НАЦІОНАЛЬНЕ АГЕНТСТВО ІЗ ЗАБЕЗПЕЧЕННЯ ЯКОСТІ ВИЩОЇ ОСВІТИ

ВІДОМОСТІ
про самооцінювання освітньої програми

Заклад вищої освіти	**Харківський національний економічний університет імені Семена Кузнеця**
Освітня програма	**23426 Кібербезпека**
Рівень вищої освіти	**Бакалавр**
Спеціальність	**125 Кібербезпека**

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

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

Використані скорочення:

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

Загальні відомості

1. Інформація про ЗВО (ВСП ЗВО)

Реєстраційний номер ЗВО у ЄДЕБО	**227**
Повна назва ЗВО	**Харківський національний економічний університет імені Семена Кузнеця**
Ідентифікаційний код ЗВО	**02071211**
ПІБ керівника ЗВО	**Пономаренко Володимир Степанович**
Посилання на офіційний веб-сайт ЗВО	**http://www.hneu.edu.ua**

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

https://registry.edbo.gov.ua/university/227

3. Загальна інформація про ОП, яка подається на акредитацію

ID освітньої програми в ЄДЕБО	**23426**
Назва ОП	**Кібербезпека**
Галузь знань	**12 Інформаційні технології**
Спеціальність	**125 Кібербезпека**
Спеціалізація (за наявності)	*відсутня*
Рівень вищої освіти	**Бакалавр**
Вид освітньої програми	**Освітньо-професійна**
Вступ на освітню програму здійснюється на основі ступеня (рівня)	**Повна загальна середня освіта, ОКР «молодший спеціаліст»**
Термін навчання на освітній програмі	**3 р. 10 міс.**
Форми здобуття освіти на ОП	**заочна, очна денна**
Структурний підрозділ (кафедра або інший підрозділ), відповідальний за реалізацію ОП	**Кафедра кібербезпеки та інформаційних технологій**
Інші навчальні структурні підрозділи (кафедра або інші підрозділи), залучені до реалізації ОП	***Навчальна лабораторія кафедри кібербезпеки та інформаційних технологій***
Місце (адреса) провадження освітньої діяльності за ОП	**м. Харків, проспект Науки, 9-А**
Освітня програма передбачає присвоєння професійної кваліфікації	*не передбачає*
Професійна кваліфікація, яка присвоюється за ОП (за наявності)	
Мова (мови) викладання	**Українська**
ID гаранта ОП у ЄДЕБО	**107556**
ПІБ гаранта ОП	**Євсеєв Сергій Петрович**

Посада гаранта ОП	**Завідувач кафедри**
Корпоративна електронна адреса гаранта ОП	**serhii.yevseiev@hneu.net**
Контактний телефон гаранта ОП	**+38(095)-360-66-13**
Додатковий телефон гаранта ОП	***+38(068)-398-66-03***

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

В Харкові незважаючи на наявність кількох потужних технічних університетів, попит на фахівців в галузі кібербезпеки суттєво перевищує можливості університетів готувати відповідні кадри. Аналіз даних формування контингенту університету вказує на те, що попит на спеціальність кібербезпеки з кожним роком зростає.
Освітньо-професійна програма (далі – ОПП “Кібербезпека”) розроблена відповідно до Стандарту вищої освіти за спеціальністю 125 “Кібербезпека” на кафедрі інформаційних систем, яка здійснює підготовку за спеціальностями 121, 122, 126. Крім того, кафедра з 2008 року щорічно проводить міжнародну науково-практичну конференцію “Проблеми і перспективи розвитку IT-індустрії”, в якої є секція “Захист інформації в інформаційно-комунікаційних системах”. За результатами конференцій з 2012 р. кафедра видає колективну монографію, в якій приймають участь провідні українські спеціалісти в галузі захисту та безпеки інформації. В 2014 р. викладачем Король О. Г. була захищена кандидатська дисертація за спеціальністю 05.13.21 – Системи захисту інформації, у 2018 р. доцентом Євсеєвим С. П. захищена докторська дисертація за спеціальністю 21.05.01 – Інформаційна безпека держави.
З 2014 – 2017 рр. студенти отримують диплом першого ступеня у Всеукраїнському конкурсі студентських наукових робіт з напряму з природничих, технічних і гуманітарних наук в галузі “Захист інформації”, “Інформаційна безпека”, “Кібербезпека”. На щорічної міжнародної науково-практичної конференції молодих вчених “Інформаційні технології в сучасному світі: дослідження молодих вчених”, яка проводиться з 2004 р. розглядаються питання, які пов’язані з забезпеченням безпеки інформаційних ресурсів, протидії кіберзагрозам, захисту інформації, які є основою дипломних проектів (дипломних робіт) випускників першого та другого рівня вищої освіти “бакалавр” та “магістр” відповідно.
Виходячи з освітніх потреб Харківського регіону, наявності відповідних ресурсів університет здатний гарантувати якісну підготовку висококваліфікованих фахівців за спеціальністю 125 “Кібербезпека”, що забезпечить ефективну роботу з удосконалення освіти у галузі безпеки інформаційних ресурсів, та дозволить задовольнити попит у кваліфікованих кадрах у бізнес-середовищі.
Відповідно до рішення ректорату (наказ ректора № 181 від 26.06.2018 р.), з 01.09.2018 р. створена кафедра кібербезпеки та інформаційних технологій та навчальна лабораторія кафедра кібербезпеки та інформаційних технологій (наказ ректора № 184 від 02.07.2018 р.).
ОПП впроваджена з 1 вересня 2018 року.
У підготовці проекту ОПП “Кібербезпека” брали участь доценти кафедри інформаційних систем: Євсеєв Сергій Петрович, Король Ольга Григорівна, Федорченко Володимир Миколайович, а також представники академічної спільноти та роботодавці: комерційний директор ТОВ “Сайфер БІС”, кандидат технічних наук Ковтун Владислав Юрійович; директор ТОВ “Талантаріум” Кулик Євгеній Юрійович.

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

Рік навчання	**Навчальний рік, у якому відбувся набір здобувачів відповідного року навчання**	**Обсяг набору на ОП у відповідному навчальному році**	**Контингент студентів на відповідному році навчання станом на 1 жовтня поточного навчального року**		**У тому числі іноземців**	
			ОД	З	ОД	З
1 курс	2019 - 2020	27	25	0	0	0
2 курс	2018 - 2019	16	12	0	0	0
3 курс	2017 - 2018	8	8	0	0	0
4 курс	2016 - 2017	2	2	0	0	0

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

6. Інформація про інші ОП ЗВО за відповідною спеціальністю

Рівень вищої	**Інформація про освітні програми**

освіти	
початковий рівень (короткий цикл)	*програми відсутні*
перший (бакалаврський) рівень	**23426 Кібербезпека**
другий (магістерський) рівень	**35202 Кібербезпека**
третій (освітньо-науковий/освітньо-творчий) рівень	*програми відсутні*

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

	Загальна площа	Навчальна площа
Усі приміщення ЗВО	75456	13250
Власні приміщення ЗВО (на праві власності, господарського відання або оперативного управління)	75320	13115
Приміщення, які використовуються на іншому праві, аніж право власності, господарського відання або оперативного управління (оренда, безоплатне користування тощо)	136	136
Приміщення, здані в оренду	334	0

Примітка. Для ЗВО із ВСП інформація зазначається:
- щодо ОП, яка реалізується у базовому ЗВО – без урахування приміщень ВСП;
- щодо ОП, яка реалізується у ВСП – лише щодо приміщень даного ВСП.

8. Документи щодо ОП

Документ	Назва файла	Хеш файла
Освітня програма	*ОПП 125 КБ бакалаври 2019-2020.pdf*	hXyVLFdDZc5J6FJG0eo2Q44w4aL3zEofHNEh9JUQWqI=
Навчальний план за ОП	*Нав план бакалавр Кібербезпека.pdf*	tS3yUu4d9VgmzjH+3ZpaJw4Jq5RZvkw3kyjzZMLuZTw=
Рецензії та відгуки роботодавців	*Автор_Рецензія.pdf*	xPGM2eu3JLOcs1+if7/WVANY3Q2hhmacBOp+aZHZFk4=
Рецензії та відгуки роботодавців	*Рецензія Distributed Lab.pdf*	NBLONU4+dh0yPA9jnpyamrwlQyzrLe9MGM/yhMbLpTI=
Рецензії та відгуки роботодавців	*РЕЦЕНЗІЯ-Сайфер.pdf*	49c4ykvUtGfgJj0DeJrVfLH3depXJJ7EHW0aCdw5FpI=

1. Проектування та цілі освітньої програми

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

Цілі ОПП “Кібербезпека” (http://bit.ly/37rYLQW) – забезпечити підготовку компетентних фахівців в галузі кібербезпеки та інформаційної безпеки, захисту інформації, здатних розробляти і використовувати технології інформаційної та кібербезпеки.
Особливостями ОПП “Кібербезпека” 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, яка дозволяє формувати компетентності на основі майстер-класів, які проводять представники компанії, реальних проектів, які пов’язані з децентралізованими системами та смарт-контрактами (http://bit.ly/2SPVIN7). На протязі навчання студенти можуть отримати сертифікати академії CISCO ХНЕУ ім. С. Кузнеця, які забезпечують формування компетентностей сучасних технологій комутації та маршрутизації комп’ютерних мереж та забезпечення безпеки. (http://bit.ly/2OUwV9A). Це дозволяє здобувачу вищої освіти бути найбільш конкурентоспроможним на ринку праці.

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

Місія ХНЕУ ім. С. Кузнеця: формування творчої, всебічно розвинутої особистості, справжнього професіонала для наукової та практичної роботи у сфері суспільно-економічної діяльності з метою підвищення рівня та якості життя людей і прогресивного розвитку суспільства. Стратегічна мета розвитку Університету – підвищення якості підготовки фахівців до рівня, що забезпечить їм можливість зайняти достойне місце в соціумі та успішно працювати за фахом у розбудові суспільства, яке базується на глобальній економіці знань.
1. Стратегічний план розвитку ХНЕУ на 2013 – 2020 р. (стор. 3-4, http://bit.ly/38rMcGL);
2. Концептуальні засади розвитку ХНЕУ ім. С. Кузнеця до 2020 року (стор. 4-8, http://bit.ly/2TiLyFd).
Концепція розвитку ХНЕУ будується на підвалинах концепції розвитку економічної освіти України, концептуальних положень і умов реалізації основних напрямів діяльності університету у функціональному розрізі та конкретних завдань за напрямами роботи.
Цілі ОПП “Кібербезпека” (підготовка фахівців, здатних розробляти і використовувати технології інформаційної безпеки) повністю відповідають місії та стратегії університету.

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

Здобувач вищої освіти Макаренко Антон, який є членом робочої групи, яка відповідальна за формування ОПП “Кібербезпека”, здобувачі вищої освіти мають можливість висловити свої пропозиції через сайт кафедри (http://bit.ly/2P0vXZy), а також під час кураторських годин (1 та 2 курс навчання). Студенти 2 курсу запропонували збільшити кількість навчальних дисциплін з циклу програмування. Антон Макаренко запропонував, збільшити практичну складову в дисциплінах. Після обговорення скореговані результати навчання та дисципліни були включені до навчального плану.

- роботодавці

Комерційний директор ТОВ “Сайфер БІС” Ковтун Владислав (член робочої групи ОПП “Кібербезпека”) запропонував включити в навчальний план за ОПП “Кібербезпека” курси з мови програмування Python, Java (з початкового рівня та закінчуючи просунутим рівнем). Після обговорення відповідні зміни включені до навчального плану, а саме в дисципліни “Технології програмування”, “Основи алгоритмізації”, “Програмування”, “Інформаційні системи та інтернет технології” (http://bit.ly/321xh3A).
Співзасновник компанії “Distributed Lab” Кравченко Павло, який є членом робочої групи, яка відповідальна за формування ОПП “Кібербезпека”, запропонував розгорнути лабораторію Блокчейн та включити відповідні дисципліни в вибіркову складову профільних дисциплін. Після обговорення сформований мейджор «Блокчейн-технологія та безпека банківських систем» (http://bit.ly/321xh3A) та сайт лабораторії Блокчейн (https://blockchain.hneu.edu.ua/).

- академічна спільнота

В роботі робочої групи активну участь приймали викладачі кафедри: професор Алексієв В.О., доцент Шматко О. В. Академічна спільнота запропонувала включити в ОПП “Кібербезпека” курси академії CISCO (http://bit.ly/2OUwV9A), які пов’язані з комп’ютерними мережами та безпекою в них, створення кіберполігону для практичного відпрацювання сучасних загроз та заходів щодо їх виявлення та припинення. Після обговорення було вирішено включити в відповідні дисципліни навчальний матеріал курсів CISCO та розпочати роботу щодо створення та розгортання кіберполігону. Таким чином більша частина пропозицій була врахована. Врахування пропозицій обумовлюється бажанням робочої групи підвищити рівень конкурентоспроможності здобувачів вищої освіти на ринку праці.

- інші стейкхолдери

Випускник магістерської програми за спеціальністю 122 “Комп’ютерні науки” Ігор Леонтієв, який працює в компанії VISEO (Chief Cloud Solution Architect, Expert DevOps et ALM) запропонував включити в навчальні дисципліни питання, які пов’язані з використанням SIEM-систем, формуванням безпеки на основі DevSecOps, безпеки контейнерів та безпеки K8S. Виключити з навчального плану вибіркову

дисципліну “Веб-програмування”. Після обговорення пропозицій на засіданні кафедри (протокол № 11 від 27.02.2019 р. (http://bit.ly/2HIdfBF) було прийнято рішення внести зміни в проект ОПП “Кібербезпека” на навчальний план на 2020-2021 н.р., в якому виключити дисципліну “Веб-програмування” та замінити її дисципліною “Безпека в DevOps”, замість дисципліни “Безпека інтернет-речей” включити дисципліну “Безпека вбудованих систем”, в якій розглянути питання застосування SIEM-систем.

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

Ринок праці України розвивається доволі стрімко, при цьому все більшу популярність набувають вакансій за категорією програміст-аналітик. Понад 47 % замовлень в IT-компаніях пов’язані з розробленням програмних застосунків, які забезпечують інформаційну безпеку та захист інформації. За результатами 2019 р. індустрія працівників IT зросла на 20% (http://bit.ly/2VeV7Ym), серед мов програмування найбільш затребуваними 2019 р. були PHP, Python і Java. ОПП “Кібербезпека” дає можливість набуття компетентностей, які дозволять здобувачам вищої освіти бути конкурентоспроможними на ринку праці. Робоча група регулярно проводить аналіз побажань замовників (роботодавців) перед початком розроблення (оновлення) програми на наступний рік.

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

Під час розроблення ОПП “Кібербезпека” враховувались рекомендації Харківського IT-кластеру, інформація стосовно останніх досліджень IT-кластеру знаходиться на їх сайті. Звіт про останні дослідження (http://bit.ly/32jqnqE).

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

Під час формування ОПП “Кібербезпека” проаналізовані освітні програми з підготовки здобувачів першого (бакалаврського) рівня вищої освіти за спеціальністю 125 “Кібербезпека” провідних технічних університетів м. Києва (Київський політехнічний інститут імені Ігоря Сікорського (http://bit.ly/39Cv7dh), Національний авіаційний університет (http://bit.ly/37pQfSx), м. Харкова (Харківський національний університет радіоелектроніки (http://bit.ly/2SJwakL), університетів м. Тернопіль (Тернопільський національний технічний університет імені Івана Пулюя (http://bit.ly/31RXC3O), м. Житомир (Державний університет «Житомирська політехніка» http://bit.ly/2USyuZi), м. Кропивницький (Центральноукраїнський національний технічний університет (http://bit.ly/39D7hOD), освітні програми з підготовки здобувачів зі спеціальності “Кібербезпека” у закладах США (http://bit.ly/2SJEiSb).
На основі аналізу були визначені основні фахові компетенції та результати навчання, 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 вищої освіти

Відповідно до результатів навчання (далі – РН) визначених стандартом вищої освіти за спеціальністю 125 “Кібербезпека” у навчальному плані визначені дисципліни: РН-1, 2, 3, 7 – дисципліни: Українська мова (за професійним спрямуванням), Іноземна мова (за професійним спрямуванням), Соціальна та економічна історія України, Філософія, Навчальна практика “Університетська освіта”; РН-9, 10 – дисципліни: Соціальна та економічна історія України, Філософія; РН- 11, 14, 18 – дисципліни: Математичні основи криптології, Вища математика, Теоретичні основи криптографії, Основи криптографічного захисту; РН-15, 19, 23, 25 – дисципліна: Інформаційна безпека держави; РН-12, 16, 19 – дисципліна: Основи побудови та функціонування мікропроцесорних систем; РН-14, 25, 28 – дисципліна: Основи математичного моделювання; РН-11, 16, 17 – дисципліни: Технології програмування, Основи криптографічного захисту, Основи технічного захисту інформації, Інформаційні системи та Інтернет технології, Основи побудови та захисту сучасних операційних систем; РН-18, 19, 20, 21 – дисципліни: Основи криптографічного захисту, Основи технічного захисту інформації, Безпека інтернет-речей, Безпека в інформаційно-комунікаційних системах; РН-17, 18 – дисципліни: Основи стеганографічного захисту інформації, Основи алгоритмізації, Програмування; РН-15, 23, 24 – дисципліна: Основи національної безпеки; РН-15, 27, 28 – дисципліна: Організаційне забезпечення захисту інформації; РН-16, 17, 18, 20 – дисципліна: Введення в мережі; РН-19, 20, 22, 24, 25 – дисципліна: Менеджмент інформаційної безпеки; РН-17, 20, 25 – дисципліна: Організація та інформаційне забезпечення управлінської діяльності; РН-4, 8, 13 – дисципліни: Тренінг курс “Безпека життєдіяльності”, Тренінг курс “Основи охорони праці”.

Якщо стандарт вищої освіти за відповідною спеціальністю та рівнем вищої освіти відсутній, поясніть, яким чином визначені ОП програмні результати навчання відповідають вимогам Національної рамки кваліфікацій для відповідного кваліфікаційного рівня?

Відповідно до наказу МОН України № 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)?

178

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

62

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

Навчальні дисципліни, 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, що використовуються для забезпечення функціонування цих об’єктів; процеси управління інформаційною і кібербезпекою об’єктів, що підлягають захисту.
Що відповідає теоретичному змісту предметної області, методам, методикам та технологіям формування компетентностей за ОПП “Кібербезпека”. Зміст ОПП “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 забезпечення його підвищення. Перелік фахових компетентностей ОПП “Кібербезпека” дозволяє сформувати комплекс знань, навичок та вмінь, які створюють високий рівень конкурентоспроможності на ринку праці. Дисципліни навчального плану ОПП “Кібербезпека” потребують спеціалізованого програмного та апаратного забезпечення. Дисципліни ОПП “Кібербезпека” в повній мірі забезпечені ліцензованим та open source програмним забезпеченням, що дозволяє досягти поставленої мети та завдань (http://bit.ly/2HIdfBF).
Навчальні дисципліни, які забезпечують формування відповідних компетентностей у здобувачів, відрізняються від ОП за суміжними спеціальностями (121 “Інженерія програмного забезпечення”, 122 “Комп’ютерні науки”, 126 “Інформаційні системи та технології”) навчанню використання сучасних механізмів, програмних застосунків, програмно-апаратних засобів щодо формування системи безпеки контуру бізнес-процесів. Дана ОПП “Кібербезпека” спрямована на підготовку фахівців за компетентностями з інформаційної та кібербезпеки, програмістів-аналітиків.

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

Відповідно до навчального плану здобувач вищої освіти має можливість формування індивідуальної освітньої траєкторії на основі вибору вибіркових дисциплін із загального університетського пулу (майнори, вільні майнори), а також вибору вибіркових дисциплін за спеціальністю (мейджори), дисципліни правового спрямування та мовної підготовки, що складає 30 та 32 кредити відповідно. Здобувачі вищої освіти у 2018 р. вибрали з Переліку загальноуніверситетських навчальних дисциплін, що забезпечують вибіркову складову (майнори) освітньо-професійних програм підготовки бакалаврів (12 майнорів) (http://bit.ly/2UTsfV1), Переліку загальноуніверситетських навчальних дисциплін, що забезпечують вибіркову складову (вільні майнори) освітньо-професійних програм підготовки бакалаврів (11 вільних майнорів) (Наказ ректора від 12.03.2018 р. № 102 “Про затвердження переліку вибіркових навчальних дисциплін на 2018-2019 н. р.”) майнор, який складає з блоку чотирьох взаємопов'язаних непрофільних навчальних дисциплін (http://bit.ly/3bzJEYR). Вибір мейджорів здійснюється на основі формування індивідуальної освітньої траєкторії здобувача вищої освіти (перелік відповідних дисциплін мейджора, знаходиться у навчальному плані (http://bit.ly/321xh3A). Копії заяв здобувачів вищої освіти за спеціальністю “Кібербезпека” знаходяться за посиланням (http://bit.ly/2HIdfBF).

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

Відповідно до “Методичних підходів до формування варіативної складової освітніх програм в Харківському національному економічному університеті імені Семена Кузнеця” (Наказ ректора від 31.12.2016 р. №251) (ст. 7-11, http://bit.ly/2OWkb28), здобувачі на 1 курсі проводять вибір вибіркової складової освітньої програми – майнор, який складається з чотирьох взаємопов'язаних непрофільних навчальних дисциплін підготовки освітнього ступеня бакалавр, або чотирьох вільних майнорів, які вивчаються на 2, 3 курсі навчання. На 2 курсі навчання здобувачі обирають мейджор – профільні навчальні дисципліни підготовки освітнього ступеня бакалавр, які поглиблюють професійну підготовку за спеціальністю, який може складати від 30 до 100 кредитів ECTS.
Дисципліна “Іноземна мова академічної та професійної комунікації”, дисципліна правового спрямування обирається на 1 курсі навчання. Вибір студентом вільних майнорів (майнор) загальноуніверситетського пулу формує право індивідуальної освітньої траєкторії, яка складає не менш як 25% загальної кількості кредитів ЄКТС. Це дозволяє поглибити знання здобувачів в інших зацікавлених галузях, підвищити рівень знання іноземної мови (навчальні дисципліни, які входять до складу майнору (вільні майнори) викладаються мовами Євросоюзу (англійською, французькою, німецькою). Студент має право вивчати або майнор (чотири пов’язані дисципліни між собою) або обирає чотири вільних майнори. Перед початком проведення вибору вибіркових дисциплін, відповідними деканатами організується проведення презентацій майнорів викладачами відповідних кафедр.
При виборі спеціальних дисциплін спрямованих на формування навичок та набуття відповідних компетентностей здобувач вищої освіти має можливість вибрати мейджор – профільні навчальні дисципліни освітньо-професійної програми, які поглиблюють професійну підготовку за певною спеціальністю. Вибір вибіркових дисциплін студентами здійснюється за допомогою сайту (http://www.elect.hneu.edu.ua/site). Копії заяв та індивідуальних планів здобувачів вищої освіти за спеціальністю “Кібербезпека” знаходяться за посиланням (http://bit.ly/2HIdfBF).

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

Навчальний план передбачає:
“Тренінг-курс “Безпека життєдіяльності”, “Тренінг-курс “Основи охорони праці”, “Виробнича практика”, “Комплексний тренінг”, “Переддипломна практика“, які забезпечують наступні компетентності: КЗ 1. Здатність застосовувати знання у практичних ситуаціях, КЗ 4. Здатність здійснювати професійну діяльність згідно з вимогами санітарно-гігієнічного режиму, охорони праці, техніки безпеки та протипожежної безпеки, КЗ 8. Прагнення до збереження навколишнього середовища, КЗ 13. Дотримання та пропагування здорового способу життя, КФ 4. Здатність здійснювати протидію несанкціонованому проникненню в ІТ системи і мережі, КФ 7. Здатність виконувати спеціальні дослідження технічних і програмно-апаратних засобів захисту обробки інформації в ІТС, КФ 8. Здатність проводити техніко-економічного аналіз й обґрунтовувати проектні рішення з забезпечення кібербезпеки, КФ 14. Здатність проводити дослідження у практичній професійній діяльності.
Тренінги проводяться в комп’ютерних класах з використанням відповідних засобів, що задовольняє потреби студентів та забезпечує формування необхідних компетентностей для подальшої професійної діяльності.
Відповідно до ОПП та навчального плану підготовки здобувачів вищої освіти загальна кількість годин, яка відводиться на практичну підготовку складає 11 тижнів протягом всього навчання, що дає можливість здобути практичні навички та відповідні компетентності (http://bit.ly/38uXrOv).

Продемонструйте, що ОП дозволяє забезпечити набуття здобувачами вищої освіти соціальних навичок (soft skills) упродовж періоду навчання, які відповідають цілям та результатам навчання ОП результатам навчання ОП

Для забезпечення набуття здобувачами вищої освіти, соціальних навичок запропоновані наступні дисципліни:
“Українська мова (за професійним спрямуванням)”, “Інтелектуальна власність”, “Соціальна та економічна історія України”, “Інформаційна безпека держави”, “Основи національної безпеки”, “Іноземна мова (за професійним спрямуванням)”, майнори, які забезпечують наступні компетентності щодо формування соціальних навичок: КЗ 3. Здатність спілкуватися рідною та другою іноземною мовою як усно, так і письмово, КЗ 7. Навички міжособистісної взаємодії, КЗ 9. Здатність діяти соціально відповідально та громадянсько свідомо, КЗ 14. Здатність бути критичним та самокритичним, КФ 1. Здатність використовувати законодавчу та нормативно-правову бази, а також вимоги відповідних, в тому числі і міжнародних, стандартів та практик щодо здійснення професійної діяльності. Що дозволяє забезпечити у студентів навички комунікації, лідерства, відповідальності, цілеспрямованості та вміння діяти в критичній ситуації.

Яким чином зміст ОП ураховує вимоги відповідного професійного стандарту?

Професійний стандарт за спеціальністю відсутній.

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

Відповідно до ст. 62 Закону України «Про вищу освіту» (http://bit.ly/3bJVoIs) обсяг вибіркових навчальних дисциплін має бути не менш як 25 % від загального обсягу програми підготовки. Базова складова навчальних планів включає обов'язкові базові навчальні дисципліни, практичну підготовку, підсумкову атестацію загальним обсягом 50-75 % від обсягу відповідної освітньої програми. Варіативна складова навчальних планів складає відповідно 25-50 % від обсягу відповідної освітньої програми та містити непрофільні навчальні дисципліни, які формують загально-професійні компетентності та профільні навчальні дисципліни. В освітніх програмах передбачаються вільний вибір здобувачами навчальних дисциплін за певними спрямуваннями. Перелік навчальних дисциплін щорічно затверджується Вченою радою університету та оприлюднюється на сайті університету (http://bit.ly/2HK9WKa). В ОПП представлено 2 мейджора (32 кредити ECTS), які поглиблюють професійну підготовку за спеціальністю.
ОПП включає блоки з загальним обсягом кредитів ECTS:
1. Цикл загальної підготовки – 34 кредити, 44.5 % (аудиторні) та 55.5 % (самостійна).
2. Цикл професійної підготовки – 206 кредитів, 40 % (аудиторні) та 60 % (самостійна).
В цілому за навчальний план аудиторне навантаження здобувачів вищої освіти складає 40.6 %, самостійна робота – 59.4 %.

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

Підготовка здобувачів вищої освіти за дуальною формою освіти не здійснюється. Відповідно до п. 1.5. "Положення про порядок організації та проведення підготовки фахівців за дуальною формою здобуття вищої освіти у ХНЕУ ім. С. Кузнеця" (http://bit.ly/3bG8V3D) "Дуальна форма здобуття вищої освіти – це спосіб здобуття вищої освіти, що передбачає поєднання навчання осіб у закладах вищої освіти з навчанням на робочих місцях на підприємствах, в установах та організаціях для набуття певної кваліфікації, як правило, на основі договору". Умови проведення конкурсного відбору здобувачів вищої освіти за дуальною формою навчання, порядок оформлення документів, та порядок укладання договору визначені в Положенні пункти 3, 4, 5 відповідно.

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-сторінка на сайті університету: http://bit.ly/37ASSAQ
Веб-сторінка на сайті факультету: http://bit.ly/38zThoF
Веб-сторінка на сайті кафедри: http://bit.ly/321ewgr

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

До вступу на спеціальність 125 "Кібербезпека" приймаються здобувачі, які успішно склали іспити ЗНО за наступними конкурсними предметами: Укр. мова та література, Математика, Іноземна мова або фізика з ваговими коефіцієнтами 0,3; 0,4; 0,2 (бюджет), ваговими коефіцієнтами 0,3; 0,3; 0,3 (контракт) за наступними конкурсними дисциплінами Укр.мова та література, Історія України, Іноземна мова або географія. Конкурсний бал розраховується за формулою: КБ= К1*П1+ К2*П2+ К3*П3+ К4*А, де П1, П2, П3 – оцінки ЗНО або вступних іспитів з першого, другого та третього предметів (не менш 100 балів); А – середній бал документа про повну загальну середню освіту вагові коефіцієнти К1, К2, К3 та К4 встановлені ХНЕУ ім. С. Кузнеця. КОНКУРСНИЙ БАЛ на основі молодшого спеціаліста 125 "Кібербезпека" розраховується за формулою: КБ= П + А, де П – оцінка фахового вступного випробування (за шкалою від 100 до 200 балів), А – середній бал додатка до диплома молодшого спеціаліста (за шкалою від 0 до 20 балів). До проведення фахового вступного випробування для абітурієнтів, які вступають на скорочений термін навчання за освітньо-кваліфікаційним рівнем бакалавра на базі молодшого спеціаліста за спеціальністю 125 "Кібербезпека" залучається гарант програми(голова атестаційної комісії). Кожний білет складається із чотирьох завдань, їх бездоганне виконання оцінюється 200 балами (максимальна оцінка) за шкалою, (математика – 100 балів, кібербезпека – 100 балів). Програма фахового вступного випробування освітній ступінь «БАКАЛАВР» (http://bit.ly/2wQ2Dyu).

Яким документом ЗВО регулюється питання визнання результатів навчання, отриманих в інших ЗВО? Яким чином забезпечується його доступність для учасників освітнього процесу?

Відповідно до "Положення про порядок реалізації права на академічну мобільність учасників

освітнього процесу в Харківському національному економічному університеті імені Семена Кузнеця” (Наказ ректора № 150/1 від 07.09.2016 р.) (http://bit.ly/2vGlThc), що регламентує мету, підстави, порядок і умови здійснення академічної мобільності учасниками освітнього процесу Харківського національного економічного університету імені Семена Кузнеця, джерела фінансування міжнародної академічної мобільності, правила визначення трудомісткості навчальної роботи студентів у кредитах і порядок зарахування результатів, отриманих студентами в процесі навчання в межах академічної мобільності студентів.
Відповідно до пунктів Положення: 4.9., 4.10., 4.11., 4.12., 4.13. Такий підхід гарантує надійність визнання результатів навчання за дисциплінами, які вивчалися у закладі-партнері.

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

Здобувачі вищої освіти за ОПП “Кібербезпека” не мали академічної мобільності.

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

Регулюється відповідно до “Положення про порядок визнання результатів неформальної та інформальної освіти у ХНЕУ ім. С. Кузнеця” (http://bit.ly/2HElTRQ), наказів ректора № 158 від 02.09.2019 р. (http://bit.ly/38DtImL), № 115 від 28.05.2019 р. (http://bit.ly/37zHWn7), № 34 від 15.01.2019 р. (http://bit.ly/38POpM0) здобувач вищої освіти має право пройти відповідний курс, який відповідає навчальній дисципліні індивідуального плану навчання за ОПП “Кібербезпека” та отримавши сертифікат (з кількістю балів за результати навчання) отримати ці бали за відповідну навчальну дисципліну. Доступність до переліку курсів академії CISCO ХНЕУ ім. С. Кузнеця розміщена на сайті університету (http://bit.ly/3bYnEqW), кафедри (http://bit.ly/2vXr2Sc). Рішенням кафедри затверджені курси неформальної освіти CS50, курси академії CISCO (протокол № 2 від 13.09.2019 р., протокол № 7 від 24.12.2019 р.). Студенти можуть запропонувати свої курси неформальної освіти. Після затвердження на засіданні кафедри здобувачу вищої освіти повідомляють, що він (вони) можуть здобувати неформальну освіту за відповідною дисципліною.

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

Здобувачі вищої освіти за ОПП “Кібербезпека” отримали:
1 курс – сертифікат CS50 – 26 студентів, сертифікат CISCO “Cybersecurity Essentials” – 16 студентів;
2 курс сертифікат CISCO “Introduction to Packet Tracer” – 8 студентів, сертифікат CISCO “Cybersecurity Essentials” – 13 студентів; сертифікат CISCO “ Introduction to Cybersecurity” – 1 студент;
2 курс (за скороченим терміном навчання) сертифікат CISCO “Introduction to Packet Tracer”, “Cybersecurity Essentials”, “Introduction to Cybersecurity” – 1 студент.

4. Навчання і викладання за освітньою програмою

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

Основними методами навчання на ОПП “Кібербезпека” є лекційні, лабораторні заняття, основними формами навчання: індивідуальне заняття, тренінг, інтерактивне дистанційне навчання, самостійна робота студента.
Відповідні документи:
1. “Тимчасове положення про організацію освітнього процесу в ХНЕУ ім. С. Кузнеця” п. 3.3 (http://bit.ly/2vGT1FA)
2. Тимчасове положення “Про порядок оцінювання результатів навчання студентів за накопичувальною бально-рейтинговою системою” п. 1.4 (http://bit.ly/2Huqrdh).
3. Положення про облік та моніторинг результатів навчання студентів з використанням програмного забезпечення корпоративної інформаційної системи управління ХНЕУ ім. С. Кузнеця п. 3 (http://bit.ly/2ullDUF)
Вказані методи та форми навчання сприяють досягненню програмних результатів навчання за рахунок поєднання теоретичних та практичних занять.

Продемонструйте, яким чином форми і методи навчання і викладання відповідають вимогам студентоцентрованого підходу? Яким є рівень задоволеності здобувачів вищої освіти методами навчання і викладання відповідно до результатів опитувань?

Студентоцентрований підхід (http://bit.ly/2SUsU6f): передбачає розроблення освітніх / навчальних програм, які зосереджуються на результатах навчання, ураховують особливості пріоритетів особи, що навчається, ґрунтуються на реалістичності запланованого навчального навантаження, яке

узгоджується із тривалістю освітньої / навчальної програми. Форми і методи навчання за відповідною дисципліною доводиться на першому лекційному занятті, вказується у робочому плані (технологічна карта) та розміщується на сайті персональних навчальних систем ХНЕУ ім. С. Кузнеця (https://pns.hneu.edu.ua/). Форми і методи обираються викладачами відповідно до змісту освітніх компонентів, це забезпечує вибір кращої практики викладання, максимальної сформованості компетентностей та досягнення програмних (професійних, загальних) результатів навчання. За результатами опитування здобувачів вищої освіти 2 та 3 курсу першого (бакалаврського) рівня вищої освіти за ОПП "Кібербезпека" отримані наступні результати: задоволеність освітньою програмою - 73 % (середнє значення) (http://bit.ly/2HIdfBF).

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

Кожен викладач вільний обирати ті форми та методи навчання, які вважає доцільними для забезпечення формування компетентностей здобувача освіти, відповідно до дисциплін, загальної мети та задач ОПП (п. 4.2 "Тимчасове положення про організацію освітнього процесу в ХНЕУ ім. С. Кузнеця" (http://bit.ly/2vGT1FA). При цьому основною задачею викладача є підбір таких форм та методів навчання, які дозволяють максимально ефективно сформувати компетентності здобувача освіти. Таким чином завдання викладача повністю відповідає інтересам здобувача вищої освіти.

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

1. Тимчасове положення "Про порядок оцінювання результатів навчання студентів за накопичувальною бально-рейтинговою системою" (Наказом ректора ХНЕУ № 1 від 30.08.2013 р.) (р. 3-8, 14, http://bit.ly/2Huqrdh);
2. Положення "Про центр персональних навчальних систем ХНЕУ" (п. 3, п.4) (http://bit.ly/322q4An).
3. Тимчасове положення про освітні програми (http://bit.ly/2SUsU6f)

Учасники освітнього процесу мають вільний доступ до сайту кафедри, де розміщені РПНД за дисциплінами навчального плану (http://bit.ly/2SVt0KG), на сайті персональних навчальних систем ХНЕУ ім. С. Кузнеця (https://pns.hneu.edu.ua/) на яких перед початком навчання лектори навчальних дисциплін зобов'язані розмістити РПНД, робочий план (технологічна карта), в яких вказується інформація щодо цілей, змісту, критеріїв оцінювання, компетентностей та очікуваних результатів навчання за дисципліною. Здобувач вищої освіти має право ознайомитись з поточними оцінками за дисциплінами семестру в електронному кабінеті студента (http://bit.ly/2V4Yhxo). Студент має право отримувати інформацію: про умови вивчення навчальної дисципліни; види навчальних завдань і контролю; критерії та процедури оцінювання знань з навчальної дисципліни; результати кожного контрольного заходу; поточного (модульного) контролю; програму підсумкового випробування; підсумкові результати поточного контролю за семестр і навчальний рік на інформаційних дошках, сайті факультету у розділі Новини.

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

Поєднання навчання і досліджень відбувається шляхом активної участі студентів у науково-дослідній роботі кафедри.

Регулюється Тимчасовим положенням про організацію освітнього процесу в ХНЕУ ім. С. Кузнеця (http://bit.ly/2vGT1FA). Відповідно до наукової діяльності кафедри здобувачі вищої освіти приймають участь у Міжнародній науково-практичній конференції "Інформаційна безпека та інформаційні технології", яка проводиться за підтримкою кафедри (http://bit.ly/2SOBEL2).

Відповідно до наукової діяльності кафедри в 2019 році відкрита ініціативна науково-дослідна робота за темою "Методологія моделювання процесів поведінки антагоністичних агентів в системах безпеки", державний реєстраційний номер 0119U103117, керівники Євсеєв С. П., Мілов О. В.

Викладачі кафедри впроваджують в навчальний процес результати наукових досліджень, а саме: в дисципліні "Безпека банківських систем" розглядаються результати досліджень крипто-кодових конструкцій Мак-Еліса та Нідеррайтера, в дисципліні "Основи криптографічного захисту" розглядаються результати досліджень побудови каскадних геш-функцій на основі алгоритму UMAC.

На кафедрі сформовано лабораторію блокчейн (http://bit.ly/320IEJ3), яка дозволяє здобувачам отримати додаткові навчальні матеріали, відпрацьовувати питання забезпечення безпеки в програмних застосунках з використанням технології блокчейн, на основі мови Python.

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

Викладачі кафедри приймають активну участь у міжнародних конференціях. Завідувач кафедри у 2019 році був спікером трьох міжнародних конгресів, які пов'язані з IT-технологіями, а саме: 3th International Symposium on Multidisciplinary Studies and Innovative Technologies 2019, Туреччина (http://bit.ly/2SPJCng); IDSES 2019 (http://www.idses.org/) Туреччина; I International scientific-practical conference - modern information, measurement and control systems: problems and perspectives 2019 (MIMCS:PP 2019). (http://bit.ly/2uUoofT) (Азербайджан).

За останні 2 роки статей у НМБ Scopus – 9, у фахових виданнях - 18. На даний час на кафедрі виконується ініціативна науково-дослідна робота за темою “Методологія моделювання процесів поведінки антагоністичних агентів в системах безпеки”, державний реєстраційний номер 0119U103117, керівники Євсеєв С. П., Мілов О. В.
Викладачі кафедри підвищують свій рівень професійної підготовки шляхом отримання сертифікатів академії CISCO. Це дозволяє використовувати ресурси відповідних навчальних курсів CISCO при викладанні навчальних дисциплін освітньої програми, а саме: “Інформаційна безпека держави” – “Введення в кібербезпеку”, “Основи національної безпеки” - “Основи кібербезпеки”, “Основи побудови та функціонування мікропроцесорних систем” – “Основи IT”, “Інформаційні системи та Інтернет-технології” – “Introduction to Packet Tracer”, CCNA Введення в мережні технології – маршрутизація і комутація, CCNA Принципи маршрутизації і комутації, CCNA Маршрутизація і комутація. масштабування мереж, CCNA Маршрутизація і комутація. підключення мереж, “Безпека в інформаційно-комунікаційних системах” – “ CCNA Security”, “Технічне забезпечення інформаційної безпеки” – “CyberOps v1.1”. В навчальних дисциплінах, які пов’язані з блокчейн-технологією використовується матеріал навчальних курсів платформи Coursera, а саме: “Blockchain: основи та приклади застосування” – “Основи блокчейн”, “Основи смарт-контрактів” – “Смарт контракти”, “Основи розробки децентралізованих застосувань (decentralized applications (DAPPS))” – “Децентралізовані застосунки”.

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

Відповідно до угоди про співпрацю № 18-10/15 від 07.10.2015 р. в університеті розгорнутий віртуальний центр сертифікації ключів, який дозволяє в повному обсязі відпрацьовувати теоретичні знання за технології PKI.
Відповідно до наказу МОН України № 1213 від 06.11.2018 р. “Про надання доступу закладам вищої освіти і науковим установам, що знаходяться у сфері управління Міністерства освіти і науки України, до електронних наукових баз даних” в університеті здобувачі вищої освіти мають право доступу до електронних наукових баз даних SCOPUS, Web of Science.
На даний час формується заявка на участь у програмі Erasmus+ (Туречинна) “Cyber-T 4.0: Cybersecurity, Data Protection and Blockchain Technologies in Tourism 4.0”. Підписана угода про співробітництво з Університетом у Бєльсько-Бялій (Польща) (http://bit.ly/2HIdfBF), що дозволить здобувачам вищої освіти отримати два дипломи за другим (магістерським) рівнем.

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?

Система оцінювання сформованих компетентностей у студентів враховує види занять, які згідно з програмою навчальної дисципліни передбачають лекційні, лабораторні, семінарські, практичні заняття, а також виконання самостійної роботи. Оцінювання сформованих компетентностей у студентів здійснюється за накопичувальною 100-бальною системою. Відповідно до Тимчасового положення “Про порядок оцінювання результатів навчання студентів за накопичувальною бально-рейтинговою системою” ХНЕУ ім. С. Кузнеця (п. 3, http://bit.ly/2Huqrdh) контрольні заходи включають: поточний контроль, що здійснюється протягом семестру під час проведення лекційних, практичних, семінарських, лабораторних занять і оцінюється сумою набраних балів (максимальна сума – 60 балів; мінімальна сума, що дозволяє студенту складати іспит, – 35 балів).
Модульний контроль, що проводиться у формі колоквіуму як проміжний міні-екзамен з ініціативи викладача з урахуванням поточного контролю за відповідний змістовий модуль і має на меті інтегровану оцінку результатів навчання студента після вивчення матеріалу з логічно завершеної частини дисципліни – змістового модуля;
підсумковий/семестровий контроль, що проводиться у формі заліку або екзамену, відповідно до графіку навчального процесу.
Студента слід вважати атестованим, якщо сума балів, одержаних за результатами підсумкової/семестрової перевірки успішності, дорівнює або перевищує 60. Мінімально можлива кількість балів за поточний і модульний контроль упродовж семестру – 35 та мінімально можлива кількість балів, набраних на екзамені, – 25. Підсумкова оцінка з навчальної дисципліни розраховується з урахуванням балів, отриманих під час екзамену, та балів, отриманих під час поточного контролю за накопичувальною системою. Сумарний результат у балах за семестр складає: “60 і більше балів – зараховано”, “59 і менше балів – не зараховано” та заноситься у залікову ”Відомість обліку успішності” навчальної дисципліни. Екзамен може проводитись з застосуванням комп’ютерів, що визначено у “Положення про проведення письмових екзаменів у ХНЕУ ім. С. Кузнеця” (http://bit.ly/38Qsjcx), “Положення про проведення іспитів із застосуванням комп’ютерів” на факультеті економічної інформатики (яке визначає порядок проведення та перевірки результатів навчання) (http://bit.ly/3bYv6SW).

Яким чином забезпечуються чіткість та зрозумілість форм контрольних заходів та критеріїв

оцінювання навчальних досягнень здобувачів вищої освіти?

Відповідно до Тимчасового положення “Про порядок оцінювання результатів навчання студентів за накопичувальною бально-рейтинговою системою” ХНЕУ ім. С. Кузнеця (п. 3-8, http://bit.ly/2Huqrdh), “Положення про проведення письмових екзаменів у ХНЕУ ім. С. Кузнеця” (http://bit.ly/38Qsjcx), в РПНД використовуються наступні контрольні заходи: поточний контроль, що здійснюється протягом семестру під час проведення лекційних, практичних, семінарських, лабораторних занять і оцінюється сумою набраних балів (максимальна сума – 60 балів; мінімальна сума, що дозволяє студенту складати іспит, – 35 балів). Інформація щодо РПНД за освітньою програмою наведена на веб-сторінці сайту університету (http://bit.ly/2uIE1at), та сайту кафедри (http://bit.ly/3bJQECz), а також РПНД, робочий план (технологічна карта) розміщуються на відповідній закладці сайту персональних навчальних систем (https://pns.hneu.edu.ua/), на сайті кафедри (http://bit.ly/38zObZx). Інформація про поточний стан успішності здобувачі вищої освіти мають можливість перевірити на сайті університету у особистому кабінеті (http://bit.ly/2V4Yhxo).

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

Відповідно до Тимчасового положення “Про порядок оцінювання результатів навчання студентів за накопичувальною бально-рейтинговою системою” ХНЕУ ім. С. Кузнеця (п. 3-8, http://bit.ly/2Huqrdh) перед початком навчання РПНД, робочий план (технологічна карта) розміщується на відповідній закладці сайту персональних навчальних систем (https://pns.hneu.edu.ua/) , а також формується електронний журнал дисципліни, в якому вказується контрольні заходи та відповідні бали. Здобувачі вищої освіти мають право переглянути отримані бали за кожною дисципліною на протязі семестру (http://bit.ly/2SzqhYp). Також РПНД розміщуються на сайті персональних навчальних систем (https://pns.hneu.edu.ua/), на сайті кафедри (http://bit.ly/38zObZx). Інформація про форми контрольних заходів розміщується сайті університету у графіку навчального процесу (http://bit.ly/2Ve06bq). Крім того, на передекзаменаційній консультації лектор доводить зміст екзаменаційного білету та критерії оцінювання кожного питання у білеті з детальним описом нарахування кожного балу, що забезпечує доведення до здобувачів вищої освіти інформацію про форми контрольних заходів та критерії оцінювання.

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

Відповідно до Стандарту вищої освіти за спеціальністю 125 “Кібербезпека” для першого (бакалаврського) рівня вищої освіти (Наказ МОН України № 1074 від 04.10.2018 р.) (п. 6, http://bit.ly/323F8NP) “Атестація здійснюється у формі публічного захисту кваліфікаційного проекту/роботи та за рішенням закладу вищої освіти кваліфікаційного екзамену”.
Відповідно до рішення Вченої ради університету (протокол № 10 від 15.07.2019 р.) атестація здобувачів вищої освіти зі спеціальності 125 “Кібербезпека” здійснюється шляхом виконання кваліфікаційного проекту (роботи) (денна форма навчання), кваліфікаційний екзамен (заочна форма навчання).

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

В “Положення про проведення письмових екзаменів у ХНЕУ ім. С. Кузнеця” (http://bit.ly/38Qsjcx), Тимчасовому положенні “Про порядок оцінювання результатів навчання студентів за накопичувальною бально-рейтинговою системою” ХНЕУ ім. С. Кузнеця (http://bit.ly/2Huqrdh) визначені процедури проведення контрольних заходів. Крім цього в “Положенні про проведення іспитів із застосуванням комп’ютерів” (п. 3, http://bit.ly/2STdJdh) визначена процедура проведення контрольних заходів з використанням комп’ютерної техніки. Здобувачі мають право ознайомитись з процедурою проведення контрольних заходів на сайті факультету (http://bit.ly/3d68hgK).

Яким чином ці процедури забезпечують об’єктивність екзаменаторів? Якими є процедури запобігання та врегулювання конфлікту інтересів? Наведіть приклади застосування відповідних процедур на ОП

Відповідно до “Положення про проведення письмових екзаменів у ХНЕУ ім. С. Кузнеця” (п. 2, http://bit.ly/38Qsjcx), Тимчасового положення "Про порядок оцінювання результатів навчання студентів за накопичувальною бально-рейтинговою системою" ХНЕУ ім. С. Кузнеця (пп. 2.12-2.13, http://bit.ly/2Huqrdh), Положення “Про проведення іспитів із застосуванням комп’ютерів” (п. 3, http://bit.ly/2STdJdh) екзамени проводяться тільки письмово, під наглядом спостерігачів.
Після проведення іспиту відповідно до “Положення про проведення письмових екзаменів у ХНЕУ ім. С. Кузнеця” (п. 3, http://bit.ly/38Qsjcx) організується шифрування та перевірка робіт.
У разі проведення он-лайн тестування співробітник деканату з файлу з результатом виконання тесту переносить результат тесту в екзаменаційну форму (форма № Н-1.08 частина 2).
“Положення про політику та процедури врегулювання конфліктних ситуацій у ХНЕУ ім. С. Кузнеця” визначає в пп. III , IV процедури запобігання, виявлення та вирішення конфліктних ситуацій в університеті (http://bit.ly/2V8lxLj). “ Положення про апеляцію результатів підсумкового контролю у

формі іспиту ” визначає порядок розгляду апеляції у разі незгоди з результатами оцінювання іспиту (http://bit.ly/2P1SKE3).

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

Відповідно до Тимчасового положення "Про порядок оцінювання результатів навчання студентів за накопичувальною бально-рейтинговою системою" ХНЕУ ім. С. Кузнеця (п. 8, http://bit.ly/2Huqrdh), Положення “Про порядок формування рейтингу успішності студентів ХНЕУ ім. С. Кузнеця для призначення академічних стипендій” (стор. 8, пп. 13, http://bit.ly/2u4LUXb), “Положення про проведення письмових екзаменів у ХНЕУ ім. С. Кузнеця” (http://bit.ly/38Qsjcx), графіку навчального процесу університету (http://bit.ly/37Ewd73) деканатами складаються детальні графіки проведення письмових іспитів, для дисциплін с формою контролю «залік» перездача відбувається протягом періоду, вказаного в графіку навчального процесу ЗВО. Це дозволяє здобувачам мати можливість двічі після закінчення семестру (до початку нового семестру) ліквідувати академічну заборгованість за навчальними дисциплінами. Наприклад: відповідно до розкладу першої перездачі зимової екзаменаційної сесії 2019/2020 н. р. по факультету економічної інформатики 29.01.2020 р. була перездача іспиту за навчальною дисципліною “Технології програмування”, група 6.04.125.010.18.01; друга перездача за цією дисципліною призначена 19.02.20 р. (http://bit.ly/3249QGA).

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

Відповідно до “Положення про апеляцію результатів підсумкового контролю у формі іспиту” (http://bit.ly/2P1SKE3) на початку року на факультеті призначається склад апеляційної комісії факультету. Після оприлюднення результатів екзамену (до початку проведення наступного екзамену) протягом доби студент має право оскаржити результати екзамену, шляхом подання відповідної заявки на ім’я декану факультету. Члени апеляційної комісії перевіряють правильність отриманих балів за кожне завдання білету, на основі критеріїв оцінки дисципліни, яка підписується викладачем та завідувачем кафедри. В разі протиріччя між критеріями та виставленою оцінкою, викладач письмово обґрунтовує свою помилку та за рішенням комісії може підвищити загальну оцінку за екзамен. Рішення апеляційної комісії доводиться до здобувача вищої освіти під підпис та оформляється протоколом. Апеляції від студентів спеціальності 125 “Кібербезпека” до апеляційної комісії не надходили.

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

Політика, стандарти і процедури дотримання академічної доброчесності наведені у:
1. Кодексі академічної доброчесності ХНЕУ ім. С. Кузнеця (п. 3, п. 5, http://bit.ly/2Swgt1k) в університеті сформована політика забезпечення середовища академічної доброчесності, впроваджені заходи щодо формування середовища академічної доброчесності.
2. Кодексі професійної етики та організаційної культури працівників і студентів ХНЕУ ім. С. Кузнеця (http://bit.ly/2SPAnn3).
3. Положення про порядок проходження рукопису від його підготовки до видання у ХНЕУ ІМ. С. Кузнеця (http://bit.ly/3cclVxg).
4. Регламент перевірки на унікальність рукописів У ХНЕУ ім. С. Кузнеця (http://bit.ly/37WuWIm).

Які технологічні рішення використовуються на ОП як інструменти протидії порушенням академічної доброчесності?

Відповідно до Кодексу академічної доброчесності ХНЕУ ім. С. Кузнеця (п. 5, http://bit.ly/2Swgt1k) методичний відділ перевіряє на наявність плагіату та встановлює рівень унікальності монографій, підручників та навчальних посібників науково-педагогічних працівників, що видаються в ХНЕУ ім. С. Кузнеця. Перевірка має на меті запобігання плагіату, підвищення якості видань, сприяє активізації самостійності та індивідуальності в процесі створення авторських творів науково-педагогічними працівниками, стимулювання добросовісної конкуренції і спрямована на формування поваги до інтелектуальних надбань, сумлінного дотримання вимог академічної етики, забезпечення довіри до результатів наукових (творчих) досягнень. У 2014 р. створено єдину електронну базу видань, яка щорічно поповнюється, кількість внесених до неї робіт (проектів) становить 10165 найменувань. (Приклад перевірки видань викладачів кафедри (http://bit.ly/39YYAhx). Між Університетом та ТОВ "Плагіат" підписаний ліцензійний договір № 218-52 від 22.05.2019 р. на 2019 рік, на 2020 рік – № 89-52 від 11.02.2020 р. про надання права користуванням антиплагіатним програмним забезпеченням, а саме доступ до системи StrikePlagiarism.com.

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

Університет популяризує академічну доброчесність серед здобувачів вищої освіти шляхом використання веб-ресурсів університету. Так Кодекс академічної доброчесності ХНЕУ ім. С. Кузнеця

розміщений на сайті університету у закладці Головна / Документи університету (п. 5, http://bit.ly/2Swgt1k). В закладці Головна / Аспірантура: Академічна доброчесність аспірантів (http://bit.ly/2SQhW1v) визначені: заходи щодо дотримання академічної доброчесності здобувачами освіти, форми порушення академічної доброчесності здобувачами освіти, відповідальність за порушення академічної доброчесності здобувачів освіти. Популяризація поняття та принципів академічної доброчесності вивчається студентами першого курсу у рамках навчальної практики "Університетська освіта". В рамках дисциплін, які пов'язані з основами наукових досліджень розглядається питання академічної доброчесності, а також при публікаціях тез та наукових статей здобувачами вищої освіти.

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

Відповідно до Кодексу академічної доброчесності ХНЕУ ім. С. Кузнеця (п. 5, http://bit.ly/2Swgt1k) за порушення академічної доброчесності педагогічні, науково-педагогічні та наукові працівники закладів освіти відповідно до закону України "Про освіти" можуть бути притягнені до такої академічної доброчесності: відмова у присудженні наукового ступеня чи присвоєнні вченого звання; позбавлення присудженого наукового (освітньо-творчого) ступеня чи присвоєння вченого звання; відмова в присвоєнні або позбавлення присвоєного педагогічного звання, кваліфікаційної категорії; позбавлення права брати участь у роботі визначених законом органів чи займати визначені законом посади. За порушення академічної доброчесності здобувачі освіти відповідно до закону України "Про освіту" можуть бути притягнені до такої академічної відповідальності: повторне проходження оцінювання (контрольна робота, іспит, залік та інше); повторне проходження відповідного освітнього компонента освітньої програми.

6. Людські ресурси

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

Відповідно до Положення "Про проведення конкурсного відбору науково-педагогічних працівників ХНЕУ ім. С. Кузнеця та укладання з ними трудових договорів (контрактів)" (Протокол № 6 від 21.12.2015 р.) (п. 2-3, http://bit.ly/37AwIyT) 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. Під час конкурентного добору викладачів ОПП "Кібербезпека" враховується наукова та професійна діяльність викладачів, а саме: публікації в науково-метричних базах SCOPUS, Web of Science, наявність сертифікатів неформальних курсів, за дисциплінами, які планується викладати, наявність сертифікатів з іноземних мов, наявність сертифікатів підвищення кваліфікації в галузі "Захисту інформації". Висновки кафедр про професійні та особистісні якості претендентів затверджуються відкритим або таємним голосуванням та передаються до експертно-кваліфікаційної комісії разом з окремими висновками учасників засідання, які викладені в письмовій формі. Оголошення конкурсу на заміщення вакантної посади науково-педагогічного працівника розміщується на сайті університету (http://bit.ly/2u4soKo) та в газеті "Харковские известия" (http://izvestia.kharkov.ua/gazeta/).

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

Під час формування ОПП "Кібербезпека" для погодження формування компетентностей здобувачів вищої освіти та на їх основі формування дисциплін навчального плану, які повинні забезпечити формування відповідних компетентностей були залучені комерційний директор ТОВ "Сайфер БІС", кан.тех.наук Ковтун Владислав Юрійович; директор ТОВ "Талантаріум" Кулик Євгеній Юрійович, Кравченко Павло Олександрович, співзасновник "Distributed Lab". Які, на основі запитів бізнесу, розвитку сучасних технологій в галузях "Захисту інформації" та "Кібербезпеки" запропонували включення до навчального плану відповідних дисциплін, а саме "Blockchain: основи та приклади застосування", "Основи смарт-контрактів", "Основи розробки децентралізованих застосувань (decentralized applications (DAPPS))", використовувати в навчальних дисциплінах сучасні курси неформальної підготовки академії Cisco, а саме "IT Essentials", " Introduction to Cybersecurity", " Cybersecurity Essentials", курси "CCNA Routing and Switching", "Introduction to Packet Tracer", "CCNA Security". В рамках співробітництва з компанією "Глобал Лоджик Україна" та "Distributed Lab" експерти компаній проводять майстер-класи за тематикою спеціальності 125 "Кібербезпека" та блокчейн-технології.

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

В рамках співробітництва з міжнародної компанією “Глобал Лоджик Україна” експерти компанії проводять майстер-класи за тематикою спеціальності 125 “Кібербезпека” (в межах співпраці ХНЕУ ім. С. Кузнеця та міжнародної компанії “Глобал Лоджик Україна” відбулись відкриті лекції: 13.11.2018 р. Місце бізнес-аналізу у циклі розробки програмного продукту (http://bit.ly/2Syk1QC), 26.03.2019 р. Огляд технологій сучасних кібератак (http://bit.ly/2UTlanE).
В рамках дисципліни “Безпека банківських систем” в режимі онлайн-конференції до лабораторних занять залучались професіонали практики компанії “Сайфер”, які проводили майстер-клас щодо використання та налаштування центру сертифікації ключів, використання програмних застосунків “Addin” для office 2010. В рамках дисципліни “Основи національної безпеки” спеціалістами компанії “Distributed Lab” будуть організовані майстер-класи з блокчейн-технології та децентралізованих систем в рамках концепції діджиталізації (http://bit.ly/2SCNI3h) 21.02.2020 р., 13.03.2020 р., 27.03.2020 р., 10.04.2020 р., 24.04.2020 р.

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

Професійному розвитку викладачів ОПП “Кібербезпека” сприяє система післядипломної освіти ХНЕУ ім. С. Кузнеця (http://bit.ly/2uT2eur), у межах якої пропонуються програми з підвищення кваліфікації та тренінги з розвитку загальних і професійних компетентностей, актуальних навичок викладача. На сайті персональних навчальних систем ХНЕУ ім. С. Кузнеця в кожній дисципліні є можливість проведення опитування “ Навчальна дисципліна очима студентів” (http://bit.ly/2HBGmq9), яка дозволяє отримати об’єктивну оцінку рівня викладання дисципліни. Для підвищення професійного рівня викладачів на сайті університету наведені Програми підвищення кваліфікації для науково-педагогічних працівників на 2019-2020 н. р. (http://bit.ly/2SUlS1l). Викладачі університету мають можливість пройти сертифікацію Business English Certificates (BEC) – кембріджські іспити на знання ділової англійської мови. Науково-педагогічні працівники мають право підвищити свій професійний рівень шляхом проходження курсів в Академії “CISCO ХНЕУ ім. С. Кузнеця”. Наприклад, професор кафедри кібербезпеки та інформаційних технологій Алексієв В. О., завідувач кафедри кібербезпеки та інформаційних технологій Євсеєв С. П. отримали сертифікати “CCNA Routing and Switching” 09.07.2019 р. Доценти кафедри Корольов Р. В., Погасій С. С., Король О. Г. отримали сертифікат академії CISCO “IT Essentials” (http://bit.ly/2HIdfBF).

Продемонструйте, що ЗВО стимулює розвиток викладацької майстерності

Матеріальне стимулювання діяльності викладачів регулюється Положенням про преміювання науково-педагогічного, наукового, адміністративно-управлінського, навчально-допоміжного та обслуговуючого персоналу університету (Додаток К до Колективного договору між ХНЕУ ім. С. Кузнеця та ППО ХНЕУ ім. С. Кузнеця на 2019 – 2020 роки (http://bit.ly/2P08ojq). Динаміка обсягів мотиваційних доплат до заробітної плати (надбавок, премій, матеріальної допомоги) ,щорічно висвітлюється у Звітах ректора (приклад, Звіт ректора ХНЕУ ім. С. Кузнеця за 2019 рік та завдання на наступний рік, с. 187, (http://bit.ly/2TdLmXL). Стимулюванню розвитку викладацької майстерності сприяє запровадження рейтингового оцінювання діяльності науково-педагогічних працівників університету з 2012 року. Первинним регулюючим документом є “Методика кількісної оцінки науково-педагогічної діяльності викладачів університету” (http://bit.ly/2HvxGll). На протязі 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?

Розподіл фінансових коштів згідно з стратегією розвитку університету можна відстежити у звітах ректора за кожний рік (наприклад, за 2018 – http://bit.ly/2SU0TwY, за 2019 – http://bit.ly/2TdLmXL). Матеріально-технічні ресурси: бібліотечний фонд за спеціальністю відповідає Ліцензійним умовам; в університеті є доступ до багатьох online-ресурсів за спеціальностями (http://library.hneu.edu.ua/e-media); використовується безкоштовне програмне забезпечення, trial-версії або ліцензійне програмне забезпечення, яке оформлене належним чином та дає можливість використовувати в навчальному-методичному процесі. Кількість мультимедійних проекторів складає 97. Інформація щодо матеріально-технічного забезпечення наведена за посиланням (http://bit.ly/2SQRNRk). Цей документ містить в собі опис площ, розрахунки відповідно до Ліцензійних умов, опис можливостей для маломобільних груп населення (осіб з інвалідністю) тощо.
Основним інструментом для надання студентом інформації щодо курсу є сайт персональних навчальних систем університету https://pns.hneu.edu.ua/, де за кожною дисципліною розміщується РПНД, робочий план (технологічна карта), а також сучасна література в електронному форматі, статті та аналітичні матеріали, завдання для виконання лабораторних робіт, практики, проміжного контролю тощо.

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?

В ХНЕУ ім. С. Кузнеця студенти можуть обрати для себе будь-яку ланку, де можуть себе самореалізувати позанавчальним процесом, основні події підтримки здобувачів вищої освіти наведені у календарі подій (http://bit.ly/2uMf2D8). Діють такі об'єднання, як орган студентського самоврядування (http://bit.ly/37DaQmv). Студенти та викладачі мають безкоштовний вільний доступ до Інтернету, інфраструктури, інформаційних ресурсів університету, можливість попереднього дистанційного замовлення видань фонду електронного каталогу бібліотеки (http://bit.ly/324XLB7), сайту персональних навчальних систем університету (https://pns.hneu.edu.ua/), Facebook (http://bit.ly/325W2LY), Instagram (http://bit.ly/2VfN6lF) для інформування та залучення. В університеті періодично проводиться опитування щодо оцінювання задоволеності потреб та інтересів здобувачів вищої освіти ОПП "Кібербезпека" (http://bit.ly/2HIdfBF).
Так, за результатами опитування навчально-педагогічного персоналу (НПП) університету, 84,9% в цілому задоволені матеріально-технічним забезпеченням університету. Зокрема, зручністю навчальних приміщень задоволені 85,6%, необхідним обладнанням – 81,3%.
Інформаційним забезпеченням задоволені 82,0% НПП. Роботою бібліотеки – 81,3%, доступом до наукометричних баз даних – 82,7%, сайтом ПНС – 92,1%, репозитарієм університету – 79,9%, електронним журналом – 67,6%, електронним розкладом – 95,7%.

Опишіть, яким чином ЗВО забезпечує безпечність освітнього середовища для життя та здоров'я здобувачів вищої освіти (включаючи психічне здоров'я)?

Медичне забезпечення (http://bit.ly/2P27a7m):
• Лікар медичного пункту – Піддубко Ольга Єгорівна.
• Медсестра медичного пункту – Гончаренко Анастасія Кирилівна
Пункт охорони здоров'я ХНЕУ ім. С. Кузнеця (розташований у приміщені гуртожитку "П'ятірочка", 1-й поверх), який є підрозділом Харківської міської студентської лікарні. Пункт охорони здоров'я обслуговує студентів університету. Одним з пріоритетних напрямків діяльності пункту охорони здоров'я є лікувально-профілактична робота. З 2017 року студенти мають можливість записатися на прийом до лікарів Харківської міської студентської лікарні через сайт (http://bit.ly/2HBGKF7).
Також на базі ХНЕУ ім. С. Кузнеця створена соціально-психологічна служба (http://bit.ly/2HB2Zvc). Психолог: Кутвицька Тетяна Олександрівна. Метою діяльності служби є соціально-психологічне забезпечення навчально-виховного процесу, підвищення ефективності навчального, наукового процесу, особистісний розвиток, захист психічного здоров'я, соціального благополуччя студентів, викладачів та працівників ХНЕУ ім. С. Кузнеця. На базі університету працює телефон довіри та скринька довіри (050–13–51–51–9, кабінет 404, 4 поверх, 1 корпус, E – mail : soc_sluzhba@hneu.edu.ua).
За результатами опитування здобувачів вищої освіти п. "Створені умови безпеки праці та навчання (дотримання санітарних норм, охорона публічного порядку тощо)" – 87,8% (http://bit.ly/2HIdfBF).

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?

В університеті діє освітня підтримка (відділ забезпечення якості освіти та інноваційного розвитку (http://bit.ly/3c2URBo), навчальний відділ (http://bit.ly/2SUbS9u), відділ молодіжної політики та соціального розвитку (http://bit.ly/37DaQmv), гарант програми тощо).
Навчально-методичне забезпечення дисциплін ОПП "Кібербезпека" доступно на сайті персональних навчальних систем (https://pns.hneu.edu.ua/). Методичні рекомендації та навчальні посібники розміщені в електронному репозитарії (http://bit.ly/3bMUxGT). Періодично кураторами груп, завідувачем кафедри проводяться зустрічі для вирішення питань навчального процесу. У Фейсбуці постійно ведеться група Інформаційних технологій та кібербезпека (http://bit.ly/325W2LY). Студенти мають можливість відвідувати Дні кар'єри та Ярмарки вакансій, що проходять на базі університету для подальшого працевлаштування, а також на сайті Відділу працевлаштування студентів та взаємодії з бізнес-структурами (http://job.hneu.edu.ua/). Соціальною підтримкою здобувачів вищої освіти являється соціальна стипендія (Постанова КМ України № 1045 28.12.2016 р. (http://bit.ly/3bWvzVM).
Організаційна підтримка здійснюється відділами: навчальний відділ, відділ працевлаштування студентів та взаємодії з бізнес-структурами (http://job.hneu.edu.ua/), методичний відділ (http://bit.ly/2T7Sd4V) тощо). Інформаційна підтримка здобувачів вищої освіти здійснюється за рахунок веб-ресурсів університету (сайт ЗВО (https://www.hneu.edu.ua/), факультету (http://www.ei.hneu.edu.ua/), кафедри (http://www.kafcbit.hneu.edu.ua/), сайт персональних навчальних систем (https://pns.hneu.edu.ua/), тощо). Консультативна підтримка здійснюється за допомогою відділу працевлаштування студентів та взаємодії з бізнес-структурами, психологічної служби тощо), соціальної (відділ молодіжної політики та соціального розвитку тощо).
За результатами опитування, рівень задоволеності якості освіти складає 74,5%.
Також університетом проводиться робота з реалізації політики гендерної рівності та недопущення дискримінації. Університетом розроблений та впроваджується План гендерної рівності (http://bit.ly/38SLen6).

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

В ХНЕУ ім. С. Кузнеця створено найбільш сприятливі умови для життєдіяльності осіб з обмеженими фізичними можливостями та інших маломобільних груп населення, надається соціальний захист студентам з особливими потребами, враховано і витримано умови для проживання у студентських гуртожитках, а саме:
1. Навчальні корпуси обладнано засобами безбар'єрного доступу: встановлено пандуси, налагоджена безперебійна робота ліфтів, розміщені інформаційні вказівники.
2. В кожному навчальному корпусі на вахті можна дізнатися про контактний телефон чергової особи для супроводу осіб з інвалідністю та маломобільних груп населення в університет
3. Майже всі студенти з обмеженими фізичними можливостями мешкають у гуртожитку №5 «П`ятірочка», який розташований на відстані 20-25 метрів від навчальних корпусів університету.
4. Чергова особа для супроводу допомагає особі з обмеженими фізичними можливостями вирішити питання, з якими особа звернулись до університету.
5. По завершенню відвідування чергова особа університету допомагає особам з обмеженими фізичними можливостями та маломобільним групам населення дістатись виходу з навчальних корпусів та впевнитись, що відвідувачам надано транспортні засоби (http://bit.ly/2V2MKyK).
Керівні документи щодо реалізації права на освіту особами з особливими освітніми потребами розміщені у закладці Інклюзія сайту університету (https://www.hneu.edu.ua/inklyuziya/).
На ОПП "Кібербезпека" такі студенти не навчаються.

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?

В ХНЕУ ім. С. Кузнеця впроваджується політика та процедури врегулювання конфліктних ситуацій (включаючи пов'язані із сексуальними домаганнями, дискримінацією та корупцією). Цим займається адміністрація разом з соціально-психологічною службою, яка діє на базі університету.
Метою діяльності служби є соціально-психологічне забезпечення навчально-виховного процесу, підвищення ефективності навчального, наукового процесу, особистісний розвиток, захист психічного здоров'я, соціального благополуччя студентів, викладачів та працівників ХНЕУ ім. С. Кузнеця.
Політика врегулювання конфліктних ситуацій в ХНЕУ ім. С. Кузнеця включає в себе:
- Просвітницькі заходи − це заходи, що пов'язані з популяризацією конфліктологічних знань, навчанням людей передбачати появу деструктивних конфліктів і їх уникнення. Крім того, сюди також належать заходи, пов'язані з психологічним просвітництвом. Це впроваджується на кураторських годинах, а також розміщується інформація на сайті ХНЕУ ім. С. Кузнеця та на інформаційних стендах університету.
- Принципи запобігання соціальних конфліктів: контролювання соціальної ситуації, свобода вибору як умова попередження конфлікту, протидія примусу, ефект поважного ставлення, принцип об'єктивності, консенсусу інтересів, випередження подій та толерантності.
- Телефон довіри та скринька довіри, до яких можна анонімно повідомити про будь-які конфліктні ситуації (включаючи пов'язані із сексуальними домаганнями, дискримінацією та корупцією). Всі ситуації будуть ретельно вивчені та вчасно відреаговані і розв'язані.
Практичний психолог приймає участь у розв'язанні та запобіганні конфліктних ситуацій на групових та індивіду. Практик застосування таких процедур на ОПП "Кібербезпека" не має.
Посилання:
- Положення про політику та процедури врегулювання конфліктних ситуацій у ХНЕУ ім. С. Кузнеця (http://bit.ly/2V8lxLj).
– Положення про проведення письмових екзаменів у ХНЕУ ім. С. Кузнеця (http://bit.ly/38Qsjcx).
– Положення про апеляцію результатів підсумкового контролю у формі іспиту (http://bit.ly/2P1SKE3).
– Кодекс професійної етики та організація культури працівників та студентів ХНЕУ ім. С. Кузнеця – (http://bit.ly/2SPAnn3 (академічна доброчесність), (http://bit.ly/2P1NrVm).
– План виховної роботи університету на 2019-2020 н.р. (http://bit.ly/2vETyrM). – Соціально-психологічна служба ХНЕУ ім. С. Кузнеця (http://bit.ly/3bNTiqU). – Питання запобігання та виявлення корупції (http://bit.ly/37C7a4v).
– Можливості для студентів з особливими потребами (http://bit.ly/2V2MKyK).
– Статут ХНЕУ ім. С. Кузнеця (http://bit.ly/39IfmRV).

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

Відповідно до Положення про систему внутрішнього забезпечення якості освітньої діяльності та якості вищої освіти, яка оприлюднена і є частиною стратегічного управління ХНЕУ ім. С. Кузнеця (http://bit.ly/2vEiWOv) система внутрішнього забезпечення якості освітньої діяльності та якості освіти (система внутрішнього забезпечення якості) охоплює всі процедури, що здійснює ХНЕУ ім. С. Кузнеця щодо безперервного вдосконалення якості навчального середовища, в якому якість освітніх програм, якість навчання і викладання, якість результатів і кваліфікацій, навчальні можливості та ресурсне забезпечення відповідають затвердженим стандартам, потребам стейколдерів, а також вимогам інших органів, що здійснюють зовнішнє забезпечення якості (http://bit.ly/32cnZBS).

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

Опитування задоволеності дисциплін ОПП “Кібербезпека” проводиться окремо за кожною дисципліною на сайті персональних навчальних систем ХНЕУ ім. С. Кузнеця (https://pns.hneu.edu.ua/), а також відділом забезпечення якості освіти та інноваційного розвитку кожні півроку з функціями: планування, моніторингу та самооцінки розвитку університету; моніторингу якості освітньої діяльності та якості вищої освіти у ЗВО; маркетингово-моніторингові, соціально-психологічні та соціально-педагогічні дослідження; координація системи моніторингу трансформації потреб суспільства для уточнення освітніх (освітньо-професійних, освітньо-наукових) програм кожної спеціальності щодо переліку та змісту компетентностей. Здійснення постійного контролю і координація стану й якості методичного забезпечення навчальних дисциплін, які викладаються забезпечують підрозділи університету: відділ забезпечення якості освіти та інноваційного розвитку стор. 2-4 (http://bit.ly/3bOLTri), методичний відділ стор. 3-4 (http://bit.ly/3aSSAr5), відділ електронних засобів навчання стор. 3-5 (http://bit.ly/2wT1shN), навчальний відділ стор. 2-3 (http://bit.ly/3cWGfE6), відділ маркетингу та корпоративних комунікацій стор. 2-5 (http://bit.ly/2Wamhjt), відділ допомоги працевлаштування студентів та взаємодії з бізнес-структурами стор. 2-5 (http://bit.ly/2WhU7TP), відділ молодіжної політики та соціального розвитку (http://bit.ly/37DaQmv), відділ міжнародних зв’язків (http://bit.ly/2u7WwVn), бібліотека (http://bit.ly/2uVvYqz). Так, результати опитування студентів 2 курсу спеціальності 125 “Кібербезпека” показали, що є необхідність введення навчальних дисциплін з циклу програмування (протокол № 1 від 26.08.2019 р.). Моніторинг результатів пропозицій стейкхолдерів розглядається на засіданнях кафедри (наприклад, протокол № 7 від 24.12.2019 р.) на основі угоди про співпрацю з ЗВО України розробляється узагальнений план підготовки магістрів за програмою двох дипломів з Університетом у Бєльсько-Бялій (Польща), що вимагає здійснення уточнення навчальних дисциплін підготовки здобувачів другого (магістерського) рівня вищої освіти (http://bit.ly/2vWeOsY).

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

Відповідно до Положення про систему внутрішнього забезпечення якості освітньої діяльності та якості вищої освіти, п. 4 (http://bit.ly/2vEiWOv) здобувачі вищої освіти мають право на індивідуалізацію та персоналізацію навчання (http://bit.ly/39JQpFY, http://www.ikt.hneu.edu.ua), академічну мобільність студентів за спільними програмами (http://bit.ly/2wjFxjs), моніторинг та самооцінку результатів навчання (http://bit.ly/2V0nIQJ). З метою періодичного перегляду ОПП “Кібербезпека” на сайті кафедри (http://bit.ly/2P0vXZy) є сторінка, яка дозволяє стейкхолдерам (здобувачі вищої освіти) переглядати ОПП “Кібербезпека” (проекти ОПП “Кібербезпека”) та надавати свої пропозиції щодо їх змін. При розробці проектів ОПП “Кібербезпека” першого (бакалаврського) та другого (магістерського) рівня залучений студент 4 курсу за спеціальністю 125 “Кібербезпека” Макаренко Антон (http://bit.ly/2P0vXZy). У кожному семестрі викладачами кафедри за дисциплінами, які викладають проводиться опитування “Навчальна дисципліна очима студентів”, що дозволяє корегувати тематику та наповненість дисципліни. За рішенням кафедри проводиться опитування задоволеності ОПП “Кібербезпека” серед студентів за спеціальністю (http://bit.ly/2HIdfBF).

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

Відповідно до Положення про систему внутрішнього забезпечення якості освітньої діяльності та якості вищої освіти, яка оприлюднена і є частиною стратегічного управління ХНЕУ ім. С. Кузнеця п. 4 (http://bit.ly/2vEiWOv) здобувачам вищої освіти пропонується онлайн опитування (http://bit.ly/2HAyXrn) результати якого обробляються відділом забезпечення якості освіти та інноваційного розвитку ХНЕУ ім. С. Кузнеця та враховуються під час обговорення питань з оновлення ОПП “Кібербезпека” на засіданнях кафедри (протокол № 3 від 18.10.2019). На сайті персональних навчальних систем (https://pns.hneu.edu.ua) в кожній дисципліні є можливість опитування “Навчальна дисципліна очима студентів”, яка дозволяє оцінити якість отримання компетенцій. Відповідно до Положення про студентське самоврядування ХНЕУ ім. С. Кузнеця п. 2-3 (http://bit.ly/3bIHztM) забезпечує захист прав та інтересів студентів щодо задоволенню їх потреб у сфері навчання; допомагають університету у роботі, спрямованій на поліпшення умов та якості навчання; вносять пропозиції щодо контролю за якістю навчального процесу, беруть участь у вирішенні конфліктних ситуацій, що виникають між студентами та представниками ЗВО (http://bit.ly/2V8lxLj). Студенти молодіжної організації входять до складу вченої ради факультету, що дає можливість впливати на формування наповненості

навчальних дисциплін ОПП (http://bit.ly/2T4t76P).

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

Гарант освітньої програми разом з членами проектної групи на протязі року (не рідше одного разу на півроку проводить обговорення та перегляд освітньої програми під час відкритих лекцій (тренінгів) з фахівцями (експертами) IT компаній). Так під час підпису угоди про співпрацю з компанією "ГлобалЛоджик Україна" (23.10.2018 р.) був проведений круглий стіл із залученням керівного складу університету та лідеру компанії (http://bit.ly/2wtLP0h), під час проведення відкритих лекцій: 13.11.2018 р. Місце бізнес-аналізу у циклі розробки програмного продукту (http://bit.ly/324F00y), 26.03.2019 р. Огляд технологій сучасних кібератак (http://bit.ly/2Huus1o), у рамках зустрічі з співзасновником компанії та експертами компанії "Distributed Lab" (12.07.2019 р., 30.09.2019 р., 11.02.2020 р.), що дозволили визначити навчальні дисципліни, які потрібні для отримання відповідних компетентностей здобувачами вищої освіти. Роботодавці (стейкхолдери) мають можливість додати пропозиції щодо ОПП "Кібербезпека" (http://bit.ly/2P0vXZy).

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

Відповідно до "Положення про систему внутрішнього забезпечення якості освітньої діяльності та якості вищої освіти" п. 7 (http://bit.ly/2vEiWOv) ЗВО забезпечує збір, аналіз і використання відповідної інформації для ефективного управління освітньою діяльністю та освітніми програмами на основі використання інформаційних систем, результати яких оброблюються відділом забезпечення якості освіти та інноваційного розвитку ХНЕУ ім. С. Кузнеця та враховуються під час обговорення питань з проходження практики та працевлаштування здобувачів вищої освіти на засіданнях кафедри. Відповідно до Положення про відділ працевлаштування студентів п. 2-3 (http://bit.ly/2WaKQwD) відділ організовує опитування моніторинг працевлаштування студентів (http://bit.ly/39JlObm). Основними траєкторіями працевлаштування випускників зі спеціальності 125 "Кібербезпека" є: системний адміністратор, спеціаліст з інформаційної безпеки, програміст-аналітик з безпеки, спеціаліст з захисту даних, адміністратор баз даних. Кафедра проводить аналіз конкурентоспроможності майбутніх випускників шляхом дослідження результатів ринку праці, як приклад аналітичний звіт "Розвиток української IT-індустрії" (http://bit.ly/2URO47K).

Які недоліки в ОП та/або освітній діяльності з реалізації ОП були виявлені у ході здійснення процедур внутрішнього забезпечення якості за час її реалізації? Яким чином система забезпечення якості ЗВО відреагувала на ці недоліки?

За результатами моніторингу вступу здобувачів вищої освіти за спеціальністю 125 "Кібербезпека" у 2018 році було виявлено недостатню увагу набуття компетентностей щодо розробки та створення програмних застосунків, які забезпечують безпеку інформації з використанням сучасних мов програмування, у 2019 р., здобувачам вищої освіти запропоновані додаткові дисципліни, а саме "Основи алгоритмізації", "Програмування", "Інформаційні системи та Інтернет-технології" (http://bit.ly/321xh3A), що дозволяє забезпечити отримання відповідних компетентностей здобувачами вищої освіти. Для проведення практичних занять навчальних дисциплін, які пов'язані з відпрацюванням практичних питань кібернападу (захисту від кібернападу) необхідне використання програмних застосунків кіберполігону. Для проведення практичних занять з використанням кіберполігону керівництво університету (завідувач кафедри кібербезпеки та інформаційних технологій Євсеєв С. П.) зверталися до Харківського національного університету внутрішніх справ з проханням (на основі підпису угоди про співробітництво між університетами) проходження практики студентами на учбових та технічних базах (кіберполігону) Харківського національного університету внутрішніх справ. Однак, у зв'язку з підключенням мережі кіберполігону до загальної мережі МВД не має можливості доступу студентів університету ХНЕУ ім. С. Кузнеця до навчальних класів Харківського національного університету внутрішніх справ. Також був направлений запит до Director NATO Information and Documentation Centre Barbora Maronkova 05.10.2019 р., з проханням матеріально-технічної, методичної допомоги у розгортанні та налагоджені навчального віртуального кіберполігону на базі локальної обчислювальної мережі ХНЕУ ім. С. Кузнеця.

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

Акредитація ОПП "Кібербезпека" відбувається вперше. Відповідно до "Положення про систему внутрішнього забезпечення якості освітньої діяльності та якості вищої освіти" п. 2.5, п. 2.6 (http://bit.ly/2vEiWOv), "Тимчасового положення про освітні програми" (http://bit.ly/2SUsU6f) з метою своєчасного врахування зауважень та пропозицій від стейкхолдерів 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 (http://bit.ly/2P0vXZy). Це дозволяє своєчасно реагувати на пропозиції та зауваження, враховуючи результати зовнішнього забезпечення якості вищої освіти, зауваження та пропозиції.

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

Відповідно до “Положення про систему внутрішнього забезпечення якості освітньої діяльності та якості вищої освіти”, яка оприлюднена і є частиною стратегічного управління ХНЕУ ім. С. Кузнеця п. 2 (http://bit.ly/2vEiWOv), “Тимчасового положення про освітні програми” (http://bit.ly/2SUsU6f) розроблення освітніх програм для кожного освітнього ступеня та спеціальності здійснюється проектними групами, до складу яких входять провідні науково-педагогічні працівники із залученням представників ринку праці, студентського самоврядування. З метою своєчасного врахування зауважень та пропозицій від стейкхолдерів, 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 (http://bit.ly/3aRH1Ap).

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

Відповідно до “Положення про систему внутрішнього забезпечення якості освітньої діяльності та якості вищої освіти”, яка оприлюднена і є частиною стратегічного управління ХНЕУ ім. С. Кузнеця (http://bit.ly/2vEiWOv) розподіл відповідальності муж структурними підрозділами університету у контексті здійснення процедур внутрішнього забезпечення якості освіти (http://bit.ly/32cnZBS): відділ забезпечення якості освіти та інноваційного розвитку стор. 2-4 (http://bit.ly/3bOLTri) , методичний відділ стор. 3-4 (http://bit.ly/3aSSAr5), відділ електронних засобів навчання стор. 3-5 (http://bit.ly/2wT1shN), навчальний відділ стор. 2-3 (http://bit.ly/3cWGfE6), відділ маркетингу та корпоративних комунікацій стор. 2-5 (http://bit.ly/2Wamhjt), відділ допомоги працевлаштування студентів та взаємодії з бізнес-структурами стор. 2-5 (http://bit.ly/2WhU7TP), відділ молодіжної політики та соціального розвитку (http://bit.ly/37DaQmv), відділ міжнародних зв’язків (http://bit.ly/2u7WwVn), бібліотека (http://bit.ly/2uVvYqz).

9. Прозорість і публічність

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

Права та обов’язки регулюються документами, які розміщені на сайті університету:
Тимчасове положення про організацію освітнього процесу в ХНЕУ ім. С. Кузнеця (http://bit.ly/2vGT1FA).
Правила внутрішнього трудового розпорядку для працівників ХНЕУ ім. С. Кузнеця (http://bit.ly/2uKbsJH).
Тимчасове положення “Про порядок оцінювання результатів навчання студентів за накопичувальною бально-рейтинговою системою” (http://bit.ly/322FpAV).
Положення про порядок конкурсного відбору науково-педагогічних працівників (http://bit.ly/38DrvaO).
Положення про порядок формування рейтингу успішності студентів ХНЕУ ім. С. Кузнеця (для призначення академічних стипендій (http://bit.ly/2P3VLUo).
Положення про порядок реалізації права на академічну мобільність учасників освітнього процесу у ХНЕУ ім.С. Кузнеця (http://bit.ly/321BKTK).
Положення про моніторинг та самооцінку якості результатів навчання студентів у ХНЕУ ім. С. Кузнеця (http://bit.ly/2vGRsaY).
Положення про порядок організації та проведення підготовки фахівців за дуальною формою здобуття вищої освіти у ХНЕУ ім. С. Кузнеця (http://bit.ly/3bG8V3D).

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

На сайті кафедри: http://bit.ly/2P0vXZy.

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

На сайті університету: http://bit.ly/2ubF02w.
На сайті кафедри: http://bit.ly/38Fw58C.

11. Перспективи подальшого розвитку ОП

Якими загалом є сильні та слабкі сторони ОП?

Сильними сторонами ОПП “Кібербезпека” є впровадження сучасного підходу до підготовки бакалаврів з кібербезпеки, а саме поєднання набуття компетентностей, які дозволяють працевлаштовуватись програмістами-аналітиками зі знанням сучасних засобів та програмних застосунків забезпечення безпеки. Вивчення блоку дисциплін з блокчейн-технології дозволяє здобувачам вищої освіти отримувати знання в сучасних новітніх технологіях. Використання неформальних форм навчання згідно з “Положення про порядок визнання результатів неформальної та інформальної освіти у ХНЕУ ім. С. Кузнеця” (http://bit.ly/2HElTRQ), а саме навчальних курсів академії CISCO дозволяє здобувачам вищої освіти отримувати компетентності, які вимагають лідери в IT-індустрії, комутації та маршрутизації з забезпеченням відповідного рівня безпеки. Впровадження в підготовку технологій PKI на основі ЦСК дозволяє здобувачам вищої освіти отримувати відповідні компетенції щодо їх застосування в електронному документообігу, майстер-класів з блокчейн-технології. Програма двох дипломів на другому (магістерському) рівні з Університетом у Бєльсько-Бялій (Польща) та університетів партнерів в Україні (НАУ, Чернігівський національний технологічний університет, Одеський державний екологічний університет) забезпечує формування компетентностей конкурентоспроможних не тільки в Україні, а також в Євросоюзі.
Слабкими сторонами ОПП “Кібербезпека” є відсутність дуальної форми навчання за окремими планами, врахування пропозицій незначної кількісті IT-компаній, громадських організацій щодо формування компетентностей здобувачів вищої освіти та результатів навчання, відсутність кіберполігону на базі університету.

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

Перспективами розвитку ОПП “Кібербезпека” є формування практичних проектів на базі лабораторії блокчейн-технологій. Розгортання кіберполігону для проведення практичних занять з навчальних дисциплін “Безпека даних та веб-додатків”, “Програмування захищених веб-систем”, “Безпека інтернет-речей”, “Тестування на проникнення та етичний хакінг”, “Цифрова криміналістика”, “Бездротова та мобільна безпека”. Впровадження в освітній процес інноваційних технологій та методів навчання, впровадження підходів до модернізації навчання, вивчення та оцінювання, розробка навчального плану для підготовки фахівців за дуальною формою навчання, розширення ОПП “Кібербезпека” для набору іноземних студентів.

Запевнення

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

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

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

Додатки:

Таблиця 1. Інформація про обов’язкові освітні компоненти ОП

Таблиця 2. Зведена інформація про викладачів ОП

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

***

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

Документ підписаний кваліфікованим електронним підписом/кваліфікованою електронною печаткою.

Інформація про КЕП

ПІБ: Пономаренко Володимир Степанович

Дата: 16.03.2020 р.

Таблиця 1. Інформація про обов’язкові освітні компоненти ОП

Назва освітнього компонента	**Вид компонента**	**Силабус або інші навчально-методичні матеріали**		**Якщо освітній компонент потребує спеціального матеріально-технічного та/або інформаційного забезпечення, наведіть відомості щодо нього***
		Назва файла	**Хеш файла**	
Комплексні системи захисту інформації	навчальна дисципліна	*Основи технічного захисту інформації.pdf*	197A6f96MzP311vTCXozpLKIdXKw4u4n9FFIEQzwQWU=	*Vmware Player*
Основи національної безпеки	навчальна дисципліна	*Основи національної безпеки.pdf*	U8mcgc1p44ON2cx/qdoT58Xh4sWByUAdXi26czE++i0=	*Cisco Packet Tracer 7.2*
Основи стеганографічного захисту інформації	навчальна дисципліна	*Основи стеганографічного захисту інформації.pdf*	wSgciS54TNbkwrR/V7dLaMrSUk6W25ZI9FUjQogDSFA=	*Mathcad 14, Steganos Privacy Suite 15-free*
Основи алгоритмізації	навчальна дисципліна	*Основи алгоритмізації.pdf*	uXehY35lyihv02Uyku0wMEpl5olcxnwYU5gwH+J4Ssc=	*CS50 IDE*
Безпека інтернет-речей	навчальна дисципліна	*Безпека_Інтернет_речей.pdf*	Nbnkkv9OXwyAvlLwBziT7tB0xCjtXA4xciJkjrnT+Co=	*Vmware Player, Kali Linux*
Програмування	навчальна дисципліна	*Програмування.pdf*	NnUHTDHzskffC5qDIwNNWdk/6OHYF/OqIY2+kgWU0Z8=	*CS50 IDE*
Організаційне забезпечення захисту інформації	навчальна дисципліна	*Організаційне забезпечення захисту інформації.pdf*	etCgX4ZLGe2/hBkC8JoqQP5F4zn7xiD79NDFJQ0169U=	*Cisco Packet Tracer 7.2*
Тренінг-курс “Безпека життєдіяльності”	навчальна дисципліна	*Тренінг-курс Безпека життєдіяльності.pdf*	Aa4CKHD5l9cStA+HBDtEAL6051Lz2NZ9NJFHJaO04Xk=	
Навчальна практика “Університетська освіта”	навчальна дисципліна	*Наскрізна програма практика.pdf*	7kZulX593k4bpK/dzuYKOZh1xKvSaBqncNJMro3shAE=	
Виробнича практика	навчальна дисципліна	*Наскрізна програма практика.pdf*	7kZulX593k4bpK/dzuYKOZh1xKvSaBqncNJMro3shAE=	
Переддипломна практика	навчальна дисципліна	*Наскрізна програма практика.pdf*	7kZulX593k4bpK/dzuYKOZh1xKvSaBqncNJMro3shAE=	
Дипломний проект	навчальна дисципліна	*Дипломний проект.pdf*	ooeXOzlRuZpoQttWOclityOMUmT9jVSRKNfxekE7L1A=	
Комплексний курсовий проект	навчальна дисципліна	*Комплексний курсовий проект.pdf*	3pfqMha/kRweXvI0+9tUpMOURLUyye9prGxvm2tGvRU=	*Vmware Player*
Курсовий проект: Введення в мережі	навчальна дисципліна	*Комплексний курсовий проект.pdf*	3pfqMha/kRweXvI0+9tUpMOURLUyye9prGxvm2tGvRU=	*Cisco Packet Tracer 7.2*
Тренінг-курс “Основи охорони праці”	навчальна дисципліна	*Тренінг-курс Основи охорони праці.pdf*	E/WLH3Kr+rKCQNN7kZbVfFdxtx76jINzOAv/lq/XpoM=	
Основи побудови та захисту сучасних операційних систем	навчальна дисципліна	*Основи побудови та функціонування мікропроцесорних систем.pdf*	rehiDl0LJhtaxjDu6BtYl4zU4puEMK3Wu+VFZpXA3eE=	*Vmware Player, Linux Ubuntu*
Організація та інформаційне забезпечення управлінської діяльності	навчальна дисципліна	*Організація та інформаційне забезпечення управлінської діяльності.pdf*	eqixdZu1dhLPiGKA+pTNJ4jZo4C3X/06ecIgRWUQdrs=	
Безпека в інформаційно-комунікаційних системах	навчальна дисципліна	*Безпека в інформаційно-комунікаційних системах.pdf*	kub2SnUNZGsPr/IKgwmwDg1LZzz7s634H4XsetsKR0U=	*Cisco Packet Tracer 7.2*
Українська мова (за професійним спрямуванням)	навчальна дисципліна	*Українська мова (за професійним спрямуванням).pdf*	FFrVYSveQF1FHezajSWOwaIvn17tTkUZBhiuIFXlRDE=	
Іноземна мова (за професійним спрямуванням)	навчальна дисципліна	*Іноземна мова (за професійним спрямуванням).pdf*	+G+kcNkm8As1DDZ/QFs6NNYzXlxR115OkAcv71MnPEo=	
Соціальна та економічна історія України	навчальна дисципліна	*Соціальна та економічна історія України.pdf*	+iZBi4j+wWb2kngzUi6iBHV41j7ZhH/RcyIZzNtUpCs=	
Філософія	навчальна дисципліна	*Філософія.pdf*	3YH9F3w4DYvZts3AY3EaxiOPx+er7sNX2maBDVnskB8=	

Математичні основи криптології	навчальна дисципліна	*Математичні основи криптології.pdf*	wVjN7Ea0guMUTmGBoXFxQIVkiGMJNeVWk+vJt1a4D1Y=	*Information Security*
Вища математика	навчальна дисципліна	*Вища математика.PDF*	483gA3toA2HQCYnGgf3cyBK2Rc0YtHa3EbmTYwdMlgk=	
Інформаційна безпека держави	навчальна дисципліна	*Інформаційна безпека держави.pdf*	81EqoVIrjtF3ItMgm6+1+8HLDewLyMW023rcyS2C9Ik=	*Cisco Packet Tracer*
Теоретичні основи криптографії	навчальна дисципліна	*Теоретичні основи криптографії.pdf*	YRIBTQ9yQeGN1h7KJzYWFG/eUF2tQpv3hl0bu5tiBRo=	*Information Security*
Основи побудови та функціонування мікропроцесорних систем	навчальна дисципліна	*Основи побудови та функціонування мікропроцесорних систем.pdf*	rehiDl0LJhtaxjDu6BtYI4zU4puEMK3Wu+VFZpXA3eE=	*Arduino IDE, AVR Studio, Proteus RemoteXY*
Основи математичного моделювання	навчальна дисципліна	*Основи математичного моделювання.pdf*	un0GOvOP9R7ev84MdpCWqwTml3hPF6g+bdBLZen1EZE=	
Технології програмування	навчальна дисципліна	*Технології програмування.pdf*	9EOgZ2zzzN6IvZUU2d0ZbZpjIDDYev2GY5VLMzBT1ns=	*Repl.it*
Основи криптографічного захисту	навчальна дисципліна	*Основи криптографічного захисту.pdf*	TKXBw35BDf6KLGN7Qco+i8GdLal4n1Z0uTgK2qjWU9o=	*PGP Desktop-free Steganos Privacy Suite 15-free Information Security*
Основи технічного захисту інформації	навчальна дисципліна	*Основи технічного захисту інформації.pdf*	197A6f96MzP311vTCXozpLKIdXKw4u4n9FFIEQzwQWU=	*Vmware Player, Kali Linux*
Менеджмент інформаційної безпеки	навчальна дисципліна	*Менеджмент інформаційної безпеки.pdf*	FGyu1DOklFfvZmHRalAI1BfQSd+Osln+orFHv1xW5cs=	
Введення в мережі	навчальна дисципліна	*Введення в мережі.pdf*	Z+JFa6zHDXvNH5E3BR8PvLUam5aWLN0qMHxHG4LUnro=	*Cisco Packet Tracer 7.2*
Комплексний тренінг	навчальна дисципліна	*Комплексний тренінг.pdf*	DzoMEb2rMys0I/kAD5hms0TkaKJ5bE/vVHG+Eq6noj8=	*Vmware Player, Kali Linux*
Інформаційні системи та інтернет технології	навчальна дисципліна	*Інформаційні системи та інтернет технології.pdf*	20jIpd+VCOYT6Pe2KjX/B1CmJX459+nsDyIh3qMCvOo=	*IntelijIdea, NetBeans, JavaDoc*

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

Таблиця 2. Зведена інформація про викладачів ОП

ID викладача	ПІБ	Посада	Структурний підрозділ	Кваліфікація викладача	Стаж	Навчальні дисципліни, що їх викладає викладач на ОП	Обґрунтування
117383	Добрунова Людмила Едуардівна	Доцент			0	Соціальна та економічна історія України	Посада: доцент кафедри українознавства і мовної підготовки іноземних громадян. Структурний підрозділ, у якому працює викладач: кафедра українознавства і мовної підготовки іноземних громадян. Інформація про кваліфікацію викладача: Харківський державний університет ім. О. М. Горького, 1982 р., кандидат історичних наук, Диплом ДК № 011458 від 01.07.2001. Доцент кафедри українознавства (атестат 02 ДЦ № 015483 від 19.11.2005 р.). Стаж науково-педагогічної роботи: 30 років. Відповідно до пункту 30 Ліцензійних вимог п. 2, 3, 10, 13, 14, 15, 17
170858	Рибалко Антоніна Павлівна	Доцент			0	Вища математика	Посада: доцент кафедри вищої математики та економіко-математичних методів. Структурний

							підрозділ, у якому працює викладач: кафедра вищої математики та економіко-математичних методів. Інформація про кваліфікацію викладача: Харківський державний університет Спеціальність: “прикладна математика”, Кваліфікація: математик-прикладник Диплом ЛО ВЕ № 00238 від 30.06.1995 р. Кандидат фізико-математичних наук 113 Прикладна математика (01.01.03: математична фізика). Тема: “Усереднення диференціальних форм на многовидах складної мікроструктури” (диплом ДК № 035889 від 04.07.2006 р.) Доцент кафедри вищої математики та економіко-математичних методів (атестат 12ДЦ № 041759 від 25.02.2015 р.) Стаж науково-педагогічної роботи: 23 роки. Відповідно до пункту 30 Ліцензійних вимог п. 1-3, 13-15
202852	Потоцька Юлія Іванівна	Доцент			0	Філософія	Посада: доцент кафедри філософії та політології. Структурний підрозділ, у якому працює викладач: кафедра філософії та політології. Інформація про кваліфікацію викладача : Харківський державний університет, спеціальність – історик, викладач історії та суспільно-політичних наук, диплом ЛГ ВС № 005783, від 27.06.1997. Науковий ступінь: Кандидат філософських наук, спеціальність: 09.00.04 – філософська антропологія, філософія культури, тема дисертації: «Образ філософа у просторі сучасної культури. Європейсько-американський діалог» диплом ДК № 020954 від 12.11.2003 р. Вчене звання: доцент кафедри філософії та політології атестат доцента 12ДЦ № 019729 від 03.07.2008 р. Підвищення кваліфікації: ХНЕУ імені Семена Кузнеця, свідоцтво про підвищення кваліфікації 12СПК 990951 від 15.01.2015 р. (з 06.10.2014 р. .до 15.01.2015 р. Тема: Розробка персональної навчальної системи з дисципліни «Філософія»). Загальна кількість наукових та науково-методичних публікацій 45 праць, серед яких 3 монографії (у співавторстві), 6 навчальних посібників (у співавторстві). Стаж

							науково-педагогічної роботи: 17 років. Відповідно до пункту 30 Ліцензійних вимог п. 2-3, 13-15, 17
200400	Томах Вікторія Володимирівна	Доцент			0	Організація та інформаційне забезпечення управлінської діяльності	Посада: доцент кафедри економіки, організації та планування діяльності підприємства. Структурний підрозділ, у якому працює викладач: кафедра економіки, організації та планування діяльності підприємства. Інформація про кваліфікацію викладача: Харківський державний економічний університет, 2001 р., “Облік і аудит”, економіст, спеціаліст диплом ХА №16790411 30 червня 2001 р. Кандидат економічних наук, 073-Менеджмент, 08.00.04 «Економіка та управління підприємствами (за видами економічної діяльності)». Тема дисертації: “Управління якістю трудового життя персоналу промислового підприємства”, диплом № 051049 від 28 квітня 2009 р. Доцент кафедри економіки, організації та планування діяльності підприємства. Атестат 12 ДЦ № 042520 28 квітня 2015 р. Стаж науково-педагогічної роботи: 15 років. Відповідно до пункту 30 Ліцензійних вимог п. 2-3, 13-16, 18
24736	Щербаков Олександр Всеволодович	Професор			0	Основи алгоритмізації	Посада: професор кафедри інформаційних систем. Структурний підрозділ, у якому працює викладач: кафедра інформаційних систем. Інформація про кваліфікацію викладача: Харківський державний університет ім. О.М. Горького, спеціальність «математика», кваліфікація математик, 1 вересня 1984 р., диплом КВ №737788. Перепідготовка по програмі НАТО-Україна з перепідготовки військовослужбовців за спеціалізацією «Комп’ютерні системи та мережі». Хмельницький національний університет. Сертифікат №2546 від 08.02.2013 р. Кандидат технічних наук, спеціальність 20.02.12 «Військова кібернетика, інформатика, системний аналіз, дослідження операцій» (старий шифр відповідно до наказу ВАК № 86 від 13.03.1997), 05.13.06 «Інформаційні технології» (новий шифр відповідно до

							наказу ВАК № 377 від 23.06.2005), спецтема, 27 травня 1997 р., диплом кандидата наук КН №014346. Доцент кафедри математичного та програмного забезпечення автоматизованих систем управління, 17 жовтня 2002 р., атестат ДЦ №005465. Стаж науково-педагогічної роботи: 35 р. Відповідно до пункту 30 Ліцензійних вимог п. 2-3, 5, 9, 11, 13, 14, 15
170252	Михайлова Євгенія Олександрівна	Доцент			0	Тренінг-курс “Безпека життєдіяльності”	Посада: доцент кафедри природоохоронних технологій, екології та БЖД. Структурний підрозділ, у якому працює викладач: кафедри природоохоронних технологій, екології та БЖД. Інформація про кваліфікацію викладача: Національний технічний університет «Харківський політехнічний інститут» Спеціальність «Хімічна технологія неорганічних речовин» Кваліфікація «Інженер-хімік-дослідник» Диплом магістра (з відзнакою) ХА №14340069 від 27.02. 2001 р. Кандидат технічних наук, 161 Хімічні технології та інженерія (05.17.01 – технологія неорганічних речовин). Тема дисертаційної роботи: «Одержання хімічно осадженого карбонату кальцію з відходів содового виробництва» (диплом ДК №039900 від 15.03.2007 р.) Доцент кафедри хімічної технології неорганічних речовин, каталізу та екології (атестат 12ДЦ №032266 від 26.09.2012 р.). Стаж науково-педагогічної роботи: 20 р. Відповідно до пункту 30 Ліцензійних вимог п. 1, 2, 3, 11, 13, 14, 15
165226	Буц Юрій Васильович	Завідувач кафедри			0	Тренінг-курс “Основи охорони праці”	Посада: завідувач кафедри природоохоронних технологій, екології та БЖД. Структурний підрозділ, у якому працює викладач: кафедра природоохоронних технологій, екології та БЖД. Інформація про кваліфікацію викладача: Сумський державний педагогічний інститут імені А.С. Макаренка, 1995 р. Спеціальність «Географія та біологія» Кваліфікація «Учитель географії та біології» Диплом ЛП 009490 від 27.06.1995 р. Харківський національний університет міського господарства імені О.М. Бекетова, диплом магістра, кваліфікація: ступінь вищої освіти магістр, спеціальність «Цивільна безпека»,

							освітня програма «Охорона праці», 28.12.2018 р. Стаж науково-педагогічної роботи: 19 р. Відповідно до пункту 30 Ліцензійних вимог п. 1, 2, 3, 4, 5, 7, 8, 10, 13, 14, 15, 16, 17
189990	Алексієв Володимир Олегович	Професор			0	Переддипломна практика	Посада: професор кафедри кібербезпеки та інформаційних технологій. Структурний підрозділ, у якому працює викладач: кафедра кібербезпеки та інформаційних технологій. Інформація про кваліфікацію викладача: Харківський державний автомобільно-дорожній технічний університет, спеціальність електрообладнання автомобілів та тракторів, кваліфікація інженер-електромеханік, диплом ЛМ ВЕ001454 від 17.06.1997 р. доктор технічних наук, 275 Транспортні технології (за видами) (05.22.01 “Транспортні системи”), диплом ДД №008806 від 10.11.2010 р. Професор, атестат 12ПР №008834 від 04.07.2013 р. Стаж науково-педагогічної роботи: 20 р. Відповідно до пункту 30 Ліцензійних вимог п. 1-3, 8, 11-13, 15-17
185780	Коц Григорій Павлович	Доцент 0,5 ст.			0	Виробнича практика	Посада: доцент кафедри кібербезпеки та інформаційних технологій. Структурний підрозділ, у якому працює викладач: кафедра кібербезпеки та інформаційних технологій. Інформація про кваліфікацію викладача: Харківський державний економічний університет, Спеціальність - “Облік і аудит” Кваліфікація - “Економіст” Диплом спеціаліста ЛЕ №010153 від 25.06.1997 р.; Харківський національний економічний університет (перепідготовка), спеціальність “Інформаційні управляючі системи та технології” кваліфікація “аналітик комп’ютерних систем” Диплом спеціаліста ДСК №064394 від 30.12.2004 р. Кандидат економічних наук, 073 Менеджмент (08.06.02 - підприємництво, менеджмент та маркетинг), диплом ДК№011892 від 10.10.2001 р. Доцент (атестат ДЦ №010440 від 17.02.2005 р.). Стаж науково-педагогічної роботи: 21 р. Відповідно до пункту 30 Ліцензійних вимог п. 1-3, 8-10, 12-13, 15.

189990	Алексієв Володимир Олегович	Професор			0	Дипломний проект	Посада: професор кафедри кібербезпеки та інформаційних технологій. Структурний підрозділ, у якому працює викладач: кафедра кібербезпеки та інформаційних технологій. Інформація про кваліфікацію викладача: Харківський державний автомобільно-дорожній технічний університет, спеціальність електрообладнання автомобілів та тракторів, кваліфікація інженер-електромеханік, диплом ЛМ ВЕ001454 від 17.06.1997 р. доктор технічних наук, 275 Транспортні технології (за видами) (05.22.01 “Транспортні системи”), диплом ДД №008806 від 10.11.2010 р. Професор, атестат 12ПР №008834 від 04.07.2013 р. Стаж науково-педагогічної роботи: 20 р. Відповідно до пункту 30 Ліцензійних вимог п. 1-3, 8, 11-13, 15-17
195299	Король Ольга Григорівна	Доцент 0,25 ст.			0	Комплексний тренінг	Посада: доцент кафедри кібербезпеки та інформаційних технологій. Структурний підрозділ, у якому працює викладач: кафедра кібербезпеки та інформаційних технологій. Інформація про кваліфікацію викладача: Харківський національний економічний університет Спеціальність “Інформаційні управляючі системи та технології” Кваліфікація “аналітик комп’ютерних систем”. Диплом спеціаліста ХА №27419687 від 30.06.2005 р. Доцент (атестат 12ДЦ № 045523 від 15.12.2015 р.) Стаж науково-педагогічної роботи: 12 р. Відповідно до пункту 30 Ліцензійних вимог п. 1-3, 12-13, 15
195299	Король Ольга Григорівна	Доцент 0,25 ст.			0	Комплексний курсовий проект	Посада: доцент кафедри кібербезпеки та інформаційних технологій. Структурний підрозділ, у якому працює викладач: кафедра кібербезпеки та інформаційних технологій. Інформація про кваліфікацію викладача: Харківський національний економічний університет Спеціальність “Інформаційні управляючі системи та технології” Кваліфікація “аналітик комп’ютерних систем”. Диплом спеціаліста ХА №27419687 від 30.06.2005 р. Доцент (атестат 12ДЦ № 045523 від 15.12.2015 р.) Стаж науково-

							педагогічної роботи: 12 р. Відповідно до пункту 30 Ліцензійних вимог п. 1-3, 12-13, 15
294414	Гаврилова Алла Андріївна	Старший викладач 0,5 ст.			0	Курсовий проект: Введення в мережі	Посада: старший викладач кафедри кібербезпеки та інформаційних технологій. Структурний підрозділ, у якому працює викладач: кафедра кібербезпеки та інформаційних технологій. Інформація про кваліфікацію викладача: Харківський державний економічний університет, Економічна інформатика і автоматизовані системи управління, інженер-економіст. 07.06.1994, диплом ЛЕ № 007629.Стаж науково-педагогічної роботи: 14 років. Відповідно до пункту 30 Ліцензійних вимог п. 1-3, 10, 13, 17
107556	Євсеєв Сергій Петрович	Завідувач кафедри			0	Навчальна практика “Університетська освіта”	Посада: завідувач кафедри кібербезпеки та інформаційних технологій. Структурний підрозділ, у якому працює викладач: кафедра кібербезпеки та інформаційних технологій. Стаж науково-педагогічної роботи: 32 роки. Інформація про кваліфікацію викладача: 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 (21.05.01 – Інформаційна безпека держави). Диплом ДД № 007606 від 5.07.2018 р. Старший науковий співробітник зі спеціальності системи захисту інформації диплом АС № 007292 від 14.04. 2010 р. Доцент (диплом 12ДЦ № 034106 від 25.01.2013 р.). Відповідно до пункту 30 Ліцензійних вимог п. 1-3, 7-8, 10, 12-15, 17.
129102	Черемська Ольга Степанівна	Завідувач кафедри			0	Українська мова (за професійним спрямуванням)	Посада: завідувач кафедри українознавства і

							мовної підготовки іноземних громадян, професор. Структурний підрозділ, у якому працює викладач: кафедра українознавства і мовної підготовки іноземних громадян. Інформація про кваліфікацію викладача: Івано-Франківський педагогічний інститут ім. В. Стефаника, спеціальність “Українська мова та література” кваліфікація: учитель української мови і літератури середньої школи. Диплом спеціаліста Г-ІІ 048082 від 30.06.1984 р. Кандидат філологічних наук, 035 Філологія (10.02.01 – українська мова). Тема: “Лексична та граматична інтерференція в сучасній українській літературній мові як наслідок українсько-російського білінгвізму (на матеріалі преси Харківщини 50-80-х років ХХ ст.)” (диплом ДК 018412 від 09.04.03 р.) Професор кафедри українознавства та мовної підготовки іноземних громадян (атестат 12ПР 010962 від 29.09.2015 р.) Стаж науково-педагогічної роботи: 33 роки. Відповідно до пункту 30 Ліцензійних вимог п. 1-4, 7-11, 13-18
355403	Ткачов Андрій Михайлович	Доцент 0,25 ст.	Факультет економічної інформатики	Диплом кандидата наук ДК 025982, виданий 13.10.2004, Атестат старшого наукового співробітника (старшого дослідника) АС 000423, виданий 26.09.2012	28	Інформаційні системи та інтернет технології	Посада: доцент кафедри кібербезпеки та інформаційних технологій. Структурний підрозділ, у якому працює викладач: кафедра кібербезпеки та інформаційних технологій. Інформація про кваліфікацію викладача: Харківський військовий університет, за спеціальністю “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., старший науковий співробітник атестат АС № 000423 від 26.09.2012 р. Відповідно до пункту 30 Ліцензійних вимог п. 2, 12, 15, 17
87073	Гонтаренко Ірина Сергіївна	Старший викладач			0	Іноземна мова (за професійним спрямуванням)	Посада: старший викладач. Структурний підрозділ, у якому працює викладач: кафедра педагогіки. іноземної філології та перекладу. Інформація про кваліфікацію викладача: 1.Кандидат педагогічних наук, галузь знань - 01

							Освіта, спеціальність 011 - Освітні, педагогічні науки (13.00.04 - теорія і методика професійної освіти). Тема дисертаційної роботи: “Формування проектної компетентності майбутніх учителів гуманітарних дисциплін засобами інтернет-ресурсів” (диплом ДК №039555 від 13.12.2016 р.). Стаж науково-педагогічної роботи: 8 р. Відповідно до пункту 30 Ліцензійних вимог п. 1-5, 13.
294414	Гаврилова Алла Андріївна	Старший викладач 0,5 ст.			0	Введення в мережі	Посада: старший викладач кафедри кібербезпеки та інформаційних технологій. Структурний підрозділ, у якому працює викладач: кафедра кібербезпеки та інформаційних технологій. Інформація про кваліфікацію викладача: Харківський державний економічний університет, Економічна інформатика і автоматизовані системи управління, інженер-економіст. 07.06.1994, диплом ЛЕ № 007629.Стаж науково-педагогічної роботи: 14 років. Відповідно до пункту 30 Ліцензійних вимог п. 1-3, 10, 13, 17
107556	Євсеєв Сергій Петрович	Завідувач кафедри			0	Безпека в інформаційно-комунікаційних системах	Посада: завідувач кафедри кібербезпеки та інформаційних технологій. Структурний підрозділ, у якому працює викладач: кафедра кібербезпеки та інформаційних технологій. Стаж науково-педагогічної роботи: 32 роки. Інформація про кваліфікацію викладача: 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 (21.05.01 – Інформаційна безпека держави). Диплом ДД № 007606

							від 5.07.2018 р. Старший науковий співробітник зі спеціальності системи захисту інформації диплом АС № 007292 від 14.04. 2010 р. Доцент (диплом 12ДЦ № 034106 від 25.01.2013 р.). Відповідно до пункту 30 Ліцензійних вимог п. 1-3, 7-8, 10, 12-15, 17.
72586	Мілов Олександр Володимирович	Доцент			0	Основи математичного моделювання	Посада: професор кафедри кібербезпеки та інформаційних технологій. Структурний підрозділ, у якому працює викладач: кафедра кібербезпеки та інформаційних технологій. Інформація про кваліфікацію викладача: Московський енергетичний інститут, Спеціальність "Промислова електроніка", Кваліфікація "Інженер електронної техніки". Диплом Я № 287387 від 20.02.1978 р. Доцент (атестат ДЦ №039210 від 04.07.1991 р.). Кандидат технічних наук, 14 Електрична інженерія, 141 Електроенергетика, електротехніка та електромеханіка (05.09.12 - Напівпровідникові перетворювачі електроенергії), диплом ТН №094834 від 12.11.1986 р. Професор, атестат АП №001430 від 16.12.2019 р. Стаж науково-педагогічної роботи: 37 років. Відповідно до пункту 30 Ліцензійних вимог п. 1-4, 6, 8, 10, 13, 15-16.
72586	Мілов Олександр Володимирович	Доцент			0	Основи криптографічного захисту	Посада: професор кафедри кібербезпеки та інформаційних технологій. Структурний підрозділ, у якому працює викладач: кафедра кібербезпеки та інформаційних технологій. Інформація про кваліфікацію викладача: Московський енергетичний інститут, Спеціальність "Промислова електроніка", Кваліфікація "Інженер електронної техніки". Диплом Я № 287387 від 20.02.1978 р. Доцент (атестат ДЦ №039210 від 04.07.1991 р.). Кандидат технічних наук, 14 Електрична інженерія, 141 Електроенергетика, електротехніка та електромеханіка (05.09.12 - Напівпровідникові перетворювачі електроенергії), диплом ТН №094834 від 12.11.1986 р. Професор, атестат АП №001430 від 16.12.2019 р. Стаж науково-педагогічної роботи: 37 років. Відповідно до пункту 30 Ліцензійних вимог п. 1-4, 6, 8, 10, 13, 15-

							16.
72586	Мілов Олександр Володимирович	Доцент			0	Теоретичні основи криптографії	Посада: професор кафедри кібербезпеки та інформаційних технологій. Структурний підрозділ, у якому працює викладач: кафедра кібербезпеки та інформаційних технологій. Інформація про кваліфікацію викладача: Московський енергетичний інститут, Спеціальність "Промислова електроніка", Кваліфікація "Інженер електронної техніки". Диплом Я № 287387 від 20.02.1978 р. Доцент (атестат ДЦ №039210 від 04.07.1991 р.). Кандидат технічних наук, 14 Електрична інженерія, 141 Електроенергетика, електротехніка та електромеханіка (05.09.12 - Напівпровідникові перетворювачі електроенергії), диплом ТН №094834 від 12.11.1986 р. Професор, атестат АП №001430 від 16.12.2019 р. Стаж науково-педагогічної роботи: 37 років. Відповідно до пункту 30 Ліцензійних вимог п. 1-4, 6, 8, 10, 13, 15-16.
72586	Мілов Олександр Володимирович	Доцент			0	Математичні основи криптології	Посада: професор кафедри кібербезпеки та інформаційних технологій. Структурний підрозділ, у якому працює викладач: кафедра кібербезпеки та інформаційних технологій. Інформація про кваліфікацію викладача: Московський енергетичний інститут, Спеціальність "Промислова електроніка", Кваліфікація "Інженер електронної техніки". Диплом Я № 287387 від 20.02.1978 р. Доцент (атестат ДЦ №039210 від 04.07.1991 р.). Кандидат технічних наук, 14 Електрична інженерія, 141 Електроенергетика, електротехніка та електромеханіка (05.09.12 - Напівпровідникові перетворювачі електроенергії), диплом ТН №094834 від 12.11.1986 р. Професор, атестат АП №001430 від 16.12.2019 р. Стаж науково-педагогічної роботи: 37 років. Відповідно до пункту 30 Ліцензійних вимог п. 1-4, 6, 8, 10, 13, 15-16.
273533	Корольов Роман Володимирович	Доцент			0	Комплексні системи захисту інформації	Посада: доцент кафедри кібербезпеки та інформаційних технологій. Структурний підрозділ, у якому працює викладач: кафедра кібербезпеки та інформаційних технологій. Інформація про кваліфікацію

							викладача: 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., ДК № 054389. Кандидат технічних наук, 05.13.06 – інформаційні технології. Диплом ДК №054389. Стаж науково-педагогічної роботи: 24 роки. Відповідно до пункту 30 Ліцензійних вимог п. 1-3, 12, 17
273533	Корольов Роман Володимирович	Доцент			0	Основи технічного захисту інформації	Посада: доцент кафедри кібербезпеки та інформаційних технологій. Структурний підрозділ, у якому працює викладач: кафедра кібербезпеки та інформаційних технологій. Інформація про кваліфікацію викладача: 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., ДК № 054389. Кандидат технічних наук, 05.13.06 – інформаційні технології. Диплом ДК №054389. Стаж науково-педагогічної роботи: 24 роки. Відповідно до пункту 30 Ліцензійних вимог п. 1-3, 12, 17
72586	Мілов Олександр Володимирович	Доцент			0	Програмування	Посада: професор кафедри кібербезпеки та інформаційних технологій. Структурний підрозділ, у якому працює викладач: кафедра кібербезпеки та інформаційних технологій. Інформація про кваліфікацію викладача: Московський енергетичний інститут, Спеціальність "Промислова електроніка", Кваліфікація "Інженер електронної техніки". Диплом Я № 287387 від 20.02.1978 р. Доцент (атестат ДЦ №039210 від 04.07.1991 р.). Кандидат технічних наук, 14 Електрична інженерія, 141 Електроенергетика, електротехніка та електромеханіка (05.09.12 - Напівпровідникові перетворювачі електроенергії), диплом ТН №094834 від 12.11.1986 р. Професор, атестат АП №001430 від 16.12.2019 р. Стаж науково-педагогічної роботи: 37 років. Відповідно до пункту

							30 Ліцензійних вимог п. 1-4, 6, 8, 10, 13, 15-16.
273557	Шматко Олександр Віталійович	Доцент 0,25 ст.			0	Технології програмування	Посада: доцент кафедри кібербезпеки та інформаційних технологій. Структурний підрозділ, у якому працює викладач: кафедра кібербезпеки та інформаційних технологій. Інформація про кваліфікацію викладача: Харківський авіаційний інститут ім. М.Є.Жуковського. 01.05.02 - математичне моделювання та обчислювальні методи, 121 – Інженерія програмного забезпечення, Комп'ютерне моделювання задач вигину, коливань та стійкості елементів тонкостінних конструкцій, 29.11.2001 № диплому. 013725 від 13 березня 2002 року. Доцент атестат №02ДЦ 011705 від 16.02. 2006 р. Стаж науково-педагогічної роботи: 13 років. Відповідно до пункту 30 Ліцензійних вимог п. 1-3, 11, 13-16
273533	Корольов Роман Володимирович	Доцент			0	Основи стеганографічного захисту інформації	Посада: доцент кафедри кібербезпеки та інформаційних технологій. Структурний підрозділ, у якому працює викладач: кафедра кібербезпеки та інформаційних технологій. Інформація про кваліфікацію викладача: 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., ДК № 054389. Кандидат технічних наук, 05.13.06 – інформаційні технології. Диплом ДК №054389. Стаж науково-педагогічної роботи: 24 роки. Відповідно до пункту 30 Ліцензійних вимог п. 1-3, 12, 17
294414	Гаврилова Алла Андріївна	Старший викладач 0,5 ст.			0	Основи національної безпеки	Посада: старший викладач кафедри кібербезпеки та інформаційних технологій. Структурний підрозділ, у якому працює викладач: кафедра кібербезпеки та інформаційних технологій. Інформація про кваліфікацію викладача: Харківський державний економічний університет, Економічна інформатика і автоматизовані системи управління, інженер-економіст. 07.06.1994, диплом ЛЕ

							№ 007629.Стаж науково-педагогічної роботи: 14 років. Відповідно до пункту 30 Ліцензійних вимог п. 1-3, 10, 13, 17
294414	Гаврилова Алла Андріївна	Старший викладач 0,5 ст.			0	Організаційне забезпечення захисту інформації	Посада: старший викладач кафедри кібербезпеки та інформаційних технологій. Структурний підрозділ, у якому працює викладач: кафедра кібербезпеки та інформаційних технологій. Інформація про кваліфікацію викладача: Харківський державний економічний університет, Економічна інформатика і автоматизовані системи управління, інженер-економіст. 07.06.1994, диплом ЛЕ № 007629.Стаж науково-педагогічної роботи: 14 років. Відповідно до пункту 30 Ліцензійних вимог п. 1-3, 10, 13, 17
274591	Мілевський Станіслав Валерійович	Доцент 0,25 ст.			0	Менеджмент інформаційної безпеки	Посада: доцент кафедри кібербезпеки та інформаційних технологій. Структурний підрозділ, у якому працює викладач: кафедра кібербезпеки та інформаційних технологій. Інформація про кваліфікацію викладача:Харківський державний економічний університет, Спеціальність "Економіка підприємства", Кваліфікація "Економіст". Диплом спеціаліста ХА №16790511 від 30.06.2001. Кандидат економічних наук, 051 Економіка (08.03.02 – економіко-математичне моделювання), диплом ДК №033701 від 13.04.2006 р. Доцент (Атестат 12ДЦ №023152 від 17.06.2010). Стаж науково-педагогічної роботи: 17 років. Відповідно до пункту 30 Ліцензійних вимог п. 1-3, 6, 10-11, 13,15
107556	Євсеєв Сергій Петрович	Завідувач кафедри			0	Інформаційна безпека держави	Посада: завідувач кафедри кібербезпеки та інформаційних технологій. Структурний підрозділ, у якому працює викладач: кафедра кібербезпеки та інформаційних технологій. Стаж науково-педагогічної роботи: 32 роки. Інформація про кваліфікацію викладача: 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 (21.05.01 – Інформаційна безпека держави). Диплом ДД № 007606 від 5.07.2018 р. Старший науковий співробітник зі спеціальності системи захисту інформації диплом АС № 007292 від 14.04. 2010 р. Доцент (диплом 12ДЦ № 034106 від 25.01.2013 р.). Відповідно до пункту 30 Ліцензійних вимог п. 1-3, 7-8, 10, 12-15, 17.
294325	Погасій Сергій Сергійович	Доцент			0	Основи побудови та захисту сучасних операційних систем	Посада: доцент кафедри кібербезпеки та інформаційних технологій. Структурний підрозділ, у якому працює викладач: кафедра кібербезпеки та інформаційних технологій. Інформація про кваліфікацію викладача: Харківський державний економічний університет, спеціальність «Фінанси і кредит», кваліфікація економіст. 25 червня 199 року, диплом ХА № 11869959. Кандидат економічних наук по 08.00.03 - економіка та управління національним, 28.04.2009 р. ДК №051003. Стаж науково-педагогічної роботи: 14 роки. Відповідно до пункту 30 Ліцензійних вимог п. 2, 3, 6, 10, 13, 15.
294325	Погасій Сергій Сергійович	Доцент			0	Основи побудови та функціонування мікропроцесорних систем	Посада: доцент кафедри кібербезпеки та інформаційних технологій. Структурний підрозділ, у якому працює викладач: кафедра кібербезпеки та інформаційних технологій. Інформація про кваліфікацію викладача: Харківський державний економічний університет, спеціальність «Фінанси і кредит», кваліфікація економіст. 25 червня 199 року, диплом ХА № 11869959. Кандидат економічних наук по 08.00.03 - економіка та управління національним, 28.04.2009 р. ДК №051003. Стаж науково-педагогічної роботи: 14 роки. Відповідно до пункту 30 Ліцензійних вимог

							п. 2, 3, 6, 10, 13, 15.
294325	Погасій Сергій Сергійович	Доцент			0	Безпека інтернет-речей	Посада: доцент кафедри кібербезпеки та інформаційних технологій. Структурний підрозділ, у якому працює викладач: кафедра кібербезпеки та інформаційних технологій. Інформація про кваліфікацію викладача: Харківський державний економічний університет, спеціальність «Фінанси і кредит», кваліфікація економіст. 25 червня 199 року, диплом ХА № 11869959. Кандидат економічних наук по 08.00.03 - економіка та управління національним, 28.04.2009 р. ДК №051003. Стаж науково-педагогічної роботи: 14 роки. Відповідно до пункту 30 Ліцензійних вимог п. 2, 3, 6, 10, 13, 15.

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

Програмні результати навчання ОП	**Методи навчання**	**Форми оцінювання**
Комплексні системи захисту інформації		
РН-21. Виявляти небезпечні сигнали технічних засобів; вимірювати параметри небезпечних сигналів для технічних каналів витоку інформації та визначати ефективність захисту від витоку інформації відповідно до вимог нормативних документів системи технічного захисту інформації інтерпретувати результати проведення спеціальних вимірювань з використанням технічних засобів, контролю характеристик ІТСМ відповідно до вимог нормативних документів системи технічного захисту інформації проводити атестацію (спираючись на облік та обстеження) режимних територій (зон), приміщень тощо в умовах додержання режиму секретності із фіксуванням результатів у відповідних документах виконувати дослідження, перевірку, аналіз та оцінювання об'єктів щодо їх відповідності вимогам нормативних документів та можливості їх використання для забезпечення інформації	Лекція, лабораторні заняття	Захист лабораторних завдань, контрольна робота, залік
РН-20. Виконувати налаштування інформаційних систем та комунікаційного обладнання; виконувати захист інформаційних систем від комп'ютерних вірусів; забезпечувати впровадження та дотримання політики кіберзахисту в ІТС, процедур, і правил; організовувати процес створення планів неперервності бізнесу; приймати участь у розробці планів відновлення, неперервності процесів організації для забезпечення здатності організації продовжувати виконувати необхідну діяльність в період порушення ІТ	Лекція, лабораторні заняття	Захист лабораторних завдань, контрольна робота, залік
РН-19. Здійснювати оцінку можливості проникнення в ІТ системи та мережі шляхом експлуатації наявних вразливостей; здійснювати оцінку захищеності ІТ систем та мереж; використовувати інструментальні засоби оцінки наявних вразливостей; оцінювати можливості та ефективність застосування, в тих чи інших умовах, інструментальних засобів оцінки вразливостей ІТ систем та мереж	Лекція, лабораторні заняття	Захист лабораторних завдань, контрольна робота, залік
РН-17. Виконувати декомпозицію ІТС; -	Лекція, лабораторні заняття	Захист лабораторних завдань,

розробляти структурні схеми з відображенням зв'язків між інформаційними процесами на віддалених системах; розробляти модель загроз, розробляти модель порушника; розробляти проекти ІТС базуючись на стандартизованих технологіях та протоколах передачі даних; вирішувати завдання захисту програм та даних ІТС програмно-апаратними засобами та давати оцінку якості прийнятих рішень; обирати основні методи та способи захисту інформації відповідно до вимог сучасних стандартів інформаційної безпеки щодо критеріїв безпеки інформаційних технологій, застосовуючи системний підхід та знання основ теорії інформаційної безпеки; проектувати та реалізувати комплексні систему захисту інформації АС організації (підприємства) відповідно до вимог нормативних документів системи технічного захисту інформації		контрольна робота, залік
РН-16. Здійснювати професійну діяльність на основі знань сучасних інформаційно-комунікаційних технологій; застосувати програмні засоби, навички роботи в телекомунікаційних та комп'ютерних мережах; використати спеціалізовані комп'ютерні програми в професійній діяльності. Обирати відповідну технологію програмування, виконати аналіз специфікації задач; виконувати аналіз програмного забезпечення з метою пошуку, ідентифікації, виявлення та усунення помилок програмування	Лекція, лабораторні заняття	Захист лабораторних завдань, контрольна робота, залік
Основи національної безпеки		
РН-24. Впроваджувати процеси виявлення, ідентифікації, аналізу та реагування на інциденти інформаційної/кібербезпеки; застосовувати національні та міжнародні регулюючі актів в сфері інформаційної безпеки для розслідування внутрішніх та зовнішніх інцендентів інформаційної безпеки;	Лекція, лабораторні заняття	Захист лабораторних завдань, контрольна робота, залік
РН-23. Приймати участь у розробці та впровадженні стратегії інформаційної безпеки та/або кібербезпеки відповідно до цілей і завдань організації; приймати участь у розробці та впровадженні політики, стандартів та процедур інформаційної безпеки та/ або кібербезпеки; на основі політики захисту організації розробляти нормативні документи для її реалізації;	Лекція, лабораторні заняття	Захист лабораторних завдань, контрольна робота, залік
РН-15. Діяти на основі законодавчої, нормативно-правової баз України та вимог відповідних стандартів, тому числі міжнародних; готувати пропозиції до нормативних актів щодо забезпечення інформаційної безпеки	Лекція, лабораторні заняття	Захист лабораторних завдань, контрольна робота, залік
Основи стеганографічного захисту інформації		
РН-18. Застосовувати теорії та методи захисту для забезпечення безпеки інформації в інформаційних і комунікаційних системах та мережах	Лекція, лабораторні заняття	Захист лабораторних завдань, контрольна робота, екзамен
РН-17. Виконувати декомпозицію ІТС; - розробляти структурні схеми з відображенням зв'язків між інформаційними процесами на віддалених системах; розробляти модель загроз, розробляти модель порушника; розробляти проекти ІТС базуючись на стандартизованих технологіях та протоколах передачі даних; вирішувати завдання захисту програм та даних ІТС програмно-апаратними засобами та давати оцінку якості прийнятих рішень; обирати основні методи та способи захисту інформації відповідно до вимог сучасних стандартів інформаційної безпеки щодо критеріїв безпеки інформаційних технологій, застосовуючи системний підхід та знання основ теорії інформаційної безпеки; проектувати та реалізувати комплексні систему захисту інформації АС організації (підприємства) відповідно до вимог нормативних документів системи	Лекція, лабораторні заняття	Захист лабораторних завдань, контрольна робота, екзамен

технічного захисту інформації		
Основи алгоритмізації		
РН-18. Застосовувати теорії та методи захисту для забезпечення безпеки інформації в інформаційних і комунікаційних системах та мережах	Лекція, лабораторні заняття	Захист лабораторних завдань, контрольна робота, екзамен
РН-17. Виконувати декомпозицію ІТС; - розробляти структурні схеми з відображенням зв'язків між інформаційними процесами на віддалених системах; розробляти модель загроз, розробляти модель порушника; розробляти проекти ІТС базуючись на стандартизованих технологіях та протоколах передачі даних; вирішувати завдання захисту програм та даних ІТС програмно-апаратними засобами та давати оцінку якості прийнятих рішень; обирати основні методи та способи захисту інформації відповідно до вимог сучасних стандартів інформаційної безпеки щодо критеріїв безпеки інформаційних технологій, застосовуючи системний підхід та знання основ теорії інформаційної безпеки; проектувати та реалізувати комплексні систему захисту інформації АС організації (підприємства) відповідно до вимог нормативних документів системи технічного захисту інформації	Лекція, лабораторні заняття	Захист лабораторних завдань, контрольна робота, екзамен
Безпека інтернет-речей		
РН-26. Виконувати конфігурування систем виявлення вторгнень та використовувати компоненти захисту для забезпечення необхідного рівня захищеності ІТС; використовувати інструментарій для моніторингу даних в ІТС; виконувати аналіз зловмисного програмного коду	Лекція, лабораторні заняття	Захист лабораторних завдань, контрольна робота, залік
РН-21. Виявляти небезпечні сигнали технічних засобів; вимірювати параметри небезпечних сигналів для технічних каналів витоку інформації та визначати ефективність захисту від витоку інформації відповідно до вимог нормативних документів системи технічного захисту інформації інтерпретувати результати проведення спеціальних вимірювань з використанням технічних засобів, контролю характеристик ІТСМ відповідно до вимог нормативних документів системи технічного захисту інформації проводити атестацію (спираючись на облік та обстеження) режимних територій (зон), приміщень тощо в умовах додержання режиму секретності із фіксуванням результатів у відповідних документах виконувати дослідження, перевірку, аналіз та оцінювання об'єктів щодо їх відповідності вимогам нормативних документів та можливості їх використання для забезпечення інформації	Лекція, лабораторні заняття	Захист лабораторних завдань, контрольна робота, залік
РН-20. Виконувати налаштування інформаційних систем та комунікаційного обладнання; виконувати захист інформаційних систем від комп'ютерних вірусів; забезпечувати впровадження та дотримання політики кіберзахисту в ІТС, процедур, і правил; організовувати процес створення планів неперервності бізнесу; приймати участь у розробці планів відновлення, неперервності процесів організації для забезпечення здатності організації продовжувати виконувати необхідну діяльність в період порушення ІТ	Лекція, лабораторні заняття	Захист лабораторних завдань, контрольна робота, залік
РН-18. Застосовувати теорії та методи захисту для забезпечення безпеки інформації в інформаційних і комунікаційних системах та мережах	Лекція, лабораторні заняття	Захист лабораторних завдань, контрольна робота, залік
Програмування		
РН-17. Виконувати декомпозицію ІТС; - розробляти структурні схеми з відображенням зв'язків між інформаційними процесами на віддалених системах;	Лекція, лабораторні заняття	Захист лабораторних завдань, контрольна робота, екзамен

розробляти модель загроз, розробляти модель порушника; розробляти проекти ІТС базуючись на стандартизованих технологіях та протоколах передачі даних; вирішувати завдання захисту програм та даних ІТС програмно-апаратними засобами та давати оцінку якості прийнятих рішень; обирати основні методи та способи захисту інформації відповідно до вимог сучасних стандартів інформаційної безпеки щодо критеріїв безпеки інформаційних технологій, застосовуючи системний підхід та знання основ теорії інформаційної безпеки; проектувати та реалізувати комплексні систему захисту інформації АС організації (підприємства) відповідно до вимог нормативних документів системи технічного захисту інформації		
РН-18. Застосовувати теорії та методи захисту для забезпечення безпеки інформації в інформаційних і комунікаційних системах та мережах	Лекція, лабораторні заняття	Захист лабораторних завдань, контрольна робота, екзамен
Організаційне забезпечення захисту інформації		
РН-27. Характеризувати стан інформаційної безпеки особистості, суспільства та держави; характеризувати основні форми інформаційного протиборства в умовах входження держави в інформаційне суспільство	Лекція, лабораторні заняття	Захист лабораторних завдань, контрольна робота, екзамен
РН-28. Використовувати теоретичні і практичні методи та методики досліджень у галузі інформаційної безпеки; застосовувати системний підхід та знання основ теорії інформаційної безпеки	Лекція, лабораторні заняття	Захист лабораторних завдань, контрольна робота, екзамен
РН-15. Діяти на основі законодавчої, нормативно-правової баз України та вимог відповідних стандартів, тому числі міжнародних; готувати пропозиції до нормативних актів щодо забезпечення інформаційної безпеки	Лекція, лабораторні заняття	Захист лабораторних завдань, контрольна робота, екзамен
Тренінг-курс “Безпека життєдіяльності”		
РН-4. Отримуватись вимог санітарно-гігієнічного режиму, охорони праці, техніки безпеки та протипожежної безпеки при здійсненні професійної діяльності	Лекція, практичні заняття, тренінгові завдання	Індивідуально компетентісно-орієнтовані завдання, захист завдання
РН-13. Демонструвати та пропагувати здоровий спосіб життя	Лекція, практичні заняття, тренінгові завдання	Індивідуально компетентісно-орієнтовані завдання, захист завдання
РН-8. Прогнозувати наслідки результатів діяльності людини з метою збереження навколишнього середовища	Лекція, практичні заняття, тренінгові завдання	Індивідуально компетентісно-орієнтовані завдання, захист завдання
Навчальна практика “Університетська освіта”		
РН-10. Вдосконалювати професійний та особистісний розвиток протягом усього життя;	Лекція, лабораторні заняття, практичні заняття	Захист індивідуальних завдань, лабораторних завдань
РН-1 Застосувати концептуальні знання з навчальних дисциплін загальної підготовки для засвоєння навчальних дисциплін професійної підготовки	Лекція, лабораторні заняття, практичні заняття	Захист індивідуальних завдань, лабораторних завдань
РН-13. Демонструвати та пропагувати здоровий спосіб життя	Лекція, лабораторні заняття, практичні заняття	Захист індивідуальних завдань, лабораторних завдань
Виробнича практика		
РН-21. Виявляти небезпечні сигнали технічних засобів; вимірювати параметри небезпечних сигналів для технічних каналів витоку інформації та визначати ефективність захисту від витоку інформації відповідно до вимог нормативних документів системи технічного захисту інформації інтерпретувати результати проведення спеціальних вимірювань з використанням технічних засобів, контролю характеристик ІТСМ відповідно до вимог нормативних документів системи технічного захисту інформації проводити атестацію (спираючись на облік та обстеження) режимних територій (зон), приміщень тощо в умовах додержання режиму секретності із фіксуванням результатів	Самостійна робота	Захист звіту з виробничої практики

у відповідних документах виконувати дослідження, перевірку, аналіз та оцінювання об’єктів щодо їх відповідності вимогам нормативних документів та можливості їх використання для забезпечення інформації		
РН-13. Демонструвати та пропагувати здоровий спосіб життя	Самостійна робота	Захист звіту з виробничої практики
РН-10. Вдосконалювати професійний та особистісний розвиток протягом усього життя;	Самостійна робота	Захист звіту з виробничої практики
РН-1 Застосувати концептуальні знання з навчальних дисциплін загальної підготовки для засвоєння навчальних дисциплін професійної підготовки	Самостійна робота	Захист звіту з виробничої практики
Переддипломна практика		
РН-11. 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;	Самостійна робота	Захист звіту
РН-14. Осмислювати критично основні теорії, принципи, методи і поняття у навчанні та професійній діяльності	Самостійна робота	Захист звіту
РН-24. Впроваджувати процеси виявлення, ідентифікації, аналізу та реагування на інциденти інформаційної/кібербезпеки; застосовувати національні та міжнародні регулюючі актів в сфері інформаційної безпеки для розслідування внутрішніх та зовнішніх інцендентів інформаційної безпеки;	Самостійна робота	Захист звіту
РН-25. Розробляти та оцінювати моделі і політику безпеки на основі використання сучасних принципів, способів та методів теорії захищених систем застосовувати політики, що базуються риск адаптивному контролі доступу здійснювати аналіз ризиків функціонування ІКС: визначати послідовність аналізу, формувати моделі порушника та загроз, використовувати сучасні методи та методики аналізу ризиків, оцінювання та управління ризиками	Самостійна робота	Захист звіту
РН-28. Використовувати теоретичні і практичні методи та методики досліджень у галузі інформаційної безпеки; застосовувати системний підхід та знання основ теорії інформаційної безпеки.	Самостійна робота	Захист звіту
РН-27. Характеризувати стан інформаційної безпеки особистості, суспільства та держави; характеризувати основні форми інформаційного протиборства в умовах входження держави в інформаційне суспільство	Самостійна робота	Захист звіту
РН-23. Приймати участь у розробці та впровадженні стратегії інформаційної безпеки та/або кібербезпеки відповідно до цілей і завдань організації; приймати участь у розробці та впровадженні політики, стандартів та процедур інформаційної безпеки та/ або кібербезпеки; на основі політики захисту організації розробляти нормативні документи для її реалізації;	Самостійна робота	Захист звіту
РН-26. Виконувати конфігурування систем виявлення вторгнень та використовувати компоненти захисту для забезпечення необхідного рівня захищеності ІТС; використовувати інструментарій для моніторингу даних в ІТС; виконувати аналіз зловмисного програмного коду	Самостійна робота	Захист звіту
Дипломний проект		
РН-28. Використовувати теоретичні і практичні методи та методики досліджень у галузі інформаційної безпеки; застосовувати системний підхід та знання основ теорії інформаційної	Самостійна робота	Захист дипломного проекту (дипломної роботи)

безпеки.		
РН-27. Характеризувати стан інформаційної безпеки особистості, суспільства та держави; характеризувати основні форми інформаційного протиборства в умовах входження держави в інформаційне суспільство	Самостійна робота	Захист дипломного проекту (дипломної роботи)
РН-26. Виконувати конфігурування систем виявлення вторгнень та використовувати компоненти захисту для забезпечення необхідного рівня захищеності ІТС; використовувати інструментарій для моніторингу даних в ІТС; виконувати аналіз зловмисного програмного коду	Самостійна робота	Захист дипломного проекту (дипломної роботи)
РН-25. Розробляти та оцінювати моделі і політику безпеки на основі використання сучасних принципів, способів та методів теорії захищених систем застосовувати політики, що базуються риск адаптивному контролі доступу здійснювати аналіз ризиків функціонування ІКС: визначати послідовність аналізу, формувати моделі порушника та загроз, використовувати сучасні методи та методики аналізу ризиків, оцінювання та управління ризиками	Самостійна робота	Захист дипломного проекту (дипломної роботи)
РН-24. Впроваджувати процеси виявлення, ідентифікації, аналізу та реагування на інциденти інформаційної/кібербезпеки; застосовувати національні та міжнародні регулюючі актів в сфері інформаційної безпеки для розслідування внутрішніх та зовнішніх інцендентів інформаційної безпеки;	Самостійна робота	Захист дипломного проекту (дипломної роботи)
РН-23. Приймати участь у розробці та впровадженні стратегії інформаційної безпеки та/або кібербезпеки відповідно до цілей і завдань організації; приймати участь у розробці та впровадженні політики, стандартів та процедур інформаційної безпеки та/ або кібербезпеки; на основі політики захисту організації розробляти нормативні документи для її реалізації;	Самостійна робота	Захист дипломного проекту (дипломної роботи)
РН-14. Осмислювати критично основні теорії, принципи, методи і поняття у навчанні та професійній діяльності	Самостійна робота	Захист дипломного проекту (дипломної роботи)
РН-11. 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;	Самостійна робота	Захист дипломного проекту (дипломної роботи)
Комплексний курсовий проект		
РН-26. Виконувати конфігурування систем виявлення вторгнень та використовувати компоненти захисту для забезпечення необхідного рівня захищеності ІТС. використовувати інструментарій для моніторингу даних в ІТС; виконувати аналіз зловмисного програмного коду	Самостійна робота	Захист курсового проекту
РН-24. Впроваджувати процеси виявлення, ідентифікації, аналізу та реагування на інциденти інформаційної/кібербезпеки; застосовувати національні та міжнародні регулюючі актів в сфері інформаційної безпеки для розслідування внутрішніх та зовнішніх інцендентів інформаційної безпеки;	Самостійна робота	Захист курсового проекту
РН-21. Виявляти небезпечні сигнали технічних засобів; вимірювати параметри небезпечних сигналів для технічних каналів витоку інформації та визначати ефективність захисту від витоку інформації відповідно до вимог нормативних документів системи технічного захисту інформації інтерпретувати результати проведення спеціальних вимірювань з використанням технічних засобів, контролю характеристик ІТСМ відповідно до вимог нормативних документів системи технічного захисту інформації проводити атестацію	Самостійна робота	Захист курсового проекту

(спираючись на облік та обстеження) режимних територій (зон), приміщень тощо в умовах додержання режиму секретності із фіксуванням результатів у відповідних документах виконувати дослідження, перевірку, аналіз та оцінювання об’єктів щодо їх відповідності вимогам нормативних документів та можливості їх використання для забезпечення інформації		
РН-19. Здійснювати оцінку можливості проникнення в ІТ системи та мережі шляхом експлуатації наявних вразливостей; здійснювати оцінку захищеності ІТ систем та мереж; використовувати інструментальні засоби оцінки наявних вразливостей; оцінювати можливості та ефективність застосування, в тих чи інших умовах, інструментальних засобів оцінки вразливостей ІТ систем та мереж	Самостійна робота	Захист курсового проекту
РН-6. Використати результати самостійного пошуку, аналізу та синтезу інформації з різних джерел для ефективного рішення спеціалізованих задач професійної діяльності	Самостійна робота	Захист курсового проекту
Курсовий проект: Введення в мережі		
РН-20. Виконувати налаштування інформаційних систем та комунікаційного обладнання; виконувати захист інформаційних систем від комп’ютерних вірусів; забезпечувати впровадження та дотримання політики кіберзахисту в ІТС, процедур, і правил; організовувати процес створення планів неперервності бізнесу; приймати участь у розробці планів відновлення, неперервності процесів організації для забезпечення здатності організації продовжувати виконувати необхідну діяльність в період порушення ІТ;	Самостійна робота	Захист курсового проекту
РН-18. Застосовувати теорії та методи захисту для забезпечення безпеки інформації в інформаційних і комунікаційних системах та мережах	Самостійна робота	Захист курсового проекту
РН-17. Виконувати декомпозицію ІТС; - розробляти структурні схеми з відображенням зв’язків між інформаційними процесами на віддалених системах; розробляти модель загроз, розробляти модель порушника; розробляти проекти ІТС базуючись на стандартизованих технологіях та протоколах передачі даних; вирішувати завдання захисту програм та даних ІТС програмно-апаратними засобами та давати оцінку якості прийнятих рішень; обирати основні методи та способи захисту інформації відповідно до вимог сучасних стандартів інформаційної безпеки щодо критеріїв безпеки інформаційних технологій, застосовуючи системний підхід та знання основ теорії інформаційної безпеки; проектувати та реалізувати комплексні систему захисту інформації АС організації (підприємства) відповідно до вимог нормативних документів системи технічного захисту інформації	Самостійна робота	Захист курсового проекту
РН-16. Здійснювати професійну діяльність на основі знань сучасних інформаційно-комунікаційних технологій; застосувати програмні засоби, навички роботи в телекомунікаційних та комп’ютерних мережах; використати спеціалізовані комп’ютерні програми в професійній діяльності. Обирати відповідну технологію програмування, виконати аналіз специфікації задач; виконувати аналіз програмного забезпечення з метою пошуку, ідентифікації, виявлення та усунення помилок програмування;	Самостійна робота	Захист курсового проекту
РН-6. Використати результати самостійного пошуку, аналізу та синтезу інформації з різних джерел для ефективного рішення спеціалізованих задач професійної діяльності	Самостійна робота	Захист курсового проекту
Тренінг-курс “Основи охорони праці”		

РН-13. Демонструвати та пропагувати здоровий спосіб життя	Лекція, практичні заняття, тренінгові завдання	Індивідуально компетентісно-орієнтовані завдання, захист завдання
РН-8. Прогнозувати наслідки результатів діяльності людини з метою збереження навколишнього середовища	Лекція, практичні заняття, тренінгові завдання	Індивідуально компетентісно-орієнтовані завдання, захист завдання
РН-4. Отримуватись вимог санітарно-гігієнічного режиму, охорони праці, техніки безпеки та протипожежної безпеки при здійсненні професійної діяльності;	Лекція, практичні заняття, тренінгові завдання	Індивідуально компетентісно-орієнтовані завдання, захист завдання
Основи побудови та захисту сучасних операційних систем		
РН-12. Адаптуватися в умовах частої зміни технологій професійної діяльності, прогнозувати кінцевий результат	Лекція, лабораторні заняття	Захист лабораторних завдань, контрольна робота, залік
РН-16. Здійснювати професійну діяльність на основі знань сучасних інформаційно-комунікаційних технологій	Лекція, лабораторні заняття	Захист лабораторних завдань, контрольна робота, залік
РН-17. Виконувати декомпозицію ІТС; - розробляти структурні схеми з відображенням зв'язків між інформаційними процесами на віддалених системах; розробляти модель загроз, розробляти модель порушника; розробляти проекти ІТС базуючись на стандартизованих технологіях та протоколах передачі даних; вирішувати завдання захисту програм та даних ІТС програмно-апаратними засобами та давати оцінку якості прийнятих рішень обирати основні методи та способи захисту інформації відповідно до вимог сучасних стандартів інформаційної безпеки щодо критеріїв безпеки інформаційних технологій, застосовуючи системний підхід та знання основ теорії інформаційної безпеки; проектувати та реалізувати комплексні систему захисту інформації АС організації (підприємства) відповідно до вимог нормативних документів системи технічного захисту інформації	Лекція, лабораторні заняття	Захист лабораторних завдань, контрольна робота, залік
Організація та інформаційне забезпечення управлінської діяльності		
РН-20. Виконувати налаштування інформаційних систем та комунікаційного обладнання; виконувати захист інформаційних систем від комп'ютерних вірусів; забезпечувати впровадження та дотримання політики кіберзахисту в ІТС, процедур, і правил; організовувати процес створення планів неперервності бізнесу; приймати участь у розробці планів відновлення, неперервності процесів організації для забезпечення здатності організації продовжувати виконувати необхідну діяльність в період порушення ІТ	Лекція, лабораторні заняття	Захист лабораторних завдань, контрольна робота, екзамен
РН-25. Розробляти та оцінювати моделі і політику безпеки на основі використання сучасних принципів, способів та методів теорії захищених систем застосовувати політики, що базуються риск адаптивному контролі доступу здійснювати аналіз ризиків функціонування ІКС: визначати послідовність аналізу, формувати моделі порушника та загроз, використовувати сучасні методи та методики аналізу ризиків, оцінювання та управління ризиками	Лекція, лабораторні заняття	Захист лабораторних завдань, контрольна робота, екзамен
РН-17. Виконувати декомпозицію ІТС; - розробляти структурні схеми з відображенням зв'язків між інформаційними процесами на віддалених системах; розробляти модель загроз, розробляти модель порушника; розробляти проекти ІТС базуючись на стандартизованих технологіях та протоколах передачі даних; вирішувати завдання захисту програм та даних ІТС програмно-апаратними засобами та давати оцінку якості прийнятих рішень; обирати основні методи та способи захисту інформації відповідно до вимог сучасних стандартів інформаційної безпеки щодо критеріїв безпеки	Лекція, лабораторні заняття	Захист лабораторних завдань, контрольна робота, екзамен

інформаційних технологій, застосовуючи системний підхід та знання основ теорії інформаційної безпеки; проектувати та реалізувати комплексні систему захисту інформації АС організації (підприємства) відповідно до вимог нормативних документів системи технічного захисту інформації		
Безпека в інформаційно-комунікаційних системах		
РН-16. Здійснювати професійну діяльність на основі знань сучасних інформаційно-комунікаційних технологій; застосувати програмні засоби, навички роботи в телекомунікаційних та комп'ютерних мережах; використати спеціалізовані комп'ютерні програми в професійній діяльності. Обирати відповідну технологію програмування, виконати аналіз специфікації задач; виконувати аналіз програмного забезпечення з метою пошуку, ідентифікації, виявлення та усунення помилок програмування	Лекція, лабораторні заняття	Захист лабораторних завдань, контрольна робота, екзамен
РН-17. Виконувати декомпозицію ІТС; - розробляти структурні схеми з відображенням зв'язків між інформаційними процесами на віддалених системах; розробляти модель загроз, розробляти модель порушника; розробляти проекти ІТС базуючись на стандартизованих технологіях та протоколах передачі даних; вирішувати завдання захисту програм та даних ІТС програмно-апаратними засобами та давати оцінку якості прийнятих рішень; обирати основні методи та способи захисту інформації відповідно до вимог сучасних стандартів інформаційної безпеки щодо критеріїв безпеки інформаційних технологій, застосовуючи системний підхід та знання основ теорії інформаційної безпеки; проектувати та реалізувати комплексні систему захисту інформації АС організації (підприємства) відповідно до вимог нормативних документів системи технічного захисту інформації	Лекція, лабораторні заняття	Захист лабораторних завдань, контрольна робота, екзамен
РН-18. Застосовувати теорії та методи захисту для забезпечення безпеки інформації в інформаційних і комунікаційних системах та мережах;	Лекція, лабораторні заняття	Захист лабораторних завдань, контрольна робота, екзамен
РН-20. Виконувати налаштування інформаційних систем та комунікаційного обладнання; виконувати захист інформаційних систем від комп'ютерних вірусів; забезпечувати впровадження та дотримання політики кіберзахисту в ІТС, процедур, і правил; організовувати процес створення планів неперервності бізнесу; приймати участь у розробці планів відновлення, неперервності процесів організації для забезпечення здатності організації продовжувати виконувати необхідну діяльність в період порушення ІТ	Лекція, лабораторні заняття	Захист лабораторних завдань, контрольна робота, екзамен
РН-21. Виявляти небезпечні сигнали технічних засобів; вимірювати параметри небезпечних сигналів для технічних каналів витоку інформації та визначати ефективність захисту від витоку інформації відповідно до вимог нормативних документів системи технічного захисту інформації інтерпретувати результати проведення спеціальних вимірювань з використанням технічних засобів, контролю характеристик ІТСМ відповідно до вимог нормативних документів системи технічного захисту інформації проводити атестацію (спираючись на облік та обстеження) режимних територій (зон), приміщень тощо в умовах додержання режиму секретності із фіксуванням результатів у відповідних документах виконувати дослідження, перевірку, аналіз та оцінювання об'єктів щодо їх відповідності вимогам нормативних документів та можливості їх використання для забезпечення інформації	Лекція, лабораторні заняття	Захист лабораторних завдань, контрольна робота, екзамен

Українська мова (за професійним спрямуванням)		
РН-2. Проектувати майбутню професійну діяльність з урахуванням її значущості для громадянина та держави, а також напрямків розвитку інформаційної та кібербезпеки	Лекція, практичні заняття	захист індивідуальних завдань, тестування, письмові контрольні роботи, участь у конференціях, олімпіадах, конкурсах, екзамен
РН-7. Дотримуватись норм міжособистісного спілкування у професійній взаємодії	Лекція, практичні заняття	захист індивідуальних завдань, тестування, письмові контрольні роботи, участь у конференціях, олімпіадах, конкурсах
РН-1. Застосувати концептуальні знання з навчальних дисциплін загальної підготовки для засвоєння навчальних дисциплін професійної підготовки	Лекція, практичні заняття	захист індивідуальних завдань, тестування, письмові контрольні роботи, участь у конференціях, олімпіадах, конкурсах, екзамен
Іноземна мова (за професійним спрямуванням)		
РН-1. Застосувати концептуальні знання з навчальних дисциплін загальної підготовки для засвоєння навчальних дисциплін професійної підготовки	Практичні заняття	Захист практичних завдань, презентація, контрольні роботи, залік
РН-2. Проектувати майбутню професійну діяльність з урахуванням її значущості для громадянина та держави, а також напрямків розвитку інформаційної та кібербезпеки	Практичні заняття	Захист практичних завдань, презентація, контрольні роботи, екзамен
РН-3. Застосувати знання державної та однієї з іноземних мов з метою забезпечення ефективності професійної комунікації	Практичні заняття	Захист практичних завдань, презентація, контрольні роботи, залік, екзамен
РН-7. Дотримуватись норм міжособистісного спілкування у професійній взаємодії	Практичні заняття	Захист практичних завдань, презентація, контрольні роботи, залік, екзамен
Соціальна та економічна історія України		
РН-1. Застосувати концептуальні знання з навчальних дисциплін загальної підготовки для засвоєння навчальних дисциплін професійної підготовки	Лекція, практичні заняття, семінарські заняття	Домашні завдання за темами, дискусія, есе-доповідь, письмова контрольна робота, екзамен
РН-2. Проектувати майбутню професійну діяльність з урахуванням її значущості для громадянина та держави, а також напрямків розвитку інформаційної та кібербезпеки	Лекція, практичні заняття, семінарські заняття	Домашні завдання за темами, дискусія, есе-доповідь, письмова контрольна робота
РН-3. Застосувати знання державної та однієї з іноземних мов з метою забезпечення ефективності професійної комунікації	Лекція, практичні заняття, семінарські заняття	Домашні завдання за темами, дискусія, есе-доповідь, письмова контрольна робота, екзамен
РН-7. Дотримуватись норм міжособистісного спілкування у професійній взаємодії	Лекція, практичні заняття, семінарські заняття	Домашні завдання за темами, дискусія, есе-доповідь, письмова контрольна робота, екзамен
РН-9. Використовувати історичну спадщину та культурні традиції свого народу для професійного зростання, саморозвитку, самовдосконалення	Лекція, практичні заняття, семінарські заняття	Домашні завдання за темами, дискусія, есе-доповідь, письмова контрольна робота
Філософія		
РН-10. Вдосконалювати професійний та особистісний розвиток протягом усього життя	Лекція, семінарські заняття	Доповідь, захист семінарських завдань, експрес-опитування, есе, письмова контрольна робота
РН-1. Застосувати концептуальні знання з навчальних дисциплін загальної підготовки для засвоєння навчальних дисциплін професійної підготовки	Лекція, семінарські заняття	Доповідь, захист семінарських завдань, експрес-опитування, есе, письмова контрольна робота, екзамен
РН-2. Проектувати майбутню професійну діяльність з урахуванням її значущості для громадянина та держави, а також напрямків розвитку інформаційної та кібербезпеки	Лекція, семінарські заняття	Доповідь, захист семінарських завдань, експрес-опитування, есе, письмова контрольна робота, екзамен
РН-3. Застосувати знання державної та однієї з іноземних мов з метою забезпечення ефективності професійної комунікації	Лекція, семінарські заняття	Доповідь, захист семінарських завдань, експрес-опитування, есе, письмова контрольна робота, екзамен
РН-7. Дотримуватись норм міжособистісного спілкування у професійній взаємодії	Лекція, семінарські заняття	Доповідь, захист семінарських завдань, експрес-опитування, есе, письмова контрольна робота, екзамен
Математичні основи криптології		
РН-11. Аналізувати, аргументувати, приймати рішення при розв’язанні складних спеціалізованих задач та	Лекція, лабораторні заняття	Захист лабораторних завдань, контрольна робота, залік

практичних проблем у професійній діяльності, які характеризуються комплексністю та неповною визначеністю умов, відповідати за прийняті рішення		
РН-18. Застосовувати теорії та методи захисту для забезпечення безпеки інформації в інформаційних і комунікаційних системах та мережах	Лекція, лабораторні заняття	Захист лабораторних завдань, контрольна робота, залік
РН-14. Осмислювати критично основні теорії, принципи, методи і поняття у навчанні та професійній діяльності	Лекція, лабораторні заняття	Захист лабораторних завдань, контрольна робота, залік
Вища математика		
РН-1. Застосувати концептуальні знання з навчальних дисциплін загальної підготовки для засвоєння навчальних дисциплін професійної підготовки	Лекція, лабораторні заняття, практичні заняття	Захист практичних, лабораторних та домашніх завдань, письмова контрольна робота, самостійна контрольна робота, колоквіум, компетентісно-орієнтовані завдання, самостійна творча робота, залік
РН-5. Організувати власну професійну діяльність, обирати оптимальні методи та способи розв’язування складних спеціалізованих задач та практичних проблему професійній діяльності, оцінювати їхню ефективність	Лекція, лабораторні заняття, практичні заняття	Захист практичних, лабораторних та домашніх завдань, письмова контрольна робота, самостійна контрольна робота, колоквіум, компетентісно-орієнтовані завдання, самостійна творча робота, залік, екзамен
РН-11. 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	Лекція, лабораторні заняття, практичні заняття	Захист практичних, лабораторних та домашніх завдань, письмова контрольна робота, самостійна контрольна робота, колоквіум, компетентісно-орієнтовані завдання, самостійна творча робота, залік, екзамен
Інформаційна безпека держави		
РН-15. Діяти на основі законодавчої, нормативно-правової баз України та вимог відповідних стандартів, тому числі міжнародних; готувати пропозиції до нормативних актів щодо забезпечення інформаційної безпеки	Лекція, лабораторні заняття	Захист лабораторних завдань, контрольна робота, залік
РН-19. Здійснювати оцінку можливості проникнення в ІТ системи та мережі шляхом експлуатації наявних вразливостей; здійснювати оцінку захищеності ІТ систем та мереж; використовувати інструментальні засоби оцінки наявних вразливостей; оцінювати можливості та ефективність застосування, в тих чи інших умовах, інструментальних засобів оцінки вразливостей ІТ систем та мереж	Лекція, лабораторні заняття	Захист лабораторних завдань, контрольна робота, залік
РН-23. Приймати участь у розробці та впровадженні стратегії інформаційної безпеки та/або кібербезпеки відповідно до цілей і завдань організації; приймати участь у розробці та впровадженні політики, стандартів та процедур інформаційної безпеки та/ або кібербезпеки; на основі політики захисту організації розробляти нормативні документи для її реалізації	Лекція, лабораторні заняття	Захист лабораторних завдань, контрольна робота, залік
РН-25. Розробляти та оцінювати моделі і політику безпеки на основі використання сучасних принципів, способів та методів теорії захищених систем застосовувати політики, що базуються риск адаптивному контролі доступу здійснювати аналіз ризиків функціонування ІКС: визначати послідовність аналізу, формувати моделі порушника та загроз, використовувати сучасні методи та методики аналізу ризиків, оцінювання та управління ризиками	Лекція, лабораторні заняття	Захист лабораторних завдань, контрольна робота, залік
Теоретичні основи криптографії		
РН-14. Осмислювати критично основні теорії, принципи, методи і поняття у навчанні та професійній діяльності	Лекція, лабораторні заняття	Захист лабораторних завдань, контрольна робота, екзамен
РН-18. Застосовувати теорії та методи захисту для забезпечення безпеки інформації в інформаційних і комунікаційних системах та мережах	Лекція, лабораторні заняття	Захист лабораторних завдань, контрольна робота, екзамен
РН-11. Аналізувати, аргументувати, приймати рішення при розв’язанні складних спеціалізованих задач та практичних проблем у професійній	Лекція, лабораторні заняття	Захист лабораторних завдань, контрольна робота, екзамен

діяльності, які характеризуються комплексністю та неповною визначеністю умов, відповідати за прийняті рішення		
Основи побудови та функціонування мікропроцесорних систем		
РН-12. Адаптуватися в умовах частої зміни технологій професійної діяльності, прогнозувати кінцевий результат	Лекція, лабораторні заняття	Захист лабораторних завдань, контрольна робота, залік
РН-16. Здійснювати професійну діяльність на основі знань сучасних інформаційно-комунікаційних технологій; застосувати програмні засоби, навички роботи в телекомунікаційних та комп'ютерних мережах; використати спеціалізовані комп'ютерні програми в професійній діяльності. Обирати відповідну технологію програмування, виконати аналіз специфікації задач; виконувати аналіз програмного забезпечення з метою пошуку, ідентифікації, виявлення та усунення помилок програмування	Лекція, лабораторні заняття	Захист лабораторних завдань, контрольна робота, залік
РН-19. Здійснювати оцінку можливості проникнення в ІТ системи та мережі шляхом експлуатації наявних вразливостей; здійснювати оцінку захищеності ІТ систем та мереж; використовувати інструментальні засоби оцінки наявних вразливостей; оцінювати можливості та ефективність застосування, в тих чи інших умовах, інструментальних засобів оцінки вразливостей ІТ систем та мереж	Лекція, лабораторні заняття	Захист лабораторних завдань, контрольна робота, залік
Основи математичного моделювання		
РН-14. Осмислювати критично основні теорії, принципи, методи і поняття у навчанні та професійній діяльності	Лекція, лабораторні заняття	Захист лабораторних завдань, контрольна робота, залік
РН-25. Розробляти та оцінювати моделі і політику безпеки на основі використання сучасних принципів, способів та методів теорії захищених систем застосовувати політики, що базуються риск адаптивному контролі доступу здійснювати аналіз ризиків функціонування ІКС: визначати послідовність аналізу, формувати моделі порушника та загроз, використовувати сучасні методи та методики аналізу ризиків, оцінювання та управління ризиками	Лекція, лабораторні заняття	Захист лабораторних завдань, контрольна робота, залік
РН-28. Використовувати теоретичні і практичні методи та методики досліджень у галузі інформаційної безпеки; застосовувати системний підхід та знання основ теорії інформаційної безпеки	Лекція, лабораторні заняття	Захист лабораторних завдань, контрольна робота, залік
Технології програмування		
РН-16. Здійснювати професійну діяльність на основі знань сучасних інформаційно-комунікаційних технологій; застосувати програмні засоби, навички роботи в телекомунікаційних та комп'ютерних мережах; використати спеціалізовані комп'ютерні програми в професійній діяльності. Обирати відповідну технологію програмування, виконати аналіз специфікації задач; виконувати аналіз програмного забезпечення з метою пошуку, ідентифікації, виявлення та усунення помилок програмування	Лекція, лабораторні заняття	Захист лабораторних завдань, контрольна робота, залік, екзамен
РН-17. Виконувати декомпозицію ІТС; - розробляти структурні схеми з відображенням зв'язків між інформаційними процесами на віддалених системах; розробляти модель загроз, розробляти модель порушника; розробляти проекти ІТС базуючись на стандартизованих технологіях та протоколах передачі даних; вирішувати завдання захисту програм та даних ІТС програмно-апаратними засобами та давати оцінку якості прийнятих рішень; обирати основні методи та способи захисту інформації відповідно до вимог сучасних стандартів інформаційної	Лекція, лабораторні заняття	Захист лабораторних завдань, контрольна робота, залік, екзамен

безпеки щодо критеріїв безпеки інформаційних технологій, застосовуючи системний підхід та знання основ теорії інформаційної безпеки; проектувати та реалізувати комплексні систему захисту інформації АС організації (підприємства) відповідно до вимог нормативних документів системи технічного захисту інформації		
РН-11. 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	Лекція, лабораторні заняття	Захист лабораторних завдань, контрольна робота, залік
Основи криптографічного захисту		
РН-11. 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	Лекція, лабораторні заняття	Захист лабораторних завдань, контрольна робота, залік
РН-14. Осмислювати критично основні теорії, принципи, методи і поняття у навчанні та професійній діяльності	Лекція, лабораторні заняття	Захист лабораторних завдань, контрольна робота, залік
РН-16. Здійснювати професійну діяльність на основі знань сучасних інформаційно-комунікаційних технологій; застосувати програмні засоби, навички роботи в телекомунікаційних та комп'ютерних мережах; використати спеціалізовані комп'ютерні програми в професійній діяльності. Обирати відповідну технологію програмування, виконати аналіз специфікації задач; виконувати аналіз програмного забезпечення з метою пошуку, ідентифікації, виявлення та усунення помилок програмування	Лекція, лабораторні заняття	Захист лабораторних завдань, контрольна робота, залік
РН-17. Виконувати декомпозицію ІТС; - розробляти структурні схеми з відображенням зв'язків між інформаційними процесами на віддалених системах; розробляти модель загроз, розробляти модель порушника; розробляти проекти ІТС базуючись на стандартизованих технологіях та протоколах передачі даних; вирішувати завдання захисту програм та даних ІТС програмно-апаратними засобами та давати оцінку якості прийнятих рішень; обирати основні методи та способи захисту інформації відповідно до вимог сучасних стандартів інформаційної безпеки щодо критеріїв безпеки інформаційних технологій, застосовуючи системний підхід та знання основ теорії інформаційної безпеки; проектувати та реалізувати комплексні систему захисту інформації АС організації (підприємства) відповідно до вимог нормативних документів системи технічного захисту інформації	Лекція, лабораторні заняття	Захист лабораторних завдань, контрольна робота, залік
РН-18. Застосовувати теорії та методи захисту для забезпечення безпеки інформації в інформаційних і комунікаційних системах та мережах	Лекція, лабораторні заняття	Захист лабораторних завдань, контрольна робота, залік
РН-20. Виконувати налаштування інформаційних систем та комунікаційного обладнання; виконувати захист інформаційних систем від комп'ютерних вірусів; забезпечувати впровадження та дотримання політики кіберзахисту в ІТС, процедур, і правил; організовувати процес створення планів неперервності бізнесу; приймати участь у розробці планів відновлення, неперервності процесів організації для забезпечення здатності організації продовжувати виконувати необхідну діяльність в період порушення ІТ	Лекція, лабораторні заняття	Захист лабораторних завдань, контрольна робота, залік
Основи технічного захисту інформації		
РН-16. Здійснювати професійну діяльність на основі знань сучасних	Лекція, лабораторні заняття	Захист лабораторних завдань, контрольна робота, екзамен

інформаційно-комунікаційних технологій; застосувати програмні засоби, навички роботи в телекомунікаційних та комп'ютерних мережах; використати спеціалізовані комп'ютерні програми в професійній діяльності. Обирати відповідну технологію програмування, виконати аналіз специфікації задач; виконувати аналіз програмного забезпечення з метою пошуку, ідентифікації, виявлення та усунення помилок програмування		
РН-17. Виконувати декомпозицію ІТС; - розробляти структурні схеми з відображенням зв'язків між інформаційними процесами на віддалених системах; розробляти модель загроз, розробляти модель порушника; розробляти проекти ІТС базуючись на стандартизованих технологіях та протоколах передачі даних; вирішувати завдання захисту програм та даних ІТС програмно-апаратними засобами та давати оцінку якості прийнятих рішень; обирати основні методи та способи захисту інформації відповідно до вимог сучасних стандартів інформаційної безпеки щодо критеріїв безпеки інформаційних технологій, застосовуючи системний підхід та знання основ теорії інформаційної безпеки; проектувати та реалізувати комплексні систему захисту інформації АС організації (підприємства) відповідно до вимог нормативних документів системи технічного захисту інформації	Лекція, лабораторні заняття	Захист лабораторних завдань, контрольна робота, екзамен
РН-19. Здійснювати оцінку можливості проникнення в ІТ системи та мережі шляхом експлуатації наявних вразливостей; здійснювати оцінку захищеності ІТ систем та мереж; використовувати інструментальні засоби оцінки наявних вразливостей; оцінювати можливості та ефективність застосування, в тих чи інших умовах, інструментальних засобів оцінки вразливостей ІТ систем та мереж;	Лекція, лабораторні заняття	Захист лабораторних завдань, контрольна робота, екзамен
РН-20. Виконувати налаштування інформаційних систем та комунікаційного обладнання; виконувати захист інформаційних систем від комп'ютерних вірусів; забезпечувати впровадження та дотримання політики кіберзахисту в ІТС, процедур, і правил; організовувати процес створення планів неперервності бізнесу; приймати участь у розробці планів відновлення, неперервності процесів організації для забезпечення здатності організації продовжувати виконувати необхідну діяльність в період порушення ІТ	Лекція, лабораторні заняття	Захист лабораторних завдань, контрольна робота, екзамен
РН-21. Виявляти небезпечні сигнали технічних засобів; вимірювати параметри небезпечних сигналів для технічних каналів витоку інформації та визначати ефективність захисту від витоку інформації відповідно до вимог нормативних документів системи технічного захисту інформації інтерпретувати результати проведення спеціальних вимірювань з використанням технічних засобів, контролю характеристик ІТСМ відповідно до вимог нормативних документів системи технічного захисту інформації проводити атестацію (спираючись на облік та обстеження) режимних територій (зон), приміщень тощо в умовах додержання режиму секретності із фіксуванням результатів у відповідних документах виконувати дослідження, перевірку, аналіз та оцінювання об'єктів щодо їх відповідності вимогам нормативних документів та можливості їх використання для забезпечення інформації	Лекція, лабораторні заняття	Захист лабораторних завдань, контрольна робота, екзамен
Менеджмент інформаційної безпеки		
РН-25. Розробляти та оцінювати моделі і політику безпеки на основі використання сучасних принципів, способів та методів теорії захищених	Лекція, лабораторні заняття	Захист лабораторних завдань, контрольна робота, залік

систем застосовувати політики, що базуються риск адаптивному контролі доступу здійснювати аналіз ризиків функціонування ІКС: визначати послідовність аналізу, формувати моделі порушника та загроз, використовувати сучасні методи та методики аналізу ризиків, оцінювання та управління ризиками		
РН-24. Впроваджувати процеси виявлення, ідентифікації, аналізу та реагування на інциденти інформаційної/кібербезпеки; застосовувати національні та міжнародні регулюючі актів в сфері інформаційної безпеки для розслідування внутрішніх та зовнішніх інцендентів інформаційної безпеки;	Лекція, лабораторні заняття	Захист лабораторних завдань, контрольна робота, залік
РН-22. Обґрунтування інвестицій в інформаційну безпеку; аналізувати економічну ефективність заходів інформаційної безпеки; визначати особливості організаційної структури та організації робіт; використовувати міжнародні та національні специфічні для сектора економіки вимоги та кращі практики	Лекція, лабораторні заняття	Захист лабораторних завдань, контрольна робота, залік
РН-19. Здійснювати оцінку можливості проникнення в ІТ системи та мережі шляхом експлуатації наявних вразливостей; здійснювати оцінку захищеності ІТ систем та мереж; використовувати інструментальні засоби оцінки наявних вразливостей; оцінювати можливості та ефективність застосування, в тих чи інших умовах, інструментальних засобів оцінки вразливостей ІТ систем та мереж	Лекція, лабораторні заняття	Захист лабораторних завдань, контрольна робота, залік
РН-20. Виконувати налаштування інформаційних систем та комунікаційного обладнання; виконувати захист інформаційних систем від комп’ютерних вірусів; забезпечувати впровадження та дотримання політики кіберзахисту в ІТС, процедур, і правил; організовувати процес створення планів неперервності бізнесу; приймати участь у розробці планів відновлення, неперервності процесів організації для забезпечення здатності організації продовжувати виконувати необхідну діяльність в період порушення ІТ	Лекція, лабораторні заняття	Захист лабораторних завдань, контрольна робота, залік
Введення в мережі		
РН-18. Застосовувати теорії та методи захисту для забезпечення безпеки інформації в інформаційних і комунікаційних системах та мережах	Лекція, лабораторні заняття	Захист лабораторних завдань, контрольна робота, екзамен
РН-20. Виконувати налаштування інформаційних систем та комунікаційного обладнання; виконувати захист інформаційних систем від комп’ютерних вірусів; забезпечувати впровадження та дотримання політики кіберзахисту в ІТС, процедур, і правил; організовувати процес створення планів неперервності бізнесу; приймати участь у розробці планів відновлення, неперервності процесів організації для забезпечення здатності організації продовжувати виконувати необхідну діяльність в період порушення ІТ	Лекція, лабораторні заняття	Захист лабораторних завдань, контрольна робота, екзамен
РН-17. Виконувати декомпозицію ІТС; - розробляти структурні схеми з відображенням зв’язків між інформаційними процесами на віддалених системах; розробляти модель загроз, розробляти модель порушника; розробляти проекти ІТС базуючись на стандартизованих технологіях та протоколах передачі даних; вирішувати завдання захисту програм та даних ІТС програмно-апаратними засобами та давати оцінку якості прийнятих рішень; обирати основні методи та способи захисту інформації відповідно до вимог сучасних стандартів інформаційної безпеки щодо критеріїв безпеки інформаційних технологій, застосовуючи системний підхід та знання основ теорії інформаційної безпеки;	Лекція, лабораторні заняття	Захист лабораторних завдань, контрольна робота, екзамен

проектувати та реалізувати комплексні систему захисту інформації АС організації (підприємства) відповідно до вимог нормативних документів системи технічного захисту інформації		
РН-16. Здійснювати професійну діяльність на основі знань сучасних інформаційно-комунікаційних технологій; застосувати програмні засоби, навички роботи в телекомунікаційних та комп'ютерних мережах; використати спеціалізовані комп'ютерні програми в професійній діяльності. Обирати відповідну технологію програмування, виконати аналіз специфікації задач; виконувати аналіз програмного забезпечення з метою пошуку, ідентифікації, виявлення та усунення помилок програмування;	Лекція, лабораторні заняття	Захист лабораторних завдань, контрольна робота, екзамен
Комплексний тренінг		
РН-28. Використовувати теоретичні і практичні методи та методики досліджень у галузі інформаційної безпеки; застосовувати системний підхід та знання основ теорії інформаційної безпеки.	Тренінгові заняття	Індивідуально компетентісно-орієнтовані завдання, захист завдання
РН-24. Впроваджувати процеси виявлення, ідентифікації, аналізу та реагування на інциденти інформаційної/кібербезпеки; застосовувати національні та міжнародні регулюючі актів в сфері інформаційної безпеки для розслідування внутрішніх та зовнішніх інцендентів інформаційної безпеки	Тренінгові заняття	Індивідуально компетентісно-орієнтовані завдання, захист завдання
РН-21. Виявляти небезпечні сигнали технічних засобів; вимірювати параметри небезпечних сигналів для технічних каналів витоку інформації та визначати ефективність захисту від витоку інформації відповідно до вимог нормативних документів системи технічного захисту інформації інтерпретувати результати проведення спеціальних вимірювань з використанням технічних засобів, контролю характеристик ІТСМ відповідно до вимог нормативних документів системи технічного захисту інформації проводити атестацію (спираючись на облік та обстеження) режимних територій (зон), приміщень тощо в умовах додержання режиму секретності із фіксуванням результатів у відповідних документах виконувати дослідження, перевірку, аналіз та оцінювання об'єктів щодо їх відповідності вимогам нормативних документів та можливості їх використання для забезпечення інформації	Тренінгові заняття	Індивідуально компетентісно-орієнтовані завдання, захист завдання
РН-19. Здійснювати оцінку можливості проникнення в ІТ системи та мережі шляхом експлуатації наявних вразливостей; здійснювати оцінку захищеності ІТ систем та мереж; використовувати інструментальні засоби оцінки наявних вразливостей; оцінювати можливості та ефективність застосування, в тих чи інших умовах, інструментальних засобів оцінки вразливостей ІТ систем та мереж;	Тренінгові заняття	Індивідуально компетентісно-орієнтовані завдання, захист завдання
РН-17. Виконувати декомпозицію ІТС; - розробляти структурні схеми з відображенням зв'язків між інформаційними процесами на віддалених системах; розробляти модель загроз, розробляти модель порушника; розробляти проекти ІТС базуючись на стандартизованих технологіях та протоколах передачі даних; вирішувати завдання захисту програм та даних ІТС програмно-апаратними засобами та давати оцінку якості прийнятих рішень; обирати основні методи та способи захисту інформації відповідно до вимог сучасних стандартів інформаційної безпеки щодо критеріїв безпеки інформаційних технологій, застосовуючи системний підхід та знання основ теорії інформаційної безпеки; проектувати та реалізувати комплексні	Тренінгові заняття	Індивідуально компетентісно-орієнтовані завдання, захист завдання

систему захисту інформації АС організації (підприємства) відповідно до вимог нормативних документів системи технічного захисту інформації		
РН-6. Використати результати самостійного пошуку, аналізу та синтезу інформації з різних джерел для ефективного рішення спеціалізованих задач професійної діяльності;	Тренінгові заняття	Індивідуально компетентісно-орієнтовані завдання, захист завдання
Інформаційні системи та інтернет технології		
РН-17. Виконувати декомпозицію ІТС; - розробляти структурні схеми з відображенням зв'язків між інформаційними процесами на віддалених системах; розробляти модель загроз, розробляти модель порушника; розробляти проекти ІТС базуючись на стандартизованих технологіях та протоколах передачі даних; вирішувати завдання захисту програм та даних ІТС програмно-апаратними засобами та давати оцінку якості прийнятих рішень; обирати основні методи та способи захисту інформації відповідно до вимог сучасних стандартів інформаційної безпеки щодо критеріїв безпеки інформаційних технологій, застосовуючи системний підхід та знання основ теорії інформаційної безпеки; проектувати та реалізувати комплексні систему захисту інформації АС організації (підприємства) відповідно до вимог нормативних документів системи технічного захисту інформації.	Лекція, лабораторні заняття	Захист лабораторних завдань, контрольна робота, залік, екзамен
РН-16. Здійснювати професійну діяльність на основі знань сучасних інформаційно-комунікаційних технологій; застосувати програмні засоби, навички роботи в телекомунікаційних та комп'ютерних мережах; використати спеціалізовані комп'ютерні програми в професійній діяльності. Обирати відповідну технологію програмування, виконати аналіз специфікації задач; виконувати аналіз програмного забезпечення з метою пошуку, ідентифікації, виявлення та усунення помилок програмування.	Лекція, лабораторні заняття	Захист лабораторних завдань, контрольна робота, залік