

**МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ХАРКІВСЬКИЙ НАЦІОНАЛЬНИЙ ЕКОНОМІЧНИЙ УНІВЕРСИТЕТ
ІМЕНІ СЕМЕНА КУЗНЕЦЯ**

УХВАЛЕНО
Рішенням вченої ради
Харківського національного
економічного університету
імені Семена Кузнеця
від 23.05.2023 р. протокол № 6

ВВЕДЕНО В ДІЮ
Наказом ректора Харківського
національного економічного університету
імені Семена Кузнеця
від 23.05.2023 р. № 144



Володимир ПОНОМАРЕНКО

**ОСВІТНЬО-ПРОФЕСІЙНА ПРОГРАМА
«КІБЕРБЕЗПЕКА»**

РІВЕНЬ ВИЩОЇ ОСВІТИ	Перший (бакалаврський)
СТУПІНЬ ВИЩОЇ ОСВІТИ	Бакалавр
ГАЛУЗЬ ЗНАНЬ	12 Інформаційні технології
СПЕЦІАЛЬНІСТЬ	125 Кібербезпека та захист інформації

Харків, 2023

ПРЕАМБУЛА

Склад робочої група освітньої програми «Кібербезпека»:

Лимаренко Вячеслав Володимирович, доцент кафедри кібербезпеки та інформаційних технологій, кандидат технічних наук – гарант освітньої-професійної програми.

Шаповалова Олена Олександрівна, доцент кафедри кібербезпеки та інформаційних технологій, кандидат технічних наук, доцент.

Венгріна Олена Сергіївна, доцент кафедри кібербезпеки та інформаційних технологій, кандидат технічних наук.

Пожидаєв Максим Геннадійович, випускник освітньої програми.

Бондар Сергій Володимирович, менеджер ТОВ «Охорона і безпека».

Розглянуто на засіданні кафедри кібербезпеки та інформаційних технологій, протокол № 9, від 09.02.2023 р.

Розглянуто вченою радою факультету інформаційних технологій, протокол № 5, від 28.02.2023 р.

ОП оновлено на підставі:

1. Законодавчих та нормативних актів: Законів України “Про освіту”, “Про вищу освіту”, Національної рамки кваліфікації, Національного класифікатору України.

2. Стандарту вищої освіти України: перший (бакалаврський) рівень, галузь знань 12 – Інформаційні технології, спеціальність 125 – Кібербезпека, затвердженого Наказом Міністерства освіти та науки України № 1074 від 04.10.2018 р.).

3. Постанови Кабінету Міністрів України № 1392 від 16 грудня 2022 р. «Про внесення змін до переліку галузей знань і спеціальностей, за якими здійснюється підготовка здобувачів вищої освіти».

4. Аналізу ринку праці, з урахуванням регіонального контексту.

5. Вивчення вітчизняного та зарубіжного досвіду.

6. Пропозицій роботодавців.

7. Рекомендації після процедур акредитація Національного агентства із забезпечення якості вищої освіти рішення від 27.04.2021, протокол № 7.

Рецензії-відгуки зовнішніх стейкхолдерів (додаються).

І. ЗАГАЛЬНА ХАРАКТЕРИСТИКА

Рівень вищої освіти	Перший (бакалаврський) рівень
Ступінь вищої освіти	Бакалавр
Галузі знань	12 Інформаційні технології
Спеціальності	125 Кібербезпека та захист інформації
Освітня програма	Кібербезпека / Cybersecurity
Форми здобуття освіти, обсяг освітньої програми в кредитах ЄКТС та терміни навчання	денна форма – 240 кредитів, 3 роки 10 місяців.
Наявність акредитації	Сертифікат про акредитацію освітньої програми НАЗЯВО № 1484 від 29.04.2021 строк дії сертифіката про акредитацію освітньої програми до 01.07.2026
Мова(и) навчання / оцінювання	українська / англійська
Структурний підрозділ відповідальний за ОП	Кафедра кібербезпеки та інформаційних технологій; Навчальна лабораторія кафедри кібербезпеки та інформаційних технологій
Вимоги до зарахування	Набір на перший (бакалаврський) здійснюється відповідно до правил та порядку прийому для здобуття вищої освіти. Правила та строки прийому розміщені на сайті ХНЕУ ім. С. Кузнеця за посиланням https://www.hneu.edu.ua/normatyvni-dokumenty/ Для успішного засвоєння освітньої програми бакалавра вступники повинні мати повну загальну середню освіту та прагнення оволодіти знаннями в галузі інформаційних технологій за спеціальністю кібербезпека та захист інформації.
Обмеження щодо форм навчання	Немає
Освітня кваліфікація	Бакалавр з кібербезпеки
Кваліфікація(-ї) професійна(-і)	Відсутня
Кваліфікація в дипломі	Ступінь вищої освіти – Бакалавр Спеціальність – 125 Кібербезпека та захист інформації Освітня програма – Кібербезпека
Мета освітньої програми	Підготовка фахівців, здатних використовувати і впроваджувати технології інформаційної та/або кібербезпеки, а також технологій цифрової економіки.
Фокус та особливості (унікальність) програми	Особливістю ОПП Кібербезпека є орієнтація на сучасні вимоги до фахівців в галузі інформаційних технологій, та набуття здобувачами вищої освіти конкурентоспроможних компетентностей на основі синергізму отримання результатів навчання з інформаційної та/або кібербезпеки та програмування.
Опис предметної області	Об'єкт вивчення: об'єкти інформатизації, включаючи комп'ютерні, автоматизовані, телекомунікаційні, інформаційні, інформаційно-аналітичні, інформаційно-телекомунікаційні системи, інформаційні ресурси і технології; – технології забезпечення безпеки інформації; – процеси управління інформаційною та/або кібербезпекою

	<p>об'єктів, що підлягають захисту.</p> <p>Цілі навчання: підготовка фахівців здатних використовувати і впроваджувати технології інформаційної та/або кібербезпеки.</p> <p>Теоретичний зміст предметної області включає знання:</p> <ul style="list-style-type: none"> – законодавчої, нормативно-правової бази України та вимог відповідних міжнародних стандартів і практик щодо здійснення професійної діяльності; – принципів супроводу систем та комплексів інформаційної та/або кібербезпеки; – теорії, моделей та принципів управління доступом до інформаційних ресурсів; – теорії систем управління інформаційною та/або кібербезпекою; – методів та засобів виявлення, управління та ідентифікації ризиків; – методів та засобів оцінювання та забезпечення необхідного рівня захищеності інформації; – методів та засобів технічного та криптографічного захисту інформації; – сучасних інформаційно-комунікаційних технологій; – сучасного програмно-апаратного забезпечення інформаційно-комунікаційних технологій; – автоматизованих систем проектування <p>Методи, методики та технології: Методи, методики, інформаційно-комунікаційні технології та інші технології забезпечення інформаційної та/або кібербезпеки.</p> <p>Інструментарій та обладнання: системи розробки, забезпечення, моніторингу та контролю процесів інформаційної та/або кібербезпеки;</p> <ul style="list-style-type: none"> – сучасне програмно-апаратне забезпечення інформаційно-комунікаційних технологій; – спеціалізований клас (кіберполігон).
Академічна мобільність	-
Академічні права	Можливість продовжити навчання за освітньою програмою ступеня магістра.
Професійні права	<p>Знання і розуміння:</p> <ul style="list-style-type: none"> – ґрунтовна математична підготовка в галузі захисту інформації, криптології та криптографії, теорії, моделей та принципів управління доступом до інформаційних ресурсів; – базові знання принципів супроводу систем та комплексів інформаційної та/або кібербезпеки та систем управління інформаційною та/або кібербезпекою; – методів та засобів виявлення, управління та ідентифікації ризиків, а також технічного та криптографічного захисту інформації; – знання мов та парадигм програмування, технологій програмування, WEB- технологій, операційних систем; – знання методів та засобів оцінювання та забезпечення необхідного рівня захищеності інформації. <p>Застосування знань і розумінь:</p> <ul style="list-style-type: none"> – здатність використання інформаційних і комунікаційних технологій з метою пошуку нової інформації, створення баз

	<p>даних, аналізу розподілених АС та їх оптимізації;</p> <ul style="list-style-type: none"> – здатність здійснювати проектування (розробку) систем, технологій і засобів інформаційної безпеки; – здатність здійснювати протидію несанкціонованому проникненню в ІТ системи і мережі; – здатність прогнозувати, виявляти та оцінювати стан інформаційної безпеки об'єктів і систем; – здатність відновлювати нормальне функціонування ІТ систем і мереж після здійснення кібернападів, збоїв та відмов; – здатність виконувати спеціальні дослідження технічних і програмно-апаратних засобів захисту обробки інформації в ІТС; – здатність формувати комплекс заходів (правил, процедур, практичних прийомів та ін.) для управління інформаційною безпекою. <p>Формування суджень:</p> <ul style="list-style-type: none"> – вміння виявляти, ставити та вирішувати проблеми за професійним спрямуванням; – здатність виконувати моніторинг даних, комп'ютерних зловживань та аномалій; – здатність до пошуку, оброблення та аналізу інформації; – здатність до роботи в команді; – здатність використовувати законодавчу та нормативно-правову бази, а також вимоги відповідних, в тому числі і міжнародних, стандартів та практик щодо здійснення професійної діяльності.
Працевлаштування випускників	<p>Професії, на підготовку з яких спрямована ОП (згідно з чинною редакцією Національного класифікатора України: Класифікатор професій ДК 003:2010)</p> <p>1495 Менеджери (управителі) систем з інформаційної безпеки, 2149.2 Фахівець (сфера захисту інформації), 3119 Технік (сфера захисту інформації), 2131.2 Адміністратор бази даних, 2131.2 Адміністратор даних, 2131.2 Адміністратор доступу, 2131.2 Адміністратор доступу (груповий), 2132.2 Інженер-програміст.</p>

II – ПЕРЕЛІК КОМПЕТЕНТНОСТЕЙ ВИПУСКНИКА

Інтегральна компетентність	Здатність розв'язувати складні спеціалізовані задачі та практичні проблеми у галузі забезпечення інформаційної безпеки і \ або кібербезпеки, що характеризується комплексністю та неповною визначеністю умов.
Загальні компетентності	<p>КЗ 1. Здатність застосовувати знання у практичних ситуаціях.</p> <p>КЗ 2. Знання та розуміння предметної області та розуміння професії.</p> <p>КЗ 3. Здатність професійно спілкуватися державною та іноземною мовами як усно, так і письмово.</p> <p>КЗ 4. Вміння виявляти, ставити та вирішувати проблеми за професійним спрямуванням.</p> <p>КЗ 5. Здатність до пошуку, оброблення та аналізу інформації.</p> <p>КЗ 6. Здатність реалізувати свої права і обов'язки як члена суспільства, усвідомлювати цінності громадянського (вільного</p>

	<p>демократичного) суспільства та необхідність його сталого розвитку, верховенства права, прав і свобод людини і громадянина в Україні.</p> <p>КЗ 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.</p>
<p>Спеціальні (фахові, предметні) компетентності</p>	<p>КФ 1. Здатність застосовувати законодавчу та нормативно-правову базу, а також державні та міжнародні вимоги, практики і стандарти з метою здійснення професійної діяльності в галузі інформаційної та/або кібербезпеки.</p> <p>КФ 2. Здатність до використання інформаційно-комунікаційних технологій, сучасних методів і моделей інформаційної безпеки та/або кібербезпеки.</p> <p>КФ 3. Здатність до використання програмних та програмно-апаратних комплексів засобів захисту інформації в інформаційно-телекомунікаційних (автоматизованих) системах.</p> <p>КФ 4. Здатність забезпечувати неперервність бізнесу згідно встановленої політики інформаційної та/або кібербезпеки.</p> <p>КФ 5. Здатність забезпечувати захист інформації, що обробляється в інформаційно-телекомунікаційних (автоматизованих) системах з метою реалізації встановленої політики інформаційної та/або кібербезпеки.</p> <p>КФ 6. Здатність відновлювати штатне функціонування інформаційних, інформаційно-телекомунікаційних (автоматизованих) систем після реалізації загроз, здійснення кібератак, збоїв та відмов різних класів та походження.</p> <p>КФ 7. Здатність впроваджувати та забезпечувати функціонування комплексних систем захисту інформації (комплекси нормативно-правових, організаційних та технічних засобів і методів, процедур, практичних прийомів та ін.).</p> <p>КФ 8. Здатність здійснювати процедури управління інцидентами, проводити розслідування, надавати їм оцінку.</p> <p>КФ 9. Здатність здійснювати професійну діяльність на основі впровадженої системи управління інформаційною та/або кібербезпекою.</p> <p>КФ 10. Здатність застосовувати методи та засоби криптографічного та технічного захисту інформації на об'єктах інформаційної діяльності.</p> <p>КФ 11. Здатність виконувати моніторинг процесів функціонування інформаційних, інформаційно-телекомунікаційних (автоматизованих) систем згідно встановленої політики інформаційної та/або кібербезпеки.</p> <p>КФ 12. Здатність аналізувати, виявляти та оцінювати можливі загрози, уразливості та дестабілізуючі чинники інформаційному простору та інформаційним ресурсам згідно з встановленою політикою інформаційної та/або кібербезпеки</p>

З метою забезпечення кореляції визначених компетентностей з класифікацією компетентностей НРК використовується матриця відповідності визначених компетентностей та дескрипторів НРК, яка є інформаційним додатком (**Таблиця 1 Пояснювальної записки**).

III – НОРМАТИВНИЙ ЗМІСТ ПІДГОТОВКИ ЗДОБУВАЧІВ ВИЩОЇ ОСВІТИ, СФОРМУЛЬОВАНИЙ У ТЕРМІНАХ РЕЗУЛЬТАТІВ НАВЧАННЯ ЗА СПЕЦІАЛЬНІСТЮ 125 КІБЕРБЕЗПЕКА

РН1 – застосовувати знання державної та іноземних мов з метою забезпечення ефективності професійної комунікації;

РН 2 – організовувати власну професійну діяльність, обирати оптимальні методи та способи розв’язування складних спеціалізованих задач та практичних проблем у професійній діяльності, оцінювати їхню ефективність;

РН 3 – використовувати результати самостійного пошуку, аналізу та синтезу інформації з різних джерел для ефективного рішення спеціалізованих задач професійної діяльності;

РН 4 – аналізувати, аргументувати, приймати рішення при розв’язанні складних спеціалізованих задач та практичних проблем у професійній діяльності, які характеризуються комплексністю та неповною визначеністю умов, відповідати за прийняті рішення;

РН 5 – адаптуватися в умовах частотої зміни технологій професійної діяльності, прогнозувати кінцевий результат;

РН 6 – критично осмислювати основні теорії, принципи, методи і поняття у навчанні та професійній діяльності;

РН 7 – діяти на основі законодавчої та нормативно-правової бази України та вимог відповідних стандартів, у тому числі міжнародних в галузі інформаційної та /або кібербезпеки;

РН 8 – готувати пропозиції до нормативних актів щодо забезпечення інформаційної та /або кібербезпеки;

РН 9 – впроваджувати процеси, що базуються на національних та міжнародних стандартах, виявлення, ідентифікації, аналізу та реагування на інциденти інформаційної та/або кібербезпеки;

РН 10 – виконувати аналіз та декомпозицію інформаційно-телекомунікаційних систем;

РН 11 – виконувати аналіз зв’язків між інформаційними процесами на віддалених обчислювальних системах;

РН 12 – розробляти моделі загроз та порушника;

РН 13 – аналізувати проекти інформаційно-телекомунікаційних систем базуючись на стандартизованих технологіях та протоколах передачі даних;

РН 14 – вирішувати завдання захисту програм та інформації, що обробляється в інформаційно-телекомунікаційних системах програмно-апаратними засобами та давати оцінку результативності якості прийнятих рішень;

РН 15 – використовувати сучасне програмно-апаратне забезпечення інформаційно-комунікаційних технологій;

РН 16 – реалізовувати комплексні системи захисту інформації в автоматизованих системах (АС) організації (підприємства) відповідно до вимог нормативно-правових документів;

РН 17 – забезпечувати процеси захисту та функціонування інформаційно-телекомунікаційних (автоматизованих) систем на основі практик, навичок та знань, щодо структурних (структурно-логічних) схем, топології мережі, сучасних архітектур та моделей захисту електронних інформаційних ресурсів з відображенням взаємозв'язків та інформаційних потоків, процесів для внутрішніх і віддалених компонент;

РН 18 – використовувати програмні та програмно-апаратні комплекси захисту інформаційних ресурсів;

РН 19 – застосовувати теорії та методи захисту для забезпечення безпеки інформації в інформаційно-телекомунікаційних системах;

РН 20 – забезпечувати функціонування спеціального програмного забезпечення, щодо захисту інформації від руйнуючих програмних впливів, руйнуючих кодів в інформаційно-телекомунікаційних системах;

РН 21 – вирішувати задачі забезпечення та супроводу (в.т. числі: огляд, тестування, підзвітність) системи управління доступом згідно встановленої політики безпеки в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах;

РН 22 – вирішувати задачі управління процедурами ідентифікації, автентифікації, авторизації процесів і користувачів в інформаційно-телекомунікаційних системах згідно встановленої політики інформаційної і\або кібербезпеки;

РН 23 – реалізовувати заходи з протидії отриманню несанкціонованого доступу до інформаційних ресурсів і процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах;

РН 24 – вирішувати задачі управління доступом до інформаційних ресурсів та процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах на основі моделей управління доступом (мандатних, дискреційних, рольових);

РН 25 – забезпечувати введення підзвітності системи управління доступом до електронних інформаційних ресурсів і процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах з використанням журналів реєстрації подій, їх аналізу та встановлених процедур захисту;

РН 26 – впроваджувати заходи та забезпечувати реалізацію процесів попередження отриманню несанкціонованого доступу і захисту інформаційних, інформаційно-телекомунікаційних (автоматизованих) систем на основі еталонної моделі взаємодії відкритих систем;

РН 27 – вирішувати задачі захисту потоків даних в інформаційних, інформаційно-телекомунікаційних (автоматизованих) системах;

РН 28 – аналізувати та проводити оцінку ефективності та рівня захищеності ресурсів різних класів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах в ході проведення випробувань згідно встановленої політики інформаційної та/або кібербезпеки;

РН 29 – здійснювати оцінювання можливості реалізації потенційних загроз інформації, що обробляється в інформаційно-телекомунікаційних системах та ефективності використання комплексів засобів захисту в умовах реалізації загроз різних класів;

РН 30 – здійснювати оцінювання можливості несанкціонованого доступу до елементів інформаційно-телекомунікаційних систем;

РН 31 – застосовувати теорії та методи захисту для забезпечення безпеки елементів інформаційно-телекомунікаційних систем;

РН 32 – вирішувати задачі управління процесами відновлення штатного функціонування інформаційно-телекомунікаційних систем з використанням процедур резервування згідно встановленої політики безпеки;

РН 33 – вирішувати задачі забезпечення безперервності бізнес процесів організації на основі теорії ризиків;

РН 34 – приймати участь у розробці та впровадженні стратегії інформаційної безпеки та/або кібербезпеки відповідно до цілей і завдань організації;

РН 35 – вирішувати задачі забезпечення та супроводу комплексних систем захисту інформації, а також протидії несанкціонованому доступу до інформаційних ресурсів і процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах згідно встановленої політики інформаційної та/або кібербезпеки;

РН 36 – виявляти небезпечні сигнали технічних засобів;

РН 37 – вимірювати параметри небезпечних та завадових сигналів під час інструментального контролю процесів захисту інформації та визначати ефективність захисту інформації від витoku технічними каналами відповідно до вимог нормативних документів системи технічного захисту інформації;

РН 38 – інтерпретувати результати проведення спеціальних вимірювань з використанням технічних засобів, контролю характеристик інформаційно-телекомунікаційних систем відповідно до вимог нормативних документів системи технічного захисту інформації;

РН 39 – проводити атестацію (спираючись на облік та обстеження) режимних територій (зон), приміщень тощо в умовах додержання режиму секретності із фіксуванням результатів у відповідних документах;

РН 40 – інтерпретувати результати проведення спеціальних вимірювань з використанням технічних засобів, контролю характеристик ІТС відповідно до вимог нормативних документів системи технічного захисту інформації;

РН 41 – забезпечувати неперервність процесу ведення журналів реєстрації подій та інцидентів на основі автоматизованих процедур;

РН 42 – впроваджувати процеси виявлення, ідентифікації, аналізу та реагування на інциденти інформаційної і/або кібербезпеки;

РН 43 – застосовувати національні та міжнародні регулюючі акти в сфері інформаційної безпеки та/ або кібербезпеки для розслідування інцидентів;

РН 44 – вирішувати задачі забезпечення безперервності бізнес-процесів організації на основі теорії ризиків та встановленої системи управління інформаційною безпекою, згідно з вітчизняними та міжнародними вимогами та стандартами;

РН 45 – застосовувати різні класи політик інформаційної безпеки та/ або кібербезпеки, що базуються на ризик-орієнтованому контролі доступу до інформаційних активів;

РН 46 – здійснювати аналіз та мінімізацію ризиків обробки інформації в інформаційно-телекомунікаційних системах;

РН 47 – вирішувати задачі захисту інформації, що обробляється в інформаційно-телекомунікаційних системах з використанням сучасних методів та засобів криптографічного захисту інформації;

РН 48 – виконувати впровадження та підтримку систем виявлення вторгнень та використовувати компоненти криптографічного захисту для забезпечення необхідного рівня захищеності інформації в інформаційно-телекомунікаційних системах;

РН 49 – забезпечувати належне функціонування системи моніторингу інформаційних ресурсів і процесів в інформаційно-телекомунікаційних системах;

РН 50 – забезпечувати) функціонування програмних та програмно-апаратних комплексів виявлення вторгнень різних рівнів та класів (статистичних, сигнатурних, статистично-сигнатурних);

РН 51 – підтримувати працездатність та забезпечувати конфігурування систем виявлення вторгнень в інформаційно-телекомунікаційних системах;

РН 52 – використовувати інструментарій для моніторингу процесів в інформаційно-телекомунікаційних системах;

РН 53 – вирішувати задачі аналізу програмного коду на наявність можливих загроз;

РН 54 – усвідомлювати цінності громадянського (вільного демократичного) суспільства та необхідність його сталого розвитку, верховенства права, прав і свобод людини і громадянина в Україні.

IV. СТРУКТУРА ОСВІТНЬОЇ ПРОГРАМИ ПІДГОТОВКИ БАКАЛАВРІВ

4.1. СТРУКТУРА ПРОГРАМИ ТА ОСВІТНІ КОМПОНЕНТИ

№	Освітні компоненти (навчальні дисципліни, курсові проекти (роботи), практики, кваліфікаційна робота)	Кредити ЄКТС	Структура, %
ЦИКЛ ЗАГАЛЬНОЇ ПІДГОТОВКИ			
1	<i>ОБОВ'ЯЗКОВІ ОСВІТНІ КОМПОНЕНТИ</i>	23	10
2	<i>ВИБІРКОВІ ОСВІТНІ КОМПОНЕНТИ</i>	25	10
ЦИКЛ ПРОФЕСІЙНОЇ ПІДГОТОВКИ			
3	<i>ОБОВ'ЯЗКОВІ ОСВІТНІ КОМПОНЕНТИ</i>	157	65
4	<i>ВИБІРКОВІ ОСВІТНІ КОМПОНЕНТИ</i>	35	15
ЗАГАЛЬНА КІЛЬКІСТЬ:		240	100%
<i>в тому числі: вибіркова складова</i>		60	25
Код ОК	Освітні компоненти (навчальні дисципліни, курсові проекти (роботи), практики, кваліфікаційна робота)	Кредити ЄКТС	Форми підсумкового контролю
ЦИКЛ ЗАГАЛЬНОЇ ПІДГОТОВКИ			
<i>ОБОВ'ЯЗКОВІ ОСВІТНІ КОМПОНЕНТИ</i>			
ОК1	Українська мова (за професійним спрямуванням)	3	ЗАЛІК
ОК2	Іноземна мова (за професійним спрямуванням)	9	ЗАЛІК, ЕКЗАМЕН
ОК3	Історія української культури	4	ЗАЛІК
ОК4	Філософія	5	ЕКЗАМЕН
ОК5	Тренінг-курс «Безпека життєдіяльності та охорона праці»	2	ЗАЛІК
<i>ВИБІРКОВІ ОСВІТНІ КОМПОНЕНТИ</i>			
ВК1	Навчальна дисципліна правового спрямування	5	ЗАЛІК
ВК2	Майнор або вільний майнор	5	ЗАЛІК
ВК3	Майнор або вільний майнор	5	ЗАЛІК
ВК4	Майнор або вільний майнор	5	ЗАЛІК
ВК5	Майнор або вільний майнор	5	ЗАЛІК
ЦИКЛ ПРОФЕСІЙНОЇ ПІДГОТОВКИ			
<i>ОБОВ'ЯЗКОВІ ОСВІТНІ КОМПОНЕНТИ</i>			
ОК 6	Вступ до фаху	6	ЗАЛІК
ОК 7	Основи алгоритмізації	6	ЕКЗАМЕН

ОК 8	Вища математика	15	ЗАЛІК, ЕКЗАМЕН
ОК 9	Програмування	10	ЕКЗАМЕН, ЕКЗАМЕН
ОК 10	Дискретна математика	5	ЗАЛІК
ОК 11	Математичні основи криптології	4	ЗАЛІК
ОК 12	Основи побудови та захисту сучасних операційних систем	5	ЕКЗАМЕН
ОК 13	Введення в мережі	5	ЕКЗАМЕН
ОК 14	Технології програмування	12	ЗАЛІК, ЕКЗАМЕН
ОК 15	Основи криптографічного захисту	5	ЕКЗАМЕН
ОК 16	Основи побудови та захисту мікропроцесорних систем	4	ЗАЛІК
ОК 17	Організаційне забезпечення захисту інформації	5	ЕКЗАМЕН
ОК 18	Основи математичного моделювання	4	ЗАЛІК
ОК 19	Розробка захищених мобільних застосунків	4	ЗАЛІК
ОК 20	Курсова робота: розробка захищених мобільних застосунків	1	КУРСОВА РОБОТА
ОК 21	Безпека в інформаційно-комунікаційних системах	5	ЕКЗАМЕН
ОК 22	Інформаційні системи та інтернет технології	12	ЕКЗАМЕН, ЕКЗАМЕН
ОК 23	Безпека інтернет-речей	6	ЕКЗАМЕН
ОК 24	Виробнича практика	3	ЗВІТ
ОК 25	Розробка захищених клієнт-серверних застосунків	4	ЗАЛІК
ОК 26	Курсова робота: розробка захищених клієнт-серверних застосунків	1	КУРСОВА РОБОТА
ОК 27	Іноземна мова академічної та професійної комунікації	4	ЗАЛІК
ОК 28	Комплексний курсовий проект	3	КОНСУЛЬТА- ЦІЙНИЙ ПРОЕКТ
ОК 29	Основи стеганографічного захисту інформації	4	ЗАЛІК
ОК 30	Хмарні технології та захист даних	4	ЗАЛІК
ОК 31	Комплексний тренінг	5	ЗВІТ
ОК 32	Переддипломна практика	5	ЗВІТ
ОК 33	Дипломний проект	10	ДИПЛОМНИЙ ПРОЕКТ

<i>ВИБІРКОВІ ОСВІТНІ КОМПОНЕНТИ</i>			
ВК6	Мейджор 1	5	ЕКЗАМЕН
ВК7	Мейджор 2	5	ЕКЗАМЕН
ВК8	Мейджор 3	5	ЕКЗАМЕН
ВК9	Мейджор 4	5	ЕКЗАМЕН
ВК10	Мейджор 5	5	ЕКЗАМЕН
ВК11	Мейджор 6	5	ЕКЗАМЕН
ВК12	Мейджор 7	5	ЕКЗАМЕН

4.2. ВИБІРКОВА СКЛАДОВА ОСВІТНЬО-ПРОФЕСІЙНОЇ ПРОГРАМИ

Вибіркова складова освітньо-професійної програми складається з:

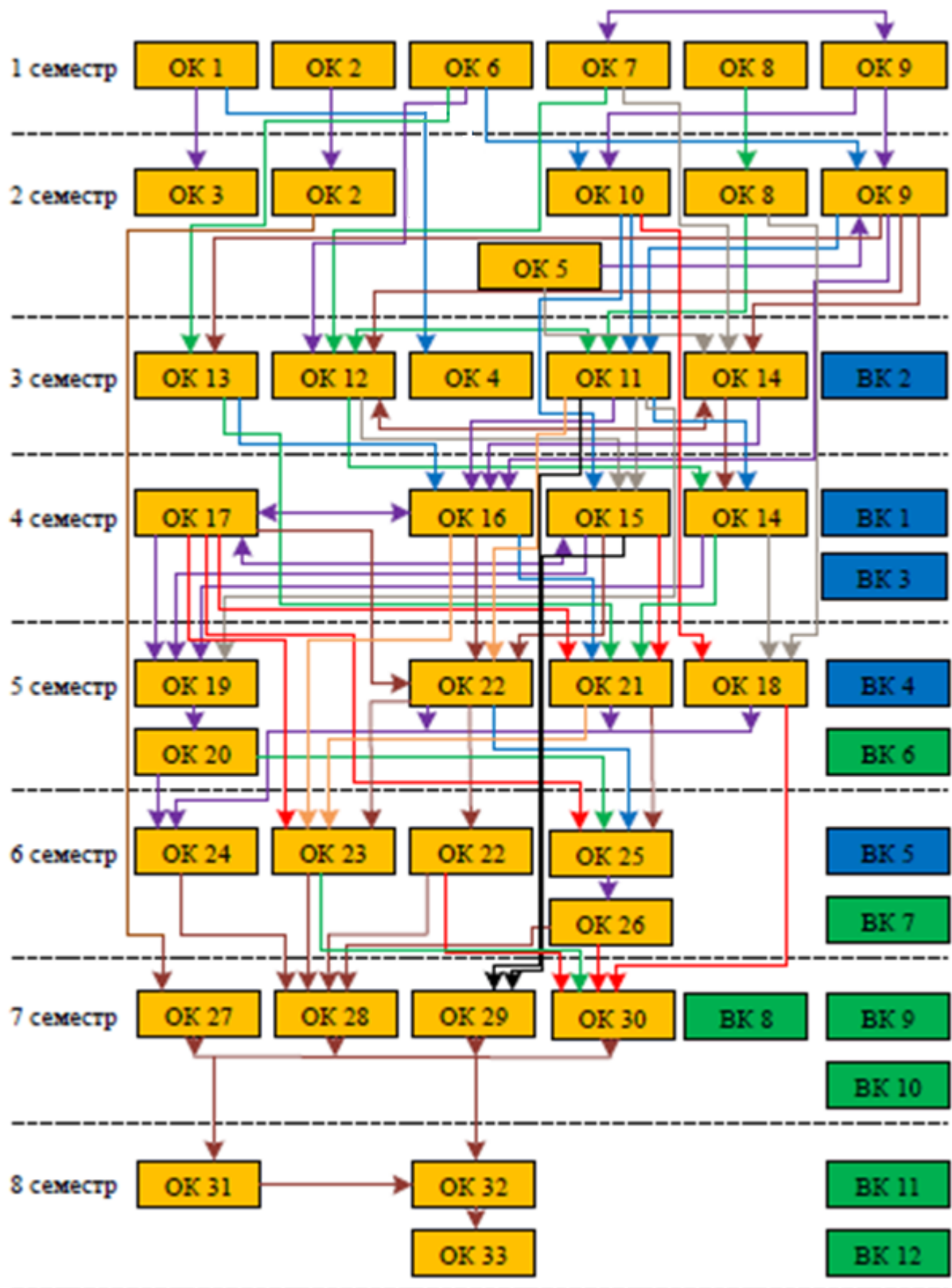
МАЙНОРІВ – блок взаємопов'язаних непрофільних навчальних дисциплін або **ВІЛЬНИЙ МАЙНОР** – окремі непрофільні навчальні дисципліни для створення власного МАЙНОРУ із загального переліку Університету (загально-університетський пул) для освітньо-кваліфікаційного рівня бакалавр. Дисципліни МАЙНОРІВ є обов'язковими для вибору здобувачами вищої освіти і входять до загального обсягу кредитів ЄКТС за освітньо-професійною програмою підготовки бакалаврів.

МЕЙДЖОР – профільні навчальні дисципліни освітньо-професійної програми, які поглиблюють професійну підготовку за певною спеціалізацією. Окрема дисципліна з обсягом 5 кредитів ЄКТС.

Дисципліна правового спрямування – окрема дисципліна з обсягом 5 кредитів ЄКТС. Загальний обсяг МАЙНОРІВ складає 20 кредитів ЄКТС (по 5 кредитів на дисципліну). Загальний обсяг МЕЙДЖЕРІВ складає 35 кредитів ЄКТС.

4.3. СТРУКТУРНО-ЛОГІЧНА СХЕМА ПІДГОТОВКИ ЗДОБУВАЧІВ ВИЩОЇ ОСВІТИ

освітньо-професійної програми «Кібербезпека» першого (бакалаврського) рівня вищої освіти



V. ФОРМИ АТЕСТАЦІЇ ЗДОБУВАЧІВ ВИЩОЇ ОСВІТИ

<p>Форми атестації здобувачів вищої освіти</p>	<p>Атестація здійснюється у формі єдиного державного кваліфікаційного іспиту.</p>
	<p>Атестація за освітньою програмою здійснюється екзаменаційною комісією після виконання студентом навчального плану у формі публічного захисту кваліфікаційної роботи бакалавра (дипломного проекту) за спеціальністю 125 Кібербезпека та захист інформації (денна форма, заочна форма). До атестації допускаються студенти, які виконали всі вимоги освітньої програми та навчального плану.</p>
<p>Вимоги до єдиного державного кваліфікаційного іспиту</p>	<p>Єдиний державний кваліфікаційний іспит передбачає оцінювання досягнень результатів навчання, визначених цим стандартом та освітньою програмою.</p>
<p>Вимоги до кваліфікаційної роботи (дипломного проекту)</p>	<p>Атестація осіб, які здобувають ступінь бакалавра, здійснюється екзаменаційною комісією (ЕК), до складу якої можуть включатися представники роботодавців та їх об'єднань. Атестація здійснюється відкрито і публічно. Дипломний проект – це робота здобувача, яка виконується на завершальному етапі здобуття кваліфікації бакалавра з кібербезпеки для встановлення відповідності отриманих здобувачами вищої освіти результатів навчання (компетентностей) вимогам освітньої програми. Вона є кваліфікаційним документом, на підставі якого ЕК визначає рівень теоретичної підготовки випускника, його готовність до самостійної роботи за фахом і приймає рішення щодо присвоєння відповідної кваліфікації та видачу диплома. Дипломний проект є інструментом закріплення та демонстрації сформованих упродовж навчання загальних та спеціальних компетентностей відповідно до освітньо-професійної програми.</p>
<p>Вимоги до публічного захисту</p>	<p>У процесі публічного захисту кандидат на присвоєння бакалаврського ступеня повинен показати уміння чітко і упевнено викладати зміст проведених досліджень, аргументовано відповідати на запитання та вести дискусію. Доповідь здобувача вищої освіти повинна супроводжуватися презентаційними матеріалами та пояснювальною запискою, призначеними для загального перегляду.</p>

VI. ВИМОГИ ДО НАЯВНОСТІ СИСТЕМИ ВНУТРІШНЬОГО ЗАБЕЗПЕЧЕННЯ ЯКОСТІ ВИЩОЇ ОСВІТИ

Визначаються відповідно до Європейських стандартів та рекомендацій щодо забезпечення якості вищої освіти (ESG) та статті 16 Закону України “Про вищу освіту”.

Політика щодо забезпечення якості вищої освіти	<p>Основні принципи внутрішнього забезпечення якості освіти у ХНЕУ ім. С. Кузнеця: відповідальності; відповідності; адекватності; автономності; вимірюваності; академічної культури; відкритості.</p> <p>Основні процедури внутрішнього забезпечення якості освіти в ХНЕУ ім. С. Кузнеця: формалізація політики якості, стратегічних цілей, завдань постійного поліпшення якості; забезпечення публічності інформації про освітні програми, ступені вищої освіти та кваліфікації; забезпечення дотримання академічної доброчесності працівниками закладів вищої освіти та здобувачами вищої освіти; підготовка та проведення маркетингово-моніторингових та соціально-психологічних досліджень для визначення потреб ринку праці, вимог стейкхолдерів вищої освіти, якості надання освітніх послуг і задоволеності якістю освітньої діяльності та якістю освіти; залучення стейкхолдерів вищої освіти (здобувачів вищої освіти, роботодавців, представників академічної спільноти тощо) до прийняття рішень за напрямками внутрішнього забезпечення якості; зовнішнє оцінювання якості діяльності ХНЕУ ім. С. Кузнеця за результатами участі в національних та міжнародних рейтингах вищих навчальних закладів, виконання Ліцензійних вимог, акредитації.</p> <p>Напрями: розроблення, затвердження, моніторинг та періодичний перегляд освітніх програм; забезпечення підвищення кваліфікації педагогічних, наукових і науково-педагогічних працівників; забезпечення студентоцентрованого навчання, викладання та оцінювання здобувачів вищої освіти; забезпечення наявності необхідних ресурсів для організації освітнього процесу; забезпечення наявності інформаційних систем для ефективного управління освітнім процесом.</p>
Забезпечення якості розроблення, затвердження, моніторингу, перегляду та оновлення освітніх програм	<p>Моніторинг та періодичний перегляд освітніх програм здійснюється згідно з діючими нормативними актами в ХНЕУ ім. С. Кузнеця.</p> <p>Перегляд освітніх програм здійснюється на основі аналізу задоволення освітніх потреб здобувачів вищої освіти: можливості побудови індивідуальної траєкторії навчання, дотримання академічних свобод в освітньому процесі, задоволеності якістю освітньої програми, тощо; роботодавців: якості формування загальних та фахових компетентностей, актуальних та соціальних навичок (softskills); інших стейкхолдерів.</p> <p>Для перегляду освітніх програм використовуються: онлайн опитування, проведення дослідження фокус-групи, аналіз документів, аналіз ситуації, самооцінка робочою групою відповідно до вимог щодо структури та змісту освітньої програми.</p> <p>Періодичність перегляду освітніх програм здійснюється: а)</p>

	щорічно за результатами моніторингу; б) після завершення освітньої програми здобувачами вищої освіти, в) в разі зміни н законодавчої та нормативної бази.
Забезпечення зарахування, досягнення, визнання та атестація здобувачів	<p>Оцінювання здобувачів вищої освіти є послідовним, прозорим та проводиться відповідно до встановлених в Університеті процедур згідно з нормативними актами.</p> <p>Щорічне оцінювання здобувачів освіти здійснюється відповідно до визначених освітньою програмою форм контролю; порядку оцінювання результатів навчання, що висвітлюється в робочих програмах навчальних дисциплін, робочих планах (технологічних картах) навчальних дисциплін, силабусах навчальних дисциплін; обліку результатів навчання, який ведеться з використанням програмного забезпечення корпоративної інформаційної системи управління (електронний журнал) та інформаційного середовища Персональної навчальної системи (ПНС) Університету. Оприлюднення результатів успішності, оцінювання результатів навчання відбувається через звіт «Інформація про поточну успішність та відвідування занять за навчальними дисциплінами семестру» (сайт Університету) та на сайті Персональних навчальних систем. Оцінювання здобувачів вищої освіти здійснюється на основі 100-бальної накопичувальної бально-рейтингової системи.</p>
Забезпечення якості студентоцентрованого навчання, викладання та оцінювання	<p>Планування, розподіл та надання навчальних ресурсів і забезпечення підтримки здобувачів вищої освіти враховують їх потреби та принципи студентоцентрованого навчання.</p> <p>Внутрішнє забезпечення якості вищої освіти гарантує, що всі необхідні ресурси відповідають цілям навчання, є загальнодоступними, а здобувачі вищої освіти поінформовані про їх наявність.</p>
Забезпечення якості науково-педагогічних працівників	<p>Щорічне рейтингове оцінювання діяльності науково-педагогічних працівників, кафедр і факультетів Університету здійснюється за рахунок використання механізмів оцінювання та самооцінювання результативності науково-педагогічної діяльності, її спрямованості на пріоритети розвитку національної системи вищої освіти, стратегії розвитку Університету, особистісного професійного розвитку науково-педагогічних працівників. Підсумки рейтингового оцінювання підводяться за результатами діяльності, досягнутими протягом навчального року. Оприлюднення результатів щорічного оцінювання науково-педагогічних працівників, кафедр та факультетів відбувається на засіданні вченої ради Університету.</p>
Ресурсне забезпечення освітнього процесу (навчальні ресурси та підтримка здобувачів вищої освіти)	<p>Заклад вищої освіти забезпечує освітній процес необхідними та доступними ресурсами (кадровими, методичними, матеріальними, інформаційними та ін.) та здійснює відповідну підтримку здобувачів вищої освіти.</p> <p>Організаційно-методична підтримка самостійної роботи здобувачів вищої освіти полягає у розробці методичних, дидактичних, інструктивних матеріалів, наданні можливості формувати, закріплювати, поглиблювати й систематизувати отримані під час аудиторних занять знання та вміння, здійснювати самопідготовку й самоконтроль опанування освітньої-професійної програми та реалізується через</p>

	Персональну навчальну систему ХНЕУ ім. С. Кузнеця.
Інформаційне забезпечення (інформаційний менеджмент)	З метою управління освітнім процесом розроблено ефективну політику в сфері інформаційного менеджменту та відповідну інтегровану інформаційну систему управління освітнім процесом. Дана система передбачає автоматизацію основних функцій управління освітнім процесом, зокрема: забезпечення проведення вступної кампанії, планування та організацію освітнього процесу; доступ до навчальних ресурсів; облік та аналіз успішності здобувачів вищої освіти; адміністрування основних та допоміжних процесів забезпечення освітньої діяльності; управління кадрами та ін.
Публічність інформації про освітні програми, освітню, наукову діяльність	Достовірна, об'єктивна, актуальна, своєчасна та легкодоступна інформація за освітньо-професійною програмою публікується на сайті ХНЕУ ім. С. Кузнеця, включаючи програми для потенційних здобувачів вищої освіти, випускників, інших стейкхолдерів і громадськості. Публічною є інформація про освітню діяльність за спеціальністю, включаючи критерії відбору на навчання; заплановані результати навчання за цією програмою; процедури навчання, викладання та оцінювання, що використовуються тощо.
Забезпечення академічної доброчесності	Забезпечення запобігання та виявлення академічного плагіату у наукових працях працівників закладу вищої освіти та здобувачів вищої освіти реалізується через політику, стандарти і процедури дотримання академічної доброчесності, регулюється такими документами ХНЕУ ім. С. Кузнеця: Кодекс академічної доброчесності; Кодекс професійної етики та організаційної культури працівників і здобувачів вищої освіти ХНЕУ ім. С. Кузнеця; Положення про комісію з питань академічної доброчесності ХНЕУ ім. С. Кузнеця. Перевірка наукових праць науково-педагогічних працівників Університету та здобувачів вищої освіти здійснюється за допомогою інтернет-сервісів на основі відкритих інтернет-ресурсів та системи StrikePlagiarism.com, що діє на підставі Ліцензійного Договору про надання права користування антиплагіатним програмним забезпеченням.

ПОЯСНЮВАЛЬНА ЗАПИСКА

Матриця відповідності визначених компетентностей дескрипторам НРК та матриця відповідності визначених результатів навчання та компетентностей представлені в Таблицях 1 і 2.

Таблиця 1
Матриця відповідності визначених компетентностей дескрипторам НРК

Класифікація компетентностей за НРК	Знання	Уміння	Комунікація	Автономія та відповідальність
ЗАГАЛЬНІ КОМПЕТЕНТНОСТІ				
КЗ 1. Здатність застосовувати знання у практичних ситуаціях.	+	+		
КЗ 2. Знання та розуміння предметної області та розуміння професії.	+	+		
КЗ 3. Здатність професійно спілкуватися державною та іноземною мовами як усно, так і письмово	+	+	+	
КЗ 4. Вміння виявляти, ставити та вирішувати проблеми за професійним спрямуванням	+	+	+	+
КЗ 5. Здатність до пошуку, оброблення та аналізу інформації.	+	+		+
КЗ 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.		+	+	+
КЗ 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.		+	+	+
СПЕЦІАЛЬНІ (ФАХОВІ) КОМПЕТЕНТНОСТІ				
КФ 1. Здатність застосовувати законодавчу та нормативно-правову базу, а також державні та міжнародні вимоги, практики і стандарти з метою здійснення професійної діяльності в галузі інформаційної та/або кібербезпеки.		+		+
КФ 2. Здатність до використання інформаційно-комунікаційних технологій, сучасних методів і моделей інформаційної безпеки та/або кібербезпеки.	+	+		+

Класифікація компетентностей за НРК	Знання	Уміння	Комунікація	Автономія та відповідальність
КФ 3. Здатність до використання програмних та програмно-апаратних комплексів засобів захисту інформації в інформаційно-телекомунікаційних (автоматизованих) системах.	+	+		+
КФ 4. Здатність забезпечувати неперервність бізнесу згідно встановленої політики інформаційної та/або кібербезпеки.	+	+	+	
КФ 5. Здатність забезпечувати захист інформації, що обробляється в інформаційно-телекомунікаційних (автоматизованих) системах з метою реалізації встановленої політики інформаційної та/або кібербезпеки.	+	+		+
КФ 6. Здатність відновлювати штатне функціонування інформаційних, інформаційно-телекомунікаційних (автоматизованих) систем після реалізації загроз, здійснення кібератак, збоїв та відмов різних класів та походження.	+	+	+	
КФ 7. Здатність впроваджувати та забезпечувати функціонування комплексних систем захисту інформації (комплекси нормативно-правових, організаційних та технічних засобів і методів, процедур, практичних прийомів та ін.)	+		+	
КФ 8. Здатність здійснювати процедури управління інцидентами, проводити розслідування, надавати їм оцінку.	+	+		+
КФ 9. Здатність здійснювати професійну діяльність на основі впровадженої системи управління інформаційною та/або кібербезпекою.	+	+	+	
КФ 10. Здатність застосовувати методи та засоби криптографічного та технічного захисту інформації на об'єктах інформаційної діяльності.	+	+	+	
КФ 11. Здатність виконувати моніторинг процесів функціонування інформаційних, інформаційно-телекомунікаційних (автоматизованих) систем згідно встановленої політики інформаційної та/або кібербезпеки.	+	+		+
КФ 12. Здатність аналізувати, виявляти та оцінювати можливі загрози, уразливості та дестабілізуючі чинники інформаційному простору та інформаційним ресурсам згідно з встановленою політикою інформаційної та/або кібербезпеки	+	+		+

Результати навчання	Компетентності																		
	Загальні							Спеціальні (фахові)											
	КЗ1	КЗ2	КЗ3	КЗ4	КЗ5	КЗ6	КЗ7	КФ1	КФ2	КФ3	КФ4	КФ5	КФ6	КФ7	КФ8	КФ9	КФ10	КФ11	КФ12
		OK31 OK32 OK33		OK31 OK32 OK33				OK31 OK32 OK33											
PH 8		OK6 OK17 OK21 OK24 OK25 OK31 OK32 OK33		OK6 OK17 OK21 OK24 OK25 OK31 OK32 OK33				OK6 OK17 OK21 OK24 OK25 OK31 OK32 OK33											
PH 9					OK6 OK12 OK16 OK17 OK19 OK20 OK23 OK25 OK26 OK30			OK6 OK12 OK16 OK17 OK19 OK20 OK23 OK25 OK26 OK30		OK6 OK12 OK16 OK17 OK19 OK20 OK23 OK25 OK26 OK30	OK6 OK12 OK16 OK17 OK19 OK20 OK23 OK25 OK26 OK30	OK6 OK12 OK16 OK17 OK19 OK20 OK23 OK25 OK26 OK30		OK6 OK12 OK16 OK17 OK19 OK20 OK23 OK25 OK26 OK30	OK6 OK12 OK16 OK17 OK19 OK20 OK23 OK25 OK26 OK30	OK6 OK12 OK16 OK17 OK19 OK20 OK23 OK25 OK26 OK30		OK6 OK12 OK16 OK17 OK19 OK20 OK23 OK25 OK26 OK30	OK6 OK12 OK16 OK17 OK19 OK20 OK23 OK25 OK26 OK30
PH 10	OK7 OK10 OK12 OK15 OK16 OK21								OK7 OK10 OK12 OK15 OK16 OK21									OK7 OK10 OK12 OK15 OK16 OK21	
PH 11	OK12 OK13 OK16 OK19 OK20 OK25 OK26 OK30								OK12 OK13 OK16 OK19 OK20 OK25 OK26 OK30									OK12 OK13 OK16 OK19 OK20 OK25 OK26 OK30	
PH 12														OK9 OK10 OK13 OK14 OK18					OK9 OK10 OK13 OK14 OK18

Результати навчання	Компетентності																		
	Загальні							Спеціальні (фахові)											
	КЗ1	КЗ2	КЗ3	КЗ4	КЗ5	КЗ6	КЗ7	КФ1	КФ2	КФ3	КФ4	КФ5	КФ6	КФ7	КФ8	КФ9	КФ10	КФ11	КФ12
														OK21 OK22					OK21 OK22
PH 13					OK12 OK16 OK17 OK21 OK25 OK26 OK30				OK12 OK16 OK17 OK21 OK25 OK26 OK30			OK12 OK16 OK17 OK21 OK25 OK26 OK30			OK12 OK16 OK17 OK21 OK25 OK26 OK30			OK12 OK16 OK17 OK21 OK25 OK26 OK30	OK12 OK16 OK17 OK21 OK25 OK26 OK30
PH 14									OK11 OK15 OK19 OK20 OK21 OK25 OK26 OK29 OK30 OK31	OK11 OK15 OK19 OK20 OK21 OK25 OK26 OK29 OK30 OK31		OK11 OK15 OK19 OK20 OK21 OK25 OK26 OK29 OK30 OK31			OK11 OK15 OK19 OK20 OK21 OK25 OK26 OK29 OK30 OK31		OK11 OK15 OK19 OK20 OK21 OK25 OK26 OK29 OK30 OK31	OK11 OK15 OK19 OK20 OK21 OK25 OK26 OK29 OK30 OK31	
PH 15									OK11 OK15 OK19 OK20 OK21 OK25 OK26 OK29 OK30 OK31	OK11 OK15 OK19 OK20 OK21 OK25 OK26 OK29 OK30 OK31								OK11 OK15 OK19 OK20 OK21 OK25 OK26 OK29 OK30 OK31	
PH 16								OK17 OK21 OK28 OK29		OK17 OK21 OK28 OK29				OK17 OK21 OK28 OK29					OK17 OK21 OK28 OK29
PH 17		OK7 OK12 OK13 OK16 OK19 OK21 OK23							OK7 OK12 OK13 OK16 OK19 OK21 OK23	OK7 OK12 OK13 OK16 OK19 OK21 OK23	OK7 OK12 OK13 OK16 OK19 OK21 OK23	OK7 OK12 OK13 OK16 OK19 OK21 OK23	OK7 OK12 OK13 OK16 OK19 OK21 OK23		OK7 OK12 OK13 OK16 OK19 OK21 OK23			OK7 OK12 OK13 OK16 OK19 OK21 OK23	

Результати навчання	Компетентності																		
	Загальні							Спеціальні (фахові)											
	КЗ1	КЗ2	КЗ3	КЗ4	КЗ5	КЗ6	КЗ7	КФ1	КФ2	КФ3	КФ4	КФ5	КФ6	КФ7	КФ8	КФ9	КФ10	КФ11	КФ12
		OK25 OK29 OK30							OK25 OK29 OK30	OK25 OK29 OK30	OK25 OK29 OK30	OK25 OK29 OK30	OK25 OK29 OK30		OK25 OK29 OK30				OK25 OK29 OK30
PH 18	OK14 OK15 OK16 OK19 OK20 OK21 OK22 OK23 OK25 OK26 OK29 OK30								OK14 OK15 OK16 OK19 OK20 OK21 OK22 OK23 OK25 OK26 OK29 OK30	OK14 OK15 OK16 OK19 OK20 OK21 OK22 OK23 OK25 OK26 OK29 OK30		OK14 OK15 OK16 OK19 OK20 OK21 OK22 OK23 OK25 OK26 OK29 OK30							OK14 OK15 OK16 OK19 OK20 OK21 OK22 OK23 OK25 OK26 OK29 OK30
PH 19	OK11 OK15 OK16 OK17 OK19 OK21 OK23 OK25 OK29								OK11 OK15 OK16 OK17 OK19 OK21 OK23 OK25 OK29			OK11 OK15 OK16 OK17 OK19 OK21 OK23 OK25 OK29		OK11 OK15 OK16 OK17 OK19 OK21 OK23 OK25 OK29					OK11 OK15 OK16 OK17 OK19 OK21 OK23 OK25 OK29
PH 20	OK12 OK14 OK16 OK19 OK21 OK25 OK29 OK30								OK12 OK14 OK16 OK19 OK21 OK25 OK29 OK30	OK12 OK14 OK16 OK19 OK21 OK25 OK29 OK30		OK12 OK14 OK16 OK19 OK21 OK25 OK29 OK30	OK12 OK14 OK16 OK19 OK21 OK25 OK29 OK30						OK12 OK14 OK16 OK19 OK21 OK25 OK29 OK30
PH 21	OK17 OK21 OK28											OK17 OK21 OK28				OK17 OK21 OK28			OK17 OK21 OK28
PH 22	OK12 OK16 OK19 OK20 OK21											OK12 OK16 OK19 OK20 OK21							OK12 OK16 OK19 OK20 OK21

Результати навчання	Компетентності																			
	Загальні							Спеціальні (фахові)												
	КЗ1	КЗ2	КЗ3	КЗ4	КЗ5	КЗ6	КЗ7	КФ1	КФ2	КФ3	КФ4	КФ5	КФ6	КФ7	КФ8	КФ9	КФ10	КФ11	КФ12	
	OK25 OK26 OK29 OK30											OK25 OK26 OK29 OK30						OK25 OK26 OK29 OK30		
PH 23												OK15 OK19 OK20 OK21 OK22 OK23 OK25 OK26 OK30	OK15 OK19 OK20 OK21 OK22 OK23 OK25 OK26 OK30		OK15 OK19 OK20 OK21 OK22 OK23 OK25 OK26 OK30			OK15 OK19 OK20 OK21 OK22 OK23 OK25 OK26 OK30		
PH 24	OK15 OK19 OK21 OK25 OK29 OK30										OK15 OK19 OK21 OK25 OK29 OK30	OK15 OK19 OK21 OK25 OK29 OK30				OK15 OK19 OK21 OK25 OK29 OK30		OK15 OK19 OK21 OK25 OK29 OK30		
PH 25												OK17 OK19 OK20 OK21 OK25 OK26 OK29 OK30			OK17 OK19 OK20 OK21 OK25 OK26 OK29 OK30	OK17 OK19 OK20 OK21 OK25 OK26 OK29 OK30		OK17 OK19 OK20 OK21 OK25 OK26 OK29 OK30		
PH 26												OK12 OK16 OK19 OK25 OK30						OK12 OK16 OK19 OK25 OK30		
PH 27	OK12 OK16 OK19 OK21 OK25 OK29 OK30										OK12 OK16 OK19 OK21 OK25 OK29 OK30	OK12 OK16 OK19 OK21 OK25 OK29 OK30	OK12 OK16 OK19 OK21 OK25 OK29 OK30							
PH 28					OK19							OK19				OK19			OK19	

Результати навчання	Компетентності																		
	Загальні							Спеціальні (фахові)											
	КЗ1	КЗ2	КЗ3	КЗ4	КЗ5	КЗ6	КЗ7	КФ1	КФ2	КФ3	КФ4	КФ5	КФ6	КФ7	КФ8	КФ9	КФ10	КФ11	КФ12
					OK23 OK25 OK30							OK23 OK25 OK30				OK23 OK25 OK30			OK23 OK25 OK30
PH 29										OK19 OK21 OK22 OK25 OK28 OK30 OK32	OK19 OK21 OK22 OK25 OK28 OK30 OK32	OK19 OK21 OK22 OK25 OK28 OK30 OK32			OK19 OK21 OK22 OK25 OK28 OK30 OK32	OK19 OK21 OK22 OK25 OK28 OK30 OK32			OK19 OK21 OK22 OK25 OK28 OK30 OK32
PH 30																			OK13 OK18 OK22
PH 31									OK11 OK13 OK14 OK15 OK16 OK21 OK22 OK23 OK31 OK32				OK11 OK13 OK14 OK15 OK16 OK21 OK22 OK23 OK31 OK32					OK11 OK13 OK14 OK15 OK16 OK21 OK22 OK23 OK31 OK32	
PH 32	OK11 OK15 OK19 OK20 OK25 OK26 OK29 OK30										OK11 OK15 OK19 OK20 OK25 OK26 OK29 OK30	OK11 OK15 OK19 OK20 OK25 OK26 OK29 OK30			OK11 OK15 OK19 OK20 OK25 OK26 OK29 OK30			OK11 OK15 OK19 OK20 OK25 OK26 OK29 OK30	
PH 33							OK8 OK17 OK18				OK8 OK17 OK18			OK8 OK17 OK18	OK8 OK17 OK18				OK8 OK17 OK18
PH 34							OK6 OK17 OK21 OK28 OK31 OK32				OK6 OK17 OK21 OK28 OK31 OK32	OK6 OK17 OK21 OK28 OK31 OK32			OK6 OK17 OK21 OK28 OK31 OK32	OK6 OK17 OK21 OK28 OK31 OK32			OK6 OK17 OK21 OK28 OK31 OK32

Результати навчання	Компетентності																			
	Загальні							Спеціальні (фахові)												
	КЗ1	КЗ2	КЗ3	КЗ4	КЗ5	КЗ6	КЗ7	КФ1	КФ2	КФ3	КФ4	КФ5	КФ6	КФ7	КФ8	КФ9	КФ10	КФ11	КФ12	
								OK33			OK33	OK33			OK33	OK33			OK33	
PH 35	OK19 OK20 OK21 OK22 OK25 OK26 OK30 OK31							OK19 OK20 OK21 OK22 OK25 OK26 OK30 OK31		OK19 OK20 OK21 OK22 OK25 OK26 OK30 OK31	OK19 OK20 OK21 OK22 OK25 OK26 OK30 OK31	OK19 OK20 OK21 OK22 OK25 OK26 OK30 OK31		OK19 OK20 OK21 OK22 OK25 OK26 OK30 OK31	OK19 OK20 OK21 OK22 OK25 OK26 OK30 OK31	OK19 OK20 OK21 OK22 OK25 OK26 OK30 OK31				OK19 OK20 OK21 OK22 OK25 OK26 OK30 OK31
PH 36																			OK21 OK23	
PH 37													OK12 OK16 OK21 OK29						OK12 OK16 OK21 OK29	
PH 38													OK12 OK16 OK21 OK29						OK12 OK16 OK21 OK29	
PH 39																			OK6 OK17	
PH 40																			OK12 OK15 OK16 OK23	
PH 41															OK17 OK19 OK21 OK25 OK29				OK17 OK19 OK21 OK25 OK29	
PH 42											OK6 OK10 OK17 OK21 OK31 OK32 OK33	OK6 OK10 OK17 OK21 OK31 OK32 OK33			OK6 OK10 OK17 OK21 OK31 OK32 OK33	OK6 OK10 OK17 OK21 OK31 OK32 OK33			OK6 OK10 OK17 OK21 OK31 OK32 OK33	OK6 OK10 OK17 OK21 OK31 OK32 OK33
PH 43		OK6 OK17 OK21						OK6 OK17 OK21			OK6 OK17 OK21	OK6 OK17 OK21			OK6 OK17 OK21	OK6 OK17 OK21			OK6 OK17 OK21	OK6 OK17 OK21

Результати навчання	Компетентності																			
	Загальні							Спеціальні (фахові)												
	КЗ1	КЗ2	КЗ3	КЗ4	КЗ5	КЗ6	КЗ7	КФ1	КФ2	КФ3	КФ4	КФ5	КФ6	КФ7	КФ8	КФ9	КФ10	КФ11	КФ12	
		OK23 OK30 OK32 OK33						OK23 OK30 OK32 OK33			OK23 OK30 OK32 OK33	OK23 OK30 OK32 OK33			OK23 OK30 OK32 OK33	OK23 OK30 OK32 OK33		OK23 OK30 OK32 OK33	OK23 OK30 OK32 OK33	
PH 44								OK8 OK17 OK18 OK21 OK23 OK30			OK8 OK17 OK18 OK21 OK23 OK30	OK8 OK17 OK18 OK21 OK23 OK30			OK8 OK17 OK18 OK21 OK23 OK30	OK8 OK17 OK18 OK21 OK23 OK30			OK8 OK17 OK18 OK21 OK23 OK30	
PH 45											OK12 OK16 OK19 OK21 OK22 OK23 OK25 OK29 OK30 OK32	OK12 OK16 OK19 OK21 OK22 OK23 OK25 OK29 OK30 OK32			OK12 OK16 OK19 OK21 OK22 OK23 OK25 OK29 OK30 OK32	OK12 OK16 OK19 OK21 OK22 OK23 OK25 OK29 OK30 OK32				OK12 OK16 OK19 OK21 OK22 OK23 OK25 OK29 OK30 OK32
PH 46											OK17 OK18 OK21 OK22	OK17 OK18 OK21 OK22			OK17 OK18 OK21 OK22	OK17 OK18 OK21 OK22			OK17 OK18 OK21 OK22	
PH 47									OK11 OK15 OK16 OK21 OK25 OK29	OK11 OK15 OK16 OK21 OK25 OK29	OK11 OK15 OK16 OK21 OK25 OK29						OK11 OK15 OK16 OK21 OK25 OK29			
PH 48											OK11 OK15 OK16 OK21 OK25 OK29	OK11 OK15 OK16 OK21 OK25 OK29			OK11 OK15 OK16 OK21 OK25 OK29		OK11 OK15 OK16 OK21 OK25 OK29	OK11 OK15 OK16 OK21 OK25 OK29		
PH 49											OK12 OK16 OK19 OK20	OK12 OK16 OK19 OK20			OK12 OK16 OK19 OK20			OK12 OK16 OK19 OK20		




Результати навчання	Компетентності																		
	Загальні							Спеціальні (фахові)											
	КЗ1	КЗ2	КЗ3	КЗ4	КЗ5	КЗ6	КЗ7	КФ1	КФ2	КФ3	КФ4	КФ5	КФ6	КФ7	КФ8	КФ9	КФ10	КФ11	КФ12
												OK21	OK21		OK21			OK21	
												OK22	OK22		OK22			OK22	
												OK23	OK23		OK23			OK23	
												OK25	OK25		OK25			OK25	
												OK26	OK26		OK26			OK26	
												OK29	OK29		OK29			OK29	
												OK30	OK30		OK30			OK30	
PH 50										OK12		OK12			OK12			OK12	
										OK16		OK16			OK16			OK16	
										OK19		OK19			OK19			OK19	
										OK25		OK25			OK25			OK25	
										OK29		OK29			OK29			OK29	
										OK30		OK30			OK30			OK30	
PH 51												OK12			OK12			OK12	
												OK16			OK16			OK16	
												OK19			OK19			OK19	
												OK25			OK25			OK25	
												OK29			OK29			OK29	
												OK30			OK30			OK30	
PH 52												OK12	OK12		OK12			OK12	
												OK16	OK16		OK16			OK16	
												OK19	OK19		OK19			OK19	
												OK25	OK25		OK25			OK25	
												OK29	OK29		OK29			OK29	
												OK30	OK30		OK30			OK30	
PH 53	OK9			OK9					OK9	OK9	OK9	OK9	OK9		OK9			OK9	OK9
	OK14			OK14					OK14	OK14	OK14	OK14	OK14		OK14			OK14	OK14
	OK19			OK19					OK19	OK19	OK19	OK19	OK19		OK19			OK19	OK19
	OK20			OK20					OK20	OK20	OK20	OK20	OK20		OK20			OK20	OK20
	OK25			OK25					OK25	OK25	OK25	OK25	OK25		OK25			OK25	OK25
	OK26			OK26					OK26	OK26	OK26	OK26	OK26		OK26			OK26	OK26
	OK29			OK29					OK29	OK29	OK29	OK29	OK29		OK29			OK29	OK29
PH 54	OK3	OK3				OK3	OK3												
	OK4	OK4				OK4	OK4												
	OK5	OK5				OK5	OK5												

Гарант ОП

підписано

Вячеслав ЛИМАРЕНКО

ЛИСТ ПОГОДЖЕННЯ
Освітньо-професійної програми «Кібербезпека»

Назва структурного / функціонального підрозділу / посадова особа	Підпис
1. Навчально-методичний відділ	
2. Відділ забезпечення якості освіти	
3. Завідувач випускової кафедри	
4. Проректор з навчально-методичної роботи	