальному плану бакалаврів усіх спеціальностей денної форми навчання. –О.:ОНАПТ, 2004. - 28 с. 9. Субота Ю.В. Оздоровчі рухові програми самостійних занять фізичною культурою і спортом: Практичний посібник / Ю.В Субота. – Київ: КНЕУ, 2007. – 164 с.
Фізичні основи технічних засобів розвідки	дисципліна спеціальна (фахова) підготовка	https://cybersecurity.kpi.kharkov.ua/sylabusy-osvitnikh-komponentiv-125-bakalavr/	**Обладнання:** Мультимедійні аудиторії **Кіберполігон:** Персональний комп` ютер 2E Integer Intel i5-11400/H510/16/480F/int/FreeDos/2E-S616/400W- 25 шт. Монітор HP P24 G5 FHD Monitor – 25 шт. Гарнітура для ПК 2E CH11, On-Ear, 3.5mm/2*3.5mm – 25 шт. Комплект 2E MK410 WL Black – 25 шт.

Назва освітнього компонента	Вид компонента	Поле для завантаження Силабусу	Якщо освітній компонент потребує спеціального матеріально-технічного та/або інформаційного забезпечення, наведіть відомості щодо нього
			Міжмережевий екран Fortinet FG- 40F 5*GE RJ45 ports (including 4* internal Ports 1* WAN Ports – 1 шт. Ноутбук/Notebook Del Vostro 3510/Core i3-1115G4/8GB/256GB SSD/15.6`` FHD/Intel UHD/Cam& Mic/WLAN + BT/Backlit Kb/3 Cell/W11Pro/3Yr – 2 шт. Багатофункціональний пристрій А4 ч/б Multifuntional device A4 b/w Xerox B235 (WI-FI) – 1 шт. Проєктор короткофокусний Epson EB-536Wi WXGA, 3400 lm, 0.65 інтерактивний – 1 шт. Проектор/ Projector Epson EB-X49 (3LCD, XGA,3600 ANSI lm) – 1 шт. Примірник П3 Microsoft Windows 11 Pro укр. OEM на DVD носії – 25 шт. Екран 2Е на тринозі,1:1, 112, (2.0*2.0) – 1 шт. Сервер R- LINE на базі Xeon Silver 421 OR – 1 шт. Точка доступу Ubiguiti UniFi 6 LR Access Point U6-LR – 1 шт. Маршрутизатор Mikro Tik RB4011iGS+5HacQ2HnD-IN – 1 шт. Комутатор D-Link DGS-1210-28X/ME – 1 шт. Сервер HPE ML350 Gen10 Hot Plug LFF CTO – 1 шт. ДБЖ HPE T1000 Gen5 INTL UPS with Management Card Slot – 1шт. Комутатор Aruba 6000 48G 4SFP Switch – 1 шт. Aruba 1G SFP LC LX 10km SMF Transceiver – 2 шт. Aruba 1G SFP RJ45T 100m Cat5e Transceiver – 2 шт. Ai-Thinker Wi-Fi модуль ESP8266 ESP-01S – 10 шт. Bluetooth модуль HC-05 – 10 шт. Бездротовий модуль NRF24L01+PA+LNA з зовнішньою SMA антеною – 10 шт. Мікрофон електретний в (6mm x 2.2mm) з ніжками – 10 шт. Модуль HC-SR04 ультразвуковий приймач передавач – 10 шт. Модуль SR602 мініатюрний інфрачервоний датчик руху – 10 шт.

Назва освітнього компонента	Вид компонента	Поле для завантаження Силабусу	Якщо освітній компонент потребує спеціального матеріально-технічного та/або інформаційного забезпечення, наведіть відомості щодо нього
			Модуль TTP223 TOUCH KEY сенсорний датчик для Arduino – 10 шт. Модуль TTP229 (сенсорна клавіатура) для Arduino – 10 шт. Модуль датчика відбитків пальцеві AS608 – 10 шт. Модуль звукового I2S ЦАП на PCM5102 32-бит 384K – 10 шт. модуль синтезу речи SYN6288 – 10 шт. Multi-Channel Relay Shield for Open Source Xbee BTbee Bluetooth – 10 шт. Модуль GPS NEO-6M Міні SMA – 10 шт. OLED дісплей 1.3" 12C/SPI інтерфейс 128x64 (синій) від Waveshare – 10 шт. RASPBERRY PI 4 MODEL B 4GB/ – 10 шт. USB адаптер модуль Zigbee CC2531 Sniffer сніфер – 10 шт. Комунікаційна плата-розширювач для Raspberry Pi с низьким енерговикористанням GSM/GPRS/GNSS/Bluetooth HAT – 10 шт. WiFi Плата NodeMCU V2 ESP8266 (CP2102) – 10 шт. Радіоприймач аналізатор спектру зібраний portapack h2+i hackrf one, жк дисплей, антени, корпус, акумулятор 2000 маг– 10 шт. Модуль читач картки rfid дублікатор ліфт карти контролю доступу читач proxmark3 простий 3.0 512 кб оперативної – 10 шт. **Література:** 1. Лаптєв О.А., Савченко В.А., Шуклін Г.В. Виявлення та блокування засобів негласного отримання інформації на об'єктах інформаційної діяльності: Навчальній посібник. – Київ: ДУТ, 2020. – 126 с. 2. Іванченко С.О., Гавриленко О.В., Липський О.А., Шевцов А.С. Технічні канали витоку інформації. Порядок створення комплексів технічного захисту інформації: Навчальній посібник. – Київ: НТУУ, 2016. – 104 с. 3. Jacobson D., Idziorek J. Computer security literacy: staying safe in a digital world. – CRC Press, 2016.

Назва освітнього компонента	Вид компонента	Поле для завантаження Силабусу	Якщо освітній компонент потребує спеціального матеріально-технічного та/або інформаційного забезпечення, наведіть відомості щодо нього
			4. Iniewski K. (ed.). Semiconductor radiation detection systems. – CRC press, 2018. Mitra S., Gofman M. (ed.). Biometrics in a data driven world: trends, technologies, and challenges. – CRC Press, 2016. 5. Цифрова схемотехніка та архітектура мікропроцесорів: навчальний посібник / Євсеєв С. П., Дженюк Н.В., Охрименко М.Ю. та ін. – Харків, – Львів: Видавництво ПП «Новий Світ – 2000», 2023. –513 с. 6. Євсеєв С.П. КІБЕРБЕЗПЕКА: ЛАБОРАТОРНИЙ ПРАКТИКУМ З ОСНОВ КРИПОГРАФІЧНОГО ЗАХИСТУ / С.П. Євсеєв, О.В. Мілов, О.Г. Король – Львів: «Новий Світ- 2000», 2020 . – 241
Філософія	дисципліна загальна підготовка	https://cybersecurity.kpi.kharkov.ua/sylabusy-osvitnikh-komponentiv-125-bakalavr/	**Обладнання:** не потребує **Література:** 1. Вступ до філософії : навч.-метод. посіб. / Владленова І.В.; Годзь Н.Б.; Городиська О.М. та ін.; за ред. Городиської О.М.; Дольської О.О. Х. : НТУ «ХПІ», 2018. 2. Філософія: навч.посіб. / О.М. Бардін, В.В. Булавіна, Н.Б. Годзь та ін.; за ред.. О.М. Бардіна, М.П. Требіна. Харків: НТУ «ХПІ», 2012. 3. Дольська О. О. Філософія сучасного суспільства: навч.-метод. Посібник. Харків : НТУ “ХПІ”, 2012. 4. Городиська О.М., Дольська О.О., Мелякова Ю.В. Проблема людини у вимірах філософського аналізу: текст лекції. Х.: НТУ «ХПІ», 2008. 5. Філософія: терміни і поняття: Навчальний енциклопедичний словник / Під ред. В.Л. Петрушенка. Львів: Новий світ – 2000, 2020. 6. Філософія. Природа, проблематика, класичні розділи: навч.

Назва освітнього компонента	Вид компонента	Поле для завантаження Силабусу	Якщо освітній компонент потребує спеціального матеріально-технічного та/або інформаційного забезпечення, наведіть відомості щодо нього
			посібник / В.П. Андрущенко та ін.; НПУ. Київ: Каравела, 2015. 7. Історія філософії: проблема людини та її меж. Вступ до філософської антропології як метаантропології: навч. посібник зі словником. 4-е вид. перероб. та доп. К:. КНТ, 2016. 8. Філософія: хрестоматія (від витоків до сьогодення): навч. посібник / КНУ; уклад. Л.В. Губерський та ін. 2-ге вид., стер. Київ: Знання, 2012. 9. Філософія: навч. посібник / К.В. Кислюк. 3-тє вид., випр. Київ: Кондор, 2016. 10. Філософія: підручник / В.Л. Петрушенко. 5-те вид., стер. Львів: «Новий світ-2000». 2019. 11. Філософія: підручник / Л.В. Губерський та ін.; ред. В.Л. Губерський. Харків: Фоліо, 2013. 12. Філософія: підручник / О.Г. Данильян, О.П. Дзьобань; НЮУ ім. Ярослава Мудрого. 2-ге вид., перероб і доп. Харків: Право, 2019.

Таблиця 2. Зведена інформація про викладачів

ПІБ викладача	Посада	Структурний підрозділ, у якому працює викладач	Інформація про кваліфікацію викладача	Стаж науково-педагогічної роботи	Навчальні дисципліни,що їх викладає викладач на ОП	Обгрунтування
Дворкін Ігор Володимирович	доцент	кафедра українознавства, культурології та історії науки НТУ «ХПІ»	Харківський національний університет імені В.Н. Каразіна, спеціальність «Архівознавство»кваліфікація «архівіст, історик, викладач, суспільно-політичних дисциплін» (диплом ХА № 28132819), 2005 рік. **Кандидат історичних наук**, 07.00.01 – Історія України (диплом ДК №056268 від 16.12.2009). **Тема дисертації:** «Трансформація музейної справи Наддніпрянщини у 1805–1920 рр.(за матеріалами Полтавської, Харківської, Чернігівської губерній та м. Києва)» **Доцент кафедри українознавства, культурології та історії науки** (атестат доцента АД №007470	15 років	ЗП 1. Історія та культура України	**Підвищення кваліфікації:** 1.Участь у циклі історичних вебінарів, літній програмі та семінарах; навчання на курсах англійської мови та отримання сертифіката В2 в обсязі 2 кредити ЄКТС (60 годин). Наказ НТУ «ХПІ» № 1982с від 24.11.2021 р. 2.Участь у лекційних курсах та дистанційних навчальних програмах 1 кредит ЄКТС (30 годин). Наказ НТУ «ХПІ» № 29с від 13.01.2023 р. 3.Закордонне стажування у Центрі наукових досліджень Голокосту імені Джека, Джозефа і Мортона Мандел Меморіального музею Голокосту Сполучених Штатів Америки **Термін навчання:** 3 місяці 180 годин (6 кредитів ЄКТС), Наказ НТУ «ХПІ» № 64с від 23.01.2023 р. **Пункти відповідності ліцензійних умов: П.1, 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. Dvorkin, I., Kharchenko, A., & Telukha, S. (2020). The establishment of the Kharkiv Practical Technological Institute in the context of modernization. History of Science and Technology, 10(2), 266-280. https://doi.org/10.32703/2415-7422-2020-10-2-266-280 **Scopus** 2. Дворкін І., Телуха С., Харченко А. Формування історичної пам'яті в підручниках з історії України: до та після Євромайдану // Сторінки історії. - 2021. – Вип. 53. https://doi.org/10.20535/2307-5244.53.2021.248570 **Web of Science** 3. Дворкін І.В. Всупереч імперській політиці: українознавство в музеях Наддніпрянщини другої половини XIX – початку XX ст. // Українознавчий альманах: КНУ ім. Т. Шевченка. Центр Українознавства. - 2019. - Вип.24. - С. 56 – 60. Index Copernicus 4. Дворкін І.В. Музейництво в Києві (1830-ті – 1919 рр.): формування, розвиток, трансформація під час революції // Місто: історія, культура, суспільство: Е-журнал урбаністичних студій: Інститут історії України НАН України, Історичний факультет Київського національного університету імені

ПІБ викладача	Посада	Структурний підрозділ, у якому працює викладач	Інформація про кваліфікацію викладача	Стаж науково-педагогічної роботи	Навчальні дисципліни,що їх викладає викладач на ОП	Обґрунтування
			від 15 квітня 2021 року) Certificate B2 iTEP International: English Language Proficiency Level: Upper Intermediate Date of test 24.12.2020			Тараса Шевченка. - Київ. – 2020. - N. 8 (Червень). - С. 24-35. Index Copernicus 5. Дворкін І. Єврейські погроми кінця XIX – початку XX ст. у сучасній українській історіографії // Українознавчий альманах: КНУ ім. Т. Шевченка. Центр Українознавства. - 2021. - Вип.29. - С. 66 – 73. Index Copernicus **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. Вандишева-Ребро В.Н., Гутник. М.В., Дворкін І.В. та ін. Плани семінарів та методичні рекомендації з дисципліни «Історія та культура України»: навч. -метод. посіб. для студентів усіх спеціальностей / За заг. ред. Петутіної О. О., Савченка Л. П. Харків: НТУ «ХПІ», 2019. - 55 с. http://repository.kpi.kharkov.ua/handle/KhPI-Press/42883 2. Гутник М.В., Дворкін І.В. Методичні вказівки до виконання підсумкової контрольної роботи з дисципліни «Історія та культура України» для бакалаврів усіх напрямків підготовки. - Харків: НТУ «ХПІ», 2019. - 34 с. http://repository.kpi.kharkov.ua/handle/KhPI-Press/43294 3. Дворкін І.В., Телуха С.С., Фрадкіна Н.В. Тематика групових занять та індивідуальних завдань з дисципліни «Історія України та українська культура»: Методичні рекомендації для курсантів Військового інституту танкових військ НТУ «ХПІ». - Харків: НТУ «ХПІ», 2020. – 25 с. http://web.kpi.kharkov.ua/ukin/wp-content/uploads/sites/195/2021/01/Metodychni-rekomendatsiyi-dlya-kursantiv-Vijskovogo-instytut-tankovyh-vijsk-NTU-HPI-.pdf 4. Методичні вказівки до семінарських занять з історії України [Електронний ресурс] : для студентів усіх спец. / уклад.: І. В. Дворкін [та ін.] ; Нац. техн. ун-т "Харків. політехн. ін-т". – Електрон. текст. дані. – Харків, 2021. – 48 с. – URI: http://repository.kpi.kharkov.ua/handle/KhPI-Press/54541 5. Дворкін І. В. Конспект лекцій з навчальної дисципліни "Сучасні напрями історичних досліджень" [Електронний ресурс] : для аспірантів спеціальності 032 "Історія та археологія" / І. В. Дворкін, А. В. Харченко ; Нац. техн. ун-т "Харків. політехн. ін-т". – Електрон. текст. дані. – Харків, 2022. – 50 с. – URI: http://repository.kpi.kharkov.ua/handle/KhPI-Press/59343 6. Методичні вказівки з навчальної дисципліни "Сучасні напрями історичних досліджень" [Електронний ресурс] : для аспірантів спец. 032 "Історія та археологія" / уклад.: І. В. Дворкін, А. В. Харченко ;

ПІБ викладача	Посада	Структурний підрозділ, у якому працює викладач	Інформація про кваліфікацію викладача	Стаж науково-педагогічної роботи	Навчальні дисципліни,що їх викладає викладач на ОП	Обґрунтування
						Нац. техн. ун-т "Харків. політехн. ін-т". – Електрон. текст. дані. – Харків, 2022. – 31 с. – URI: http://repository.kpi.kharkov.ua/handle/KhPI-Press/59344 **П.10. Участь у міжнародних наукових та/або освітніх проектах, залучення до міжнародної експертизи, наявність звання "суддя міжнародної категорії** 1. Призма Україна: Війна, Міграція, Пам'ять / Prisma Ukraïna "War, Migration and Memory", участь у міждисциплінарному дослідницькому проекті, 2022-2023 рр. 2. The Foundation of Hamburg Memorials and Learning Centres Commemorating the Victims of Nazi Crimes "Project: (Post)Soviet culture of remembrance of Nazi persecution during occupation in Eastern Europe"/ sub-area "Official culture(s) of remembrance in Ukraine (Post)Soviet society", дослідницька робота у рамках міжнародного наукового проекту 2022 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. Дворкін І. В. Пам'ять про польських офіцерів – жертв репресій у Харкові / І. В. Дворкін // Інформаційні технології: наука, техніка, технологія, освіта, здоров'я = Information technologies: science, engineering, technology, education, health : тези доп. 30-ї Міжнар. наук.-практ. конф. MicroCAD-2022, 19-21 жовтня 2022 р. / ред. Є. І. Сокол ; уклад. Г. В. Лісачук. – Харків : НТУ "ХПІ", 2022. – С. 699 2. Дворкін І.В. Внесок Володимира Антоновича у розвиток музейної справи. Інформаційні технології: наука, техніка, технологія, освіта, здоров'я: тези доповідей XXVII міжнародної науково-практичної конференції MicroCAD-2019, 15-17 травня 2019р.: у 4 ч. Ч. IV. /за ред. проф. Сокола Є.І. Харків: НТУ «ХПІ». С. 66. URL: http://www.kpi.kharkov.ua/archive/MicroCAD/2019/%D0%A1%D0%B5%D0%BA%D1%86%D0%B8%D1%8F_17/s17_8.pdf 3. Дворкін І.В. Масовий спорт в ХПІ у 1950-1991 рр. Здоров'я нації і вдосконалення фізкультурно-спортивної освіти: матеріали І Міжнародної на-уково-практичної конференції, 3-4 жовтня 2019 р. / ред. колегія А. В. Кіпенський, О. В. Білоус [та ін.]. Харків: Друкарня Мадрид, 2019. С. 308-312. 4. Дворкін І.В. Етнографічний музей Харківського історико-філологічного товариства - український національний музей імперського періоду. Інформаційні технології: наука, техніка, технологія, освіта, здоров'я: тези доповідей XXVII міжнародної науково-практичної конференції MicroCAD-2020, 21-23 жовтня 2020

ПІБ викладача	Посада	Структурний підрозділ, у якому працює викладач	Інформація про кваліфікацію викладача	Стаж науково-педагогічної роботи	Навчальні дисципліни,що їх викладає викладач на ОП	Обґрунтування
						р.: у 5 ч. Ч. IV/ за ред. проф. Сокола Є.І. Харків : НТУ “ХПІ”. С. 71. http://repository.kpi.kharkov.ua/bitstream/KhPI-Press/49069/1/Conference_NTU_KhPI_2020_MicroCAD_Ch_4.pdf 5. Фізична культура і спорт Харківського Політеху. Історія. Досягнення. Перспективи / О.В. Білоус, К.М. Блещунова, Н.Ю. Борейко та ін.; За заг. ред. А.В. Кіпенського та В.М. Скляра. – Харків: Друкарня Мадрид, 2020. – 185/30 с. http://repository.kpi.kharkov.ua/handle/KhPI-Press/50955?locale=en (у співавторстві) 6. Дворкін І.В. “Місця пам’яті” Другої світової війни у Харкові // Двадцять сьома Всеукраїнська наукова конференція молодих істориків науки, техніки і освіти та спеціалістів за темою: «Молодь в історії науки і техніки: консолідація української нації». мат. Конф., 22 квітня 2022 р., м. Київ, 2022. – С.59-61. 7. Dvorkin I, Telukha S. Holocaust-Gedenkorte in Charkiw. Memorialisierung im städtischen Raum. Aktives Museum Faschismus und Widerstand in Berlin e.V, Mitgliederrundbrief 87, august 2022, S.26-27. 8. Dvorkin Ihor. May 8th/9th: Commemoration in Ukraine // https://www.dialogueperspectives.org/blog/commemoration-in-ukraine/ **П. 13. Проведення навчальних занять із спеціальних дисциплін іноземною мовою (крім дисциплін мовної підготовки) в обсязі не менше 50 аудиторних годин на навчальний рік:** Certificate B2 iTEP International: English Language Proficiency Level: Upper Intermediate, Date of test 24.12.2020 Викладання дисципліни «Історія та культура України» іноземним студентам та групам, що навчаються англійською мовою. 2019-2020 навчальний рік: групи КІТ 119і.е., БЕМ 519ае, БЕМ 619ае. Загальний обсяг 77 годин; 2020-2021 навчальний рік: групи КІТ 120і.е, КІТ 220і.е.К КІТ220і.е. Загальний обсяг 80 годин. 2021-2022 навчальний рік: групи КН 221бе, 421ае, 421іае, 221іае, 221ібе, 221іве. І-221іае Загальний обсяг: 90 годин. 2022-2023навчальний рік: групи КН 222ае, 1122іа, 922іа, 922зіа. Загальний обсяг 60 годин **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:** 1. Співголова студентського наукового гуртка «Історик» кафедри

ПІБ викладача	Посада	Структурний підрозділ, у якому працює викладач	Інформація про кваліфікацію викладача	Стаж науково-педагогічної роботи	Навчальні дисципліни,що їх викладає викладач на ОП	Обґрунтування
						країнознавства, культурології та історії науки (наказ НТУ «ХПІ» № 394 ОД від 10 вересня 2019 р. Наказ НТУ «ХПІ» № 272 ОД від 11 червня 2021 р., наказ № 344 ОД НТУ «ХПІ» від 14.11.2022 р.) 2. Керівництво студентмами, які зайняли призові місця на І етапі Всеукраїнської студентської олімпіади з історії України – Баландін Д. (КН-319а – ІІ місце, 2019 р.), Ненахова Ю. (КН-819 – ІІ місце, 2019 р.), Анісімова В. (КН-619 – І місце, 2019 р.). **П. 19 Діяльність за спеціальністю у формі участі у професійних та/або громадських об'єднаннях:** 1. Центр дослідження міжетнічних відносин Східної Європи (з 2011 року до теперішнього часу). Співзасновник 2. Наукове товариство імен Тараса Шевченка НТШ-А (США) (2022 р.) Зв'язок із організацією 6 місяців
Кримець Оксана Михайлівна	доцент	кафедра української мови НТУ «ХПІ»	**Освіта:** «Харківський державний університет», 1993р. **Спеціальність:** «Російська мова та література». Диплом КЗ № 004303 від 30.06.1993 р. **Кваліфікація спеціаліста:** Філолог. Викладач російської мови та літератури. **Науковий ступінь:** Кандидат філологічних наук, 10.02.01 – зі спеціальності українська мова. Диплом ДК № 067739 від 22.04.2011 р. **Тема дисертації:** «Метафора і метонімія як чинники творення та розвитку української технічної	31 рік	ЗП 2. Українська мова (за професійним спрямуванням)	**Підвищення кваліфікації:** кафедра української та російської мов як іноземних Харківського національного університету міського господарства ім. О.М. Бекетова Свідоцтво № 431 від 16.02.2021 р., **Тема:** «Інновації у викладанні української мови як іноземної» **Термін навчання:** 3 місяці Наказ НТУ «ХПІ»: № 1728 с від 03.11.2020) Сертифікат В2: UA 1534 від 03.12.2021р. **Пункти відповідності ліцензійних умов:** **П. 1, 3, 4, 12, 14** **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. Кримець О.М. Наукова картина як інтегральна модель пізнання світу // Науковий вісник Національного університету біоресурсів і природокористування України. Серія: Філологічні науки.− К.: Міленіум, 2018. −Вип. 292.− С. 202 – 208. http://repository.kpi.kharkov.ua/ha ndle/KhPI-Press/41941 2. Кримець О.М. Польова та мікропольова структура термінології нанотехнологій // Наукові праці Кам'янець-Подільського національного університету імені Івана Огієнка: Філологічні науки.− Кам'янець-Подільський: Аксіома, 2019. – Випуск 50.− С. 86 – 89. http://repository.kpi.kharkov.ua/handle/KhPI-Press/46752 3. Кримець О.М. Специфіка семантичних процесів в українській науково-технічній термінології. Лінгвістичні дослідження // Збірник наукових праць ХНПУ ім. Г.С. Сковороди, 2020.− Вип.52. – С. 64 – 72. http://repository.kpi.kharkov.ua/handle/KhPI-Press/46754 4. Кримець О.М. Міжгалузеві терміни в українській науково-

ПІБ викладача	Посада	Структурний підрозділ, у якому працює викладач	Інформація про кваліфікацію викладача	Стаж науково-педагогічної роботи	Навчальні дисципліни,що їх викладає викладач на ОП	Обґрунтування
			термінології», 2010 р. **Вчене звання:** Доцент кафедри української, російської мов і прикладної лінгвістики НТУ «ХПІ». Атестат 12ДЦ№034061 від 25.01.2013 р.			технічній термінології. Лінгвістичні дослідження: збірник наукових праць ХНПУ ім. Г.С. Сковороди.– Харків, 2020.– Вип.53.– С. 192 – 199. http://repository.kpi.kharkov.ua/handle/KhPI-Press/50055 5. Кримець О.М. Запозичення в термінології нанотехнологій // Лінгвістичні дослідження: зб. наук. праць ХНПУ імені Г. С. Сковороди, 2021. – Вип. 55.– С 68-75. http://repository.kpi.kharkov.ua/handle/KhPI-Press/55219 6. Кримець О.М. Шляхи формування термінології нанотехнологій. Лінгвістичні дослідження: зб. наук. пр. Харк. нац. пед. ун-ту імені Г. С. Сковороди / гол. ред. О. В. Халіман. Харків, 2022. Вип. 57. С. 3–9. http://repository.kpi.kharkov.ua/handle/KhPI-Press/59882 **П.3 наявність виданого підручника чи навчального посібника (включаючи електронні) або монографії (загальним обсягом не менше 5 авторських аркушів), в тому числі видані у співавторстві (обсягом не менше 1,5 авторського аркуша на кожного співавтора);** 1. Кримець О.М. Офіційно-діловий стиль: Правила укладання документів різних видів: навчальний посібник щодо самостійної роботи студентів. – Харків: НТУ «ХПІ», 2019. – 140 с., ум. друк арк.16,2 (співавтори: Чернявська С.М., Заверющенко М.П., Шокуров О.В). http://repository.kpi.kharkov.ua/handle/KhPI-Press/41937 2. Кримець О.М. Українська мова як іноземна: початковий рівень [Електронний ресурс] : навч. посібник / Г. І. Сабадир [та ін.] ; Нац. техн. ун-т "Харків. політехн. ін-т". – Електрон. текст. дані. – Харків, 2022. – 120 с. – Ум. друк. арк.5,4 (співавтори: Чернявська С.М., Дяченко О.В., Лухіна М.Ю., Сабадир Г.І.) http://repository.kpi.kharkov.ua/handle/KhPI-Press/62926 **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. Кримець О.М. Оброблення наукової інформації: навчально-методичний посібник для студентів І курсу всіх спеціальностей.–

ПІБ викладача	Посада	Структурний підрозділ, у якому працює викладач	Інформація про кваліфікацію викладача	Стаж науково-педагогічної роботи	Навчальні дисципліни,що їх викладає викладач на ОП	Обґрунтування
						Харків: НТУ «ХПІ», 2019. – 108 с. (співавтор: Гомон А.М.) http://repository.kpi.kharkov.ua/handle/KhPI-Press/46756 2. Кримець О.М. Научный стиль речи: Компрессия текста: учебное пособие для иностранных студентов технических специальностей. – Харьков: НТУ «ХПИ», 2019. – 120 с. (співавтори: Чернявська С.М., Заверющенко М.П., Немерцова О.Є). http://repository.kpi.kharkov.ua/handle/KhPI-Press/41936 3. Кримець О.М. Сборник упражнений по грамматике.− Харків: НТУ «ХПІ», 2020.− 45 с. - методичні вказівки. (співавтори: Чернявська С.М., Немерцова О.Є., Сабадир Г.І., Шокуров О.В.) http://repository.kpi.kharkov.ua/handle/KhPI-Press/44812 4. Кримець О.М. Методичні рекомендації до самостійної роботи з курсу "Українська мова" [Електронний ресурс] : для студентів комп'ютерних спеціальностей / уклад.: С. М. Чернявська [та ін.] ; Нац. техн. ун-т "Харків. політехн. ін-т". – Електрон. текст. дані. – Харків, 2022. – 40 с. (співавтори: Чернявська С.М., Заверющенко М.П., Лухіна М.Ю., Сабадир Г.І.) http://repository.kpi.kharkov.ua/handle/KhPI-Press/57551 5. Кримець О.М. Методичні рекомендації до самостійної роботи з курсу "Українська мова" [Електронний ресурс] : для студентів електроенергетичних спеціальностей / уклад.: С. М. Чернявська [та ін.] ; Нац. техн. ун-т "Харків. політехн. ін-т". – Електрон. текст. дані. – Харків, 2022. – 44 с. (співавтори: Чернявська С.М., Заверющенко М.П., Лухіна М.Ю., Сабадир Г.І.) http://repository.kpi.kharkov.ua/handle/KhPI-Press/57550 6. Кримець О.М. Методичні вказівки з курсу «Українська мова (професійного спрямування)» для студентів спеціальності 162 «Біотехнології та біоінженерія» / Укл.: С. М. Чернявська, О. М. Кримець, О. Є. Немерцова, О. В. Дяченко, Близнюк О. М., Масалітіна Н. Ю. – Харків: НТУ «ХПІ», 2022. – 38 с. http://repository.kpi.kharkov.ua/handle/KhPI-Press/60446 7. Кримець О.М. Робоча програма навчальної дисципліни «Ділова українська мова та професійна комунікація» для спеціальності 113 «Прикладна математика», 2022 р. (співавтор: Заверющенко М.П.) https://web.kpi.kharkov.ua/lingvo/uk/robocha-programa/ 8. Кримець О.М. Методичні рекомендації до самостійної роботи з

ПІБ викладача	Посада	Структурний підрозділ, у якому працює викладач	Інформація про кваліфікацію викладача	Стаж науково-педагогічної роботи	Навчальні дисципліни,що їх викладає викладач на ОП	Обгрунтування
						курсу «Українська мова» для студентів економічних спеціальностей / уклад. О.М. Кримець, М.Ю. Лухіна, А.М. Гомон. – Харків : НТУ «ХПІ», 2023. – 40 с. **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. Кримець О.М. Стан та перспективи розвитку української технічної термінології // Актуальні проблеми сучасної філології та методики викладання мов у вишах: матеріали Всеукраїнської науково-практичної конференції (6 квітня 2018 р., м. Харків). – Харків: ФОП Бровін О.В., 2018. – С. 20 – 21. http://repository.kpi.kharkov.ua/handle/KhPI-Press/36197 2.Кримець О.М. Розвиток української науково-технічної термінології сьогодні: напрями і перспективи // Key issues of education and sciences: development prospects for Ukraine and Poland. 20-21 July 2018.− Volume 2.−− Stalowa Wola: Izdevnieciba Baltija Publishing, 2018.− P.193–196. (Співавтор: Петрова Т.О.). http://repository.kpi.kharkov.ua/handle/KhPI-Press/41943 3. Кримець О.М. Розбудова технічної термінології шляхом реінтегрування наукових знань інших галузей // Матеріали Міжнародної науково-практичної конференції з нагоди ювілею доктора філологічних наук, професора К. Г. Городенської «Соціокультурні та комунікативні аспекти функціонування мовних одиниць». 29-30 листопада 2018 року. – К.: Міленіум, 2018.− С. 125 – 126. http://repository.kpi.kharkov.ua/handle/KhPI-Press/41940 4. Кримець О.М. Військова лексика в метафоричному науково-технічному дискурсі // Актуальні проблеми сучасної філології та методики викладання мов у вишах : матеріали II Всеукраїнської науково-практичної конференції 8 жовтня 2019 року (Харківський національний аграрний університет ім. В.В. Докучаєва). – Харків: Мадрид, 2019. – С. 21 – 23. http://repository.kpi.kharkov.ua/handle/KhPI-Press/46750 5. Кримець О.М. Застосування флокулянтів природного походження для підвищення ефективності біотехнології очищення стічних вод харчових харчових виробництв // Хімія, біо- і нанотехнології, екологія та економіка в харчовій і косметичній промисловості: Збірник матеріалів IX Міжнародної науково-практичної конференції, 18–19 листопада 2021 року – Х., 2021. − С. 167-168. (співавтори:

ПІБ викладача	Посада	Структурний підрозділ, у якому працює викладач	Інформація про кваліфікацію викладача	Стаж науково-педагогічної роботи	Навчальні дисципліни,що їх викладає викладач на ОП	Обґрунтування
						Близнюк О.М., Масалітіна Н.Ю., Чернявська С.М.). http://repository.kpi.kharkov.ua/handle/KhPI-Press/55178 6. Кримець О.М. Біотехнологія виробництва молочної кислоти для використання в косметології // Хімія, біо- і нанотехнології, екологія та економіка в харчовій і косметичній промисловості: Збірник матеріалів IX Міжнародної науково-практичної конференції, 18–19 листопада 2021 року – Х., 2021. − С. 241-242. (співавтори: Зленко К.А., Масалітіна Н.Ю, Близнюк О.М.) http://repository.kpi.kharkov.ua/handle/KhPI-Press/55179 **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;** Керівництво студенткою групи БЕМ- БЕМ-919а Зленко Владиславою Олегівною, яка посіла 1 місце в І етапі XX Міжнародного конкурсу з української мови ім. П. Яцика у 2019/20 н.р.

ПІБ викладача	Посада	Структурний підрозділ, у якому працює викладач	Інформація про кваліфікацію викладача	Стаж науково-педагогічної роботи	Навчальні дисципліни,що їх викладає викладач на ОП	Обґрунтування
						Керівництво студенткою групи КІТ-220а Кошелевою Марією, яка стала переможницею в І етапі Всеукраїнської студентської олімпіади з української мови у 2020/21 н.р. Керівництво студенткою групи БЕМ-1021д Остапенко Катериною Олексіївною, яка посіла 2 місце в І етапі XXII Міжнародного конкурсу з української мови ім. Петра Яцика у 2021/22 н.р. Керівництво студенткою групи ХТ-422б Навчально-наукового інституту хімічних технологій та інженерії Купець Дариною Михайлівною, яка посіла 1 місце в І етапі XXIII Міжнародного конкурсу з української мови імені Петра Яцика 2022/2023 н.р.
Гончаренко Тетяна Євгенівна	завідувач кафедри	кафедра іноземних мов НТУ «ХПІ»	**Освіта:** Харківський державний університет ім. О.М. Горького, 1990. Диплом УВ № 717045 **Спеціальність**: «Англійська мова та література», **Кваліфікація:** викладач англійської мови, перекладач, викладач французької мови **Кандидат пед. наук:** 13.00.04 «Теорія і методика професійної освіти». **Тема дисертації**: «Педагогічні умови професійної підготовки майбутніх інженерів-програмістів у технічному університеті». Диплом ДК № 048392 від 05.07.2018р. **Доцент** кафедри	34 роки	ЗП 3. Іноземна мова	**Підвищення кваліфікації:** 1. Тренінги «Англійська для спеціальних цілей» та «Англійська для академічних цілей» в рамках проекту Британської Ради “English for Universities” 2016 р. Наказ НТУ»ХПІ» № 2257 С від 05.12.2016р**.** 2. Харківський національний університет радіоелектроніки, **Термін навчання:** з 15.10.2020 по 29.12.2020, 6 кредитів ЄКТС, Свідоцтво № 469 від 02.03.2021 р. **Пункти відповідності ліцензійних умов:** **П. 1. 3, 5, 10, 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) Михайло Годлевський, Тетяна Гончаренко, Георгій Бурлаков, Дмитро Малець Шляхи підвищення якості процесу розробки програмного забезпечення на основі моделей зрілості. *Вісник Національного технічного університету. - Серія: Системний аналіз, управління та інформаційні технології.* - Х: НТУ "ХПІ",2019. № 2. С. 63-69. 2)Sergey Orekhov, Henadii Malyhon, Irina Liutenko, Tetiana Goncharenko Using Internet News Flows as Marketing Data Component// Proceedings of the 4th International Conference on Computational Linguistics and Intelligent Systems (COLINS 2020). Volume I: Main Conference, Lviv, Ukraine, April 23-24, 2020. CEUR Workshop Proceedings 2604, CEUR-WS.org 2020, p. 358-373. 3) Goncharenko, T. Orekhov, S., Malyhon, H Mathematical model of semantic kernel of WEB site CEUR Workshop Proceedings, 2021, 2917, pp. 273–282

ПІБ викладача	Посада	Структурний підрозділ, у якому працює викладач	Інформація про кваліфікацію викладача	Стаж науково-педагогічної роботи	Навчальні дисципліни,що їх викладає викладач на ОП	Обгрунтування
			іноземних мов: Атестат доцента АД № 005335 від 24.09.2020 р.			4) Goncharenko, T. Orekhov, S., Malyhon, H., Stratienko, N. Software development for semantic kernel forming CEUR Workshop Proceedings, 2021, 2870, pp. 1312–1322. 5) Shtefan, V.V., Kanunnikova, N.O. & Goncharenko, T.Y. Analysis of the Structure and Anticorrosion Properties of Oxide Coatings on AISI 304 Steel. Mater Sci 57, Springer Nature, 248–255, 2022 6) Гончаренко Т. Є., Костенко О. В. ВІДПОВІДНІСТЬ НАВЧАЛЬНИХ ПРОГРАМ ESP КАФЕДРИ ІНОЗЕМНИХ МОВ НТУ «ХПІ» РОЗВИТКУ ЗАГАЛЬНИХ ПРОФЕСФЙНИХ КОМПЕТЕНТНОСТЕЙ МАЙБУТНІХ ІТФАХІВЦІВ № 3, 2022. – С. 96-102 7) Sergey Orekhov, Hennadiy Malyhon, Tetiana Goncharenko. A New Method of Search Engine Optimization Based on Semantic Kernel Idea // Lecture Notes on Data Engineering and Communication Technologies. Springer Nature Switzerland, Vol.159, pp.67-78, 2023 **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):** Гончаренко Т. Є., Воловщиков В. Ю., Іванов Л. В., Рубін Е. Ю. Гончаренко Т. Є. Мова С++ в програмуванні та комп'ютерних науках : навчальний посібник. Х. : ФОП Мезіна В.В., 2017. 280 с. (25%) **П.5 Захист дисертації на здобуття наукового ступеня:** **Кандидат пед. наук:** шифр: 13.00.04 «Теорія і методика професійної освіти», тема дисертації: «Педагогічні умови професійної підготовки майбутніх інженерів-програмістів у технічному університеті». ХНПУ ім. Г.С.Сковороди, диплом ДК № 048392 від 05.07.2018р. **П.10 Участь у міжнародних наукових та/або освітніх проектах, залучення до міжнародної експертизи, наявність звання "суддя міжнародної категорії":** Участь у роботі Міжнародного проекту Британської Ради в Україні English for Universities project. (2016-19рр.) **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**

ПІБ викладача	Посада	Структурний підрозділ, у якому працює викладач	Інформація про кваліфікацію викладача	Стаж науково-педагогічної роботи	Навчальні дисципліни,що їх викладає викладач на ОП	Обґрунтування
						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: Керівництво студентом Гуляковим О. група КН 219 а, який зайняв призове (І) місце у Всеукраїнської студентської олімпіади з англійської мови (2019 р.) **П.19 Діяльність за спеціальністю у формі участі у професійних та/або громадських об'єднаннях:** Є членом професійного об'єднання TESOL (Teaching English to Speakers of Other Languages) з листопада 2018 року
Тавріна Тетяна Володимирівна	доцент	кафедра фізики НТУ «ХПІ»	Харківський Державний політехнічний інститут (нині НТУ «ХПІ»), 1996 р. **Спеціальність:** фізика металів, Диплом КД № 900709 від 28.02.1996 р. **Кваліфікація:** інженер-фізик **Кандидат технічних**	28 років	ЗП 4. Фізика	**Підвищення кваліфікації:** 1. Харківський національний університет ім. В.Н. Каразіна, Інститут післядипломної освіти та заочного (дистанційного) навчання, свідоцтво № 956, квіт. 2018 р., тема: «Впровадження в навчальний процес сучасних технологій, методів і форм викладання дисципліни «Загальна фізика», Наказ НТУ «ХПІ» № 2372С від 18.12.2017, наказ ХНУ ім. В.Н. Каразіна № 0207-3/119 від 14.02.2018 р. 2. Сертифікат про проходження тренінгу «TEACHERS' SMART UP» від Sigma Software University, 24.01.2022-28.01.2022 р., Харків, Україна – 30 год. (1 кред.). 3. Сертифікат про участь у XIX Міжнародній школі-семінарі «Сучасні педагогічні технології в освіті», 02.02.2022-04.02.2022, НТУ ХПІ, Харків, Україна – 18 год. (0,6 кред.).

ПІБ викладача	Посада	Структурний підрозділ, у якому працює викладач	Інформація про кваліфікацію викладача	Стаж науково-педагогічної роботи	Навчальні дисципліни,що їх викладає викладач на ОП	Обгрунтування
			наук 01.04.10 – фізика напівпровідників і діелектриків, листопад 2002 р., диплом ДК № 016623 від 13.11.2002 р., **Тема дисертації:** «Вплив відхилу від стехіометрії та введення сульфіду кадмію на структуру і фізичні властивості $CuInSe_2$»; **Доцент** кафедри теоретичної та експериментальної фізики, аттестат доцента 12 ДЦ № 024975 від 14.04.2011 р.			4. Сертифікат про закінчення курсу «Компетенції викладачів 4.0» від центру «Розвиток КСВ» та Servier Ukraine, липень 2022, (2 год.). 5. Сертифікат про закінчення курсу «Інформаційна гігієна під час війни» на платформі масових відкритих онлайн-курсів PROMETEUS, - жовтень 2022, 15 год. (0,5 кред.) 6. Сертифікат про закінчення курсу «Introduction to Systematic Review and Meta-Analysis Course» від Європейської Академії наук і досліджень, жовтень 2022, 14 год. (0,47 кред.) 7. Сертифікат про закінчення курсу «SSWU TCHR002: Teachers' Smartup Winter Productivity» від Sigma Software University, 23.01.2023-27.01.2023 р., Україна – 30 год. (1 кред.). 8. Сертифікат про участь у XX Міжнародній школі-семінарі «Сучасні педагогічні технології в освіті», 04.04.2023-08.04.2023, НТУ ХПІ, Харків, Україна – 15 год. (0,5 кред.). **Пункти відповідності ліцензійних умов** **П. 1, 3, 4, 8, 11, 12, 13, 14, 19** **П.1 Публікації у періодичних виданнях, що включені до переліку фахових видань України, до наукометричних баз Scopus, Web of Science Core Collection):** 1. Nikolaenko G.O., Thermal conductivity of $PbSe_{1-x}Te_x$ (x = 0 – 0.04) solid solutions / G.O. Nikolaenko, Vodoriz O.S., Rogachova O.I., **Tavrina T.V.,** Lisachuk G.V. // Journal of Thermoelectricity. – 2020. – No. 4 – P. 5-13. http://jt.inst.cv.ua/jt/jt_2020_04_en.pdf 2. S. Buriakovskyi, B. Liubarskyi, A. Maslii, D. Pomazan, **T. Tavrina** Research of a hybrid diesel locomotive power plant based on a free-piston engine // Communications-Scientific Letters of the University of Zilina. – 2020. – V. 22 (3). – P. 103-109. DOI: 10.26552/com.C.2020.3.103-109 https://komunikacie.uniza.sk/pdfs/csl/2020/03/11.pdf 3. O. Rogacheva O. Vodoriz, **T. Tavrina** Mechanical and Thermoelectric Properties of PbSe1-xTex Solid Solutions // Proc. X Intern. Sci. and Practical Conf. "Electronics and Information Technologies" – 2018 - B-49-B-50, DOI: https://doi.org/10.30970/elit2018.B14 4. Y. Gutsalenko, C. Iancu, **T. Tavrina**, M. Rucki, A. Rudnev Environmental actuality, technological competitive environment and prediction of the prospects of anhydrous diamond-spark grinding using solid lubricants // Annals of the Constantin Brancusi̇ University of Targu Jiu, Engineering Series. – 2019 – N. 2. – P. 13-17. https://scholar.google.com/citations?view_op=view_citation&hl=uk&user=q1Qz2wgAAAAJ&sortby=pubdate&citation_for_view=q1Qz2wgAAAAJ:blknAaTinKkC

ПІБ викладача	Посада	Структурний підрозділ, у якому працює викладач	Інформація про кваліфікацію викладача	Стаж науково-педагогічної роботи	Навчальні дисципліни,що їх викладає викладач на ОП	Обґрунтування
						5. O.S. Vodoriz, **T.V. Tavrina,** G.O. Nikolaenko, O.I. Rogachova Mechanical and Thermoelectric Properties of $PbSe_{1-x}Te_x$ Semiconductor Solid Solutions // Metallophysics and Advanced Technologies.- 2020. – V. 42 (4) – P. 487-495. https://mfint.imp.kiev.ua/article/v42/i04/MFiNT.42.0487.pdf 6. O. Ovcharenko, **T. Tavrina**, N. Dyakonenko, O. Lyubchenko Computation of the parameters of single- and double-layer anti-reflective coatings for their effective use. - 2022 IEEE 3rd KhPI Week on Advanced Technology Conference Proceeding 2022, 724-728. DOI: 10.1109/KhPIWeek57572.2022.9916469 7. O. Rogacheva, O. Vodoriz, O. Nashchekina, **T. Tavrina**, Yu. Men'shov Effect of long-term aging on thermolectric properties of tin telluride based semiconductor solid solutions. - 2022 IEEE 3rd KhPI Week on Advanced Technology Conference Proceedings 2022, 921-924. DOI: 10.1109/KhPIWeek57572.2022.9916421 **П.3 Наявність виданого підручника чи навчального посібника:** О.А. Любченко, **Т.В. Тавріна,** О.С. Водоріз Навчальний посібник «Оптика, атомна і ядерна фізика» з грифом вченої ради НТУ «ХПІ» (http://repository.kpi.kharkov.ua/handle/KhPI-Press/54012, – Харків: НТУ «ХПІ», 2021.- 159 с. **П.4 наявність виданих навчально-методичних посібників:** 1. Электричество и магнетизм: учебно-метод. пособие по курсу «Общая физика» З.К. Ветчинкина, Е.А. Любченко, **Т.В.Таврина** – Харьков: НТУ «ХПИ», 2016. – 166 с. http://repository.kpi.kharkov.ua/handle/KhPI-Press/26422 2. Оптика. Атомная и ядерная физика: учебно-метод. пособие по курсу «Общая физика» З.К. Ветчинкина, Е.А. Любченко, **Т.В. Таврина** – Харьков: НТУ «ХПИ», 2016. – 300 с. http://repository.kpi.kharkov.ua/handle/KhPI-Press/26416 3. О.А. Любченко, О.С. Водоріз, **Т.В. Тавріна** Навчально-методичний посібник «Оптика, атомна і ядерна фізика: посібник з розв'язання задач», – Харків: НТУ «ХПІ», 2021. – 172 с. http://repository.kpi.kharkov.ua/handle/KhPI-Press/54001 **П. 8 Виконання функцій (повноважень, обов'язків) наукового керівника або відповідального виконавця наукової теми (проекту), або головного редактора/члена редакційної колегії/експерта (рецензента) наукового видання, включеного до переліку фахових видань України, або іноземного наукового видання, що індексується в бібліографічних базах;** 1. Рецензент наукових статей у виданні, включеному до переліку

ПІБ викладача	Посада	Структурний підрозділ, у якому працює викладач	Інформація про кваліфікацію викладача	Стаж науково-педагогічної роботи	Навчальні дисципліни,що їх викладає викладач на ОП	Обґрунтування
						наукових фахових видань України – Віснику НТУ «ХПІ». Серія: Нові рішення в сучасних технологіях 2. Рецензент наукових статей у виданні, включеному до базі SCOPUS – 2022 IEEE 3rd KhPI Week on Advanced Technology Conference Proceedings 2022. **П. 11 Наукове консультування підприємств, установ, організацій:** наукове консультування Приватного підприємства «ВЕЛЕС КОМ» за темою «Фізико-технологічні аспекти контроля якості запасних частин та приладів для ремонту моторних транспортних засобів». **П. 12 Наявність апробаційних та/або науково-популярних, та/або науково-експертиних публікацій з наукової тематики:** 1. **Тавріна Т.В.,** Водоріз О.С., Рогачова О.І. Температурні залежності гальваномагнітних властивостей напівпровідникових твердих розчинів PbSe1-xTex // XXVI Міжнародна науково-практична конференція «Інформаційні технології: наука, техніка, технологія, освіта, здоров'я». - ISSN 2222-2944. – 2018. – Ч. І. – С. 340. http://science.kpi.kharkov.ua/wp-content/uploads/2018/05/Tezisy_sbornik_part1_2018.pdf 2. Водоріз О.С., **Тавріна Т.В.,** Рогачова О.І. Теплопровідність напівпровідникових твердих розчинів PbSe-PbTe // XXVI Міжнародна науково-практична конференція «Інформаційні технології: наука, техніка, технологія, освіта, здоров'я». – ISSN 2222-2944. – 2018. – Ч. І. – Секц. 7. – С. 318. http://science.kpi.kharkov.ua/wp-content/uploads/2018/05/Tezisy_sbornik_part1_2018.pdf 3. Водоріз О.С., **Тавріна Т.В.,** Рогачова О.І. Вплив пресування на механічні та термоелектричні властивості твердих розчинів $PbSe_{1-x}Te_x$ // Тези доповідей. Функціональні матеріали для інноваційної енергетики – ФМІЕ-2019, Київ, Україна. – 13-15 травня 2019 р. – С. 21. 4. **Тавріна Т.В.,** Водоріз О.С. Вплив пресування і старіння на мікротвердість твердих розчинів $PbSe_{1-x}Te_x$ // XXVII Міжнародна науково-практична конференція "MicroCAD", 15 – 17 травня 2019: тези доповідей, т.1. – Харків: НТУ «ХПІ», 2019. – С. 362. http://science.kpi.kharkov.ua/wp-content/uploads/2019/05/Tezisy-sbornika-chast-1_2019.pdf 5. Vodoriz O.S., **Tavrina T.V.,** Rogachova O.I. Thermoelectric properties of $PbSe_{1-x}Te_x$ solid solutions // XVII International Conference of Physics and Technology of Thin Films and Nanosystems (ICPTTFN-XVII), Івано-Франківськ, Україна. – 20-25 травня 2019. – С. 337.

ПІБ викладача	Посада	Структурний підрозділ, у якому працює викладач	Інформація про кваліфікацію викладача	Стаж науково-педагогічної роботи	Навчальні дисципліни,що їх викладає викладач на ОП	Обґрунтування
						https://conference.pu.if.ua/phys_che/start/conference_17/zbirn_%202019_internet.pdf **П.13 Проведення навчальних занять із спеціальних дисциплін іноземною мовою:** читання лекцій, проведення практичних і лабораторних занять з курсу фізики для студентів, які навчаються за спеціальностями 123 і 172 у ННІ КМПФМ та 141 у ННІ ЕЕЕ. **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):** 1. Керівництво студентами, які зайняли призові місця у І етапі Всеукраїнської студентської олімпіади з фізики: студ. гр. КН-819 Нєнахова Ю.О. – 2 місце, 2020 р. 2. Керівництво студентами, які зайняли призові місця у І етапі Всеукраїнської студентської олімпіади з фізики та прийняли участь у ІІ етапі: ст. гр. КІТ-77 Гура Валерія – 2 місце, 2018 р. **П.19 Діяльність за спеціальністю у формі участі у професійних об'єднаннях:** Член International Association of Engineers (member number: 287372)
Городиська Ольга Миколаївна	доцент	кафедра філософії НТУ «ХПІ»	**Освіта:** Харківський національний університет, 1997. **Спеціальність** – Історія, **Кваліфікація** – історик, викладач суспільно-політичних дисциплін, ЛР ВЕ № 006040, 27.06.1997. **Канд. філос. н.**, 09.00.04 – філософська антропологія, філософія культури (033 –філософія) **Тема дисертації**: «Божевілля: культурно-символічні	25 роки	ЗП 5. Філософія	**Підвищення кваліфікації:** Підвищення кваліфікації – Харківський Національний педагогічний університет імені Г.С. Сковороди. **Тема:** «Комплексні проблеми в галузі професійної діяльності у сфері філософії», посвідчення про стажування № 07/23 – 101, **Термін навчання:** 2 міс. Наказ НТУ «ХПІ» № 876 С від 26 червня 2021 р. **Пункти відповідності ліцензійних умов:** **П.1, 3, 4, 10, 11, 12** **П.1. Наявність не менше п'яти публікацій у періодичних наукових виданнях, що включені до переліку фахових видань України, до наукометричних баз, зокрема Scopus, Web of Science Core Collection;** 1. **Horodyska O.** Care of the self as Limit-experience. *Вісник Харківського національного університету імені В.Н. Каразіна, серія «Теорія культури і філософія науки»*, випуск № 63, 2021. 2. Dolska, O., **Gorodiskaya, O**., & Tararoyev, J. (2020). Anthropological Dimension of Constructivism in the Culture of Presence. *Studia Warmińskie, 56,* 105-121. https://doi.org/10.31648/sw.4308

ПІБ викладача	Посада	Структурний підрозділ, у якому працює викладач	Інформація про кваліфікацію викладача	Стаж науково-педагогічної роботи	Навчальні дисципліни,що їх викладає викладач на ОП	Обґрунтування
			модуси»; диплом кандидата наук ДК №020946 від 12.11.2003. **Доцент** кафедри філософії, атестат доцента 12ДЦ № 016910 від 19.04.2007. Інститут післядипломної освіти Харківського національного педагогічного університету ім. Г.С. Сковороди, 2011. **Спеціальність** – Педагогіка та методика середньої освіти. Мова та література (Англійська), **Кваліфікація** – викладач англійської мови, 12ДСК № 186450, 24.06.2011.			(https://czasopisma.uwm.edu.pl/index.php/sw/article/view/4308) **(Web of Science)** 3. **Городиська О.М.** Антропологический кризис: в поисках стратеги преодоления. *Вісник Харківського національного університету імені В.Н. Каразіна, серія «Теорія культури і філософія науки»*, випуск № 60, 2019. С.15-26. 4. **Городиська О.М.** Масова людина та проблема психагогіки в умовах поглиблювання антропологічної кризи. *Вісник Національного університету «Юридична академія України імені Ярослава Мудрого». Серія: Філософія, філософія права, політологія, соціологія*. Вип. 3 (38). Харків, 2018. С. 144–154. 5. **Городиська О.М.** Проблема человеческой самости в современном мире. *"VERSUS" : Науково-теоретичний часопис ; Мелітопольський державний педагогічний університет ім. Б. Хмельницького*. 2017. № 1 (9). С. 36–40. **П.3. Наявність виданого підручника чи навчального посібника (включаючи електронні) або монографії (загальним обсягом не менше** **5 авторських аркушів), в тому числі видані у співавторстві (обсягом не менше 1,5 авторського аркуша на кожного співавтора);** 1. Дольська О. О., Годзь Н.Б., **Городиська О.М.**, Дишкант Т.М., Тагліна Ю.С. Багатовимірність людини та культури у сучасних філософських ландшафтах. Монографія. Харків: 2021. 170 с. 1,6 а.а. 2. Человек в современном мире: на пути к новой парадигме образования : монография / О.А. Дольська, А.В. Голозубов, **Городиська О.М.**. Харків: НТУ «ХПІ», 2016. 216 с. 2 а.а. **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. **Городиська О.М.** Антична філософія, Середньовічна філософія, Антропологія (філософська). *Філософія: терміни і поняття: Навчальний енциклопедичний словник* / Під редакцією В.Л. Петрушенка. Львів: «Новий Світ-2000», 2020. 520 с. 2. Вступ до філософії : навч.-метод. посіб. / Владленова І.В.; Годзь Н.Б.; **Городиська О.М.** та ін.; за ред. Городиської, О.М.; Дольської О.О. Х.: НТУ «ХПІ», 2018. 185 с.

ПІБ викладача	Посада	Структурний підрозділ, у якому працює викладач	Інформація про кваліфікацію викладача	Стаж науково-педагогічної роботи	Навчальні дисципліни,що їх викладає викладач на ОП	Обґрунтування
						3. **Городиська О.М.** Філософія античності: Текст лекції по курсу «Філософія» для аспирантів и студентів всіх спеціальностей и форм навчання Х.: НТУ «ХПИ», 2018. 46 с. (электроний ресурс). **П.10. Участь у міжнародних наукових та/або освітніх проектах, залучення до міжнародної експертизи, наявність звання "суддя міжнародної категорії":** 1. Участь у міжнародному проекті: Why Is Ukraine a Democracy? TCUP Conference. Ukrainian Research Institute, Harvard University (H/URI), February, 1–5, 2021. 2. Участь у міжнародному польсько-українському науковому проекті із досліджень роботи Львівсько-Варшавської школи. Філософські майстер-класи. Центр досліджень традиції Львівсько-Варшавської школи. Львівське філософське товариство ім. Казимира Твардовського. Варшава, 11-14 лютого, 2021. **П.11. Наукове консультування підприємств, установ, організацій не менше трьох років, що здійснювалося на підставі договору із закладом вищої освіти (науковою установою);** Наукове консультування та співпраця з громадською організацією «Харківський науково-дослідний інститут козацтва» та Академією військово-історичних наук і козацтва (на підставі договору 25/236-2019, терміном 2018-2023 р.р.). **П.12. Наявність апробаційних та/або науково-популярних, та/або консультаційних (дорадчих), та/або науково-експертних публікацій з наукової або професійної тематики загальною кількістю не менше п'яти публікацій;** 1. **Horodyska O.M.** Searching for the self: human as limit. Матеріали X міжнародної наукової конференції «Антропологічні виміри філософських досліджень». 21 апреля 2021. Дніпро. http://conf-ampr.diit.edu.ua/AMPRX/paper/view/23713/12874 http://conf-ampr.diit.edu.ua/AMPRX/schedConf/presentations 2. **Городиська О**. Зв'язок «вчитель-учень»: минуле й сьогодення. Освіта і людина: сучасні виклики та актуальні практики: матеріали Міжнародного науково-практичного семінару 26 лютого 2021 р. / Ред. кол. О.О. Дольська, А.В. Кіпенський, Я.В. Тараоєв та ін. – Харків : НТУ «ХПІ», 2021. – С. 39-41. – укр., англ. мовами. Електронний ресурс, режим доступу : http://repository.kpi.kharkov.ua/handle/KhPI-Press/51167 3. **Городиська О.М.** Governmentality як принцип управління та самоуправління суб'єкту. Матеріали всеукраїнської науково-практичної конференції «Інноваційні технології публічного

ПІБ викладача	Посада	Структурний підрозділ, у якому працює викладач	Інформація про кваліфікацію викладача	Стаж науково-педагогічної роботи	Навчальні дисципліни,що їх викладає викладач на ОП	Обгрунтування
						управління та адміністрування: теорія і кращі практики 21 століття» (17 жовтня 2020 року). Мелітополь, 2020. С. 6-8. 4. **Horodyska O.** Limit-experience and freedom. Матеріали I міжнародної науково-практичної конференції «Філософія у сучасному світі». Харків, 2020. С. 89-91. 5. **Городиська О.М.** Психагогика и «забота о себе» как практики жизни в современном мире. Theory and Practice: Problems and Prospects. Scientific articles. Scientific articles. Kaunas, Lithuania. 2020. p. 236-243. http://dspace.lsu.lt/handle/123456789/78 6. **Городиська О.М.** Трансформации способа бытия человека как преодоление антропологического кризиса. International Scientific-practical Conference. Theory and Practice: Problems and Prospects. Book of abstracts. 21st –22nd of May, 2020, Marijampole and Kaunas, Lithuania. p. 39. http://dspace.lsu.lt/bitstream/handle/123456789/77/BOOK%20OF%20ABSTRACTS_Galutinis_Patikslintas.pdf?sequence=1&isAllowed=y 7. **Городиська О.М.** Антропологічна катастрофа та формування техно-людини. Інформаційні технології: наука, техніка, технологія, освіта, здоров'я. Тези доповідей XX IV Міжнародної науково-практичної конференції (травень 2019 р., Харків). Харків, НТУ «ХПІ», 2019. Ч. IV. С. 252. 8. **Городиська О.М.** Экстропия как философия будущего человека. International Scientific-practical Conference Theory and Practice: Problems and Prospects. Book of abstracts. 2019 May 9–10th, Kaunas. – p. 22. http://dspace.lsu.lt/handle/123456789/62 **П.13. Проведення навчальних занять із спеціальних дисциплін іноземною мовою (крім дисциплін мовної підготовки) в обсязі не менше 50 аудиторних годин на навчальний рік:** «Філософія» (англ.) – 128
Іглін Сергій Петрович	професор	кафедра комп'ютерної математики і аналізу даних НТУ «ХПІ»	Харківський політехнічний інститут, 1976р., **Спеціальність** "Динаміка та міцність машин", **Кваліфікація** інженер-механік-дослідник	45 роки	ЗП 6. Вища математика	**Підвищення кваліфікації:** 1. Інститут проблем машинобудування ім.А.М.Підгорного НАН України, з 01.11.2018 по 31.01.2019, Звіт про проходження довгострокового підвищення кваліфікації, **Тема:**"Застосування математичного пакету MATLAB для розв'язання задач математичної фізики", 11.03.2019, **Термін навчання:** 3 місяці. 2. Підвищення кваліфікації в Університеті у Бєльсько-Бялій на кафедрі інформатики та автоматики (м. Бєльсько-Бяла, Польща), з 10 жовтня по 20 грудня 2022 р. **Термін навчання:** 2,3 місяця (6 кредитів ЄКТС – 180 академічних

ПІБ викладача	Посада	Структурний підрозділ, у якому працює викладач	Інформація про кваліфікацію викладача	Стаж науково-педагогічної роботи	Навчальні дисципліни,що їх викладає викладач на ОП	Обґрунтування
						годин). Наказ: 273С від 28.02.2023р. Сертфікат № К18/36-12-20/2022 від 20.12.2022 р. 3. Стажування – участь у XXX міжнародній науково-практичній конференції **Тема:** «Інформаційні технології: наука, техніка, технологія, освіта, здоров'я» (MicroCAD-2022), секція 9.2 «Комп'ютерне та математичне моделювання. Системний аналіз і управління проектами» **Термін навчання:** з 19.10.2022 р. по 21.10.2022 р. в обсязі 15 годин (0,5 кредитів ЄКТС). Наказ НТУ «ХПІ»: ПК № 27С від 13.01.2023р. **Пункти відповідності ліцензійних умов:** **П.1, 4, 11, 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;** **Scopus:** 1. I.Khomenko, I.Stasiuk, S.Iglin. On the Influence of Electromagnetic Processes of Power Transformer on Parameters of Normal Regime of Electric Network Operation. - 2018 IEEE 3rd International Conference on Intelligent Energy and Power Systems (IEPS), September 10-14, 2018, Kharkiv, Ukraine. p.248-252. ISBN 978-1-5386-9546-3 У фахових виданнях: 2. Бухкало С.І., Іглін С.П., Ольховська О.І. Можливості розвитку компетентностей комплексних екологічнобезпечних проектів утилізації-модифікації. - Вісник НТУ "ХПІ", вип. 18 (1294), 2018. с.3-9. ISSN 2220-4784. 3. Іглін С.П., Дмитрик В.В., Скульський В.Ю. Моделювання руху рідкого металу в зварювальній ванні. - Електронне моделювання. 2020. Том 42, № 1. с.51-71. ISSN 0204-3572 4. Дмитрик В.В., Глушко А.В., Іглін С.П. Структурні зміни металу зварних з'єднань тривало експлуатованих паропроводів. - Автоматичне зварювання. 2020. № 2. с.24-28. ISSN 0005-111X 5. Коваленко В.О., Стрижак В.В., Іглін С.П., Коваленко О.О., Стрижак М.Г. Динамічні характеристики пуску механізму повороту крану з частотно-регульованим приводом. - Технічний сервіс агропромислового, лісового та транспортного комплексів, 2020, №21. с.201-210. DOI 10.37700/ts.2020.21.201-210 6. Коваленко В.О., Стрижак В.В., Іглін С.П., Коваленко О.О., Стрижак

ПІБ викладача	Посада	Структурний підрозділ, у якому працює викладач	Інформація про кваліфікацію викладача	Стаж науково-педагогічної роботи	Навчальні дисципліни,що їх викладає викладач на ОП	Обгрунтування
						М.Г. Динамічні характеристики роботи механізму повороту крану на колоні. - Підйомно-транспортна техніка, 2021, №2(66). с.80-100. DOI 10.15276/pidtt.2.66.2021 **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 (не менш ніж 50 лекцій на Youtube);** повний список на сторінці http://www.iglin.epizy.com/openlectures.html **П.11 наукове консультування підприємств, установ, організацій не менше трьох років, що здійснювалося на підставі договору із закладом вищої освіти (науковою установою).** Наукове консультування ТОВ «Клауд Воркс» за темою «Математичне моделювання процесів при розробці омніканальної ритейл-платформи» (договір № 99/332-2021 від 22.04.2021 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. Бухкало С.І., Іглін С.П., Соловей В.М., Ольховська О.І., Головченко Г.М., Машталер К.К., Гуцул К.В., Носальська Л.К., Мочалов О.Ю. Складові розрахунку параметрів очищення стічних вод комплексних підприємств. - XXVI Міжнародна науково-практична конференція «Інформаційні технології: наука, техніка, технологія, освіта, здоров'я» (MicroCAD-2018) 16-18 травня 2018, частина 2, с. 202. ISSN 2222-2944. http://science.kpi.kharkov.ua/wp-content/uploads/2018/05/Tezisy_sbornik_part2_2018.pdf 2. Бухкало С.І., Іглін С.П., Соловей В.М., Ольховська О.І. Деякі особливості розрахунку параметрів ефективного очищення стічних вод комплексних підприємств. - XXVI Міжнародна науково-практична конференція «Інформаційні технології: наука, техніка, технологія, освіта, здоров'я» (MicroCAD-2018) 16-18 травня 2018, частина 2, с. 203. ISSN 2222-2944. http://science.kpi.kharkov.ua/wp-content/uploads/2018/05/Tezisy_sbornik_part2_2018.pdf 3. Бухкало С.І., Іглін С.П., Соловей В.М., Ольховська О.І., Головченко Г.М., Машталер К.К., Гуцул К.В., Мочалов О.Ю., Носальська Л.К., Дудкіна Є.В. Алгоритм управління ефективним очищенням стічних

ПІБ викладача	Посада	Структурний підрозділ, у якому працює викладач	Інформація про кваліфікацію викладача	Стаж науково-педагогічної роботи	Навчальні дисципліни,що їх викладає викладач на ОП	Обґрунтування
						вод комплексних підприємств. - XXVI Міжнародна науково-практична конференція «Інформаційні технології: наука, техніка, технологія, освіта, здоров'я» (MicroCAD-2018) 16-18 травня 2018, частина 2, с. 204. ISSN 2222-2944. http://science.kpi.kharkov.ua/wp-content/uploads/2018/05/Tezisy_sbornik_part2_2018.pdf 4. Бухкало С.І., Іглін С.П., Ольховська О.І., Рогозіна М.А., Скляр В.В., Фролова І.Р. Деякі закономірності процесів кристалізації цукру. - XXVI Міжнародна науково-практична конференція «Інформаційні технології: наука, техніка, технологія, освіта, здоров'я» (MicroCAD-2018) 16-18 травня 2018, частина 2, с. 207. ISSN 2222-2944. http://science.kpi.kharkov.ua/wp-content/uploads/2018/05/Tezisy_sbornik_part2_2018.pdf 5. Бухкало С.І., Іглін С.П., Ольховська О.І., Рогозіна М.А. Особливості управління розробками об'єктів інтелектуальної власності зі студентами. - XXVI Міжнародна науково-практична конференція «Інформаційні технології: наука, техніка, технологія, освіта, здоров'я» (MicroCAD-2018) 16-18 травня 2018, частина 2, с. 208. ISSN 2222-2944. http://science.kpi.kharkov.ua/wp-content/uploads/2018/05/Tezisy_sbornik_part2_2018.pdf 6. Бухкало С.І., Іглін С.П., Ольховська О.І., Мочалов О.Ю. Особливості інформаційного простору об'єктів інтелектуальної власності. - XXVI Міжнародна науково-практична конференція «Інформаційні технології: наука, техніка, технологія, освіта, здоров'я» (MicroCAD-2018) 16-18 травня 2018, частина 2, с. 209. ISSN 2222-2944. http://science.kpi.kharkov.ua/wp-content/uploads/2018/05/Tezisy_sbornik_part2_2018.pdf **П.19 діяльність за спеціальністю у формі участі у професійних та/або громадських об'єднаннях** Європейська федерація хімічної інженерії EFCE, український філіал EFC-UA
Арабаджи Тимур Дмитрович	доцент	кафедра фізичного виховання НТУ «ХПІ»	Національний технічний університет «Харківський політехнічний інститут», 2004 р. **Спеціальність** «Фізичне виховання», **Кваліфікація** «Викладач фізичного	16 років	ЗП Фізичне виховання	**Пункти відповідності ліцензійних умов:** **П. 1, 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. Journal of Physical Education and Sport. – Electronic text data. – 2020. – Vol. 20, iss. 3. –P. 1606-1612. – [Electronic resource]. Access mode: https://efsupit.ro/images/stories/mai2020/Art%20219.pdf http://repository.kpi.kharkov.ua/bitstream/KhPI-

ПІБ викладача	Посада	Структурний підрозділ, у якому працює викладач	Інформація про кваліфікацію викладача	Стаж науково-педагогічної роботи	Навчальні дисципліни,що їх викладає викладач на ОП	Обґрунтування
			виховання», «Інженер-менеджер спорту» (диплом ХА №23668471). Національний технічний університет «Харківський політехнічний інститут», 2007 р. **Спеціальність** «Фізичне виховання», **Кваліфікація** «Викладач фізичного виховання», «Інженер-дослідник спорту» (диплом ХА №32899565), 2007 р. Національний технічний університет «Харківський політехнічний інститут», 2014 р. **Спеціальність** «Педагогіка вищої школи», **Кваліфікація** «Викладач вищих навчальних закладів» (диплом ХА №47370392). **Кандидат педагогічних наук**, 13.00.04 – «Теорія та методика професійної освіти» (диплом ДК № 043551), від 26.06.2017.			Press/47111/1/JPES_2020_20_3_Rochniak_Effect_of_young.pdf 2. Арабаджи Т.Д. Лідерські якості спортсменів як складова їх готовності до професійного самовизначення після завершення спортивної кар'єри / А. О. Тіняков, Т. Д. Арабаджи //Теорія і практика управління соціальними системами: філософія, психологія, педагогіка, соціологія. – Харків, 2019. – № 2. – С. 67-80. http://repository.kpi.kharkov.ua/bitstream/KhPI-Press/43672/1/TIPUSS_2019_4_Tiniakov_Liderski.pdf 3. Арабаджи Т.Д. Технології організації занять з фізичного виховання з використанням інформаційно-комунікаційних технологій для врахування динаміки пульсометрії / А. Ю. Арабаджи, Г. М. Тимченко, Т. Д. Арабаджи // Вісник Національного університету "Чернігівський колегіум" імені Т.Г. Шевченка. Серія: Педагогічні науки. – Чернігів: НУЧК імені Т.Г. Шевченка, 2020. – Вип. 7 (163). – С. 81-86. https://visnyk.chnpu.edu.ua/20-7-163-14/ 4. Арабаджи Т. Д. Оцінка спеціальної фізичної підготовленості студентів, які займаються армспортом у загальних групах з фізичного виховання / Т. Д. Арабаджи, А. Ю. Арабаджи, В. В. Фоменко // Науковий часопис Національного педагогічного університету ім. М. П. Драгоманова. Сер. 15 : Науково-педагогічні проблеми фізичної культури (фізична культура і спорт) : зб. наук. пр. – Київ : НПУ, 2022. – Вип. 3К (147). – С. 30-33. https://drive.google.com/file/d/1ISzM-5Ot5GHtUwoiZNhXs1GPMBH1FgmO/view 5. Арабаджи Т.Д. Організація навчального процесу з фізичного виховання студентів зі спеціалізації «баскетбол» в умовах військового стану з використанням інформаційно-комунікаційних технологій / Т. Д. Арабаджи, А. Ю. Арабаджи, Б. Д. Жиров // Науковий часопис Національного педагогічного університету ім. М. П. Драгоманова. Сер. 15 : Науково-педагогічні проблеми фізичної культури (фізична культура і спорт) : зб. наук. пр. – Київ : НПУ, 2023 (віддано до друку) **П.4 Наявність виданих навчально-методичних посібників/посібників для самостійної роботи здобувачів вищої освіти та дистанційного навчання, електронних курсів на освітніх платформах ліцензіатів, конспектів лекцій/практикумів/методичних вказівок/рекомендацій/ робочих програм, інших друкованих навчально-методичних праць загальною кількістю три найменування;** 1. Методичні вказівки до практичних занять з фізичного виховання за спеціалізацією «Баскетбол», розділ «Профілактично-реабілітаційні

ПІБ викладача	Посада	Структурний підрозділ, у якому працює викладач	Інформація про кваліфікацію викладача	Стаж науково-педагогічної роботи	Навчальні дисципліни,що їх викладає викладач на ОП	Обґрунтування
			Тема дисертації: «Формування готовності до професійного самовизначення спортсменів після закінчення спортивної кар'єри». диплом ДК № 043551 від 26.06.2017, МОН України. **Доцент** кафедри «Фізичного виховання» АД № 007466 від 15.04.2021			заходи при остеохондрозі» для студентів усіх спеціальностей денної та дистанційної форми навчання / уклад. Т. Д. Арабаджи, А. Ю. Арабаджи, Т. Є. Федорина, Н. А. Матузна – Харків: НТУ «ХПІ», 2020. – 29 с. http://library.kpi.kharkov.ua/TUF/prohramy_2020_Osteokhondroz.pdf#7s8d6f87 2. «Легка атлетика» для студентів спеціалізації легка атлетика, для самостійної роботи та дистанційного навчання. Конспект лекцій / Т. Д. Арабаджи, А. Ю. Арабаджи, Т. Є. Федорина, Н. А. Матузна, В. О. Шаповалова – Харків: НТУ «ХПІ» 2020. – 87 с. http://library.kpi.kharkov.ua/TUF/prohramy_2020_Lehka_atletyka.pdf 3. «Баскетбол» для студентів спеціалізації баскетбол, для самостійної роботи та дистанційного навчання. Конспект лекцій / Т.Д. Арабаджи, А.Ю. Арабаджи, С.Б. Храпов, Т. Є. Федорина, Н. А. Матузна – Харків: НТУ «ХПІ» 2020. – 93 с. http://library.kpi.kharkov.ua/TUF/prohramy_2020_Fizychne_vykhovannia.pdf **П.8 Виконання функцій (повноважень, обов'язків) наукового керівника або відповідального виконавця наукової теми (проекту), або головного редактора/члена редакційної колегії/експерта (рецензента) наукового видання, включеного до переліку фахових видань України, або іноземного наукового видання, що індексується в бібліографічних базах:** 1. «Розробка методології розвитку лідерського потенціалу національної гуманітарно-технічної та управлінської еліти в інформаційному суспільстві» (державний номер реєстрації 0115U000520); 2. «Формування готовності у спортсменів до самовизначення після закінчення спортивної кар'єри» (державний номер реєстрації 0117U004895). **П.10 Участь у міжнародних наукових та/або освітніх проектах, залучення до міжнародної експертизи, наявність звання "суддя міжнародної категорії";** В 2019 році здобувач брав участь у міжнародному стажуванні – конференціях та семінарах: - «The problem of modern European basketball» 03 серпня у м. Сольнок, Угорщина, на базі International Basketball Federation (FIBA) (підтверджено відповідною довідкою); - «Basketball clinic about innovation in basketball 3x3» 29 серпня у м. Дебрецен, Угорщина, на базі International Basketball Federation (FIBA)

ПІБ викладача	Посада	Структурний підрозділ, у якому працює викладач	Інформація про кваліфікацію викладача	Стаж науково-педагогічної роботи	Навчальні дисципліни,що їх викладає викладач на ОП	Обґрунтування
						(підтверджено відповідною довідкою); - «Improvement of the system of holding international competitions» 14 вересня у м. Будапешт, Угорщина, на базі International Basketball Federation (FIBA) (підтверджено відповідною довідкою); - «Progressive trends in the development of basketball in the world» 05 жовтня у м. Ланьчжоу, Китай, на базі International Basketball Federation (FIBA) (підтверджено відповідною довідкою). **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. Арабаджи Т.Д. Технології організації занять з фізичного виховання з використанням інформаційно-комунікаційних технологій для врахування динаміки пульсометрії / А. Арабаджи, Г. Тимченко, Т. Арабаджи // Сучасні проблеми підготовки та професійного удосконалення працівників сфери освіти : тези доповідей – Черкаси : Чабаненко Ю. А., 2020. – С. 7-8. 2. Арабаджи Т.Д. Лідерські якості провідних гравців у баскетболі 3х3 / Т. Арабаджи // Лідери XXI століття. Формування особистості харизматичного лідера на основі гуманітарних технологій для управління соціальними системами : тези доповідей – Харків: НТУ «ХПІ», 2020. 3. Арабаджи Т.Д. Тренувальний процесс професійної баскетбольної команди в умовах пандемії covid-19 / А. Арабаджи // Перспективи, проблеми та наявні здобутки розвитку фізичної культури і спорту в Україні : тези доповідей – Віннецький державний педагогічний університет ім. Михайло Коцюбинського, 2021. – С. 186-189. 4. Арабаджи Т.Д. Оцінка спеціальної фізичної підготовленості студентів, які займаються армспортом у загальних групах з фізичного виховання / XIII Міжнародна науково-практична конференція. Сучасні проблеми та перспективи розвитку іфзичного виховання, здоров'я і професійної підготовки майбутніх фахівців з фізичної культури та спорту – Київ: 24-25 березня 2022 року. 5. Арабаджи Т.Д. Організація навчального процесу з фізичного виховання студентів зі спеціалізації «баскетбол» в умовах військового стану з використанням інформаційно-комунікаційних технологій / XIV Міжнародна науково-практична конференція. Сучасні проблеми та перспективи розвитку іфзичного виховання, здоров'я і професійної підготовки майбутніх фахівців з фізичної культури та спорту – Київ: 23-24 березня 2023 року. (віддано до друку)

ПІБ викладача	Посада	Структурний підрозділ, у якому працює викладач	Інформація про кваліфікацію викладача	Стаж науково-педагогічної роботи	Навчальні дисципліни,що їх викладає викладач на ОП	Обґрунтування
						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. Тренер Молодіжної Національної збірної команди України з баскетболу 3х3 (з 2018 року по теперішній час) 2. Тренер Національної чоловічої збірної команди України з баскетболу 3х3 (з 2022 року по теперішній час) 3. Керівництво студентом, який став призером Молодіжного Чемпіонату Світу з баскетболу 3х3 (2-6 жовтня 2019 р., м. Лоньчжоу, Китай, Антон Мусієнко) 4. Керівництво студентом, який став переможцем Національного Чемпіонату України з баскетболу серед чоловіків у Першій лізі (сезон 2021/2022, Максим Фоменко) 5. Керівництво студентом, який став переможцем Національного Чемпіонату України з баскетболу серед чоловіків у Першій лізі (сезон 2021/2022, Ярослав Пивовар)

ПІБ викладача	Посада	Структурний підрозділ, у якому працює викладач	Інформація про кваліфікацію викладача	Стаж науково-педагогічної роботи	Навчальні дисципліни,що їх викладає викладач на ОП	Обґрунтування
						6. Керівництво студентом, який став переможцем Національного Чемпіонату України з баскетболу серед чоловіків у Першій лізі (сезон 2021/2022, Ілля Солошенко) 7. Керівництво студентом, який став переможцем Національного Чемпіонату України з баскетболу серед чоловіків у Першій лізі (сезон 2021/2022, Богдан Різниченко) 8. Керівництво студентом, який став переможцем Національного Чемпіонату України з баскетболу серед чоловіків у Першій лізі (сезон 2021/2022, Рафаїл Хрисостоміді) 9. Керівництво студентом, який став переможцем Національного Чемпіонату України з баскетболу серед чоловіків у Першій лізі (сезон 2021/2022, Богдан Каленик) 10. Керівництво студентом, який став переможцем Національного Чемпіонату України з баскетболу серед чоловіків у Першій лізі (сезон 2021/2022, Владислав Білошенко) **П.19 Діяльність за спеціальністю у формі участі у професійних та/або громадських об'єднаннях:** 1. Член Федерації баскетболу України з 1997 року по теперішній час. 2. Член Федерації баскетболу Харківської області з 2002 року по теперішній час. 3. Член Президії Федерації баскетболу Харківської області з 2021 року по теперішній час. **П.20 досвід практичної роботи за спеціальністю не менше п'яти років (крім педагогічної, науково-педагогічної, наукової діяльності):** 1. Робота в Федерації баскетбола України тренером Молодіжної Національної збірної команди України з баскетболу 3х3 (з 11.12.2018 року по теперішній час). 2. Робота в Федерації баскетбола України тренером Національної чоловічої збірної команди України з баскетболу 3х3 (з 08.04.2022 року по теперішній час).
Поляков Ігор Олександрович	доцент	кафедра фізичного виховання НТУ «ХПІ»	1.Університет цивільного захисту України, 2007р. **Спеціальність:** "Пожежна безпека" **Кваліфікація:** "інженер з профілактичних робіт"	17 років	ЗП Фізичне виховання	**Підвищення кваліфікації:** Харківський національний педагогічний університет ім. Г.С. Сковороди на кафедрі фізичного виховання **Термін навчання:** з 30 листопада по 26 лютого 2021 р. Посвідчення №07/23-62 **Пункти відповідності ліцензійних умов:** **П. 1, 3, 4, 12, 14, 19.** **П.1 наявність не менше п'яти публікацій у періодичних наукових виданнях, що включені до переліку фахових видань України, до**

ПІБ викладача	Посада	Структурний підрозділ, у якому працює викладач	Інформація про кваліфікацію викладача	Стаж науково-педагогічної роботи	Навчальні дисципліни,що їх викладає викладач на ОП	Обґрунтування
			Диплом ХА №31346972 2. Харківська державна академія фізичної культури, 2008р. **Спеціальність:** “Олімпійський та професійний спорт” **Кваліфікація:** **“**Олімпійський та професійний спорт та психологія спорту” Диплом ХА№35223082 **Кандидат психологічних наук,** 19.00.09 - Психологія діяльності в особливих умовах **Тема:** “Професіографічний аналіз діяльності рятувальників ДСАПСПРТ МНС України” Диплом ДК №003062 **Старший науковий співробітник** зі спеціальності Психологія діяльності в особливих умовах Диплом АС № 000614			**наукометричних баз, зокрема Scopus, Web of Science Core Collection:** 1. Поляков І.О. Стрес-фактори змагальної діяльності як детермінанти помилкових дій у спортивній боротьбі / Поляков І.О., Курій О.В. // Scientific Journal Virtus, December #18, Canada, Monreal, 2018. p. 61-68. 2. Поляков І.О. Модельні характеристики та спортивно значущі якості у спортивній боротьбі / Поляков І.О., Грдзелідзе С.Р. // Scientific Journal Virtus, November #22, Canada, Monreal, 2019. p. 59-64. 3. Поляков І.О., Полякова О.О., Лотвінов О.В. Харківська школа екстремальної психології: історія становлення та розвитку / Проблеми екстремальної та кризової психології. Зб. наук. праць. Вип. 29. – Х.: НУЦЗУ, 2020. – С.76-88 4. Поляков І. О. Особливості планування навчально-тренувального процесу борців-вільників високої кваліфікації / І. О. Поляков // Вісник Національного технічного університету "ХПІ". Сер. : Актуальні проблеми розвитку українського суспільства = Bulletin of the National Technical University "KhPI". Ser. : Actual problems of Ukrainian society development : зб. наук. пр. – Харків : НТУ "ХПІ", 2021. – № 2. – С. 112-117. http://repository.kpi.kharkov.ua/bitstream/KhPI-Press/57126/1/visnyk_KhPI_2021_2_APRUS_Poliakov_Osoblyvosti.pdf 5. Поляков І. О. Теоретичні аспекти формування психофізичної готовності військовослужбовців підрозділів спеціального призначення до виконання стрибка з парашутом / В. В. Халеп, М. Г. Саморок, Марек Грачик, І. О. Поляков, С. Р. Грдзелідзе, В. В. Пастернацький // Науковий часопис Національного педагогічного університету імені М. П. Драгоманова. Серія 15 : Науково-педагогічні проблеми фізичної культури (фізична культура і спорт) : зб. наук. праць. – Київ : Вид-во НПУ імені М. П. Драгоманова, 2021. – Вип. 12 (144). – С. 163-169. – DOI 10.31392/NPU-nc.series15.2021.12(144).33 http://enpuir.npu.edu.ua/bitstream/handle/123456789/36342/Khalep%20V.pdf?sequence=1&isAllowed=y 6. Поляков І. О. Сутність та структура формування готовності тренерів з одноборств до побудови раціональних тактичних схем / І.О. Поляков, М.Б. Гуска, В.Й. Мазур, І.О. Романенко, Л.І. Мачковська // Науковий часопис Національного педагогічного університету імені М. П. Драгоманова. Серія 5 : Науково-педагогічні проблеми фізичної культури (фізична культура і спорт) : зб. наук. праць. – Київ : Вид-во

ПІБ викладача	Посада	Структурний підрозділ, у якому працює викладач	Інформація про кваліфікацію викладача	Стаж науково-педагогічної роботи	Навчальні дисципліни,що їх викладає викладач на ОП	Обгрунтування
						НПУ імені М. П. Драгоманова, 2022. – Вип. 87 (133). – С. 77-82. – DOI 10.31392/NPU-nc.series5.2022.87.16 http://www.chasopys.ps.npu.kiev.ua/archive/87/16.pdf 7. 7. Поляков І. О. Факторна структура фізичної підготовленості борців вільного стилю на етапі початкової підготовки / А. С. Євтифієв, С. В. Бочкарев, І. О. Поляков, І. І. Євтифієва, Ю. Г. Донець, // Фізичне виховання та спорт. Одеса: Видавничий дім «Гельветика», 2022. – № 4. – С. 43-49. http://journalsofznu.zp.ua/index.php/sport/issue/view/155 8. **Web of Science Core Collection:** Poliakov, I. Practices for readiness of future specialists for professional self- determination in the information society / Knysh, I., Dubinka, M., Kochubei, O., Poliakov, I., Tiahur, V. // (2022).. Amazonia Investiga, 11(59), 108-118. https://doi.org/10.34069/AI/2022.59.11.10 https://amazoniainvestiga.info/index.php/amazonia/article/view/2196/3074 **П.3 наявність виданого підручника чи навчального посібника (включаючи електронні) або монографії (загальним обсягом не менше 5 авторських аркушів), в тому числі видані у співавторстві (обсягом не менше 1,5 авторського аркуша на кожного співавтора):** 1. The Role of Science in Society sustaible Development. / Poliakov I. and other.- Katowice: Katowice School of Techology: monografy. – K.: 2020. – 243 c. http://repository.kpi.kharkov.ua/handle/KhPI-Press/56604 **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. Психологія фізичної активності та спорту: курс лекцій / уклад. Поляков І.О.: Нац. техн. ун-т "Харків. політехн. ін-т". – Харків : НТУ "ХПІ", 2018. – 165 с. 2. Поляков І.О., Полякова О.О. Основи PR: курс лекцій. – НУЦЗУ. – 2019. – 119с. **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:**

ПІБ викладача	Посада	Структурний підрозділ, у якому працює викладач	Інформація про кваліфікацію викладача	Стаж науково-педагогічної роботи	Навчальні дисципліни,що їх викладає викладач на ОП	Обґрунтування
						1. Поляков І.О. Популяризація і пр-технології в спорті // І Міжнародна науково-практична конференція «Здоров'я нації і вдосконалення фізкультурноспортивної освіти», 3–4 жовтня 2019р. / за ред. проф. Кіпенського А.В.. – Харків: НТУ «ХПІ» http://repository.kpi.kharkov.ua/bitstream/KhPI-Press/42462/1/Conference_NTU_KhPI_2019_Zdorovia_natsii.pdf 2. Поляков І.О. Використання ПР-технологій сучастості у спортивній боротьбі «Фізична культура і спорт» // ІІІ Всеукраїнська науково-практична інтернет конференція «Науково-методичні основи використання інформаційних технологій в галузі фізичної культури та спорту» збірник наукових праць [Електронний ресурс]. – Харків : ХДАФК, 2019. – 143 с 3. Поляков І.О. PR-технології у сучасній спортивній боротьбі // Науково-практична конференція, «Лідери XXI століття. Формування особистості харизматичного лідера на основі гуманітарних технологій для управління соціальними системами», Харків, 29-30 жовтня 2020р. / за ред. проф. Сокола Є.І. – Харків: НТУ «ХПІ» http://repository.kpi.kharkov.ua/bitstream/KhPI-Press/51175/1/Conference_NTU_KhPI_2020_Lidery_XXI_stolittia.pdf 4. Поляков І.О., Полякова О.О., Керимов К.Е. Новітні тенденції у навчально-тренувальному процесі борців високої кваліфікації // Збірник тез за результатами Всеукраїнської науково-практичної конференці «Традиції та новації університетської науки в часі та просторі культури». –Х: НУЦЗУ, 2021. - С. 39-41. https://nuczu.edu.ua/images/topmenu/science/konferentsii/2021/9.pdf 5. Поляков І.О., Полякова О.О. Динаміка показників рівня розвитку швидкісно-силових здібностей у борців-юніорів під впливом розробленої програми навчально-тренувальних зборів // Актуальні проблеми фізичного виховання різних верств населення. - Х.:ХДАФК, 2022. - С. 29-37. https://drive.google.com/drive/folders/1NRGYYCzVgTB50uYDYAnmLQU0-so-oeEV 6. Полякова О.О., Поляков І.О. Війна як форма маніфестації Numen // Збірник тез за результатами Всеукраїнської науково-практичної конференці «Трансформаційні процеси в умовах війни та післявоєнного періоду». – Чернігів, 2022. - С. 42-43. https://reicst.com.ua/asp/issue/view/conf_mult_06_2022/conf_mult_06_2022 7. Полякова О.О., Поляков І.О. Портрет сучасного українського педагога: філософське осмислення // Збірник тез за результатами

ПІБ викладача	Посада	Структурний підрозділ, у якому працює викладач	Інформація про кваліфікацію викладача	Стаж науково-педагогічної роботи	Навчальні дисципліни,що їх викладає викладач на ОП	Обґрунтування
						Міжнародної науково-практичної конференції «Філософія в сучасному світі» НТУ "ХПІ". – Харків, 2022. http://repository.kpi.kharkov.ua/bitstream/KhPI-Press/59653/1/Poliakova_Portret_2022.pdf **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. Суддя національної категорії (Наказ асоціації спортивної боротьби України №3 від 20.12.21 м.Київ), Суддя всеукраїнських змагань серед юнаків з вільної боротьби: «Всеукраїнський турнір з вільної боротьби «Колізей»» щороку з 2017 по 2022рр.м.Харків, «Всеукраїнський турнір з вільної боротьби «День Космонавтики»» щороку з 2016 по 2022рр.м.Харків, «Всеукраїнський турнір з вільної боротьби «Зоряна осінь»» щороку з 2017 по 2022рр.м.Харків, «Ій Всеукраїнський турнір з вільної боротьби, пам'яті воїнів АТО/ООС, 2019рр., м.Хмельницький, «Всеукраїнський турнір з вільної боротьби

ПІБ викладача	Посада	Структурний підрозділ, у якому працює викладач	Інформація про кваліфікацію викладача	Стаж науково-педагогічної роботи	Навчальні дисципліни,що їх викладає викладач на ОП	Обґрунтування
						пам'яті Ю.Руденка 2018р., м.Лозова, «Всеукраїнський турнір з вільної боротьби «Black Sea Festival», 2020рр., м.Одеса. 2. Керівництво студентами Панасюк А. група СГТ-117 (2018 рік); Михайловська Т. група І-26Б (2018-2019 рік) які брали участь в Всеукраїнській Універсіаді, чемпіонаті Європи, чемпіонаті та кубку України; **П.19 Діяльність за спеціальністю у формі участі у професійних та/або громадських об'єднаннях:** 1. Співзасновник ГРОМАДСЬКОЇ ОРГАНІЗАЦІЇ «СПОРТИВНИЙ КЛУБ З БОРОТЬБИ ВІЛЬНОЇ КОЛІЗЕЙ» (18.10.2021 №1009371020000001299) від 23.10.2021
Король Ольга Григорівна	доцент	кафедра кібербезпеки НТУ «ХПІ»	**Освіта:** Харківський національний економічний університет **Спеціальність:** "Інформаційні управляючі системи та технології" **Кваліфікація:** "аналітик комп'ютерних систем". Диплом спеціаліста ХА №27419687 від 30.06.2005 р. **Кандидат технічних наук,** 05.13.21 – системи захисту інформації. **Тема:** "Моделі і методи контролю цілісності та автентичності пакетів даних у протоколах безпеки телекомунікаційних мереж" (диплом ДК №020725 від	17 років	СП 6. Інформаційна безпека держави	**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. 1-4, 8, 12,19** **П. 1. наявність не менше п'яти публікацій у періодичних наукових виданнях, що включені до переліку фахових видань України, до наукометричних баз, зокрема Scopus, Web of Science Core Collection.** 1. Korol O. and other. Research of collision propeties of the modified UMAC algorithm on crypto-code constructions. "EUREKA: Physical Sciences and Engineering", № 1. – 2022. P. 34–44. (Scopus) – Режим доступу: https://journal.eu-jr.eu/engineering/article/view/2213. ум.др.арк./власний внесок 0,1 авторських аркушів 2. Korol O. and other. Development of methodological foundations for a classifier of threats to cyberphysical systems design. Eastern-European Journal of Enterprise Technologies – 3/9 (105) –2020, – P. 6–19. (Scopus) – Режим доступу: http://journals.uran.ua/eejet/article/view/205702. ум.др.арк./власний внесок 0,4 авторських аркушів 3. Korol O. The development of the method of multifactor authentication based on hybrid crypto-code constructions on defective codes. / S. Yevseiev, H. Kots, S. Minukhin, O. Korol, A. Kholodkova // Восточно-европейский журнал передовых технологий. – 2017. – 5/9(89). – С. 19–35. – Режим доступу: https://cyberleninka.ru/article/n/razrabotka-metoda-mnogofaktornoy-autentifikatsii-na-osnove-gibridnyh-kripto-kodovyh-konstruktsiy-na-uscherbnyh-kodah/viewer (Scopus) 0,85 ум.др.арк./власний внесок 0,17 авторських аркушів. 4. Korol O. Development of methodology for modeling the interaction of antagonistic agents in cybersecurity systems / O. Korol, O. Milov, A.

ПІБ викладача	Посада	Структурний підрозділ, у якому працює викладач	Інформація про кваліфікацію викладача	Стаж науково-педагогічної роботи	Навчальні дисципліни,що їх викладає викладач на ОП	Обгрунтування
			03.04.2014 р.) **Доцент** кафедри інформаційних систем (атестат 12ДЦ № 045523 від 15.12.2015 р.).			Voitko, I. Husarova, O. Domaskin, E. Ivanchenko, I. Ivanchenko, H. Kots, I. Opirskyy, O. Fraze-Frazenko // 2019. –2/9 (98). – С. 56-66. – Режим доступу: http://journals.uran.ua/eejet/article/view/164730/164998 (Scopus) 0,55 ум.др.арк./власний внесок 0,055 авторських аркушів. 5. Korol O. and other 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//Восточно-европейский журнал передовых технологий, 2020. – 3/9 (105). – С. 6-19. – Режим доступу: https://www.researchgate.net/publication/342912870_Development_of_methodological_foundations_for_designing_a_classifier_of_threats_to_cyberphysical_systems (Scopus) 0,7 ум.др.арк./власний внесок 0,07 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.** 1. Пат. u202103665, МПК (51) G009C 1/00;Спосіб криптографічного перетворення інформації. Заявл. 23.06.2021; Опубл. 01.12.2021 р 2. Пат. u202103680, МПК (51) G009C 1/00;Спосіб криптографічного перетворення інформації. Заявл. 23.06.2021; Опубл. 01.12.2021 р 3. Пат. u202103683, МПК (51) G009C 1/00; Спосіб криптографічного перетворення інформації. Заявл. 23.06.2021; Опубл. 01.12.2021 р. 4. Пат. u202103704, МПК (51) G009C 1/00; Спосіб криптографічного перетворення інформації. Заявл. 23.06.2021; Опубл. 01.12.2021 р. 5. Пат. u202103726, МПК (51) G009C 1/00; Спосіб криптографічного перетворення інформації. Заявл. 23.06.2021; Опубл. 01.12.2021 р. **П. 3 наявність виданого підручника чи навчального посібника (включаючи електронні) або монографії (загальним обсягом не менше 5 авторських аркушів), в тому числі видані у співавторстві (обсягом не менше 1,5 авторського аркуша на кожного співавтора).** Кібербезпека: сучасні технології захисту. / С.П. Євсеєв,С.Е. Остапов, О.Г. Король // Навчальний посібник для студентів вищих навчальних закладів. Львів: "Новий Світ- 2000", 2020. – 678. – Режим доступу: http://ns2000.com.ua/wp-content/uploads/2019/11/Kiberbezpeka-suchasni-tekhnolohii-zakhystu.pdf. – ISBN 978-617-7519-44-6. Власний внесок 13,3 авторських аркушів. **П.4 наявність виданих навчально-методичних посібників/посібників для самостійної роботи здобувачів вищої**

ПІБ викладача	Посада	Структурний підрозділ, у якому працює викладач	Інформація про кваліфікацію викладача	Стаж науково-педагогічної роботи	Навчальні дисципліни,що їх викладає викладач на ОП	Обгрунтування
						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. 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. 2. Методичні рекомендації щодо написання курсових проєктів для студентів спеціальності 125 “Кібербезпека” першого (бакалаврського) рівня [Електронний ресурс] / укл. С. П. Євсеєв, А. А. Гаврилова, О. Г. Король, Г. П. Коц; Харківський національний економічний університет ім. С. Кузнеця. - Електрон. текстові дан. (2,97 МБ). - Харків : ХНЕУ ім. С. Кузнеця, 2020. -.Загол. з титул. екрану. Режим доступу: http://www.repository.hneu.edu.ua/handle/123456789/23326 3. Інформаційна безпека держави: робоча програма навчальної дисципліни для студентів спеціальності 125 “Кібербезпека” першого (бакалаврського) рівня [Електронне видання] / укл. О. Г. Король, С. П. Євсеєв. – Харків : ХНЕУ ім. С. Кузнеця, 2020. Режим доступу: http://www.repository.hneu.edu.ua/handle/123456789/24043 **П. 8 виконання функцій (повноважень, обов’язків) наукового керівника або відповідального виконавця наукової теми (проекту), або головного редактора/члена редакційної колегії/експерта (рецензента) наукового видання, включеного до переліку фахових видань України, або іноземного наукового видання, що індексується в бібліографічних базах** Відповідальний виконавець госпдоговірної НДР №403-46 від 29.11.2021 р. **П. 12 наявність апробаційних та/або науково-популярних, та/або консультаційних (дорадчих), та/або науково-експертних публікацій з наукової або професійної тематики загальною кількістю не менше п’яти публікацій** 1. Король О. Evaluation of cryptographic strength and energy intensity of de-sign of modified crypto-code struc-ture of McEliece with modified el-liptic codes / Yevseiev S., Korol O., Veselska O., Pohasii S., Khvostenko V.// International Scientific And Practical Conference “In-formation Security And In-formation Technologies”: Conference Proceedings.

ПІБ викладача	Посада	Структурний підрозділ, у якому працює викладач	Інформація про кваліфікацію викладача	Стаж науково-педагогічної роботи	Навчальні дисципліни,що їх викладає викладач на ОП	Обґрунтування
						Kharkiv – Odesa : Simon Kuznets Kharkiv National University of Economics, 2021. 298 p., P. 144–158. – URL: http://repository.hneu.edu.ua/bitstream/123456789/26827/1/144-157.pdf 2. Король О.Г. 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, вільний (дата звернення 06.10.2021). 3. Korol O. 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, вільний (дата звернення 16.04.2019). 4. Король О. Побудова гібридної крипто-кодової конструкції Мак-Еліса / С.П. Євсеєв, О.Г. Король А.А. Гаврилова, К. Четінкайя // Матеріали Міжнародної науково-практичної конференції «Інформаційна безпека та інформаційні технології» : тези доповідей, 24-25 квітня 2019 р. – Х. : ХНЕУ ім. С. Кузнеця. – 2019 – 68 с. (С. 9). – URL: http://repository.hneu.edu.ua/handle/123456789/21639, вільний (дата звернення 10.10.2021). 5. Synergy of building cybersecurity systems / S. Yevseiev, V. Ponomarenko, O. Laptiev, O. Milov, O. Korol, S. Milevskyi, S. Pohasii, A. Tkachov, O. Shmatko, Y. Melenti, O. Sievierinov, S. Ostapov, A. Gavrilova, O. Tsyhanenko, S. Herasimov, E. Nyemkova, B. Tomashevsky, I. Hrod, I. Opirskyy, V. Zvieriev, O. Prokopenko, V. Savchenko, O. Barabash, V. Sobchuk, G. Shuklin, V. Khvostenko, O. Tymochko, M. Pavlenko, A. Trystan, S. Florov // monograph. – Kharkiv: PC TECHNOLOGY CENTER, 2021. – 188 p.(P. 102 – 147). Acces mode: https://repository.entc.com.ua/publications/345382/synergy-of-building-cybersecurity-systems#id-section-content, вільний (дата звернення 8.10.2021). **П. 19 . Діяльність за спеціальністю у формі участі у професійних та/або громадських об'єднаннях** член громадської організації "Східноєвропейське наукове товариство", посвідчення ES № 057

ПІБ викладача	Посада	Структурний підрозділ, у якому працює викладач	Інформація про кваліфікацію викладача	Стаж науково-педагогічної роботи	Навчальні дисципліни,що їх викладає викладач на ОП	Обгрунтування
Євсеєв Сергій Петрович	завідувач кафедри	кафедра кібербезпеки НТУ «ХПІ»	**Освіта:** Пермське вище військове командно-інженерне Червонопрапорне училище ракетних військ імені Маршала Радянського Союзу Чуйкова В.І. **Спеціальність:** “Автоматизовані системи управління” **Кваліфікація** “офіцер з вищою військово-спеціальною освітою, інженер-кібернетик” Диплом спеціаліста УВ №584991 від 23.06.1991 р. ХВУ Спеціальність “Організація технічного забезпечення військ (за видами та родами військ і сил)” **Кваліфікація:** “магістр військового управління, офіцер військового управління оперативно-тактичного рівня” Диплом магістра МО №13590538 від 21.06.2002 р. **Доктор технічних наук**, 125 – Кібербезпека	37 років	СП 10. Введення в мережі СП 13. Менеджмент інформаційної безпеки СП 15. Основи криптографічного захисту СП 21. Основи соціальної інженерії СП 26. Антивірусний захист інформації	**Підвищення кваліфікації:** Центр підтримки академій Cisco Національний технічний університет “Харківський політехнічний інститут”. Сертифікат від “30” червня 2021 р. 6 кредитів. Тема “CCNA CyberOps” **Пункти відповідності ліцензійних умов:** **П. 1-10, 12, 13, 19** **П. 1 наявність не менше п’яти публікацій у періодичних наукових виданнях, що включені до переліку фахових видань України, до наукометричних баз, зокрема Scopus, Web of Science Core Collection** 1. Yevseiev and other. Development of a modification of the method for constructing energy-efficient sensor networks using static and dynamic sensors. Eastern-European Journal of Enterprise Technologies. 2022. 1/9 (115). P. 15–23. (Scopus) – Режим доступу: http://journals.uran.ua/eejet/article/view/252988. ум.др.арк./власний внесок 0,1 2. Yevseiev and other. Development of crypto code structures on LDPC-codes. Eastern-European Journal of Enterprise Technologies. 2022. 2/9 (116). P. 44–59. (Scopus) – Режим доступу: http://journals.uran.ua/eejet/article/view/254545. ум.др.арк./власний внесок 0,3 3. Yevseiev and other. Development of a method for determining the indicators of manipulation based on morphological synthesis. Eastern-European Journal of Enterprise Technologies. 2022. 3/9 (117). P. 22–35. (Scopus) – Режим доступу: https://www.researchgate.net/publication/361877056_Development_of_a_method_for_determining_the_indicators_of_manipulation_based_on_morphological_synthesis ум.др.арк./власний внесок 0,3 4. Yevseiev and other. Development of concepts for the cyber security metrics classification. Eastern-European Journal of Enterprise Technologies. 4/4 (118). 2022. P. 6–18. (Scopus) – Режим доступу: https://www.engpaper.com/technology-center/development-of-a-concept-for-cybersecurity-metrics-classification.html ум.др.арк./власний внесок 0,3 5. Yevseiev and other. Development of a hardware cryptosystem based on a random number generator with two types of entropy sources. Eastern-European Journal of Enterprise Technologies. 5/9 (119). 2022. P. 6–16.

ПІБ викладача	Посада	Структурний підрозділ, у якому працює викладач	Інформація про кваліфікацію викладача	Стаж науково-педагогічної роботи	Навчальні дисципліни,що їх викладає викладач на ОП	Обґрунтування
			(21.05.01 – Інформаційна безпека держави). Диплом ДД №007606 від 5.07.2018 р. **Тема дисертації:** Методологія побудови системи безпеки банківських інформаційних ресурсів" **Професор** кафедри кібербезпеки та інформаційних технологій диплом АП № 001633 від 26.02.2020 р.			(Scopus) – Режим доступу: https://www.researchgate.net/publication/365395598_Development_of_a_hardware_cryptosystem_based_on_a_random_number_generator_with_two_types_of_entropy_sources. ум.др.арк./власний внесок 0,25 **П. 2 наявність одного патенту на винахід або п'яти деклараційних патентів на винахід чи корисну модель, включаючи секретні, або наявність не менше п'яти свідоцтв про реєстрацію авторського права на твір** 1. Пат. u202103665, МПК (51) G009C 1/00;Спосіб криптографічного перетворення інформації. Заявл. 23.06.2021; Опубл. 01.12.2021 р 2. Пат. u202103680, МПК (51) G009C 1/00;Спосіб криптографічного перетворення інформації. Заявл. 23.06.2021; Опубл. 01.12.2021 р 3. Пат. u202103683, МПК (51) G009C 1/00; Спосіб криптографічного перетворення інформації. Заявл. 23.06.2021; Опубл. 01.12.2021 р. 4. Пат. u202103704, МПК (51) G009C 1/00; Спосіб криптографічного перетворення інформації. Заявл. 23.06.2021; Опубл. 01.12.2021 р. 5. Пат. u202103726, МПК (51) G009C 1/00; Спосіб криптографічного перетворення інформації. Заявл. 23.06.2021; Опубл. 01.12.2021 р. **П. 3 наявність виданого підручника чи навчального посібника (включаючи електронні) або монографії (загальним обсягом не менше 5 авторських аркушів), в тому числі видані у співавторстві (обсягом не менше 1,5 авторського аркуша на кожного співавтора)** Євсеєв С.П. Кібербезпека: Криптографія з Python. / С.П. Євсеєв, О.В. Шматко, О.Г. Король // Навчальний посібник для студентів вищих навчальних закладів. Навчальний посібник. Львів: "Новий Світ–2000", 2020. – 120. – Режим доступу: https://lib.nadpsu.edu.ua/?page=/NewBooks/2021/NewBooks11/NewBooks11. Власний внесок 2,5 авторських аркушів. **П. 4 наявність виданих навчально-методичних посібників/посібників для самостійної роботи здобувачів вищої освіти та дистанційного навчання, електронних курсів на освітніх платформах ліцензіатів, конспектів лекцій/практикумів/методичних вказівок/рекомендацій/ робочих програм, інших друкованих навчально-методичних праць загальною кількістю три найменування** 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:

ПІБ викладача	Посада	Структурний підрозділ, у якому працює викладач	Інформація про кваліфікацію викладача	Стаж науково-педагогічної роботи	Навчальні дисципліни,що їх викладає викладач на ОП	Обгрунтування
						http://repository.hneu.edu.ua/handle/123456789/24508. Робочі програми навчальних дисциплін: 1. Безпека банківських систем: робоча програма навчальної дисципліни для студентів спеціальності 125 «Кібербезпека» першого (бакалаврського) рівня / укл. С. П. Євсеєв.– Харків : ХНЕУ ім. С. Кузнеця, 2020. – 13 с. (Укр. мовою). Режим доступу: ttps://pns.hneu.edu.ua/course/view.php?id=7549 2. Безпека в інформаційно-комунікаційних системах: робоча програма навчальної дисципліни для студентів спеціальності 125 “Кібербезпека” першого (бакалаврського) рівня / уклад. С. П. Євсеєв, Р. В. Корольов. – Харків : ХНЕУ ім. С. Кузнеця, 2020. – 13 с. (Укр. мовою). Режим доступу: https://pns.hneu.edu.ua/course/view.php?id=5388 3. Введення в мережі: робоча програма навчальної дисципліни для студентів спеціальності 125 “Кібербезпека” першого (бакалаврського) рівня [Електронне видання] / укл. С. П. Євсеєв – Харків : ХНЕУ ім. С. Кузнеця, 2020. – 11 с. Режим доступу: https://pns.hneu.edu.ua/course/view.php?id=5732 4. Менеджмент інформаційної безпеки: робоча програма навчальної дисципліни для студентів спеціальності 125 «Кібербезпека» першого (бакалаврського) рівня / уклад. С. П. Євсеєв. – Харків : ХНЕУ ім. С. Кузнеця, 2020. – 12 с. (Укр. мовою). Режим доступу: https://pns.hneu.edu.ua/course/view.php?id=4924 5. Бездротові та оптичноволоконні мережі: робоча програма навчальної дисципліни для студентів спеціальності 125 «Кібербезпека» другого (магістерського) рівня [Електронне видання] / укл. С. П. Євсеєв. – Харків : ХНЕУ ім. С. Кузнеця, 2020. – 10 с. Режим доступу: https://pns.hneu.edu.ua/course/view.php?id=7212 **П. 5 захист дисертації на здобуття наукового ступеня** Доктор технічних наук, 21.05.01 - Інформаційна безпека держави, тема дисертації: Методологія побудови систем безпеки банківських інформаційних ресурсів. Диплом ДД № 007606 від 5 липня 2018 року, Міністерство освіти і науки України, Національний авіаційний університет. **П. 6 наукове керівництво (консультування) здобувача, який одержав документ про присудження наукового ступеня** Мілов Олександр Володимирович, доктор технічних наук, 05.13.21. Системи захисту інформації, тема дисертації: Методологія моделювання процесів поведінки антагоністичних агентів в системах безпеки, 2020 рік. Диплом ДД №010482 від 26 листопада 2020 року,

ПІБ викладача	Посада	Структурний підрозділ, у якому працює викладач	Інформація про кваліфікацію викладача	Стаж науково-педагогічної роботи	Навчальні дисципліни,що їх викладає викладач на ОП	Обґрунтування
						Міністерство освіти і науки України. Національний університет "Львівська політехніка". Циганенко Олексій Сергійович, доктор філософії зі спеціальності 122 – комп'ютерні науки, тема дисертації: "Моделі та методи підвищення якості обслуговування інформаційних систем", 2022 р., Диплом ДР №003787 від 1 лютого 2022 року, Міністерство освіти і науки України. Одеський державний екологічний університет. **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** Ахромович Володимир Миколайович, здобуття наукового ступеня доктора технічних наук за спеціальністю 05.13.21 "Системи захисту інформації", "Методологічні основи захисту інформації в соціальних мережах", 21.04.2020 р., Державний університет телекомунікацій. Улічев Олександр Сергійович, здобуття наукового ступеня кандидата технічних наук за спеціальністю 21.05.01 – "Інформаційна безпека держави", "Модель та методи поширення інформаційних впливів у соціальних мережах в умовах інформаційного протиборства", 13.05. 2021 р., Національний авіаційний університет. Костяк Марина Юріївна, здобуття наукового ступеня кандидата технічних наук за спеціальністю 05.13.21 – системи захисту інформації, "Підвищення ефективності функціонування захищених інформаційних мереж спеціального призначення", 2021 р., Національний університет "Львівська політехника". **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** Член редакційної колегії наукового фахового видання "Безпека інформації" (https://jrnl.nau.edu.ua/index.php/Infosecurity/about) Член редакційної колегії наукового фахового видання "Наука і техніка Повітряних Сил Збройних Сил України" (http://www.hups.mil.gov.ua/periodic-app/journal/nitps) Член редакційної колегії наукового фахового видання "Восточно Европейский журнал передвіх технологій"(https://publons.com/researcher/4702171/serhii-yevseiev/peer-review/) Виконання функцій наукового керівника науково-дослідної роботи за

ПІБ викладача	Посада	Структурний підрозділ, у якому працює викладач	Інформація про кваліфікацію викладача	Стаж науково-педагогічної роботи	Навчальні дисципліни,що їх викладає викладач на ОП	Обґрунтування
						темою: “Методологія моделювання процесів поведінки антагоністичних агентів в системах безпеки”, державний реєстраційний номер 0119U103117, № 2/2019 (і) Відповідальний виконавець науково-дослідної роботи за темою: “Розробка методичного та модельно-інформаційного забезпечення побудови університету інноваційного типу на засадах якості освіти та протидії корупції”, № 46/2020-2021, державний реєстраційний № 0120U102152 (Наказ №14-НДС від 17.04.2020р.). **П.9 робота у складі експертної ради з питань проведення експертизи дисертацій МОН або у складі галузевої експертної ради як експерта Національного агентства із забезпечення якості вищої освіти, або у складі Акредитаційної комісії, або міжгалузевої експертної ради з вищої освіти Акредитаційної комісії, або трьох експертних комісій МОН/зазначеного Агентства, або Науково-методичної ради/науково-методичних комісій (підкомісій) з вищої або фахової передвищої освіти МОН, наукових/науково-методичних/експертних рад органів державної влади та органів місцевого самоврядування, або у складі комісій Державної служби якості освіти із здійснення планових (позапланових) заходів державного нагляду (контролю)** Робота у складі науково-методичної комісії 7 “ З інформаційних технологій, автоматизації та телекомунікацій”, підкомісія 125 “Кібербезпека” сектору вищої освіти Науково-методичної ради Міністерства освіти і науки України (2019–2020 р.р., Наказ Міністерства освіти і науки України від 25 квітня 2019 р. № 582 «Про персональний склад Науково-методичних комісій (підкомісій) сектору вищої освіти науково-методичної ради МОН») Експерт Національного фонду досліджень України (2020 - 2021 рр) Експерт МОН України Секція: 2. Інформатика та кібернетика (2022 р.) **П. 10 участь у міжнародних наукових та/або освітніх проектах, залучення до міжнародної експертизи, наявність звання “суддя міжнародної категорії”** 1) Євсеєв Сергій Петрович - координатор угоди про співробітництво між університетом у Бельско-Бялій, м. Польща та ХНЕУ ім. С. Кузнеця, м. Харків. Угода підписана 14.01.2020 р. (програма двох дипломів). 2) Євсеєв Сергій Петрович - координатор робочої групи з реалізації міжнародного гранту “Conducting e-learning cyberhygiene” **П. 12 наявність апробаційних та/або науково-популярних, та/або консультаційних (дорадчих), та/або науково-експертних**

ПІБ викладача	Посада	Структурний підрозділ, у якому працює викладач	Інформація про кваліфікацію викладача	Стаж науково-педагогічної роботи	Навчальні дисципліни,що їх викладає викладач на ОП	Обгрунтування
						публікацій з наукової або професійної тематики загальною кількістю не менше п'яти публікацій. 1. Yevseiev Serhii Socio-Cyber-Physical Systems Security Concept / Serhii Yevseiev, Stanislav Milevskyi, Leonid Bortnik, Voropay Alexey, Kyrylo Bondarenko, Serhii Pohasii / 4th International Congress on Human-Computer Interaction, Optimization and Robotic Applications. June 9-11, 2022, Ankara, Turkey. URL: https://www.aconf.org/conf_181999.html 2. Yevseiev Serhii. Solving the Problem of Convergence of the Results of Analog Signals Conversion in the Process of Aircraft Control. / Serhii Yevseiev, Oleksandr Laptiev, Serhii Yevseiev, Andrii Trystan, Valerii Chystov, Olha Matiushchenko, Iryna Zakharchenko / 2022 IEEE Third International Conference on SYSTEM ANALYSIS & INTELLIGENT COMPUTING (SAIC), 04-07 Oktober, Kyiv, Ukraine. p. 118-124. URL: http://saic.ieee.org.ua/?page_id=96https://ieeexplore.ieee.org/abstract/document/9297102/metrics#metrics, 3. Yevseiev Serhii. Measuring Signals Synthesis Method on the Basis of Triangular Time-Pulse Modulation for Control of Radiotechnic Systems Technical Condition. Concept / Sergiy Tymchenko, Volodymyr Kutsenko, Serhii Yevseiev, Stanislav Milevskyi, Serhii Pohasii / 4th International Congress on Human-Computer Interaction, Optimization and Robotic Applications. June 9-11, 2022, Ankara, Turkey URL: https://www.aconf.org/conf_181999.html 4. Yevseiev Serhii Development of Methods for Improving Crypto Transformations in the Block-Symmetric Code [Електронний ресурс] /S. Yevseiev, R. Korolyov, S.Milevskyi, I. Ireifidzh, T. Gancarczyk, R. Szklarczyk/ 2020 IEEE 5th International Symposium on Smart and Wireless Systems within the Conferences on Intelligent Data Acquisition and Advanced Computing Systems (IDAACS-SWS), 17-18 сентября 2020. - Дортмунд, Германия. URL: https://ieeexplore.ieee.org/abstract/document/9297102/metrics#metrics, вільний (дата звернення 1.08.2021). 5. Yevseiev S. PERSPECTIVE NATIONAL COMMUNICATION SYSTEM FOR CYBER MANAGEMENT OF CRITICAL FACILITIES / Tomashevsky B. Yevseiev S. Tkachov A. // 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, вільний (дата звернення 1.02.2021).

ПІБ викладача	Посада	Структурний підрозділ, у якому працює викладач	Інформація про кваліфікацію викладача	Стаж науково-педагогічної роботи	Навчальні дисципліни,що їх викладає викладач на ОП	Обґрунтування
						П.13. проведення навчальних занять із спеціальних дисциплін іноземною мовою (крім дисциплін мовної підготовки) в обсязі не менше **50 аудиторних годин на навчальний рік** 1. Information security of the state, кредитів 4,0 (64 години) **П. 19 . Діяльність за спеціальністю у формі участі у професійних та/або громадських об'єднаннях** член громадської організації "Східноєвропейське наукове товариство", посвідчення ES № 053.
Мілов Олександр Володимирович	професор	кафедра кібербезпеки НТУ «ХПІ»	**Освіта:** Московський енергетичний інститут, факультет електронної техніки **Спеціальність:** "Промислова електроніка", **Кваліфікація:** "Інженер електронної техніки". Диплом Я № 287387 від 20.02.1978 р. **Доктор технічних наук**, 05.13.21 – Системи захисту інформації ДД № 010482 від 26.11.2020 р. **Тема:** "Методологія моделювання процесів поведінки антагоністичних агентів в системах безпеки". **Кандидат технічних наук,** 14 - Електрична інженерія, 141 Електроенергетика, електротехніка та	41 років	СП 7. Структури даних СП 8. Математичні основи криптології	**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. Milov O. Practical implementation of the Niederreiter modified crypto-code system on truncated elliptic codes / Yevseiev S., Milov O., Tsyhanenko O., Ivanchenko S., Aleksiyev V., Verheles D., Volkov S., Korolev R., Kots H., Shmatko O. // Eastern-Europe Joutnal of Enterprise Technologies, 6/4 (96) 2018. p. 24-31. - Access mode: http://journals.uran.ua/eejet/article/view/150903 (1,6 ум.друк.арк./власний внесок 0,16 авторських аркушів.) 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

ПІБ викладача	Посада	Структурний підрозділ, у якому працює викладач	Інформація про кваліфікацію викладача	Стаж науково-педагогічної роботи	Навчальні дисципліни,що їх викладає викладач на ОП	Обгрунтування
			електромеханіка (05.09.12 - Напівпровідникові перетворювачі), диплом ТН № 094834 від 12.11.1986 р. **Професор** кафедри кібербезпеки та інформаційних технологій, диплом АП № 001430 від 16.12.2019 р.			(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

ПІБ викладача	Посада	Структурний підрозділ, у якому працює викладач	Інформація про кваліфікацію викладача	Стаж науково-педагогічної роботи	Навчальні дисципліни,що їх викладає викладач на ОП	Обгрунтування
						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

ПІБ викладача	Посада	Структурний підрозділ, у якому працює викладач	Інформація про кваліфікацію викладача	Стаж науково-педагогічної роботи	Навчальні дисципліни,що їх викладає викладач на ОП	Обгрунтування
						[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

ПІБ викладача	Посада	Структурний підрозділ, у якому працює викладач	Інформація про кваліфікацію викладача	Стаж науково-педагогічної роботи	Навчальні дисципліни,що їх викладає викладач на ОП	Обґрунтування
						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%b

ПІБ викладача	Посада	Структурний підрозділ, у якому працює викладач	Інформація про кваліфікацію викладача	Стаж науково-педагогічної роботи	Навчальні дисципліни,що їх викладає викладач на ОП	Обгрунтування
						b%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.

ПІБ викладача	Посада	Структурний підрозділ, у якому працює викладач	Інформація про кваліфікацію викладача	Стаж науково-педагогічної роботи	Навчальні дисципліни,що їх викладає викладач на ОП	Обґрунтування
						П. 19 діяльність за спеціальністю у формі участі у професійних та/або громадських об'єднаннях Член громадської організації "Східноєвропейське наукове товариство", свідотство ES № 060
Корольов Роман Володимирович	доцент	кафедра кібербезпеки НТУ «ХПІ»	**Освіта:** Харківський військовий університет. **Спеціальність:** "Системи управління і автоматики". **Кваліфікація:** "інженер комп'ютеризованих систем управління і автоматики, офіцера військового управління тактичного рівня". Диплом спеціаліста від 26.06.1999 р. **Кандидат технічних наук,** 05.13.06 – інформаційні технології.Диплом ДК №054389. **Тема:** "Методи формування псевдовипадкових чисел на основі надлишкових кодів". **Доцент** кафедри кібербезпеки та інформаційних технологій АД№006041 від 26.11.2020 р.	28 років	СП 5. Фізичні основи технічних засобів розвідки СП 16. Безпека в інформаційно-комунікаційних системах. СП 20. Основи стеганографічного захисту інформації. СП 23. Бізнес інтелідженс СП 24. Комплексні засоби захисту інформації	**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, 12, 14, 19** **П. 1 наявність не менше п'яти публікацій у періодичних наукових виданнях, що включені до переліку фахових видань України, до наукометричних баз, зокрема Scopus, Web of Science Core Collection** 1. Корольов Р. Використання міні-версій для оцінки стійкості блоково-симетричних шифрів / С. Євсеєв, С. Остапов, Р. Королев // Науково-технічний журнал "Безпека інформації". – 2017. – том 23, № 2 – С. 100 – 108. (0,5 ум. др. арк. / 0,16 ум. друк. арк. власного внеску). (фахове, категорія Б) 2. Корольов Р. Верифікація методики оцінювання функціональної ефективності передачі банківських інформаційних ресурсів в автоматизованих банківських системах / С. Євсеєв, , А. Комишан , Р.Корольов, І. Бонь,С. Солоненко, В. Богульський // Збірник наукових праць Харківського національного університету Повітряних Сил. – 2018. – том 2(56). – С.170 – 186. – Режим доступу: https://www.researchgate.net/publication/325874469_Verifikacia_metodiki_ocinuvanna_funkcionalnoi_efektivnosti_peredaci_bankivskih_informacijnih_resursiv_v_avtomatizovanih_bankivskih_sistemah (фахове видання). 0,85 ум.др.арк./власний внесок 0,21 авторських аркушів. 3. Корольов Р. Аналіз сучасних засобів знищення безпілотних літальних апаратів / Р.Корольов, Н. Королюк, О.Петров, К.Сюлев // Збірник наукових праць Харківського національного університету Повітряних Сил. – 2017. – том 4(53). – С.17 – 21. Режим доступу: http://www.hups.mil.gov.ua/periodic-app/article/17779 (фахове видання). 0,25 ум.др.арк./власний внесок 0,06 авторських аркушів. 4. Korolev R. Practical implementation of the Niederreiter modified crypto-code system on truncated elliptic codes / S.Yevseiev, O.Tsyhanenko, S.Ivanchenko, V.Aleksiyev, D.Verheles, S.Volkov, R. Korolev, H.Kots H, O.Milov, O.Shmatko // Восточно-европейский

ПІБ викладача	Посада	Структурний підрозділ, у якому працює викладач	Інформація про кваліфікацію викладача	Стаж науково-педагогічної роботи	Навчальні дисципліни,що їх викладає викладач на ОП	Обгрунтування
						журнал передовых технологий. – Харьков. – 2018. 6/4(96). С. 24 –31 – Режим доступу: http://journals.uran.ua/eejet/article/view/150903/152760 (фахове, категорія А) (Scopus). 0,4 ум.др.арк./власний внесок 0,04 авторських аркушів. 5. Gavrilova A. Chekunova O Development of a modified umac algorithm based on crypto-code constructions / A.Gavrilova, I.Volkov, Y.Kozhedub, O.Lezik, V.Medvediev, O.Milov, B.Tomashevsky, A.Trystan, O.Chekunova // Восточно-европейский журнал передовых технологий. – Харьков. – 2020. 4/9(106). С. 45 –63 – Режим доступу: https://poseidon01.ssrn.com/delivery.php?ID=588125096113082100100900102102410012103503107705401701306511202907702611110208603108111810710600210401900411402907401610910212400608608705908300000408507700206408711805405806212006911610610906401302806602009401008509809602806409308712002801307506709106 8&EXT=pdf&INDEX=TRUE (фахове, категорія А) (Scopus) . 0,95 ум.др.арк./власний внесок 0,095 авторських аркушів. 6. Korolev R. Modification of the algorithm (OFM) S-box, which provides increasing crypto resistance in the post-quantum period / S.Yevseiev, R. Korolyov, A. Tkachov, O. Laptiev, I. Opirskyy, O. Soloviova // International Journal of Advanced Trends in Computer Science and Engineering, 9(5), September-October 2020, pp. 8725 - 8729 Режим доступу: 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) 7. Korolev R. Development of procedures for modifying the cipher GOST 28147 / Yevseiev S., Korolyov R., Tkachov A., Nimchenko A. // Advanced Information Systems. 2021. Vol. 5, No. 2. P. 125-129. – Режим доступу: http://repository.kpi.kharkov.ua/handle/KhPI-Press/53790 (фахове, категорія Б). 0,25 ум.др.арк./власний внесок 0,06 авторських аркушів. 8. Korolev. R. Enhancement of productivity of random sequences generation for information protection systems / R.Korolev, S.Ivanchenko, S.Yevseiev, V.Bezshtanko, V.Bondarenko, O.Gavrylenko, N.Kazakova, S.Mazor, / Eastern-European Journal of Enterprise Technologies – 2018.– №9(94) – p. 50 – 60. – Режим доступу:http://journals.uran.ua/eejet/article/view/139755 (фахове, категорія А) (Scopus). 0,55 ум.др.арк./власний внесок 0,055 авторських аркушів. **П. 2 наявність одного патенту на винахід або п’яти деклараційних**

ПІБ викладача	Посада	Структурний підрозділ, у якому працює викладач	Інформація про кваліфікацію викладача	Стаж науково-педагогічної роботи	Навчальні дисципліни,що їх викладає викладач на ОП	Обґрунтування
						патентів на винахід чи корисну модель, включаючи секретні, або наявність не менше п'яти свідоцтв про реєстрацію авторського права на твір 1. Патент. Пат. U 2017 123375, МПК (51). G009C 1/00 Спосіб криптографічного перетворення інформації з використанням подовжених кодів. Заявл. 11.09. 2017; Опубл. 26.02.2018, Бюл. № 4, 2018 р. – 4 с. 2. Пат. U 2017 123379, МПК (51) G009C 1/00 Спосіб криптографічного перетворення інформації з використанням укорочених кодів. Заявл. 11.09. 2017; Опубл. 26.02.2018, Бюл. № 4, 2018 р. – 4 с. 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. Бездротова та мобільна безпека: робоча програма навчальної дисципліни для студентів спеціальності 125 «Кібербезпека» другого (магістерського) рівня [Електронне видання] / укл. Р. В. Корольов. – Харків : ХНЕУ ім. С. Кузнеця, 2020. – 9 с. Режим доступу: https://pns.hneu.edu.ua/course/view.php?id=7124 2. Бізнес інтеленденс (Business intelligence): робоча програма навчальної дисципліни для студентів спеціальності 073 «Менеджмент» другого (магістерського) рівня [Електронне видання] / укл. Р. В. Корольов. – Харків : ХНЕУ ім. С. Кузнеця, 2020. – 8 с. Режим доступу: https://pns.hneu.edu.ua/course/view.php?id=4768 3. Комп'ютерні системи та архітектура комп'ютерів: робоча програма навчальної дисципліни для студентів спеціальності 121 "Інженерія

ПІБ викладача	Посада	Структурний підрозділ, у якому працює викладач	Інформація про кваліфікацію викладача	Стаж науково-педагогічної роботи	Навчальні дисципліни,що їх викладає викладач на ОП	Обґрунтування
						програмного забезпечення" першого (бакалаврського) рівня [Електронне видання] / укл. Р. В. Корольов, С. С. Погасій. – Харків : ХНЕУ ім. С. Кузнеця, 2020. – 10 с. Режим доступу: https://pns.hneu.edu.ua/course/view.php?id=5241. 4 Комплексні системи захисту інформації: робоча програма навчальної дисципліни для студентів спеціальності 125 "Кібербезпека" першого (бакалаврського) рівня [Електронне видання] / укл. Р. В. Корольов – Харків : ХНЕУ ім. С. Кузнеця, 2020. – 11 с. Режим доступу: https://pns.hneu.edu.ua/course/view.php?id=4940 5. Основи розробки децентралізованих застосувань (decentralized applications (dapps)): робоча програма навчальної дисципліни для студентів спеціальності 125 "Кібербезпека" першого (бакалаврського) рівня / уклад. Р. В. Корольов. – Харків : ХНЕУ ім. С. Кузнеця, 2020. – 13 с. (Укр. мовою). Режим доступу: https://pns.hneu.edu.ua/course/view.php?id=5399 6. Основи стеганографічного захисту інформації: робоча програма навчальної дисципліни для студентів спеціальності 125 "Кібербезпека" першого (бакалаврського) рівня [Електронне видання] / укл. Р. В. Корольов – Харків : ХНЕУ ім. С. Кузнеця, 2020. – 10 с. Режим доступу: https://pns.hneu.edu.ua/course/view.php?id=5390 7. Основи технічного захисту інформації: робоча програма навчальної дисципліни для студентів спеціальності 125 "Кібербезпека" першого (бакалаврського) рівня [Електронне видання] / укл. Р. В. Корольов – Харків : ХНЕУ ім. С. Кузнеця, 2020. – 13 с. Режим доступу: https://pns.hneu.edu.ua/course/view.php?id=5389 8. Основи IT: 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: https://pns.hneu.edu.ua/course/view.php?id=5409 **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.Корольов Р.В. Розробка методів вдосконалення криптоперетворень в блочно-симетричному шифрі ГОСТ 28147:2009 [Електронний ресурс]/Р.В. Корольов, А.А. Лапушинська ./ Актуальні питання забезпечення службово-бойової діяльності сил сектору безпеки і оборони : матеріали регіон. круг. столу (м. Харків,24 квіт. 2020 р.) Вип. 4.– с.266-270. –URL:

ПІБ викладача	Посада	Структурний підрозділ, у якому працює викладач	Інформація про кваліфікацію викладача	Стаж науково-педагогічної роботи	Навчальні дисципліни,що їх викладає викладач на ОП	Обґрунтування
						http://www.hups.mil.gov.ua/assets/uploads/library/nadhodzhennya/kv%D1%96ten-cherven-2020/pdf/1.pdf, вільний (дата звернення 1.08.2021 р.) 2. Korolyov R. Development of Methods for Improving Crypto Transformations in the Block-Symmetric Code [Електронний ресурс] /S. Yevseiev, R. Korolyov, S.Milevskyi, I. Ireifidzh, T. Gancarczyk, R. Szklarczyk/ 2020 IEEE 5th International Symposium on Smart and Wireless Systems within the Conferences on Intelligent Data Acquisition and Advanced Computing Systems (IDAACS-SWS) URL: https://ieeexplore.ieee.org/abstract/document/9297102/metrics#metrics, (дата звернення 1.08.2021) 3. Корольов Р. В. Анализ уязвимостей технологии блокчейн при работе с криптовалютами [Електронний ресурс] /А. Гаврилова, Р.В. Корольов/ 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 (дата звернення 1.08.2021) 4. Корольов Р. В. /Теоретичні основи автоматизації процесів управління військами та озброєнням: навч.посіб. для слухачів, курс. Та студ. Вищ.навч. закл. / О.І.Тимочко, Н.О.Королюк, Р.В.Корольов та ін..; за заг.ред О.І.Тимочко. – Х. :ХНУПС, 2017. – 220 с. (дата звернення 1.08.2021) http://www.hups.mil.gov.ua/assets/uploads/library/nadhodzhennya/january-march-2018/42.pdf 5. Korolyov R. / Development of Methods for Improving Crypto Transformations in the Block-Symmetric Code [Електронний ресурс] /S. Yevseiev, R. Korolyov, S.Milevskyi, I. Ireifidzh, T. Gancarczyk, R. Szklarczyk/ 2020 IEEE 5th International Symposium on Smart and Wireless Systems within the Conferences on Intelligent Data Acquisition and Advanced Computing Systems (IDAACS-SWS), 17-18 сентября 2020. - Дортмунд, Германия. URL: https://ieeexplore.ieee.org/abstract/document/9297102/metrics#metrics, вільний (дата звернення 1.08.2021). **П. 14 керівництво студентом, який зайняв призове місце на І або ІІ етапі Всеукраїнської студентської олімпіади (Всеукраїнського**

ПІБ викладача	Посада	Структурний підрозділ, у якому працює викладач	Інформація про кваліфікацію викладача	Стаж науково-педагогічної роботи	Навчальні дисципліни,що їх викладає викладач на ОП	Обґрунтування
						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. Експерт 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 I етапу Всеукраїнського конкурсу професійної майстерності «WorldSkills Ukraine» у 2021 році» Режим доступу https://drive.google.com/file/d/1bjtYbubJ0VA66EhjL8JYSrtFlN-Nw2FB/view?usp=sharing 2. Керівництво студентом переможцем 1 етапу Всеукраїнського конкурсу студентських наукових робіт за напрямом Кібербезпека. **П. 19 діяльність за спеціальністю у формі участі у професійних та/або громадських об'єднаннях** асоційований член Громадської організації "Association of STEM

ПІБ викладача	Посада	Структурний підрозділ, у якому працює викладач	Інформація про кваліфікацію викладача	Стаж науково-педагогічної роботи	Навчальні дисципліни,що їх викладає викладач на ОП	Обгрунтування
						researchers and inventors" довідка №2 від 7.10.2021р.
Ткачов Андрій Михайлович	доцент	кафедра кібербезпеки НТУ «ХПІ»	**Освіта:** Харківський військовий університет. **Спеціальність:** "Програмне забезпечення обчислювальної техніки і автоматизованих систем. **Кваліфікація:** спеціаліста "інженера-математика", диплом спеціаліста ВЕ № 006749, від 22.06.1996 р. **Кандидат технічних наук** зі спеціальності військова кібернетика, системи управління та зв'язок. диплом ДК № 025982, від 13.04.2004 р. **Тема:** спеціальна. **Старший науковий співробітник** атестат АС №000423 від 26.09.2012 р.	32 рік	СП 2. Основи програмування СП 4. Розробка та аналіз алгоритмів СП 11. Технології програмування СП 17. Сучасні інформаційні системи (з елементами кібербезпеки)	**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.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 http://www.hups.mil.gov.ua/periodic-app/article/18332 (0,28 ум. др. арк. / 0,055 ум. др. арк. власного внеску) вільний (дата звернення 11.10.2021). (фахове, категорія Б) 2. 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) 3. 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) 4. S.Yevseiev, R. Korolyov, A. Tkachov, O. Laptiev, I. Opirskyy, O.

ПІБ викладача	Посада	Структурний підрозділ, у якому працює викладач	Інформація про кваліфікацію викладача	Стаж науково-педагогічної роботи	Навчальні дисципліни,що їх викладає викладач на ОП	Обґрунтування
						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) 5. 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) 6. 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) **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**

ПІБ викладача	Посада	Структурний підрозділ, у якому працює викладач	Інформація про кваліфікацію викладача	Стаж науково-педагогічної роботи	Навчальні дисципліни,що їх викладає викладач на ОП	Обґрунтування
						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

ПІБ викладача	Посада	Структурний підрозділ, у якому працює викладач	Інформація про кваліфікацію викладача	Стаж науково-педагогічної роботи	Навчальні дисципліни,що їх викладає викладач на ОП	Обґрунтування
						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

ПІБ викладача	Посада	Структурний підрозділ, у якому працює викладач	Інформація про кваліфікацію викладача	Стаж науково-педагогічної роботи	Навчальні дисципліни,що їх викладає викладач на ОП	Обґрунтування
						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**

ПІБ викладача	Посада	Структурний підрозділ, у якому працює викладач	Інформація про кваліфікацію викладача	Стаж науково-педагогічної роботи	Навчальні дисципліни,що їх викладає викладач на ОП	Обґрунтування
						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.
Гаврилова Алла Андріївна	доцент	кафедра кібербезпеки НТУ «ХПІ»	**Освіта:** Харківський державний економічний університет. **Спеціальність:** Економічна інформатика і автоматизовані системи управління. **Кваліфікація:** інженер-економіст. 07.06.1994, диплом	19 років	СП 1. Вступ до спеціальності. Ознайомча практика СП 18. Комплексні системи захисту інформації	**Підвищення кваліфікації:** 1) **Доктор філософії**, 125 – Кібербезпека та захист інформації, **Тема:** «Моделі та методи контролю цілісності та автентичності на основі каскадного алгоритму UMAC», Диплом Н23 № 001755, від 6 грудня 2023 року, Міністерство освіти і науки України, Національний авіаційний університет 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**

ПІБ викладача	Посада	Структурний підрозділ, у якому працює викладач	Інформація про кваліфікацію викладача	Стаж науково-педагогічної роботи	Навчальні дисципліни,що їх викладає викладач на ОП	Обгрунтування
			ЛЕ № 007629. **Освіта:** Харківський національний університет радіоелектроніки. **Спеціальність:** Кібербезпека **Кваліфікація:** магістр. 31.12.2021, диплом М21 № 089064. **Доктор філософії**, 125 – Кібербезпека та захист інформації, **Тема:** «Моделі та методи контролю цілісності та автентичності на основі каскадного алгоритму UMAC», Диплом Н23 № 001755, від 6 грудня 2023 року, Міністерство освіти і науки України, Національний авіаційний університет			**наукометричних баз, зокрема Scopus, Web of Science Core Collection** 1. Models of socio-cyber-physical systems security: monograph / S. Yevseiev, Yu. Khokhlachova, S. Ostapov, O. Laptiev and others. – Kharkiv: PC TECHNOLOGY CENTER, 2023. – 168 p. (DOI: 10.15587/978-617-7319-72-5) (Scopus) (10,5 ум. др. арк. / 0,35 ум. друк. арк. власного внеску) 2. Yevseiev, S., Havrylova, A., Milevskyi, S., Sinitsyn, I., Chalapko, V., Dukin, H., Hrebeniuk, V., Diedov, M., Bekirova, L., & Shpak, O. (2023). Development of an improved SSL/TLS protocol using post-quantum algorithms. Eastern-European Journal of Enterprise Technologies, 3(9 (123), 33–48. (DOI:10.15587/1729-4061.2023.281795/) (Scopus) (1,0 ум. др. арк. / 0,1 ум. друк. арк. власного внеску) 3. Гаврилова Алла, Хохлачова Юлія, Погорелов Володимир. Аналіз застосування гібридних крипто-кодових конструкцій для підвищення рівня стійкості геш-кодів до зламу / Алла Гаврилова, Юлія Хохлачова, Володимир Погорелов // «Безпека інформації», 2022. – Том 28. – № 2. – URL: https://jrnl.nau.edu.ua/index.php/Infosecurity (DOI: 10.18372/2225-5036.28.16953) (0,938 ум. др. арк. / 0,313 ум. друк. арк. власного внеску) 4. Havrylova Alla, Tkachov Andrii, Rahimova Irada Rahim qizi. Estimating the Efficiency of Using the Modified UMAC Algorithm / Alla Havrylova, Andrii Tkachov, Irada Rahim qizi Rahimova // 2022 IEEE 3rd KhPI Week on Advanced Technology (KhPIWeek) 03-07 October 2022 .– 2022. Kharkiv, Ukraine: Publisher: IEEE, P. 1 – 5 URL:https://ieeexplore.ieee.org/document/9916425 (Scopus) DOI: 10.1109/KhPIWeek57572.2022. 9916425 (0,625 ум. др. арк. / 0,208 ум. друк. арк. власного внеску). 5. 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). – С. 45 – 63. – URL: 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). 6. 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.

ПІБ викладача	Посада	Структурний підрозділ, у якому працює викладач	Інформація про кваліфікацію викладача	Стаж науково-педагогічної роботи	Навчальні дисципліни,що їх викладає викладач на ОП	Обгрунтування
						Shmatko // Eastern-European Journal of Enterprise Technologies. – 2019. – № 1/9 (97). – P. 27 – 38. – URL:http://webcache.googleusercontent.com/search?q=cache:E9OE7avPTy0J: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). 7. 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. URL: 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). 8. 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. – URL: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. 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

ПІБ викладача	Посада	Структурний підрозділ, у якому працює викладач	Інформація про кваліфікацію викладача	Стаж науково-педагогічної роботи	Навчальні дисципліни,що їх викладає викладач на ОП	Обґрунтування
						"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. – URL: 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. 5 захист дисертації на здобуття наукового ступеня** Диплом доктора філософії, 125 – Кібербезпека та захист інформації, тема дисертації: Моделі та методи контролю цілісності та автентичності на основі каскадного алгоритму UMAC. Диплом Н23 № 001755, від 6 грудня 2023 року, Міністерство освіти і науки України, Національний авіаційний університет. **П. 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**

ПІБ викладача	Посада	Структурний підрозділ, у якому працює викладач	Інформація про кваліфікацію викладача	Стаж науково-педагогічної роботи	Навчальні дисципліни,що їх викладає викладач на ОП	Обгрунтування
						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. – URLhttp://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). 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_o=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). 5. Гаврилова А. А. Анализ состояния блокчейн-проектов на рынке украинских сервисов / А. А. Гаврилова // Material of International

ПІБ викладача	Посада	Структурний підрозділ, у якому працює викладач	Інформація про кваліфікацію викладача	Стаж науково-педагогічної роботи	Навчальні дисципліни,що їх викладає викладач на ОП	Обгрунтування
						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). 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: BCPmofo M5hwJ: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). 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.googleuser content.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. 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. – URL: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). 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/

ПІБ викладача	Посада	Структурний підрозділ, у якому працює викладач	Інформація про кваліфікацію викладача	Стаж науково-педагогічної роботи	Навчальні дисципліни,що їх викладає викладач на ОП	Обгрунтування
						iblock/431/Mono_Shmatko.pdf (0,25 ум. др. арк. / 0,125 ум. друк. арк. власного внеску). 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). 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). 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%3D 183%26article-id%3D419827+&cd=2&hl=ru&ct=clnk &gl=ua (0,6 ум. др. арк. / 0,6 ум. друк. арк. власного внеску). 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). 14. Гаврилова А. А. Формування кортежу показників оцінки блокчейн-гаманців / Н. О. Бринза, А. А. Гаврилова // Матеріали

ПІБ викладача	Посада	Структурний підрозділ, у якому працює викладач	Інформація про кваліфікацію викладача	Стаж науково-педагогічної роботи	Навчальні дисципліни,що їх викладає викладач на ОП	Обґрунтування
						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) 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). 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). 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). 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). – URL:http://webcache.googleuser content.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.

ПІБ викладача	Посада	Структурний підрозділ, у якому працює викладач	Інформація про кваліфікацію викладача	Стаж науково-педагогічної роботи	Навчальні дисципліни,що їх викладає викладач на ОП	Обґрунтування
						арк. / 0,077 ум. друк. арк. власного внеску) 19. Yevseiev Serhii, Havrylova Alla, Olha Korol, Dmitriiev Oleh, Nesmiian Oleksii, Yufa Yevhen, Hrebennikov Asadi. Research of collision properties of the modified UMAC algorithm on crypto-code constructions / Serhii Yevseiev, Alla Havrylova, Olha Korol, Oleh Dmitriiev, Oleksii Nesmiian, Yevhen Yufa, Asadi Hrebennikov // "EUREKA: Physics and Engineering". – 2022. – Number 1 (38), P. 34 – 43. https://journal.eu-jr.eu/engineering/article/view/2213 – URL:https://journal.eu-jr.eu/engineering/article/view/ 2213 (0,625 ум. др. арк. / 0,089 ум. друк. арк. власного внеску) (DOI: 10.21303/2461-4262. 2021.002213) 20. Євсеєв С. П., Гаврилова А. А. Перевірка на колізійність геш-кодів які сформовано за допомогою алгоритму UMAC на крипто-кодових конструкціях / С. П. Євсеєв, А. А. Гаврилова // "Математика. Інформаційні технології. Освіта"; тези доповідей на XI Міжнародній науково-практичній конференції, Луцьк-Світязь, 3 – 5 червня 2022 р. – Луцьк, 2022. – С. 66 – 68. 21. Гаврилова А. А., Король О. Г., Євсеєв С. П. Дослідження колізійних властивостей модифікованого алгоритму UMAC на криптокодових конструкціях / А.А. Гаврилова, О.Г. Король, С.П. Євсеєв // Інформатика, управління та штучний інтелект; тези дев'ятої міжнародної науково-технічної конференції, Харків – Краматорськ, 2022. – URL:http://repository .kpi.kharkov.ua/bitstream/KhPI-Press/57536/1/Havry-lova_Doslidzhennia_2022.pdf. **П. 19 діяльність за спеціальністю у формі участі у професійних та/або громадських об'єднаннях** член Громадської організації "СХІДНО-ЄВРОПЕЙСЬКЕ НАУКОВЕ ТОВАРИСТВО" з 20.05.2022р. посвідчення № ES 055.
Мілевський Станіслав Валерійович	доцент	кафедра кібербезпеки НТУ «ХПІ»	**Освіта:** 1). Харківський державний економічний університет. 2). Національний авіаційний університет. **Спеціальність:** 1). Економіка підприємства. 2). Кібербезпека.	22 рік	СП 14. Основи математичного моделювання систем безпеки СП 19. Організація і безпека баз даних СП 22. Комплексний тренінг	**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.

ПІБ викладача	Посада	Структурний підрозділ, у якому працює викладач	Інформація про кваліфікацію викладача	Стаж науково-педагогічної роботи	Навчальні дисципліни,що їх викладає викладач на ОП	Обгрунтування
			Кваліфікація: 1). Економіст. Диплом спеціаліста ХА №16790511 від 30.06.2001. 2). Магістр з кібербезпеки. Диплом М21№ 067385 від 31.12.2021. **Кандидат економічних наук,** 051 Економіка (08.03.02 – економіко-математичне моделювання) диплом ДК №033701 від 13.04.2006 р. **Тема:** "Моделі оцінки конкурентоспроможності підприємств". **Доцент** кафедри кібербезпеки та інформаційних технологій АД№006043 від 26.11.2020 р.			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

ПІБ викладача	Посада	Структурний підрозділ, у якому працює викладач	Інформація про кваліфікацію викладача	Стаж науково-педагогічної роботи	Навчальні дисципліни,що їх викладає викладач на ОП	Обгрунтування
						видання, Scopus) 2 ум. друк. арк. / 0,2 ум. др. 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 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.)

ПІБ викладача	Посада	Структурний підрозділ, у якому працює викладач	Інформація про кваліфікацію викладача	Стаж науково-педагогічної роботи	Навчальні дисципліни,що їх викладає викладач на ОП	Обґрунтування
						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-

ПІБ викладача	Посада	Структурний підрозділ, у якому працює викладач	Інформація про кваліфікацію викладача	Стаж науково-педагогічної роботи	Навчальні дисципліни,що їх викладає викладач на ОП	Обгрунтування
						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.
Погасій Сергій Сергійович	доцент	кафедра кібербезпеки НТУ «ХПІ»	**Освіта:** 1). Харківський державний економічний університет. 2). Харківський національний університет радіоелектроніки. **Спеціальність**: 1). Фінанси і кредит. 2). Кібербезпека. **Кваліфікація:** 1). Економіст. 25.06.1999 року,	19 років	СП 9. Основи побудови та захисту сучасних операційних систем СП 12. Основи побудови та захисту мікропроцесорних систем СП 25. Безпека інтернет-речей.	**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:

ПІБ викладача	Посада	Структурний підрозділ, у якому працює викладач	Інформація про кваліфікацію викладача	Стаж науково-педагогічної роботи	Навчальні дисципліни,що їх викладає викладач на ОП	Обґрунтування
			диплом ХА №11869959. 2). Магістр з кібербезпеки. 31.12.2021 р. диплом М21 №089409 **Кандидат економічних наук,** 08.00.03 - економіка та управління національним, 28.04.2009 р. ДК №051003. **Тема:** "Прогнозування динаміка валютного курсу на основі нелінійних моделей". **Доцент** кафедри кібербезпеки та інформаційних технологій АД№006046 від 26.11.2020 р.			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. **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

ПІБ викладача	Посада	Структурний підрозділ, у якому працює викладач	Інформація про кваліфікацію викладача	Стаж науково-педагогічної роботи	Навчальні дисципліни,що їх викладає викладач на ОП	Обгрунтування
						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. –

ПІБ викладача	Посада	Структурний підрозділ, у якому працює викладач	Інформація про кваліфікацію викладача	Стаж науково-педагогічної роботи	Навчальні дисципліни,що їх викладає викладач на ОП	Обґрунтування
						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.

ПІБ викладача	Посада	Структурний підрозділ, у якому працює викладач	Інформація про кваліфікацію викладача	Стаж науково-педагогічної роботи	Навчальні дисципліни,що їх викладає викладач на ОП	Обґрунтування
						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

ПІБ викладача	Посада	Структурний підрозділ, у якому працює викладач	Інформація про кваліфікацію викладача	Стаж науково-педагогічної роботи	Навчальні дисципліни,що їх викладає викладач на ОП	Обґрунтування
						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/1bjtYbubJ0VA66EhjL8JYSrtFlN-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" **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.
Хвостенко Владислав Сергійович	доцент	кафедра кібербезпеки НТУ «ХПІ»	**Освіта:** 1) ХНЕУ ім. С. Кузнеця: **Спеціальність** "фінанси" Кваліфікація: Диплом магістра № ХА № 29837486, 2006 рік. **Спеціальність** економічна статистика. Диплом спеціаліста № ХА № 33040881, 2007 2) L'UNIVERSITÉ LYON 2. FRANCAISE: DIPLOME de MASTER SCIENCES ECONOMIQUES ET DE GESTION. INFORMATIQUE DÉCISIONNELLE №	16 років	СПЗ. Кібербезпека. Правові основи та технології.	**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

ПІБ викладача	Посада	Структурний підрозділ, у якому працює викладач	Інформація про кваліфікацію викладача	Стаж науково-педагогічної роботи	Навчальні дисципліни,що їх викладає викладач на ОП	Обґрунтування
			LYONII 7470721, 2007 р. 3) Інститут інтелектуальної власності НУ “Одеська юридична академія”, м. Київ Магістр зі спеціальності “Інтелектуальна власність”. Диплом КВ №47583761, 2014. Кандидат економічних наук, 08.00.08 – Гроші, фінанси і кредит, Диплом № ДК № 008014, 14 червня 2012 р. Тема: “Формування стратегії фінансового розвитку підприємств промисловості”. Доцент кафедри кібербезпеки та інформаційних технологій АД №006909 від 09.02.2021 р.			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

ПІБ викладача	Посада	Структурний підрозділ, у якому працює викладач	Інформація про кваліфікацію викладача	Стаж науково-педагогічної роботи	Навчальні дисципліни,що їх викладає викладач на ОП	Обґрунтування
						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**

ПІБ викладача	Посада	Структурний підрозділ, у якому працює викладач	Інформація про кваліфікацію викладача	Стаж науково-педагогічної роботи	Навчальні дисципліни,що їх викладає викладач на ОП	Обґрунтування
						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:

ПІБ викладача	Посада	Структурний підрозділ, у якому працює викладач	Інформація про кваліфікацію викладача	Стаж науково-педагогічної роботи	Навчальні дисципліни,що їх викладає викладач на ОП	Обґрунтування
						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 **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/

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

Назва освітнього компонента		
Результати навчання	**Методи навчання**	**Форми оцінювання**
Історія та культури України		
РН 1 – застосовувати знання державної та іноземних мов з метою забезпечення ефективності професійної комунікації; РН 54 – усвідомлювати цінності громадянського (вільного демократичного) суспільства та необхідність його сталого розвитку, верховенства права, прав і свобод людини і громадянина в Україні.	Словесні: опитування, бесіда, дискусія Наочні: презентація, використання відео- та аудіо джерел і матеріалів етнографічного музею кафедри «Слобожанські скарби», виставкових експозицій музеїв та художніх Практичні: конспектування та обговорення історичних, культурологічних та філософських джерел Інтерактивні лекції з презентаціями, дискусії, практичні заняття виконання індивідуальних творчих завдань на семінарах, тестування, написання рефератів Підготовка тез на студентську науково-практичну конференцію. Підготовка історичних есе на проблемні питання історії та культури України.	Оцінювання знань на практичних заняттях (семінарах) у тому числі доповіді, участь у дискусіях тощо (CAS). Письмове завдання – контрольна робота (CAS) Написання та захист історичних есе (CAS) Написання та захист реферату (CAS) Складання екзамену (FAS)
Українська мова (за професійним спрямуванням)		
РН 1 – застосовувати знання державної та іноземних мов з метою забезпечення ефективності професійної комунікації; РН 54 – усвідомлювати цінності громадянського (вільного демократичного) суспільства та необхідність його сталого розвитку, верховенства права, прав і свобод людини і громадянина в Україні.	- виклад нового навчального матеріалу; пояснення; бесіда (вступна, репродуктивна, евристична, контрольна); - таблиці, схеми, роздаткові матеріали, робота з навчальними посібниками; - виконання вправ і письмових завдань, перекладання та редагування фахових текстів; - репродуктивні та проблемно-пошукові методи; - пізнавальні ігри, навчальні дискусії та диспути, аналіз ситуацій у професійній діяльності тощо.	Оцінювання знань на практичних заняттях, перевірка конспектів, виконаних вправ і завдань, рефератів, усні опитування, тестування (CAS); іспит у формі виконання залікових завдань (FAS)

Іноземна мова		
РН 1 – застосовувати знання державної та іноземних мов з метою забезпечення ефективності професійної комунікації; РН 54 – усвідомлювати цінності громадянського (вільного демократичного) суспільства та необхідність його сталого розвитку, верховенства права, прав і свобод людини і громадянина в Україні.	Бесіди (з викладачем та одногрупниками), робота в парах та групах, виконання ситуативних завдань, робота за підручниками і посібниками, написання листів, документів, анотацій, рефератів, пошук інформації в друкованій літературі за завданням, виступ з короткою презентацією тощо	Письмові індивідуальні завдання (CAS), оцінювання знань на практичних заняттях (CAS), написання напівформальних листів (CAS), онлайн-тести (CAS), заповнення анкет (CAS), написання рефератів (CAS), написання листа (FAS) Підсумковий контроль у вигляді екзамену.
Фізика		
РН 1 – застосовувати знання державної та іноземних мов з метою забезпечення ефективності професійної комунікації; РН 2 – організовувати власну професійну діяльність, обирати оптимальні методи та способи розв'язування складних спеціалізованих задач та практичних проблем у професійній діяльності, оцінювати їхню ефективність; РН 3 – використовувати результати самостійного пошуку, аналізу та синтезу інформації з різних джерел для ефективного рішення спеціалізованих задач професійної діяльності; РН 4 – аналізувати, аргументувати, приймати рішення при розв'язанні складних спеціалізованих задач та практичних проблем у професійній діяльності, які характеризуються комплексністю та неповною визначеністю умов, відповідати за прийняті рішення; РН 5 – адаптуватися в умовах частої зміни технологій професійної діяльності, прогнозувати кінцевий результат; РН 6 – критично осмислювати основні теорії, принципи, методи і поняття у навчанні та професійній діяльності; РН 7 – діяти на основі законодавчої та	Словесні (лекції), наочні (ілюстрації та демонстрації із застосуванням експериментального обладнання, мультимедіа, науково-популярних фільмів тощо) і практичні (лабораторний експеримент, практичні роботи), самостійна робота, консультації.	Поточне оцінювання CAS: Оцінювання роботи студентів у процесі практичних занять. Підсумкове оцінювання FAS: Екзамен

нормативно-правової бази України та вимог відповідних стандартів, у тому числі міжнародних в галузі інформаційної та /або кібербезпеки; РН 8 – готувати пропозиції до нормативних актів щодо забезпечення інформаційної та /або кібербезпеки; РН 9 – проваджувати процеси, що базуються на національних та міжнародних стандартах, виявлення, ідентифікації, аналізу та реагування на інциденти інформаційної та/або кібербезпеки; РН 17 – забезпечувати процеси захисту та функціонування інформаційно-телекомунікаційних (автоматизованих) систем на основі практик, навичок та знань, щодо структурних (структурно-логічних) схем, топології мережі, сучасних архітектур та моделей захисту електронних інформаційних ресурсів з відображенням взаємозв'язків та інформаційних потоків, процесів для внутрішніх і віддалених компонент; РН 19 – застосовувати теорії та методи захисту для забезпечення безпеки інформації в інформаційно-телекомунікаційних системах; РН 28 – аналізувати та проводити оцінку ефективності та рівня захищеності ресурсів різних класів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах в ході проведення випробувань згідно встановленої політики інформаційної та\або кібербезпеки. РН 43 – застосовувати національні та міжнародні регулюючі акти в сфері інформаційної безпеки та/ або		

кібербезпеки для розслідування інцидентів РН 54 – усвідомлювати цінності громадянського (вільного демократичного) суспільства та необхідність його сталого розвитку, верховенства права, прав і свобод людини і громадянина в Україні.		
Філософія		
РН 1 – застосовувати знання державної та іноземних мов з метою забезпечення ефективності професійної комунікації; РН 54 – усвідомлювати цінності громадянського (вільного демократичного) суспільства та необхідність його сталого розвитку, верховенства права, прав і свобод людини і громадянина в Україні.	Лекції з презентаціями, дискусії, практичні заняття (семінари, практикуми), виконання індивідуальної роботи (реферат, есе, участь у конференціях та спеціалізованих семінарах, робота з оригінальними роботами з філософії)	Оцінювання знань на семінарських заняттях (CAS), оцінювання контрольних робіт, тестів (CAS), перевірка лекційного конспекту (CAS), оцінювання індивідуального завдання (CAS), екзамен (FAS)
Вища математика		
РН 1 – Застосовувати знання державної та іноземних мов з метою забезпечення ефективності професійної комунікації. РН 2 – організовувати власну професійну діяльність, обирати оптимальні методи та способи розв’язування складних спеціалізованих задач та практичних проблем у професійній діяльності, оцінювати їхню ефективність; РН 3 – використовувати результати самостійного пошуку, аналізу та синтезу інформації з різних джерел для ефективного рішення спеціалізованих задач професійної діяльності; РН 4 – аналізувати, аргументувати, приймати рішення при розв’язанні складних спеціалізованих задач та практичних проблем у професійній діяльності, які характеризуються	Інтерактивні лекції з презентаціями, «багтрекинг лекцій», практичні заняття із застосуванням групової динаміки, проектне навчання	Письмові індивідуальні завдання до розрахунково-графічних робіт (CAS), оцінювання знань на практичних заняттях (CAS), експрес-опитування (CAS), онлайн тестування (CAS), підсумковий/семестровий контроль у формі семестрового екзамену, відповідно до графіку навчального процесу (FAS)

комплексністю та неповною визначеністю умов, відповідати за прийняті рішення; РН 5 – адаптуватися в умовах частої зміни технологій професійної діяльності, прогнозувати кінцевий результат; РН 7 – діяти на основі законодавчої та нормативно-правової бази України та вимог відповідних стандартів, у тому числі міжнародних в галузі інформаційної та /або кібербезпеки; РН 8 – готувати пропозиції до нормативних актів щодо забезпечення інформаційної та /або кібербезпеки; РН 53 – вирішувати задачі аналізу програмного коду на наявність можливих загроз.		
Фізичне виховання		
РН–54 – усвідомлювати цінності громадянського (вільного демократичного) суспільства та необхідність його сталого розвитку, верховенства права, прав і свобод людини і громадянина в Україні.	Словесні, наочні, практичні; методи організації та здійснення навчально-пізнавальної діяльності; методи стимулювання і мотивації навчально-пізнавальної діяльності; методи контролю та самоконтролю у навчанні; бінарні (подвійні) методи навчання	Залік
Вступ до спеціальності. Ознайомча практика		
РН 1 – застосовувати знання державної та іноземних мов з метою забезпечення ефективності професійної комунікації; РН 2 – організовувати власну професійну діяльність, обирати оптимальні методи та способи розв’язування складних спеціалізованих задач та практичних проблем у професійній діяльності, оцінювати їхню ефективність; РН 3 – використовувати результати самостійного пошуку, аналізу та синтезу інформації з різних джерел для	Пояснювально-ілюстративний (інформаційно-рецептивний) та репродуктивний	Захист практичних робіт, експрес-опитування, контрольні роботи, залік

ефективного рішення спеціалізованих задач професійної діяльності; РН 4 – аналізувати, аргументувати, приймати рішення при розв'язанні складних спеціалізованих задач та практичних проблем у професійній діяльності, які характеризуються комплексністю та неповною визначеністю умов, відповідати за прийняті рішення; РН 5 – адаптуватися в умовах частої зміни технологій професійної діяльності, прогнозувати кінцевий результат; РН 6 – критично осмислювати основні теорії, принципи, методи і поняття у навчанні та професійній діяльності; РН 7 – діяти на основі законодавчої та нормативно-правової бази України та вимог відповідних стандартів, у тому числі міжнародних в галузі інформаційної та /або кібербезпеки; РН 8 – готувати пропозиції до нормативних актів щодо забезпечення інформаційної та /або кібербезпеки; РН 9 – впроваджувати процеси, що базуються на національних та міжнародних стандартах, виявлення, ідентифікації, аналізу та реагування на інциденти інформаційної та/або кібербезпеки; РН 10 – виконувати аналіз та декомпозицію інформаційно-телекомунікаційних систем; РН 11 – виконувати аналіз зв'язків між інформаційними процесами на віддалених обчислювальних системах; РН 12 – розробляти моделі загроз та порушника; РН 13 – аналізувати проекти інформаційно-телекомунікаційних систем		

базуючись на стандартизованих технологіях та протоколах передачі даних; РН 14 – вирішувати завдання захисту програм та інформації, що обробляється в інформаційно-телекомунікаційних системах програмно-апаратними засобами та давати оцінку результативності якості прийнятих рішень; РН 15 – використовувати сучасне програмно-апаратне забезпечення інформаційно-комунікаційних технологій; РН 16 – реалізовувати комплексні системи захисту інформації в автоматизованих системах (АС) організації (підприємства) відповідно до вимог нормативно-правових документів; РН 17 – забезпечувати процеси захисту та функціонування інформаційно-телекомунікаційних (автоматизованих) систем на основі практик, навичок та знань, щодо структурних (структурно-логічних) схем, топології мережі, сучасних архітектур та моделей захисту електронних інформаційних ресурсів з відображенням взаємозв'язків та інформаційних потоків, процесів для внутрішніх і віддалених компонент; РН 18 – використовувати програмні та програмно-апаратні комплекси захисту інформаційних ресурсів; РН 19 – застосовувати теорії та методи захисту для забезпечення безпеки інформації в інформаційно-телекомунікаційних системах; РН 20 – забезпечувати функціонування спеціального програмного забезпечення, щодо захисту інформації від руйнуючих програмних впливів, руйнуючих кодів в		

інформаційно-телекомунікаційних системах; РН 21 – вирішувати задачі забезпечення та супроводу (в.т. числі: огляд, тестування, підзвітність) системи управління доступом згідно встановленої політики безпеки в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах; РН 22 – вирішувати задачі управління процедурами ідентифікації, автентифікації, авторизації процесів і користувачів в інформаційно-телекомунікаційних системах згідно встановленої політики інформаційної і\або кібербезпеки; РН 23 – реалізовувати заходи з протидії отриманню несанкціонованого доступу до інформаційних ресурсів і процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах; РН 24 – вирішувати задачі управління доступом до інформаційних ресурсів та процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах на основі моделей управління доступом (мандатних, дискреційних, рольових); РН 25 – забезпечувати введення підзвітності системи управління доступом до електронних інформаційних ресурсів і процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах з використанням журналів реєстрації подій, їх аналізу та встановлених процедур захисту; РН 26 – впроваджувати заходи та		

забезпечувати реалізацію процесів попередження отриманню несанкціонованого доступу і захисту інформаційних, інформаційно-телекомунікаційних (автоматизованих) систем на основі еталонної моделі взаємодії відкритих систем; РН 27 – вирішувати задачі захисту потоків даних в інформаційних, інформаційно-телекомунікаційних (автоматизованих) системах; РН 28 – аналізувати та проводити оцінку ефективності та рівня захищеності ресурсів різних класів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах в ході проведення випробувань згідно встановленої політики інформаційної та\або кібербезпеки; РН 29 – здійснювати оцінювання можливості реалізації потенційних загроз інформації, що обробляється в інформаційно-телекомунікаційних системах та ефективності використання комплексів засобів захисту в умовах реалізації загроз різних класів; РН 30 – здійснювати оцінювання можливості несанкціонованого доступу до елементів інформаційно-телекомунікаційних систем; РН 31 – застосовувати теорії та методи захисту для забезпечення безпеки елементів інформаційно-телекомунікаційних систем; РН 32 – вирішувати задачі управління процесами відновлення штатного функціонування інформаційно-телекомунікаційних систем з використанням процедур резервування		

згідно встановленої політики безпеки; РН 33 – вирішувати задачі забезпечення безперервності бізнес процесів організації на основі теорії ризиків; РН 34 – приймати участь у розробці та впровадженні стратегії інформаційної безпеки та/або кібербезпеки відповідно до цілей і завдань організації; РН 35 – вирішувати задачі забезпечення та супроводу комплексних систем захисту інформації, а також протидії несанкціонованому доступу до інформаційних ресурсів і процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах згідно встановленої політики інформаційної і\або кібербезпеки; РН 37 – вимірювати параметри небезпечних та завадових сигналів під час інструментального контролю процесів захисту інформації та визначати ефективність захисту інформації від витоку технічними каналами відповідно до вимог нормативних документів системи технічного захисту інформації; РН 38 – інтерпретувати результати проведення спеціальних вимірювань з використанням технічних засобів, контролю характеристик інформаційно-телекомунікаційних систем відповідно до вимог нормативних документів системи технічного захисту інформації; РН 41 – забезпечувати неперервність процесу ведення журналів реєстрації подій та інцидентів на основі автоматизованих процедур; РН 42 – впроваджувати процеси виявлення, ідентифікації, аналізу та реагування на інциденти інформаційної		

і/або кібербезпеки; РН 43 – застосовувати національні та міжнародні регулюючі акти в сфері інформаційної безпеки та/ або кібербезпеки для розслідування інцидентів; РН 44 – вирішувати задачі забезпечення безперервності бізнес-процесів організації на основі теорії ризиків та встановленої системи управління інформаційною безпекою, згідно з вітчизняними та міжнародними вимогами та стандартами; РН 45 – застосовувати ріні класи політик інформаційної безпеки та/ або кібербезпеки, що базуються на ризик-орієнтованому контролі доступу до інформаційних активів; РН 46 – здійснювати аналіз та мінімізацію ризиків обробки інформації в інформаційно-телекомунікаційних системах. РН 47 – вирішувати задачі захисту інформації, що обробляється в інформаційно-телекомунікаційних системах з використанням сучасних методів та засобів криптографічного захисту інформації; РН 48 – виконувати впровадження та підтримку систем виявлення вторгнень та використовувати компоненти криптографічного захисту для забезпечення необхідного рівня захищеності інформації в інформаційно-телекомунікаційних системах; РН 49 – забезпечувати належне функціонування системи моніторингу інформаційних ресурсів і процесів в інформаційно-телекомунікаційних системах;		

РН 50 – забезпечувати функціонування програмних та програмно-апаратних комплексів виявлення вторгнень різних рівнів та класів (статистичних, сигнатурних, статистично-сигнатурних); РН 51 – підтримувати працездатність та забезпечувати конфігурування систем виявлення вторгнень в інформаційно-телекомунікаційних системах; РН 52 – використовувати інструментарій для моніторингу процесів в інформаційно-телекомунікаційних системах. РН 53 – вирішувати задачі аналізу програмного коду на наявність можливих загроз; РН 54 – усвідомлювати цінності громадянського (вільного демократичного) суспільства та необхідність його сталого розвитку, верховенства права, прав і свобод людини і громадянина в Україні.		
Основи програмування		
РН 1 – застосовувати знання державної та іноземних мов з метою забезпечення ефективності професійної комунікації; РН 2 – організовувати власну професійну діяльність, обирати оптимальні методи та способи розв’язування складних спеціалізованих задач та практичних проблем у професійній діяльності, оцінювати їхню ефективність; РН 3 – використовувати результати самостійного пошуку, аналізу та синтезу інформації з різних джерел для ефективного рішення спеціалізованих задач професійної діяльності; РН 4 – аналізувати, аргументувати, приймати рішення при розв’язанні складних спеціалізованих задач та	Пояснювально-ілюстративний (інформаційно-рецептивний) та репродуктивний	Захист лабораторних робіт, контрольні роботи, тестування, екзамен

практичних проблем у професійній діяльності, які характеризуються комплексністю та неповною визначеністю умов, відповідати за прийняті рішення; РН 5 – адаптуватися в умовах частої зміни технологій професійної діяльності, прогнозувати кінцевий результат; РН 7 – діяти на основі законодавчої та нормативно-правової бази України та вимог відповідних стандартів, у тому числі міжнародних в галузі інформаційної та /або кібербезпеки; РН 8 – готувати пропозиції до нормативних актів щодо забезпечення інформаційної та /або кібербезпеки; РН 9 – впроваджувати процеси, що базуються на національних та міжнародних стандартах, виявлення, ідентифікації, аналізу та реагування на інциденти інформаційної та/або кібербезпеки; РН 10 – виконувати аналіз та декомпозицію інформаційно-телекомунікаційних систем; РН 11 – виконувати аналіз зв'язків між інформаційними процесами на віддалених обчислювальних системах; РН 12 – розробляти моделі загроз та порушника; РН 13 – аналізувати проекти інформаційно-телекомунікаційних систем базуючись на стандартизованих технологіях та протоколах передачі даних; РН 14 – вирішувати завдання захисту програм та інформації, що обробляється в інформаційно-телекомунікаційних системах програмно-апаратними засобами та давати оцінку результативності якості		

прийнятих рішень; РН 15 – використовувати сучасне програмно-апаратне забезпечення інформаційно-комунікаційних технологій; РН 16 – реалізовувати комплексні системи захисту інформації в автоматизованих системах (АС) організації (підприємства) відповідно до вимог нормативно-правових документів; РН 17 – забезпечувати процеси захисту та функціонування інформаційно-телекомунікаційних (автоматизованих) систем на основі практик, навичок та знань, щодо структурних (структурно-логічних) схем, топології мережі, сучасних архітектур та моделей захисту електронних інформаційних ресурсів з відображенням взаємозв'язків та інформаційних потоків, процесів для внутрішніх і віддалених компонент; РН 18 – використовувати програмні та програмно-апаратні комплекси захисту інформаційних ресурсів; РН 19 – застосовувати теорії та методи захисту для забезпечення безпеки інформації в інформаційно-телекомунікаційних системах; РН 20 – забезпечувати функціонування спеціального програмного забезпечення, щодо захисту інформації від руйнуючих програмних впливів, руйнуючих кодів в інформаційно-телекомунікаційних системах; РН 21 – вирішувати задачі забезпечення та супроводу (в.т. числі: огляд, тестування, підзвітність) системи управління доступом згідно встановленої політики безпеки в інформаційних та інформаційно-телекомунікаційних		

(автоматизованих) системах; РН 22 – вирішувати задачі управління процедурами ідентифікації, автентифікації, авторизації процесів і користувачів в інформаційно-телекомунікаційних системах згідно встановленої політики інформаційної і\або кібербезпеки; РН 23 – реалізовувати заходи з протидії отриманню несанкціонованого доступу до інформаційних ресурсів і інформаційно-телекомунікаційних (автоматизованих) системах; РН 24 – вирішувати задачі управління доступом до інформаційних ресурсів та процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах на основі моделей управління доступом (мандатних, дискреційних, рольових); РН 25 – забезпечувати введення підзвітності системи управління доступом до електронних інформаційних ресурсів і процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах з використанням журналів реєстрації подій, їх аналізу та встановлених процедур захисту; РН 26 – впроваджувати заходи та забезпечувати реалізацію процесів попередження отриманню несанкціонованого доступу і захисту інформаційних, інформаційно-телекомунікаційних (автоматизованих) систем на основі еталонної моделі взаємодії відкритих систем; РН 27 – вирішувати задачі захисту потоків даних в інформаційних,		

інформаційно-телекомунікаційних (автоматизованих) системах; РН 28 – аналізувати та проводити оцінку ефективності та рівня захищеності ресурсів різних класів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах в ході проведення випробувань згідно встановленої політики інформаційної та\або кібербезпеки; РН 29 – здійснювати оцінювання можливості реалізації потенційних загроз інформації, що обробляється в інформаційно-телекомунікаційних системах та ефективності використання комплексів засобів захисту в умовах реалізації загроз різних класів; РН 30 – здійснювати оцінювання можливості несанкціонованого доступу до елементів інформаційно-телекомунікаційних систем; РН 32 – вирішувати задачі управління процесами відновлення штатного функціонування інформаційно-телекомунікаційних систем з використанням процедур резервування згідно встановленої політики безпеки; РН 33 – вирішувати задачі забезпечення безперервності бізнес процесів організації на основі теорії ризиків; РН 34 – приймати участь у розробці та впровадженні стратегії інформаційної безпеки та/або кібербезпеки відповідно до цілей і завдань організації; РН 35 – вирішувати задачі забезпечення та супроводу комплексних систем захисту інформації, а також протидії несанкціонованому доступу до інформаційних ресурсів і процесів в		

інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах згідно встановленої політики інформаційної і\або кібербезпеки; РН 41 – забезпечувати неперервність процесу ведення журналів реєстрації подій та інцидентів на основі автоматизованих процедур; РН 42 – впроваджувати процеси виявлення, ідентифікації, аналізу та реагування на інциденти інформаційної і/або кібербезпеки; РН 43 – застосовувати національні та міжнародні регулюючі акти в сфері інформаційної безпеки та/ або кібербезпеки для розслідування інцидентів; РН 44 – вирішувати задачі забезпечення безперервності бізнес-процесів організації на основі теорії ризиків та встановленої системи управління інформаційною безпекою, згідно з вітчизняними та міжнародними вимогами та стандартами; РН 45 – застосовувати різні класи політик інформаційної безпеки та/ або кібербезпеки, що базуються на ризик-орієнтованому контролі доступу до інформаційних активів; РН 46 – здійснювати аналіз та мінімізацію ризиків обробки інформації в інформаційно-телекомунікаційних системах; РН 47 – вирішувати задачі захисту інформації, що обробляється в інформаційно-телекомунікаційних системах з використанням сучасних методів та засобів криптографічного захисту інформації; РН 48 – виконувати впровадження та		

підтримку систем виявлення вторгнень та використовувати компоненти криптографічного захисту для забезпечення необхідного рівня захищеності інформації в інформаційно-телекомунікаційних системах; РН 49 – забезпечувати належне функціонування системи моніторингу інформаційних ресурсів і процесів в інформаційно-телекомунікаційних системах; РН 50 – забезпечувати функціонування програмних та програмно-апаратних комплексів виявлення вторгнень різних рівнів та класів (статистичних, сигнатурних, статистично-сигнатурних); РН 51 – підтримувати працездатність та забезпечувати конфігурування систем виявлення вторгнень в інформаційно-телекомунікаційних системах; РН 52 – використовувати інструментарій для моніторингу процесів в інформаційно-телекомунікаційних системах; РН 53 – вирішувати задачі аналізу програмного коду на наявність можливих загроз; РН 54 – усвідомлювати цінності громадянського (вільного демократичного) суспільства та необхідність його сталого розвитку, верховенства права, прав і свобод людини і громадянина в Україні.		
Кібербезпека. Правові основи та технології.		
РН–1. Застосовувати знання державної та іноземних мов з метою забезпечення ефективності професійної комунікації; РН–2. Організовувати власну професійну діяльність, обирати оптимальні методи та способи розв’язування складних	Пояснювально-ілюстративний (інформаційно-рецептивний) та репродуктивний	Захист практичних робіт, контрольні роботи, тестування, презентації докладів за темами лекційних занять, залік

спеціалізованих задач та практичних проблем у професійній діяльності, оцінювати їхню ефективність; РН–3. Використовувати результати самостійного пошуку, аналізу та синтезу інформації з різних джерел для ефективного рішення спеціалізованих задач професійної діяльності. РН–4. Аналізувати, аргументувати, приймати рішення при розв'язанні складних спеціалізованих задач та практичних проблем у професійній діяльності, які характеризуються комплексністю та неповною визначеністю умов, відповідати за прийняті рішення. РН–7. Діяти на основі законодавчої та нормативно-правової бази України та вимог відповідних стандартів, у тому числі міжнародних в галузі інформаційної та /або кібербезпеки. РН–8. Готувати пропозиції до нормативних актів щодо забезпечення інформаційної та /або кібербезпеки. РН–9. Впроваджувати процеси, що базуються на національних та міжнародних стандартах, виявлення, ідентифікації, аналізу та реагування на інциденти інформаційної та/або кібербезпеки. РН–10. Виконувати аналіз та декомпозицію інформаційно-телекомунікаційних систем. РН–11. Виконувати аналіз зв'язків між інформаційними процесами на віддалених обчислювальних системах. РН–12. Розробляти моделі загроз та порушника. РН–16. Реалізовувати комплексні системи захисту інформації в автоматизованих		

системах (АС) організації (підприємства) відповідно до вимог нормативно-правових документів. РН–18. Використовувати програмні та програмно-апаратні комплекси захисту інформаційних ресурсів. РН–19. Застосовувати теорії та методи захисту для забезпечення безпеки інформації в інформаційно-телекомунікаційних системах. РН–20. Забезпечувати функціонування спеціального програмного забезпечення, щодо захисту інформації від руйнуючих програмних впливів, руйнуючих кодів в інформаційно-телекомунікаційних системах. РН–21. Вирішувати задачі забезпечення та супроводу (в.т. числі: огляд, тестування, підзвітність) системи управління доступом згідно встановленої політики безпеки в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах. РН–22. Вирішувати задачі управління процедурами ідентифікації, автентифікації, авторизації процесів і користувачів в інформаційно-телекомунікаційних системах згідно встановленої політики інформаційної і\або кібербезпеки. РН–24. Вирішувати задачі управління доступом до інформаційних ресурсів та процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах на основі моделей управління доступом (мандатних, дискреційних, рольових). РН–27. Вирішувати задачі захисту потоків даних в інформаційних, інформаційно-		

телекомунікаційних (автоматизованих) системах. РН–32. Вирішувати задачі управління процесами відновлення штатного функціонування інформаційно-телекомунікаційних систем з використанням процедур резервування згідно встановленої політики безпеки. РН–33. Вирішувати задачі забезпечення безперервності бізнес процесів організації на основі теорії ризиків. РН–34. Приймати участь у розробці та впровадженні стратегії інформаційної безпеки та/або кібербезпеки відповідно до цілей і завдань організації. РН–35. Вирішувати задачі забезпечення та супроводу комплексних систем захисту інформації, а також протидії несанкціонованому доступу до інформаційних ресурсів і процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах згідно встановленої політики інформаційної і\або кібербезпеки. РН–43. Застосовувати національні та міжнародні регулюючі акти в сфері інформаційної безпеки та/ або кібербезпеки для розслідування інцидентів. РН–44. Вирішувати задачі забезпечення безперервності бізнес-процесів організації на основі теорії ризиків та встановленої системи управління інформаційною безпекою, згідно з вітчизняними та міжнародними вимогами та стандартами. РН–45. Застосовувати ріні класи політик інформаційної безпеки та/ або кібербезпеки, що базуються на ризик-орієнтованому контролі доступу до		

інформаційних активів. РН–46. Здійснювати аналіз та мінімізацію ризиків обробки інформації в інформаційно-телекомунікаційних системах. РН–47. Вирішувати задачі захисту інформації, що обробляється в інформаційно-телекомунікаційних системах з використанням сучасних методів та засобів криптографічного захисту інформації. РН–48. Виконувати впровадження та підтримку систем виявлення вторгнень та використовувати компоненти криптографічного захисту для забезпечення необхідного рівня захищеності інформації в інформаційно-телекомунікаційних системах. РН–49. Забезпечувати належне функціонування системи моніторингу інформаційних ресурсів і процесів в інформаційно-телекомунікаційних системах. РН–50. Забезпечувати функціонування програмних та програмно-апаратних комплексів виявлення вторгнень різних рівнів та класів (статистичних, сигнатурних, статистично-сигнатурних). РН–51. Підтримувати працездатність та забезпечувати конфігурування систем виявлення вторгнень в інформаційно-телекомунікаційних системах. РН–52. Використовувати інструментарій для моніторингу процесів в інформаційно-телекомунікаційних системах. РН–53. Вирішувати задачі аналізу програмного коду на наявність можливих загроз.		

РН–54. Усвідомлювати цінності громадянського (вільного демократичного) суспільства та необхідність його сталого розвитку, верховенства права, прав і свобод людини і громадянина в Україні.		
Розробка та аналіз алгоритмів		
РН 1 – застосовувати знання державної та іноземних мов з метою забезпечення ефективності професійної комунікації; РН 2 – організовувати власну професійну діяльність, обирати оптимальні методи та способи розв'язування складних спеціалізованих задач та практичних проблем у професійній діяльності, оцінювати їхню ефективність; РН 3 – використовувати результати самостійного пошуку, аналізу та синтезу інформації з різних джерел для ефективного рішення спеціалізованих задач професійної діяльності; РН 4 – аналізувати, аргументувати, приймати рішення при розв'язанні складних спеціалізованих задач та практичних проблем у професійній діяльності, які характеризуються комплексністю та неповною визначеністю умов, відповідати за прийняті рішення; РН 5 – адаптуватися в умовах частої зміни технологій професійної діяльності, прогнозувати кінцевий результат; РН 6 – критично осмислювати основні теорії, принципи, методи і поняття у навчанні та професійній діяльності; РН 7 – діяти на основі законодавчої та нормативно-правової бази України та вимог відповідних стандартів, у тому числі міжнародних в галузі інформаційної та /або кібербезпеки;	Пояснювально-ілюстративний (інформаційно-рецептивний) та репродуктивний	Захист лабораторних робіт, експрес-опитування, контрольні роботи, екзамен

РН 8 – готувати пропозиції до нормативних актів щодо забезпечення інформаційної та /або кібербезпеки; РН 9 – впроваджувати процеси, що базуються на національних та міжнародних стандартах, виявлення, ідентифікації, аналізу та реагування на інциденти інформаційної та/або кібербезпеки; РН 10 – виконувати аналіз та декомпозицію інформаційно-телекомунікаційних систем; РН 11 – виконувати аналіз зв'язків між інформаційними процесами на віддалених обчислювальних системах; РН 12 – розробляти моделі загроз та порушника; РН 13 – аналізувати проекти інформаційно-телекомунікаційних систем базуючись на стандартизованих технологіях та протоколах передачі даних; РН 14 – вирішувати завдання захисту програм та інформації, що обробляється в інформаційно-телекомунікаційних системах програмно-апаратними засобами та давати оцінку результативності якості прийнятих рішень; РН 15 – використовувати сучасне програмно-апаратне забезпечення інформаційно-комунікаційних технологій; РН 16 – реалізовувати комплексні системи захисту інформації в автоматизованих системах (АС) організації (підприємства) відповідно до вимог нормативно-правових документів; РН 17 – забезпечувати процеси захисту та функціонування інформаційно-телекомунікаційних (автоматизованих)		

систем на основі практик, навичок та знань, щодо структурних (структурно-логічних) схем, топології мережі, сучасних архітектур та моделей захисту електронних інформаційних ресурсів з відображенням взаємозв'язків та інформаційних потоків, процесів для внутрішніх і віддалених компонент; РН 18 – використовувати програмні та програмно-апаратні комплекси захисту інформаційних ресурсів; РН 19 – застосовувати теорії та методи захисту для забезпечення безпеки інформації в інформаційно-телекомунікаційних системах; РН 20 – забезпечувати функціонування спеціального програмного забезпечення, щодо захисту інформації від руйнуючих програмних впливів, руйнуючих кодів в інформаційно-телекомунікаційних системах; РН 21 – вирішувати задачі забезпечення та супроводу (в.т. числі: огляд, тестування, підзвітність) системи управління доступом згідно встановленої політики безпеки в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах; РН 22 – вирішувати задачі управління процедурами ідентифікації, автентифікації, авторизації процесів і користувачів в інформаційно-телекомунікаційних системах згідно встановленої політики інформаційної і\або кібербезпеки; РН 23 – реалізовувати заходи з протидії отриманню несанкціонованого доступу до інформаційних ресурсів і процесів в інформаційних та інформаційно-		

телекомунікаційних (автоматизованих) системах; РН 24 – вирішувати задачі управління доступом до інформаційних ресурсів та процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах на основі моделей управління доступом (мандатних, дискреційних, рольових); РН 25 – забезпечувати введення підзвітності системи управління доступом до електронних інформаційних ресурсів і процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах з використанням журналів реєстрації подій, їх аналізу та встановлених процедур захисту; РН 26 – впроваджувати заходи та забезпечувати реалізацію процесів попередження отриманню несанкціонованого доступу і захисту інформаційних, інформаційно-телекомунікаційних (автоматизованих) систем на основі еталонної моделі взаємодії відкритих систем; РН 27 – вирішувати задачі захисту потоків даних в інформаційних, інформаційно-телекомунікаційних (автоматизованих) системах; РН 28 – аналізувати та проводити оцінку ефективності та рівня захищеності ресурсів різних класів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах в ході проведення випробувань згідно встановленої політики інформаційної та\або кібербезпеки; РН 29 – здійснювати оцінювання		

можливості реалізації потенційних загроз інформації, що обробляється в інформаційно-телекомунікаційних системах та ефективності використання комплексів засобів захисту в умовах реалізації загроз різних класів; РН 30 – здійснювати оцінювання можливості несанкціонованого доступу до елементів інформаційно-телекомунікаційних систем; РН 31 – застосовувати теорії та методи захисту для забезпечення безпеки елементів інформаційно-телекомунікаційних систем; РН 32 – вирішувати задачі управління процесами відновлення штатного функціонування інформаційно-телекомунікаційних систем з використанням процедур резервування згідно встановленої політики безпеки; РН 33 – вирішувати задачі забезпечення безперервності бізнес процесів організації на основі теорії ризиків; РН 34 – приймати участь у розробці та впровадженні стратегії інформаційної безпеки та/або кібербезпеки відповідно до цілей і завдань організації; РН 35 – вирішувати задачі забезпечення та супроводу комплексних систем захисту інформації, а також протидії несанкціонованому доступу до інформаційних ресурсів і процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах згідно встановленої політики інформаційної і\або кібербезпеки; РН 37 – вимірювати параметри небезпечних та завадових сигналів під час інструментального контролю процесів		

захисту інформації та визначати ефективність захисту інформації від витоку технічними каналами відповідно до вимог нормативних документів системи технічного захисту інформації; РН 38 – інтерпретувати результати проведення спеціальних вимірювань з використанням технічних засобів, контролю характеристик інформаційно-телекомунікаційних систем відповідно до вимог нормативних документів системи технічного захисту інформації; РН 41 – забезпечувати неперервність процесу ведення журналів реєстрації подій та інцидентів на основі автоматизованих процедур; РН 42 – впроваджувати процеси виявлення, ідентифікації, аналізу та реагування на інциденти інформаційної і/або кібербезпеки; РН 43 – застосовувати національні та міжнародні регулюючі акти в сфері інформаційної безпеки та/ або кібербезпеки для розслідування інцидентів; РН 44 – вирішувати задачі забезпечення безперервності бізнес-процесів організації на основі теорії ризиків та встановленої системи управління інформаційною безпекою, згідно з вітчизняними та міжнародними вимогами та стандартами; РН 45 – застосовувати ріні класи політик інформаційної безпеки та/ або кібербезпеки, що базуються на ризик-орієнтованому контролі доступу до інформаційних активів; РН 46 – здійснювати аналіз та мінімізацію ризиків обробки інформації в інформаційно-телекомунікаційних		

системах. РН 47 – вирішувати задачі захисту інформації, що обробляється в інформаційно-телекомунікаційних системах з використанням сучасних методів та засобів криптографічного захисту інформації; РН 48 – виконувати впровадження та підтримку систем виявлення вторгнень та використовувати компоненти криптографічного захисту для забезпечення необхідного рівня захищеності інформації в інформаційно-телекомунікаційних системах; РН 49 – забезпечувати належне функціонування системи моніторингу інформаційних ресурсів і процесів в інформаційно-телекомунікаційних системах; РН 50 – забезпечувати функціонування програмних та програмно-апаратних комплексів виявлення вторгнень різних рівнів та класів (статистичних, сигнатурних, статистично-сигнатурних); РН 51 – підтримувати працездатність та забезпечувати конфігурування систем виявлення вторгнень в інформаційно-телекомунікаційних системах; РН 52 – використовувати інструментарій для моніторингу процесів в інформаційно-телекомунікаційних системах. РН 53 – вирішувати задачі аналізу програмного коду на наявність можливих загроз; РН 54 – усвідомлювати цінності громадянського (вільного демократичного) суспільства та необхідність його сталого розвитку, верховенства права, прав і свобод людини		

і громадянина в Україні.		
Фізичні основи технічних засобів розвідки		
РН 1 – застосовувати знання державної та іноземних мов з метою забезпечення ефективності професійної комунікації; РН 2 – організовувати власну професійну діяльність, обирати оптимальні методи та способи розв'язування складних спеціалізованих задач та практичних проблем у професійній діяльності, оцінювати їхню ефективність; РН 3 – використовувати результати самостійного пошуку, аналізу та синтезу інформації з різних джерел для ефективного рішення спеціалізованих задач професійної діяльності; РН 4 – аналізувати, аргументувати, приймати рішення при розв'язанні складних спеціалізованих задач та практичних проблем у професійній діяльності, які характеризуються комплексністю та неповною визначеністю умов, відповідати за прийняті рішення; РН 5 – адаптуватися в умовах частої зміни технологій професійної діяльності, прогнозувати кінцевий результат; РН 6 – критично осмислювати основні теорії, принципи, методи і поняття у навчанні та професійній діяльності; РН 7 – діяти на основі законодавчої та нормативно-правової бази України та вимог відповідних стандартів, у тому числі міжнародних в галузі інформаційної та /або кібербезпеки; РН 8 – готувати пропозиції до нормативних актів щодо забезпечення інформаційної та /або кібербезпеки; РН 9 – впроваджувати процеси, що базуються на національних та	Пояснювально-ілюстративний (інформаційно-рецептивний) та репродуктивний	Захист лабораторних робіт, експрес-опитування, контрольні роботи, залік

міжнародних стандартах, виявлення, ідентифікації, аналізу та реагування на інциденти інформаційної та/або кібербезпеки; РН 10 – виконувати аналіз та декомпозицію інформаційно-телекомунікаційних систем; РН 11 – виконувати аналіз зв'язків між інформаційними процесами на віддалених обчислювальних системах; РН 12 – розробляти моделі загроз та порушника; РН 13 – аналізувати проекти інформаційно-телекомунікаційних систем базуючись на стандартизованих технологіях та протоколах передачі даних; РН 14 – вирішувати завдання захисту програм та інформації, що обробляється в інформаційно-телекомунікаційних системах програмно-апаратними засобами та давати оцінку результативності якості прийнятих рішень; РН 15 – використовувати сучасне програмно-апаратне забезпечення інформаційно-комунікаційних технологій; РН 16 – реалізовувати комплексні системи захисту інформації в автоматизованих системах (АС) організації (підприємства) відповідно до вимог нормативно-правових документів; РН 17 – забезпечувати процеси захисту та функціонування інформаційно-телекомунікаційних (автоматизованих) систем на основі практик, навичок та знань, щодо структурних (структурно-логічних) схем, топології мережі, сучасних архітектур та моделей захисту електронних інформаційних ресурсів з		

відображенням взаємозв'язків та інформаційних потоків, процесів для внутрішніх і віддалених компонент; РН 18 – використовувати програмні та програмно-апаратні комплекси захисту інформаційних ресурсів; РН 19 – застосовувати теорії та методи захисту для забезпечення безпеки інформації в інформаційно-телекомунікаційних системах; РН 20 – забезпечувати функціонування спеціального програмного забезпечення, щодо захисту інформації від руйнуючих програмних впливів, руйнуючих кодів в інформаційно-телекомунікаційних системах; РН 21 – вирішувати задачі забезпечення та супроводу (в.т. числі: огляд, тестування, підзвітність) системи управління доступом згідно встановленої політики безпеки в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах; РН 22 – вирішувати задачі управління процедурами ідентифікації, автентифікації, авторизації процесів і користувачів в інформаційно-телекомунікаційних системах згідно встановленої політики інформаційної і\або кібербезпеки; РН 23 – реалізовувати заходи з протидії отриманню несанкціонованого доступу до інформаційних ресурсів і процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах; РН 24 – вирішувати задачі управління доступом до інформаційних ресурсів та процесів в інформаційних та		

інформаційно-телекомунікаційних (автоматизованих) системах на основі моделей управління доступом (мандатних, дискреційних, рольових); РН 25 – забезпечувати введення підзвітності системи управління доступом до електронних інформаційних ресурсів і процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах з використанням журналів реєстрації подій, їх аналізу та встановлених процедур захисту; РН 26 – впроваджувати заходи та забезпечувати реалізацію процесів попередження отриманню несанкціонованого доступу і захисту інформаційних, інформаційно-телекомунікаційних (автоматизованих) систем на основі еталонної моделі взаємодії відкритих систем; РН 27 – вирішувати задачі захисту потоків даних в інформаційних, інформаційно-телекомунікаційних (автоматизованих) системах; РН 28 – аналізувати та проводити оцінку ефективності та рівня захищеності ресурсів різних класів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах в ході проведення випробувань згідно встановленої політики інформаційної та\або кібербезпеки; РН 29 – здійснювати оцінювання можливості реалізації потенційних загроз інформації, що обробляється в інформаційно-телекомунікаційних системах та ефективності використання комплексів засобів захисту в умовах		

реалізації загроз різних класів; РН 30 – здійснювати оцінювання можливості несанкціонованого доступу до елементів інформаційно-телекомунікаційних систем; РН 31 – застосовувати теорії та методи захисту для забезпечення безпеки елементів інформаційно-телекомунікаційних систем; РН 32 – вирішувати задачі управління процесами відновлення штатного функціонування інформаційно-телекомунікаційних систем з використанням процедур резервування згідно встановленої політики безпеки; РН 33 – вирішувати задачі забезпечення безперервності бізнес процесів організації на основі теорії ризиків; РН 34 – приймати участь у розробці та впровадженні стратегії інформаційної безпеки та/або кібербезпеки відповідно до цілей і завдань організації; РН 35 – вирішувати задачі забезпечення та супроводу комплексних систем захисту інформації, а також протидії несанкціонованому доступу до інформаційних ресурсів і процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах згідно встановленої політики інформаційної і\або кібербезпеки; РН 36 – виявляти небезпечні сигнали технічних засобів; РН 37 – вимірювати параметри небезпечних та завадових сигналів під час інструментального контролю процесів захисту інформації та визначати ефективність захисту інформації від витоку технічними каналами відповідно		

до вимог нормативних документів системи технічного захисту інформації; РН 38 – інтерпретувати результати проведення спеціальних вимірювань з використанням технічних засобів, контролю характеристик інформаційно-телекомунікаційних систем відповідно до вимог нормативних документів системи технічного захисту інформації; РН 39 – проводити атестацію (спираючись на облік та обстеження) режимних територій (зон), приміщень тощо в умовах додержання режиму секретності із фіксуванням результатів у відповідних документах; РН 40 – інтерпретувати результати проведення спеціальних вимірювань з використанням технічних засобів, контролю характеристик ІТС відповідно до вимог нормативних документів системи технічного захисту інформації; РН 41 – забезпечувати неперервність процесу ведення журналів реєстрації подій та інцидентів на основі автоматизованих процедур; РН 42 – впроваджувати процеси виявлення, ідентифікації, аналізу та реагування на інциденти інформаційної і/або кібербезпеки; РН 43 – застосовувати національні та міжнародні регулюючі акти в сфері інформаційної безпеки та/ або кібербезпеки для розслідування інцидентів; РН 44 – вирішувати задачі забезпечення безперервності бізнес-процесів організації на основі теорії ризиків та встановленої системи управління інформаційною безпекою, згідно з вітчизняними та		

міжнародними вимогами та стандартами; РН 45 – застосовувати ріні класи політик інформаційної безпеки та/ або кібербезпеки, що базуються на ризик-орієнтованому контролі доступу до інформаційних активів; РН 46 – здійснювати аналіз та мінімізацію ризиків обробки інформації в інформаційно-телекомунікаційних системах. РН 47 – вирішувати задачі захисту інформації, що обробляється в інформаційно-телекомунікаційних системах з використанням сучасних методів та засобів криптографічного захисту інформації; РН 48 – виконувати впровадження та підтримку систем виявлення вторгнень та використовувати компоненти криптографічного захисту для забезпечення необхідного рівня захищеності інформації в інформаційно-телекомунікаційних системах; РН 49 – забезпечувати належне функціонування системи моніторингу інформаційних ресурсів і процесів в інформаційно-телекомунікаційних системах; РН 50 – забезпечувати функціонування програмних та програмно-апаратних комплексів виявлення вторгнень різних рівнів та класів (статистичних, сигнатурних, статистично-сигнатурних); РН 51 – підтримувати працездатність та забезпечувати конфігурування систем виявлення вторгнень в інформаційно-телекомунікаційних системах; РН 52 – використовувати інструментарій для моніторингу процесів в інформаційно-		

телекомунікаційних системах. РН 53 – вирішувати задачі аналізу програмного коду на наявність можливих загроз; РН 54 – усвідомлювати цінності громадянського (вільного демократичного) суспільства та необхідність його сталого розвитку, верховенства права, прав і свобод людини і громадянина в Україні.		
Інформаційна безпека держави		
РН 1 – застосовувати знання державної та іноземних мов з метою забезпечення ефективності професійної комунікації; РН 2 – організовувати власну професійну діяльність, обирати оптимальні методи та способи розв'язування складних спеціалізованих задач та практичних проблем у професійній діяльності, оцінювати їхню ефективність; РН 3 – використовувати результати самостійного пошуку, аналізу та синтезу інформації з різних джерел для ефективного рішення спеціалізованих задач професійної діяльності; РН 4 – аналізувати, аргументувати, приймати рішення при розв'язанні складних спеціалізованих задач та практичних проблем у професійній діяльності, які характеризуються комплексністю та неповною визначеністю умов, відповідати за прийняті рішення; РН 5 – адаптуватися в умовах частої зміни технологій професійної діяльності, прогнозувати кінцевий результат; РН 6 – критично осмислювати основні теорії, принципи, методи і поняття у навчанні та професійній діяльності; РН 7 – діяти на основі законодавчої та	Пояснювально-ілюстративний (інформаційно-рецептивний) та репродуктивний	Захист лабораторних робіт, експрес-опитування, контрольні роботи, залік

нормативно-правової бази України та вимог відповідних стандартів, у тому числі міжнародних в галузі інформаційної та /або кібербезпеки; РН 8 – готувати пропозиції до нормативних актів щодо забезпечення інформаційної та /або кібербезпеки; РН 9 – впроваджувати процеси, що базуються на національних та міжнародних стандартах, виявлення, ідентифікації, аналізу та реагування на інциденти інформаційної та/або кібербезпеки; РН 10 – виконувати аналіз та декомпозицію інформаційно-телекомунікаційних систем; РН 11 – виконувати аналіз зв'язків між інформаційними процесами на віддалених обчислювальних системах; РН 12 – розробляти моделі загроз та порушника; РН 13 – аналізувати проекти інформаційно-телекомунікаційних систем базуючись на стандартизованих технологіях та протоколах передачі даних; РН 14 – вирішувати завдання захисту програм та інформації, що обробляється в інформаційно-телекомунікаційних системах програмно-апаратними засобами та давати оцінку результативності якості прийнятих рішень; РН 15 – використовувати сучасне програмно-апаратне забезпечення інформаційно-комунікаційних технологій; РН 16 – реалізовувати комплексні системи захисту інформації в автоматизованих системах (АС) організації (підприємства) відповідно до вимог нормативно-правових		

документів; РН 17 – забезпечувати процеси захисту та функціонування інформаційно-телекомунікаційних (автоматизованих) систем на основі практик, навичок та знань, щодо структурних (структурно-логічних) схем, топології мережі, сучасних архітектур та моделей захисту електронних інформаційних ресурсів з відображенням взаємозв'язків та інформаційних потоків, процесів для внутрішніх і віддалених компонент; РН 18 – використовувати програмні та програмно-апаратні комплекси захисту інформаційних ресурсів; РН 19 – застосовувати теорії та методи захисту для забезпечення безпеки інформації в інформаційно-телекомунікаційних системах; РН 20 – забезпечувати функціонування спеціального програмного забезпечення, щодо захисту інформації від руйнуючих програмних впливів, руйнуючих кодів в інформаційно-телекомунікаційних системах; РН 21 – вирішувати задачі забезпечення та супроводу (в.т. числі: огляд, тестування, підзвітність) системи управління доступом згідно встановленої політики безпеки в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах; РН 22 – вирішувати задачі управління процедурами ідентифікації, автентифікації, авторизації процесів і користувачів в інформаційно-телекомунікаційних системах згідно встановленої політики інформаційної і\або кібербезпеки;		

РН 23 – реалізовувати заходи з протидії отриманню несанкціонованого доступу до інформаційних ресурсів і процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах; РН 24 – вирішувати задачі управління доступом до інформаційних ресурсів та процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах на основі моделей управління доступом (мандатних, дискреційних, рольових); РН 25 – забезпечувати введення підзвітності системи управління доступом до електронних інформаційних ресурсів і процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах з використанням журналів реєстрації подій, їх аналізу та встановлених процедур захисту; РН 26 – впроваджувати заходи та забезпечувати реалізацію процесів попередження отриманню несанкціонованого доступу і захисту інформаційних, інформаційно-телекомунікаційних (автоматизованих) систем на основі еталонної моделі взаємодії відкритих систем; РН 27 – вирішувати задачі захисту потоків даних в інформаційних, інформаційно-телекомунікаційних (автоматизованих) системах; РН 28 – аналізувати та проводити оцінку ефективності та рівня захищеності ресурсів різних класів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах в ході		

проведення випробувань згідно встановленої політики інформаційної та\або кібербезпеки; РН 29 – здійснювати оцінювання можливості реалізації потенційних загроз інформації, що обробляється в інформаційно-телекомунікаційних системах та ефективності використання комплексів засобів захисту в умовах реалізації загроз різних класів; РН 30 – здійснювати оцінювання можливості несанкціонованого доступу до елементів інформаційно-телекомунікаційних систем; РН 31 – застосовувати теорії та методи захисту для забезпечення безпеки елементів інформаційно-телекомунікаційних систем; РН 32 – вирішувати задачі управління процесами відновлення штатного функціонування інформаційно-телекомунікаційних систем з використанням процедур резервування згідно встановленої політики безпеки; РН 33 – вирішувати задачі забезпечення безперервності бізнес процесів організації на основі теорії ризиків; РН 34 – приймати участь у розробці та впровадженні стратегії інформаційної безпеки та/або кібербезпеки відповідно до цілей і завдань організації; РН 35 – вирішувати задачі забезпечення та супроводу комплексних систем захисту інформації, а також протидії несанкціонованому доступу до інформаційних ресурсів і процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах згідно встановленої політики		

інформаційної і\або кібербезпеки; РН 36 – виявляти небезпечні сигнали технічних засобів; РН 37 – вимірювати параметри небезпечних та завадових сигналів під час інструментального контролю процесів захисту інформації та визначати ефективність захисту інформації від витоку технічними каналами відповідно до вимог нормативних документів системи технічного захисту інформації; РН 38 – інтерпретувати результати проведення спеціальних вимірювань з використанням технічних засобів, контролю характеристик інформаційно-телекомунікаційних систем відповідно до вимог нормативних документів системи технічного захисту інформації; РН 39 – проводити атестацію (спираючись на облік та обстеження) режимних територій (зон), приміщень тощо в умовах додержання режиму секретності із фіксуванням результатів у відповідних документах; РН 40 – інтерпретувати результати проведення спеціальних вимірювань з використанням технічних засобів, контролю характеристик ІТС відповідно до вимог нормативних документів системи технічного захисту інформації; РН 41 – забезпечувати неперервність процесу ведення журналів реєстрації подій та інцидентів на основі автоматизованих процедур; РН 42 – впроваджувати процеси виявлення, ідентифікації, аналізу та реагування на інциденти інформаційної і/або кібербезпеки; РН 43 – застосовувати національні та		

міжнародні регулюючі акти в сфері інформаційної безпеки та/ або кібербезпеки для розслідування інцидентів; РН 44 – вирішувати задачі забезпечення безперервності бізнес-процесів організації на основі теорії ризиків та встановленої системи управління інформаційною безпекою, згідно з вітчизняними та міжнародними вимогами та стандартами; РН 45 – застосовувати ріні класи політик інформаційної безпеки та/ або кібербезпеки, що базуються на ризик-орієнтованому контролі доступу до інформаційних активів; РН 46 – здійснювати аналіз та мінімізацію ризиків обробки інформації в інформаційно-телекомунікаційних системах. РН 47 – вирішувати задачі захисту інформації, що обробляється в інформаційно-телекомунікаційних системах з використанням сучасних методів та засобів криптографічного захисту інформації; РН 48 – виконувати впровадження та підтримку систем виявлення вторгнень та використовувати компоненти криптографічного захисту для забезпечення необхідного рівня захищеності інформації в інформаційно-телекомунікаційних системах; РН 49 – забезпечувати належне функціонування системи моніторингу інформаційних ресурсів і процесів в інформаційно-телекомунікаційних системах; РН 50 – забезпечувати функціонування програмних та програмно-апаратних		

комплексів виявлення вторгнень різних рівнів та класів (статистичних, сигнатурних, статистично-сигнатурних); РН 51 – підтримувати працездатність та забезпечувати конфігурування систем виявлення вторгнень в інформаційно-телекомунікаційних системах; РН 52 – використовувати інструментарій для моніторингу процесів в інформаційно-телекомунікаційних системах. РН 53 – вирішувати задачі аналізу програмного коду на наявність можливих загроз; РН 54 – усвідомлювати цінності громадянського (вільного демократичного) суспільства та необхідність його сталого розвитку, верховенства права, прав і свобод людини і громадянина в Україні.		
Структури даних		
РН 2 – організовувати власну професійну діяльність, обирати оптимальні методи та способи розв'язування складних спеціалізованих задач та практичних проблем у професійній діяльності, оцінювати їхню ефективність; РН 3 – використовувати результати самостійного пошуку, аналізу та синтезу інформації з різних джерел для ефективного рішення спеціалізованих задач професійної діяльності; РН 4 – аналізувати, аргументувати, приймати рішення при розв'язанні складних спеціалізованих задач та практичних проблем у професійній діяльності, які характеризуються комплексністю та неповною визначеністю умов, відповідати за прийняті рішення; РН 5 – адаптуватися в умовах частої зміни	Виконання лабораторних робіт, виконання та демонстрація індивідуальних завдань (використовуючи необхідні програмні та апаратні інструментальні засоби: CodeBlocks, IntelijIdea, git, VisualStudioCode), розробка реальних проєктів, взявши участь у програмі "Інноваційний кампус" НТУ "ХПІ"	Опитування, захист лабораторних робіт, контрольні роботи, тестування, екзамен

технологій професійної діяльності, прогнозувати кінцевий результат; РН 7 – діяти на основі законодавчої та нормативно-правової бази України та вимог відповідних стандартів, у тому числі міжнародних в галузі інформаційної та /або кібербезпеки; РН 8 – готувати пропозиції до нормативних актів щодо забезпечення інформаційної та /або кібербезпеки; РН 10 – виконувати аналіз та декомпозицію інформаційнотелекомунікаційних систем; РН 11 – виконувати аналіз зв'язків між інформаційними процесами на віддалених обчислювальних системах; РН 13 – аналізувати проекти інформаційно-телекомунікаційних систем базуючись на стандартизованих технологіях та протоколах передачі даних; РН 14 – вирішувати завдання захисту програм та інформації, що обробляється в інформаційно-телекомунікаційних системах програмно-апаратними засобами та давати оцінку результативності якості прийнятих рішень; РН 15 – використовувати сучасне програмно-апаратне забезпечення інформаційно-комунікаційних технологій; РН 17 – забезпечувати процеси захисту та функціонування інформаційно-телекомунікаційних (автоматизованих) систем на основі практик, навичок та знань, щодо структурних (структурно-логічних) схем, топології мережі, сучасних архітектур та моделей захисту електронних інформаційних ресурсів з		

відображенням взаємозв'язків та інформаційних потоків, процесів для внутрішніх і віддалених компонент; РН 18 – використовувати програмні та програмно-апаратні комплекси захисту інформаційних ресурсів; РН 19 – застосовувати теорії та методи захисту для забезпечення безпеки інформації в інформаційно-телекомунікаційних системах; РН 20 – забезпечувати функціонування спеціального програмного забезпечення, щодо захисту інформації від руйнуючих програмних впливів, руйнуючих кодів в інформаційно-телекомунікаційних системах; РН 23 – реалізовувати заходи з протидії отриманню несанкціонованого доступу до інформаційних ресурсів і процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах; РН 27 – вирішувати задачі захисту потоків даних в інформаційних, інформаційно-телекомунікаційних (автоматизованих) системах; РН 31 – застосовувати теорії та методи захисту для забезпечення безпеки елементів інформаційно-телекомунікаційних систем; РН 37 – вимірювати параметри небезпечних та завадових сигналів під час інструментального контролю процесів захисту інформації та визначати ефективність захисту інформації від витоку технічними каналами відповідно до вимог нормативних документів системи технічного захисту інформації; РН 38 – інтерпретувати результати		

проведення спеціальних вимірювань з використанням технічних засобів, контролю характеристик інформаційно-телекомунікаційних систем відповідно до вимог нормативних документів системи технічного захисту інформації; РН 41 – забезпечувати неперервність процесу ведення журналів реєстрації подій та інцидентів на основі автоматизованих процедур; РН 48 – виконувати впровадження та підтримку систем виявлення вторгнень та використовувати компоненти криптографічного захисту для забезпечення необхідного рівня захищеності інформації в інформаційно-телекомунікаційних системах; РН 49 – забезпечувати належне функціонування системи моніторингу інформаційних ресурсів і процесів в інформаційно- системах; РН 52 – використовувати інструментарій для моніторингу процесів в інформаційно-телекомунікаційних системах; РН 53 – вирішувати задачі аналізу програмного коду на наявність можливих загроз.		
Математичні основи криптології		
РН 1 – застосовувати знання державної та іноземних мов з метою забезпечення ефективності професійної комунікації; РН 2 – організовувати власну професійну діяльність, обирати оптимальні методи та способи розв'язування складних спеціалізованих задач та практичних проблем у професійній діяльності, оцінювати їхню ефективність; РН 3 – використовувати результати самостійного пошуку, аналізу та синтезу	Пояснювально-ілюстративний (інформаційно-рецептивний) та репродуктивний	Захист лабораторних робіт, експрес-опитування, контрольні роботи, залік

інформації з різних джерел для ефективного рішення спеціалізованих задач професійної діяльності; РН 4 – аналізувати, аргументувати, приймати рішення при розв'язанні складних спеціалізованих задач та практичних проблем у професійній діяльності, які характеризуються комплексністю та неповною визначеністю умов, відповідати за прийняті рішення; РН 5 – адаптуватися в умовах частої зміни технологій професійної діяльності, прогнозувати кінцевий результат; РН 6 – критично осмислювати основні теорії, принципи, методи і поняття у навчанні та професійній діяльності; РН 7 – діяти на основі законодавчої та нормативно-правової бази України та вимог відповідних стандартів, у тому числі міжнародних в галузі інформаційної та /або кібербезпеки; РН 8 – готувати пропозиції до нормативних актів щодо забезпечення інформаційної та /або кібербезпеки; РН 9 – впроваджувати процеси, що базуються на національних та міжнародних стандартах, виявлення, ідентифікації, аналізу та реагування на інциденти інформаційної та/або кібербезпеки; РН 10 – виконувати аналіз та декомпозицію інформаційно-телекомунікаційних систем; РН 11 – виконувати аналіз зв'язків між інформаційними процесами на віддалених обчислювальних системах; РН 12 – розробляти моделі загроз та порушника; РН 13 – аналізувати проекти		

інформаційно-телекомунікаційних систем базуючись на стандартизованих технологіях та протоколах передачі даних; РН 14 – вирішувати завдання захисту програм та інформації, що обробляється в інформаційно-телекомунікаційних системах програмно-апаратними засобами та давати оцінку результативності якості прийнятих рішень; РН 15 – використовувати сучасне програмно-апаратне забезпечення інформаційно-комунікаційних технологій; РН 16 – реалізовувати комплексні системи захисту інформації в автоматизованих системах (АС) організації (підприємства) відповідно до вимог нормативно-правових документів; РН 17 – забезпечувати процеси захисту та функціонування інформаційно-телекомунікаційних (автоматизованих) систем на основі практик, навичок та знань, щодо структурних (структурно-логічних) схем, топології мережі, сучасних архітектур та моделей захисту електронних інформаційних ресурсів з відображенням взаємозв'язків та інформаційних потоків, процесів для внутрішніх і віддалених компонент; РН 18 – використовувати програмні та програмно-апаратні комплекси захисту інформаційних ресурсів; РН 19 – застосовувати теорії та методи захисту для забезпечення безпеки інформації в інформаційно-телекомунікаційних системах; РН 20 – забезпечувати функціонування спеціального програмного забезпечення, щодо захисту інформації від руйнуючих		

програмних впливів, руйнуючих кодів в інформаційно-телекомунікаційних системах; РН 21 – вирішувати задачі забезпечення та супроводу (в.т. числі: огляд, тестування, підзвітність) системи управління доступом згідно встановленої політики безпеки в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах; РН 22 – вирішувати задачі управління процедурами ідентифікації, автентифікації, авторизації процесів і користувачів в інформаційно-телекомунікаційних системах згідно встановленої політики інформаційної і\або кібербезпеки; РН 23 – реалізовувати заходи з протидії отриманню несанкціонованого доступу до інформаційних ресурсів і процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах; РН 24 – вирішувати задачі управління доступом до інформаційних ресурсів та процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах на основі моделей управління доступом (мандатних, дискреційних, рольових); РН 25 – забезпечувати введення підзвітності системи управління доступом до електронних інформаційних ресурсів і процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах з використанням журналів реєстрації подій, їх аналізу та встановлених процедур захисту;		

РН 26 – впроваджувати заходи та забезпечувати реалізацію процесів попередження отриманню несанкціонованого доступу і захисту інформаційних, інформаційно-телекомунікаційних (автоматизованих) систем на основі еталонної моделі взаємодії відкритих систем; РН 27 – вирішувати задачі захисту потоків даних в інформаційних, інформаційно-телекомунікаційних (автоматизованих) системах; РН 28 – аналізувати та проводити оцінку ефективності та рівня захищеності ресурсів різних класів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах в ході проведення випробувань згідно встановленої політики інформаційної та\або кібербезпеки; РН 29 – здійснювати оцінювання можливості реалізації потенційних загроз інформації, що обробляється в інформаційно-телекомунікаційних системах та ефективності використання комплексів засобів захисту в умовах реалізації загроз різних класів; РН 30 – здійснювати оцінювання можливості несанкціонованого доступу до елементів інформаційно-телекомунікаційних систем; РН 31 – застосовувати теорії та методи захисту для забезпечення безпеки елементів інформаційно-телекомунікаційних систем; РН 32 – вирішувати задачі управління процесами відновлення штатного функціонування інформаційно-телекомунікаційних систем з		

використанням процедур резервування згідно встановленої політики безпеки; РН 33 – вирішувати задачі забезпечення безперервності бізнес процесів організації на основі теорії ризиків; РН 34 – приймати участь у розробці та впровадженні стратегії інформаційної безпеки та/або кібербезпеки відповідно до цілей і завдань організації; РН 35 – вирішувати задачі забезпечення та супроводу комплексних систем захисту інформації, а також протидії несанкціонованому доступу до інформаційних ресурсів і процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах згідно встановленої політики інформаційної і\або кібербезпеки; РН 36 – виявляти небезпечні сигнали технічних засобів; РН 37 – вимірювати параметри небезпечних та завадових сигналів під час інструментального контролю процесів захисту інформації та визначати ефективність захисту інформації від витоку технічними каналами відповідно до вимог нормативних документів системи технічного захисту інформації; РН 38 – інтерпретувати результати проведення спеціальних вимірювань з використанням технічних засобів, контролю характеристик інформаційно-телекомунікаційних систем відповідно до вимог нормативних документів системи технічного захисту інформації; РН 39 – проводити атестацію (спираючись на облік та обстеження) режимних територій (зон), приміщень тощо в умовах додержання режиму		

секретності із фіксуванням результатів у відповідних документах; РН 40 – інтерпретувати результати проведення спеціальних вимірювань з використанням технічних засобів, контролю характеристик ІТС відповідно до вимог нормативних документів системи технічного захисту інформації; РН 41 – забезпечувати неперервність процесу ведення журналів реєстрації подій та інцидентів на основі автоматизованих процедур; РН 42 – впроваджувати процеси виявлення, ідентифікації, аналізу та реагування на інциденти інформаційної і/або кібербезпеки; РН 43 – застосовувати національні та міжнародні регулюючі акти в сфері інформаційної безпеки та/ або кібербезпеки для розслідування інцидентів; РН 44 – вирішувати задачі забезпечення безперервності бізнес-процесів організації на основі теорії ризиків та встановленої системи управління інформаційною безпекою, згідно з вітчизняними та міжнародними вимогами та стандартами; РН 45 – застосовувати різні класи політик інформаційної безпеки та/ або кібербезпеки, що базуються на ризик-орієнтованому контролі доступу до інформаційних активів; РН 46 – здійснювати аналіз та мінімізацію ризиків обробки інформації в інформаційно-телекомунікаційних системах. РН 47 – вирішувати задачі захисту інформації, що обробляється в інформаційно-телекомунікаційних		

системах з використанням сучасних методів та засобів криптографічного захисту інформації; РН 48 – виконувати впровадження та підтримку систем виявлення вторгнень та використовувати компоненти криптографічного захисту для забезпечення необхідного рівня захищеності інформації в інформаційно-телекомунікаційних системах; РН 49 – забезпечувати належне функціонування системи моніторингу інформаційних ресурсів і процесів в інформаційно-телекомунікаційних системах; РН 50 – забезпечувати функціонування програмних та програмно-апаратних комплексів виявлення вторгнень різних рівнів та класів (статистичних, сигнатурних, статистично-сигнатурних); РН 51 – підтримувати працездатність та забезпечувати конфігурування систем виявлення вторгнень в інформаційно-телекомунікаційних системах; РН 52 – використовувати інструментарій для моніторингу процесів в інформаційно-телекомунікаційних системах. РН 53 – вирішувати задачі аналізу програмного коду на наявність можливих загроз; РН 54 – усвідомлювати цінності громадянського (вільного демократичного) суспільства та необхідність його сталого розвитку, верховенства права, прав і свобод людини і громадянина в Україні.		
Основи побудови та захисту сучасних операційних систем		
РН 1 – застосовувати знання державної та іноземних мов з метою забезпечення	Пояснювально-ілюстративний (інформаційно-рецептивний) та	Захист лабораторних завдань, експрес-опитування, контрольні роботи, екзамен

ефективності професійної комунікації; РН 2 – організовувати власну професійну діяльність, обирати оптимальні методи та способи розв'язування складних спеціалізованих задач та практичних проблем у професійній діяльності, оцінювати їхню ефективність; РН 3 – використовувати результати самостійного пошуку, аналізу та синтезу інформації з різних джерел для ефективного рішення спеціалізованих задач професійної діяльності; РН 4 – аналізувати, аргументувати, приймати рішення при розв'язанні складних спеціалізованих задач та практичних проблем у професійній діяльності, які характеризуються комплексністю та неповною визначеністю умов, відповідати за прийняті рішення; РН 5 – адаптуватися в умовах частої зміни технологій професійної діяльності, прогнозувати кінцевий результат; РН 6 – критично осмислювати основні теорії, принципи, методи і поняття у навчанні та професійній діяльності; РН 7 – діяти на основі законодавчої та нормативно-правової бази України та вимог відповідних стандартів, у тому числі міжнародних в галузі інформаційної та /або кібербезпеки; РН 8 – готувати пропозиції до нормативних актів щодо забезпечення інформаційної та /або кібербезпеки; РН 9 – впроваджувати процеси, що базуються на національних та міжнародних стандартах, виявлення, ідентифікації, аналізу та реагування на інциденти інформаційної та/або кібербезпеки;	репродуктивний	

РН 10 – виконувати аналіз та декомпозицію інформаційно-телекомунікаційних систем; РН 11 – виконувати аналіз зв'язків між інформаційними процесами на віддалених обчислювальних системах; РН 12 – розробляти моделі загроз та порушника; РН 13 – аналізувати проекти інформаційно-телекомунікаційних систем базуючись на стандартизованих технологіях та протоколах передачі даних; РН 14 – вирішувати завдання захисту програм та інформації, що обробляється в інформаційно-телекомунікаційних системах програмно-апаратними засобами та давати оцінку результативності якості прийнятих рішень; РН 15 – використовувати сучасне програмно-апаратне забезпечення інформаційно-комунікаційних технологій; РН 16 – реалізовувати комплексні системи захисту інформації в автоматизованих системах (АС) організації (підприємства) відповідно до вимог нормативно-правових документів; РН 17 – забезпечувати процеси захисту та функціонування інформаційно-телекомунікаційних (автоматизованих) систем на основі практик, навичок та знань, щодо структурних (структурно-логічних) схем, топології мережі, сучасних архітектур та моделей захисту електронних інформаційних ресурсів з відображенням взаємозв'язків та інформаційних потоків, процесів для внутрішніх і віддалених компонент; РН 18 – використовувати програмні та		

програмно-апаратні комплекси захисту інформаційних ресурсів; РН 19 – застосовувати теорії та методи захисту для забезпечення безпеки інформації в інформаційно-телекомунікаційних системах; РН 20 – забезпечувати функціонування спеціального програмного забезпечення, щодо захисту інформації від руйнуючих програмних впливів, руйнуючих кодів в інформаційно-телекомунікаційних системах; РН 21 – вирішувати задачі забезпечення та супроводу (в.т. числі: огляд, тестування, підзвітність) системи управління доступом згідно встановленої політики безпеки в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах; РН 22 – вирішувати задачі управління процедурами ідентифікації, автентифікації, авторизації процесів і користувачів в інформаційно-телекомунікаційних системах згідно встановленої політики інформаційної і\або кібербезпеки; РН 23 – реалізовувати заходи з протидії отриманню несанкціонованого доступу до інформаційних ресурсів і процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах; РН 24 – вирішувати задачі управління доступом до інформаційних ресурсів та процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах на основі моделей управління доступом (мандатних, дискреційних, рольових);		

РН 25 – забезпечувати введення підзвітності системи управління доступом до електронних інформаційних ресурсів і процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах з використанням журналів реєстрації подій, їх аналізу та встановлених процедур захисту; РН 26 – впроваджувати заходи та забезпечувати реалізацію процесів попередження отриманню несанкціонованого доступу і захисту інформаційних, інформаційно-телекомунікаційних (автоматизованих) систем на основі еталонної моделі взаємодії відкритих систем; РН 27 – вирішувати задачі захисту потоків даних в інформаційних, інформаційно-телекомунікаційних (автоматизованих) системах; РН 28 – аналізувати та проводити оцінку ефективності та рівня захищеності ресурсів різних класів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах в ході проведення випробувань згідно встановленої політики інформаційної та\або кібербезпеки; РН 29 – здійснювати оцінювання можливості реалізації потенційних загроз інформації, що обробляється в інформаційно-телекомунікаційних системах та ефективності використання комплексів засобів захисту в умовах реалізації загроз різних класів; РН 30 – здійснювати оцінювання можливості несанкціонованого доступу до елементів інформаційно-		

телекомунікаційних систем; РН 31 – застосовувати теорії та методи захисту для забезпечення безпеки елементів інформаційно-телекомунікаційних систем; РН 32 – вирішувати задачі управління процесами відновлення штатного функціонування інформаційно-телекомунікаційних систем з використанням процедур резервування згідно встановленої політики безпеки; РН 33 – вирішувати задачі забезпечення безперервності бізнес процесів організації на основі теорії ризиків; РН 34 – приймати участь у розробці та впровадженні стратегії інформаційної безпеки та/або кібербезпеки відповідно до цілей і завдань організації; РН 35 – вирішувати задачі забезпечення та супроводу комплексних систем захисту інформації, а також протидії несанкціонованому доступу до інформаційних ресурсів і процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах згідно встановленої політики інформаційної і\або кібербезпеки; РН 36 – виявляти небезпечні сигнали технічних засобів; РН 37 – вимірювати параметри небезпечних та завадових сигналів під час інструментального контролю процесів захисту інформації та визначати ефективність захисту інформації від витоку технічними каналами відповідно до вимог нормативних документів системи технічного захисту інформації; РН 38 – інтерпретувати результати проведення спеціальних вимірювань з		

використанням технічних засобів, контролю характеристик інформаційно-телекомунікаційних систем відповідно до вимог нормативних документів системи технічного захисту інформації; РН 39 – проводити атестацію (спираючись на облік та обстеження) режимних територій (зон), приміщень тощо в умовах додержання режиму секретності із фіксуванням результатів у відповідних документах; РН 40 – інтерпретувати результати проведення спеціальних вимірювань з використанням технічних засобів, контролю характеристик ІТС відповідно до вимог нормативних документів системи технічного захисту інформації; РН 41 – забезпечувати неперервність процесу ведення журналів реєстрації подій та інцидентів на основі автоматизованих процедур; РН 42 – впроваджувати процеси виявлення, ідентифікації, аналізу та реагування на інциденти інформаційної і/або кібербезпеки; РН 43 – застосовувати національні та міжнародні регулюючі акти в сфері інформаційної безпеки та/ або кібербезпеки для розслідування інцидентів; РН 44 – вирішувати задачі забезпечення безперервності бізнес-процесів організації на основі теорії ризиків та встановленої системи управління інформаційною безпекою, згідно з вітчизняними та міжнародними вимогами та стандартами; РН 45 – застосовувати ріні класи політик інформаційної безпеки та/ або кібербезпеки, що базуються на ризик-		

орієнтованому контролі доступу до інформаційних активів; РН 46 – здійснювати аналіз та мінімізацію ризиків обробки інформації в інформаційно-телекомунікаційних системах. РН 47 – вирішувати задачі захисту інформації, що обробляється в інформаційно-телекомунікаційних системах з використанням сучасних методів та засобів криптографічного захисту інформації; РН 48 – виконувати впровадження та підтримку систем виявлення вторгнень та використовувати компоненти криптографічного захисту для забезпечення необхідного рівня захищеності інформації в інформаційно-телекомунікаційних системах; РН 49 – забезпечувати належне функціонування системи моніторингу інформаційних ресурсів і процесів в інформаційно-телекомунікаційних системах; РН 50 – забезпечувати функціонування програмних та програмно-апаратних комплексів виявлення вторгнень різних рівнів та класів (статистичних, сигнатурних, статистично-сигнатурних); РН 51 – підтримувати працездатність та забезпечувати конфігурування систем виявлення вторгнень в інформаційно-телекомунікаційних системах; РН 52 – використовувати інструментарій для моніторингу процесів в інформаційно-телекомунікаційних системах. РН 53 – вирішувати задачі аналізу програмного коду на наявність можливих загроз;		

РН 54 – усвідомлювати цінності громадянського (вільного демократичного) суспільства та необхідність його сталого розвитку, верховенства права, прав і свобод людини і громадянина в Україні.		
Введення в мережі		
РН 1 – застосовувати знання державної та іноземних мов з метою забезпечення ефективності професійної комунікації; РН 2 – організовувати власну професійну діяльність, обирати оптимальні методи та способи розв'язування складних спеціалізованих задач та практичних проблем у професійній діяльності, оцінювати їхню ефективність; РН 3 – використовувати результати самостійного пошуку, аналізу та синтезу інформації з різних джерел для ефективного рішення спеціалізованих задач професійної діяльності; РН 4 – аналізувати, аргументувати, приймати рішення при розв'язанні складних спеціалізованих задач та практичних проблем у професійній діяльності, які характеризуються комплексністю та неповною визначеністю умов, відповідати за прийняті рішення; РН 5 – адаптуватися в умовах частої зміни технологій професійної діяльності, прогнозувати кінцевий результат; РН 6 – критично осмислювати основні теорії, принципи, методи і поняття у навчанні та професійній діяльності; РН 7 – діяти на основі законодавчої та нормативно-правової бази України та вимог відповідних стандартів, у тому числі міжнародних в галузі інформаційної та /або кібербезпеки;	Пояснювально-ілюстративний (інформаційно-рецептивний) та репродуктивний	Захист лабораторних робіт, експрес-опитування, контрольні роботи, виконання курсового проєкту, залік

РН 8 – готувати пропозиції до нормативних актів щодо забезпечення інформаційної та /або кібербезпеки; РН 9 – впроваджувати процеси, що базуються на національних та міжнародних стандартах, виявлення, ідентифікації, аналізу та реагування на інциденти інформаційної та/або кібербезпеки; РН 10 – виконувати аналіз та декомпозицію інформаційно-телекомунікаційних систем; РН 11 – виконувати аналіз зв'язків між інформаційними процесами на віддалених обчислювальних системах; РН 12 – розробляти моделі загроз та порушника; РН 13 – аналізувати проекти інформаційно-телекомунікаційних систем базуючись на стандартизованих технологіях та протоколах передачі даних; РН 14 – вирішувати завдання захисту програм та інформації, що обробляється в інформаційно-телекомунікаційних системах програмно-апаратними засобами та давати оцінку результативності якості прийнятих рішень; РН 15 – використовувати сучасне програмно-апаратне забезпечення інформаційно-комунікаційних технологій; РН 16 – реалізовувати комплексні системи захисту інформації в автоматизованих системах (АС) організації (підприємства) відповідно до вимог нормативно-правових документів; РН 17 – забезпечувати процеси захисту та функціонування інформаційно-телекомунікаційних (автоматизованих)		

систем на основі практик, навичок та знань, щодо структурних (структурно-логічних) схем, топології мережі, сучасних архітектур та моделей захисту електронних інформаційних ресурсів з відображенням взаємозв'язків та інформаційних потоків, процесів для внутрішніх і віддалених компонент; РН 18 – використовувати програмні та програмно-апаратні комплекси захисту інформаційних ресурсів; РН 19 – застосовувати теорії та методи захисту для забезпечення безпеки інформації в інформаційно-телекомунікаційних системах; РН 20 – забезпечувати функціонування спеціального програмного забезпечення, щодо захисту інформації від руйнуючих програмних впливів, руйнуючих кодів в інформаційно-телекомунікаційних системах; РН 21 – вирішувати задачі забезпечення та супроводу (в.т. числі: огляд, тестування, підзвітність) системи управління доступом згідно встановленої політики безпеки в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах; РН 22 – вирішувати задачі управління процедурами ідентифікації, автентифікації, авторизації процесів і користувачів в інформаційно-телекомунікаційних системах згідно встановленої політики інформаційної і\або кібербезпеки; РН 23 – реалізовувати заходи з протидії отриманню несанкціонованого доступу до інформаційних ресурсів і процесів в інформаційних та інформаційно-		

телекомунікаційних (автоматизованих) системах; РН 24 – вирішувати задачі управління доступом до інформаційних ресурсів та процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах на основі моделей управління доступом (мандатних, дискреційних, рольових); РН 25 – забезпечувати введення підзвітності системи управління доступом до електронних інформаційних ресурсів і процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах з використанням журналів реєстрації подій, їх аналізу та встановлених процедур захисту; РН 26 – впроваджувати заходи та забезпечувати реалізацію процесів попередження отриманню несанкціонованого доступу і захисту інформаційних, інформаційно-телекомунікаційних (автоматизованих) систем на основі еталонної моделі взаємодії відкритих систем; РН 27 – вирішувати задачі захисту потоків даних в інформаційних, інформаційно-телекомунікаційних (автоматизованих) системах; РН 28 – аналізувати та проводити оцінку ефективності та рівня захищеності ресурсів різних класів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах в ході проведення випробувань згідно встановленої політики інформаційної та\або кібербезпеки; РН 29 – здійснювати оцінювання		

можливості реалізації потенційних загроз інформації, що обробляється в інформаційно-телекомунікаційних системах та ефективності використання комплексів засобів захисту в умовах реалізації загроз різних класів; РН 30 – здійснювати оцінювання можливості несанкціонованого доступу до елементів інформаційно-телекомунікаційних систем; РН 31 – застосовувати теорії та методи захисту для забезпечення безпеки елементів інформаційно-телекомунікаційних систем; РН 32 – вирішувати задачі управління процесами відновлення штатного функціонування інформаційно-телекомунікаційних систем з використанням процедур резервування згідно встановленої політики безпеки; РН 33 – вирішувати задачі забезпечення безперервності бізнес процесів організації на основі теорії ризиків; РН 34 – приймати участь у розробці та впровадженні стратегії інформаційної безпеки та/або кібербезпеки відповідно до цілей і завдань організації; РН 35 – вирішувати задачі забезпечення та супроводу комплексних систем захисту інформації, а також протидії несанкціонованому доступу до інформаційних ресурсів і процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах згідно встановленої політики інформаційної і\або кібербезпеки; РН 36 – виявляти небезпечні сигнали технічних засобів; РН 37 – вимірювати параметри		

небезпечних та завадових сигналів під час інструментального контролю процесів захисту інформації та визначати ефективність захисту інформації від витоку технічними каналами відповідно до вимог нормативних документів системи технічного захисту інформації; РН 38 – інтерпретувати результати проведення спеціальних вимірювань з використанням технічних засобів, контролю характеристик інформаційно-телекомунікаційних систем відповідно до вимог нормативних документів системи технічного захисту інформації; РН 39 – проводити атестацію (спираючись на облік та обстеження) режимних територій (зон), приміщень тощо в умовах додержання режиму секретності із фіксуванням результатів у відповідних документах; РН 40 – інтерпретувати результати проведення спеціальних вимірювань з використанням технічних засобів, контролю характеристик ІТС відповідно до вимог нормативних документів системи технічного захисту інформації; РН 41 – забезпечувати неперервність процесу ведення журналів реєстрації подій та інцидентів на основі автоматизованих процедур; РН 42 – впроваджувати процеси виявлення, ідентифікації, аналізу та реагування на інциденти інформаційної і/або кібербезпеки; РН 43 – застосовувати національні та міжнародні регулюючі акти в сфері інформаційної безпеки та/ або кібербезпеки для розслідування інцидентів;		

РН 44 – вирішувати задачі забезпечення безперервності бізнес-процесів організації на основі теорії ризиків та встановленої системи управління інформаційною безпекою, згідно з вітчизняними та міжнародними вимогами та стандартами; РН 45 – застосовувати ріні класи політик інформаційної безпеки та/ або кібербезпеки, що базуються на ризик-орієнтованому контролі доступу до інформаційних активів; РН 46 – здійснювати аналіз та мінімізацію ризиків обробки інформації в інформаційно-телекомунікаційних системах. РН 47 – вирішувати задачі захисту інформації, що обробляється в інформаційно-телекомунікаційних системах з використанням сучасних методів та засобів криптографічного захисту інформації; РН 48 – виконувати впровадження та підтримку систем виявлення вторгнень та використовувати компоненти криптографічного захисту для забезпечення необхідного рівня захищеності інформації в інформаційно-телекомунікаційних системах; РН 49 – забезпечувати належне функціонування системи моніторингу інформаційних ресурсів і процесів в інформаційно-телекомунікаційних системах; РН 50 – забезпечувати функціонування програмних та програмно-апаратних комплексів виявлення вторгнень різних рівнів та класів (статистичних, сигнатурних, статистично-сигнатурних); РН 51 – підтримувати працездатність та		

забезпечувати конфігурування систем виявлення вторгнень в інформаційно-телекомунікаційних системах; РН 52 – використовувати інструментарій для моніторингу процесів в інформаційно-телекомунікаційних системах. РН 53 – вирішувати задачі аналізу програмного коду на наявність можливих загроз; РН 54 – усвідомлювати цінності громадянського (вільного демократичного) суспільства та необхідність його сталого розвитку, верховенства права, прав і свобод людини і громадянина в Україні.		
Технології програмування		
РН 1 – застосовувати знання державної та іноземних мов з метою забезпечення ефективності професійної комунікації; РН 2 – організовувати власну професійну діяльність, обирати оптимальні методи та способи розв'язування складних спеціалізованих задач та практичних проблем у професійній діяльності, оцінювати їхню ефективність; РН 3 – використовувати результати самостійного пошуку, аналізу та синтезу інформації з різних джерел для ефективного рішення спеціалізованих задач професійної діяльності; РН 4 – аналізувати, аргументувати, приймати рішення при розв'язанні складних спеціалізованих задач та практичних проблем у професійній діяльності, які характеризуються комплексністю та неповною визначеністю умов, відповідати за прийняті рішення; РН 5 – адаптуватися в умовах частої зміни технологій професійної діяльності,	Пояснювально-ілюстративний (інформаційно-рецептивний) та репродуктивний	Захист лабораторних робіт, експрес-опитування, тестування, контрольні роботи, залік, екзамен

прогнозувати кінцевий результат; РН 6 – критично осмислювати основні теорії, принципи, методи і поняття у навчанні та професійній діяльності; РН 7 – діяти на основі законодавчої та нормативно-правової бази України та вимог відповідних стандартів, у тому числі міжнародних в галузі інформаційної та /або кібербезпеки; РН 8 – готувати пропозиції до нормативних актів щодо забезпечення інформаційної та /або кібербезпеки; РН 9 – впроваджувати процеси, що базуються на національних та міжнародних стандартах, виявлення, ідентифікації, аналізу та реагування на інциденти інформаційної та/або кібербезпеки; РН 10 – виконувати аналіз та декомпозицію інформаційно-телекомунікаційних систем; РН 11 – виконувати аналіз зв'язків між інформаційними процесами на віддалених обчислювальних системах; РН 12 – розробляти моделі загроз та порушника; РН 13 – аналізувати проекти інформаційно-телекомунікаційних систем базуючись на стандартизованих технологіях та протоколах передачі даних; РН 14 – вирішувати завдання захисту програм та інформації, що обробляється в інформаційно-телекомунікаційних системах програмно-апаратними засобами та давати оцінку результативності якості прийнятих рішень; РН 15 – використовувати сучасне програмно-апаратне забезпечення		

інформаційно-комунікаційних технологій; РН 16 – реалізовувати комплексні системи захисту інформації в автоматизованих системах (АС) організації (підприємства) відповідно до вимог нормативно-правових документів; РН 17 – забезпечувати процеси захисту та функціонування інформаційно-телекомунікаційних (автоматизованих) систем на основі практик, навичок та знань, щодо структурних (структурно-логічних) схем, топології мережі, сучасних архітектур та моделей захисту електронних інформаційних ресурсів з відображенням взаємозв'язків та інформаційних потоків, процесів для внутрішніх і віддалених компонент; РН 18 – використовувати програмні та програмно-апаратні комплекси захисту інформаційних ресурсів; РН 19 – застосовувати теорії та методи захисту для забезпечення безпеки інформації в інформаційно-телекомунікаційних системах; РН 20 – забезпечувати функціонування спеціального програмного забезпечення, щодо захисту інформації від руйнуючих програмних впливів, руйнуючих кодів в інформаційно-телекомунікаційних системах; РН 21 – вирішувати задачі забезпечення та супроводу (в.т. числі: огляд, тестування, підзвітність) системи управління доступом згідно встановленої політики безпеки в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах; РН 22 – вирішувати задачі управління процедурами ідентифікації,		

автентифікації, авторизації процесів і користувачів в інформаційно-телекомунікаційних системах згідно встановленої політики інформаційної і\або кібербезпеки; РН 23 – реалізовувати заходи з протидії отриманню несанкціонованого доступу до інформаційних ресурсів і процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах; РН 24 – вирішувати задачі управління доступом до інформаційних ресурсів та процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах на основі моделей управління доступом (мандатних, дискреційних, рольових); РН 25 – забезпечувати введення підзвітності системи управління доступом до електронних інформаційних ресурсів і процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах з використанням журналів реєстрації подій, їх аналізу та встановлених процедур захисту; РН 26 – впроваджувати заходи та забезпечувати реалізацію процесів попередження отриманню несанкціонованого доступу і захисту інформаційних, інформаційно-телекомунікаційних (автоматизованих) систем на основі еталонної моделі взаємодії відкритих систем; РН 27 – вирішувати задачі захисту потоків даних в інформаційних, інформаційно-телекомунікаційних (автоматизованих) системах;		

РН 28 – аналізувати та проводити оцінку ефективності та рівня захищеності ресурсів різних класів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах в ході проведення випробувань згідно встановленої політики інформаційної та\або кібербезпеки; РН 29 – здійснювати оцінювання можливості реалізації потенційних загроз інформації, що обробляється в інформаційно-телекомунікаційних системах та ефективності використання комплексів засобів захисту в умовах реалізації загроз різних класів; РН 30 – здійснювати оцінювання можливості несанкціонованого доступу до елементів інформаційно-телекомунікаційних систем; РН 31 – застосовувати теорії та методи захисту для забезпечення безпеки елементів інформаційно-телекомунікаційних систем; РН 32 – вирішувати задачі управління процесами відновлення штатного функціонування інформаційно-телекомунікаційних систем з використанням процедур резервування згідно встановленої політики безпеки; РН 33 – вирішувати задачі забезпечення безперервності бізнес процесів організації на основі теорії ризиків; РН 34 – приймати участь у розробці та впровадженні стратегії інформаційної безпеки та/або кібербезпеки відповідно до цілей і завдань організації; РН 35 – вирішувати задачі забезпечення та супроводу комплексних систем захисту інформації, а також протидії		

несанкціонованому доступу до інформаційних ресурсів і процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах згідно встановленої політики інформаційної і\або кібербезпеки; РН 36 – виявляти небезпечні сигнали технічних засобів; РН 37 – вимірювати параметри небезпечних та завадових сигналів під час інструментального контролю процесів захисту інформації та визначати ефективність захисту інформації від витоку технічними каналами відповідно до вимог нормативних документів системи технічного захисту інформації; РН 38 – інтерпретувати результати проведення спеціальних вимірювань з використанням технічних засобів, контролю характеристик інформаційно-телекомунікаційних систем відповідно до вимог нормативних документів системи технічного захисту інформації; РН 39 – проводити атестацію (спираючись на облік та обстеження) режимних територій (зон), приміщень тощо в умовах додержання режиму секретності із фіксуванням результатів у відповідних документах; РН 40 – інтерпретувати результати проведення спеціальних вимірювань з використанням технічних засобів, контролю характеристик ІТС відповідно до вимог нормативних документів системи технічного захисту інформації; РН 41 – забезпечувати неперервність процесу ведення журналів реєстрації подій та інцидентів на основі автоматизованих процедур;		

РН 42 – впроваджувати процеси виявлення, ідентифікації, аналізу та реагування на інциденти інформаційної і/або кібербезпеки; РН 43 – застосовувати національні та міжнародні регулюючі акти в сфері інформаційної безпеки та/ або кібербезпеки для розслідування інцидентів; РН 44 – вирішувати задачі забезпечення безперервності бізнес-процесів організації на основі теорії ризиків та встановленої системи управління інформаційною безпекою, згідно з вітчизняними та міжнародними вимогами та стандартами; РН 45 – застосовувати ріні класи політик інформаційної безпеки та/ або кібербезпеки, що базуються на ризик-орієнтованому контролі доступу до інформаційних активів; РН 46 – здійснювати аналіз та мінімізацію ризиків обробки інформації в інформаційно-телекомунікаційних системах. РН 47 – вирішувати задачі захисту інформації, що обробляється в інформаційно-телекомунікаційних системах з використанням сучасних методів та засобів криптографічного захисту інформації; РН 48 – виконувати впровадження та підтримку систем виявлення вторгнень та використовувати компоненти криптографічного захисту для забезпечення необхідного рівня захищеності інформації в інформаційно-телекомунікаційних системах; РН 49 – забезпечувати належне функціонування системи моніторингу		

інформаційних ресурсів і процесів в інформаційно-телекомунікаційних системах; РН 50 – забезпечувати функціонування програмних та програмно-апаратних комплексів виявлення вторгнень різних рівнів та класів (статистичних, сигнатурних, статистично-сигнатурних); РН 51 – підтримувати працездатність та забезпечувати конфігурування систем виявлення вторгнень в інформаційно-телекомунікаційних системах; РН 52 – використовувати інструментарій для моніторингу процесів в інформаційно-телекомунікаційних системах. РН 53 – вирішувати задачі аналізу програмного коду на наявність можливих загроз; РН 54 – усвідомлювати цінності громадянського (вільного демократичного) суспільства та необхідність його сталого розвитку, верховенства права, прав і свобод людини і громадянина в Україні.		
Основи побудови та захисту мікропроцесорних систем		
РН 1 – застосовувати знання державної та іноземних мов з метою забезпечення ефективності професійної комунікації; РН 2 – організовувати власну професійну діяльність, обирати оптимальні методи та способи розв’язування складних спеціалізованих задач та практичних проблем у професійній діяльності, оцінювати їхню ефективність; РН 3 – використовувати результати самостійного пошуку, аналізу та синтезу інформації з різних джерел для ефективного рішення спеціалізованих задач професійної діяльності;	Пояснювально-ілюстративний (інформаційно-рецептивний) та репродуктивний	Захист лабораторних робіт, експрес-опитування, тестування, контрольні роботи, залік

РН 4 – аналізувати, аргументувати, приймати рішення при розв'язанні складних спеціалізованих задач та практичних проблем у професійній діяльності, які характеризуються комплексністю та неповною визначеністю умов, відповідати за прийняті рішення; РН 5 – адаптуватися в умовах частої зміни технологій професійної діяльності, прогнозувати кінцевий результат; РН 6 – критично осмислювати основні теорії, принципи, методи і поняття у навчанні та професійній діяльності; РН 7 – діяти на основі законодавчої та нормативно-правової бази України та вимог відповідних стандартів, у тому числі міжнародних в галузі інформаційної та /або кібербезпеки; РН 8 – готувати пропозиції до нормативних актів щодо забезпечення інформаційної та /або кібербезпеки; РН 9 – впроваджувати процеси, що базуються на національних та міжнародних стандартах, виявлення, ідентифікації, аналізу та реагування на інциденти інформаційної та/або кібербезпеки; РН 10 – виконувати аналіз та декомпозицію інформаційно-телекомунікаційних систем; РН 11 – виконувати аналіз зв'язків між інформаційними процесами на віддалених обчислювальних системах; РН 12 – розробляти моделі загроз та порушника; РН 13 – аналізувати проекти інформаційно-телекомунікаційних систем базуючись на стандартизованих технологіях та протоколах передачі		

даних; РН 14 – вирішувати завдання захисту програм та інформації, що обробляється в інформаційно-телекомунікаційних системах програмно-апаратними засобами та давати оцінку результативності якості прийнятих рішень; РН 15 – використовувати сучасне програмно-апаратне забезпечення інформаційно-комунікаційних технологій; РН 16 – реалізовувати комплексні системи захисту інформації в автоматизованих системах (АС) організації (підприємства) відповідно до вимог нормативно-правових документів; РН 17 – забезпечувати процеси захисту та функціонування інформаційно-телекомунікаційних (автоматизованих) систем на основі практик, навичок та знань, щодо структурних (структурно-логічних) схем, топології мережі, сучасних архітектур та моделей захисту електронних інформаційних ресурсів з відображенням взаємозв'язків та інформаційних потоків, процесів для внутрішніх і віддалених компонент; РН 18 – використовувати програмні та програмно-апаратні комплекси захисту інформаційних ресурсів; РН 19 – застосовувати теорії та методи захисту для забезпечення безпеки інформації в інформаційно-телекомунікаційних системах; РН 20 – забезпечувати функціонування спеціального програмного забезпечення, щодо захисту інформації від руйнуючих програмних впливів, руйнуючих кодів в інформаційно-телекомунікаційних системах;		

РН 21 – вирішувати задачі забезпечення та супроводу (в.т. числі: огляд, тестування, підзвітність) системи управління доступом згідно встановленої політики безпеки в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах; РН 22 – вирішувати задачі управління процедурами ідентифікації, автентифікації, авторизації процесів і користувачів в інформаційно-телекомунікаційних системах згідно встановленої політики інформаційної і\або кібербезпеки; РН 23 – реалізовувати заходи з протидії отриманню несанкціонованого доступу до інформаційних ресурсів і процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах; РН 24 – вирішувати задачі управління доступом до інформаційних ресурсів та процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах на основі моделей управління доступом (мандатних, дискреційних, рольових); РН 25 – забезпечувати введення підзвітності системи управління доступом до електронних інформаційних ресурсів і процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах з використанням журналів реєстрації подій, їх аналізу та встановлених процедур захисту; РН 26 – впроваджувати заходи та забезпечувати реалізацію процесів попередження отриманню		

несанкціонованого доступу і захисту інформаційних, інформаційно-телекомунікаційних (автоматизованих) систем на основі еталонної моделі взаємодії відкритих систем; РН 27 – вирішувати задачі захисту потоків даних в інформаційних, інформаційно-телекомунікаційних (автоматизованих) системах; РН 28 – аналізувати та проводити оцінку ефективності та рівня захищеності ресурсів різних класів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах в ході проведення випробувань згідно встановленої політики інформаційної та\або кібербезпеки; РН 29 – здійснювати оцінювання можливості реалізації потенційних загроз інформації, що обробляється в інформаційно-телекомунікаційних системах та ефективності використання комплексів засобів захисту в умовах реалізації загроз різних класів; РН 30 – здійснювати оцінювання можливості несанкціонованого доступу до елементів інформаційно-телекомунікаційних систем; РН 31 – застосовувати теорії та методи захисту для забезпечення безпеки елементів інформаційно-телекомунікаційних систем; РН 32 – вирішувати задачі управління процесами відновлення штатного функціонування інформаційно-телекомунікаційних систем з використанням процедур резервування згідно встановленої політики безпеки; РН 33 – вирішувати задачі забезпечення		

безперервності бізнес процесів організації на основі теорії ризиків; РН 34 – приймати участь у розробці та впровадженні стратегії інформаційної безпеки та/або кібербезпеки відповідно до цілей і завдань організації; РН 35 – вирішувати задачі забезпечення та супроводу комплексних систем захисту інформації, а також протидії несанкціонованому доступу до інформаційних ресурсів і процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах згідно встановленої політики інформаційної і\або кібербезпеки; РН 36 – виявляти небезпечні сигнали технічних засобів; РН 37 – вимірювати параметри небезпечних та завадових сигналів під час інструментального контролю процесів захисту інформації та визначати ефективність захисту інформації від витоку технічними каналами відповідно до вимог нормативних документів системи технічного захисту інформації; РН 38 – інтерпретувати результати проведення спеціальних вимірювань з використанням технічних засобів, контролю характеристик інформаційно-телекомунікаційних систем відповідно до вимог нормативних документів системи технічного захисту інформації; РН 39 – проводити атестацію (спираючись на облік та обстеження) режимних територій (зон), приміщень тощо в умовах додержання режиму секретності із фіксуванням результатів у відповідних документах; РН 40 – інтерпретувати результати		

проведення спеціальних вимірювань з використанням технічних засобів, контролю характеристик ІТС відповідно до вимог нормативних документів системи технічного захисту інформації; РН 41 – забезпечувати неперервність процесу ведення журналів реєстрації подій та інцидентів на основі автоматизованих процедур; РН 42 – впроваджувати процеси виявлення, ідентифікації, аналізу та реагування на інциденти інформаційної і/або кібербезпеки; РН 43 – застосовувати національні та міжнародні регулюючі акти в сфері інформаційної безпеки та/ або кібербезпеки для розслідування інцидентів; РН 44 – вирішувати задачі забезпечення безперервності бізнес-процесів організації на основі теорії ризиків та встановленої системи управління інформаційною безпекою, згідно з вітчизняними та міжнародними вимогами та стандартами; РН 45 – застосовувати ріні класи політик інформаційної безпеки та/ або кібербезпеки, що базуються на ризик-орієнтованому контролі доступу до інформаційних активів; РН 46 – здійснювати аналіз та мінімізацію ризиків обробки інформації в інформаційно-телекомунікаційних системах. РН 47 – вирішувати задачі захисту інформації, що обробляється в інформаційно-телекомунікаційних системах з використанням сучасних методів та засобів криптографічного захисту інформації;		

РН 48 – виконувати впровадження та підтримку систем виявлення вторгнень та використовувати компоненти криптографічного захисту для забезпечення необхідного рівня захищеності інформації в інформаційно-телекомунікаційних системах; РН 49 – забезпечувати належне функціонування системи моніторингу інформаційних ресурсів і процесів в інформаційно-телекомунікаційних системах; РН 50 – забезпечувати функціонування програмних та програмно-апаратних комплексів виявлення вторгнень різних рівнів та класів (статистичних, сигнатурних, статистично-сигнатурних); РН 51 – підтримувати працездатність та забезпечувати конфігурування систем виявлення вторгнень в інформаційно-телекомунікаційних системах; РН 52 – використовувати інструментарій для моніторингу процесів в інформаційно-телекомунікаційних системах. РН 53 – вирішувати задачі аналізу програмного коду на наявність можливих загроз; РН 54 – усвідомлювати цінності громадянського (вільного демократичного) суспільства та необхідність його сталого розвитку, верховенства права, прав і свобод людини і громадянина в Україні.		
Менеджмент інформаційної безпеки		
РН 1 – застосовувати знання державної та іноземних мов з метою забезпечення ефективності професійної комунікації; РН 2 – організовувати власну професійну діяльність, обирати оптимальні методи та	Пояснювально-ілюстративний (інформаційно-рецептивний) та репродуктивний	Захист лабораторних робіт, експрес-опитування, контрольні роботи, залік

способи розв'язування складних спеціалізованих задач та практичних проблем у професійній діяльності, оцінювати їхню ефективність; РН 3 – використовувати результати самостійного пошуку, аналізу та синтезу інформації з різних джерел для ефективного рішення спеціалізованих задач професійної діяльності; РН 4 – аналізувати, аргументувати, приймати рішення при розв'язанні складних спеціалізованих задач та практичних проблем у професійній діяльності, які характеризуються комплексністю та неповною визначеністю умов, відповідати за прийняті рішення; РН 5 – адаптуватися в умовах частої зміни технологій професійної діяльності, прогнозувати кінцевий результат; РН 6 – критично осмислювати основні теорії, принципи, методи і поняття у навчанні та професійній діяльності; РН 7 – діяти на основі законодавчої та нормативно-правової бази України та вимог відповідних стандартів, у тому числі міжнародних в галузі інформаційної та /або кібербезпеки; РН 8 – готувати пропозиції до нормативних актів щодо забезпечення інформаційної та /або кібербезпеки; РН 9 – впроваджувати процеси, що базуються на національних та міжнародних стандартах, виявлення, ідентифікації, аналізу та реагування на інциденти інформаційної та/або кібербезпеки; РН 10 – виконувати аналіз та декомпозицію інформаційно-телекомунікаційних систем;		

РН 11 – виконувати аналіз зв'язків між інформаційними процесами на віддалених обчислювальних системах; РН 12 – розробляти моделі загроз та порушника; РН 13 – аналізувати проекти інформаційно-телекомунікаційних систем базуючись на стандартизованих технологіях та протоколах передачі даних; РН 14 – вирішувати завдання захисту програм та інформації, що обробляється в інформаційно-телекомунікаційних системах програмно-апаратними засобами та давати оцінку результативності якості прийнятих рішень; РН 15 – використовувати сучасне програмно-апаратне забезпечення інформаційно-комунікаційних технологій; РН 16 – реалізовувати комплексні системи захисту інформації в автоматизованих системах (АС) організації (підприємства) відповідно до вимог нормативно-правових документів; РН 17 – забезпечувати процеси захисту та функціонування інформаційно-телекомунікаційних (автоматизованих) систем на основі практик, навичок та знань, щодо структурних (структурно-логічних) схем, топології мережі, сучасних архітектур та моделей захисту електронних інформаційних ресурсів з відображенням взаємозв'язків та інформаційних потоків, процесів для внутрішніх і віддалених компонент; РН 18 – використовувати програмні та програмно-апаратні комплекси захисту інформаційних ресурсів; РН 19 – застосовувати теорії та методи		

захисту для забезпечення безпеки інформації в інформаційно-телекомунікаційних системах; РН 20 – забезпечувати функціонування спеціального програмного забезпечення, щодо захисту інформації від руйнуючих програмних впливів, руйнуючих кодів в інформаційно-телекомунікаційних системах; РН 21 – вирішувати задачі забезпечення та супроводу (в.т. числі: огляд, тестування, підзвітність) системи управління доступом згідно встановленої політики безпеки в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах; РН 22 – вирішувати задачі управління процедурами ідентифікації, автентифікації, авторизації процесів і користувачів в інформаційно-телекомунікаційних системах згідно встановленої політики інформаційної і\або кібербезпеки; РН 23 – реалізовувати заходи з протидії отриманню несанкціонованого доступу до інформаційних ресурсів і процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах; РН 24 – вирішувати задачі управління доступом до інформаційних ресурсів та процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах на основі моделей управління доступом (мандатних, дискреційних, рольових); РН 25 – забезпечувати введення підзвітності системи управління доступом до електронних інформаційних ресурсів і		

процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах з використанням журналів реєстрації подій, їх аналізу та встановлених процедур захисту; РН 26 – впроваджувати заходи та забезпечувати реалізацію процесів попередження отриманню несанкціонованого доступу і захисту інформаційних, інформаційно-телекомунікаційних (автоматизованих) систем на основі еталонної моделі взаємодії відкритих систем; РН 27 – вирішувати задачі захисту потоків даних в інформаційних, інформаційно-телекомунікаційних (автоматизованих) системах; РН 28 – аналізувати та проводити оцінку ефективності та рівня захищеності ресурсів різних класів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах в ході проведення випробувань згідно встановленої політики інформаційної та\або кібербезпеки; РН 29 – здійснювати оцінювання можливості реалізації потенційних загроз інформації, що обробляється в інформаційно-телекомунікаційних системах та ефективності використання комплексів засобів захисту в умовах реалізації загроз різних класів; РН 30 – здійснювати оцінювання можливості несанкціонованого доступу до елементів інформаційно-телекомунікаційних систем; РН 31 – застосовувати теорії та методи захисту для забезпечення безпеки		

елементів інформаційно-телекомунікаційних систем; РН 32 – вирішувати задачі управління процесами відновлення штатного функціонування інформаційно-телекомунікаційних систем з використанням процедур резервування згідно встановленої політики безпеки; РН 33 – вирішувати задачі забезпечення безперервності бізнес процесів організації на основі теорії ризиків; РН 34 – приймати участь у розробці та впровадженні стратегії інформаційної безпеки та/або кібербезпеки відповідно до цілей і завдань організації; РН 35 – вирішувати задачі забезпечення та супроводу комплексних систем захисту інформації, а також протидії несанкціонованому доступу до інформаційних ресурсів і процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах згідно встановленої політики інформаційної і\або кібербезпеки; РН 36 – виявляти небезпечні сигнали технічних засобів; РН 37 – вимірювати параметри небезпечних та завадових сигналів під час інструментального контролю процесів захисту інформації та визначати ефективність захисту інформації від витоку технічними каналами відповідно до вимог нормативних документів системи технічного захисту інформації; РН 38 – інтерпретувати результати проведення спеціальних вимірювань з використанням технічних засобів, контролю характеристик інформаційно-телекомунікаційних систем відповідно до		

вимог нормативних документів системи технічного захисту інформації; РН 39 – проводити атестацію (спираючись на облік та обстеження) режимних територій (зон), приміщень тощо в умовах додержання режиму секретності із фіксуванням результатів у відповідних документах; РН 40 – інтерпретувати результати проведення спеціальних вимірювань з використанням технічних засобів, контролю характеристик ІТС відповідно до вимог нормативних документів системи технічного захисту інформації; РН 41 – забезпечувати неперервність процесу ведення журналів реєстрації подій та інцидентів на основі автоматизованих процедур; РН 42 – впроваджувати процеси виявлення, ідентифікації, аналізу та реагування на інциденти інформаційної і/або кібербезпеки; РН 43 – застосовувати національні та міжнародні регулюючі акти в сфері інформаційної безпеки та/ або кібербезпеки для розслідування інцидентів; РН 44 – вирішувати задачі забезпечення безперервності бізнес-процесів організації на основі теорії ризиків та встановленої системи управління інформаційною безпекою, згідно з вітчизняними та міжнародними вимогами та стандартами; РН 45 – застосовувати ріні класи політик інформаційної безпеки та/ або кібербезпеки, що базуються на ризик-орієнтованому контролі доступу до інформаційних активів; РН 46 – здійснювати аналіз та мінімізацію		

ризиків обробки інформації в інформаційно-телекомунікаційних системах. РН 47 – вирішувати задачі захисту інформації, що обробляється в інформаційно-телекомунікаційних системах з використанням сучасних методів та засобів криптографічного захисту інформації; РН 48 – виконувати впровадження та підтримку систем виявлення вторгнень та використовувати компоненти криптографічного захисту для забезпечення необхідного рівня захищеності інформації в інформаційно-телекомунікаційних системах; РН 49 – забезпечувати належне функціонування системи моніторингу інформаційних ресурсів і процесів в інформаційно-телекомунікаційних системах; РН 50 – забезпечувати функціонування програмних та програмно-апаратних комплексів виявлення вторгнень різних рівнів та класів (статистичних, сигнатурних, статистично-сигнатурних); РН 51 – підтримувати працездатність та забезпечувати конфігурування систем виявлення вторгнень в інформаційно-телекомунікаційних системах; РН 52 – використовувати інструментарій для моніторингу процесів в інформаційно-телекомунікаційних системах. РН 53 – вирішувати задачі аналізу програмного коду на наявність можливих загроз; РН 54 – усвідомлювати цінності громадянського (вільного демократичного) суспільства та		

необхідність його сталого розвитку, верховенства права, прав і свобод людини і громадянина в Україні.		
Основи математичного моделювання систем безпеки		
РН 1 – застосовувати знання державної та іноземних мов з метою забезпечення ефективності професійної комунікації; РН 2 – організовувати власну професійну діяльність, обирати оптимальні методи та способи розв'язування складних спеціалізованих задач та практичних проблем у професійній діяльності, оцінювати їхню ефективність; РН 3 – використовувати результати самостійного пошуку, аналізу та синтезу інформації з різних джерел для ефективного рішення спеціалізованих задач професійної діяльності; РН 4 – аналізувати, аргументувати, приймати рішення при розв'язанні складних спеціалізованих задач та практичних проблем у професійній діяльності, які характеризуються комплексністю та неповною визначеністю умов, відповідати за прийняті рішення; ації в інформаційно-телекомунікаційних системах; РН 5 – адаптуватися в умовах частої зміни технологій професійної діяльності, прогнозувати кінцевий результат; РН 6 – критично осмислювати основні теорії, принципи, методи і поняття у навчанні та професійній діяльності; РН 7 – діяти на основі законодавчої та нормативно-правової бази України та вимог відповідних стандартів, у тому числі міжнародних в галузі інформаційної та /або кібербезпеки; РН 8 – готувати пропозиції до	Пояснювально-ілюстративний (інформаційно-рецептивний) та репродуктивний	Захист лабораторних робіт, експрес-опитування, тестування, контрольні роботи, залік

нормативних актів щодо забезпечення інформаційної та /або кібербезпеки; РН 9 – впроваджувати процеси, що базуються на національних та міжнародних стандартах, виявлення, ідентифікації, аналізу та реагування на інциденти інформаційної та/або кібербезпеки; РН 10 – виконувати аналіз та декомпозицію інформаційно-телекомунікаційних систем; РН 11 – виконувати аналіз зв'язків між інформаційними процесами на віддалених обчислювальних системах; РН 12 – розробляти моделі загроз та порушника; РН 13 – аналізувати проекти інформаційно-телекомунікаційних систем базуючись на стандартизованих технологіях та протоколах передачі даних; РН 14 – вирішувати завдання захисту програм та інформації, що обробляється в інформаційно-телекомунікаційних системах програмно-апаратними засобами та давати оцінку результативності якості прийнятих рішень; РН 15 – використовувати сучасне програмно-апаратне забезпечення інформаційно-комунікаційних технологій; РН 16 – реалізовувати комплексні системи захисту інформації в автоматизованих системах (АС) організації (підприємства) відповідно до вимог нормативно-правових документів; РН 17 – забезпечувати процеси захисту та функціонування інформаційно-телекомунікаційних (автоматизованих) систем на основі практик, навичок та		

знань, щодо структурних (структурно-логічних) схем, топології мережі, сучасних архітектур та моделей захисту електронних інформаційних ресурсів з відображенням взаємозв'язків та інформаційних потоків, процесів для внутрішніх і віддалених компонент; РН 18 – використовувати програмні та програмно-апаратні комплекси захисту інформаційних ресурсів; РН 19 – застосовувати теорії та методи захисту для забезпечення безпеки інформації в інформаційно-телекомунікаційних системах; РН 20 – забезпечувати функціонування спеціального програмного забезпечення, щодо захисту інформації від руйнуючих програмних впливів, руйнуючих кодів в інформаційно-телекомунікаційних системах; РН 21 – вирішувати задачі забезпечення та супроводу (в.т. числі: огляд, тестування, підзвітність) системи управління доступом згідно встановленої політики безпеки в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах; РН 22 – вирішувати задачі управління процедурами ідентифікації, автентифікації, авторизації процесів і користувачів в інформаційно-телекомунікаційних системах згідно встановленої політики інформаційної і\або кібербезпеки; РН 23 – реалізовувати заходи з протидії отриманню несанкціонованого доступу до інформаційних ресурсів і процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих)		

системах; РН 24 – вирішувати задачі управління доступом до інформаційних ресурсів та процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах на основі моделей управління доступом (мандатних, дискреційних, рольових); РН 25 – забезпечувати введення підзвітності системи управління доступом до електронних інформаційних ресурсів і процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах з використанням журналів реєстрації подій, їх аналізу та встановлених процедур захисту; РН 26 – впроваджувати заходи та забезпечувати реалізацію процесів попередження отриманню несанкціонованого доступу і захисту інформаційних, інформаційно-телекомунікаційних (автоматизованих) систем на основі еталонної моделі взаємодії відкритих систем; РН 27 – вирішувати задачі захисту потоків даних в інформаційних, інформаційно-телекомунікаційних (автоматизованих) системах; РН 28 – аналізувати та проводити оцінку ефективності та рівня захищеності ресурсів різних класів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах в ході проведення випробувань згідно встановленої політики інформаційної та\або кібербезпеки; РН 29 – здійснювати оцінювання можливості реалізації потенційних загроз		

інформації, що обробляється в інформаційно-телекомунікаційних системах та ефективності використання комплексів засобів захисту в умовах реалізації загроз різних класів; РН 30 – здійснювати оцінювання можливості несанкціонованого доступу до елементів інформаційно-телекомунікаційних систем; РН 31 – застосовувати теорії та методи захисту для забезпечення безпеки елементів інформаційно-телекомунікаційних систем; РН 32 – вирішувати задачі управління процесами відновлення штатного функціонування інформаційно-телекомунікаційних систем з використанням процедур резервування згідно встановленої політики безпеки; РН 33 – вирішувати задачі забезпечення безперервності бізнес процесів організації на основі теорії ризиків; РН 34 – приймати участь у розробці та впровадженні стратегії інформаційної безпеки та/або кібербезпеки відповідно до цілей і завдань організації; РН 35 – вирішувати задачі забезпечення та супроводу комплексних систем захисту інформації, а також протидії несанкціонованому доступу до інформаційних ресурсів і процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах згідно встановленої політики інформаційної і\або кібербезпеки; РН 36 – виявляти небезпечні сигнали технічних засобів; РН 37 – вимірювати параметри небезпечних та завадових сигналів під час		

інструментального контролю процесів захисту інформації та визначати ефективність захисту інформації від витоку технічними каналами відповідно до вимог нормативних документів системи технічного захисту інформації; РН 38 – інтерпретувати результати проведення спеціальних вимірювань з використанням технічних засобів, контролю характеристик інформаційно-телекомунікаційних систем відповідно до вимог нормативних документів системи технічного захисту інформації; РН 39 – проводити атестацію (спираючись на облік та обстеження) режимних територій (зон), приміщень тощо в умовах додержання режиму секретності із фіксуванням результатів у відповідних документах; РН 40 – інтерпретувати результати проведення спеціальних вимірювань з використанням технічних засобів, контролю характеристик ІТС відповідно до вимог нормативних документів системи технічного захисту інформації; РН 41 – забезпечувати неперервність процесу ведення журналів реєстрації подій та інцидентів на основі автоматизованих процедур; РН 42 – впроваджувати процеси виявлення, ідентифікації, аналізу та реагування на інциденти інформаційної і/або кібербезпеки; РН 43 – застосовувати національні та міжнародні регулюючі акти в сфері інформаційної безпеки та/ або кібербезпеки для розслідування інцидентів; РН 44 – вирішувати задачі забезпечення		

безперервності бізнес-процесів організації на основі теорії ризиків та встановленої системи управління інформаційною безпекою, згідно з вітчизняними та міжнародними вимогами та стандартами; РН 45 – застосовувати різні класи політик інформаційної безпеки та/ або кібербезпеки, що базуються на ризик-орієнтованому контролі доступу до інформаційних активів; РН 46 – здійснювати аналіз та мінімізацію ризиків обробки інформації в інформаційно-телекомунікаційних системах. РН 47 – вирішувати задачі захисту інформації, що обробляється в інформаційно-телекомунікаційних системах з використанням сучасних методів та засобів криптографічного захисту інформації; РН 48 – виконувати впровадження та підтримку систем виявлення вторгнень та використовувати компоненти криптографічного захисту для забезпечення необхідного рівня захищеності інформації в інформаційно-телекомунікаційних системах; РН 49 – забезпечувати належне функціонування системи моніторингу інформаційних ресурсів і процесів в інформаційно-телекомунікаційних системах; РН 50 – забезпечувати функціонування програмних та програмно-апаратних комплексів виявлення вторгнень різних рівнів та класів (статистичних, сигнатурних, статистично-сигнатурних); РН 51 – підтримувати працездатність та забезпечувати конфігурування систем		

виявлення вторгнень в інформаційно-телекомунікаційних системах; РН 52 – використовувати інструментарій для моніторингу процесів в інформаційно-телекомунікаційних системах. РН 53 – вирішувати задачі аналізу програмного коду на наявність можливих загроз; РН 54 – усвідомлювати цінності громадянського (вільного демократичного) суспільства та необхідність його сталого розвитку, верховенства права, прав і свобод людини і громадянина в Україні.		
Основи криптографічного захисту		
РН 1 – застосовувати знання державної та іноземних мов з метою забезпечення ефективності професійної комунікації; РН 2 – організовувати власну професійну діяльність, обирати оптимальні методи та способи розв'язування складних спеціалізованих задач та практичних проблем у професійній діяльності, оцінювати їхню ефективність; РН 3 – використовувати результати самостійного пошуку, аналізу та синтезу інформації з різних джерел для ефективного рішення спеціалізованих задач професійної діяльності; РН 4 – аналізувати, аргументувати, приймати рішення при розв'язанні складних спеціалізованих задач та практичних проблем у професійній діяльності, які характеризуються комплексністю та неповною визначеністю умов, відповідати за прийняті рішення; РН 5 – адаптуватися в умовах частої зміни технологій професійної діяльності, прогнозувати кінцевий результат;	Пояснювально-ілюстративний (інформаційно-рецептивний) та репродуктивний	Захист лабораторних робіт, експрес-опитування, тестування, контрольні роботи, залік

РН 6 – критично осмислювати основні теорії, принципи, методи і поняття у навчанні та професійній діяльності; РН 7 – діяти на основі законодавчої та нормативно-правової бази України та вимог відповідних стандартів, у тому числі міжнародних в галузі інформаційної та /або кібербезпеки; РН 8 – готувати пропозиції до нормативних актів щодо забезпечення інформаційної та /або кібербезпеки; РН 9 – впроваджувати процеси, що базуються на національних та міжнародних стандартах, виявлення, ідентифікації, аналізу та реагування на інциденти інформаційної та/або кібербезпеки; РН 10 – виконувати аналіз та декомпозицію інформаційно-телекомунікаційних систем; РН 11 – виконувати аналіз зв'язків між інформаційними процесами на віддалених обчислювальних системах; РН 12 – розробляти моделі загроз та порушника; РН 13 – аналізувати проекти інформаційно-телекомунікаційних систем базуючись на стандартизованих технологіях та протоколах передачі даних; РН 14 – вирішувати завдання захисту програм та інформації, що обробляється в інформаційно-телекомунікаційних системах програмно-апаратними засобами та давати оцінку результативності якості прийнятих рішень; РН 15 – використовувати сучасне програмно-апаратне забезпечення інформаційно-комунікаційних технологій;		

РН 16 – реалізовувати комплексні системи захисту інформації в автоматизованих системах (АС) організації (підприємства) відповідно до вимог нормативно-правових документів; РН 17 – забезпечувати процеси захисту та функціонування інформаційно-телекомунікаційних (автоматизованих) систем на основі практик, навичок та знань, щодо структурних (структурно-логічних) схем, топології мережі, сучасних архітектур та моделей захисту електронних інформаційних ресурсів з відображенням взаємозв'язків та інформаційних потоків, процесів для внутрішніх і віддалених компонент; РН 18 – використовувати програмні та програмно-апаратні комплекси захисту інформаційних ресурсів; РН 19 – застосовувати теорії та методи захисту для забезпечення безпеки інформації в інформаційно-телекомунікаційних системах; РН 20 – забезпечувати функціонування спеціального програмного забезпечення, щодо захисту інформації від руйнуючих програмних впливів, руйнуючих кодів в інформаційно-телекомунікаційних системах; РН 21 – вирішувати задачі забезпечення та супроводу (в.т. числі: огляд, тестування, підзвітність) системи управління доступом згідно встановленої політики безпеки в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах; РН 22 – вирішувати задачі управління процедурами ідентифікації, автентифікації, авторизації процесів і		

користувачів в інформаційно-телекомунікаційних системах згідно встановленої політики інформаційної і\або кібербезпеки; РН–23 реалізовувати заходи з протидії отриманню несанкціонованого доступу до інформаційних ресурсів і процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах; РН 24 – вирішувати задачі управління доступом до інформаційних ресурсів та процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах на основі моделей управління доступом (мандатних, дискреційних, рольових); РН 25 – забезпечувати введення підзвітності системи управління доступом до електронних інформаційних ресурсів і процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах з використанням журналів реєстрації подій, їх аналізу та встановлених процедур захисту; РН 26 – впроваджувати заходи та забезпечувати реалізацію процесів попередження отриманню несанкціонованого доступу і захисту інформаційних, інформаційно-телекомунікаційних (автоматизованих) систем на основі еталонної моделі взаємодії відкритих систем; РН 27 – вирішувати задачі захисту потоків даних в інформаційних, інформаційно-телекомунікаційних (автоматизованих) системах; РН 28 – аналізувати та проводити оцінку		

ефективності та рівня захищеності ресурсів різних класів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах в ході проведення випробувань згідно встановленої політики інформаційної та\або кібербезпеки; РН 29 – здійснювати оцінювання можливості реалізації потенційних загроз інформації, що обробляється в інформаційно-телекомунікаційних системах та ефективності використання комплексів засобів захисту в умовах реалізації загроз різних класів; РН 30 – здійснювати оцінювання можливості несанкціонованого доступу до елементів інформаційно-телекомунікаційних систем; РН 31 – застосовувати теорії та методи захисту для забезпечення безпеки елементів інформаційно-телекомунікаційних систем; РН 32 – вирішувати задачі управління процесами відновлення штатного функціонування інформаційно-телекомунікаційних систем з використанням процедур резервування згідно встановленої політики безпеки; РН 33 – вирішувати задачі забезпечення безперервності бізнес процесів організації на основі теорії ризиків; РН 34 – приймати участь у розробці та впровадженні стратегії інформаційної безпеки та/або кібербезпеки відповідно до цілей і завдань організації; РН 35 – вирішувати задачі забезпечення та супроводу комплексних систем захисту інформації, а також протидії несанкціонованому доступу до		

інформаційних ресурсів і процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах згідно встановленої політики інформаційної і\або кібербезпеки; РН 36 – виявляти небезпечні сигнали технічних засобів; РН 37 – вимірювати параметри небезпечних та завадових сигналів під час інструментального контролю процесів захисту інформації та визначати ефективність захисту інформації від витоку технічними каналами відповідно до вимог нормативних документів системи технічного захисту інформації; РН 38 – інтерпретувати результати проведення спеціальних вимірювань з використанням технічних засобів, контролю характеристик інформаційно-телекомунікаційних систем відповідно до вимог нормативних документів системи технічного захисту інформації; РН 39 – проводити атестацію (спираючись на облік та обстеження) режимних територій (зон), приміщень тощо в умовах додержання режиму секретності із фіксуванням результатів у відповідних документах; РН 40 – інтерпретувати результати проведення спеціальних вимірювань з використанням технічних засобів, контролю характеристик ІТС відповідно до вимог нормативних документів системи технічного захисту інформації; РН 41 – забезпечувати неперервність процесу ведення журналів реєстрації подій та інцидентів на основі автоматизованих процедур; РН 42 – впроваджувати процеси		

виявлення, ідентифікації, аналізу та реагування на інциденти інформаційної і/або кібербезпеки; РН 43 – застосовувати національні та міжнародні регулюючі акти в сфері інформаційної безпеки та/ або кібербезпеки для розслідування інцидентів; РН 44 – вирішувати задачі забезпечення безперервності бізнес-процесів організації на основі теорії ризиків та встановленої системи управління інформаційною безпекою, згідно з вітчизняними та міжнародними вимогами та стандартами; РН 45 – застосовувати ріні класи політик інформаційної безпеки та/ або кібербезпеки, що базуються на ризик-орієнтованому контролі доступу до інформаційних активів; РН 46 – здійснювати аналіз та мінімізацію ризиків обробки інформації в інформаційно-телекомунікаційних системах. РН 47 – вирішувати задачі захисту інформації, що обробляється в інформаційно-телекомунікаційних системах з використанням сучасних методів та засобів криптографічного захисту інформації; РН 48 – виконувати впровадження та підтримку систем виявлення вторгнень та використовувати компоненти криптографічного захисту для забезпечення необхідного рівня захищеності інформації в інформаційно-телекомунікаційних системах; РН 49 – забезпечувати належне функціонування системи моніторингу інформаційних ресурсів і процесів в		

інформаційно-телекомунікаційних системах; РН 50 – забезпечувати функціонування програмних та програмно-апаратних комплексів виявлення вторгнень різних рівнів та класів (статистичних, сигнатурних, статистично-сигнатурних); РН 51 – підтримувати працездатність та забезпечувати конфігурування систем виявлення вторгнень в інформаційно-телекомунікаційних системах; РН 52 – використовувати інструментарій для моніторингу процесів в інформаційно-телекомунікаційних системах. РН 53 – вирішувати задачі аналізу програмного коду на наявність можливих загроз; РН 54 – усвідомлювати цінності громадянського (вільного демократичного) суспільства та необхідність його сталого розвитку, верховенства права, прав і свобод людини і громадянина в Україні.		
Безпека в інформаційно-комунікаційних системах		
РН 1 – застосовувати знання державної та іноземних мов з метою забезпечення ефективності професійної комунікації; РН 2 – організовувати власну професійну діяльність, обирати оптимальні методи та способи розв'язування складних спеціалізованих задач та практичних проблем у професійній діяльності, оцінювати їхню ефективність; РН 3 – використовувати результати самостійного пошуку, аналізу та синтезу інформації з різних джерел для ефективного рішення спеціалізованих задач професійної діяльності; РН 4 – аналізувати, аргументувати,	Пояснювально-ілюстративний (інформаційно-рецептивний) та репродуктивний	Захист лабораторних завдань, експрес-опитування, контрольна робота, залік

приймати рішення при розв’язанні складних спеціалізованих задач та практичних проблем у професійній діяльності, які характеризуються комплексністю та неповною визначеністю умов, відповідати за прийняті рішення; РН 5 – адаптуватися в умовах частої зміни технологій професійної діяльності, прогнозувати кінцевий результат; РН 6 – критично осмислювати основні теорії, принципи, методи і поняття у навчанні та професійній діяльності; РН 7 – діяти на основі законодавчої та нормативно-правової бази України та вимог відповідних стандартів, у тому числі міжнародних в галузі інформаційної та /або кібербезпеки; РН 8 – готувати пропозиції до нормативних актів щодо забезпечення інформаційної та /або кібербезпеки; РН 9 – впроваджувати процеси, що базуються на національних та міжнародних стандартах, виявлення, ідентифікації, аналізу та реагування на інциденти інформаційної та/або кібербезпеки; РН 10 – виконувати аналіз та декомпозицію інформаційно-телекомунікаційних систем; РН 11 – виконувати аналіз зв’язків між інформаційними процесами на віддалених обчислювальних системах; РН 12 – розробляти моделі загроз та порушника; РН 13 – аналізувати проекти інформаційно-телекомунікаційних систем базуючись на стандартизованих технологіях та протоколах передачі даних;		

РН 14 – вирішувати завдання захисту програм та інформації, що обробляється в інформаційно-телекомунікаційних системах програмно-апаратними засобами та давати оцінку результативності якості прийнятих рішень; РН 15 – використовувати сучасне програмно-апаратне забезпечення інформаційно-комунікаційних технологій; РН 16 – реалізовувати комплексні системи захисту інформації в автоматизованих системах (АС) організації (підприємства) відповідно до вимог нормативно-правових документів; РН 17 – забезпечувати процеси захисту та функціонування інформаційно-телекомунікаційних (автоматизованих) систем на основі практик, навичок та знань, щодо структурних (структурно-логічних) схем, топології мережі, сучасних архітектур та моделей захисту електронних інформаційних ресурсів з відображенням взаємозв'язків та інформаційних потоків, процесів для внутрішніх і віддалених компонент; РН 18 – використовувати програмні та програмно-апаратні комплекси захисту інформаційних ресурсів; РН 19 – застосовувати теорії та методи захисту для забезпечення безпеки інформації в інформаційно-телекомунікаційних системах; РН 20 – забезпечувати функціонування спеціального програмного забезпечення, щодо захисту інформації від руйнуючих програмних впливів, руйнуючих кодів в інформаційно-телекомунікаційних системах; РН 21 – вирішувати задачі забезпечення		

та супроводу (в.т. числі: огляд, тестування, підзвітність) системи управління доступом згідно встановленої політики безпеки в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах; РН 22 – вирішувати задачі управління процедурами ідентифікації, автентифікації, авторизації процесів і користувачів в інформаційно-телекомунікаційних системах згідно встановленої політики інформаційної і\або кібербезпеки; РН 23 – реалізовувати заходи з протидії отриманню несанкціонованого доступу до інформаційних ресурсів і процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах; РН 24 – вирішувати задачі управління доступом до інформаційних ресурсів та процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах на основі моделей управління доступом (мандатних, дискреційних, рольових); РН 25 – забезпечувати введення підзвітності системи управління доступом до електронних інформаційних ресурсів і процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах з використанням журналів реєстрації подій, їх аналізу та встановлених процедур захисту; РН 26 – впроваджувати заходи та забезпечувати реалізацію процесів попередження отриманню несанкціонованого доступу і захисту		

інформаційних, інформаційно-телекомунікаційних (автоматизованих) систем на основі еталонної моделі взаємодії відкритих систем; РН 27 – вирішувати задачі захисту потоків даних в інформаційних, інформаційно-телекомунікаційних (автоматизованих) системах; РН 28 – аналізувати та проводити оцінку ефективності та рівня захищеності ресурсів різних класів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах в ході проведення випробувань згідно встановленої політики інформаційної та\або кібербезпеки; РН 29 – здійснювати оцінювання можливості реалізації потенційних загроз інформації, що обробляється в інформаційно-телекомунікаційних системах та ефективності використання комплексів засобів захисту в умовах реалізації загроз різних класів; РН 30 – здійснювати оцінювання можливості несанкціонованого доступу до елементів інформаційно-телекомунікаційних систем; РН 31 – застосовувати теорії та методи захисту для забезпечення безпеки елементів інформаційно-телекомунікаційних систем; РН 32 – вирішувати задачі управління процесами відновлення штатного функціонування інформаційно-телекомунікаційних систем з використанням процедур резервування згідно встановленої політики безпеки; РН 33 – вирішувати задачі забезпечення безперервності бізнес процесів організації		

на основі теорії ризиків; РН 34 – приймати участь у розробці та впровадженні стратегії інформаційної безпеки та/або кібербезпеки відповідно до цілей і завдань організації; РН 35 – вирішувати задачі забезпечення та супроводу комплексних систем захисту інформації, а також протидії несанкціонованому доступу до інформаційних ресурсів і процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах згідно встановленої політики інформаційної і\або кібербезпеки; РН 36 – виявляти небезпечні сигнали технічних засобів; РН 37 – вимірювати параметри небезпечних та завадових сигналів під час інструментального контролю процесів захисту інформації та визначати ефективність захисту інформації від витоку технічними каналами відповідно до вимог нормативних документів системи технічного захисту інформації; РН 38 – інтерпретувати результати проведення спеціальних вимірювань з використанням технічних засобів, контролю характеристик інформаційно-телекомунікаційних систем відповідно до вимог нормативних документів системи технічного захисту інформації; РН 39 – проводити атестацію (спираючись на облік та обстеження) режимних територій (зон), приміщень тощо в умовах додержання режиму секретності із фіксуванням результатів у відповідних документах; РН 40 – інтерпретувати результати проведення спеціальних вимірювань з		

використанням технічних засобів, контролю характеристик ІТС відповідно до вимог нормативних документів системи технічного захисту інформації; РН 41 – забезпечувати неперервність процесу ведення журналів реєстрації подій та інцидентів на основі автоматизованих процедур; РН 42 – впроваджувати процеси виявлення, ідентифікації, аналізу та реагування на інциденти інформаційної і/або кібербезпеки; РН 43 – застосовувати національні та міжнародні регулюючі акти в сфері інформаційної безпеки та/ або кібербезпеки для розслідування інцидентів; РН 44 – вирішувати задачі забезпечення безперервності бізнес-процесів організації на основі теорії ризиків та встановленої системи управління інформаційною безпекою, згідно з вітчизняними та міжнародними вимогами та стандартами; РН 45 – застосовувати ріні класи політик інформаційної безпеки та/ або кібербезпеки, що базуються на ризик-орієнтованому контролі доступу до інформаційних активів; РН 46 – здійснювати аналіз та мінімізацію ризиків обробки інформації в інформаційно-телекомунікаційних системах. РН 47 – вирішувати задачі захисту інформації, що обробляється в інформаційно-телекомунікаційних системах з використанням сучасних методів та засобів криптографічного захисту інформації; РН 48 – виконувати впровадження та		

підтримку систем виявлення вторгнень та використовувати компоненти криптографічного захисту для забезпечення необхідного рівня захищеності інформації в інформаційно-телекомунікаційних системах; РН 49 – забезпечувати належне функціонування системи моніторингу інформаційних ресурсів і процесів в інформаційно-телекомунікаційних системах; РН 50 – забезпечувати функціонування програмних та програмно-апаратних комплексів виявлення вторгнень різних рівнів та класів (статистичних, сигнатурних, статистично-сигнатурних); РН 51 – підтримувати працездатність та забезпечувати конфігурування систем виявлення вторгнень в інформаційно-телекомунікаційних системах; РН 52 – використовувати інструментарій для моніторингу процесів в інформаційно-телекомунікаційних системах. РН 53 – вирішувати задачі аналізу програмного коду на наявність можливих загроз; РН 54 – усвідомлювати цінності громадянського (вільного демократичного) суспільства та необхідність його сталого розвитку, верховенства права, прав і свобод людини і громадянина в Україні.		
Сучасні інформаційні системи (з елементами кібербезпеки)		
РН 1 – застосовувати знання державної та іноземних мов з метою забезпечення ефективності професійної комунікації; РН 2 – організовувати власну професійну діяльність, обирати оптимальні методи та способи розв’язування складних	Пояснювально-ілюстративний (інформаційно-рецептивний) та репродуктивний	Захист лабораторних робіт, лекції, самостійна робота, експрес-опитування, залік, екзамен

спеціалізованих задач та практичних проблем у професійній діяльності, оцінювати їхню ефективність; РН 3 – використовувати результати самостійного пошуку, аналізу та синтезу інформації з різних джерел для ефективного рішення спеціалізованих задач професійної діяльності; РН 4 – аналізувати, аргументувати, приймати рішення при розв'язанні складних спеціалізованих задач та практичних проблем у професійній діяльності, які характеризуються комплексністю та неповною визначеністю умов, відповідати за прийняті рішення; РН 5 – адаптуватися в умовах частої зміни технологій професійної діяльності, прогнозувати кінцевий результат; РН 6 – критично осмислювати основні теорії, принципи, методи і поняття у навчанні та професійній діяльності; РН 7 – діяти на основі законодавчої та нормативно-правової бази України та вимог відповідних стандартів, у тому числі міжнародних в галузі інформаційної та /або кібербезпеки; РН 8 – готувати пропозиції до нормативних актів щодо забезпечення інформаційної та /або кібербезпеки; РН 9 – впроваджувати процеси, що базуються на національних та міжнародних стандартах, виявлення, ідентифікації, аналізу та реагування на інциденти інформаційної та/або кібербезпеки; РН 10 – виконувати аналіз та декомпозицію інформаційно-телекомунікаційних систем; РН 11 – виконувати аналіз зв'язків між		

інформаційними процесами на віддалених обчислювальних системах; РН 12 – розробляти моделі загроз та порушника; РН 13 – аналізувати проекти інформаційно-телекомунікаційних систем базуючись на стандартизованих технологіях та протоколах передачі даних; РН 14 – вирішувати завдання захисту програм та інформації, що обробляється в інформаційно-телекомунікаційних системах програмно-апаратними засобами та давати оцінку результативності якості прийнятих рішень; РН 15 – використовувати сучасне програмно-апаратне забезпечення інформаційно-комунікаційних технологій; РН 16 – реалізовувати комплексні системи захисту інформації в автоматизованих системах (АС) організації (підприємства) відповідно до вимог нормативно-правових документів; РН 17 – забезпечувати процеси захисту та функціонування інформаційно-телекомунікаційних (автоматизованих) систем на основі практик, навичок та знань, щодо структурних (структурно-логічних) схем, топології мережі, сучасних архітектур та моделей захисту електронних інформаційних ресурсів з відображенням взаємозв'язків та інформаційних потоків, процесів для внутрішніх і віддалених компонент; РН 18 – використовувати програмні та програмно-апаратні комплекси захисту інформаційних ресурсів; РН 19 – застосовувати теорії та методи захисту для забезпечення безпеки		

інформації в інформаційно-телекомунікаційних системах; РН 20 – забезпечувати функціонування спеціального програмного забезпечення, щодо захисту інформації від руйнуючих програмних впливів, руйнуючих кодів в інформаційно-телекомунікаційних системах; РН 21 – вирішувати задачі забезпечення та супроводу (в.т. числі: огляд, тестування, підзвітність) системи управління доступом згідно встановленої політики безпеки в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах; РН 22 – вирішувати задачі управління процедурами ідентифікації, автентифікації, авторизації процесів і користувачів в інформаційно-телекомунікаційних системах згідно встановленої політики інформаційної і\або кібербезпеки; РН 23 – реалізовувати заходи з протидії отриманню несанкціонованого доступу до інформаційних ресурсів і процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах; РН 24 – вирішувати задачі управління доступом до інформаційних ресурсів та процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах на основі моделей управління доступом (мандатних, дискреційних, рольових); РН 25 – забезпечувати введення підзвітності системи управління доступом до електронних інформаційних ресурсів і процесів в інформаційних та		

інформаційно-телекомунікаційних (автоматизованих) системах з використанням журналів реєстрації подій, їх аналізу та встановлених процедур захисту; РН 26 – впроваджувати заходи та забезпечувати реалізацію процесів попередження отриманню несанкціонованого доступу і захисту інформаційних, інформаційно-телекомунікаційних (автоматизованих) систем на основі еталонної моделі взаємодії відкритих систем; РН 27 – вирішувати задачі захисту потоків даних в інформаційних, інформаційно-телекомунікаційних (автоматизованих) системах; РН 28 – аналізувати та проводити оцінку ефективності та рівня захищеності ресурсів різних класів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах в ході проведення випробувань згідно встановленої політики інформаційної та\або кібербезпеки; РН 29 – здійснювати оцінювання можливості реалізації потенційних загроз інформації, що обробляється в інформаційно-телекомунікаційних системах та ефективності використання комплексів засобів захисту в умовах реалізації загроз різних класів; РН 30 – здійснювати оцінювання можливості несанкціонованого доступу до елементів інформаційно-телекомунікаційних систем; РН 31 – застосовувати теорії та методи захисту для забезпечення безпеки елементів інформаційно-		

телекомунікаційних систем; РН 32 – вирішувати задачі управління процесами відновлення штатного функціонування інформаційно-телекомунікаційних систем з використанням процедур резервування згідно встановленої політики безпеки; РН 33 – вирішувати задачі забезпечення безперервності бізнес процесів організації на основі теорії ризиків; РН 34 – приймати участь у розробці та впровадженні стратегії інформаційної безпеки та/або кібербезпеки відповідно до цілей і завдань організації; РН 35 – вирішувати задачі забезпечення та супроводу комплексних систем захисту інформації, а також протидії несанкціонованому доступу до інформаційних ресурсів і процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах згідно встановленої політики інформаційної і\або кібербезпеки; РН 36 – виявляти небезпечні сигнали технічних засобів; РН 37 – вимірювати параметри небезпечних та завадових сигналів під час інструментального контролю процесів захисту інформації та визначати ефективність захисту інформації від витоку технічними каналами відповідно до вимог нормативних документів системи технічного захисту інформації; РН 38 – інтерпретувати результати проведення спеціальних вимірювань з використанням технічних засобів, контролю характеристик інформаційно-телекомунікаційних систем відповідно до вимог нормативних документів системи		

технічного захисту інформації; РН 39 – проводити атестацію (спираючись на облік та обстеження) режимних територій (зон), приміщень тощо в умовах додержання режиму секретності із фіксуванням результатів у відповідних документах; РН 40 – інтерпретувати результати проведення спеціальних вимірювань з використанням технічних засобів, контролю характеристик ІТС відповідно до вимог нормативних документів системи технічного захисту інформації; РН 41 – забезпечувати неперервність процесу ведення журналів реєстрації подій та інцидентів на основі автоматизованих процедур; РН 42 – впроваджувати процеси виявлення, ідентифікації, аналізу та реагування на інциденти інформаційної і/або кібербезпеки; РН 43 – застосовувати національні та міжнародні регулюючі акти в сфері інформаційної безпеки та/ або кібербезпеки для розслідування інцидентів; РН 44 – вирішувати задачі забезпечення безперервності бізнес-процесів організації на основі теорії ризиків та встановленої системи управління інформаційною безпекою, згідно з вітчизняними та міжнародними вимогами та стандартами; РН 45 – застосовувати різні класи політик інформаційної безпеки та/ або кібербезпеки, що базуються на ризик-орієнтованому контролі доступу до інформаційних активів; РН 46 – здійснювати аналіз та мінімізацію ризиків обробки інформації в		

інформаційно-телекомунікаційних системах. РН 47 – вирішувати задачі захисту інформації, що обробляється в інформаційно-телекомунікаційних системах з використанням сучасних методів та засобів криптографічного захисту інформації; РН 48 – виконувати впровадження та підтримку систем виявлення вторгнень та використовувати компоненти криптографічного захисту для забезпечення необхідного рівня захищеності інформації в інформаційно-телекомунікаційних системах; РН 49 – забезпечувати належне функціонування системи моніторингу інформаційних ресурсів і процесів в інформаційно-телекомунікаційних системах; РН 50 – забезпечувати функціонування програмних та програмно-апаратних комплексів виявлення вторгнень різних рівнів та класів (статистичних, сигнатурних, статистично-сигнатурних); РН 51 – підтримувати працездатність та забезпечувати конфігурування систем виявлення вторгнень в інформаційно-телекомунікаційних системах; РН 52 – використовувати інструментарій для моніторингу процесів в інформаційно-телекомунікаційних системах. РН 53 – вирішувати задачі аналізу програмного коду на наявність можливих загроз; РН 54 – усвідомлювати цінності громадянського (вільного демократичного) суспільства та необхідність його сталого розвитку,		

верховенства права, прав і свобод людини і громадянина в Україні.		
Комплексні системи захисту інформації		
РН 1 – застосовувати знання державної та іноземних мов з метою забезпечення ефективності професійної комунікації; щодо захисту інформації від руйнуючих програмних впливів, руйнуючих кодів в інформаційно-телекомунікаційних системах; РН 2 – організовувати власну професійну діяльність, обирати оптимальні методи та способи розв'язування складних спеціалізованих задач та практичних проблем у професійній діяльності, оцінювати їхню ефективність; РН 3 – використовувати результати самостійного пошуку, аналізу та синтезу інформації з різних джерел для ефективного рішення спеціалізованих задач професійної діяльності; РН 4 – аналізувати, аргументувати, приймати рішення при розв'язанні складних спеціалізованих задач та практичних проблем у професійній діяльності, які характеризуються комплексністю та неповною визначеністю умов, відповідати за прийняті рішення; РН 5 – адаптуватися в умовах частої зміни технологій професійної діяльності, прогнозувати кінцевий результат; РН 6 – критично осмислювати основні теорії, принципи, методи і поняття у навчанні та професійній діяльності; РН 7 – діяти на основі законодавчої та нормативно-правової бази України та вимог відповідних стандартів, у тому числі міжнародних в галузі інформаційної та /або кібербезпеки;	Пояснювально-ілюстративний (інформаційно-рецептивний) та репродуктивний	Захист лабораторних робіт, експрес-опитування, контрольні роботи, залік

РН 8 – готувати пропозиції до нормативних актів щодо забезпечення інформаційної та /або кібербезпеки; РН 9 – впроваджувати процеси, що базуються на національних та міжнародних стандартах, виявлення, ідентифікації, аналізу та реагування на інциденти інформаційної та/або кібербезпеки; РН 10 – виконувати аналіз та декомпозицію інформаційно-телекомунікаційних систем; РН 11 – виконувати аналіз зв'язків між інформаційними процесами на віддалених обчислювальних системах; РН 12 – розробляти моделі загроз та порушника; РН 13 – аналізувати проекти інформаційно-телекомунікаційних систем базуючись на стандартизованих технологіях та протоколах передачі даних; РН 14 – вирішувати завдання захисту програм та інформації, що обробляється в інформаційно-телекомунікаційних системах програмно-апаратними засобами та давати оцінку результативності якості прийнятих рішень; РН 15 – використовувати сучасне програмно-апаратне забезпечення інформаційно-комунікаційних технологій; РН 16 – реалізовувати комплексні системи захисту інформації в автоматизованих системах (АС) організації (підприємства) відповідно до вимог нормативно-правових документів; РН 17 – забезпечувати процеси захисту та функціонування інформаційно-телекомунікаційних (автоматизованих)		

систем на основі практик, навичок та знань, щодо структурних (структурно-логічних) схем, топології мережі, сучасних архітектур та моделей захисту електронних інформаційних ресурсів з відображенням взаємозв'язків та інформаційних потоків, процесів для внутрішніх і віддалених компонент; РН 18 – використовувати програмні та програмно-апаратні комплекси захисту інформаційних ресурсів; РН 19 – застосовувати теорії та методи захисту для забезпечення безпеки інформації в інформаційно-телекомунікаційних системах; РН 20 – забезпечувати функціонування спеціального програмного забезпечення, щодо захисту інформації від руйнуючих програмних впливів, руйнуючих кодів в інформаційно-телекомунікаційних системах; РН 21 – вирішувати задачі забезпечення та супроводу (в.т. числі: огляд, тестування, підзвітність) системи управління доступом згідно встановленої політики безпеки в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах; РН 22 – вирішувати задачі управління процедурами ідентифікації, автентифікації, авторизації процесів і користувачів в інформаційно-телекомунікаційних системах згідно встановленої політики інформаційної і\або кібербезпеки; РН 23 – реалізовувати заходи з протидії отриманню несанкціонованого доступу до інформаційних ресурсів і процесів в інформаційних та інформаційно-		

телекомунікаційних (автоматизованих) системах; РН 24 – вирішувати задачі управління доступом до інформаційних ресурсів та процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах на основі моделей управління доступом (мандатних, дискреційних, рольових); РН 25 – забезпечувати введення підзвітності системи управління доступом до електронних інформаційних ресурсів і процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах з використанням журналів реєстрації подій, їх аналізу та встановлених процедур захисту; РН 26 – впроваджувати заходи та забезпечувати реалізацію процесів попередження отриманню несанкціонованого доступу і захисту інформаційних, інформаційно-телекомунікаційних (автоматизованих) систем на основі еталонної моделі взаємодії відкритих систем; РН 27 – вирішувати задачі захисту потоків даних в інформаційних, інформаційно-телекомунікаційних (автоматизованих) системах; РН 28 – аналізувати та проводити оцінку ефективності та рівня захищеності ресурсів різних класів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах в ході проведення випробувань згідно встановленої політики інформаційної та\або кібербезпеки; РН 29 – здійснювати оцінювання		

можливості реалізації потенційних загроз інформації, що обробляється в інформаційно-телекомунікаційних системах та ефективності використання комплексів засобів захисту в умовах реалізації загроз різних класів; РН 30 – здійснювати оцінювання можливості несанкціонованого доступу до елементів інформаційно-телекомунікаційних систем; РН 31 – застосовувати теорії та методи захисту для забезпечення безпеки елементів інформаційно-телекомунікаційних систем; РН 32 – вирішувати задачі управління процесами відновлення штатного функціонування інформаційно-телекомунікаційних систем з використанням процедур резервування згідно встановленої політики безпеки; РН 33 – вирішувати задачі забезпечення безперервності бізнес процесів організації на основі теорії ризиків; РН 34 – приймати участь у розробці та впровадженні стратегії інформаційної безпеки та/або кібербезпеки відповідно до цілей і завдань організації; РН 35 – вирішувати задачі забезпечення та супроводу комплексних систем захисту інформації, а також протидії несанкціонованому доступу до інформаційних ресурсів і процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах згідно встановленої політики інформаційної і\або кібербезпеки; РН 36 – виявляти небезпечні сигнали технічних засобів; РН 37 – вимірювати параметри		

небезпечних та завадових сигналів під час інструментального контролю процесів захисту інформації та визначати ефективність захисту інформації від витоку технічними каналами відповідно до вимог нормативних документів системи технічного захисту інформації; РН 38 – інтерпретувати результати проведення спеціальних вимірювань з використанням технічних засобів, контролю характеристик інформаційно-телекомунікаційних систем відповідно до вимог нормативних документів системи технічного захисту інформації; РН 39 – проводити атестацію (спираючись на облік та обстеження) режимних територій (зон), приміщень тощо в умовах додержання режиму секретності із фіксуванням результатів у відповідних документах; РН 40 – інтерпретувати результати проведення спеціальних вимірювань з використанням технічних засобів, контролю характеристик ІТС відповідно до вимог нормативних документів системи технічного захисту інформації; РН 41 – забезпечувати неперервність процесу ведення журналів реєстрації подій та інцидентів на основі автоматизованих процедур; РН 42 – впроваджувати процеси виявлення, ідентифікації, аналізу та реагування на інциденти інформаційної і/або кібербезпеки; РН 43 – застосовувати національні та міжнародні регулюючі акти в сфері інформаційної безпеки та/ або кібербезпеки для розслідування інцидентів;		

РН 44 – вирішувати задачі забезпечення безперервності бізнес-процесів організації на основі теорії ризиків та встановленої системи управління інформаційною безпекою, згідно з вітчизняними та міжнародними вимогами та стандартами; РН 45 – застосовувати ріні класи політик інформаційної безпеки та/ або кібербезпеки, що базуються на ризик-орієнтованому контролі доступу до інформаційних активів; РН 46 – здійснювати аналіз та мінімізацію ризиків обробки інформації в інформаційно-телекомунікаційних системах. РН 47 – вирішувати задачі захисту інформації, що обробляється в інформаційно-телекомунікаційних системах з використанням сучасних методів та засобів криптографічного захисту інформації; РН 48 – виконувати впровадження та підтримку систем виявлення вторгнень та використовувати компоненти криптографічного захисту для забезпечення необхідного рівня захищеності інформації в інформаційно-телекомунікаційних системах; РН 49 – забезпечувати належне функціонування системи моніторингу інформаційних ресурсів і процесів в інформаційно-телекомунікаційних системах; РН 50 – забезпечувати функціонування програмних та програмно-апаратних комплексів виявлення вторгнень різних рівнів та класів (статистичних, сигнатурних, статистично-сигнатурних); РН 51 – підтримувати працездатність та		

забезпечувати конфігурування систем виявлення вторгнень в інформаційно-телекомунікаційних системах; РН 52 – використовувати інструментарій для моніторингу процесів в інформаційно-телекомунікаційних системах. РН 53 – вирішувати задачі аналізу програмного коду на наявність можливих загроз; РН 54 – усвідомлювати цінності громадянського (вільного демократичного) суспільства та необхідність його сталого розвитку, верховенства права, прав і свобод людини і громадянина в Україні.		
Організація і безпека баз даних		
РН 1 – застосовувати знання державної та іноземних мов з метою забезпечення ефективності професійної комунікації; РН 2 – організовувати власну професійну діяльність, обирати оптимальні методи та способи розв'язування складних спеціалізованих задач та практичних проблем у професійній діяльності, оцінювати їхню ефективність; РН 3 – використовувати результати самостійного пошуку, аналізу та синтезу інформації з різних джерел для ефективного рішення спеціалізованих задач професійної діяльності; РН 4 – аналізувати, аргументувати, приймати рішення при розв'язанні складних спеціалізованих задач та практичних проблем у професійній діяльності, які характеризуються комплексністю та неповною визначеністю умов, відповідати за прийняті рішення; РН 5 – адаптуватися в умовах частої зміни технологій професійної діяльності,	Пояснювально-ілюстративний (інформаційно-рецептивний) та репродуктивний	Захист лабораторних завдань, експрес-опитування, контрольна робота, залік

прогнозувати кінцевий результат; РН 6 – критично осмислювати основні теорії, принципи, методи і поняття у навчанні та професійній діяльності; РН 7 – діяти на основі законодавчої та нормативно-правової бази України та вимог відповідних стандартів, у тому числі міжнародних в галузі інформаційної та /або кібербезпеки; РН 8 – готувати пропозиції до нормативних актів щодо забезпечення інформаційної та /або кібербезпеки; РН 9 – впроваджувати процеси, що базуються на національних та міжнародних стандартах, виявлення, ідентифікації, аналізу та реагування на інциденти інформаційної та/або кібербезпеки; РН 10 – виконувати аналіз та декомпозицію інформаційно-телекомунікаційних систем; РН 11 – виконувати аналіз зв'язків між інформаційними процесами на віддалених обчислювальних системах; РН 12 – розробляти моделі загроз та порушника; РН13 – аналізувати проекти інформаційно-телекомунікаційних систем базуючись на стандартизованих технологіях та протоколах передачі даних; РН 14 – вирішувати завдання захисту програм та інформації, що обробляється в інформаційно-телекомунікаційних системах програмно-апаратними засобами та давати оцінку результативності якості прийнятих рішень; РН 15 – використовувати сучасне програмно-апаратне забезпечення		

інформаційно-комунікаційних технологій; РН 16 – реалізовувати комплексні системи захисту інформації в автоматизованих системах (АС) організації (підприємства) відповідно до вимог нормативно-правових документів; РН 17 – забезпечувати процеси захисту та функціонування інформаційно-телекомунікаційних (автоматизованих) систем на основі практик, навичок та знань, щодо структурних (структурно-логічних) схем, топології мережі, сучасних архітектур та моделей захисту електронних інформаційних ресурсів з відображенням взаємозв'язків та інформаційних потоків, процесів для внутрішніх і віддалених компонент; РН 18 – використовувати програмні та програмно-апаратні комплекси захисту інформаційних ресурсів; РН 19 – застосовувати теорії та методи захисту для забезпечення безпеки інформації в інформаційно-телекомунікаційних системах; РН 20 – забезпечувати функціонування спеціального програмного забезпечення, щодо захисту інформації від руйнуючих програмних впливів, руйнуючих кодів в інформаційно-телекомунікаційних системах; РН 21 – вирішувати задачі забезпечення та супроводу (в.т. числі: огляд, тестування, підзвітність) системи управління доступом згідно встановленої політики безпеки в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах; РН 22 – вирішувати задачі управління процедурами ідентифікації,		

автентифікації, авторизації процесів і користувачів в інформаційно-телекомунікаційних системах згідно встановленої політики інформаційної і\або кібербезпеки; РН 23 – реалізовувати заходи з протидії отриманню несанкціонованого доступу до інформаційних ресурсів і процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах; РН 24 – вирішувати задачі управління доступом до інформаційних ресурсів та процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах на основі моделей управління доступом (мандатних, дискреційних, рольових); РН 25 – забезпечувати введення підзвітності системи управління доступом до електронних інформаційних ресурсів і процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах з використанням журналів реєстрації подій, їх аналізу та встановлених процедур захисту; РН 26 – впроваджувати заходи та забезпечувати реалізацію процесів попередження отриманню несанкціонованого доступу і захисту інформаційних, інформаційно-телекомунікаційних (автоматизованих) систем на основі еталонної моделі взаємодії відкритих систем; РН 27 – вирішувати задачі захисту потоків даних в інформаційних, інформаційно-телекомунікаційних (автоматизованих) системах;		

РН 28 – аналізувати та проводити оцінку ефективності та рівня захищеності ресурсів різних класів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах в ході проведення випробувань згідно встановленої політики інформаційної та\або кібербезпеки; РН 29 – здійснювати оцінювання можливості реалізації потенційних загроз інформації, що обробляється в інформаційно-телекомунікаційних системах та ефективності використання комплексів засобів захисту в умовах реалізації загроз різних класів; РН 30 – здійснювати оцінювання можливості несанкціонованого доступу до елементів інформаційно-телекомунікаційних систем; РН 31 – застосовувати теорії та методи захисту для забезпечення безпеки елементів інформаційно-телекомунікаційних систем; РН 32 – вирішувати задачі управління процесами відновлення штатного функціонування інформаційно-телекомунікаційних систем з використанням процедур резервування згідно встановленої політики безпеки; РН 33 – вирішувати задачі забезпечення безперервності бізнес процесів організації на основі теорії ризиків; РН 34 – приймати участь у розробці та впровадженні стратегії інформаційної безпеки та/або кібербезпеки відповідно до цілей і завдань організації; РН 35 – вирішувати задачі забезпечення та супроводу комплексних систем захисту інформації, а також протидії		

несанкціонованому доступу до інформаційних ресурсів і процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах згідно встановленої політики інформаційної і\або кібербезпеки; РН 36 – виявляти небезпечні сигнали технічних засобів; РН 37 – вимірювати параметри небезпечних та завадових сигналів під час інструментального контролю процесів захисту інформації та визначати ефективність захисту інформації від витоку технічними каналами відповідно до вимог нормативних документів системи технічного захисту інформації; РН 38 – інтерпретувати результати проведення спеціальних вимірювань з використанням технічних засобів, контролю характеристик інформаційно-телекомунікаційних систем відповідно до вимог нормативних документів системи технічного захисту інформації; РН 39 – проводити атестацію (спираючись на облік та обстеження) режимних територій (зон), приміщень тощо в умовах додержання режиму секретності із фіксуванням результатів у відповідних документах; РН 40 – інтерпретувати результати проведення спеціальних вимірювань з використанням технічних засобів, контролю характеристик ІТС відповідно до вимог нормативних документів системи технічного захисту інформації; РН 41 – забезпечувати неперервність процесу ведення журналів реєстрації подій та інцидентів на основі автоматизованих процедур;		

РН 42 – впроваджувати процеси виявлення, ідентифікації, аналізу та реагування на інциденти інформаційної і/або кібербезпеки; РН 43 – застосовувати національні та міжнародні регулюючі акти в сфері інформаційної безпеки та/ або кібербезпеки для розслідування інцидентів; РН 44 – вирішувати задачі забезпечення безперервності бізнес-процесів організації на основі теорії ризиків та встановленої системи управління інформаційною безпекою, згідно з вітчизняними та міжнародними вимогами та стандартами; РН 45 – застосовувати ріні класи політик інформаційної безпеки та/ або кібербезпеки, що базуються на ризик-орієнтованому контролі доступу до інформаційних активів; РН 46 – здійснювати аналіз та мінімізацію ризиків обробки інформації в інформаційно-телекомунікаційних системах. РН 47 – вирішувати задачі захисту інформації, що обробляється в інформаційно-телекомунікаційних системах з використанням сучасних методів та засобів криптографічного захисту інформації; РН 48 – виконувати впровадження та підтримку систем виявлення вторгнень та використовувати компоненти криптографічного захисту для забезпечення необхідного рівня захищеності інформації в інформаційно-телекомунікаційних системах; РН 49 – забезпечувати належне функціонування системи моніторингу		

інформаційних ресурсів і процесів в інформаційно-телекомунікаційних системах; РН 50 – забезпечувати функціонування програмних та програмно-апаратних комплексів виявлення вторгнень різних рівнів та класів (статистичних, сигнатурних, статистично-сигнатурних); РН 51 – підтримувати працездатність та забезпечувати конфігурування систем виявлення вторгнень в інформаційно-телекомунікаційних системах; РН 52 – використовувати інструментарій для моніторингу процесів в інформаційно-телекомунікаційних системах. РН 53 – вирішувати задачі аналізу програмного коду на наявність можливих загроз; РН 54 – усвідомлювати цінності громадянського (вільного демократичного) суспільства та необхідність його сталого розвитку, верховенства права, прав і свобод людини і громадянина в Україні.		
Основи стеганографічного захисту інформації		
РН 1 – застосовувати знання державної та іноземних мов з метою забезпечення ефективності професійної комунікації; РН 2 – організовувати власну професійну діяльність, обирати оптимальні методи та способи розв’язування складних спеціалізованих задач та практичних проблем у професійній діяльності, оцінювати їхню ефективність; РН 3 – використовувати результати самостійного пошуку, аналізу та синтезу інформації з різних джерел для ефективного рішення спеціалізованих задач професійної діяльності;	Пояснювально-ілюстративний (інформаційно-рецептивний) та репродуктивний	Захист лабораторних завдань, експрес-опитування, контрольна робота, залік

РН 4 – аналізувати, аргументувати, приймати рішення при розв'язанні складних спеціалізованих задач та практичних проблем у професійній діяльності, які характеризуються комплексністю та неповною визначеністю умов, відповідати за прийняті рішення; РН 5 – адаптуватися в умовах частої зміни технологій професійної діяльності, прогнозувати кінцевий результат; РН 7 – діяти на основі законодавчої та нормативно-правової бази України та вимог відповідних стандартів, у тому числі міжнародних в галузі інформаційної та /або кібербезпеки; РН 8 – готувати пропозиції до нормативних актів щодо забезпечення інформаційної та /або кібербезпеки; РН 9 – впроваджувати процеси, що базуються на національних та міжнародних стандартах, виявлення, ідентифікації, аналізу та реагування на інциденти інформаційної та/або кібербезпеки; РН 10 – виконувати аналіз та декомпозицію інформаційно-телекомунікаційних систем; РН 11 – виконувати аналіз зв'язків між інформаційними процесами на віддалених обчислювальних системах; РН 12 – розробляти моделі загроз та порушника; РН 13 – аналізувати проекти інформаційно-телекомунікаційних систем базуючись на стандартизованих технологіях та протоколах передачі даних; РН 14 – вирішувати завдання захисту програм та інформації, що обробляється в		

інформаційно-телекомунікаційних системах програмно-апаратними засобами та давати оцінку результативності якості прийнятих рішень; РН 15 – використовувати сучасне програмно-апаратне забезпечення інформаційно-комунікаційних технологій; РН 16 – реалізовувати комплексні системи захисту інформації в автоматизованих системах (АС) організації (підприємства) відповідно до вимог нормативно-правових документів; РН 17 – забезпечувати процеси захисту та функціонування інформаційно-телекомунікаційних (автоматизованих) систем на основі практик, навичок та знань, щодо структурних (структурно-логічних) схем, топології мережі, сучасних архітектур та моделей захисту електронних інформаційних ресурсів з відображенням взаємозв'язків та інформаційних потоків, процесів для внутрішніх і віддалених компонент; РН 18 – використовувати програмні та програмно-апаратні комплекси захисту інформаційних ресурсів; РН 19 – застосовувати теорії та методи захисту для забезпечення безпеки інформації в інформаційно-телекомунікаційних системах; РН 20 – забезпечувати функціонування спеціального програмного забезпечення, щодо захисту інформації від руйнуючих програмних впливів, руйнуючих кодів в інформаційно-телекомунікаційних системах; РН 21 – вирішувати задачі забезпечення та супроводу (в.т. числі: огляд, тестування, підзвітність) системи		

управління доступом згідно встановленої політики безпеки в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах; РН 22 – вирішувати задачі управління процедурами ідентифікації, автентифікації, авторизації процесів і користувачів в інформаційно-телекомунікаційних системах згідно встановленої політики інформаційної і\або кібербезпеки; РН 24 – вирішувати задачі управління доступом до інформаційних ресурсів та процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах на основі моделей управління доступом (мандатних, дискреційних, рольових); РН 25 – забезпечувати введення підзвітності системи управління доступом до електронних інформаційних ресурсів і процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах з використанням журналів реєстрації подій, їх аналізу та встановлених процедур захисту; РН 26 – впроваджувати заходи та забезпечувати реалізацію процесів попередження отриманню несанкціонованого доступу і захисту інформаційних, інформаційно-телекомунікаційних (автоматизованих) систем на основі еталонної моделі взаємодії відкритих систем; РН 27 – вирішувати задачі захисту потоків даних в інформаційних, інформаційно-телекомунікаційних (автоматизованих) системах;		

РН 28 – аналізувати та проводити оцінку ефективності та рівня захищеності ресурсів різних класів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах в ході проведення випробувань згідно встановленої політики інформаційної та\або кібербезпеки; РН 29 – здійснювати оцінювання можливості реалізації потенційних загроз інформації, що обробляється в інформаційно-телекомунікаційних системах та ефективності використання комплексів засобів захисту в умовах реалізації загроз різних класів; РН 32 – вирішувати задачі управління процесами відновлення штатного функціонування інформаційно-телекомунікаційних систем з використанням процедур резервування згідно встановленої політики безпеки; РН 33 – вирішувати задачі забезпечення безперервності бізнес процесів організації на основі теорії ризиків; РН 34 – приймати участь у розробці та впровадженні стратегії інформаційної безпеки та/або кібербезпеки відповідно до цілей і завдань організації; РН 35 – вирішувати задачі забезпечення та супроводу комплексних систем захисту інформації, а також протидії несанкціонованому доступу до інформаційних ресурсів і процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах згідно встановленої політики інформаційної і\або кібербезпеки; РН 41 – забезпечувати неперервність процесу ведення журналів реєстрації		

подій та інцидентів на основі автоматизованих процедур; РН 42 – впроваджувати процеси виявлення, ідентифікації, аналізу та реагування на інциденти інформаційної і/або кібербезпеки; РН 43 – застосовувати національні та міжнародні регулюючі акти в сфері інформаційної безпеки та/ або кібербезпеки для розслідування інцидентів; РН 44 – вирішувати задачі забезпечення безперервності бізнес-процесів організації на основі теорії ризиків та встановленої системи управління інформаційною безпекою, згідно з вітчизняними та міжнародними вимогами та стандартами; РН 45 – застосовувати ріні класи політик інформаційної безпеки та/ або кібербезпеки, що базуються на ризик-орієнтованому контролі доступу до інформаційних активів; РН 46 – здійснювати аналіз та мінімізацію ризиків обробки інформації в інформаційно-телекомунікаційних системах; РН 47 – вирішувати задачі захисту інформації, що обробляється в інформаційно-телекомунікаційних системах з використанням сучасних методів та засобів криптографічного захисту інформації; РН 48 – виконувати впровадження та підтримку систем виявлення вторгнень та використовувати компоненти криптографічного захисту для забезпечення необхідного рівня захищеності інформації в інформаційно-телекомунікаційних системах;		

РН 49 – забезпечувати належне функціонування системи моніторингу інформаційних ресурсів і процесів в інформаційно-телекомунікаційних системах; РН 50 – забезпечувати функціонування програмних та програмно-апаратних комплексів виявлення вторгнень різних рівнів та класів (статистичних, сигнатурних, статистично-сигнатурних); РН 51 – підтримувати працездатність та забезпечувати конфігурування систем виявлення вторгнень в інформаційно-телекомунікаційних системах; РН 52 – використовувати інструментарій для моніторингу процесів в інформаційно-телекомунікаційних системах. РН 53 – вирішувати задачі аналізу програмного коду на наявність можливих загроз; РН 54 – усвідомлювати цінності громадянського (вільного демократичного) суспільства та необхідність його сталого розвитку, верховенства права, прав і свобод людини і громадянина в Україні.		
Основи соціальної інженерії		
РН 9 – впроваджувати процеси, що базуються на національних та міжнародних стандартах, виявлення, ідентифікації, аналізу та реагування на інциденти інформаційної та/або кібербезпеки; РН 13 – аналізувати проекти інформаційно-телекомунікаційних систем базуючись на стандартизованих технологіях та протоколах передачі даних; РН 14 – вирішувати завдання захисту	Пояснювально-ілюстративний (інформаційно-рецептивний) та репродуктивний	Захист практичних робіт, проведення контрольних робіт, тестування, презентації докладів за темами лекційних занять, залік

програм та інформації, що обробляється в інформаційно-телекомунікаційних системах програмно-апаратними засобами та давати оцінку результативності якості прийнятих рішень; РН 17 – забезпечувати процеси захисту та функціонування інформаційно-телекомунікаційних (автоматизованих) систем на основі практик, навичок та знань, щодо структурних (структурно-логічних) схем, топології мережі, сучасних архітектур та моделей захисту електронних інформаційних ресурсів з відображенням взаємозв'язків та інформаційних потоків, процесів для внутрішніх і віддалених компонент; РН 18 – використовувати програмні та програмно-апаратні комплекси захисту інформаційних ресурсів; РН 19 – застосовувати теорії та методи захисту для забезпечення безпеки інформації в інформаційно-телекомунікаційних системах; РН 20 – забезпечувати функціонування спеціального програмного забезпечення, щодо захисту інформації від руйнуючих програмних впливів, руйнуючих кодів в інформаційно-телекомунікаційних системах; РН 21 – вирішувати задачі забезпечення та супроводу (в.т. числі: огляд, тестування, підзвітність) системи управління доступом згідно встановленої політики безпеки в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах; РН 22 – вирішувати задачі управління процедурами ідентифікації,		

автентифікації, авторизації процесів і користувачів в інформаційно-телекомунікаційних системах згідно встановленої політики інформаційної і\або кібербезпеки; РН 23 – реалізовувати заходи з протидії отриманню несанкціонованого доступу до інформаційних ресурсів і процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах; РН 24 – вирішувати задачі управління доступом до інформаційних ресурсів та процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах на основі моделей управління доступом (мандатних, дискреційних, рольових); РН 25 – забезпечувати введення підзвітності системи управління доступом до електронних інформаційних ресурсів і процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах з використанням журналів реєстрації подій, їх аналізу та встановлених процедур захисту; РН 26 – впроваджувати заходи та забезпечувати реалізацію процесів попередження отриманню несанкціонованого доступу і захисту інформаційних, інформаційно-телекомунікаційних (автоматизованих) систем на основі еталонної моделі взаємодії відкритих систем; РН 27 – вирішувати задачі захисту потоків даних в інформаційних, інформаційно-телекомунікаційних (автоматизованих) системах;		

РН 28 – аналізувати та проводити оцінку ефективності та рівня захищеності ресурсів різних класів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах в ході проведення випробувань згідно встановленої політики інформаційної та\або кібербезпеки; РН 29 – здійснювати оцінювання можливості реалізації потенційних загроз інформації, що обробляється в інформаційно-телекомунікаційних системах та ефективності використання комплексів засобів захисту в умовах реалізації загроз різних класів; РН 32 – вирішувати задачі управління процесами відновлення штатного функціонування інформаційно-телекомунікаційних систем з використанням процедур резервування згідно встановленої політики безпеки; РН 33 – вирішувати задачі забезпечення безперервності бізнес процесів організації на основі теорії ризиків; РН 34 – приймати участь у розробці та впровадженні стратегії інформаційної безпеки та/або кібербезпеки відповідно до цілей і завдань організації; РН 35 – вирішувати задачі забезпечення та супроводу комплексних систем захисту інформації, а також протидії несанкціонованому доступу до інформаційних ресурсів і процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах згідно встановленої політики інформаційної і\або кібербезпеки; РН 41 – забезпечувати неперервність процесу ведення журналів реєстрації		

подій та інцидентів на основі автоматизованих процедур; РН 42 – впроваджувати процеси виявлення, ідентифікації, аналізу та реагування на інциденти інформаційної і/або кібербезпеки; РН 43 – застосовувати національні та міжнародні регулюючі акти в сфері інформаційної безпеки та/ або кібербезпеки для розслідування інцидентів; РН 44 – вирішувати задачі забезпечення безперервності бізнес-процесів організації на основі теорії ризиків та встановленої системи управління інформаційною безпекою, згідно з вітчизняними та міжнародними вимогами та стандартами; РН 45 – застосовувати ріні класи політик інформаційної безпеки та/ або кібербезпеки, що базуються на ризик-орієнтованому контролі доступу до інформаційних активів; РН 46 – здійснювати аналіз та мінімізацію ризиків обробки інформації в інформаційно-телекомунікаційних системах; РН 47 – вирішувати задачі захисту інформації, що обробляється в інформаційно-телекомунікаційних системах з використанням сучасних методів та засобів криптографічного захисту інформації; РН 48 – виконувати впровадження та підтримку систем виявлення вторгнень та використовувати компоненти криптографічного захисту для забезпечення необхідного рівня захищеності інформації в інформаційно-телекомунікаційних		

системах; РН 49 – забезпечувати належне функціонування системи моніторингу інформаційних ресурсів і процесів в інформаційно-телекомунікаційних системах; РН 50 – забезпечувати функціонування програмних та програмно-апаратних комплексів виявлення вторгнень різних рівнів та класів (статистичних, сигнатурних, статистично-сигнатурних); РН 51 – підтримувати працездатність та забезпечувати конфігурування систем виявлення вторгнень в інформаційно-телекомунікаційних системах; РН 52 – використовувати інструментарій для моніторингу процесів в інформаційно-телекомунікаційних системах; РН 53 – вирішувати задачі аналізу програмного коду на наявність можливих загроз.		
Комплексний тренінг		
РН 1 – застосовувати знання державної та іноземних мов з метою забезпечення ефективності професійної комунікації; РН 2 – організовувати власну професійну діяльність, обирати оптимальні методи та способи розв'язування складних спеціалізованих задач та практичних проблем у професійній діяльності, оцінювати їхню ефективність; РН 3 – використовувати результати самостійного пошуку, аналізу та синтезу інформації з різних джерел для ефективного рішення спеціалізованих задач професійної діяльності; РН 4 – аналізувати, аргументувати, приймати рішення при розв'язанні складних спеціалізованих задач та	Пояснювально-ілюстративний (інформаційно-рецептивний) та репродуктивний	Захист лабораторних завдань, тестування, залік

практичних проблем у професійній діяльності, які характеризуються комплексністю та неповною визначеністю умов, відповідати за прийняті рішення; РН 5 – адаптуватися в умовах частої зміни технологій професійної діяльності, прогнозувати кінцевий результат; РН 6 – критично осмислювати основні теорії, принципи, методи і поняття у навчанні та професійній діяльності; РН 7 – діяти на основі законодавчої та нормативно-правової бази України та вимог відповідних стандартів, у тому числі міжнародних в галузі інформаційної та /або кібербезпеки; РН 8 – готувати пропозиції до нормативних актів щодо забезпечення інформаційної та /або кібербезпеки; РН 9 – впроваджувати процеси, що базуються на національних та міжнародних стандартах, виявлення, ідентифікації, аналізу та реагування на інциденти інформаційної та/або кібербезпеки; РН 10 – виконувати аналіз та декомпозицію інформаційно-телекомунікаційних систем; РН 11 – виконувати аналіз зв'язків між інформаційними процесами на віддалених обчислювальних системах; РН 12 – розробляти моделі загроз та порушника; РН 13 – аналізувати проекти інформаційно-телекомунікаційних систем базуючись на стандартизованих технологіях та протоколах передачі даних; РН 14 – вирішувати завдання захисту програм та інформації, що обробляється в		

інформаційно-телекомунікаційних системах програмно-апаратними засобами та давати оцінку результативності якості прийнятих рішень; РН 15 – використовувати сучасне програмно-апаратне забезпечення інформаційно-комунікаційних технологій; РН 16 – реалізовувати комплексні системи захисту інформації в автоматизованих системах (АС) організації (підприємства) відповідно до вимог нормативно-правових документів; РН 17 – забезпечувати процеси захисту та функціонування інформаційно-телекомунікаційних (автоматизованих) систем на основі практик, навичок та знань, щодо структурних (структурно-логічних) схем, топології мережі, сучасних архітектур та моделей захисту електронних інформаційних ресурсів з відображенням взаємозв'язків та інформаційних потоків, процесів для внутрішніх і віддалених компонент; РН 18 – використовувати програмні та програмно-апаратні комплекси захисту інформаційних ресурсів; РН 19 – застосовувати теорії та методи захисту для забезпечення безпеки інформації в інформаційно-телекомунікаційних системах; РН 20 – забезпечувати функціонування спеціального програмного забезпечення, щодо захисту інформації від руйнуючих програмних впливів, руйнуючих кодів в інформаційно-телекомунікаційних системах; РН 21 – вирішувати задачі забезпечення та супроводу (в.т. числі: огляд, тестування, підзвітність) системи		

управління доступом згідно встановленої політики безпеки в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах; РН 22 – вирішувати задачі управління процедурами ідентифікації, автентифікації, авторизації процесів і користувачів в інформаційно-телекомунікаційних системах згідно встановленої політики інформаційної і\або кібербезпеки; РН 23 – реалізовувати заходи з протидії отриманню несанкціонованого доступу до інформаційних ресурсів і процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах; РН 24 – вирішувати задачі управління доступом до інформаційних ресурсів та процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах на основі моделей управління доступом (мандатних, дискреційних, рольових); РН 25 – забезпечувати введення підзвітності системи управління доступом до електронних інформаційних ресурсів і процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах з використанням журналів реєстрації подій, їх аналізу та встановлених процедур захисту; РН 26 – впроваджувати заходи та забезпечувати реалізацію процесів попередження отриманню несанкціонованого доступу і захисту інформаційних, інформаційно-телекомунікаційних (автоматизованих)		

систем на основі еталонної моделі взаємодії відкритих систем; РН 27 – вирішувати задачі захисту потоків даних в інформаційних, інформаційно-телекомунікаційних (автоматизованих) системах; РН 28 – аналізувати та проводити оцінку ефективності та рівня захищеності ресурсів різних класів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах в ході проведення випробувань згідно встановленої політики інформаційної та\або кібербезпеки; РН 29 – здійснювати оцінювання можливості реалізації потенційних загроз інформації, що обробляється в інформаційно-телекомунікаційних системах та ефективності використання комплексів засобів захисту в умовах реалізації загроз різних класів; РН 30 – здійснювати оцінювання можливості несанкціонованого доступу до елементів інформаційно-телекомунікаційних систем; РН 31 – застосовувати теорії та методи захисту для забезпечення безпеки елементів інформаційно-телекомунікаційних систем; РН 32 – вирішувати задачі управління процесами відновлення штатного функціонування інформаційно-телекомунікаційних систем з використанням процедур резервування згідно встановленої політики безпеки; РН 33 – вирішувати задачі забезпечення безперервності бізнес процесів організації на основі теорії ризиків; РН 34 – приймати участь у розробці та		

впровадженні стратегії інформаційної безпеки та/або кібербезпеки відповідно до цілей і завдань організації; РН 35 – вирішувати задачі забезпечення та супроводу комплексних систем захисту інформації, а також протидії несанкціонованому доступу до інформаційних ресурсів і процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах згідно встановленої політики інформаційної і\або кібербезпеки; РН 36 – виявляти небезпечні сигнали технічних засобів; РН 37 – вимірювати параметри небезпечних та завадових сигналів під час інструментального контролю процесів захисту інформації та визначати ефективність захисту інформації від витоку технічними каналами відповідно до вимог нормативних документів системи технічного захисту інформації; РН 38 – інтерпретувати результати проведення спеціальних вимірювань з використанням технічних засобів, контролю характеристик інформаційно-телекомунікаційних систем відповідно до вимог нормативних документів системи технічного захисту інформації; РН 39 – проводити атестацію (спираючись на облік та обстеження) режимних територій (зон), приміщень тощо в умовах додержання режиму секретності із фіксуванням результатів у відповідних документах; РН 40 – інтерпретувати результати проведення спеціальних вимірювань з використанням технічних засобів, контролю характеристик ІТС відповідно		

до вимог нормативних документів системи технічного захисту інформації; РН 41 – забезпечувати неперервність процесу ведення журналів реєстрації подій та інцидентів на основі автоматизованих процедур; РН 42 – впроваджувати процеси виявлення, ідентифікації, аналізу та реагування на інциденти інформаційної і/або кібербезпеки; РН 43 – застосовувати національні та міжнародні регулюючі акти в сфері інформаційної безпеки та/ або кібербезпеки для розслідування інцидентів; РН 44 – вирішувати задачі забезпечення безперервності бізнес-процесів організації на основі теорії ризиків та встановленої системи управління інформаційною безпекою, згідно з вітчизняними та міжнародними вимогами та стандартами; РН 45 – застосовувати ріні класи політик інформаційної безпеки та/ або кібербезпеки, що базуються на ризик-орієнтованому контролі доступу до інформаційних активів; РН 46 – здійснювати аналіз та мінімізацію ризиків обробки інформації в інформаційно-телекомунікаційних системах; РН 47 – вирішувати задачі захисту інформації, що обробляється в інформаційно-телекомунікаційних системах з використанням сучасних методів та засобів криптографічного захисту інформації; РН 48 – виконувати впровадження та підтримку систем виявлення вторгнень та використовувати компоненти		

криптографічного захисту для забезпечення необхідного рівня захищеності інформації в інформаційно-телекомунікаційних системах; РН 49 – забезпечувати належне функціонування системи моніторингу інформаційних ресурсів і процесів в інформаційно-телекомунікаційних системах; РН 50 – забезпечувати функціонування програмних та програмно-апаратних комплексів виявлення вторгнень різних рівнів та класів (статистичних, сигнатурних, статистично-сигнатурних); РН 51 – підтримувати працездатність та забезпечувати конфігурування систем виявлення вторгнень в інформаційно-телекомунікаційних системах; РН 52 – використовувати інструментарій для моніторингу процесів; РН 53 – вирішувати задачі аналізу програмного коду на наявність можливих загроз; РН 54 – усвідомлювати цінності громадянського (вільного демократичного) суспільства та необхідність його сталого розвитку, верховенства права, прав і свобод людини і громадянина в Україні.		
Бізнес інтелідженс		
РН 9 – впроваджувати процеси, що базуються на національних та міжнародних стандартах, виявлення, ідентифікації, аналізу та реагування на інциденти інформаційної та/або кібербезпеки; РН 10 – виконувати аналіз та декомпозицію інформаційно-телекомунікаційних систем;	Пояснювально-ілюстративний (інформаційно-рецептивний) та репродуктивний	Опитування, захист лабораторних завдань, контрольна робота, залік

РН 11 – виконувати аналіз зв'язків між інформаційними процесами на віддалених обчислювальних системах; РН 12 – розробляти моделі загроз та порушника; РН 13 – аналізувати проекти інформаційно-телекомунікаційних систем базуючись на стандартизованих технологіях та протоколах передачі даних; РН 14 – вирішувати завдання захисту програм та інформації, що обробляється в інформаційно-телекомунікаційних системах програмно-апаратними засобами та давати оцінку результативності якості прийнятих рішень; РН 15 – використовувати сучасне програмно-апаратне забезпечення інформаційно-комунікаційних технологій; РН 16 – реалізовувати комплексні системи захисту інформації в автоматизованих системах (АС) організації (підприємства) відповідно до вимог нормативно-правових документів; РН 17 – забезпечувати процеси захисту та функціонування інформаційно-телекомунікаційних (автоматизованих) систем на основі практик, навичок та знань, щодо структурних (структурно-логічних) схем, топології мережі, сучасних архітектур та моделей захисту електронних інформаційних ресурсів з відображенням взаємозв'язків та інформаційних потоків, процесів для внутрішніх і віддалених компонент; РН 18 – використовувати програмні та програмно-апаратні комплекси захисту інформаційних ресурсів; РН 19 – застосовувати теорії та методи		

захисту для забезпечення безпеки інформації в інформаційно-телекомунікаційних системах; РН 21 – вирішувати задачі забезпечення та супроводу (в.т. числі: огляд, тестування, підзвітність) системи управління доступом згідно встановленої політики безпеки в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах; РН 22 – вирішувати задачі управління процедурами ідентифікації, автентифікації, авторизації процесів і користувачів в інформаційно-телекомунікаційних системах згідно встановленої політики інформаційної і\або кібербезпеки; РН 23 – реалізовувати заходи з протидії отриманню несанкціонованого доступу до інформаційних ресурсів і процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах; РН 24 – вирішувати задачі управління доступом до інформаційних ресурсів та процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах на основі моделей управління доступом (мандатних, дискреційних, рольових); РН 25 – забезпечувати введення підзвітності системи управління доступом до електронних інформаційних ресурсів і процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах з використанням журналів реєстрації подій, їх аналізу та встановлених процедур захисту;		

РН 26 – впроваджувати заходи та забезпечувати реалізацію процесів попередження отриманню несанкціонованого доступу і захисту інформаційних, інформаційно-телекомунікаційних (автоматизованих) систем на основі еталонної моделі взаємодії відкритих систем; РН 28 – аналізувати та проводити оцінку ефективності та рівня захищеності ресурсів різних класів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах в ході проведення випробувань згідно встановленої політики інформаційної та\або кібербезпеки; РН 29 – здійснювати оцінювання можливості реалізації потенційних загроз інформації, що обробляється в інформаційно-телекомунікаційних системах та ефективності використання комплексів засобів захисту в умовах реалізації загроз різних класів; РН 30 – здійснювати оцінювання можливості несанкціонованого доступу до елементів інформаційно-телекомунікаційних систем; РН 32 – вирішувати задачі управління процесами відновлення штатного функціонування інформаційно-телекомунікаційних систем з використанням процедур резервування згідно встановленої політики безпеки; РН 33 – вирішувати задачі забезпечення безперервності бізнес процесів організації на основі теорії ризиків; РН 34 – приймати участь у розробці та впровадженні стратегії інформаційної безпеки та/або кібербезпеки відповідно до		

цілей і завдань організації; РН 35 – вирішувати задачі забезпечення та супроводу комплексних систем захисту інформації, а також протидії несанкціонованому доступу до інформаційних ресурсів і процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах згідно встановленої політики інформаційної і\або кібербезпеки; РН 41 – забезпечувати неперервність процесу ведення журналів реєстрації подій та інцидентів на основі автоматизованих процедур; РН 42 – впроваджувати процеси виявлення, ідентифікації, аналізу та реагування на інциденти інформаційної і/або кібербезпеки; РН 43 – застосовувати національні та міжнародні регулюючі акти в сфері інформаційної безпеки та/ або кібербезпеки для розслідування інцидентів; РН 44 – вирішувати задачі забезпечення безперервності бізнес-процесів організації на основі теорії ризиків та встановленої системи управління інформаційною безпекою, згідно з вітчизняними та міжнародними вимогами та стандартами; РН 45 – застосовувати ріні класи політик інформаційної безпеки та/ або кібербезпеки, що базуються на ризик-орієнтованому контролі доступу до інформаційних активів; РН 46 – здійснювати аналіз та мінімізацію ризиків обробки інформації в інформаційно-телекомунікаційних системах; РН 48 – виконувати впровадження та		

підтримку систем виявлення вторгнень та використовувати компоненти криптографічного захисту для забезпечення необхідного рівня захищеності інформації в інформаційно-телекомунікаційних системах; РН 49 – забезпечувати належне функціонування системи моніторингу інформаційних ресурсів і процесів в інформаційно-телекомунікаційних системах; РН 50 – забезпечувати функціонування програмних та програмно-апаратних комплексів виявлення вторгнень різних рівнів та класів (статистичних, сигнатурних, статистично-сигнатурних); РН 51 – підтримувати працездатність та забезпечувати конфігурування систем виявлення вторгнень в інформаційно-телекомунікаційних системах; РН 52 – використовувати інструментарій для моніторингу процесів в інформаційно-телекомунікаційних системах; РН 53 – вирішувати задачі аналізу програмного коду на наявність можливих загроз.		
Комплексні засоби захисту інформації		
РН 1 – застосовувати знання державної та іноземних мов з метою забезпечення ефективності професійної комунікації; РН 2 – організовувати власну професійну діяльність, обирати оптимальні методи та способи розв'язування складних спеціалізованих задач та практичних проблем у професійній діяльності, оцінювати їхню ефективність; РН 3 – використовувати результати самостійного пошуку, аналізу та синтезу інформації з різних джерел для	Виконання лабораторних робіт, виконання та демонстрація індивідуальних завдань, використання необхідних програмних та апаратних інструментальних засобив: CodeBlocks, IntelijIdea, git, VisualStudioCode, розробка реальних проєктів, взявши участь у програмі "Інноваційний кампус" НТУ "ХПІ"	Захист лабораторних робіт, контрольні роботи, тестування, презентації докладів за темами лекційних занять, залік

ефективного рішення спеціалізованих задач професійної діяльності; РН 4 – аналізувати, аргументувати, приймати рішення при розв'язанні складних спеціалізованих задач та практичних проблем у професійній діяльності, які характеризуються комплексністю та неповною визначеністю умов, відповідати за прийняті рішення; РН 5 – адаптуватися в умовах частої зміни технологій професійної діяльності, прогнозувати кінцевий результат; РН 6 – критично осмислювати основні теорії, принципи, методи і поняття у навчанні та професійній діяльності; РН 7 – діяти на основі законодавчої та нормативно-правової бази України та вимог відповідних стандартів, у тому числі міжнародних в галузі інформаційної та /або кібербезпеки; РН 8 – готувати пропозиції до нормативних актів щодо забезпечення інформаційної та /або кібербезпеки; РН 9 – впроваджувати процеси, що базуються на національних та міжнародних стандартах, виявлення, ідентифікації, аналізу та реагування на інциденти інформаційної та/або кібербезпеки; РН 10 – виконувати аналіз та декомпозицію інформаційно-телекомунікаційних систем; РН 11 – виконувати аналіз зв'язків між інформаційними процесами на віддалених обчислювальних системах; РН 12 – розробляти моделі загроз та порушника; РН 13 – аналізувати проекти інформаційно-телекомунікаційних систем		

базуючись на стандартизованих технологіях та протоколах передачі даних; РН 14 – вирішувати завдання захисту програм та інформації, що обробляється в інформаційно-телекомунікаційних системах програмно-апаратними засобами та давати оцінку результативності якості прийнятих рішень; РН 15 – використовувати сучасне програмно-апаратне забезпечення інформаційно-комунікаційних технологій; РН 16 – реалізовувати комплексні системи захисту інформації в автоматизованих системах (АС) організації (підприємства) відповідно до вимог нормативно-правових документів; РН 17 – забезпечувати процеси захисту та функціонування інформаційно-телекомунікаційних (автоматизованих) систем на основі практик, навичок та знань, щодо структурних (структурно-логічних) схем, топології мережі, сучасних архітектур та моделей захисту електронних інформаційних ресурсів з відображенням взаємозв'язків та інформаційних потоків, процесів для внутрішніх і віддалених компонент; РН 18 – використовувати програмні та програмно-апаратні комплекси захисту інформаційних ресурсів; РН 19 – застосовувати теорії та методи захисту для забезпечення безпеки інформації в інформаційно-телекомунікаційних системах; РН 20 – забезпечувати функціонування спеціального програмного забезпечення, щодо захисту інформації від руйнуючих програмних впливів, руйнуючих кодів в		

інформаційно-телекомунікаційних системах; РН 21 – вирішувати задачі забезпечення та супроводу (в.т. числі: огляд, тестування, підзвітність) системи управління доступом згідно встановленої політики безпеки в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах; РН 22 – вирішувати задачі управління процедурами ідентифікації, автентифікації, авторизації процесів і користувачів в інформаційно-телекомунікаційних системах згідно встановленої політики інформаційної і\або кібербезпеки; РН 23 – реалізовувати заходи з протидії отриманню несанкціонованого доступу до інформаційних ресурсів і процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах; РН 24 – вирішувати задачі управління доступом до інформаційних ресурсів та процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах на основі моделей управління доступом (мандатних, дискреційних, рольових); РН 25 – забезпечувати введення підзвітності системи управління доступом до електронних інформаційних ресурсів і процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах з використанням журналів реєстрації подій, їх аналізу та встановлених процедур захисту;		

РН 26 – впроваджувати заходи та забезпечувати реалізацію процесів попередження отриманню несанкціонованого доступу і захисту інформаційних, інформаційно-телекомунікаційних (автоматизованих) систем на основі еталонної моделі взаємодії відкритих систем; РН 27 – вирішувати задачі захисту потоків даних в інформаційних, інформаційно-телекомунікаційних (автоматизованих) системах; РН 28 – аналізувати та проводити оцінку ефективності та рівня захищеності ресурсів різних класів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах в ході проведення випробувань згідно встановленої політики інформаційної та\або кібербезпеки; РН 29 – здійснювати оцінювання можливості реалізації потенційних загроз інформації, що обробляється в інформаційно-телекомунікаційних системах та ефективності використання комплексів засобів захисту в умовах реалізації загроз різних класів; РН 30 – здійснювати оцінювання можливості несанкціонованого доступу до елементів інформаційно-телекомунікаційних систем; РН 31 – застосовувати теорії та методи захисту для забезпечення безпеки елементів інформаційнотелекомунікаційних систем; РН 32 – вирішувати задачі управління процесами відновлення штатного функціонування інформаційно-телекомунікаційних систем з		

використанням процедур резервування згідно встановленої політики безпеки; РН 33 – вирішувати задачі забезпечення безперервності бізнес процесів організації на основі теорії ризиків; РН 34 – приймати участь у розробці та впровадженні стратегії інформаційної безпеки та/або кібербезпеки відповідно до цілей і завдань організації; РН 35 – вирішувати задачі забезпечення та супроводу комплексних систем захисту інформації, а також протидії несанкціонованому доступу до інформаційних ресурсів і процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах згідно встановленої політики інформаційної і\або кібербезпеки; РН 36 – виявляти небезпечні сигнали технічних засобів; РН 37 – вимірювати параметри небезпечних та завадових сигналів під час інструментального контролю процесів захисту інформації та визначати ефективність захисту інформації від витоку технічними каналами відповідно до вимог нормативних документів системи технічного захисту інформації; РН 38 – інтерпретувати результати проведення спеціальних вимірювань з використанням технічних засобів, контролю характеристик інформаційно-телекомунікаційних систем відповідно до вимог нормативних документів системи технічного захисту інформації; РН 39 – проводити атестацію (спираючись на облік та обстеження) режимних територій (зон), приміщень тощо в умовах		

додержання режиму секретності із фіксуванням результатів у відповідних документах; РН 40 – інтерпретувати результати проведення спеціальних вимірювань з використанням технічних засобів, контролю характеристик ІТС відповідно до вимог нормативних документів системи технічного захисту інформації; РН 41 – забезпечувати неперервність процесу ведення журналів реєстрації подій та інцидентів на основі автоматизованих процедур; РН 42 – впроваджувати процеси виявлення, ідентифікації, аналізу та реагування на інциденти інформаційної і/або кібербезпеки; РН 43 – застосовувати національні та міжнародні регулюючі акти в сфері інформаційної безпеки та/ або кібербезпеки для розслідування інцидентів; РН 44 – вирішувати задачі забезпечення безперервності бізнес-процесів організації на основі теорії ризиків та встановленої системи управління інформаційною безпекою, згідно з вітчизняними та міжнародними вимогами та стандартами; РН 45 – застосовувати ріні класи політик інформаційної безпеки та/ або кібербезпеки, що базуються на ризикорієнтованому контролі доступу до інформаційних активів; РН 46 – здійснювати аналіз та мінімізацію ризиків обробки інформації в інформаційно-телекомунікаційних системах; РН 47 – вирішувати задачі захисту інформації, що обробляється в		

інформаційно-телекомунікаційних системах з використанням сучасних методів та засобів криптографічного захисту інформації; РН 48 – виконувати впровадження та підтримку систем виявлення вторгнень та використовувати компоненти криптографічного захисту для забезпечення необхідного рівня захищеності інформації в інформаційно-телекомунікаційних системах; РН 49 – забезпечувати належне функціонування системи моніторингу інформаційних ресурсів і процесів в інформаційно-телекомунікаційних системах; РН 50 – забезпечувати функціонування програмних та програмно-апаратних комплексів виявлення вторгнень різних рівнів та класів (статистичних, сигнатурних, статистично-сигнатурних); РН 51 – підтримувати працездатність та забезпечувати конфігурування систем виявлення вторгнень в інформаційно-телекомунікаційних системах; РН 52 – використовувати інструментарій для моніторингу процесів в інформаційно-телекомунікаційних системах; РН 53 – вирішувати задачі аналізу програмного коду на наявність можливих загроз. РН 54 – усвідомлювати цінності громадянського (вільного демократичного) суспільства та необхідність його сталого розвитку, верховенства права, прав і свобод людини і громадянина в Україні.		
Безпека інтернет-речей		
РН 9 – впроваджувати процеси, що	Пояснювально-ілюстративний	Опитування, захист лабораторних робіт,

базуються на національних та міжнародних стандартах, виявлення, ідентифікації, аналізу та реагування на інциденти інформаційної та/або кібербезпеки; РН 13 – аналізувати проекти інформаційно-телекомунікаційних систем базуючись на стандартизованих технологіях та протоколах передачі даних; РН 14 – вирішувати завдання захисту програм та інформації, що обробляється в інформаційно-телекомунікаційних системах програмно-апаратними засобами та давати оцінку результативності якості прийнятих рішень; РН 17 – забезпечувати процеси захисту та функціонування інформаційно-телекомунікаційних (автоматизованих) систем на основі практик, навичок та знань, щодо структурних (структурно-логічних) схем, топології мережі, сучасних архітектур та моделей захисту електронних інформаційних ресурсів з відображенням взаємозв'язків та інформаційних потоків, процесів для внутрішніх і віддалених компонент; РН 18 – використовувати програмні та програмно-апаратні комплекси захисту інформаційних ресурсів; РН 19 – застосовувати теорії та методи захисту для забезпечення безпеки інформації в інформаційно-телекомунікаційних системах; РН 20 – забезпечувати функціонування спеціального програмного забезпечення, щодо захисту інформації від руйнуючих програмних впливів, руйнуючих кодів в	(інформаційно-рецептивний) та репродуктивний	проведення контрольних робіт, проведення тестування, презентації докладів за темами лекційних занять, екзамен

інформаційно-телекомунікаційних системах; РН 21 – вирішувати задачі забезпечення та супроводу (в.т. числі: огляд, тестування, підзвітність) системи управління доступом згідно встановленої політики безпеки в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах; РН 22 – вирішувати задачі управління процедурами ідентифікації, автентифікації, авторизації процесів і користувачів в інформаційно-телекомунікаційних системах згідно встановленої політики інформаційної і\або кібербезпеки; РН 23 – реалізовувати заходи з протидії отриманню несанкціонованого доступу до інформаційних ресурсів і процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах; РН 24 – вирішувати задачі управління доступом до інформаційних ресурсів та процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах на основі моделей управління доступом (мандатних, дискреційних, рольових); РН 25 – забезпечувати введення підзвітності системи управління доступом до електронних інформаційних ресурсів і процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах з використанням журналів реєстрації подій, їх аналізу та встановлених процедур захисту; РН 26 – впроваджувати заходи та		

забезпечувати реалізацію процесів попередження отриманню несанкціонованого доступу і захисту інформаційних, інформаційно-телекомунікаційних (автоматизованих) систем на основі еталонної моделі взаємодії відкритих систем; РН 27 – вирішувати задачі захисту потоків даних в інформаційних, інформаційно-телекомунікаційних (автоматизованих) системах; РН 28 – аналізувати та проводити оцінку ефективності та рівня захищеності ресурсів різних класів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах в ході проведення випробувань згідно встановленої політики інформаційної та\або кібербезпеки; РН 29 – здійснювати оцінювання можливості реалізації потенційних загроз інформації, що обробляється в інформаційно-телекомунікаційних системах та ефективності використання комплексів засобів захисту в умовах реалізації загроз різних класів; РН 31 – застосовувати теорії та методи захисту для забезпечення безпеки елементів інформаційно-телекомунікаційних систем; РН 32 – вирішувати задачі управління процесами відновлення штатного функціонування інформаційно-телекомунікаційних систем з використанням процедур резервування згідно встановленої політики безпеки; РН 34 – приймати участь у розробці та впровадженні стратегії інформаційної безпеки та/або кібербезпеки відповідно		

до цілей і завдань організації; РН 35 – вирішувати задачі забезпечення та супроводу комплексних систем захисту інформації, а також протидії несанкціонованому доступу до інформаційних ресурсів і процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах згідно встановленої політики інформаційної і\або кібербезпеки; РН 36 – виявляти небезпечні сигнали технічних засобів; РН 37 – вимірювати параметри небезпечних та завадових сигналів під час інструментального контролю процесів захисту інформації та визначати ефективність захисту інформації від витоку технічними каналами відповідно до вимог нормативних документів системи технічного захисту інформації; РН 38 – інтерпретувати результати проведення спеціальних вимірювань з використанням технічних засобів, контролю характеристик інформаційно-телекомунікаційних систем відповідно до вимог нормативних документів системи технічного захисту інформації; РН 39 – проводити атестацію (спираючись на облік та обстеження) режимних територій (зон), приміщень тощо в умовах додержання режиму секретності із фіксуванням результатів у відповідних документах; РН 40 – інтерпретувати результати проведення спеціальних вимірювань з використанням технічних засобів, контролю характеристик ІТС відповідно до вимог нормативних документів системи технічного захисту інформації;		

РН 41 – забезпечувати неперервність процесу ведення журналів реєстрації подій та інцидентів на основі автоматизованих процедур; РН 42 – впроваджувати процеси виявлення, ідентифікації, аналізу та реагування на інциденти інформаційної і/або кібербезпеки; РН 43 – застосовувати національні та міжнародні регулюючі акти в сфері інформаційної безпеки та/ або кібербезпеки для розслідування інцидентів; РН 44 – вирішувати задачі забезпечення безперервності бізнес-процесів організації на основі теорії ризиків та встановленої системи управління інформаційною безпекою, згідно з вітчизняними та міжнародними вимогами та стандартами; РН 45 – застосовувати ріні класи політик інформаційної безпеки та/ або кібербезпеки, що базуються на ризик-орієнтованому контролі доступу до інформаційних активів; РН 46 – здійснювати аналіз та мінімізацію ризиків обробки інформації в інформаційно-телекомунікаційних системах; РН 47 – вирішувати задачі захисту інформації, що обробляється в інформаційно-телекомунікаційних системах з використанням сучасних методів та засобів криптографічного захисту інформації; РН 48 – виконувати впровадження та підтримку систем виявлення вторгнень та використовувати компоненти криптографічного захисту для		

забезпечення необхідного рівня захищеності інформації в інформаційно-телекомунікаційних системах; РН 49 – забезпечувати належне функціонування системи моніторингу інформаційних ресурсів і процесів в інформаційно-телекомунікаційних системах; РН 50 – забезпечувати функціонування програмних та програмно-апаратних комплексів виявлення вторгнень різних рівнів та класів (статистичних, сигнатурних, статистично-сигнатурних); РН 51 – підтримувати працездатність та забезпечувати конфігурування систем виявлення вторгнень в інформаційно-телекомунікаційних системах; РН 52 – використовувати інструментарій для моніторингу процесів в інформаційно-телекомунікаційних системах; РН 53 – вирішувати задачі аналізу програмного коду на наявність можливих загроз.		
Антивірусний захист інформації		
РН 7 – діяти на основі законодавчої та нормативно-правової бази України та вимог відповідних стандартів, у тому числі міжнародних в галузі інформаційної та /або кібербезпеки; РН 8 – готувати пропозиції до нормативних актів щодо забезпечення інформаційної та /або кібербезпеки; РН 9 – впроваджувати процеси, що базуються на національних та міжнародних стандартах, виявлення, ідентифікації, аналізу та реагування на інциденти інформаційної та/або кібербезпеки; РН 10 – виконувати аналіз та декомпозицію	Пояснювально-ілюстративний (інформаційно-рецептивний) та репродуктивний	Опитування, захист лабораторних робіт, проведення контрольних робіт, проведення тестування, презентації докладів за темами лекційних занять, залік

інформаційно-телекомунікаційних систем; РН 11 – виконувати аналіз зв'язків між інформаційними процесами на віддалених обчислювальних системах; РН 13 – аналізувати проекти інформаційно-телекомунікаційних систем базуючись на стандартизованих технологіях та протоколах передачі даних; РН 14 – вирішувати завдання захисту програм та інформації, що обробляється в інформаційно-телекомунікаційних системах програмно-апаратними засобами та давати оцінку результативності якості прийнятих рішень; РН 15 – використовувати сучасне програмно-апаратне забезпечення інформаційно-комунікаційних технологій; РН 16 – реалізовувати комплексні системи захисту інформації в автоматизованих системах (АС) організації (підприємства) відповідно до вимог нормативно-правових документів; РН 17 – забезпечувати процеси захисту та функціонування інформаційно-телекомунікаційних (автоматизованих) систем на основі практик, навичок та знань, щодо структурних (структурно-логічних) схем, топології мережі, сучасних архітектур та моделей захисту електронних інформаційних ресурсів з відображенням взаємозв'язків та інформаційних потоків, процесів для внутрішніх і віддалених компонент; РН 18 – використовувати програмні та програмно-апаратні комплекси захисту інформаційних ресурсів; РН 19 – застосовувати теорії та методи захисту для забезпечення безпеки інформації в інформаційно-		

телекомунікаційних системах; РН 20 – забезпечувати функціонування спеціального програмного забезпечення, щодо захисту інформації від руйнуючих програмних впливів, руйнуючих кодів в інформаційно-телекомунікаційних системах; РН 23 – реалізовувати заходи з протидії отриманню несанкціонованого доступу до інформаційних ресурсів і процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах; РН 25 – забезпечувати введення підзвітності системи управління доступом до електронних інформаційних ресурсів і процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах з використанням журналів реєстрації подій, їх аналізу та встановлених процедур захисту; РН 27 – вирішувати задачі захисту потоків даних в інформаційних, інформаційно-телекомунікаційних (автоматизованих) системах; РН 29 – здійснювати оцінювання можливості реалізації потенційних загроз інформації, що обробляється в інформаційно-телекомунікаційних системах та ефективності використання комплексів засобів захисту в умовах реалізації загроз різних класів; РН 31 – застосовувати теорії та методи захисту для забезпечення безпеки елементів інформаційно-телекомунікаційних систем; РН 32 – вирішувати задачі управління процесами відновлення штатного функціонування інформаційно-		

телекомунікаційних систем з використанням процедур резервування згідно встановленої політики безпеки; РН 33 – вирішувати задачі забезпечення безперервності бізнес процесів організації на основі теорії ризиків; РН 34 – приймати участь у розробці та впровадженні стратегії інформаційної безпеки та/або кібербезпеки відповідно до цілей і завдань організації; РН 35 – вирішувати задачі забезпечення та супроводу комплексних систем захисту інформації, а також протидії несанкціонованому доступу до інформаційних ресурсів і процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах згідно встановленої політики інформаційної і\або кібербезпеки; РН 37 – вимірювати параметри небезпечних та завадових сигналів під час інструментального контролю процесів захисту інформації та визначати ефективність захисту інформації від витоку технічними каналами відповідно до вимог нормативних документів системи технічного захисту інформації; РН 38 – інтерпретувати результати проведення спеціальних вимірювань з використанням технічних засобів, контролю характеристик інформаційно-телекомунікаційних систем відповідно до вимог нормативних документів системи технічного захисту інформації; РН 41 – забезпечувати неперервність процесу ведення журналів реєстрації подій та інцидентів на основі автоматизованих процедур; РН 42 – впроваджувати процеси виявлення,		

ідентифікації, аналізу та реагування на інциденти інформаційної і/або кібербезпеки; РН 43 – застосовувати національні та міжнародні регулюючі акти в сфері інформаційної безпеки та/ або кібербезпеки для розслідування інцидентів; РН 44 – вирішувати задачі забезпечення безперервності бізнес-процесів організації на основі теорії ризиків та встановленої системи управління інформаційною безпекою, згідно з вітчизняними та міжнародними вимогами та стандартами; РН 45 – застосовувати ріні класи політик інформаційної безпеки та/ або кібербезпеки, що базуються на ризик-орієнтованому контролі доступу до інформаційних активів; РН 46 – здійснювати аналіз та мінімізацію ризиків обробки інформації в інформаційно-телекомунікаційних системах; РН 47 – вирішувати задачі захисту інформації, що обробляється в інформаційно-телекомунікаційних системах з використанням сучасних методів та засобів криптографічного захисту інформації; РН 48 – виконувати впровадження та підтримку систем виявлення вторгнень та використовувати компоненти криптографічного захисту для забезпечення необхідного рівня захищеності інформації в інформаційно-телекомунікаційних системах; РН 49 – забезпечувати належне функціонування системи моніторингу інформаційних ресурсів і процесів в інформаційно-телекомунікаційних		

системах; РН 50 – забезпечувати функціонування програмних та програмно-апаратних комплексів виявлення вторгнень різних рівнів та класів (статистичних, сигнатурних, статистично-сигнатурних); РН 51 – підтримувати працездатність та забезпечувати конфігурування систем виявлення вторгнень в інформаційно-телекомунікаційних системах; РН 52 – використовувати інструментарій для моніторингу процесів в інформаційно-телекомунікаційних системах; РН 53 – вирішувати задачі аналізу програмного коду на наявність можливих загроз.		