НАЦІОНАЛЬНЕ АГЕНТСТВО ІЗ ЗАБЕЗПЕЧЕННЯ ЯКОСТІ ВИЩОЇ ОСВІТИ

ВІДОМОСТІ
про самооцінювання освітньої програми

Заклад вищої освіти	**Харківський національний економічний університет імені Семена Кузнеця**
Освітня програма	**35202 Кібербезпека**
Рівень вищої освіти	**Магістр**
Спеціальність	**125 Кібербезпека**

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

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

Використані скорочення:

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

Загальні відомості

1. Інформація про ЗВО (ВСП ЗВО)

Реєстраційний номер ЗВО у ЄДЕБО	**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	**35202**
Назва ОП	**Кібербезпека**
Галузь знань	**12 Інформаційні технології**
Спеціальність	**125 Кібербезпека**
Спеціалізація (за наявності)	*відсутня*
Рівень вищої освіти	**Магістр**
Тип освітньої програми	**Освітньо-професійна**
Вступ на освітню програму здійснюється на основі ступеня (рівня)	**Бакалавр**
Структурний підрозділ (кафедра або інший підрозділ), відповідальний за реалізацію ОП	**Кафедра кібербезпеки та інформаційних технологій**
Інші навчальні структурні підрозділи (кафедра або інші підрозділи), залучені до реалізації ОП	**Навчальна лабораторія кафедри кібербезпеки та інформаційних технологій, кафедра педагогіки, іноземної філології та перекладу, кафедра управління соціальними комунікаціями, відділ міжнародних зв'зків**
Місце (адреса) провадження освітньої діяльності за ОП	**м. Харків, пр-т Науки 9-А, 61166**
Освітня програма передбачає присвоєння професійної кваліфікації	*не передбачає*
Професійна кваліфікація, яка присвоюється за ОП (за наявності)	***відсутня***
Мова (мови) викладання	**Українська, Англійська**
ID гаранта ОП у ЄДЕБО	**72586**
ПІБ гаранта ОП	**Мілов Олександр Володимирович**
Посада гаранта ОП	**Професор**
Корпоративна електронна адреса гаранта ОП	**oleksandr.milov@hneu.net**
Контактний телефон гаранта ОП	**+38(066)-431-35-36**
Додатковий телефон гаранта ОП	*відсутній*

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

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

Незважаючи на наявність кількох потужних технічних університетів в Харкові, 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 на кафедрі Кібербезпеки та інформаційних технологій, яка створена в 2018 року та здійснює підготовку за спеціальністю 125. Кафедра щорічно проводить міжнародну науково-практичну конференцію "Інформаційна безпека та інформаційні технології". За результатами конференцій кафедра видає колективну монографію, в якій приймають участь провідні українські та закордонні спеціалісти в галузі захисту та безпеки інформації.
На основі Договору з Університетом у Бєльсько-Бялій (м. Бельсько-Бяла, Польща) діє освітньо-професійна програма двох дипломів, яка забезпечує підготовку магістрів за спеціальністю "Кібербезпека". Програма двох дипломів реалізується на основі двосторонніх Угод про співпрацю, укладених з Університетами–партнерами (УП) в Йорданії, Казахстані та Україні, згідно зі ст. 60 Закону про вищу освіту та науку Польщі від 20 липня 2018 р., Вісник законів 2018.1668, зі ст. 204 Закону про вищу освіту від 3 липня 2018 р., положення про введення в дію Закону про вищу освіту, Вісник законів 2018.1669, Розпорядженням Міністра науки та вищої освіти від 27 вересня 2018 р. щодо навчання, Вісник законів 2018.1861, Статутом УББ затвердженим Ухвалою № 1464/07/VI/2019 Сенату УББ від 16 липня 2019 р. з пізн. зм. та Ухвалою № 1551/07/VI/2020 Сенату УББ від 14 липня 2020 р., та рішенням вченої ради ХНЕУ ім С. Кузнеця (протокол № 1 від 02 червня 2020 р.).
Виходячи з освітніх потреб Харківського регіону, наявності освітніх ресурсів, університет забезпечує якісну підготовку висококваліфікованих фахівців за спеціальністю 125 "Кібербезпека", які забезпечують ефективну роботу у галузі безпеки інформаційних ресурсів, що задовольняє попит у кваліфікованих кадрах у бізнес-середовищі.
У підготовці ОПП "Кібербезпека" брали участь викладачі кафедри: Мілов Олександр Володимирович, Євсеєв Сергій Петрович, Алексієв Володимир Олегович, а також Макаренко Антон Олегович, здобувач вищої освіти за спеціальністю 125 "Кібербезпека", та роботодавці: технічний директор ТОВ "Сайфер БІС", кандидат технічних наук Ковтун Владислав Юрійович; співзасновник "Distributed Lab" Кравченко Павло Олександрович.

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

Рік навчання	Навчальний рік, у якому відбувся набір здобувачів відповідного року навчання	Обсяг набору на ОП у відповідному навчальному році	Контингент студентів на відповідному році навчання станом на 1 жовтня поточного навчального року		У тому числі іноземців	
			ОД	*З*	*ОД*	*З*
1 курс	2020 - 2021	6	6	0	0	0
2 курс	2019 - 2020	3	3	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 освіти	Інформація про освітні програми
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	75452	13115

Власні приміщення ЗВО (на праві власності, господарського відання або оперативного управління)	75380	13115
Приміщення, які використовуються на іншому праві, аніж право власності, господарського відання або оперативного управління (оренда, безоплатне користування тощо)	70	0
Приміщення, здані в оренду	331	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 Кібербезпека магістр.pdf*	R1T1E3IP1yNjurvUdi1HhACobL+XyZGYPku+7GpDb6I=
Навчальний план за ОП	*Навчальний план Кібербезпека магістри (укр).pdf*	tcnBypPs/LPhiF6b+PlUCoJ3yH/8kDo6W5b/2zYSACA=
Рецензії та відгуки роботодавців	*Рецензия Воробьев.pdf*	OhoHQZ2Zy2dSzeej76ErS+qmfsgaTctboceiWUHkRZg=
Рецензії та відгуки роботодавців	*Рецензия Кириченко.pdf*	HUiCkHcSWuS7YKjXjAEvUU7c7NMsYckcdsk9ChJj3G4=
Рецензії та відгуки роботодавців	*Рецензія Сайфер IT.pdf*	EkZFqQ9dNxG5jSZlxarNZ26DZ4LqfZjkMS9CX4fWEAE=
Рецензії та відгуки роботодавців	*Рецензія ITCluster.pdf*	DgKaJmdgZOwCbMVJHKeIgvxX/UTeL/nsFoibTgPfgLw=
Рецензії та відгуки роботодавців	*Рецензія на освітньо-наукову програму Кібербезпека.pdf*	1r3eHomcx1fS0A9fgsNQsYOqWwJc/mjV4ECMCD4n9Ac=

1. Проектування та цілі освітньої програми

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

Цілі ОП "Кібербезпека" – підготовка професіоналів, здатних розробляти та використовувати технології та засоби інформаційної та/або кібербезпеки, які володіють методами забезпечення безпеки в децентралізованих системах, ефективними засобами ризик-менеджменту, створення та використання криптовалют і смартконтрактів. Особливостями програми є формування у здобувачів навичок побудови комплексних систем захисту інформації для забезпечення безпеки контуру бізнес-процесів на основі сучасних технологій та програмних застосунків. Для цього на кафедрі разом з компанією "Distributed Lab" розгорнута лабораторія Блокчейн, на базі якої представники компанії, виконавці реальних проектів, які пов'язані з децентралізованими системами та смарт-контрактами (http://bit.ly/2SPVIN7) проводять майстер-класи, що дозволяє формувати відповідні компетентності. За допомогою ТОВ "Сайфер БІС" розгорнутий ЦСК. За проектом Темпус № 544455–TEMPUS-1-2013-1-SE-TEMPUS-JPCR кафедрою Інфокомунікаційної інженерії ім. В.В. Поповського ХНУРЕ надані 6 курсів ("Advanced Network & Cloud Security", " Digital Forensic", "Penetration testing and ethical hacking", "WebSecurity", "Software security", ""Wireless&Mobile Security"), які погоджені з дисциплінами за спеціальністю "Кібербезпека" в Університеті Бельско-Бяла. Протягом навчання здобувачі можуть отримати сертифікати академії CISCO (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, https://www.hneu.edu.ua/wp-content/uploads/2018/11/Strategic-Plan-HNEU-2013-2020-years-1.pdf);
2. Концептуальні засади розвитку ХНЕУ ім. С. Кузнеця до 2020 року (стор. 4-8, https://www.hneu.edu.ua/wp-content/uploads/2018/02/zasadu.pdf).
Місія та стратегія розвитку ХНЕУ ім. С. Кузнеця визначаються базовими положеннями концепції розвитку економічної освіти України, концептуальними положеннми і умовами реалізації основних напрямів діяльності університету у функціональному розрізі та конкретними завданнями за напрямами роботи.
Цілі ОПП "Кібербезпека" 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, запропонував надати можливість здобувачам вищої освіти висловлювати свої пропозиції через сайт кафедри (http://bit.ly/2PovXZy), а також запропонував залучати дослідників компанії DistrsbutedLab до визначення тематики та консультування дипломних проектів, пов'язаних з технологією блокчейн, децентралізованих систем та смарт-контрактів.

- роботодавці

Технічний директор ТОВ "Сайфер БІС" Ковтун Владислав (член робочої групи ОПП "Кібербезпека") запропонував включити в освітній процес підготовки здобувачів другого (магістерського) рівня питання, які пов'язані з забезпеченням протидії корупції в університеті, впровадження елементів е-послуг на рівні деканатів кафедр за допомогою технології PKI, та провести тренінги із здобувачами.
Співзасновник компанії "Distributed Lab" Кравченко Павло, який є членом робочої групи, запропонував розгорнути лабораторію Блокчейн та включити відповідні дисципліни в вибіркову складову університету. Після обговорення було розроблено сайт лабораторії Блокчейн (https://blockchain.hneu.edu.ua/), а також запропоновано магмайнер "Валюта, криптовалюта і блокчейн технології", "Основи блокчейн-технології" та тренінг-курс "Блокчейн: математичні проблеми та застосунки"

- академічна спільнота

В обговорені освітніх компонентів активну участь приймали завідувач кафедри безпеки інформаційних технологій Національного авіаційного університету (м. Київ) д.т.н., проф. Корченко О.Г, завідувач кафедри кібербезпеки та математичного моделювання Чернігівського державного технологічного університету (м. Чернігів) д.пед.н., доц. Ткач Ю.М., завідувач кафедри комп'ютерних наук та автоматики університету Більсько-Бяла (Польща) проф., д.т.н. Карпінський М.П., які погодились включити в навчальний план дисципліни: "Інформаційна безпека телекомунікаційних та хмарних технологій", "Тестування на проникнення та етичний хакінг", "Безпека бездротових та мобільних мереж", "Безпека Web-ресурсів", "Цифрова криміналістика", "Безпека Інтернет-речей".

- інші стейкхолдери

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

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

Ринок праці ІТ-галузі України розвивається доволі стрімко, при цьому все більшу популярність набувають вакансій за категорією програміст-аналітик. Понад 47 % замовлень в ІТ-компаніях пов'язані з розробленням програмних застосунків, які забезпечують інформаційну безпеку та захист інформації. За результатами 2019-2020 р. індустрія працівників ІТ зросла на 20% (https://bit.ly/2Gcq9ux), серед мов програмування найбільш затребуваними 2019 р. були PHP, Python і Java. ОПП "Кібербезпека" дає можливість набуття компетентностей з використання зазначених мов програмування, що дозволять здобувачам вищої освіти підвищити свою конкурентоспроможність на ринку праці. Робоча група регулярно проводить аналіз побажань стейкхолдерів (роботодавців) перед початком оновлення (перегляд) програми на наступний рік.

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

Під час формулювання цілей та програмних результатів навчання ОП "Кібербезпека" враховувались рекомендації Харківського ІТ-кластеру, інформація стосовно останніх досліджень ІТ-кластеру знаходиться на їх сайті. Звіт про останні дослідження (https://bit.ly/2Gcq9ux).

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

Під час формулювання цілей та програмних результатів навчання з ОП "Кібербезпека" були проаналізовані освітні програми з підготовки здобувачів другого (магістерського) рівня вищої освіти за спеціальністю 125 "Кібербезпека" провідних технічних університетів м. Києва (Київський політехнічний інститут імені Ігоря Сікорського (http://bit.ly/39Cv7dh), Національний авіаційний університет (http://bit.ly/37pQfSx)), м. Харкова (Харківський національний університет радіоелектроніки (http://bit.ly/2SJwakL), Харківський національний університет ім. В.Н. Каразіна (http://bit.ly/2SJwakL)), освітні програми з підготовки здобувачів зі спеціальності "Кібербезпека" у закладах США (http://bit.ly/2SJEiSb), а також освітні компоненти погоджені в рамках Польсько-української програми обміну та двох дипломів для підготовки магістрів за спеціальністю "Кібербезпека" з Університетом у

Бєльсько-Бялій (м. Бельсько-Бяла, Польща), до якої приєднались кафедра Безпеки інформаційних технологій (Національний авіаційний університет), кафедра кібербезпеки та математичного моделювання (Чернігівський національний технологічний університет), а також університеті Казахстану та Йорданії.
На основі аналізу були визначені основні фахові компетентності 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

Стандарт за спеціальністю 125 «Кібербезпека» відсутній.

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 вимог Національної рамки кваліфікацій (магістр – 7) формування спеціалізованих концептуальних знань, що включають сучасні наукові здобутки у сфері професійної діяльності або галузі знань і є основою для оригінального мислення та проведення досліджень, критичне осмислення проблем у галузі та на межі галузей знань відбувається через освітні компоненти базової складової (циклу професійної підготовки) а саме: «Передові методики програмування», «Безпека Інтернет речей», «Розширена мережева та хмарна безпека», «Цифрова криміналістика», «Тестування на проникнення та етичний хакінг», «Веб-безпека», «Бездротова та мобільна безпека».
Спеціалізовані уміння/навички розв'язання проблем, необхідні для проведення досліджень та/або провадження інноваційної діяльності з метою розвитку нових знань та процедур отримуються під час проведення лабораторних занять за освітніми компонентами в спеціалізованому середовище "Кіберполігон", який дозволяє в повному обсязі відпрацьовувати спеціалізовані завдання.
Здатність інтегрувати знання та розв'язувати складні задачі у широких або мультидисциплінарних контекстах формуються під час тренінг-курсу: Блокчейн: математичні проблеми та застосунки, проведення науково-дослідної практики танаписання дипломного проекту.
Здатність розв'язувати проблеми у нових або незнайомих середовищах за наявності неповної або обмеженої інформації з урахуванням аспектів соціальної та етичної відповідальності формуються під час виконання завдань за освітніми компонентами як базової складової, так і вибіркової, а саме: Інженерія безпеки інформаційно-комунікаційних систем, Розширене адміністрування серверних сервісів, Безпека серверних систем, Бездротові та оптичноволоконні мережі.
Зрозуміле і недвозначне донесення власних знань, висновків та аргументації до фахівців і нефахівців, зокрема до осіб, які навчаються формується під час виконання контрольних заходів за всіма освітніми компоентами навчального Плану підготовки магістрів, а також на окремих освітніх компонентах базової складової: Презентація та обробка знань, Захист інтелектуальної власності, Мистецтво редагування та риторика.
Управління робочими або навчальними процесами, які є складними, непередбачуваними та потребують нових стратегічних підходів, відповідальність за внесок до професійних знань і практики та/або оцінювання результатів діяльності команд та колективів формується під час проведення лабораторних занять за освітніми компонентами базової складової в спеціалізованому середовище "Кіберполігону", де мається можливість виконувати завдання у складі команд.
Здатність продовжувати навчання з високим ступенем автономії формується під час проведення тренінг-курсу: Блокчейн: математичні проблеми та застосунки, проведення науково-дослідної практики танаписання дипломного проекту.

2. Структура та зміст освітньої програми

Яким є обсяг ОП (у кредитах ЄКТС)?

90

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

67

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

23

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, які використовуються для забезпечення функціонування цих об'єктів; процеси управління інформаційною і кібербезпекою об'єктів, що підлягають захисту. Ці питання відповідають 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 освітніх компонентів ОПП "Кібербезпека" дозволяє сформувати комплекс знань, навичок та вмінь, які відповідають високому рівню 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 (https://bit.ly/2HH3Gq0).
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") використанням сучасних механізмів, програмних застосунків, програмно-апаратних засобів щодо формування системи безпеки контуру бізнес-процесів. Таким чином, ОПП "Кібербезпека", що спрямована на підготовку фахівців з інформаційної та кібербезпеки, програмістів-аналітиків, за своїм змістом відповідає предмітній області заявленої спеціальності.

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

Відповідно до навчального плану здобувачі вищої освіти мають можливість формування індивідуальної освітньої траєкторії на основі вибору вибіркових дисциплін із загального університетського пулу (маг-майнори), що складає 23 кредити.
Здобувачі вищої освіти у 2019 р. вибрали з Переліку загальноуніверситетського пулу навчальних дисциплін, що забезпечують вибіркову складову (маг-майнори) освітньо-професійних програм підготовки магістрів (26 маг-майнерів для першого та 23 маг-майнера для другого семестрів) (https://wvww.hneu.edu.ua/vybirkova-skladova-osvitno-profesijnyh-program-2019-2020-n-r/mag-majnor-2019-2020/), здобувачі вищої освіти набору 2020 р. вибрали з Переліку магмайнерів (33 маг-майнера для першого та 34 маг-майнера для другого семестрів) (https://www.hneu.edu.ua/mag-majnor-2020-2021/). Вибор дисциплін проводиться за допомогою веб-сайту (https://bit.ly/343F8iq). Також здобувачам вищої освіти надається можливість навчатися по індивідуальному навчальному плану.
Таким чином здобувачам вищої освіти забезпечена можливість формування індивідуальної освітньої траєкторії.

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) здобувачам надається можливість вільного вибору навчальних дисциплін у межах 25% загального обсягу відповідної освітньо-професійної програми. Обрані дисципліни увійдуть до індивідуального навчального плану кожного студента, а результати навчання будуть відображені у додатку до диплому.
Принцип вільного вибору дає змогу кожному здобувачу вивчати навчальні дисципліни, які відображають індивідуальні вподобання, інтереси та плани на майбутнє працевлаштування.
Реєстрація на вибіркову складову освітньо-професійної програми підготовки відбувається на підставі форми-заяви, що заповнюється та подається до відповідного деканату. Вибір варіативної складової (маг-майнерів) здійснюється за допомогою веб-сайту (http://elect.hneu.edu.ua/ru)

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

У відповідності до навчального плані практична підготовка здійснюється під час проведення лабораторних та практичних занять за освітніми компонентами базової складової, а саме при вивченні дисциплін «Передові методики програмування», «Безпека Інтернет речей», «Розширена мережева та хмарна безпека», «Цифрова криміналістика», «Тестування на проникнення та етичний хакінг», «Веб-безпека», «Бездротова та мобільна безпека», вибіркової складової, а саме: «Інженерія безпеки інформаційно-комунікаційних систем», «Безпека серверних систем», «Розширене адміністрування серверних сервісів» в спеціалізованому середовищі "Кіберполігону", а також під час проведення тренінг-курсу: «Блокчейн: математичні проблеми та застосунки» з залученням фахівців компанії DistributedLab, яка спеціалізується на розробці програмних застосунків на основі технології Блокчейн, децентралізованих систем та смарт-контрактів.

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: Англійська мова, Господарське право, Мистецтво редагування та риторика, Захист інтелектуальної власності, які забезпечують наступні компетентності щодо формування соціальних навичок: ЗК 3 – здатність професійно спілкуватися державною та іноземною мовами як усно, так і письмово; ЗК 6 – здатність реалізувати свої права і

обов'язки як члена суспільства, усвідомлювати цінності громадянського (вільного демократичного) суспільства та необхідність його сталого розвитку, верховенства права, прав і свобод людини і громадянина в Україні; ЗК 7 – здатність зберігати та примножувати моральні, культурні, наукові цінності і досягнення суспільства на основі розуміння історії та закономірностей розвитку предметної області, її місця у загальній системі знань про природу і суспільство та у розвитку суспільства, техніки і технологій, використовувати різні види та форми рухової активності для активного відпочинку та ведення здорового способу життя. Запропоновані дисципліни дозволяють зформувати 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 містить як профільні навчальні дисципліни, так і непрофільні, які формують загально-професійні компетентності. 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).
ОПП включає блоки з загальним обсягом кредитів ECTS:
1. Цикл професійної підготовки (базова складова) – 67 кредити, 14.4 % (аудиторні) та 85.6 % (самостійна).
2. Цикл професійної підготовки (вибіркова складова) – 23 кредита, 27,5 % (аудиторні) та 72,5 % (самостійна).
В цілому за навчальний план аудиторне навантаження здобувачів вищої освіти складає 17,8 %, самостійна робота – 82,2 %.

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, але в університеті пернедбачені можливості підготовки фахівців за дуальною формою (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).

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?

Набір на спеціальність освітнього рівня "магістр" здійснюється на загальних умовах вступу за результатами:
1) з іноземної мови за результатами незалежного зовнішнього тестування;
2) за комплексом навчальних дисциплін з галузі знань 12 "Інформаційні технології";
3) з урахуванням середнього балу документа про вищу освіту першого (бакалаврського) рівня.
Для успішного засвоєння освітньо-професійної програми магістра абітурієнти повинні мати перший (бакалаврський) рівень вищої освіти (диплом бакалавра), підтверджений документом державного зразка, що виданий закладом вищої освіти III-IV рівня акредитації.
Програма фахового вступного випробування освітнього ступеню "Магістр" доступна на сайті кафедри (https://www.hneu.edu.ua/wp-content/uploads/2020/04/Kiberbezpeka-2020.pdf).

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

Питання визнання результатів навчання, отриманих в інших ЗВО, регулюється "Положенням 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),

яке 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. Реалізація пунктів Положення 4.9., 4.10., 4.11., 4.12., 4.13 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)?

Відповідно до програми двох дипломів Університету у Бєльсько-Бялій (Польща) здобувачі вищої освіти другого (магістерського) рівня набору 2020 р. за ОПП "Кібербезпека" Харківського національного економічного університету імені Семена Кузнеця (ХНЕУ ім С. Кузнеця) (Україна) на напрямі/в галузі знань Інформатика/Інформаційні технології (IT), віднесеної до наукової дисципліни/спеціальності "Технічна інформатика та телекомунікація"/"Кібербезпека" мають право отримати другий диплом Університету у Бєльсько-Бялій (Польща). При цьому перший рік навчання студенти навчаються в ХНЕУ ім С. Кузнеця, другий рік (Переддипломна практика, Дипломний проект) в Університеті у Бєльсько-Бялій (Польща) (https://www.hneu.edu.ua/polsko-ukrayinska-programa-dlya-pidgotovky-magistriv-za-spetsialnistyu-kiberbezpeka-z-universytetom-u-byelsko-byalij/).

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

Питання визнання результатів навчання, отриманих у неформальній освіті регулюються "Положенням про порядок визнання результатів неформальної та інформальної освіти у ХНЕУ ім. С. Кузнеця" (http://bit.ly/2VKT3HC), наказів ректора № 158 від 02.09.2019 р. (https://bit.ly/3iaZlHZ), № 115 від 28.05.2019 р. (https://bit.ly/2GgrSPo), № 34 від 15.01.2019 р. (https://bit.ly/3ieqidO). Згідно положенню 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) зарахувати ці бали за відповідну навчальну дисципліну. Студенти можуть запропонувати курси неформальної освіти у відповідності до індивідуальної траєкторії навчання. На основі сертифікату рішенням засідання кафедри результати можуть бути зараховані за відповідною дисципліною.

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

На сайті університету (https://bit.ly/3n0HQho) та кафедри (https://bit.ly/36d3fxX) розміщено перелік курсів академії CISCO ХНЕУ ім. С. Кузнеця. Рішенням кафедри затверджені курси неформальної освіти: курси академії CISCO (протокол № 2 від 13.09.2019 р., протокол № 7 від 24.12.2019 р.).
Здобувачі вищої освіти за ОПП "Кібербезпека" 2019 р. набору отримали:
Сертифікат CISCO «Introduction to cybersecurity» - 2 студента (Бофанов А.В., Москаленко Є.О.)

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 та практичні заняття, основними формами навчання: індивідуальне заняття, тренінг, інтерактивне дистанційне навчання, самостійна робота студента.
Вказані методи та форми навчання сприяють досягненню програмних результатів навчання за рахунок поєднання теоретичних та практичних занять.
Посилання на відповідні документи:
1. "Тимчасове положення про організацію освітнього процесу в ХНЕУ ім. С. Кузнеця" п. 3.3 (https://bit.ly/3n0uyBt)
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 (https://bit.ly/345J42k)

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 (https://bit.ly/2S8Iv1Z): 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 1 курсу другого (магістерського) рівня вищої освіти за ОПП "Кібербезпека" отримані наступні результати: задоволеність освітньою програмою – 99,1 % (середнє значення) (https://bit.ly/2HH3Gq0).

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" (https://bit.ly/3nouyBt). 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. Положення про розроблення, затвердження, моніторінг періодичний перегляд та оновлення освітніх програм (https://bit.ly/3l9re57)

Учасники освітнього процесу мають вільний доступ до сайту кафедри, де розміщені РПНД за дисциплінами навчального плану (https://bit.ly/30hp3EQ), 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/2SzqhYp). 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 під час розробки проектів та науково-дослідних тем.

В рамках наукової діяльності кафедри в 2019 році виконувалась 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.

Оприлюднити результати своїх наукових досліджень здобувачі вищої освіти можуть в рамках проведення Міжнародної науково-практичної конференції "Інформаційна безпека та інформаційні технології", яка проводиться за підтримкою кафедри (https://bit.ly/3kXsLLH).

Цей вид студенської активності регулюється Тимчасовим положенням про організацію освітнього процесу в ХНЕУ ім. С. Кузнеця (https://bit.ly/3nouyBt).

З боку викладачів результати дослідження, отримані при виконанні наукової роботи, використовуються при викладанні таких дисциплін як «Тестування на проникнення та етичний хакінг», «Цифрова криміналістика», «Розширена мережева та хмарна безпека» та «Бездротова та мобільна безпека».

В освітній процес викладачами кафедри впроваджено результати наукових досліджень, отриманих під час виконання ініціативної теми, 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.

З метою практичної реалізації результатів наукових досліджень на кафедрі сформовано лабораторію блокчейн (http://bit.ly/2SPVIN7), яка дозволяє здобувачам отримати додаткові навчальні матеріали, відпрацьовувати питання забезпечення безпеки в програмних застосунках з використанням технології блокчейн, на основі мови Python, та виконувати індивідуальні наукові дослідження.

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

Викладачі оновлюють зміст освітніх компонентів на основі наукових досягнень і сучасних практик у галузі кібербезпеки наступним чином. Викладачі кафедри приймають активну участь у міжнародних конференціях: 5th IEEE International Symposium on Smart and Wireless Systems Within the INTERNATIONAL CONFERENCES ON INTELLIGENT DATA ACQUISITION AND ADVANCED COMPUTING SYSTEMS (IDAACS-SWS 2020) (http://www.idaacs.net/2020), (MIMCS:PP 2020). (https://www.mimcs.org/) (Азербайджан).

За останні 3 роки викладачами кафедри надрукованл статей у НМБ Scopus – 20, у фахових виданнях - 18.

На даний час на кафедрі завершена 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.
В навчальних дисциплінах, які пов'язані з блокчейн-технологією використовується матеріал навчальних курсів платформи Coursera, а також навчальні матеріали компаній Сайфер і DistributedLab, 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.
На даний час кафедра чекає рішення 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), що дозволить здобувачам вищої освіти отримати два дипломи за другим (магістерським) рівнем (https://www.hneu.edu.ua/polsko-ukrayinska-programa-dlya-pidgotovky-magistriv-za-spetsialnistyu-kiberbezpeka-z-universytetom-u-byelsko-byalij/).

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 здобувачив враховує види занять, які згідно з програмою навчальної дисципліни передбачають лекційні, лабораторні, семінарські, практичні заняття, а також виконання самостійної роботи. Оцінювання сформованих компетентностей у здобувачів 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.
Здобувача 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" (https://bit.ly/2GoCgeo), "Положення про проведення іспитів із застосуванням комп'ютерів" на факультеті економічної інформатики (яке визначає порядок проведення та перевірки результатів навчання) (http://bit.ly/2STdJdh).

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" (https://bit.ly/2GoCgeo), 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 (https://bit.ly/30hp3EQ). Інформація про поточний стан успішності здобувачі вищої освіти мають можливість перевірити на сайті університету у особистому кабінеті (http://bit.ly/2SzqhYp).

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 на відповідній закладці сайту персональних навчальних систем (https://pns.hneu.edu.ua/) розміщуються РПНД, робочий план (технологічна карта) , а також формується електронний журнал дисципліни, в якому вказуються контрольні заходи та відповідні бали. Здобувачі вищої освіти мають право переглянути отримані бали за кожною дисципліною протягом семестру (http://bit.ly/2SzqhYp). РПНД також розміщуються на сайті кафедри (https://bit.ly/30hp3EQ). Інформація про форми контрольних заходів відображається також на сайті університету у графіку навчального процесу (http://bit.ly/37Ewd73). Крім того, на передекзаменаційній консультації лектор доводить зміст екзаменаційного білету та критерії оцінювання кожного питання у білеті з детальним описом нарахування кожного балу. Все це забезпечує доведення до здобувачів вищої освіти інформації про форми контрольних заходів та критерії оцінювання.

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

Стандарт за спеціальністю відсутній.

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

Процедура проведення контрольних заходів регулюється “Положенням про проведення письмових екзаменів у ХНЕУ ім. С. Кузнеця” (https://bit.ly/2GoCgeo), 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 (https://bit.ly/2GfjsHU). Доступність для учасників освітнього процесу забезпечується розміщенням зазначених документів на сайтах універитету та факультету.

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

Об’єктивність екзаменаторів забезпечується виконанням відповідних пунктів наступних нормативних документів: “Положення про проведення письмових екзаменів у ХНЕУ ім. С. Кузнеця” (п. 2, https://bit.ly/2GoCgeo), Тимчасове 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). Ці документи затверджують форму та процедуру проведення екзамену, а саме ☐ екзамени проводяться тільки письмово, під наглядом спостерігачів.
Після проведення іспиту відповідно до “Положення про проведення письмових екзаменів у ХНЕУ ім. С. Кузнеця” (п. 3, https://bit.ly/2GoCgeo) організується шифрування робіт співторібтниками деканату, після цього роботи перевіряє екзаменаційна комісія.
У разі проведення он-лайн тестування співробітник деканату переносить результат виконання тесту з файлу роботи здобувача до екзаменаційної форми (форма № Н-1.08 частина 2).
Процедури запобігання, виявлення та вирішення конфліктних ситуацій в університеті визначаються “Положенням про політику та процедури врегулювання конфліктних ситуацій у ХНЕУ ім. С. Кузнеця” пп. ІІІ , IV (http://bit.ly/2V8lxLj).
Порядок розгляду апеляції у разі незгоди з результатами оцінювання іспиту визначає “Положення про апеляцію результатів підсумкового контролю у формі іспиту” (https://bit.ly/3jhh3v4).

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

Порядок повторного проходження контрольних заходів регулюється наступними нормативними документами: Тимчасовим положенням "Про порядок оцінювання результатів навчання студентів за накопичувальною бально-рейтинговою системою" ХНЕУ ім. С. Кузнеця (п. 8, http://bit.ly/2Huqrdh), Положенням “Про порядок формування рейтингу успішності студентів ХНЕУ ім. С. Кузнеця для призначення академічних стипендій” (стор. 8, пп. 13, http://bit.ly/2u4LUXb), “Положенням про проведення письмових екзаменів у ХНЕУ ім. С. Кузнеця” (https://bit.ly/2GoCgeo). У відповідності до 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: Згідно з графіком навчального процесу університету до розкладу першої перездачі літної екзаменаційної сесії 2019/2020 н. р. факультету економічної інформатики (22–27.06.2020 р.) були перездачи іспитів за навчальним дисциплінами “Децентралізовані застосунки”, “Ризик-менеджмент”, “Інтелектуальні системи даних”; друга перездача згідно графіку навчального процессу університету призначена з 19 серпня по 22 серпня 2020 р.(https://bit.ly/2Gjggei).

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

Порядок оскарження процедури та результатів проведення контрольних заходів здійснюється відповідно до “Положення про апеляцію результатів підсумкового контролю у формі іспиту” (https://bit.ly/3jhh3v4). На початку

навчального 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 декана 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 оцінку, а 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?

Наступні документи ХНЕУ ім. С. Кузнеця містять політику, стандарти і процедури дотримання академічної доброчесності:
1. Кодекс академічної доброчесності ХНЕУ ім. С. Кузнеця (п. 3, п. 5, http://bit.ly/2Swgt1k), в яком прописана сформована політика забезпечення середовища академічної доброчесності та заходи щодо формування середовища академічної доброчесності.
2. Кодексі професійної етики та організаційної культури працівників і студентів ХНЕУ ім. С. Кузнеця (https://bit.ly/3kWMniV).
3. Положення про порядок проходження рукопису від його підготовки до видання у ХНЕУ ІМ. С. Кузнеця (https://bit.ly/33c5WxA).
4. Регламент перевірки на унікальність рукописів У ХНЕУ ім. С. Кузнеця (https://bit.ly/36fdlhA).

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

Як інструменти протидії порушенням академічної доброчесності застосовуються наступні технологічні рішення. 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 забезпечення, а саме доступ до системи StrikePlagiarism.com.
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 можна переглянути за посиланням (https://bit.ly/2S5WOV2).

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). На відповіжній сторінці сайту університету (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. В рамках дисциплін, які пов'язані з основами наукових досліджень розглядається питання академічної доброчесності, які виникають, зокрема, 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

Реакція ЗВО на порушення академічної доброчесності регламентується законом України "Про освіту" та Кодексом академічної доброчесності ХНЕУ ім. С. Кузнеця (п. 5, http://bit.ly/2Swgt1k). За порушення академічної доброчесності педагогічні, науково-педагогічні та наукові працівники закладів освіти можуть бути притягнені до відповідальності, наслідком чого є: 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 можуть бути притягнені до такої академічної відповідальності: повторне проходження оцінювання (контрольна робота, іспит, залік та інше); повторне проходження відповідного освітнього компонента освітньо-професійної 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 конкурсного добору НПП ОП “Кібербезпека” враховується їх наукова та професійна діяльність, а саме: публікації в науково-метричних базах SCOPUS, Web of Science, наявність сертифікатів неформальних курсів за напрямами викладання, наявність сертифікатів на знання іноземних мов, наявність сертифікатів підвищення кваліфікації в галузі “Захисту інформації”. Оголошення конкурсу на заміщення вакантної посади науково-педагогічного працівника розміщується на сайті університету (http://bit.ly/2u4soKo).

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

Під час розробки ОП “Кібербезпека” для погодження переліку компетентностей здобувачів вищої освіти другого (магістерського) рівня та на їх основі вибору дисциплін навчального плану, які повинні забезпечити формування відповідних компетентностей були залучені комерційний директор ТОВ “Сайфер БІС”, кан.тех.наук Ковтун Владислав 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 тренінг-курсу: Блокчейн: математичні проблеми та застосунки, використовувати в навчальних дисциплінах сучасні курси неформальної підготовки академії Cisco, а саме 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. На вибірковому тренінг-курсі «Блокчейн» планується в рамках співпраці з “Distributed Lab” проведення мастер-класів.

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

В рамках тренінг-курсу: Блокчейн: математичні проблеми та застосунки спеціалістами компанії “Distributed Lab” були проведені 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

Професійний розвиток НПП за ОП “Кібербезпека” забезпечується програмами підвищення кваліфікації розроблених в Університеті та регулюються положенням. В Університеті, впродовж 8 років, успішно функціонує Центр підготовки кандидатів до участі у незалежному міжнародному тестуванні щодо оцінювання рівня володіння діловою англійською мовою (Business English Certificates). Також розвинена практика подання грантових заявок на викладання, навчання, стажування, проведення досліджень в університетах країн ЄС, що забезпечується відділом міжнародних зав’язків http://depint.hneu.edu.ua/.
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). Викладачи кафедри Погасій С.С., Гаврилова А. А. поступили на заочну форму навчання в ХНУРЕ (наказ про зарахування № 136Стз від 15.09.2020 р. освітньо-професійна програма “Адміністративний менеджмент у сфері захисту інформації” другого рівня вищої освіти за спеціальністю 125 “Кібербезпека” кваліфікація “Магістр. Кібербезпека. Адміністративний менеджмент у сфері захисту інформації”), Мілевський С.В. поступив на заочну форму навчання в НАУ (освітньо-професійна програма “Адміністративний менеджмент у сфері захисту інформації” другого рівня вищої освіти за спеціальністю 125 “Кібербезпека” кваліфікація “Магістр. Кібербезпека. Адміністративний менеджмент у сфері захисту інформації”).

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). Протегом 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. Вченої Радою університету (протокол № 4 від 23.09.2020 р.) прийнято рішення про присвоєння Корольову Р.В., Погасію С.С., Мілевському С.В. вченого звання доцента по кафедрі кібербезпеки та інформаційних технологій.

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 2019 – (https://bit.ly/33d89co).
Матеріально-технічні ресурси: бібліотечний фонд за спеціальністю відповідає Ліцензійним умовам; в Університеті є доступ до багатьох online-ресурсів за спеціальностями (https://bit.ly/30hiRfY); використовується безкоштовне програмне забезпечення, trial-версії або ліцензійне програмне забезпечення, яке оформлене належним чином та використовується в освітньому процесі. В репозитарії університету розміщені освітньо-методичні видання викладачів університету та наукові статті, які було надруковано в журналах, індексуємих Scopus (Східно-Європейський журнал передових технолгій). Кількість мультимедійних проекторів складає 97. Навчально-методичне забезпечення ОП за усіма компонентами розміщується на сайт персональних навчальних систем Університету https://pns.hneu.edu.ua/, де для кожної дисципліни 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 здобувачі можуть обрати для себе будь-яку ланку, для самореалізації позанавчальним процесом. В університеті тіє орган студентського самоврядування (https://bit.ly/2EMqZh4). Студенти та викладачі мають безкоштовний вільний доступ до Інтернету, інфраструктури, інформаційних ресурсів університету, можливість попереднього дистанційного замовлення видань фонду електронного каталогу бібліотеки (https://bit.ly/3kUVD7i), сайту персональних навчальних систем університету (https://pns.hneu.edu.ua/). Соціальні мережі Facebook (https://bit.ly/30z5qs7), Instagram (https://bit.ly/3cNZ8tu) використовуються для інформування та залучення. В університеті періодично проводиться опитування щодо оцінювання задоволеності потреб та інтересів здобувачів вищої освіти ОПП “Кібербезпека” (https://bit.ly/2HH3Gq0).
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)?

Безпечність освітнього середовища для життя та здоров’я здобувачів вищої освіти ЗВО забезпечує наступним чином:
Медичне забезпечення (https://bit.ly/2EMrmIu):
• 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 (https://bit.ly/30iMjCb).
Також на базі ХНЕУ ім. С. Кузнеця створена соціально-психологічна служба (https://bit.ly/33e9Y8O). 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 (+38050–1351–519, 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% (https://bit.ly/2HH3Gq0).

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?

Освітня підтримка в Університеті (відділ забезпечення якості освіти та інноваційного розвитку (https://bit.ly/33aeWDv), навчальний відділ (https://bit.ly/36igMEw), відділ молодіжної політики та соціального розвитку (https://bit.ly/2EMqZh4), гарант програми тощо) реалізується за рахунок навчально-методичного забезпечення дисциплін ОПП “Кібербезпека” через сайт персональних навчальних систем (https://pns.hneu.edu.ua/); відкритого доступу до методичних рекомендацій та навчальних посібників розміщені в електронному репозитарії (https://bit.ly/3jd3I6Z). Періодично кураторами груп, завідувачем кафедри проводяться зустрічі для вирішення питань навчального процесу. У Фейсбуці постійно ведеться група Інформаційних технологій та кібербезпека (https://bit.ly/3cHbS4V/). 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. (https://bit.ly/33egFYx). Організаційна підтримка здійснюється відділами: навчальний відділ, відділ працевлаштування студентів та взаємодії з бізнес-структурами (http://job.hneu.edu.ua/), методичний відділ (https://bit.ly/2GdWzod) 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 здобувачів освіти за ОП, рівень задоволеності якості освіти складає 99,1%.
Також університетом проводиться робота з реалізації політики гендерної рівності та недопущення дискримінації. Університетом розроблений та впроваджується План гендерної рівності (https://bit.ly/30dZuEw).

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 (https://bit.ly/348oRZt).
Керівні документи щодо реалізації права на освіту особами з особливими освітніми потребами розміщені у закладці Інклюзія сайту університету (https://bit.ly/30l1Ame).
За ОП "Кібербезпека" студенти з особливими потребами 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 регулюється положенням 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 (https://bit.ly/3cISEvC).
– Положення про проведення письмових екзаменів у ХНЕУ ім. С. Кузнеця (https://bit.ly/2GoCgeo).
– Положення про апеляцію результатів підсумкового контролю у формі іспиту (https://bit.ly/3jhh3v4).
– Кодекс професійної етики та організація культури працівників та студентів ХНЕУ ім. С. Кузнеця – (https://bit.ly/3kWMniV (академічна доброчесність), (https://bit.ly/2EIUvEp).
– План виховної роботи університету на 2020-2021 н.р. (https://bit.ly/3n03Skn). – Соціально-психологічна служба ХНЕУ ім. С. Кузнеця (https://bit.ly/3iimDf3). – Питання запобігання та виявлення корупції (https://bit.ly/3kRWJ3u).
– Можливості для студентів з особливими потребами (https://bit.ly/348oRZt).
– Статут ХНЕУ ім. С. Кузнеця (https://bit.ly/33cyDdV).

8. Внутрішнє забезпечення якості освітньої програми

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

Процедури розроблення, затвердження, моніторингу та періодичного перегляду ОП регулюються Положенням про розроблення, затвердження, моніторінг, періодичний перегляд та оновлення освітніх програм у ХНЕУ ім. С. Кузнеця (https://www.hneu.edu.ua/wp-content/uploads/2020/09/Polozhennya-pro-rozroblennya-zatverdzhennya-monitoring-periodychnyj-pereglyad-ta-onovlennya-osvitnih-program-u-HNEU.pdf). 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 (https://bit.ly/3n2l4Wo), система внутрішнього забезпечення якості освітньої діяльності та якості освіти охоплює всі процедури, що здійснює ХНЕУ ім. С. Кузнеця щодо безперервного вдосконалення якості освітнього 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 (https://bit.ly/33ffSXr).

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

Перегляд ОП здійснюється наступним чином. Кожні півроку 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 проводиться опитування задоволеності здобувачами дисциплін ОПП “Кібербезпека”. Ця процедура здійснюється для виконання наступних функцій управління ЗВО: 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 (https://bit.ly/2Hy295o, с.2-4), методичний відділ (http://bit.ly/3aSSAr5, с. 3-4), відділ електронних засобів навчання (http://bit.ly/2wT1shN, с. 3-5), навчальний відділ (http://bit.ly/3cWGfE6, с. 2-3), відділ маркетингу та корпоративних комунікацій (http://bit.ly/2Wamhjt, с. 2-5), відділ допомоги працевлаштування студентів та взаємодії з бізнес-структурами (http://bit.ly/2WhU7TP, с. 2-5), відділ молодіжної політики та соціального розвитку (https://bit.ly/2EMqZh4), відділ міжнародних зв’язків (https://bit.ly/2S61zxS), бібліотека (https://bit.ly/36fibeK).
Відповідно до програми двох дипломів останні зміни були внесені в ОПП на основі спільного обговорення освітніх компонентів з завідувачем кафедри безпеки інформаційних технологій Національного авіаційного університету (м. Київ) д.т.н., проф. Корченко О.Г, завідувачем кафедри кібербезпеки та математичного моделювання Чернігівського державного технологічного університету (м. Чернігів) д.пед.н., доц. Ткач Ю.М., завідувачем кафедри комп’ютерних наук та автоматики університету Більсько-Бяла (Польща) проф., д.т.н. Карпінський М.П., які погодились включити в навчальний план дисципліни: “Інформаційна безпека телекомунікаційних та хмарних технологій“, “Тестування на проникнення та етичний хакінг”, “Безпека бездротових та мобільних мереж”, “Безпека Web-ресурсів”, “Цифрова криміналістика”, “Безпека Інтернет-речей”, та включені в діючу ОПП.

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 розроблення, затвердження, моніторінг, періодичний перегляд та оновлення освітніх програм у ХНЕУ ім. С. Кузнеця здобувачі вищої освіти залучаються до процесу періодичного перегляду ОП та інших процедур забезпечення її якості через опитування. За результатами опитування оцінюється задоволеність здобувачами ОП та виявляються її недоліки, потім ця інформація використовуються для подальшого перегляду ОП на засіданнях робочої групи. Так, наприклад, за результатами опитування здобувачів за ОП «Кібербезпека» задоволеність якістю освіти складає 91,1 %.
За кожним навчальним семестром, проводиться опитування здобувачів вищої освіти «Дисципліна очима студента», результати якого дозволяють покращувати освітній процес за ОП, якість викладання навчальної дисицпліни, корегувати навантаження та інше. Останне опитування дозволило вдосконалити практичну складову освітніх компонент за рахунок введення в дію лабораторних занять в умовах використання Кіберполігону.
Згідно Положення про розроблення, затвердження, моніторінг, періодичний перегляд та оновлення освітніх програм у ХНЕУ ім. С. Кузнеця здобувачі вищої освіти входять до складу робочої групи та, таким чином, приймають участь в обговоренні оновлення ОП.
З метою періодичного перегляду ОП “Кібербезпека” на сайті кафедри (http://bit.ly/2PovXZy) є сторінка, яка дозволяє стейкхолдерам та здобувачам вищої освіти переглядати ОП “Кібербезпека” та надавати свої пропозиції щодо їх змін.

Яким чином студентське самоврядування бере участь у процедурах внутрішнього забезпечення

якості ОП

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).
Студентське самоврядування бере участь у процедурах внутрішнього забезпечення якості через залучення студентів до моніторингу та перегляді освітніх програм. Також студенти є членами Вченої ради ХНЕУ ім. С. Кузнеця (https://www.hneu.edu.ua/wp-content/uploads/2019/04/Sklad-chleniv-vchenoyi-rady- HNEU-S-Kuznetsya-2019.pdf), та входять до вченої ради факультету. Обрання делегатів конференції трудового колективу Університету з числа студентів здійснюється органами студентського самоврядування через прямі таємні вибори. Квота представників студентів, які навчаються в Університеті, розподіляється пропорційно до їх кількості на факультетах та становлять не менш як 15 відсотків. (п.п. 3.3, 3.12 Положення про конференцію трудового колективу https://www.hneu.edu.ua/wp-content/uploads/2018/11/Polozhennya-prokonferentsiyu-trudovoho-kolektyvu-2018.pdf)

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

Роботодавці (стейкхолдери) мають можливість безпосереньо подати пропозиції щодо ОПП "Кібербезпека" через відповідну сторінку сайту кафедри (http://bit.ly/3aRH1Ap). Відповідно до співпраці з Громадською спілкою «Харьківський кластер Інформаційних технологій» ОПП була розглянута та надана відповідна рецензія виконавчим директором Шаповал О.С. В склад робочої групи залучені провідні фахівці компанії ТОВ "Сайфер БІС" та компанії "Distributed Lab".

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 (https://bit.ly/3n2l4Wo) ЗВО забезпечує збір, аналіз і використання відповідної інформації для ефективного управління освітньою діяльністю та освітніми програмами на основі використання інформаційних систем. Отримані результати 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 та взаємодії з бізнес-структурами п. 2-3 (http://bit.ly/2WaKQwD) здійснюється опитування та 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 із захисту даних, адміністратор баз даних. Кафедра проводить аналіз конкурентоспроможності майбутніх випускників шляхом дослідження результатів ринку працю. У якості приклада можна навести аналітичний звіт "Розвиток української IT-індустрії" (https://bit.ly/2S6wdr1).

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

За результатами співбесід зі здобувачами вступу 2019 року другого (магістерського) рівня вищох освіти було виявлено, що недостатня увага приділяється набуттю компетентностей щодо практичної роботи з виявлення та аналізу сучасних загроз за допомогою програмних функцій Kali Linux, формуванню превентивних заходів. Зауваження здобувачів були враховані при оновденні (перегляді) ОП "Кібербезпека".
З метою покращення якости проведення практичних занять навчальних дисциплін, які пов'язані з відпрацюванням практичних питань кібернападу (захисту від кібернападу) на основі рішення Вченої ради університету сформований спеціалізований клас "Кіберполігон" на базі ОЦ-9.

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 ураховані під час удосконалення цієї ОП?

Акредитація ОПП "Кібербезпека" є первинною, тому зауваження (приписи) контролюючих органів відсутні, відповідно і заходи щодо їх усунення не зазначаються.

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

Учасники академічної спільноти змістовно залучаються до процедур внутрішнього забезпечення якості ОП наступним чином. В обговорені освітніх компонентів активну участь приймали завідувач кафедри безпеки інформаційних технологій Національного авіаційного університету (м. Київ) д.т.н., проф. Корченко О.Г, завідувач кафедри кібербезпеки та математичного моделювання Чернігівського державного технологічного університету (м.

Чернігів) д.пед.н., доц. Ткач Ю.М., завідувач кафедри комп'ютерних наук та автоматики університету Більсько-Бяла (Польща) проф., д.т.н. Карпінський М.П., які погодились включити в навчальний план дисципліни: "Інформаційна безпека телекомунікаційних та хмарних технологій", "Тестування на проникнення та етичний хакінг", "Безпека бездротових та мобільних мереж", "Безпека Web-ресурсів", "Цифрова криміналістика", "Безпека Інтернет-речей". З метою своєчасного врахування зауважень та пропозицій від академічної спільноти на сайті кафедри створена сторінка, яка дозволяє своєчасно ознайомитись з пропозиціями внесення змін до ОПП "Кібербезпека". Крім цього, є можливість відправити свої пропозиції та зауваження з використання веб-застосунку (http://bit.ly/3aRH1Ap).

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

Розподіл відповідальності між різними структурними підрозділами ЗВО у контексті здійснення процесів і процедур внутрішнього забезпечення якості освіти регламентується у відповідності до "Положення про систему внутрішнього забезпечення якості освітньої діяльності та якості вищої освіти", яка оприлюднена і є частиною стратегічного управління ХНЕУ ім. С. Кузнеця (https://bit.ly/3n2l4Wo). Розподіл відповідальності муж структурними підрозділами університету у контексті здійснення процедур внутрішнього забезпечення якості освіти (https://bit.ly/33ffSXr) такий: відділ забезпечення якості освіти та інноваційного розвитку (https://bit.ly/2Hy295o, с. 2-4), методичний відділ (http://bit.ly/3aSSAr5, с. 3-4), відділ електронних засобів навчання (http://bit.ly/2wT1shN, с. 3-5), навчальний відділ (http://bit.ly/3cWGfE6, с. 2-3), відділ маркетингу та корпоративних комунікацій (https://bit.ly/30iiWjq, с. 2-5), відділ допомоги працевлаштування студентів та взаємодії з бізнес-структурами (http://bit.ly/2WhU7TP, с. 2-5), відділ молодіжної політики та соціального розвитку (https://bit.ly/2EMqZh4), відділ міжнародних зв'язків (https://bit.ly/2S61zxS), бібліотека (https://bit.ly/36fibeK).

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 регулюються Статутом ХНЕУ ім. С. Кузнеця та іншими документами, які розміщені на сайті Університету https://www.hneu.edu.ua/dokumenty-universytetu/.

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/3aRH1Ap.

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/2uIE1at.
На сайті кафедри: http://bit.ly/3bJQECz.

11. Перспективи подальшого розвитку ОП

Якими загалом є сильні та слабкі сторони ОП?

Сильними сторонами ОПП "Кібербезпека" є впровадження сучасного підходу до підготовки магістрів з кібербезпеки, а саме поєднання набуття компетентностей з елементами науково-дослідницької роботи, що дозволяє працевлаштовуватись програмістами-аналітиками зі знанням сучасних засобів та програмних застосунків забезпечення безпеки. Проведення мастер класів спеціалістами компанії DistributedLab в рамках тренинг-курсу з блокчейн-технології дозволяє здобувачам вищої освіти отримувати знання в сучасних новітніх технологіях. Використання неформальних форм навчання згідно "Положенню про порядок визнання результатів неформальної та інформальної освіти у ХНЕУ ім. С. Кузнеця" (http://bit.ly/2VKT3HC), а саме навчальних курсів академії CISCO, дозволяє здобувачам вищої освіти отримувати компетентності, які притаманні лідерам в IT-індустрії, у сферах 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 сферы електронного документообігу. Майстер-класи з блокчейн-технології орієнтують здобувачів на сучасні задачі та новітні технології у сфері кібербезпеки. Програма двох дипломів другого (магістерського) рівня 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 і в Євросоюзі.
Слабкими сторонами ОП "Кібербезпека" є відсутність дуальної форми навчання за окремими планами, повязаними з прохожденням практики у підприємствах банківського сектору.

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;
- удосокналення 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” на базі кіберполігону, проведення кібернавчань;
- 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 ОП “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: 05.10.2020 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**	
Науково-дослідна практика	практика	*Науково-дослідна практика.pdf*	PoRmjbdyeEHBRFv8xP5bppu52vQSrJDQRiXvCEfhcrY=	*Vmware Player, Kali Linux*
Дипломний проєкт	підсумкова атестація	*Дипломний проєкт.pdf*	azcL3W7PQoZFW5fikOo7iG5f9jO7a0Hl3UtFvc9B4XM=	*Vmware Player, Kali Linux, Cisco Packet Tracer 7.2*
Переддипломна практика	практика	*Переддипломна практика.pdf*	piHiCf/yPiJ/PVUoCCGYtgHoBVcrEIbX1NuMtBPMgJM=	*Vmware Player, Kali Linux*
Мистецтво редагування та риторика	навчальна дисципліна	*Мистецтво редагування та риторика.pdf*	dJvNiRa8JbekA2YEmc1JFv9BfL/R7DnQsEXVkkQu9No=	
Захист інтелектуальної власності	навчальна дисципліна	*ЗАХИСТ ІНТЕЛЕКТУАЛЬНОЇ ВЛАСНОСТІ.pdf*	T21T1wY/BJRqFJ1BdpXJ3btQ6aiErZjdnlRPxLLo7w4=	
Бездротова та мобільна безпека	навчальна дисципліна	*БЕЗДРОТОВА ТА МОБІЛЬНА БЕЗПЕКА.pdf*	372QoOkkFGffbfDBv7PQ+HWlVwAFrFwIwsekKN2q4Bk=	*Vmware Player, Kali Linux*
Веб-безпека	навчальна дисципліна	*Веб-БЕЗПЕКА.pdf*	X5klz39cTyUq+CGD+Dz43BQMIpfJveeuDenkRGbG1Nw=	*Ресурси AWS Educate, Vmware Player або Oracle VM VirtualBox, Ubuntu Server, Windows Server – безкоштовна пробна версія*
Тестування на проникнення та етичний хакінг	навчальна дисципліна	*ТЕСТУВАННЯ НА ПРОНИКНЕННЯ ТА ЕТИЧНИЙ ХАКІНГ.pdf*	zC0do0QDXBjmxGjGGZZ/o773biVzoN6xwpMxy5YT1hI=	*Cisco Packet Tracer 7.2*
Цифрова криміналістика	навчальна дисципліна	*ЦИФРОВА КРИМІНАЛІСТИКА .pdf*	pQ7GUvdODqwBcDMo5t1+reD5lik81Owk2XvIU0g+4Y0=	*Cisco Packet Tracer 7.2*
Розширена мережева та хмарна безпека	навчальна дисципліна	*РОЗШИРЕНА МЕРЕЖЕВА ТА ХМАРНА БЕЗПЕКА.pdf*	L658phKCnwnubAO2OPeseWp9z1b/zOarX6UTqXEvWQ0=	*Ресурси AWS Educate, Vmware Player або Oracle VM VirtualBox, Ubuntu Server, Windows Server – безкоштовна пробна версія*
Безпека інтернет речей	навчальна дисципліна	*БЕЗПЕКА ІНТЕРНЕТ РЕЧЕЙ.pdf*	/PjBW4e1rshUPofzXCbyWQcjlCkU1iVhC9/qdT+YU3k=	*Cisco Packet Tracer 7.2*
Передові методики програмування	навчальна дисципліна	*ПЕРЕДОВІ МЕТОДИКИ ПРОГРАМУВАННЯ. pdf*	FYCtoFUmbRUhuiLTpPHbl5/E+wf0yFXRh7A9QPYvka0=	*NetBean, IntelliJ Idea, Visual Studio Code, PyCharm, XAAMP, Atom, mySQL, Android Studio*
Презентація та обробка знань	навчальна дисципліна	*ПРЕЗЕНТАЦІЯ ТА ОБРОБКА ЗНАНЬ.pdf*	qFgw3aRouRKYqIaf31M6CADFlPqwvmk9+ZLwtOw0fdg=	*Visual Prolog 9 Personal Edition*
Англійська мова	навчальна дисципліна	*Англійська мова.pdf*	uhYI6c7KsvCq3EDaVpsSTAb3rK+v2+hl/6ir7ntI1Yk=	
Господарське право	навчальна дисципліна	*ГОСПОДАРСЬКЕ ПРАВО.pdf*	SJN/YvnQHuGGFNOCwmPyOepdlRy84wuBUTJVEMTr554=	

* 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
72586	Мілов Олександр Володимирович	Професор, Основне місце роботи	Факультет економічної інформатики	Диплом кандидата наук ТН 094834, виданий 12.11.1986, Атестат доцента ДЦ 039210, виданий 04.07.1991, Атестат професора АП 001430, виданий 16.12.2019	38	Презентація та обробка знань	Відповідно до пункту 30 Ліцензійних вимог п. 1-4, 6, 8, 10, 13, 15-16
355403	Ткачов Андрій Михайлович	Доцент, Основне місце роботи	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	Передові методики програмування	Відповідно до пункту 30 Ліцензійних вимог п. 2, 12, 15, 17
72586	Мілов Олександр Володимирович	Професор, Основне місце роботи	Факультет економічної інформатики	Диплом кандидата наук ТН 094834, виданий 12.11.1986, Атестат доцента ДЦ 039210, виданий 04.07.1991, Атестат професора АП 001430, виданий 16.12.2019	38	Цифрова криміналістика	Відповідно до пункту 30 Ліцензійних вимог п. 1-4, 6, 8, 10, 13, 15-16
107556	Євсеєв Сергій Петрович	Завідувач кафедри, Основне місце роботи	Факультет економічної інформатики	Диплом доктора наук ДД 007606, виданий 05.07.2018, Диплом кандидата наук ДК 035254, виданий 04.07.2006, Атестат доцента 12ДЦ 034106, виданий 25.01.2013, Атестат професора АП 001633,	34	Безпека інтернет речей	Відповідно до пункту 30 Ліцензійних вимог П. 1-3, 7-8, 10, 12-15, 17

				виданий 26.02.2020, Атестат старшого наукового співробітника (старшого дослідника) АС 007292, виданий 14.04.2010			
306980	Іванова Ірина Борисівна	Професор, Основне місце роботи	Факультет економіки і права	Диплом доктора наук ДД 007648, виданий 05.07.2018, Диплом кандидата наук ДК 051516, виданий 28.04.2009, Атестат доцента 12ДЦ 044394, виданий 29.09.2015	25	Мистецтво редагування та риторика	Відповідно до пункту 30 Ліцензійних вимог відповідає 12 пунктам (П. 1, 2, 3, 4, 5, 7, 8, 11, 13, 14, 16, 17)
39891	Борова Тетяна Анатоліївна	Завідувач кафедри, Основне місце роботи	Факультет міжнародних економічних відносин	Диплом доктора наук ДД 001158, виданий 26.09.2012, Диплом кандидата наук ДК 011276, виданий 04.07.2001, Атестат доцента 02ДЦ 000371, виданий 24.12.2003, Атестат професора 12ПР 008835, виданий 04.07.2013	25	Англійська мова	Відповідає пунктам 1,2,3,4,5,8,10,11,13,15,17 п.п 30 Ліцензійних умов
119185	Хвостенко Владислав Сергійович	Доцент 0,5 ст., Основне місце роботи	Факультет економічної інформатики	Диплом бакалавра, Харківський національний економічний університет, рік закінчення: 2005, спеціальність: 0501 Економіка і підприємництво, Диплом спеціаліста, Харківський національний економічний університет, рік закінчення: 2007, спеціальність: 050107 Економічна статистика, Диплом магістра, Харківський національний економічний університет, рік закінчення: 2006,	13	Захист інтелектуальної власності	Відповідно до пункту 30 Ліцензійних вимог П. 1-3, 8, 9, 12, 13, 15, 17

				спеціальність: 050104 Фінанси, Диплом кандидата наук ДК 008014, виданий 26.09.2012, Атестат доцента АД 003303, виданий 15.10.2019			
119185	Хвостенко Владислав Сергійович	Доцент 0,5 ст., Основне місце роботи	Факультет економічної інформатики	Диплом бакалавра, Харківський національний економічний університет, рік закінчення: 2005, спеціальність: 0501 Економіка і підприємництво, Диплом спеціаліста, Харківський національний економічний університет, рік закінчення: 2007, спеціальність: 050107 Економічна статистика, Диплом магістра, Харківський національний економічний університет, рік закінчення: 2006, спеціальність: 050104 Фінанси, Диплом кандидата наук ДК 008014, виданий 26.09.2012, Атестат доцента АД 003303, виданий 15.10.2019	13	Господарське право	Відповідно до пункту 30 Ліцензійних вимог П. 1-3, 8, 9, 12, 13, 15, 17
189990	Алексієв Володимир Олегович	Професор, Основне місце роботи	Факультет економічної інформатики	Диплом доктора наук ДД 008806, виданий 10.11.2010, Диплом кандидата наук ДК 003162, виданий 12.05.1999, Атестат доцента ДЦ 010437, виданий 17.02.2005, Атестат професора 12ПР 008834, виданий 04.07.2013, Атестат	22	Веб-безпека	Відповідно до пункту 30 Ліцензійних вимог п. 1-3, 8, 11-13, 15-17

				старшого наукового співробітника (старшого дослідника) АС 004798, виданий 15.12.2005			
273533	Корольов Роман Володимирович	Доцент, Основне місце роботи	Факультет економічної інформатики	Диплом кандидата наук ДК 054389, виданий 08.07.2009	25	Бездротова та мобільна безпека	Відповідно до пункту 30 Ліцензійних вимог п. 1-3, 12, 17
189990	Алексієв Володимир Олегович	Професор, Основне місце роботи	Факультет економічної інформатики	Диплом доктора наук ДД 008806, виданий 10.11.2010, Диплом кандидата наук ДК 003162, виданий 12.05.1999, Атестат доцента ДЦ 010437, виданий 17.02.2005, Атестат професора 12ПР 008834, виданий 04.07.2013, Атестат старшого наукового співробітника (старшого дослідника) АС 004798, виданий 15.12.2005	22	Розширена мережева та хмарна безпека	Відповідно до пункту 30 Ліцензійних вимог п. 1-3, 8, 11-13, 15-17
189990	Алексієв Володимир Олегович	Професор, Основне місце роботи	Факультет економічної інформатики	Диплом доктора наук ДД 008806, виданий 10.11.2010, Диплом кандидата наук ДК 003162, виданий 12.05.1999, Атестат доцента ДЦ 010437, виданий 17.02.2005, Атестат професора 12ПР 008834, виданий 04.07.2013, Атестат старшого наукового співробітника (старшого дослідника) АС 004798, виданий 15.12.2005	22	Безпека інтернет речей	Відповідно до пункту 30 Ліцензійних вимог п. 1-3, 8, 11-13, 15-17
72586	Мілов Олександр Володимирович	Професор, Основне місце роботи	Факультет економічної інформатики	Диплом кандидата наук ТН 094834, виданий 12.11.1986, Атестат	38	Тестування на проникнення та етичний хакінг	Відповідно до пункту 30 Ліцензійних вимог п. 1-4, 6, 8, 10, 13, 15-16

				доцента ДЦ 039210, виданий 04.07.1991, Атестат професора АП 001430, виданий 16.12.2019			

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

Програмні результати навчання ОП	**ПРН відповідає результату навчання, визначеному стандартом вищої освіти (або охоплює його)**	**Обов'язкові освітні компоненти, що забезпечують ПРН**	**Методи навчання**	**Форми та методи оцінювання**
ПРН-1 – постійно вдосконалювати та застосовувати знання державної та іноземних мов з метою забезпечення ефективності професійної комунікації; ПРН-2 – планувати, аналізувати та організовувати власну професійну діяльність, обирати оптимальні методи та способи розв'язування складних спеціалізованих задач та практичних проблем у професійній діяльності, оцінювати їхню ефективність; ПРН-3 – аналізувати та адаптувати професійну діяльність в умовах частої зміни та прогресу інформаційних технологій, що застосовуються в організації, планувати і прогнозувати кінцевий результат; ПРН-4 – діяти на основі законодавчої, нормативно-правової бази України та вимог відповідних	☐	Презентація та обробка знань	Лекція, лабораторні заняття	Захист лабораторних завдань, контрольна робота, залік

міжнародних стандартів і практик щодо здійснення професійної діяльності; *ПРН-5 – аналізувати та впроваджувати процедури контуру бізнес-процесів підприємства, що базуються на національних та міжнародних стандартах інформаційної та/або кібербезпеки;* *ПРН-6 – розробляти, впроваджувати та супроводжувати програмні та програмно-апаратні комплекси засобів інформаційної безпеки та/або кібербезпеки в інформаційно-комунікаційних (автоматизованих) системах та у інфраструктурі організації в цілому;* *ПРН-7 – виявляти, описувати та використовувати систему аналізу зв'язків між інформаційними потоками та ресурсами (в.ч. критичними) в контурі бізнес-процесів організації (підприємства);* *ПРН-8 – проектувати, впроваджувати, та супроводжувати системи захисту інформаційних систем та ресурсів, інфраструктури установи, розробляти сучасні архітектури використання інформаційних технологій та їх безпеки (архітектури безпеки, моделі інформаційної безпеки, режими безпечного функціонування, методи оцінки якості функціонування відкритих та закритих систем, тощо);* *ПРН-9 – проектувати, впроваджувати,*					

супроводжувати системи та комплекси (програмні, програмно-апаратні) захисту застосунків (в.ч. веб-застосунків) з метою забезпечення якісного функціонування інформаційно-комунікаційних систем, згідно встановленої політики інформаційної безпеки та/або кібербезпеки; ПРН-10 – аналізувати та впроваджувати системи класифікації загроз інформаційним ресурсам (активам), проводити їх ранжування у відповідності до різних класів параметрів (за ймовірністю появи, вартістю, якісними і кількісними показниками, тощо); ПРН-11 – планувати, впроваджувати, забезпечувати та контролювати безперервність бізнес/операційних процесів організації (підприємства), згідно встановленої політики інформаційної безпеки та/або кібербезпеки і стратегії організації (підприємства); ПРН-12 – розробляти, планувати, аналізувати та впроваджувати систему доступу до інформаційних ресурсів, інформаційно-комунікаційних систем (вузлів доступу до глобальних мереж, програмно-апаратних комплексів, підсистем, програмного забезпечення, тощо), згідно встановленої політики інформаційної безпеки та/або кібербезпеки;					

ПРН-13 – розробляти, планувати, аналізувати та впроваджувати систему аудиту і контролю ефективності функціонування інформаційно-комунікаційних систем (вузлів доступу до глобальних мереж, програмно-апаратних комплексів, підсистем, тощо), згідно встановленої політики інформаційної безпеки та/або кібербезпеки; *ПРН-14 – розробляти та впроваджувати заходи протидії кіберінцидентам, а також аналізувати, здійснювати процедури управління та контролю інцидентами, організовувати та проводити розслідування, надавати рекомендації щодо заходів їх попередження та протидії;* *ПРН-15 – розробляти, впроваджувати та супроводжувати процеси управління процедурами ідентифікації, автентифікації, авторизації користувачів і інформаційних ресурсів, операційних процесів інфраструктури організації (підприємства), згідно встановленої політики інформаційної безпеки та кібербезпеки;* *ПРН-16 – розробляти, впроваджувати, та організовувати реалізацію процесів з використанням методів та засобів криптографічного та технічного захисту інформації на об'єктах інформаційної діяльності, згідно встановленої політики*					

інформаційної безпеки та/або кібербезпеки; ПРН-17 – розробляти, впроваджувати та супроводжувати процеси виявлення та ідентифікації кібератак, їх аналізу та впроваджувати процедури реагування і управління інцидентами інформаційної і/або кібербезпеки; ПРН-18 – проводити науково-освітню діяльність, розробляти та впроваджувати систему науково-прикладних досліджень в галузі захисту інформації у відповідності до сучасних норм, вимог, внутрішніх правил і політики безпеки організації (підприємства);				
ПРН-1 – постійно вдосконалювати та застосовувати знання державної та іноземних мов з метою забезпечення ефективності професійної комунікації; ПРН-2 – планувати, аналізувати та організовувати власну професійну діяльність, обирати оптимальні методи та способи розв'язування складних спеціалізованих задач та практичних проблем у професійній діяльності, оцінювати їхню ефективність; ПРН-3 – аналізувати та адаптувати професійну діяльність в умовах частої зміни та прогресу інформаційних технологій, що застосовуються в організації, планувати і прогнозувати кінцевий результат; ПРН-5 – аналізувати та	☐	Розширена мережева та хмарна безпека	Лекція, лабораторні заняття	Захист лабораторних завдань, контрольна робота, екзамен

впроваджувати процедури контуру бізнес-процесів підприємства, що базуються на національних та міжнародних стандартах інформаційної та/або кібербезпеки; *ПРН-6 – розробляти, впроваджувати та супроводжувати програмні та програмно-апаратні комплекси засобів інформаційної безпеки та/або кібербезпеки в інформаційно-комунікаційних (автоматизованих) системах та у інфраструктурі організації в цілому;* *ПРН-7 – виявляти, описувати та використовувати систему аналізу зв'язків між інформаційними потоками та ресурсами (в.ч. критичними) в контурі бізнес-процесів організації (підприємства);* *ПРН-8 – проектувати, впроваджувати, та супроводжувати системи захисту інформаційних систем та ресурсів, інфраструктури установи, розробляти сучасні архітектури використання інформаційних технологій та їх безпеки (архітектури безпеки, моделі інформаційної безпеки, режими безпечного функціонування, методи оцінки якості функціонування відкритих та закритих систем, тощо);* *ПРН-9 – проектувати, впроваджувати, супроводжувати системи та комплекси (програмні, програмно-апаратні) захисту застосунків (в.ч. веб-застосунків) з*					

метою забезпечення якісного функціонування інформаційно-комунікаційних систем, згідно встановленої політики інформаційної безпеки та/або кібербезпеки; *ПРН-10 – аналізувати та впроваджувати системи класифікації загроз інформаційним ресурсам (активам), проводити їх ранжування у відповідності до різних класів параметрів (за ймовірністю появи, вартістю, якісними і кількісними показниками, тощо);* *ПРН-11 – планувати, впроваджувати, забезпечувати та контролювати безперервність бізнес/операційних процесів організації (підприємства), згідно встановленої політики інформаційної безпеки та/або кібербезпеки і стратегії організації (підприємства);* *ПРН-12 – розробляти, планувати, аналізувати та впроваджувати систему доступу до інформаційних ресурсів, інформаційно-комунікаційних систем (вузлів доступу до глобальних мереж, програмно-апаратних комплексів, підсистем, програмного забезпечення, тощо), згідно встановленої політики інформаційної безпеки та/або кібербезпеки;* *ПРН-13 – розробляти, планувати, аналізувати та впроваджувати систему аудиту і контролю ефективності*					

функціонування інформаційно-комунікаційних систем (вузлів доступу до глобальних мереж, програмно-апаратних комплексів, підсистем, тощо), згідно встановленої політики інформаційної безпеки та/або кібербезпеки; ПРН-14 – розробляти та впроваджувати заходи протидії кіберінцидентам, а також аналізувати, здійснювати процедури управління та контролю інцидентами, організовувати та проводити розслідування, надавати рекомендації щодо заходів їх попередження та протидії; ПРН-15 – розробляти, впроваджувати та супроводжувати процеси управління процедурами ідентифікації, автентифікації, авторизації користувачів і інформаційних ресурсів, операційних процесів інфраструктури організації (підприємства), згідно встановленої політики інформаційної безпеки та кібербезпеки; ПРН-19 – розробляти, впроваджувати, супроводжувати систему управління персоналом з інформаційної безпеки та/або кібербезпеки на підприємстві;				
ПРН-1 – постійно вдосконалювати та застосовувати знання державної та іноземних мов з метою забезпечення ефективності професійної комунікації; ПРН-2 –	☐	Господарське право	Лекція, практичні заняття	захист індивідуальних завдань, тестування, письмові контрольні роботи, участь у конференціях, олімпіадах, конкурсах, залік

планувати, аналізувати та організовувати власну професійну діяльність, обирати оптимальні методи та способи розв'язування складних спеціалізованих задач та практичних проблем у професійній діяльності, оцінювати їхню ефективність; ПРН-3 – аналізувати та адаптувати професійну діяльність в умовах частої зміни та прогресу інформаційних технологій, що застосовуються в організації, планувати і прогнозувати кінцевий результат; ПРН-4 – діяти на основі законодавчої, нормативно-правової бази України та вимог відповідних міжнародних стандартів і практик щодо здійснення професійної діяльності; ПРН-5 – аналізувати та впроваджувати процедури контуру бізнес-процесів підприємства, що базуються на національних та міжнародних стандартах інформаційної та/або кібербезпеки; ПРН-6 – розробляти, впроваджувати та супроводжувати програмні та програмно-апаратні комплекси засобів інформаційної безпеки та/або кібербезпеки в інформаційно-комунікаційних (автоматизованих) системах та у інфраструктурі організації в цілому; ПРН-8 – проектувати, впроваджувати, та					

супроводжувати системи захисту інформаційних систем та ресурсів, інфраструктури установи, розробляти сучасні архітектури використання інформаційних технологій та їх безпеки (архітектури безпеки, моделі інформаційної безпеки, режими безпечного функціонування, методи оцінки якості функціонування відкритих та закритих систем, тощо); *ПРН-9 – проектувати, впроваджувати, супроводжувати системи та комплекси (програмні, програмно-апаратні) захисту застосунків (в.ч. веб-застосунків) з метою забезпечення якісного функціонування інформаційно-комунікаційних систем, згідно встановленої політики інформаційної безпеки та/або кібербезпеки;* *ПРН-10 – аналізувати та впроваджувати системи класифікації загроз інформаційним ресурсам (активам), проводити їх ранжування у відповідності до різних класів параметрів (за ймовірністю появи, вартістю, якісними і кількісними показниками, тощо);* *ПРН-11 – планувати, впроваджувати, забезпечувати та контролювати безперервність бізнес/операційних процесів організації (підприємства), згідно встановленої політики інформаційної безпеки та/або кібербезпеки і*					

стратегії організації (підприємства); ПРН-12 – розробляти, планувати, аналізувати та впроваджувати систему доступу до інформаційних ресурсів, інформаційно-комунікаційних систем (вузлів доступу до глобальних мереж, програмно-апаратних комплексів, підсистем, програмного забезпечення, тощо), згідно встановленої політики інформаційної безпеки та/або кібербезпеки; ПРН-13 – розробляти, планувати, аналізувати та впроваджувати систему аудиту і контролю ефективності функціонування інформаційно-комунікаційних систем (вузлів доступу до глобальних мереж, програмно-апаратних комплексів, підсистем, тощо), згідно встановленої політики інформаційної безпеки та/або кібербезпеки; ПРН-14 – розробляти та впроваджувати заходи протидії кіберінцидентам, а також аналізувати, здійснювати процедури управління та контролю інцидентами, організовувати та проводити розслідування, надавати рекомендації щодо заходів їх попередження та протидії; ПРН-15 – розробляти, впроваджувати та супроводжувати процеси управління процедурами ідентифікації, автентифікації, авторизації					

користувачів і інформаційних ресурсів, операційних процесів інфраструктури організації (підприємства), згідно встановленої політики інформаційної безпеки та кібербезпеки; ПРН-16 – розробляти, впроваджувати, та організовувати реалізацію процесів з використанням методів та засобів криптографічного та технічного захисту інформації на об'єктах інформаційної діяльності, згідно встановленої політики інформаційної безпеки та/або кібербезпеки; ПРН-17 – розробляти, впроваджувати та супроводжувати процеси виявлення та ідентифікації кібератак, їх аналізу та впроваджувати процедури реагування і управління інцидентами інформаційної і/або кібербезпеки; ПРН-18 – проводити науково-освітню діяльність, розробляти та впроваджувати систему науково-прикладних досліджень в галузі захисту інформації у відповідності до сучасних норм, вимог, внутрішніх правил і політики безпеки організації (підприємства); ПРН-19 – розробляти, впроваджувати, супроводжувати систему управління персоналом з інформаційної безпеки та/або кібербезпеки на підприємстві; ПРН-20 – усвідомлювати цінності громадянського (вільного демократичного) суспільства та необхідність його					

сталого розвитку, верховенства права, прав і свобод людини і громадянина в Україні.				
ПРН-1 – постійно вдосконалювати та застосовувати знання державної та іноземних мов з метою забезпечення ефективності професійної комунікації; *ПРН-2 – планувати, аналізувати та організовувати власну професійну діяльність, обирати оптимальні методи та способи розв'язування складних спеціалізованих задач та практичних проблем у професійній діяльності, оцінювати їхню ефективність;* *ПРН-3 – аналізувати та адаптувати професійну діяльність в умовах частої зміни та прогресу інформаційних технологій, що застосовуються в організації, планувати і прогнозувати кінцевий результат;* *ПРН-4 – діяти на основі законодавчої, нормативно-правової бази України та вимог відповідних міжнародних стандартів і практик щодо здійснення професійної діяльності;* *ПРН-5 – аналізувати та впроваджувати процедури контуру бізнес-процесів підприємства, що базуються на національних та міжнародних стандартах інформаційної та/або кібербезпеки;* *ПРН-6 – розробляти, впроваджувати та супроводжувати*	☐	Науково-дослідна практика	Самостійна робота	Захист звіту з науково-дослідної практики

програмні та програмно-апаратні комплекси засобів інформаційної безпеки та/або кібербезпеки в інформаційно-комунікаційних (автоматизованих) системах та у інфраструктурі організації в цілому; *ПРН-7 – виявляти, описувати та використовувати систему аналізу зв'язків між інформаційними потоками та ресурсами (в.ч. критичними) в контурі бізнес-процесів організації (підприємства);* *ПРН-8 – проектувати, впроваджувати, та супроводжувати системи захисту інформаційних систем та ресурсів, інфраструктури установи, розробляти сучасні архітектури використання інформаційних технологій та їх безпеки (архітектури безпеки, моделі інформаційної безпеки, режими безпечного функціонування, методи оцінки якості функціонування відкритих та закритих систем, тощо);* *ПРН-9 – проектувати, впроваджувати, супроводжувати системи та комплекси (програмні, програмно-апаратні) захисту застосунків (в.ч. веб-застосунків) з метою забезпечення якісного функціонування інформаційно-комунікаційних систем, згідно встановленої політики інформаційної безпеки та/або кібербезпеки;* *ПРН-10 – аналізувати та впроваджувати*					

системи класифікації загроз інформаційним ресурсам (активам), проводити їх ранжування у відповідності до різних класів параметрів (за ймовірністю появи, вартістю, якісними і кількісними показниками, тощо); *ПРН-11 – планувати, впроваджувати, забезпечувати та контролювати безперервність бізнес/операційних процесів організації (підприємства), згідно встановленої політики інформаційної безпеки та/або кібербезпеки і стратегії організації (підприємства);* *ПРН-12 – розробляти, планувати, аналізувати та впроваджувати систему доступу до інформаційних ресурсів, інформаційно-комунікаційних систем (вузлів доступу до глобальних мереж, програмно-апаратних комплексів, підсистем, програмного забезпечення, тощо), згідно встановленої політики інформаційної безпеки та/або кібербезпеки;* *ПРН-13 – розробляти, планувати, аналізувати та впроваджувати систему аудиту і контролю ефективності функціонування інформаційно-комунікаційних систем (вузлів доступу до глобальних мереж, програмно-апаратних комплексів, підсистем, тощо), згідно встановленої політики інформаційної безпеки та/або кібербезпеки;*					

ПРН-14 – розробляти та впроваджувати заходи протидії кіберінцидентам, а також аналізувати, здійснювати процедури управління та контролю інцидентами, організовувати та проводити розслідування, надавати рекомендації щодо заходів їх попередження та протидії; *ПРН-15 – розробляти, впроваджувати та супроводжувати процеси управління процедурами ідентифікації, автентифікації, авторизації користувачів і інформаційних ресурсів, операційних процесів інфраструктури організації (підприємства), згідно встановленої політики інформаційної безпеки та кібербезпеки;* *ПРН-16 – розробляти, впроваджувати, та організовувати реалізацію процесів з використанням методів та засобів криптографічного та технічного захисту інформації на об'єктах інформаційної діяльності, згідно встановленої політики інформаційної безпеки та/або кібербезпеки;* *ПРН-17 – розробляти, впроваджувати та супроводжувати процеси виявлення та ідентифікації кібератак, їх аналізу та впроваджувати процедури реагування і управління інцидентами інформаційної і/або кібербезпеки;* *ПРН-18 – проводити науково-освітню діяльність, розробляти та*					

впроваджувати систему науково-прикладних досліджень в галузі захисту інформації у відповідності до сучасних норм, вимог, внутрішніх правил і політики безпеки організації (підприємства); ПРН-19 – розробляти, впроваджувати, супроводжувати систему управління персоналом з інформаційної безпеки та/або кібербезпеки на підприємстві; ПРН-20 – усвідомлювати цінності громадянського (вільного демократичного) суспільства та необхідність його сталого розвитку, верховенства права, прав і свобод людини і громадянина в Україні.				
ПРН-1 – постійно вдосконалювати та застосовувати знання державної та іноземних мов з метою забезпечення ефективності професійної комунікації; ПРН-2 – планувати, аналізувати та організовувати власну професійну діяльність, обирати оптимальні методи та способи розв'язування складних спеціалізованих задач та практичних проблем у професійній діяльності, оцінювати їхню ефективність; ПРН-3 – аналізувати та адаптувати професійну діяльність в умовах частої зміни та прогресу інформаційних технологій, що застосовуються в організації, планувати і прогнозувати кінцевий	☐	Дипломний проєкт	Самостійна робота	Захист дипломного проекту (дипломної роботи)

результат; *ПРН-4 – діяти на основі законодавчої, нормативно-правової бази України та вимог відповідних міжнародних стандартів і практик щодо здійснення професійної діяльності;* *ПРН-5 – аналізувати та впроваджувати процедури контуру бізнес-процесів підприємства, що базуються на національних та міжнародних стандартах інформаційної та/або кібербезпеки;* *ПРН-6 – розробляти, впроваджувати та супроводжувати програмні та програмно-апаратні комплекси засобів інформаційної безпеки та/або кібербезпеки в інформаційно-комунікаційних (автоматизованих) системах та у інфраструктурі організації в цілому;* *ПРН-7 – виявляти, описувати та використовувати систему аналізу зв'язків між інформаційними потоками та ресурсами (в.ч. критичними) в контурі бізнес-процесів організації (підприємства);* *ПРН-8 – проектувати, впроваджувати, та супроводжувати системи захисту інформаційних систем та ресурсів, інфраструктури установи, розробляти сучасні архітектури використання інформаційних технологій та їх безпеки (архітектури безпеки, моделі інформаційної безпеки, режими безпечного функціонування, методи оцінки*					

якості функціонування відкритих та закритих систем, тощо); *ПРН-9 – проектувати, впроваджувати, супроводжувати системи та комплекси (програмні, програмно-апаратні) захисту застосунків (в.ч. веб-застосунків) з метою забезпечення якісного функціонування інформаційно-комунікаційних систем, згідно встановленої політики інформаційної безпеки та/або кібербезпеки;* *ПРН-10 – аналізувати та впроваджувати системи класифікації загроз інформаційним ресурсам (активам), проводити їх ранжування у відповідності до різних класів параметрів (за ймовірністю появи, вартістю, якісними і кількісними показниками, тощо);* *ПРН-11 – планувати, впроваджувати, забезпечувати та контролювати безперервність бізнес/операційних процесів організації (підприємства), згідно встановленої політики інформаційної безпеки та/або кібербезпеки і стратегії організації (підприємства);* *ПРН-12 – розробляти, планувати, аналізувати та впроваджувати систему доступу до інформаційних ресурсів, інформаційно-комунікаційних систем (вузлів доступу до глобальних мереж, програмно-апаратних комплексів, підсистем,*					

програмного забезпечення, тощо), згідно встановленої політики інформаційної безпеки та/або кібербезпеки; ПРН-13 – розробляти, планувати, аналізувати та впроваджувати систему аудиту і контролю ефективності функціонування інформаційно-комунікаційних систем (вузлів доступу до глобальних мереж, програмно-апаратних комплексів, підсистем, тощо), згідно встановленої політики інформаційної безпеки та/або кібербезпеки; ПРН-14 – розробляти та впроваджувати заходи протидії кіберінцидентам, а також аналізувати, здійснювати процедури управління та контролю інцидентами, організовувати та проводити розслідування, надавати рекомендації щодо заходів їх попередження та протидії; ПРН-15 – розробляти, впроваджувати та супроводжувати процеси управління процедурами ідентифікації, автентифікації, авторизації користувачів і інформаційних ресурсів, операційних процесів інфраструктури організації (підприємства), згідно встановленої політики інформаційної безпеки та кібербезпеки; ПРН-16 – розробляти, впроваджувати, та організовувати реалізацію процесів з використанням методів та засобів					

криптографічного та технічного захисту інформації на об'єктах інформаційної діяльності, згідно встановленої політики інформаційної безпеки та/або кібербезпеки; ПРН-17 – розробляти, впроваджувати та супроводжувати процеси виявлення та ідентифікації кібератак, їх аналізу та впроваджувати процедури реагування і управління інцидентами інформаційної і/або кібербезпеки; ПРН-18 – проводити науково-освітню діяльність, розробляти та впроваджувати систему науково-прикладних досліджень в галузі захисту інформації у відповідності до сучасних норм, вимог, внутрішніх правил і політики безпеки організації (підприємства); ПРН-19 – розробляти, впроваджувати, супроводжувати систему управління персоналом з інформаційної безпеки та/або кібербезпеки на підприємстві; ПРН-20 – усвідомлювати цінності громадянського (вільного демократичного) суспільства та необхідність його сталого розвитку, верховенства права, прав і свобод людини і громадянина в Україні.				
ПРН-1 – постійно вдосконалювати та застосовувати знання державної та іноземних мов з метою забезпечення ефективності професійної комунікації; ПРН-2 – планувати, аналізувати та	☐	Переддипломна практика	Самостійна робота	Захист звіту

організовувати власну професійну діяльність, обирати оптимальні методи та способи розв'язування складних спеціалізованих задач та практичних проблем у професійній діяльності, оцінювати їхню ефективність; *ПРН-3 – аналізувати та адаптувати професійну діяльність в умовах частої зміни та прогресу інформаційних технологій, що застосовуються в організації, планувати і прогнозувати кінцевий результат;* *ПРН-4 – діяти на основі законодавчої, нормативно-правової бази України та вимог відповідних міжнародних стандартів і практик щодо здійснення професійної діяльності;* *ПРН-5 – аналізувати та впроваджувати процедури контуру бізнес-процесів підприємства, що базуються на національних та міжнародних стандартах інформаційної та/або кібербезпеки;* *ПРН-6 – розробляти, впроваджувати та супроводжувати програмні та програмно-апаратні комплекси засобів інформаційної безпеки та/або кібербезпеки в інформаційно-комунікаційних (автоматизованих) системах та у інфраструктурі організації в цілому;* *ПРН-7 – виявляти, описувати та використовувати систему аналізу зв'язків між інформаційними*					

потоками та ресурсами (в.ч. критичними) в контурі бізнес-процесів організації (підприємства); *ПРН-8 – проектувати, впроваджувати, та супроводжувати системи захисту інформаційних систем та ресурсів, інфраструктури установи, розробляти сучасні архітектури використання інформаційних технологій та їх безпеки (архітектури безпеки, моделі інформаційної безпеки, режими безпечного функціонування, методи оцінки якості функціонування відкритих та закритих систем, тощо);* *ПРН-9 – проектувати, впроваджувати, супроводжувати системи та комплекси (програмні, програмно-апаратні) захисту застосунків (в.ч. веб-застосунків) з метою забезпечення якісного функціонування інформаційно-комунікаційних систем, згідно встановленої політики інформаційної безпеки та/або кібербезпеки;* *ПРН-10 – аналізувати та впроваджувати системи класифікації загроз інформаційним ресурсам (активам), проводити їх ранжування у відповідності до різних класів параметрів (за ймовірністю появи, вартістю, якісними і кількісними показниками, тощо);* *ПРН-11 – планувати, впроваджувати, забезпечувати та*					

контролювати безперервність бізнес/операційних процесів організації (підприємства), згідно встановленої політики інформаційної безпеки та/або кібербезпеки і стратегії організації (підприємства); ПРН-12 – розробляти, планувати, аналізувати та впроваджувати систему доступу до інформаційних ресурсів, інформаційно-комунікаційних систем (вузлів доступу до глобальних мереж, програмно-апаратних комплексів, підсистем, програмного забезпечення, тощо), згідно встановленої політики інформаційної безпеки та/або кібербезпеки; ПРН-13 – розробляти, планувати, аналізувати та впроваджувати систему аудиту і контролю ефективності функціонування інформаційно-комунікаційних систем (вузлів доступу до глобальних мереж, програмно-апаратних комплексів, підсистем, тощо), згідно встановленої політики інформаційної безпеки та/або кібербезпеки; ПРН-14 – розробляти та впроваджувати заходи протидії кіберінцидентам, а також аналізувати, здійснювати процедури управління та контролю інцидентами, організовувати та проводити розслідування, надавати рекомендації щодо заходів їх попередження та протидії;					

ПРН-15 – розробляти, впроваджувати та супроводжувати процеси управління процедурами ідентифікації, автентифікації, авторизації користувачів і інформаційних ресурсів, операційних процесів інфраструктури організації (підприємства), згідно встановленої політики інформаційної безпеки та кібербезпеки; *ПРН-16 – розробляти, впроваджувати, та організовувати реалізацію процесів з використанням методів та засобів криптографічного та технічного захисту інформації на об'єктах інформаційної діяльності, згідно встановленої політики інформаційної безпеки та/або кібербезпеки;* *ПРН-17 – розробляти, впроваджувати та супроводжувати процеси виявлення та ідентифікації кібератак, їх аналізу та впроваджувати процедури реагування і управління інцидентами інформаційної і/або кібербезпеки;* *ПРН-18 – проводити науково-освітню діяльність, розробляти та впроваджувати систему науково-прикладних досліджень в галузі захисту інформації у відповідності до сучасних норм, вимог, внутрішніх правил і політики безпеки організації (підприємства);* *ПРН-19 – розробляти, впроваджувати, супроводжувати систему управління персоналом з інформаційної безпеки та/або*					

кібербезпеки на підприємстві; ПРН-20 – усвідомлювати цінності громадянського (вільного демократичного) суспільства та необхідність його сталого розвитку, верховенства права, прав і свобод людини і громадянина в Україні.				
ПРН-1 – постійно вдосконалювати та застосовувати знання державної та іноземних мов з метою забезпечення ефективності професійної комунікації; ПРН-2 – планувати, аналізувати та організовувати власну професійну діяльність, обирати оптимальні методи та способи розв'язування складних спеціалізованих задач та практичних проблем у професійній діяльності, оцінювати їхню ефективність; ПРН-3 – аналізувати та адаптувати професійну діяльність в умовах частої зміни та прогресу інформаційних технологій, що застосовуються в організації, планувати і прогнозувати кінцевий результат; ПРН-4 – діяти на основі законодавчої, нормативно-правової бази України та вимог відповідних міжнародних стандартів і практик щодо здійснення професійної діяльності; ПРН-5 – аналізувати та впроваджувати процедури контуру бізнес-процесів підприємства, що базуються на національних та	☐	Мистецтво редагування та риторика	Лекція, практичні заняття	Захист індивідуальних завдань, тестування, письмові контрольні роботи, участь у конференціях, олімпіадах, конкурсах, залік

міжнародних стандартах інформаційної та/або кібербезпеки; ПРН-6 – розробляти, впроваджувати та супроводжувати програмні та програмно-апаратні комплекси засобів інформаційної безпеки та/або кібербезпеки в інформаційно-комунікаційних (автоматизованих) системах та у інфраструктурі організації в цілому; ПРН-8 – проектувати, впроваджувати, та супроводжувати системи захисту інформаційних систем та ресурсів, інфраструктури установи, розробляти сучасні архітектури використання інформаційних технологій та їх безпеки (архітектури безпеки, моделі інформаційної безпеки, режими безпечного функціонування, методи оцінки якості функціонування відкритих та закритих систем, тощо); ПРН-9 – проектувати, впроваджувати, супроводжувати системи та комплекси (програмні, програмно-апаратні) захисту застосунків (в.ч. веб-застосунків) з метою забезпечення якісного функціонування інформаційно-комунікаційних систем, згідно встановленої політики інформаційної безпеки та/або кібербезпеки; ПРН-10 – аналізувати та впроваджувати системи класифікації загроз інформаційним					

ресурсам (активам), проводити їх ранжування у відповідності до різних класів параметрів (за ймовірністю появи, вартістю, якісними і кількісними показниками, тощо); *ПРН-11 – планувати, впроваджувати, забезпечувати та контролювати безперервність бізнес/операційних процесів організації (підприємства), згідно встановленої політики інформаційної безпеки та/або кібербезпеки і стратегії організації (підприємства);* *ПРН-12 – розробляти, планувати, аналізувати та впроваджувати систему доступу до інформаційних ресурсів, інформаційно-комунікаційних систем (вузлів доступу до глобальних мереж, програмно-апаратних комплексів, підсистем, програмного забезпечення, тощо), згідно встановленої політики інформаційної безпеки та/або кібербезпеки;* *ПРН-13 – розробляти, планувати, аналізувати та впроваджувати систему аудиту і контролю ефективності функціонування інформаційно-комунікаційних систем (вузлів доступу до глобальних мереж, програмно-апаратних комплексів, підсистем, тощо), згідно встановленої політики інформаційної безпеки та/або кібербезпеки;* *ПРН-14 – розробляти та впроваджувати*					

заходи протидії кіберінцидентам, а також аналізувати, здійснювати процедури управління та контролю інцидентами, організовувати та проводити розслідування, надавати рекомендації щодо заходів їх попередження та протидії; *ПРН-15 – розробляти, впроваджувати та супроводжувати процеси управління процедурами ідентифікації, автентифікації, авторизації користувачів і інформаційних ресурсів, операційних процесів інфраструктури організації (підприємства), згідно встановленої політики інформаційної безпеки та кібербезпеки;* *ПРН-16 – розробляти, впроваджувати, та організовувати реалізацію процесів з використанням методів та засобів криптографічного та технічного захисту інформації на об'єктах інформаційної діяльності, згідно встановленої політики інформаційної безпеки та/або кібербезпеки;* *ПРН-17 – розробляти, впроваджувати та супроводжувати процеси виявлення та ідентифікації кібератак, їх аналізу та впроваджувати процедури реагування і управління інцидентами інформаційної і/або кібербезпеки;* *ПРН-18 – проводити науково-освітню діяльність, розробляти та впроваджувати систему науково-прикладних*					

досліджень в галузі захисту інформації у відповідності до сучасних норм, вимог, внутрішніх правил і політики безпеки організації (підприємства); ПРН-19 – розробляти, впроваджувати, супроводжувати систему управління персоналом з інформаційної безпеки та/або кібербезпеки на підприємстві; ПРН-20 – усвідомлювати цінності громадянського (вільного демократичного) суспільства та необхідність його сталого розвитку, верховенства права, прав і свобод людини і громадянина в Україні.				
ПРН-1 – постійно вдосконалювати та застосовувати знання державної та іноземних мов з метою забезпечення ефективності професійної комунікації; ПРН-2 – планувати, аналізувати та організовувати власну професійну діяльність, обирати оптимальні методи та способи розв'язування складних спеціалізованих задач та практичних проблем у професійній діяльності, оцінювати їхню ефективність; ПРН-5 – аналізувати та впроваджувати процедури контуру бізнес-процесів підприємства, що базуються на національних та міжнародних стандартах інформаційної та/або кібербезпеки; ПРН-6 – розробляти, впроваджувати та супроводжувати програмні та	☐	Захист інтелектуальної власності	Лекція, практичні заняття	Захист індивідуальних завдань, тестування, письмові контрольні роботи, участь у конференціях, олімпіадах, конкурсах, залік

програмно-апаратні комплекси засобів інформаційної безпеки та/або кібербезпеки в інформаційно-комунікаційних (автоматизованих) системах та у інфраструктурі організації в цілому; *ПРН-7 – виявляти, описувати та використовувати систему аналізу зв'язків між інформаційними потоками та ресурсами (в.ч. критичними) в контурі бізнес-процесів організації (підприємства);* *ПРН-8 – проектувати, впроваджувати, та супроводжувати системи захисту інформаційних систем та ресурсів, інфраструктури установи, розробляти сучасні архітектури використання інформаційних технологій та їх безпеки (архітектури безпеки, моделі інформаційної безпеки, режими безпечного функціонування, методи оцінки якості функціонування відкритих та закритих систем, тощо);* *ПРН-9 – проектувати, впроваджувати, супроводжувати системи та комплекси (програмні, програмно-апаратні) захисту застосунків (в.ч. веб-застосунків) з метою забезпечення якісного функціонування інформаційно-комунікаційних систем, згідно встановленої політики інформаційної безпеки та/або кібербезпеки;* *ПРН-11 – планувати, впроваджувати, забезпечувати та*					

контролювати безперервність бізнес/операційних процесів організації (підприємства), згідно встановленої політики інформаційної безпеки та/або кібербезпеки і стратегії організації (підприємства); ПРН-12 – розробляти, планувати, аналізувати та впроваджувати систему доступу до інформаційних ресурсів, інформаційно-комунікаційних систем (вузлів доступу до глобальних мереж, програмно-апаратних комплексів, підсистем, програмного забезпечення, тощо), згідно встановленої політики інформаційної безпеки та/або кібербезпеки; ПРН-13 – розробляти, планувати, аналізувати та впроваджувати систему аудиту і контролю ефективності функціонування інформаційно-комунікаційних систем (вузлів доступу до глобальних мереж, програмно-апаратних комплексів, підсистем, тощо), згідно встановленої політики інформаційної безпеки та/або кібербезпеки; ПРН-14 – розробляти та впроваджувати заходи протидії кіберінцидентам, а також аналізувати, здійснювати процедури управління та контролю інцидентами, організовувати та проводити розслідування, надавати рекомендації щодо заходів їх попередження та протидії;					

ПРН-15 – розробляти, впроваджувати та супроводжувати процеси управління процедурами ідентифікації, автентифікації, авторизації користувачів і інформаційних ресурсів, операційних процесів інфраструктури організації (підприємства), згідно встановленої політики інформаційної безпеки та кібербезпеки; ПРН-20 – усвідомлювати цінності громадянського (вільного демократичного) суспільства та необхідність його сталого розвитку, верховенства права, прав і свобод людини і громадянина в Україні.				
ПРН-1 – постійно вдосконалювати та застосовувати знання державної та іноземних мов з метою забезпечення ефективності професійної комунікації; ПРН-2 – планувати, аналізувати та організовувати власну професійну діяльність, обирати оптимальні методи та способи розв'язування складних спеціалізованих задач та практичних проблем у професійній діяльності, оцінювати їхню ефективність; ПРН-3 – аналізувати та адаптувати професійну діяльність в умовах частої зміни та прогресу інформаційних технологій, що застосовуються в організації, планувати і прогнозувати	☐	Бездротова та мобільна безпека	Лекція, лабораторні заняття	Захист лабораторних завдань, контрольна робота, екзамен

кінцевий результат; ПРН-4 – діяти на основі законодавчої, нормативно-правової бази України та вимог відповідних міжнародних стандартів і практик щодо здійснення професійної діяльності; ПРН-5 – аналізувати та впроваджувати процедури контуру бізнес-процесів підприємства, що базуються на національних та міжнародних стандартах інформаційної та/або кібербезпеки; ПРН-6 – розробляти, впроваджувати та супроводжувати програмні та програмно-апаратні комплекси засобів інформаційної безпеки та/або кібербезпеки в інформаційно-комунікаційних (автоматизованих) системах та у інфраструктурі організації в цілому; ПРН-8 – проектувати, впроваджувати, та супроводжувати системи захисту інформаційних систем та ресурсів, інфраструктури установи, розробляти сучасні архітектури використання інформаційних технологій та їх безпеки (архітектури безпеки, моделі інформаційної безпеки, режими безпечного функціонування, методи оцінки якості функціонування відкритих та закритих систем, тощо); ПРН-9 – проектувати, впроваджувати, супроводжувати системи та комплекси					

(програмні, програмно-апаратні) захисту застосунків (в.ч. веб-застосунків) з метою забезпечення якісного функціонування інформаційно-комунікаційних систем, згідно встановленої політики інформаційної безпеки та/або кібербезпеки; ПРН-10 – аналізувати та впроваджувати системи класифікації загроз інформаційним ресурсам (активам), проводити їх ранжування у відповідності до різних класів параметрів (за ймовірністю появи, вартістю, якісними і кількісними показниками, тощо); ПРН-11 – планувати, впроваджувати, забезпечувати та контролювати безперервність бізнес/операційних процесів організації (підприємства), згідно встановленої політики інформаційної безпеки та/або кібербезпеки і стратегії організації (підприємства); ПРН-12 – розробляти, планувати, аналізувати та впроваджувати систему доступу до інформаційних ресурсів, інформаційно-комунікаційних систем (вузлів доступу до глобальних мереж, програмно-апаратних комплексів, підсистем, програмного забезпечення, тощо), згідно встановленої політики інформаційної безпеки та/або кібербезпеки; ПРН-13 – розробляти, планувати,					

аналізувати та впроваджувати систему аудиту і контролю ефективності функціонування інформаційно-комунікаційних систем (вузлів доступу до глобальних мереж, програмно-апаратних комплексів, підсистем, тощо), згідно встановленої політики інформаційної безпеки та/або кібербезпеки; ПРН-14 – розробляти та впроваджувати заходи протидії кіберінцидентам, а також аналізувати, здійснювати процедури управління та контролю інцидентами, організовувати та проводити розслідування, надавати рекомендації щодо заходів їх попередження та протидії; ПРН-15 – розробляти, впроваджувати та супроводжувати процеси управління процедурами ідентифікації, автентифікації, авторизації користувачів і інформаційних ресурсів, операційних процесів інфраструктури організації (підприємства), згідно встановленої політики інформаційної безпеки та кібербезпеки; ПРН-16 – розробляти, впроваджувати, та організовувати реалізацію процесів з використанням методів та засобів криптографічного та технічного захисту інформації на об'єктах інформаційної діяльності, згідно встановленої політики інформаційної безпеки та/або кібербезпеки;					

ПРН-17 – розробляти, впроваджувати та супроводжувати процеси виявлення та ідентифікації кібератак, їх аналізу та впроваджувати процедури реагування і управління інцидентами інформаційної і/або кібербезпеки; ПРН-18 – проводити науково-освітню діяльність, розробляти та впроваджувати систему науково-прикладних досліджень в галузі захисту інформації у відповідності до сучасних норм, вимог, внутрішніх правил і політики безпеки організації (підприємства);				
ПРН-1 – постійно вдосконалювати та застосовувати знання державної та іноземних мов з метою забезпечення ефективності професійної комунікації; ПРН-2 – планувати, аналізувати та організовувати власну професійну діяльність, обирати оптимальні методи та способи розв'язування складних спеціалізованих задач та практичних проблем у професійній діяльності, оцінювати їхню ефективність; ПРН-4 – діяти на основі законодавчої, нормативно-правової бази України та вимог відповідних міжнародних стандартів і практик щодо здійснення професійної діяльності; ПРН-5 – аналізувати та впроваджувати процедури контуру бізнес-процесів підприємства, що базуються на національних та	☐	Веб-безпека	Лекція, лабораторні заняття	Захист лабораторних завдань, контрольна робота, екзамен

міжнародних стандартах інформаційної та/або кібербезпеки; ПРН-7 – виявляти, описувати та використовувати систему аналізу зв'язків між інформаційними потоками та ресурсами (в.ч. критичними) в контурі бізнес-процесів організації (підприємства); ПРН-8 – проектувати, впроваджувати, та супроводжувати системи захисту інформаційних систем та ресурсів, інфраструктури установи, розробляти сучасні архітектури використання інформаційних технологій та їх безпеки (архітектури безпеки, моделі інформаційної безпеки, режими безпечного функціонування, методи оцінки якості функціонування відкритих та закритих систем, тощо); ПРН-13 – розробляти, планувати, аналізувати та впроваджувати систему аудиту і контролю ефективності функціонування інформаційно-комунікаційних систем (вузлів доступу до глобальних мереж, програмно-апаратних комплексів, підсистем, тощо), згідно встановленої політики інформаційної безпеки та/або кібербезпеки; ПРН-18 – проводити науково-освітню діяльність, розробляти та впроваджувати систему науково-прикладних досліджень в галузі захисту інформації у відповідності до сучасних норм,					

вимог, внутрішніх правил і політики безпеки організації (підприємства);				
ПРН-1 – постійно вдосконалювати та застосовувати знання державної та іноземних мов з метою забезпечення ефективності професійної комунікації; *ПРН-2 – планувати, аналізувати та організовувати власну професійну діяльність, обирати оптимальні методи та способи розв'язування складних спеціалізованих задач та практичних проблем у професійній діяльності, оцінювати їхню ефективність;* *ПРН-5 – аналізувати та впроваджувати процедури контуру бізнес-процесів підприємства, що базуються на національних та міжнародних стандартах інформаційної та/або кібербезпеки;* *ПРН-6 – розробляти, впроваджувати та супроводжувати програмні та програмно-апаратні комплекси засобів інформаційної безпеки та/або кібербезпеки в інформаційно-комунікаційних (автоматизованих) системах та у інфраструктурі організації в цілому;* *ПРН-7 – виявляти, описувати та використовувати систему аналізу зв'язків між інформаційними потоками та ресурсами (в.ч. критичними) в контурі бізнес-процесів організації (підприємства);* *ПРН-8 – проектувати, впроваджувати, та супроводжувати*	☐	Тестування на проникнення та етичний хакінг	Лекція, лабораторні заняття	Захист лабораторних завдань, контрольна робота, екзамен

системи захисту інформаційних систем та ресурсів, інфраструктури установи, розробляти сучасні архітектури використання інформаційних технологій та їх безпеки (архітектури безпеки, моделі інформаційної безпеки, режими безпечного функціонування, методи оцінки якості функціонування відкритих та закритих систем, тощо); *ПРН-9 – проектувати, впроваджувати, супроводжувати системи та комплекси (програмні, програмно-апаратні) захисту застосунків (в.ч. веб-застосунків) з метою забезпечення якісного функціонування інформаційно-комунікаційних систем, згідно встановленої політики інформаційної безпеки та/або кібербезпеки;* *ПРН-10 – аналізувати та впроваджувати системи класифікації загроз інформаційним ресурсам (активам), проводити їх ранжування у відповідності до різних класів параметрів (за ймовірністю появи, вартістю, якісними і кількісними показниками, тощо);* *ПРН-11 – планувати, впроваджувати, забезпечувати та контролювати безперервність бізнес/операційних процесів організації (підприємства), згідно встановленої політики інформаційної безпеки та/або кібербезпеки і стратегії*					

організації (підприємства); ПРН-12 – розробляти, планувати, аналізувати та впроваджувати систему доступу до інформаційних ресурсів, інформаційно-комунікаційних систем (вузлів доступу до глобальних мереж, програмно-апаратних комплексів, підсистем, програмного забезпечення, тощо), згідно встановленої політики інформаційної безпеки та/або кібербезпеки; ПРН-13 – розробляти, планувати, аналізувати та впроваджувати систему аудиту і контролю ефективності функціонування інформаційно-комунікаційних систем (вузлів доступу до глобальних мереж, програмно-апаратних комплексів, підсистем, тощо), згідно встановленої політики інформаційної безпеки та/або кібербезпеки; ПРН-14 – розробляти та впроваджувати заходи протидії кіберінцидентам, а також аналізувати, здійснювати процедури управління та контролю інцидентами, організовувати та проводити розслідування, надавати рекомендації щодо заходів їх попередження та протидії; ПРН-15 – розробляти, впроваджувати та супроводжувати процеси управління процедурами ідентифікації, автентифікації, авторизації користувачів і					

інформаційних ресурсів, операційних процесів інфраструктури організації (підприємства), згідно встановленої політики інформаційної безпеки та кібербезпеки; ПРН-16 – розробляти, впроваджувати, та організовувати реалізацію процесів з використанням методів та засобів криптографічного та технічного захисту інформації на об'єктах інформаційної діяльності, згідно встановленої політики інформаційної безпеки та/або кібербезпеки; ПРН-17 – розробляти, впроваджувати та супроводжувати процеси виявлення та ідентифікації кібератак, їх аналізу та впроваджувати процедури реагування і управління інцидентами інформаційної і/або кібербезпеки; ПРН-18 – проводити науково-освітню діяльність, розробляти та впроваджувати систему науково-прикладних досліджень в галузі захисту інформації у відповідності до сучасних норм, вимог, внутрішніх правил і політики безпеки організації (підприємства); ПРН-19 – розробляти, впроваджувати, супроводжувати систему управління персоналом з інформаційної безпеки та/або кібербезпеки на підприємстві;				
ПРН-1 – постійно вдосконалювати та застосовувати знання державної та іноземних мов з метою забезпечення	☐	Цифрова криміналістика	Лекція, лабораторні заняття	Захист лабораторних завдань, контрольна робота, екзамен

ефективності професійної комунікації; *ПРН-2 – планувати, аналізувати та організовувати власну професійну діяльність, обирати оптимальні методи та способи розв'язування складних спеціалізованих задач та практичних проблем у професійній діяльності, оцінювати їхню ефективність;* *ПРН-4 – діяти на основі законодавчої, нормативно-правової бази України та вимог відповідних міжнародних стандартів і практик щодо здійснення професійної діяльності;* *ПРН-5 – аналізувати та впроваджувати процедури контуру бізнес-процесів підприємства, що базуються на національних та міжнародних стандартах інформаційної та/або кібербезпеки;* *ПРН-6 – розробляти, впроваджувати та супроводжувати програмні та програмно-апаратні комплекси засобів інформаційної безпеки та/або кібербезпеки в інформаційно-комунікаційних (автоматизованих) системах та у інфраструктурі організації в цілому;* *ПРН-7 – виявляти, описувати та використовувати систему аналізу зв'язків між інформаційними потоками та ресурсами (в.ч. критичними) в контурі бізнес-процесів організації (підприємства);* *ПРН-8 – проектувати, впроваджувати,*					

та супроводжувати системи захисту інформаційних систем та ресурсів, інфраструктури установи, розробляти сучасні архітектури використання інформаційних технологій та їх безпеки (архітектури безпеки, моделі інформаційної безпеки, режими безпечного функціонування, методи оцінки якості функціонування відкритих та закритих систем, тощо); *ПРН-9 – проектувати, впроваджувати, супроводжувати системи та комплекси (програмні, програмно-апаратні) захисту застосунків (в.ч. веб-застосунків) з метою забезпечення якісного функціонування інформаційно-комунікаційних систем, згідно встановленої політики інформаційної безпеки та/або кібербезпеки;* *ПРН-10 – аналізувати та впроваджувати системи класифікації загроз інформаційним ресурсам (активам), проводити їх ранжування у відповідності до різних класів параметрів (за ймовірністю появи, вартістю, якісними і кількісними показниками, тощо);* *ПРН-11 – планувати, впроваджувати, забезпечувати та контролювати безперервність бізнес/операційних процесів організації (підприємства), згідно встановленої політики інформаційної безпеки та/або*					

кібербезпеки і стратегії організації (підприємства); ПРН-12 – розробляти, планувати, аналізувати та впроваджувати систему доступу до інформаційних ресурсів, інформаційно-комунікаційних систем (вузлів доступу до глобальних мереж, програмно-апаратних комплексів, підсистем, програмного забезпечення, тощо), згідно встановленої політики інформаційної безпеки та/або кібербезпеки; ПРН-13 – розробляти, планувати, аналізувати та впроваджувати систему аудиту і контролю ефективності функціонування інформаційно-комунікаційних систем (вузлів доступу до глобальних мереж, програмно-апаратних комплексів, підсистем, тощо), згідно встановленої політики інформаційної безпеки та/або кібербезпеки; ПРН-14 – розробляти та впроваджувати заходи протидії кіберінцидентам, а також аналізувати, здійснювати процедури управління та контролю інцидентами, організовувати та проводити розслідування, надавати рекомендації щодо заходів їх попередження та протидії; ПРН-15 – розробляти, впроваджувати та супроводжувати процеси управління процедурами ідентифікації, автентифікації,					

авторизації користувачів і інформаційних ресурсів, операційних процесів інфраструктури організації (підприємства), згідно встановленої політики інформаційної безпеки та кібербезпеки; ПРН-16 – розробляти, впроваджувати, та організовувати реалізацію процесів з використанням методів та засобів криптографічного та технічного захисту інформації на об'єктах інформаційної діяльності, згідно встановленої політики інформаційної безпеки та/або кібербезпеки; ПРН-17 – розробляти, впроваджувати та супроводжувати процеси виявлення та ідентифікації кібератак, їх аналізу та впроваджувати процедури реагування і управління інцидентами інформаційної і/або кібербезпеки; ПРН-19 – розробляти, впроваджувати, супроводжувати систему управління персоналом з інформаційної безпеки та/або кібербезпеки на підприємстві;				
ПРН-1 – постійно вдосконалювати та застосовувати знання державної та іноземних мов з метою забезпечення ефективності професійної комунікації; ПРН-2 – планувати, аналізувати та організовувати власну професійну діяльність, обирати оптимальні методи та способи розв'язування складних спеціалізованих	☐	Безпека інтернет речей	Лекція, лабораторні заняття	Захист лабораторних завдань, контрольна робота, залік

задач та практичних проблем у професійній діяльності, оцінювати їхню ефективність; ПРН-3 – аналізувати та адаптувати професійну діяльність в умовах частої зміни та прогресу інформаційних технологій, що застосовуються в організації, планувати і прогнозувати кінцевий результат; ПРН-4 – діяти на основі законодавчої, нормативно-правової бази України та вимог відповідних міжнародних стандартів і практик щодо здійснення професійної діяльності; ПРН-5 – аналізувати та впроваджувати процедури контуру бізнес-процесів підприємства, що базуються на національних та міжнародних стандартах інформаційної та/або кібербезпеки; ПРН-6 – розробляти, впроваджувати та супроводжувати програмні та програмно-апаратні комплекси засобів інформаційної безпеки та/або кібербезпеки в інформаційно-комунікаційних (автоматизованих) системах та у інфраструктурі організації в цілому; ПРН-7 – виявляти, описувати та використовувати систему аналізу зв'язків між інформаційними потоками та ресурсами (в.ч. критичними) в контурі бізнес-процесів організації (підприємства); ПРН-8 – проектувати, впроваджувати,					

та супроводжувати системи захисту інформаційних систем та ресурсів, інфраструктури установи, розробляти сучасні архітектури використання інформаційних технологій та їх безпеки (архітектури безпеки, моделі інформаційної безпеки, режими безпечного функціонування, методи оцінки якості функціонування відкритих та закритих систем, тощо); *ПРН-9 – проектувати, впроваджувати, супроводжувати системи та комплекси (програмні, програмно-апаратні) захисту застосунків (в.ч. веб-застосунків) з метою забезпечення якісного функціонування інформаційно-комунікаційних систем, згідно встановленої політики інформаційної безпеки та/або кібербезпеки;* *ПРН-13 – розробляти, планувати, аналізувати та впроваджувати систему аудиту і контролю ефективності функціонування інформаційно-комунікаційних систем (вузлів доступу до глобальних мереж, програмно-апаратних комплексів, підсистем, тощо), згідно встановленої політики інформаційної безпеки та/або кібербезпеки;* *ПРН-14 – розробляти та впроваджувати заходи протидії кіберінцидентам, а також аналізувати, здійснювати процедури*					

управління та контролю інцидентами, організовувати та проводити розслідування, надавати рекомендації щодо заходів їх попередження та протидії; *ПРН-15 – розробляти, впроваджувати та супроводжувати процеси управління процедурами ідентифікації, автентифікації, авторизації користувачів і інформаційних ресурсів, операційних процесів інфраструктури організації (підприємства), згідно встановленої політики інформаційної безпеки та кібербезпеки;* *ПРН-16 – розробляти, впроваджувати, та організовувати реалізацію процесів з використанням методів та засобів криптографічного та технічного захисту інформації на об'єктах інформаційної діяльності, згідно встановленої політики інформаційної безпеки та/або кібербезпеки;* *ПРН-17 – розробляти, впроваджувати та супроводжувати процеси виявлення та ідентифікації кібератак, їх аналізу та впроваджувати процедури реагування і управління інцидентами інформаційної і/або кібербезпеки;* *ПРН-18 – проводити науково-освітню діяльність, розробляти та впроваджувати систему науково-прикладних досліджень в галузі захисту інформації у відповідності до сучасних норм, вимог, внутрішніх правил і політики*					

безпеки організації (підприємства);				
ПРН-1 – постійно вдосконалювати та застосовувати знання державної та іноземних мов з метою забезпечення ефективності професійної комунікації; *ПРН-2 – планувати, аналізувати та організовувати власну професійну діяльність, обирати оптимальні методи та способи розв'язування складних спеціалізованих задач та практичних проблем у професійній діяльності, оцінювати їхню ефективність;* *ПРН-3 – аналізувати та адаптувати професійну діяльність в умовах частої зміни та прогресу інформаційних технологій, що застосовуються в організації, планувати і прогнозувати кінцевий результат;* *ПРН-4 – діяти на основі законодавчої, нормативно-правової бази України та вимог відповідних міжнародних стандартів і практик щодо здійснення професійної діяльності;* *ПРН-6 – розробляти, впроваджувати та супроводжувати програмні та програмно-апаратні комплекси засобів інформаційної безпеки та/або кібербезпеки в інформаційно-комунікаційних (автоматизованих) системах та у інфраструктурі організації в цілому;* *ПРН-7 – виявляти, описувати та використовувати систему аналізу*	☐	Передові методики програмування	Лекція, лабораторні заняття	Захист лабораторних завдань, контрольна робота, екзамен

зв'язків між інформаційними потоками та ресурсами (в.ч. критичними) в контурі бізнес-процесів організації (підприємства); *ПРН-8 – проектувати, впроваджувати, та супроводжувати системи захисту інформаційних систем та ресурсів, інфраструктури установи, розробляти сучасні архітектури використання інформаційних технологій та їх безпеки (архітектури безпеки, моделі інформаційної безпеки, режими безпечного функціонування, методи оцінки якості функціонування відкритих та закритих систем, тощо);* *ПРН-9 – проектувати, впроваджувати, супроводжувати системи та комплекси (програмні, програмно-апаратні) захисту застосунків (в.ч. веб-застосунків) з метою забезпечення якісного функціонування інформаційно-комунікаційних систем, згідно встановленої політики інформаційної безпеки та/або кібербезпеки;* *ПРН-14 – розробляти та впроваджувати заходи протидії кіберінцидентам, а також аналізувати, здійснювати процедури управління та контролю інцидентами, організовувати та проводити розслідування, надавати рекомендації щодо заходів їх попередження та протидії;* *ПРН-15 –*					

розробляти, впроваджувати та супроводжувати процеси управління процедурами ідентифікації, автентифікації, авторизації користувачів і інформаційних ресурсів, операційних процесів інфраструктури організації (підприємства), згідно встановленої політики інформаційної безпеки та кібербезпеки; ПРН-16 – розробляти, впроваджувати, та організовувати реалізацію процесів з використанням методів та засобів криптографічного та технічного захисту інформації на об'єктах інформаційної діяльності, згідно встановленої політики інформаційної безпеки та/або кібербезпеки; ПРН-17 – розробляти, впроваджувати та супроводжувати процеси виявлення та ідентифікації кібератак, їх аналізу та впроваджувати процедури реагування і управління інцидентами інформаційної і/або кібербезпеки; ПРН-18 – проводити науково-освітню діяльність, розробляти та впроваджувати систему науково-прикладних досліджень в галузі захисту інформації у відповідності до сучасних норм, вимог, внутрішніх правил і політики безпеки організації (підприємства); ПРН-19 – розробляти, впроваджувати, супроводжувати систему управління персоналом з інформаційної безпеки та/або кібербезпеки на					

підприємстві;				
ПРН-1 – постійно вдосконалювати та застосовувати знання державної та іноземних мов з метою забезпечення ефективності професійної комунікації; *ПРН-4 – діяти на основі законодавчої, нормативно-правової бази України та вимог відповідних міжнародних стандартів і практик щодо здійснення професійної діяльності;* *ПРН-5 – аналізувати та впроваджувати процедури контуру бізнес-процесів підприємства, що базуються на національних та міжнародних стандартах інформаційної та/або кібербезпеки;* *ПРН-6 – розробляти, впроваджувати та супроводжувати програмні та програмно-апаратні комплекси засобів інформаційної безпеки та/або кібербезпеки в інформаційно-комунікаційних (автоматизованих) системах та у інфраструктурі організації в цілому;* *ПРН-7 – виявляти, описувати та використовувати систему аналізу зв'язків між інформаційними потоками та ресурсами (в.ч. критичними) в контурі бізнес-процесів організації (підприємства);* *ПРН-8 – проектувати, впроваджувати, та супроводжувати системи захисту інформаційних систем та ресурсів, інфраструктури установи, розробляти сучасні*	☐	Англійська мова	Практичні заняття	Захист практичних завдань, презентація, контрольні роботи, залік

архітектури використання інформаційних технологій та їх безпеки (архітектури безпеки, моделі інформаційної безпеки, режими безпечного функціонування, методи оцінки якості функціонування відкритих та закритих систем, тощо); *ПРН-9 – проектувати, впроваджувати, супроводжувати системи та комплекси (програмні, програмно-апаратні) захисту застосунків (в.ч. веб-застосунків) з метою забезпечення якісного функціонування інформаційно-комунікаційних систем, згідно встановленої політики інформаційної безпеки та/або кібербезпеки;* *ПРН-14 – розробляти та впроваджувати заходи протидії кіберінцидентам, а також аналізувати, здійснювати процедури управління та контролю інцидентами, організовувати та проводити розслідування, надавати рекомендації щодо заходів їх попередження та протидії;* *ПРН-15 – розробляти, впроваджувати та супроводжувати процеси управління процедурами ідентифікації, автентифікації, авторизації користувачів і інформаційних ресурсів, операційних процесів інфраструктури організації (підприємства), згідно встановленої політики інформаційної*					

безпеки та кібербезпеки; ПРН-18 – проводити науково-освітню діяльність, розробляти та впроваджувати систему науково-прикладних досліджень в галузі захисту інформації у відповідності до сучасних норм, вимог, внутрішніх правил і політики безпеки організації (підприємства);				