ПРОЄКТ освітньо програми для обговорення на 2025-2026 навчальний рік

ОСВІТНЬО-ПРОФЕСІЙНА ПРОГРАМА
«Кібербезпека»

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

ПРЕАМБУЛА

Робоча група освітньо-професійної 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.

Бойко Софія Олегівна, здобувач вищої освіти.

Губін Андрій Михайлович, Security Consultant, Engineering, GlobalLogic Ukraine.

ОП розроблена/оновлена на підставі:

1. Законодавчих та нормативних актів: Законів України «Про освіту», «Про вищу освіту», Національної рамки кваліфікації, Національного класифікатору України.
2. Стандарту вищої освіти за спеціальністю 125 «Кібербезпека» галузі знань 12 «Інформаційні технології» для першого (бакалаврського) рівня вищої освіти, затвердженого наказом Міністерства освіти і науки України від 29.10.2024 р. № 1547.
3. Аналізу ринку праці, з урахуванням регіонального контексту.
4. Вивчення вітчизняного та зарубіжного досвіду.
5. Пропозицій роботодавців.
6. Рекомендації після процедур акредитації освітньої програми Національним агентством із забезпечення якості вищої освіти, протокол № 7 (50) від 27 квітня 2021 року.

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	На базі повної загальної середньої освіти: денна форма – 240 кредитів, 3 роки 10 місяців. На базі ступеня «молодший бакалавр» (освітньо-кваліфікаційного рівня «молодший спеціаліст»): денна форма – 240 кредитів, 2 роки 10 місяців.
Наявність акредитації	Сертифікат про акредитацію освітньої програми НАЗЯВО № 1484, дійсний до 01.07.2026 р.
Мова(и) навчання / оцінювання	українська
Структурний підрозділ відповідальний за ОП	Кафедра кібербезпеки та інформаційних технологій; https://www.kafcbit.hneu.edu.ua/
Вимоги до зарахування	Вступ на перший (бакалаврський) рівень вищої освіти здійснюється відповідно до Правил прийому та Порядку прийому на навчання для здобуття вищої освіти. Правила та строки прийому на навчання розміщенні на сайті ХНЕУ ім. С. Кузнеця за посиланням https://pk.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	Денна, заочна, дистанційна
Освітня кваліфікація	Бакалавр з кібербезпеки та захисту інформації
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’єкти вивчення:** технології кібербезпеки та захисту інформації; процеси управління кібербезпекою та захистом інформації; об'єкти інформаційної діяльності, в тому числі інформаційні та Інформаційно-комунікаційні системи, інформаційні ресурси і технології. **Цілі навчання:** підготовка фахівців, здатних

	використовувати і впроваджувати технології кібербезпеки та захисту інформації та розв'язувати складні задачі у галузі кібербезпеки та захисту інформації. **Теоретичний зміст предметної області: п**ринципи, концепції, теорії захисту життєво важливих інтересів людини, суспільства, держави під час використання кіберпростору, за якого забезпечуються сталий розвиток інформаційного суспільства та цифрового комунікативного середовища, своєчасне виявлення, запобігання і нейтралізація реальних і потенційних загроз національній безпеці України у кіберпросторі. **Методи, методики та технології:** методи, методики та технології розв'язання теоретичних і практичних задач кібербезпеки та захисту інформації. **Інструменти та обладнання:** засоби, пристрої, мережне устаткування, прикладне та спеціалізоване програмне забезпечення, інформаційні системи та комплекси проектування, моделювання, контролю, моніторингу, зберігання, обробки, відображення та захисту даних (інформаційних потоків), спеціалізований клас (кіберполігон).
Академічна мобільність	-
Академічні права	Мають право на здобуття освіти на другому (магістерському) рівні вищої освіти. Здобуття або вдосконалення освіти та професійної підготовки в системі освіти дорослих.
Професійні права	-
Працевлаштування випускників	Професії, на підготовку з яких спрямована ОП (згідно з чинною редакцією Національного класифікатора України: Класифікатор професій ДК 003:2010): адміністратор безпеки мереж і систем, 2139.2; фахівець сфери захисту інформації, 2139.2; фахівець з питань безпеки (Інформаційно-комунікаційні технології), 2139.2; конструктор систем кібербезпеки, 2132.2; фахівець з підтримки інфраструктури кіберзахисту, 2139.2; фахівець з реагування на інциденти кібербезпеки, 2139.2; фахівець з криптографічного захисту інформації, 2139.2; фахівець з технічного захисту інформації, 2139.2; фахівець з тестування систем захисту інформації, 2139.2; аудитор інформаційних технологій (з кібербезпеки), 2139.2; фахівець з оцінки заходів захисту інформації (кібербезпеки), 2139.2. А також на посади у структурних підрозділах установ/підприємств/організацій, які передбачають наявність вищої освіти зі спеціальності 125 Кібербезпека та захист інформації
Силабуси освітніх компонентів	https://www.hneu.edu.ua/informatsijnyj-paket-bakalavr-kiberbezpeka-2024/

ІІ – ПЕРЕЛІК КОМПЕТЕНТНОСТЕЙ ВИПУСКНИКА

Інтегральна компетентність	Здатність розв'язувати складні спеціалізовані задачі і практичні завдання у галузі кібербезпеки та захисту інформації.

Загальні компетентності	**ЗК1.** Здатність застосовувати знання у практичних ситуаціях. **ЗК2.** Знання та розуміння предметної області і розуміння професійної діяльності. **ЗК3.** Здатність спілкуватися державною мовою як усно, так і письмово. **ЗК4.** Здатність спілкуватися іноземною мовою. **ЗК5.** Здатність вчитися і оволодівати сучасними знаннями. **ЗК6.** Здатність реалізувати свої права і обов'язки як члена суспільства, усвідомлювати цінності громадянського (вільного демократичного) суспільства та необхідність його сталого розвитку, верховенства права, прав та свобод людини і громадянина в Україні. **ЗК7.** Здатність ухвалювати рішення й діяти дотримуючись принципу неприпустимості корупції та будь-яких інших проявів недоброчесності. **ЗК8.** 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, предметні) компетентності	**СК1.** Здатність застосовувати законодавчу та нормативно-правову базу, а також державні і міжнародні вимоги, практики і стандарти у професійній діяльності. **СК2.** Здатність використовувати інформаційні технології, сучасні методи і моделі кібербезпеки та системи захисту інформації. **СК3.** Здатність забезпечувати неперервність бізнес-процесів згідно встановленої політики кібербезпеки та захисту інформації. **СК4.** Здатність забезпечувати захист Інформації в інформаційних та інформаційно-комунікаційних системах згідно встановленої політики кібербезпеки й захисту інформації. **СК5.** Здатність відновлювати функціонування Інформаційних та інформаційно-комунікаційних систем після реалізації загроз, здійснення кібератак, збоїв і відмов різних класів та походження. **СК6.** Здатність впроваджувати та забезпечувати функціонування комплексних систем захисту інформації (комплекси нормативно-правових, організаційних та технічних засобів і методів, процедур, практичних прийомів тощо). **СК7.** Здатність здійснювати професійну діяльність на основі впровадженої системи управління інформаційною та кібербезпекою. **СК8.** Здатність застосовувати методи та засоби криптографічного захисту інформації на об'єктах інформаційної діяльності. **СК9.** Здатність застосовувати методи та засоби технічного

	захисту Інформації на об’єктах інформаційної діяльності. **СК10.** Здатність виконувати моніторинг інформаційних процесів, аналізувати, виявляти, оцінювати можливі вразливості та загрози інформаційному простору й інформаційним ресурсам згідно з встановленою політикою інформаційної безпеки.

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**).

ІІІ – НОРМАТИВНИЙ ЗМІСТ ПІДГОТОВКИ ЗДОБУВАЧІВ ВИЩОЇ ОСВІТИ, СФОРМУЛЬОВАНИЙ У ТЕРМІНАХ РЕЗУЛЬТАТІВ НАВЧАННЯ ЗА СПЕЦІАЛЬНІСТЮ 125 КІБЕРБЕЗПЕКА ТА ЗАХИСТ ІНФОРМАЦІЇ ОПП «КІБЕРБЕЗПЕКА»

РН1. Вільно спілкуватися державною мовою усно та письмово при виконанні професійних обов’язків.

РН2. Спілкуватися іноземною мовою з метою забезпечення ефективності професійної комунікації.

РН3. Застосовувати принцип неприпустимості корупції та будь-яких інших проявів недоброчесності у професійній діяльності.

РН4. Організовувати власну професійну діяльність, обирати і використовувати оптимальні методи та способи розв’язання складних спеціалізованих задач і практичних проблем у професійній діяльності, оцінювати їхню ефективність.

РН5. Аналізувати, аргументувати, приймати рішення при розв’язанні складних спеціалізованих задач і практичних завдань у професійній діяльності, які характеризуються комплексністю та неповною визначеністю умов, відповідати за прийняті рішення.

РН6. Адаптуватися до нових умов і технологій професійної діяльності, прогнозувати кінцевий результат.

РН7. Застосовувати й адаптувати теорії інформації та кодування, математичної статистики, чисел, криптографії та стеганографії, оброблення і передачі сигналів тощо, принципи, методи, поняття кібербезпеки та захисту інформації у навчанні та професійній діяльності.

РН8. Застосовувати знання й розуміння математики та фізики в професійній діяльності, формалізувати задачі предметної галузі кібербезпеки та захисту інформації, формулювати їх математичну постановку та обирати раціональний метод вирішення.

РН9. Знати та застосовувати законодавство України та міжнародні вимоги, практики і стандарти з метою здійснення професійної діяльності в галузі кібербезпеки та захисту інформації.

РН10. Використовувати сучасні інформаційні технології, методи і моделі кібербезпеки та систем захисту інформації для здійснення професійної діяльності.

РН11. Планувати підготовку та забезпечувати неперервність бізнес-процесів в організаціях згідно зі встановленою політикою кібербезпеки з урахування вимог до захисту інформації.

РН12. Застосовувати методи та засоби захисту інформації в інформаційних та інформаційно-комунікаційних системах відповідно до встановленої політики інформаційної безпеки.

РН13. Впроваджувати, налаштовувати, супроводжувати та підтримувати функціонування програмних і програмно-апаратних комплексів і систем кібербезпеки та захисту інформації як необхідні процедури для функціонування інформаційних й Інформаційно-комунікаційних систем та\або інфраструктури організації в цілому.

РН14. Вирішувати задачі управління процесами відновлення штатного функціонування інформаційних та інформаційно-комунікаційних систем з використанням процедур резервування згідно встановленої політики безпеки і забезпечувати функціонування спеціального програмного забезпечення щодо захисту та відновлення інформації.

РН15. Збирати, обробляти, зберігати, аналізувати критичні дані для доказу реалізації кіберзагроз, проводити аналіз та дослідження кіберінциденту з метою оперативного відновлення функціонування інформаційної системи.

РН16. Вирішувати задачі впровадження та супроводу комплексних систем захисту інформації в інформаційних системах.

РН17. Забезпечувати функціонування системи управління кібербезпекою і захистом інформації організації, включаючи персонал та управління наслідками реалізації загроз інформаційній безпеці в кризових ситуаціях, на основі здійснення процедур кількісної і якісної оцінки ризиків.

РН18. Аналізувати, застосовувати методи та засоби криптографічного захисту інформації на об'єктах інформаційної діяльності.

РН19. Вирішувати задачі щодо організації та контролю стану криптографічного захисту інформації, зокрема відповідно до вимог нормативних документів.

РН20. Визначати загрози створення технічних каналів витоку інформації на об'єктах інформаційної діяльності; впроваджувати засоби і заходи технічного захисту інформації від витоку технічними каналами, проводити обслуговування і контроль стану апаратних засобів захисту інформації та комплексів технічного захисту інформації.

РН21. Виконувати впровадження, підтримку, аналіз ефективності систем виявлення несанкціонованого доступу, дій з інформацією в інформаційній системі, вразливостей, можливих загроз інформаційному простору й інформаційним ресурсам та використовувати комплекси захисту для забезпечення необхідного рівня захищеності інформації в інформаційних системах.

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	*ОБОВ'ЯЗКОВІ ОСВІТНІ КОМПОНЕНТИ*	23	10
2	*ВИБІРКОВІ ОСВІТНІ КОМПОНЕНТИ*	25	10
ЦИКЛ ПРОФЕСІЙНОЇ ПІДГОТОВКИ			
3	*ОБОВ'ЯЗКОВІ ОСВІТНІ КОМПОНЕНТИ*	157	65
4	*ВИБІРКОВІ ОСВІТНІ КОМПОНЕНТИ*	35	15
	ЗАГАЛЬНА КІЛЬКІСТЬ:	***240***	***100%***
	в тому числі: вибіркова складова	60	25

Код ОК	Освітні компоненти (навчальні дисципліни, курсові проекти (роботи), практики, кваліфікаційна робота)	Кредити ЄКТС	Форми підсумкового контролю
ЦИКЛ ЗАГАЛЬНОЇ ПІДГОТОВКИ			
ОБОВ'ЯЗКОВІ ОСВІТНІ КОМПОНЕНТИ			
ОК 1	Українська мова (за професійним спрямуванням)	3	ЗАЛІК
ОК 2	Іноземна мова (за професійним спрямуванням)	9	ЗАЛІК, ЕКЗАМЕН

ОК 3	Історія української культури	4	ЗАЛІК
ОК 4	Філософія	5	ЕКЗАМЕН
ОК 5	Тренінг-курс «Безпека життєдіяльності та охорона праці»	2	ЗАЛІК
ВИБІРКОВІ ОСВІТНІ КОМПОНЕНТИ			
ВК 1	Навчальна дисципліна правового спрямування	5	ЗАЛІК
ВК 2	Майнор або вільний майнор	5	ЗАЛІК
ВК 3	Майнор або вільний майнор	5	ЗАЛІК
ВК 4	Майнор або вільний майнор	5	ЗАЛІК
ВК 5	Майнор або вільний майнор	5	ЗАЛІК
ЦИКЛ ПРОФЕСІЙНОЇ ПІДГОТОВКИ			
ОБОВ'ЯЗКОВІ ОСВІТНІ КОМПОНЕНТИ			
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 проєкт	3	КОНСУЛЬТА-ЦІЙНИЙ ПРОЄКТ
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 проєкт	9	ДИПЛОМНИЙ ПРОЄКТ
ОК 34	Єдиний державний кваліфікаційний іспит	1	ЄДКІ
ВИБІРКОВІ ОСВІТНІ КОМПОНЕНТИ			
ВК 6	Мейджор 1	5	ЕКЗАМЕН
ВК 7	Мейджор 2	5	ЕКЗАМЕН
ВК 8	Мейджор 3	5	ЕКЗАМЕН
ВК 9	Мейджор 4	5	ЕКЗАМЕН
ВК 10	Мейджор 5	5	ЕКЗАМЕН
ВК 11	Мейджор 6	5	ЕКЗАМЕН
ВК 12	Мейджор 7	5	ЕКЗАМЕН

4.2. ВИБІРКОВА СКЛАДОВА ОСВІТНЬО-ПРОФЕСІЙНОЇ ПРОГРАМИ

Вибіркова складова навчального плану першого (бакалаврського) рівня вищої освіти складається з: вибіркової навчальної дисципліни за спрямуванням, майнора або вільних майнорів, мейджорів.

Здобувач вищої освіти обирає 1 майнор або 4 вільні майнори з загальноуніверситетського пулу дисциплін. Майнор, як правило, складається з 4 навчальних дисциплін. Обсяг кожної дисципліни майнора (вільного майнора) – 5 кредитів ЄКТС.

Як виняток, майнор може складатися з 2 навчальних дисциплін. Тоді, обсяг кожної дисципліни майнора – 10 кредитів ЄКТС. Дисципліни майнора (вільного майнора) викладаються по одній дисципліні в 3, 4, 5, 6 семестрах для здобувачів вищої освіти очної (денної) форми навчання. Формою підсумкового контролю дисциплін майнора (вільного майнора) є залік.

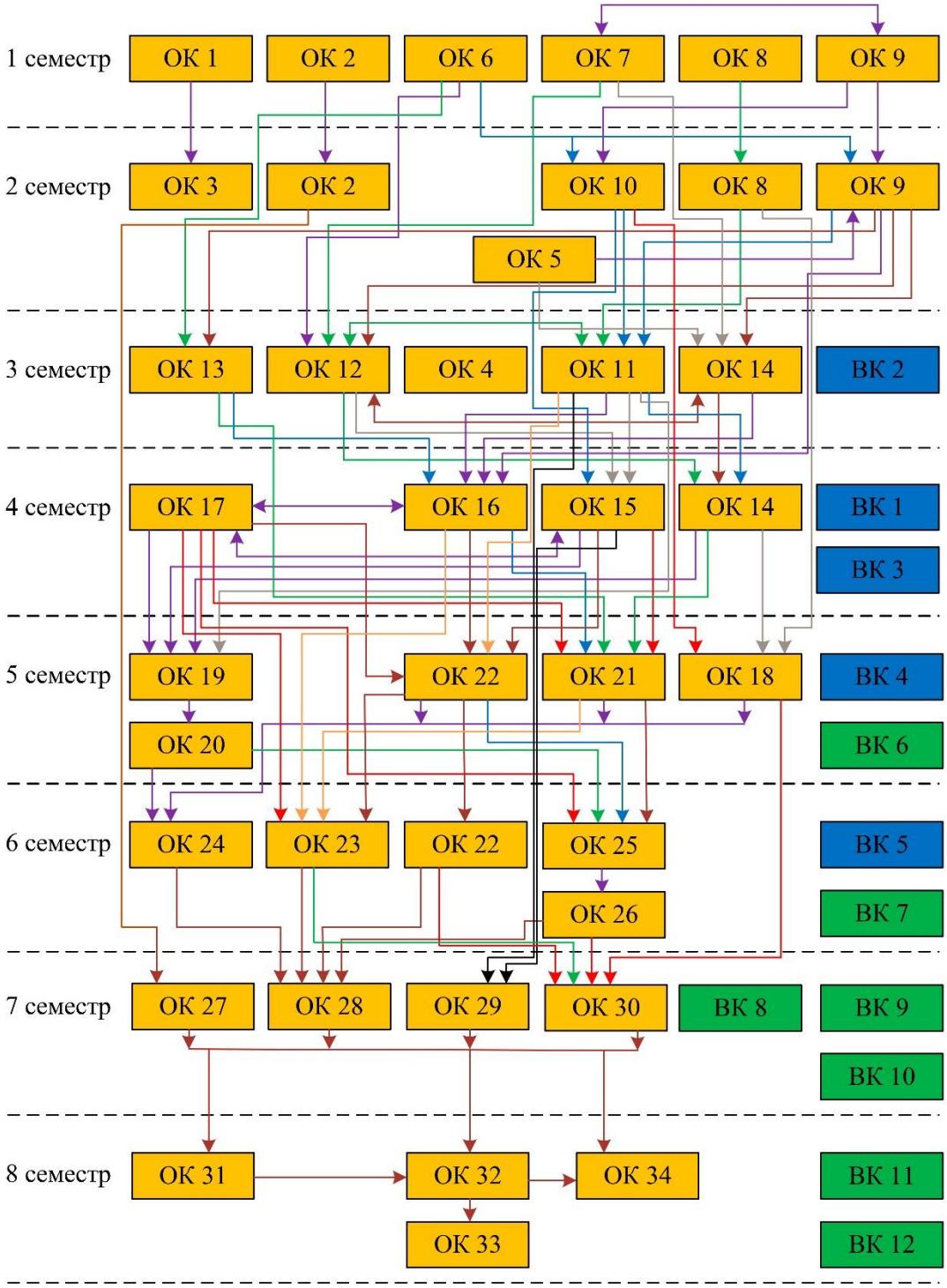
Здобувачеві вищої освіти пропонується обирати 1 дисципліну правового спрямування. Обсяг кожної вибіркової навчальної дисципліни за спрямуванням – 5 кредитів ЄКТС.

Формою підсумкового контролю за вибірковою навчальною дисципліною правового спрямування – залік.

Вибіркова навчальна дисципліна правового спрямування викладається в 3 або 4, або 5, або 6 семестрі для здобувачів вищої освіти очної (денної) форми навчання. Семестр, у якому викладається дисципліна, визначається навчальним планом освітньої програми.

Обсяг вибіркової навчальної дисципліни мейджора – 5 кредитів ЄКТС. Формою підсумкового контролю дисциплін мейджорів є екзамен (іспит). Дисципліни мейджори викладаються в 5, 6, 7, 8 семестрі для здобувачів вищої освіти очної (денної) форми навчання. Кількість дисциплін мейджорів, яка викладається в певному семестрі, визначається навчальним планом освітньої програми.

4.3. СТРУКТУРНО-ЛОГІЧНА СХЕМА ПІДГОТОВКИ ЗДОБУВАЧІВ ВИЩОЇ ОСВІТИ



ПРОЄКТ освітньо програми для обговорення на 2025-2026 навчальний рік

V. ФОРМИ АТЕСТАЦІЇ ЗДОБУВАЧІВ ВИЩОЇ ОСВІТИ

Форми атестації здобувачів вищої освіти	Атестація здійснюється у формі єдиного державного кваліфікаційного іспиту та дипломного проєкту.
Вимоги до єдиного державного кваліфікаційного іспиту	Єдиний державний кваліфікаційний іспит передбачає оцінювання досягнень результатів навчання, визначених стандартом та освітньою програмою.
Вимоги до кваліфікаційної роботи	Атестація за освітньою програмою здійснюється екзаменаційною комісією після виконання студентом навчального плану у формі публічного захисту кваліфікаційної роботи бакалавра (дипломного проєкту) за спеціальністю 125 Кібербезпека та захист інформації. 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 проєкт – це робота здобувача, яка виконується на завершальному етапі здобуття кваліфікації бакалавра з кібербезпеки та захисту інформації 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. У дипломному проекті не повинно бути академічного плагіату, фальсифікації та фабрикації. Дипломний проект має бути оприлюднений (за виключенням робіт, що містять інформацію з обмеженим доступом) на офіційному сайті закладу вищої освіти або його структурного підрозділу, або у репозитарії закладу вищої освіти.
Вимоги до публічного захисту	У процесі публічного захисту кандидат на присвоєння бакалаврського ступеня повинен показати уміння чітко і впевнено викладати зміст проведених досліджень, аргументовано відповідати на запитання та вести дискусію. Доповідь здобувача вищої освіти повинна супроводжуватися презентаційними матеріалами, призначеними для загального перегляду.

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	Основні принципи внутрішнього забезпечення якості освіти у ХНЕУ ім. С. Кузнеця: відповідальності; відповідності; адекватності; автономності; вимірюваності; академічної культури; відкритості. 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 напрямами 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. 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.
Забезпечення якості розроблення, затвердження, моніторингу, перегляду та оновлення освітніх програм	Моніторинг та періодичний перегляд освітніх програм здійснюється згідно з діючими нормативними актами в ХНЕУ ім. С. Кузнеця. 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 (soft skills); інших стейкхолдерів. 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. Періодичність перегляду освітніх програм здійснюється: а) 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	Оцінювання здобувачів вищої освіти є послідовним, прозорим та проводиться відповідно до встановлених в Університеті процедур згідно з нормативними актами. 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.
Забезпечення якості студентоцентрованого навчання, викладання та оцінювання	Планування, розподіл та надання навчальних ресурсів і забезпечення підтримки здобувачів вищої освіти враховують їх потреби та принципи студентоцентрованого навчання. Внутрішнє забезпечення якості вищої освіти гарантує, що всі необхідні ресурси відповідають цілям навчання, є загальнодоступними, а здобувачі вищої освіти поінформовані про їх наявність.
Забезпечення якості науково-педагогічних працівників	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.
Ресурсне забезпечення освітнього процесу (навчальні ресурси та підтримка здобувачів вищої освіти)	Заклад вищої освіти забезпечує освітній процес необхідними та доступними ресурсами (кадровими, методичними, матеріальними, інформаційними та ін.) та здійснює відповідну підтримку здобувачів вищої освіти. 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 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				
ЗК1. Здатність застосовувати знання у практичних ситуаціях.	+	+		
ЗК2. Знання та розуміння предметної області і розуміння професійної діяльності.	+	+	+	
ЗК3. Здатність спілкуватися державною мовою як усно, так і письмово.			+	
ЗК4. Здатність спілкуватися іноземною мовою.			+	+
ЗК5. Здатність вчитися і оволодівати сучасними знаннями.	+	+	+	+
ЗК6. Здатність реалізувати свої права і обов'язки як члена суспільства, усвідомлювати цінності громадянського (вільного демократичного) суспільства та необхідність його сталого розвитку, верховенства права, прав та свобод людини і громадянина в Україні.	+		+	+
ЗК7. Здатність ухвалювати рішення й діяти дотримуючись принципу неприпустимості корупції та будь-яких інших проявів недоброчесності.			+	+
ЗК8. 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				
СК1. Здатність застосовувати законодавчу та нормативно- правову базу, а також державні і міжнародні вимоги, практики і стандарти у професійній діяльності.	+	+	+	
СК2. Здатність використовувати інформаційні технології, сучасні методи і моделі кібербезпеки та системи захисту інформації.	+	+	+	
СК3. Здатність забезпечувати неперервність бізнес-процесів згідно встановленої політики кібербезпеки та захисту інформації.		+		+
СК4. Здатність забезпечувати захист Інформації в інформаційних та інформаційно-комунікаційних системах згідно встановленої політики кібербезпеки й захисту інформації.		+		+
СК5. Здатність відновлювати функціонування Інформаційних та інформаційно-		+	+	+

комунікаційних систем після реалізації загроз, здійснення кібератак, збоїв і відмов різних класів та походження.				
СК6. Здатність впроваджувати та забезпечувати функціонування комплексних систем захисту інформації (комплекси нормативно-правових, організаційних та технічних засобів і методів, процедур, практичних прийомів тощо).		+	+	+
СК7. Здатність здійснювати професійну діяльність на основі впровадженої системи управління інформаційною та кібербезпекою.		+	+	+
СК8. Здатність застосовувати методи та засоби криптографічного захисту інформації на об’єктах інформаційної діяльності.	+	+		
СК9. Здатність застосовувати методи та засоби технічного захисту Інформації на об’єктах інформаційної діяльності.	+	+		
СК10. Здатність виконувати моніторинг інформаційних процесів, аналізувати, виявляти, оцінювати можливі вразливості та загрози інформаційному простору й інформаційним ресурсам згідно з встановленою політикою інформаційної безпеки.		+	+	+

Таблиця 2

Матриця відповідності визначених результатів навчання, компетентностей та освітніх компонентів

Результати навчання	Компетентності																	
	Загальні								Спеціальні (фахові)									
	ЗК1	ЗК2	ЗК3	ЗК4	ЗК5	ЗК6	ЗК7	ЗК8	СК1	СК2	СК3	СК4	СК5	СК6	СК7	СК8	СК9	СК10
РН1. Вільно спілкуватися державною мовою усно та письмово при виконанні професійних обов'язків.	ОК1		ОК1 ОК3 ОК4		ОК1 ОК3 ОК4			ОК3 ОК5	ОК3 ОК5									
РН2. Спілкуватися іноземною мовою з метою забезпечення ефективності професійної комунікації.		ОК2 ОК27		ОК2 ОК27				ОК2 ОК27	ОК2 ОК27									
РН3. Застосовувати принцип неприпустимості корупції та будь-яких інших проявів недоброчесності у професійній діяльності.						ОК6 ОК17 ОК21 ОК23 ОК28	ОК6 ОК17 ОК21 ОК23 ОК28		ОК6 ОК17 ОК21 ОК23 ОК28									
РН4. Організовувати власну професійну діяльність, обирати і використовувати оптимальні методи та способи розв'язання складних спеціалізованих задач і практичних проблем у професійній діяльності, оцінювати їхню ефективність.	ОК5 ОК12 ОК13 ОК16 ОК19 ОК20 ОК25 ОК26	ОК5 ОК6 ОК12 ОК13 ОК25 ОК26			ОК25 ОК26				ОК5	ОК12 ОК13 ОК25 ОК26								
РН5. Аналізувати, аргументувати, приймати рішення при розв'язанні складних спеціалізованих задач і практичних завдань у професійній діяльності, які характеризуються комплексністю та неповною визначеністю умов, відповідати за прийняті рішення.					ОК7 ОК9 ОК30					ОК9 ОК30		ОК9		ОК7				ОК14 ОК30
РН6. Адаптуватися до нових умов і технологій професійної діяльності, прогнозувати кінцевий результат.		ОК22			ОК30					ОК22 ОК30		ОК21	ОК22	ОК21	ОК22		ОК22	
РН7. Застосовувати й адаптувати теорії інформації та кодування, математичної статистики, чисел, криптографії та стеганографії, оброблення і передачі сигналів тощо, принципи, методи, поняття кібербезпеки та захисту інформації у навчанні та професійній діяльності.					ОК8 ОК10					ОК16 ОК29	ОК16			ОК16 ОК29	ОК7	ОК8 ОК10 ОК11 ОК29		
РН8. Застосовувати знання й розуміння математики та фізики в професійній діяльності,					ОК8 ОК10					ОК18				ОК8 ОК10		ОК8 ОК10 ОК11		

Результати навчання	Компетентності																	
	Загальні								Спеціальні (фахові)									
	ЗК1	ЗК2	ЗК3	ЗК4	ЗК5	ЗК6	ЗК7	ЗК8	СК1	СК2	СК3	СК4	СК5	СК6	СК7	СК8	СК9	СК10
формалізувати задачі предметної галузі кібербезпеки та захисту інформації, формулювати їх математичну постановку та обирати раціональний метод вирішення.																		
РН9. Знати та застосовувати законодавство України та міжнародні вимоги, практики і стандарти з метою здійснення професійної діяльності в галузі кібербезпеки та захисту інформації.						ОК6 ОК17 ОК21 ОК23 ОК28	ОК6 ОК17 ОК21 ОК23 ОК28		ОК6 ОК17 ОК21 ОК23 ОК28	ОК6 ОК17 ОК21 ОК23 ОК28								
РН10. Використовувати сучасні інформаційні технології, методи і моделі кібербезпеки та систем захисту інформації для здійснення професійної діяльності.	ОК12 ОК13 ОК19 ОК20 ОК22 ОК25 ОК26 ОК30	ОК12 ОК13 ОК19 ОК20 ОК21 ОК22 ОК25 ОК26 ОК30								ОК6 ОК12 ОК13 ОК19 ОК20 ОК21 ОК22 ОК25 ОК26 ОК30		ОК15 ОК19 ОК20 ОК21 ОК22 ОК30	ОК22	ОК21 ОК30	ОК15 ОК19 ОК20 ОК22		ОК22	ОК13 ОК30
РН11. Планувати підготовку та забезпечувати неперервність бізнес-процесів в організаціях згідно зі встановленою політикою кібербезпеки з урахування вимог до захисту інформації.		ОК22 ОК30 ОК13								ОК17 ОК30	ОК6	ОК17 ОК21						
РН12. Застосовувати методи та засоби захисту інформації в інформаційних та інформаційно-комунікаційних системах відповідно до встановленої політики інформаційної безпеки.	ОК22 ОК30	ОК12 ОК19 ОК20 ОК22 ОК30								ОК12 ОК22 ОК30 ОК31		ОК31 ОК21 ОК22 ОК30 ОК12 ОК19 ОК20	ОК21 ОК22	ОК21	ОК22 ОК30		ОК22	
РН13. Впроваджувати, налаштовувати, супроводжувати та підтримувати функціонування програмних і програмно-апаратних комплексів і систем кібербезпеки та захисту інформації як необхідні процедури для функціонування інформаційних й Інформаційно-комунікаційних систем та\або інфраструктури організації в цілому.	ОК22 ОК30 ОК13	ОК22 ОК30 ОК13								ОК12 ОК13 ОК19 ОК20 ОК25 ОК26		ОК21 ОК22 ОК30 ОК12	ОК21	ОК21	ОК19 ОК20 ОК25 ОК26		ОК22	ОК12 ОК19 ОК20 ОК25 ОК26 ОК30
РН14. Вирішувати задачі управління процесами відновлення штатного функціонування інформаційних та інформаційно-комунікаційних систем з										ОК12		ОК17 ОК21	ОК21	ОК13 ОК17 ОК21				ОК17

Результати навчання	Компетентності																	
	Загальні								Спеціальні (фахові)									
	ЗК1	ЗК2	ЗК3	ЗК4	ЗК5	ЗК6	ЗК7	ЗК8	СК1	СК2	СК3	СК4	СК5	СК6	СК7	СК8	СК9	СК10
використанням процедур резервування згідно встановленої політики безпеки і забезпечувати функціонування спеціального програмного забезпечення щодо захисту та відновлення інформації.																		
РН15. Збирати, обробляти, зберігати, аналізувати критичні дані для доказу реалізації кіберзагроз, проводити аналіз та дослідження кіберінциденту з метою оперативного відновлення функціонування інформаційної системи.										ОК13		ОК17 ОК21	ОК21	ОК17 ОК21				ОК14 ОК17
РН16. Вирішувати задачі впровадження та супроводу комплексних систем захисту інформації в інформаційних системах.	ОК30	ОК30							ОК24 ОК32	ОК30	ОК30	ОК21 ОК24 ОК32	ОК21 ОК24 ОК32	ОК21 ОК24 ОК32			ОК22	ОК22 ОК30
РН17. Забезпечувати функціонування системи управління кібербезпекою і захистом інформації організації, включаючи персонал та управління наслідками реалізації загроз інформаційній безпеці в кризових ситуаціях, на основі здійснення процедур кількісної і якісної оцінки ризиків.		ОК13										ОК17 ОК21	ОК21	ОК17 ОК21				ОК17
РН18. Аналізувати, застосовувати методи та засоби криптографічного захисту інформації на об'єктах інформаційної діяльності.					ОК24 ОК32							ОК15 ОК24 ОК32				ОК15 ОК24 ОК32	ОК22 ОК24 ОК32	ОК22 ОК24 ОК32
РН19. Вирішувати задачі щодо організації та контролю стану криптографічного захисту інформації, зокрема відповідно до вимог нормативних документів.					ОК8 ОК10 ОК11 ОК12 ОК15							ОК8 ОК10 ОК11 ОК12 ОК15				ОК8 ОК10 ОК11 ОК12 ОК15		
РН20. Визначати загрози створення технічних каналів витоку інформації на об'єктах інформаційної діяльності; впроваджувати засоби і заходи технічного захисту інформації від витоку технічними каналами, проводити обслуговування і контроль стану апаратних засобів захисту інформації та комплексів технічного захисту інформації.		ОК13 ОК16 ОК17 ОК21 ОК23										ОК13 ОК16 ОК17 ОК21 ОК23	ОК13 ОК16 ОК17 ОК21 ОК23	ОК13 ОК16 ОК17 ОК21 ОК23				ОК13 ОК16 ОК17 ОК21 ОК23

Результати навчання	Компетентності																	
	Загальні								Спеціальні (фахові)									
	ЗК1	ЗК2	ЗК3	ЗК4	ЗК5	ЗК6	ЗК7	ЗК8	СК1	СК2	СК3	СК4	СК5	СК6	СК7	СК8	СК9	СК10
РН21. Виконувати впровадження, підтримку, аналіз ефективності систем виявлення несанкціонованого доступу, дій з інформацією в інформаційній системі, вразливостей, можливих загроз інформаційному простору й інформаційним ресурсам та використовувати комплекси захисту для забезпечення необхідного рівня захищеності інформації в інформаційних системах.										ОК12 ОК21 ОК25 ОК26				ОК21	ОК19 ОК20 ОК25 ОК26			ОК21

Гарант ОП *підписано* **Вячеслав ЛИМАРЕНКО**