ПРОЄКТ освітньої програми для обговорення
на 2025-2026 навчальний рік

ОСВІТНЬО-ПРОФЕСІЙНА ПРОГРАМА
«КІБЕРБЕЗПЕКА»

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

ПРОЄКТ освітньої програми для обговорення
на 2025-2026 навчальний рік

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 04.10.2018 р. № 1074.
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).

ПРОЄКТ освітньої програми для обговорення
на 2025-2026 навчальний рік

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’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

	об’єктів, що підлягають захисту. **Цілі навчання:** підготовка фахівців здатних використовувати і впроваджувати технології інформаційної та/або кібербезпеки. **Теоретичний зміст предметної області включає знання:** 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. **Методи, методики та технології:** Методи, методики, інформаційно-комунікаційні технології та інші технології забезпечення інформаційної та/ або кібербезпеки. **Інструментарій та обладнання:** системи розробки, забезпечення, моніторингу та контролю процесів інформаційної та/ або кібербезпеки; сучасне програмно-апаратне забезпечення інформаційно-комунікаційних технологій; спеціалізований клас (кіберполігон).
Академічна мобільність	-
Академічні права	Можливість продовжити навчання за освітньою програмою ступеня магістра.
Професійні права	-
Працевлаштування випускників	Професії, на підготовку з яких спрямована ОП (згідно з чинною редакцією Національного класифікатора України: Класифікатор професій ДК 003:2010) 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.
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 та практичні проблеми у галузі забезпечення інформаційної безпеки і\або кібербезпеки, що характеризується комплексністю та неповною визначеністю умов.

ПРОЄКТ освітньої програми для обговорення
на 2025-2026 навчальний рік

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. КЗ8. Здатність ухвалювати рішення та діяти, дотримуючись принципу неприпустимості корупції та будь-яких проявів недоброчесності.
Спеціальні (фахові, предметні) 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. 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

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 ЗА СПЕЦІАЛЬНІСТЮ «КІБЕРБЕЗПЕКА» ОПП «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 частої зміни технологій професійної діяльності, прогнозувати кінцевий результат;

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

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

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

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

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

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

РН 12 – розробляти моделі загроз та порушника;

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

РН 36 – виявляти небезпечні сигнали технічних засобів;

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

РН 38 – інтерпретувати результати проведення спеціальних вимірювань з використанням технічних засобів, контролю характеристик

інформаційно-телекомунікаційних систем відповідно до вимог нормативних документів системи технічного захисту інформації;

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

ПРОЄКТ освітньої програми для обговорення
на 2025-2026 навчальний рік

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	4	ЗАЛІК

	систем		
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.

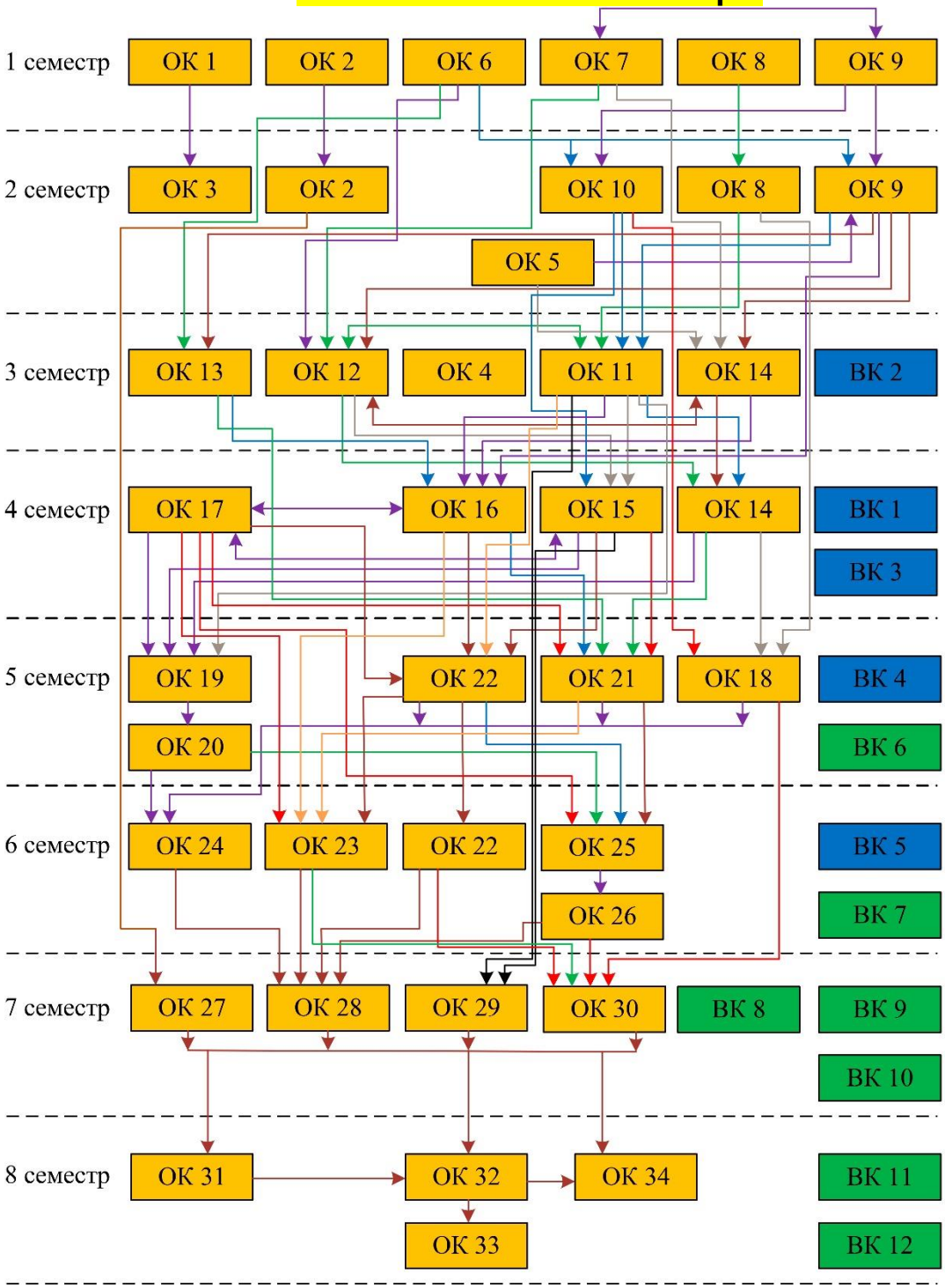
Формою підсумкового контролю за вибірковою навчальною дисципліною правового спрямування – залік.

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 освітньої програми для обговорення
на 2025-2026 навчальний рік



ПРОЄКТ освітньої 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.
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.

ПРОЄКТ освітньої програми для обговорення на 2025-2026 навчальний рік

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.		+	+	+
КЗ 8. Здатність ухвалювати рішення та діяти, дотримуючись принципу неприпустимості корупції та будь-яких проявів недоброчесності.	+	+	+	+
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.	+	+		+
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	+	+		+

Таблиця 2

Матриця відповідності визначених результатів навчання, компетентностей та освітніх компонентів

Результати навчання	Компетентності																		
	Загальні								Спеціальні (фахові)										
	КЗ 1	КЗ 2	КЗ 3	КЗ 4	КЗ 5	КЗ 6	КЗ 7	КЗ 8	КФ 1	КФ 2	КФ 3	КФ 4	КФ 5	КФ 6	КФ 7	КФ 8	КФ 9	КФ 10	КФ 11	КФ 12
РН1 – застосовувати знання державної та іноземних мов з метою забезпечення ефективності професійної комунікації	ОК1 ОК2 ОК27	ОК1 ОК2 ОК27	ОК1 ОК2 ОК27					ОК6 ОК32 ОК33 ОК34												
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	ОК4 ОК5 ОК6 ОК10 ОК11 ОК15 ОК21 ОК22 ОК24 ОК28 ОК31 ОК32 ОК33	ОК4 ОК5 ОК6 ОК10 ОК11 ОК15 ОК21 ОК22 ОК24 ОК28 ОК31 ОК32 ОК33		ОК4 ОК5 ОК6 ОК10 ОК11 ОК15 ОК21 ОК22 ОК24 ОК28 ОК31 ОК32 ОК33	ОК4 ОК5 ОК6 ОК10 ОК11 ОК15 ОК21 ОК22 ОК24 ОК28 ОК31 ОК32 ОК33			ОК6 ОК32 ОК33 ОК34											
РН 3 – використовувати результати самостійного пошуку, аналізу та синтезу інформації з різних джерел для ефективного рішення спеціалізованих задач професійної діяльності	ОК6 ОК13 ОК15 ОК17 ОК21 ОК22 ОК24 ОК28 ОК31 ОК32 ОК33	ОК6 ОК13 ОК15 ОК17 ОК21 ОК22 ОК24 ОК28 ОК31 ОК32 ОК33		ОК6 ОК13 ОК15 ОК17 ОК21 ОК22 ОК24 ОК28 ОК31 ОК32 ОК33	ОК6 ОК13 ОК15 ОК17 ОК21 ОК22 ОК24 ОК28 ОК31 ОК32 ОК33			ОК6 ОК32 ОК33 ОК34											
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	ОК6 ОК7 ОК10 ОК11 ОК15 ОК17 ОК19 ОК21 ОК22 ОК24 ОК28 ОК30 ОК31 ОК32 ОК33	ОК6 ОК7 ОК10 ОК11 ОК15 ОК17 ОК19 ОК21 ОК22 ОК24 ОК28 ОК30 ОК31 ОК32 ОК33		ОК6 ОК7 ОК10 ОК11 ОК15 ОК17 ОК19 ОК21 ОК22 ОК24 ОК28 ОК30 ОК31 ОК32 ОК33	ОК6 ОК7 ОК10 ОК11 ОК15 ОК17 ОК19 ОК21 ОК22 ОК24 ОК28 ОК30 ОК31 ОК32 ОК33														
РН 5 – адаптуватися в умовах частої зміни технологій професійної діяльності, прогнозувати кінцевий результат		ОК6 ОК9 ОК14 ОК17		ОК6 ОК9 ОК14 ОК17	ОК6 ОК9 ОК14 ОК17															

Результати навчання	Компетентності																			
	Загальні								Спеціальні (фахові)											
	КЗ 1	**КЗ 2**	**КЗ 3**	**КЗ 4**	**КЗ 5**	**КЗ 6**	**КЗ 7**	**КЗ 8**	**КФ 1**	**КФ 2**	**КФ 3**	**КФ 4**	**КФ 5**	**КФ 6**	**КФ 7**	**КФ 8**	**КФ 9**	**КФ 10**	**КФ 11**	**КФ 12**
		ОК18 ОК22 ОК24 ОК31 ОК32 ОК33		ОК18 ОК22 ОК24 ОК31 ОК32 ОК33	ОК18 ОК22 ОК24 ОК31 ОК32 ОК33															
РН 6 – критично осмислювати основні теорії, принципи, методи і поняття у навчанні та професійній діяльності		ОК4 ОК6 ОК17 ОК21 ОК22 ОК28 ОК29 ОК31 ОК32 ОК33						ОК6 ОК32 ОК33 ОК34												
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		ОК6 ОК17 ОК21 ОК24 ОК25 ОК31 ОК32 ОК33		ОК6 ОК17 ОК21 ОК24 ОК25 ОК31 ОК32 ОК33				ОК6 ОК32 ОК33 ОК34	ОК6 ОК17 ОК21 ОК24 ОК25 ОК31 ОК32 ОК33											
РН 8 – готувати пропозиції до нормативних актів щодо забезпечення інформаційної та /або кібербезпеки		ОК6 ОК17 ОК21 ОК24 ОК25 ОК31 ОК32 ОК33		ОК6 ОК17 ОК21 ОК24 ОК25 ОК31 ОК32 ОК33					ОК6 ОК17 ОК21 ОК24 ОК25 ОК31 ОК32 ОК33											
РН 9 – впроваджувати процеси, що базуються на національних та міжнародних стандартах, виявлення, ідентифікації, аналізу та реагування на інциденти інформаційної та/або кібербезпеки					ОК6 ОК12 ОК16 ОК17 ОК19 ОК20 ОК23 ОК25 ОК26 ОК30				ОК6 ОК12 ОК16 ОК17 ОК19 ОК20 ОК23 ОК25 ОК26 ОК30		ОК6 ОК12 ОК16 ОК17 ОК19 ОК20 ОК23 ОК25 ОК26 ОК30	ОК6 ОК12 ОК16 ОК17 ОК19 ОК20 ОК23 ОК25 ОК26 ОК30	ОК6 ОК12 ОК16 ОК17 ОК19 ОК20 ОК23 ОК25 ОК26 ОК30		ОК6 ОК12 ОК16 ОК17 ОК19 ОК20 ОК23 ОК25 ОК26 ОК30	ОК6 ОК12 ОК16 ОК17 ОК19 ОК20 ОК23 ОК25 ОК26 ОК30	ОК6 ОК12 ОК16 ОК17 ОК19 ОК20 ОК23 ОК25 ОК26 ОК30		ОК6 ОК12 ОК16 ОК17 ОК19 ОК20 ОК23 ОК25 ОК26 ОК30	ОК6 ОК12 ОК16 ОК17 ОК19 ОК20 ОК23 ОК25 ОК26 ОК30
РН 10 – виконувати аналіз та декомпозицію інформаційно-телекомунікаційних систем	ОК7 ОК10 ОК12 ОК15 ОК16 ОК21									ОК7 ОК10 ОК12 ОК15 ОК16 ОК21									ОК7 ОК10 ОК12 ОК15 ОК16 ОК21	
РН 11 – виконувати аналіз зв'язків між інформаційними процесами на віддалених обчислювальних	ОК12 ОК13 ОК16									ОК12 ОК13 ОК16									ОК12 ОК13 ОК16	

Результати навчання	Компетентності																		
	Загальні								Спеціальні (фахові)										
	КЗ 1	КЗ 2	КЗ 3	КЗ 4	КЗ 5	КЗ 6	КЗ 7	КЗ 8	КФ 1	КФ 2	КФ 3	КФ 4	КФ 5	КФ 6	КФ 7	КФ 8	КФ 9	КФ 10	КФ 11	КФ 12
системах	ОК19 ОК20 ОК25 ОК26 ОК30									ОК19 ОК20 ОК25 ОК26 ОК30									ОК19 ОК20 ОК25 ОК26 ОК30	
РН 12 – розробляти моделі загроз та порушника															ОК9 ОК10 ОК13 ОК14 ОК18 ОК21 ОК22					ОК9 ОК10 ОК13 ОК14 ОК18 ОК21 ОК22
РН 13 – аналізувати проекти інформаційно-телекомунікаційних систем базуючись на стандартизованих технологіях та протоколах передачі даних					ОК12 ОК16 ОК17 ОК21 ОК25 ОК26 ОК30					ОК12 ОК16 ОК17 ОК21 ОК25 ОК26 ОК30			ОК12 ОК16 ОК17 ОК21 ОК25 ОК26 ОК30			ОК12 ОК16 ОК17 ОК21 ОК25 ОК26 ОК30			ОК12 ОК16 ОК17 ОК21 ОК25 ОК26 ОК30	ОК12 ОК16 ОК17 ОК21 ОК25 ОК26 ОК30
РН 14 – вирішувати завдання захисту програм та інформації, що обробляється в інформаційно-телекомунікаційних системах програмно-апаратними засобами та давати оцінку результативності якості прийнятих рішень										ОК11 ОК15 ОК19 ОК20 ОК21 ОК25 ОК26 ОК29 ОК30 ОК31	ОК11 ОК15 ОК19 ОК20 ОК21 ОК25 ОК26 ОК29 ОК30 ОК31		ОК11 ОК15 ОК19 ОК20 ОК21 ОК25 ОК26 ОК29 ОК30 ОК31			ОК11 ОК15 ОК19 ОК20 ОК21 ОК25 ОК26 ОК29 ОК30 ОК31		ОК11 ОК15 ОК19 ОК20 ОК21 ОК25 ОК26 ОК29 ОК30 ОК31	ОК11 ОК15 ОК19 ОК20 ОК21 ОК25 ОК26 ОК29 ОК30 ОК31	
РН 15 – використовувати сучасне програмно-апаратне забезпечення інформаційно-комунікаційних технологій										ОК11 ОК15 ОК19 ОК20 ОК21 ОК25 ОК26 ОК29 ОК30 ОК31	ОК11 ОК15 ОК19 ОК20 ОК21 ОК25 ОК26 ОК29 ОК30 ОК31								ОК11 ОК15 ОК19 ОК20 ОК21 ОК25 ОК26 ОК29 ОК30 ОК31	
РН 16 – реалізовувати комплексні системи захисту інформації в автоматизованих системах (АС) організації (підприємства) відповідно до вимог нормативно-правових документів									ОК17 ОК21 ОК28 ОК29		ОК17 ОК21 ОК28 ОК29				ОК17 ОК21 ОК28 ОК29					ОК17 ОК21 ОК28 ОК29
РН 17 – забезпечувати процеси захисту та функціонування інформаційно-телекомунікаційних (автоматизованих) систем на основі практик, навичок та знань, щодо структурних (структурно-логічних)		ОК7 ОК12 ОК13 ОК16 ОК19 ОК21								ОК7 ОК12 ОК13 ОК16 ОК19 ОК21	ОК7 ОК12 ОК13 ОК16 ОК19 ОК21	ОК7 ОК12 ОК13 ОК16 ОК19 ОК21	ОК7 ОК12 ОК13 ОК16 ОК19 ОК21	ОК7 ОК12 ОК13 ОК16 ОК19 ОК21		ОК7 ОК12 ОК13 ОК16 ОК19 ОК21			ОК7 ОК12 ОК13 ОК16 ОК19 ОК21	

Результати навчання	Компетентності																		
	Загальні								Спеціальні (фахові)										
	КЗ 1	КЗ 2	КЗ 3	КЗ 4	КЗ 5	КЗ 6	КЗ 7	КЗ 8	КФ 1	КФ 2	КФ 3	КФ 4	КФ 5	КФ 6	КФ 7	КФ 8	КФ 9	КФ 10	КФ 11	КФ 12
схем, топології мережі, сучасних архітектур та моделей захисту електронних інформаційних ресурсів з відображенням взаємозв'язків та інформаційних потоків, процесів для внутрішніх і віддалених компонент		ОК23 ОК25 ОК29 ОК30								ОК23 ОК25 ОК29 ОК30	ОК23 ОК25 ОК29 ОК30	ОК23 ОК25 ОК29 ОК30	ОК23 ОК25 ОК29 ОК30	ОК23 ОК25 ОК29 ОК30		ОК23 ОК25 ОК29 ОК30			ОК23 ОК25 ОК29 ОК30	
РН 18 – використовувати програмні та програмно-апаратні комплекси захисту інформаційних ресурсів	ОК14 ОК15 ОК16 ОК19 ОК20 ОК21 ОК22 ОК23 ОК25 ОК26 ОК29 ОК30									ОК14 ОК15 ОК16 ОК19 ОК20 ОК21 ОК22 ОК23 ОК25 ОК26 ОК29 ОК30	ОК14 ОК15 ОК16 ОК19 ОК20 ОК21 ОК22 ОК23 ОК25 ОК26 ОК29 ОК30		ОК14 ОК15 ОК16 ОК19 ОК20 ОК21 ОК22 ОК23 ОК25 ОК26 ОК29 ОК30						ОК14 ОК15 ОК16 ОК19 ОК20 ОК21 ОК22 ОК23 ОК25 ОК26 ОК29 ОК30	
РН 19 – застосовувати теорії та методи захисту для забезпечення безпеки інформації в інформаційно-телекомунікаційних системах	ОК11 ОК15 ОК16 ОК17 ОК19 ОК21 ОК23 ОК25 ОК29									ОК11 ОК15 ОК16 ОК17 ОК19 ОК21 ОК23 ОК25 ОК29			ОК11 ОК15 ОК16 ОК17 ОК19 ОК21 ОК23 ОК25 ОК29			ОК11 ОК15 ОК16 ОК17 ОК19 ОК21 ОК23 ОК25 ОК29			ОК11 ОК15 ОК16 ОК17 ОК19 ОК21 ОК23 ОК25 ОК29	
РН 20 – забезпечувати функціонування спеціального програмного забезпечення, щодо захисту інформації від руйнуючих програмних впливів, руйнуючих кодів в інформаційно-телекомунікаційних системах	ОК12 ОК14 ОК16 ОК19 ОК21 ОК25 ОК29 ОК30									ОК12 ОК14 ОК16 ОК19 ОК21 ОК25 ОК29 ОК30	ОК12 ОК14 ОК16 ОК19 ОК21 ОК25 ОК29 ОК30		ОК12 ОК14 ОК16 ОК19 ОК21 ОК25 ОК29 ОК30	ОК12 ОК14 ОК16 ОК19 ОК21 ОК25 ОК29 ОК30				ОК12 ОК14 ОК16 ОК19 ОК21 ОК25 ОК29 ОК30		
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	ОК17 ОК21 ОК28												ОК17 ОК21 ОК28				ОК17 ОК21 ОК28		ОК17 ОК21 ОК28	
РН 22 – вирішувати задачі управління процедурами ідентифікації, автентифікації, авторизації процесів і користувачів в інформаційно-телекомунікаційних системах	ОК12 ОК16 ОК19 ОК20 ОК21 ОК25												ОК12 ОК16 ОК19 ОК20 ОК21 ОК25						ОК12 ОК16 ОК19 ОК20 ОК21 ОК25	

Результати навчання	Компетентності																			
	Загальні								Спеціальні (фахові)											
	КЗ 1	КЗ 2	КЗ 3	КЗ 4	КЗ 5	КЗ 6	КЗ 7	КЗ 8	КФ 1	КФ 2	КФ 3	КФ 4	КФ 5	КФ 6	КФ 7	КФ 8	КФ 9	КФ 10	КФ 11	КФ 12
згідно встановленої політики інформаційної і\або кібербезпеки	ОК26 ОК29 ОК30												ОК26 ОК29 ОК30						ОК26 ОК29 ОК30	
РН 23 – реалізовувати заходи з протидії отриманню несанкціонованого доступу до інформаційних ресурсів і процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах													ОК15 ОК19 ОК20 ОК21 ОК22 ОК23 ОК25 ОК26 ОК30	ОК15 ОК19 ОК20 ОК21 ОК22 ОК23 ОК25 ОК26 ОК30		ОК15 ОК19 ОК20 ОК21 ОК22 ОК23 ОК25 ОК26 ОК30			ОК15 ОК19 ОК20 ОК21 ОК22 ОК23 ОК25 ОК26 ОК30	
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)	ОК15 ОК19 ОК21 ОК25 ОК29 ОК30											ОК15 ОК19 ОК21 ОК25 ОК29 ОК30	ОК15 ОК19 ОК21 ОК25 ОК29 ОК30				ОК15 ОК19 ОК21 ОК25 ОК29 ОК30		ОК15 ОК19 ОК21 ОК25 ОК29 ОК30	
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													ОК17 ОК19 ОК20 ОК21 ОК25 ОК26 ОК29 ОК30			ОК17 ОК19 ОК20 ОК21 ОК25 ОК26 ОК29 ОК30	ОК17 ОК19 ОК20 ОК21 ОК25 ОК26 ОК29 ОК30		ОК17 ОК19 ОК20 ОК21 ОК25 ОК26 ОК29 ОК30	
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													ОК12 ОК16 ОК19 ОК25 ОК30						ОК12 ОК16 ОК19 ОК25 ОК30	
РН 27 – вирішувати задачі захисту потоків даних в інформаційних, інформаційно-телекомунікаційних (автоматизованих) системах	ОК12 ОК16 ОК19 ОК21 ОК25 ОК29 ОК30											ОК12 ОК16 ОК19 ОК21 ОК25 ОК29 ОК30	ОК12 ОК16 ОК19 ОК21 ОК25 ОК29 ОК30	ОК12 ОК16 ОК19 ОК21 ОК25 ОК29 ОК30						
РН 28 – аналізувати та проводити оцінку ефективності та рівня захищеності ресурсів різних класів в інформаційних та інформаційно-					ОК19 ОК23 ОК25 ОК30								ОК19 ОК23 ОК25 ОК30				ОК19 ОК23 ОК25 ОК30			ОК19 ОК23 ОК25 ОК30

Результати навчання	Компетентності																			
	Загальні								Спеціальні (фахові)											
	КЗ 1	КЗ 2	КЗ 3	КЗ 4	КЗ 5	КЗ 6	КЗ 7	КЗ 8	КФ 1	КФ 2	КФ 3	КФ 4	КФ 5	КФ 6	КФ 7	КФ 8	КФ 9	КФ 10	КФ 11	КФ 12
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											ОК19 ОК21 ОК22 ОК25 ОК28 ОК30 ОК32	ОК19 ОК21 ОК22 ОК25 ОК28 ОК30 ОК32	ОК19 ОК21 ОК22 ОК25 ОК28 ОК30 ОК32			ОК19 ОК21 ОК22 ОК25 ОК28 ОК30 ОК32	ОК19 ОК21 ОК22 ОК25 ОК28 ОК30 ОК32			ОК19 ОК21 ОК22 ОК25 ОК28 ОК30 ОК32
РН 30 – здійснювати оцінювання можливості несанкціонованого доступу до елементів інформаційно-телекомунікаційних систем																				ОК13 ОК18 ОК22
РН 31 – застосовувати теорії та методи захисту для забезпечення безпеки елементів інформаційно-телекомунікаційних систем										ОК11 ОК13 ОК14 ОК15 ОК16 ОК21 ОК22 ОК23 ОК31 ОК32				ОК11 ОК13 ОК14 ОК15 ОК16 ОК21 ОК22 ОК23 ОК31 ОК32				ОК11 ОК13 ОК14 ОК15 ОК16 ОК21 ОК22 ОК23 ОК31 ОК32		
РН 32 – вирішувати задачі управління процесами відновлення штатного функціонування інформаційно-телекомунікаційних систем з використанням процедур резервування згідно встановленої політики безпеки	ОК11 ОК15 ОК19 ОК20 ОК25 ОК26 ОК29 ОК30											ОК11 ОК15 ОК19 ОК20 ОК25 ОК26 ОК29 ОК30	ОК11 ОК15 ОК19 ОК20 ОК25 ОК26 ОК29 ОК30			ОК11 ОК15 ОК19 ОК20 ОК25 ОК26 ОК29 ОК30			ОК11 ОК15 ОК19 ОК20 ОК25 ОК26 ОК29 ОК30	
РН 33 – вирішувати задачі забезпечення безперервності бізнес процесів організації на основі теорії ризиків								ОК6 ОК32 ОК33 ОК34	ОК8 ОК17 ОК18			ОК8 ОК17 ОК18				ОК8 ОК17 ОК18	ОК8 ОК17 ОК18			ОК8 ОК17 ОК18
РН 34 – приймати участь у розробці та впровадженні стратегії інформаційної безпеки та/або кібербезпеки відповідно до цілей і завдань організації									ОК6 ОК17 ОК21 ОК28 ОК31 ОК32 ОК33			ОК6 ОК17 ОК21 ОК28 ОК31 ОК32 ОК33	ОК6 ОК17 ОК21 ОК28 ОК31 ОК32 ОК33			ОК6 ОК17 ОК21 ОК28 ОК31 ОК32 ОК33	ОК6 ОК17 ОК21 ОК28 ОК31 ОК32 ОК33			ОК6 ОК17 ОК21 ОК28 ОК31 ОК32 ОК33
РН 35 – вирішувати задачі забезпечення та супроводу комплексних систем захисту	ОК19 ОК20 ОК21								ОК19 ОК20 ОК21		ОК19 ОК20 ОК21	ОК19 ОК20 ОК21	ОК19 ОК20 ОК21		ОК19 ОК20 ОК21	ОК19 ОК20 ОК21	ОК19 ОК20 ОК21			ОК19 ОК20 ОК21

Результати навчання	Компетентності																			
	Загальні								Спеціальні (фахові)											
	КЗ 1	КЗ 2	КЗ 3	КЗ 4	КЗ 5	КЗ 6	КЗ 7	КЗ 8	КФ 1	КФ 2	КФ 3	КФ 4	КФ 5	КФ 6	КФ 7	КФ 8	КФ 9	КФ 10	КФ 11	КФ 12
інформації, а також протидії несанкціонованому доступу до інформаційних ресурсів і процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах згідно встановленої політики інформаційної і/або кібербезпеки	ОК22 ОК25 ОК26 ОК30 ОК31								ОК22 ОК25 ОК26 ОК30 ОК31		ОК22 ОК25 ОК26 ОК30 ОК31	ОК22 ОК25 ОК26 ОК30 ОК31	ОК22 ОК25 ОК26 ОК30 ОК31		ОК22 ОК25 ОК26 ОК30 ОК31	ОК22 ОК25 ОК26 ОК30 ОК31	ОК22 ОК25 ОК26 ОК30 ОК31			ОК22 ОК25 ОК26 ОК30 ОК31
РН 36 – виявляти небезпечні сигнали технічних засобів																		ОК21 ОК23		
РН 37 – вимірювати параметри небезпечних та завадових сигналів під час інструментального контролю процесів захисту інформації та визначати ефективність захисту інформації від витоку технічними каналами відповідно до вимог нормативних документів системи технічного захисту інформації														ОК12 ОК16 ОК21 ОК29				ОК12 ОК16 ОК21 ОК29		
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								ОК6						ОК12 ОК16 ОК21 ОК29				ОК12 ОК16 ОК21 ОК29		
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																		ОК6 ОК17		
РН 40 – інтерпретувати результати проведення спеціальних вимірювань з використанням технічних засобів, контролю характеристик ІТС відповідно до вимог нормативних документів системи технічного захисту інформації																		ОК12 ОК15 ОК16 ОК23		
РН 41 – забезпечувати неперервність процесу ведення журналів реєстрації подій та інцидентів на основі автоматизованих процедур																ОК17 ОК19 ОК21 ОК25 ОК29			ОК17 ОК19 ОК21 ОК25 ОК29	
РН 42 – впроваджувати процеси виявлення, ідентифікації, аналізу та								ОК6 ОК32				ОК6 ОК10	ОК6 ОК10			ОК6 ОК10	ОК6 ОК10		ОК6 ОК10	ОК6 ОК10

Результати навчання	Компетентності																			
	Загальні								Спеціальні (фахові)											
	КЗ 1	КЗ 2	КЗ 3	КЗ 4	КЗ 5	КЗ 6	КЗ 7	КЗ 8	КФ 1	КФ 2	КФ 3	КФ 4	КФ 5	КФ 6	КФ 7	КФ 8	КФ 9	КФ 10	КФ 11	КФ 12
реагування на інциденти інформаційної і/або кібербезпеки								ОК33 ОК34				ОК17 ОК21 ОК31 ОК32 ОК33	ОК17 ОК21 ОК31 ОК32 ОК33			ОК17 ОК21 ОК31 ОК32 ОК33	ОК17 ОК21 ОК31 ОК32 ОК33		ОК17 ОК21 ОК31 ОК32 ОК33	ОК17 ОК21 ОК31 ОК32 ОК33
РН 43 – застосовувати національні та міжнародні регулюючі акти в сфері інформаційної безпеки та/ або кібербезпеки для розслідування інцидентів		ОК6 ОК17 ОК21 ОК23 ОК30 ОК32 ОК33							ОК6 ОК17 ОК21 ОК23 ОК30 ОК32 ОК33			ОК6 ОК17 ОК21 ОК23 ОК30 ОК32 ОК33	ОК6 ОК17 ОК21 ОК23 ОК30 ОК32 ОК33			ОК6 ОК17 ОК21 ОК23 ОК30 ОК32 ОК33	ОК6 ОК17 ОК21 ОК23 ОК30 ОК32 ОК33		ОК6 ОК17 ОК21 ОК23 ОК30 ОК32 ОК33	ОК6 ОК17 ОК21 ОК23 ОК30 ОК32 ОК33
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									ОК8 ОК17 ОК18 ОК21 ОК23 ОК30			ОК8 ОК17 ОК18 ОК21 ОК23 ОК30	ОК8 ОК17 ОК18 ОК21 ОК23 ОК30			ОК8 ОК17 ОК18 ОК21 ОК23 ОК30	ОК8 ОК17 ОК18 ОК21 ОК23 ОК30			ОК8 ОК17 ОК18 ОК21 ОК23 ОК30
РН 45 – застосовувати різні класи політик інформаційної безпеки та/ або кібербезпеки, що базуються на ризик-орієнтованому контролі доступу до інформаційних активів												ОК12 ОК16 ОК19 ОК21 ОК22 ОК23 ОК25 ОК29 ОК30 ОК32	ОК12 ОК16 ОК19 ОК21 ОК22 ОК23 ОК25 ОК29 ОК30 ОК32			ОК12 ОК16 ОК19 ОК21 ОК22 ОК23 ОК25 ОК29 ОК30 ОК32	ОК12 ОК16 ОК19 ОК21 ОК22 ОК23 ОК25 ОК29 ОК30 ОК32			ОК12 ОК16 ОК19 ОК21 ОК22 ОК23 ОК25 ОК29 ОК30 ОК32
РН 46 – здійснювати аналіз та мінімізацію ризиків обробки інформації в інформаційно-телекомунікаційних системах												ОК17 ОК18 ОК21 ОК22	ОК17 ОК18 ОК21 ОК22			ОК17 ОК18 ОК21 ОК22	ОК17 ОК18 ОК21 ОК22			ОК17 ОК18 ОК21 ОК22
РН 47 – вирішувати задачі захисту інформації, що обробляється в інформаційно-телекомунікаційних системах з використанням сучасних методів та засобів криптографічного захисту інформації										ОК11 ОК15 ОК16 ОК21 ОК25 ОК29	ОК11 ОК15 ОК16 ОК21 ОК25 ОК29		ОК11 ОК15 ОК16 ОК21 ОК25 ОК29					ОК11 ОК15 ОК16 ОК21 ОК25 ОК29		
РН 48 – виконувати впровадження та підтримку систем виявлення вторгнень та використовувати компоненти криптографічного захисту для забезпечення необхідного рівня захищеності інформації в інформаційно-телекомунікаційних системах													ОК11 ОК15 ОК16 ОК21 ОК25 ОК29	ОК11 ОК15 ОК16 ОК21 ОК25 ОК29		ОК11 ОК15 ОК16 ОК21 ОК25 ОК29		ОК11 ОК15 ОК16 ОК21 ОК25 ОК29	ОК11 ОК15 ОК16 ОК21 ОК25 ОК29	
РН 49 – забезпечувати належне функціонування системи													ОК12 ОК16	ОК12 ОК16		ОК12 ОК16			ОК12 ОК16	

Результати навчання	Компетентності																			
	Загальні								Спеціальні (фахові)											
	КЗ 1	КЗ 2	КЗ 3	КЗ 4	КЗ 5	КЗ 6	КЗ 7	КЗ 8	КФ 1	КФ 2	КФ 3	КФ 4	КФ 5	КФ 6	КФ 7	КФ 8	КФ 9	КФ 10	КФ 11	КФ 12
моніторингу інформаційних ресурсів і процесів в інформаційно-телекомунікаційних системах													ОК19 ОК20 ОК21 ОК22 ОК23 ОК25 ОК26 ОК29 ОК30	ОК19 ОК20 ОК21 ОК22 ОК23 ОК25 ОК26 ОК29 ОК30		ОК19 ОК20 ОК21 ОК22 ОК23 ОК25 ОК26 ОК29 ОК30			ОК19 ОК20 ОК21 ОК22 ОК23 ОК25 ОК26 ОК29 ОК30	
РН 50 – забезпечувати) функціонування програмних та програмно-апаратних комплексів виявлення вторгнень різних рівнів та класів (статистичних, сигнатурних, статистично-сигнатурних)											ОК12 ОК16 ОК19 ОК25 ОК29 ОК30		ОК12 ОК16 ОК19 ОК25 ОК29 ОК30			ОК12 ОК16 ОК19 ОК25 ОК29 ОК30			ОК12 ОК16 ОК19 ОК25 ОК29 ОК30	
РН 51 – підтримувати працездатність та забезпечувати конфігурування систем виявлення вторгнень в інформаційно-телекомунікаційних системах													ОК12 ОК16 ОК19 ОК25 ОК29 ОК30			ОК12 ОК16 ОК19 ОК25 ОК29 ОК30			ОК12 ОК16 ОК19 ОК25 ОК29 ОК30	
РН 52 – використовувати інструментарій для моніторингу процесів в інформаційно-телекомунікаційних системах													ОК12 ОК16 ОК19 ОК25 ОК29 ОК30	ОК12 ОК16 ОК19 ОК25 ОК29 ОК30		ОК12 ОК16 ОК19 ОК25 ОК29 ОК30			ОК12 ОК16 ОК19 ОК25 ОК29 ОК30	
РН 53 – вирішувати задачі аналізу програмного коду на наявність можливих загроз	ОК9 ОК14 ОК19 ОК20 ОК25 ОК26 ОК29			ОК9 ОК14 ОК19 ОК20 ОК25 ОК26 ОК29						ОК9 ОК14 ОК19 ОК20 ОК25 ОК26 ОК29	ОК9 ОК14 ОК19 ОК20 ОК25 ОК26 ОК29	ОК9 ОК14 ОК19 ОК20 ОК25 ОК26 ОК29	ОК9 ОК14 ОК19 ОК20 ОК25 ОК26 ОК29	ОК9 ОК14 ОК19 ОК20 ОК25 ОК26 ОК29		ОК9 ОК14 ОК19 ОК20 ОК25 ОК26 ОК29			ОК9 ОК14 ОК19 ОК20 ОК25 ОК26 ОК29	ОК9 ОК14 ОК19 ОК20 ОК25 ОК26 ОК29
РН 54 – усвідомлювати цінності громадянського (вільного демократичного) суспільства та необхідність його сталого розвитку, верховенства права, прав і свобод людини і громадянина в Україні	ОК3 ОК4 ОК5	ОК3 ОК4 ОК5				ОК3 ОК4 ОК5	ОК3 ОК4 ОК5													

Гарант ОП *підписано* **Вячеслав ЛИМАРЕНКО**