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

УХВАЛЕНО
Рішенням вченої ради
Харківського національного
економічного університету імені
Семена Кузнеця
від 25.05.2022 р. протокол № 4

ВВЕДЕНО В ДІЮ
Наказом ректора Харківського
національного економічного університету
імені Семена Кузнеця
від 25.05.2022 р. № 123

Володимир ПОНОМАРЕНКО

ОСВІТНЬО-ПРОФЕСІЙНА ПРОГРАМА
«КІБЕРБЕЗПЕКА»

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

Харків, 2022

ПРЕАМБУЛА

Робоча група освітньої програми:

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

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

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

Пожидаєв Максим Геннадійович, здобувач вищої освіти.

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

Розглянуто на засіданні кафедри кібербезпеки та інформаційних технологій, протокол № 15, від 16.05.2022 р.

Розглянуто вченою радою факультету інформаційних технологій, протокол № 6, від 17 травня 2022 р.

ОП оновлено на підставі:

1. Законодавчих та нормативних актів: Законів України “Про освіту”, “Про вищу освіту”, Національної рамки кваліфікації, Національного класифікатору України.
2. Стандарту вищої освіти України: перший (бакалаврський) рівень, галузь знань 12 – Інформаційні технології, спеціальність 125 – Кібербезпека, затвердженого Наказом Міністерства освіти та науки України № 1074 від 04.10.2018 р.).
3. Аналізу ринку праці, з урахуванням регіонального контексту.
4. Вивчення вітчизняного та зарубіжного досвіду.
5. Пропозицій роботодавців.
6. Рекомендації після процедур акредитація Національного агентства із забезпечення якості вищої освіти рішення від 27.04.2021, протокол № 7.

Рецензії-відгуки зовнішніх стейкхолдерів (додаються).

І. ЗАГАЛЬНА ХАРАКТЕРИСТИКА

Рівень вищої освіти	Перший (бакалаврський) рівень
Ступінь вищої освіти	Бакалавр
Галузі знань	12 Інформаційні технології
Спеціальності	125 Кібербезпека
Освітня програма (укр. та англ. мовою)	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 від 29.04.2021 строк дії сертифіката про акредитацію освітньої програми до 01.07.2026
Мова(и) навчання / оцінювання	українська / англійська
Структурний підрозділ відповідальний за ОП	Кафедра кібербезпеки та інформаційних технологій; Навчальна лабораторія кафедри кібербезпеки та інформаційних технологій
Вимоги до зарахування	Набір на перший (бакалаврський) рівень вищої освіти здійснюється за результатами складання національного мультипредметного тесту та мотиваційного листа. Для успішного засвоєння освітньої програми бакалавра абітурієнти повинні мати повну загальну середню освіту та прагнення оволодіти знаннями у галузі інформаційних технологій зі спеціальності кібербезпека. Правила та строки прийому розміщені на сайті ХНЕУ ім. С. Кузнеця за посиланням https://www.hneu.edu.ua/normatyvni-dokumenty/
Обмеження щодо форм навчання	Немає
Освітня кваліфікація	Бакалавр з кібербезпеки
Кваліфікація(-ї) професійна(-і)	Відсутня
Кваліфікація в дипломі	Ступінь вищої освіти − Бакалавр Спеціальність – 125 Кібербезпека 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	**Знання і розуміння:** – ґрунтовна математична підготовка в галузі захисту інформації, криптології та криптографії, теорії, моделей та принципів управління доступом до інформаційних ресурсів; – базові знання принципів супроводу систем та комплексів інформаційної та/або кібербезпеки та систем управління інформаційною та/або кібербезпекою; – методів та засобів виявлення, управління та ідентифікації ризиків, а також технічного та криптографічного захисту інформації;

	– знання мов та парадигм програмування, технологій програмування, WEB- технологій, операційних систем; – знання методів та засобів оцінювання та забезпечення необхідного рівня захищеності інформації. **Застосування знань і розумінь:** – здатність використання інформаційних і комунікаційних технологій з метою пошуку нової інформації, створення баз даних, аналізу розподілених АС та їх оптимізації; – здатність здійснювати проектування (розробку) систем, технологій і засобів інформаційної безпеки; – здатність здійснювати протидію несанкціонованому проникненню в ІТ системи і мережі; – здатність прогнозувати, виявляти та оцінювати стан інформаційної безпеки об'єктів і систем; – здатність відновлювати нормальне функціонування ІТ систем і мереж після здійснення кібернападів, збоїв та відмов; – здатність виконувати спеціальні дослідження технічних і програмно-апаратних засобів захисту обробки інформації в ІТС; – здатність формувати комплекс заходів (правил, процедур, практичних прийомів та ін.) для управління інформаційною безпекою. **Формування суджень:** – вміння виявляти, ставити та вирішувати проблеми за професійним спрямуванням; – здатність виконувати моніторинг даних, комп'ютерних зловживань та аномалій; – здатність до пошуку, оброблення та аналізу інформації; – здатність до роботи в команді; – здатність використовувати законодавчу та нормативно-правову бази, а також вимоги відповідних, в тому числі і міжнародних, стандартів та практик щодо здійснення професійної діяльності.
Працевлаштування випускників	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.

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.
Загальні компетентності	КЗ 1. Здатність застосовувати знання у практичних ситуаціях. КЗ 2. Знання та розуміння предметної області та розуміння професії.

	КЗ 3. Здатність професійно спілкуватися державною та іноземною мовами як усно, так і письмово. КЗ 4. Вміння виявляти, ставити та вирішувати проблеми за професійним спрямуванням. КЗ 5. Здатність до пошуку, оброблення та аналізу інформації. КЗ 6. Здатність реалізувати свої права і обов'язки як члена суспільства, усвідомлювати цінності громадянського (вільного демократичного) суспільства та необхідність його сталого розвитку, верховенства права, прав і свобод людини і громадянина в Україні. КЗ 7. Здатність зберігати та примножувати моральні, культурні, наукові цінності і досягнення суспільства на основі розуміння історії та закономірностей розвитку предметної області, її місця у загальній системі знань про природу і суспільство та у розвитку суспільства, техніки і технологій, використовувати різні види та форми рухової активності для активного відпочинку та ведення здорового способу життя.
Спеціальні (фахові, 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

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 ріні класи політик інформаційної безпеки та/ або кібербезпеки, що базуються на ризик-орієнтованому контролі доступу до інформаційних активів;

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

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

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

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

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

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

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

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

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

IV. СТРУКТУРА ОСВІТНЬОЇ ПРОГРАМИ ПІДГОТОВКИ БАКАЛАВРІВ

4.1. СТРУКТУРА ПРОГРАМИ ТА ОСВІТНІ КОМПОНЕНТИ

№	Освітні компоненти (навчальні дисципліни, курсові проекти (роботи), практики, кваліфікаційна робота)	Кредити ЄКТС	Структура, %
ЦИКЛ ЗАГАЛЬНОЇ ПІДГОТОВКИ			
1	*ОБОВ'ЯЗКОВІ ОСВІТНІ КОМПОНЕНТИ*	24	10
2	*ВИБІРКОВІ ОСВІТНІ КОМПОНЕНТИ*	25	10
ЦИКЛ ПРОФЕСІЙНОЇ ПІДГОТОВКИ			
3	*ОБОВ'ЯЗКОВІ ОСВІТНІ КОМПОНЕНТИ*	156	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			
ОК1	Українська мова (за професійним спрямуванням)	3	ЗАЛІК
ОК2	Іноземна мова (за професійним спрямуванням)	9	ЗАЛІК, ЕКЗАМЕН
ОК3	Соціальна та економічна історія України	4	ЗАЛІК
ОК4	Безпека життєдіяльності та охорона праці	3	ЗАЛІК
ОК5	Філософія	5	ЕКЗАМЕН
ВИБІРКОВІ ОСВІТНІ КОМПОНЕНТИ			
ВК1	Навчальна дисципліна правового спрямування	5	ЗАЛІК
ВК2	Майнор або вільний майнор	5	ЗАЛІК
ВК3	Майнор або вільний майнор	5	ЗАЛІК
ВК4	Майнор або вільний майнор	5	ЗАЛІК
ВК5	Майнор або вільний майнор	5	ЗАЛІК
ЦИКЛ ПРОФЕСІЙНОЇ ПІДГОТОВКИ			
ОБОВ'ЯЗКОВІ ОСВІТНІ КОМПОНЕНТИ			
ОК6	Вступ до фаху	6	ЗАЛІК
ОК7	Інформаційна безпека держави	5	ЕКЗАМЕН
ОК8	Основи програмування	6	ЕКЗАМЕН

ОК9	Вища математика	15	ЗАЛІК, ЕКЗАМЕН
ОК10	Розробка та аналіз алгоритмів	5	ЕКЗАМЕН
ОК11	Фізичні основи технічних засобів розвідки	4	ЗАЛІК
ОК12	Математичні основи криптології	4	ЗАЛІК
ОК13	Основи побудови та захисту сучасних операційних систем	5	ЕКЗАМЕН
ОК14	Введення в мережі	5	ЕКЗАМЕН
ОК15	Технології програмування	12	ЗАЛІК, ЕКЗАМЕН
ОК16	Теоретичні основи криптографії	5	ЕКЗАМЕН
ОК17	Основи побудови та захисту мікропроцесорних систем	4	ЗАЛІК
ОК18	Менеджмент інформаційної безпеки	5	ЕКЗАМЕН
ОК19	Основи математичного моделювання	4	ЗАЛІК
ОК20	Основи криптографічного захисту	5	ЗАЛІК
ОК21	Безпека в інформаційно-комунікаційних системах	5	ЕКЗАМЕН
ОК22	Інформаційні системи та Інтернет технології	12	ЕКЗАМЕН, ЕКЗАМЕН
ОК23	Безпека Інтернет-речей	6	ЕКЗАМЕН
ОК24	Виробнича практика	3	ЗВІТ
ОК25	Комплексні системи захисту інформації	5	ЗАЛІК
ОК26	Іноземна мова академічної та професійної комунікації	4	ЗАЛІК
ОК27	Комплексний курсовий проект	3	КОНСУЛЬТАЦІЙНИЙ ПРОЕКТ
ОК28	Основи стеганографічного захисту інформації	4	ЗАЛІК
ОК29	Організаційне забезпечення захисту інформації	4	ЗАЛІК
ОК30	Комплексний тренінг	5	ЗВІТ
ОК31	Переддипломна практика	5	ЗВІТ
ОК32	Дипломний проект	10	ДИПЛОМНИЙ ПРОЕКТ
ВИБІРКОВІ ОСВІТНІ КОМПОНЕНТИ			
ВК6	Мейджор 1	5	ЕКЗАМЕН
ВК7	Мейджор 2	5	ЕКЗАМЕН
ВК8	Мейджор 3	5	ЕКЗАМЕН
ВК9	Мейджор 4	5	ЕКЗАМЕН

ВК10	Мейджор 5	5	ЕКЗАМЕН
ВК11	Мейджор 6	5	ЕКЗАМЕН
ВК12	Мейджор 7	5	ЕКЗАМЕН

4.2. ВИБІРКОВА СКЛАДОВА ОСВІТНЬО-ПРОФЕСІЙНОЇ ПРОГРАМИ

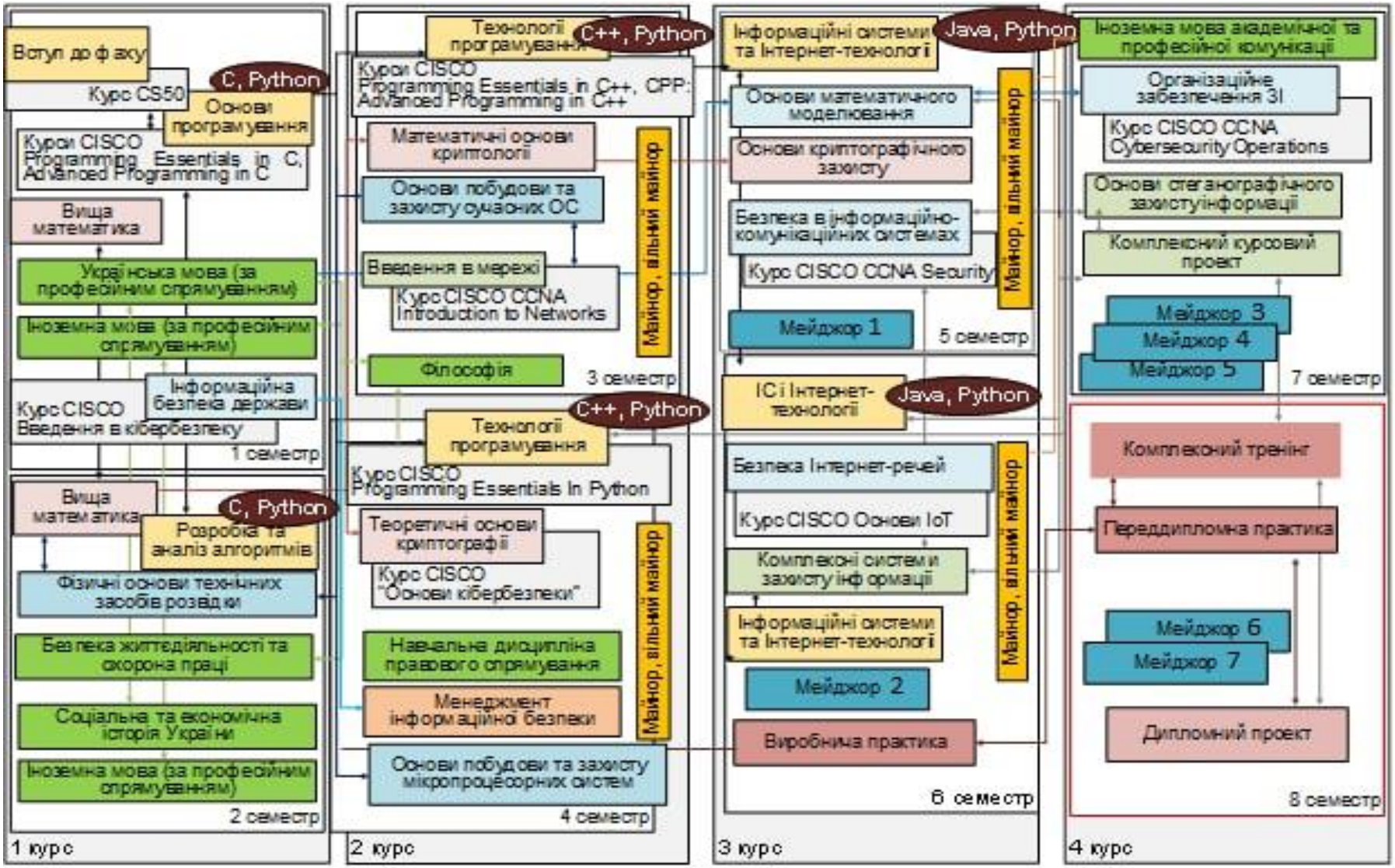
Вибіркова складова освітньо-професійної програми складається з:

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

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

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

4.3. СТРУКТУРНО-ЛОГІЧНА СХЕМА ПІДГОТОВКИ ЗДОБУВАЧІВ ВИЩОЇ ОСВІТИ



V. ФОРМИ АТЕСТАЦІЇ ЗДОБУВАЧІВ ВИЩОЇ ОСВІТИ

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

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				
КЗ 1. Здатність застосовувати знання у практичних ситуаціях.	+	+		
КЗ 2. Знання та розуміння предметної області та розуміння професії.	+	+		
КЗ 3. Здатність професійно спілкуватися державною та іноземною мовами як усно, так і письмово	+	+	+	
КЗ 4. Вміння виявляти, ставити та вирішувати проблеми за професійним спрямуванням	+	+	+	+
КЗ 5. Здатність до пошуку, оброблення та аналізу інформації.	+	+		+
КЗ 6. Здатність реалізувати свої права і обов'язки як члена суспільства, усвідомлювати цінності громадянського (вільного демократичного) суспільства та необхідність його сталого розвитку, верховенства права, прав і свобод людини і громадянина в Україні.		+	+	+
КЗ 7. Здатність зберігати та примножувати моральні, культурні, наукові цінності і досягнення суспільства на основі розуміння історії та закономірностей розвитку предметної області, її місця у загальній системі знань про природу і суспільство та у розвитку суспільства, техніки і технологій, використовувати різні види та форми рухової активності для активного відпочинку та ведення здорового способу життя.		+	+	+
СПЕЦІАЛЬНІ (ФАХОВІ) КОМПЕТЕНТНОСТІ				
КФ 1. Здатність застосовувати законодавчу та нормативно-правову базу, а також державні та міжнародні вимоги, практики і стандарти з метою здійснення професійної діяльності в галузі інформаційної та/або кібербезпеки.		+		+
КФ 2. Здатність до використання інформаційно-комунікаційних технологій, сучасних методів і моделей інформаційної безпеки та/або кібербезпеки.	+	+		+

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

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**	**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 ОК4 ОК5 ОК6 ОК7 ОК12 ОК16 ОК18 ОК21 ОК22 ОК24 ОК25 ОК26 ОК27 ОК29 ОК30 ОК31 ОК32	ОК1 ОК2 ОК4 ОК5 ОК6 ОК7 ОК12 ОК16 ОК18 ОК21 ОК22 ОК24 ОК25 ОК26 ОК27 ОК29 ОК30 ОК31 ОК32	ОК1 ОК2 ОК4 ОК5 ОК6 ОК7 ОК12 ОК16 ОК18 ОК21 ОК22 ОК24 ОК25 ОК26 ОК27 ОК29 ОК30 ОК31 ОК32																
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	ОК1 ОК4 ОК5 ОК6 ОК7 ОК12 ОК16 ОК18 ОК21 ОК22 ОК24 ОК25 ОК27 ОК29 ОК30 ОК31 ОК32	ОК1 ОК4 ОК5 ОК6 ОК7 ОК12 ОК16 ОК18 ОК21 ОК22 ОК24 ОК25 ОК27 ОК29 ОК30 ОК31 ОК32		ОК1 ОК4 ОК5 ОК6 ОК7 ОК12 ОК16 ОК18 ОК21 ОК22 ОК24 ОК25 ОК27 ОК29 ОК30 ОК31 ОК32	ОК1 ОК4 ОК5 ОК6 ОК7 ОК12 ОК16 ОК18 ОК21 ОК22 ОК24 ОК25 ОК27 ОК29 ОК30 ОК31 ОК32														

Результати навчання	Компетентності																		
	Загальні							Спеціальні (фахові)											
	КЗ 1	**КЗ 2**	**КЗ 3**	**КЗ 4**	**КЗ 5**	**КЗ 6**	**КЗ 7**	**КФ 1**	**КФ 2**	**КФ 3**	**КФ 4**	**КФ 5**	**КФ 6**	**КФ 7**	**КФ 8**	**КФ 9**	**КФ 10**	**КФ 11**	**КФ 12**
РН 3 – використовувати результати самостійного пошуку, аналізу та синтезу інформації з різних джерел для ефективного рішення спеціалізованих задач професійної діяльності	ОК1 ОК4 ОК5 ОК6 ОК7 ОК12 ОК16 ОК18 ОК21 ОК22 ОК24 ОК25 ОК27 ОК29 ОК30 ОК31 ОК32	ОК1 ОК4 ОК5 ОК6 ОК7 ОК12 ОК16 ОК18 ОК21 ОК22 ОК24 ОК25 ОК27 ОК29 ОК30 ОК31 ОК32		ОК1 ОК4 ОК5 ОК6 ОК7 ОК12 ОК16 ОК18 ОК21 ОК22 ОК24 ОК25 ОК27 ОК29 ОК30 ОК31 ОК32	ОК1 ОК4 ОК5 ОК6 ОК7 ОК12 ОК16 ОК18 ОК21 ОК22 ОК24 ОК25 ОК27 ОК29 ОК30 ОК31 ОК32														
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	ОК1 ОК4 ОК5 ОК6 ОК7 ОК12 ОК16 ОК18 ОК21 ОК22 ОК24 ОК25 ОК27 ОК29 ОК30 ОК31 ОК32	ОК1 ОК4 ОК5 ОК6 ОК7 ОК12 ОК16 ОК18 ОК21 ОК22 ОК24 ОК25 ОК27 ОК29 ОК30 ОК31 ОК32		ОК1 ОК4 ОК5 ОК6 ОК7 ОК12 ОК16 ОК18 ОК21 ОК22 ОК24 ОК25 ОК27 ОК29 ОК30 ОК31 ОК32	ОК1 ОК4 ОК5 ОК6 ОК7 ОК12 ОК16 ОК18 ОК21 ОК22 ОК24 ОК25 ОК27 ОК29 ОК30 ОК31 ОК32														
РН 5 – адаптуватися в умовах частої зміни технологій професійної діяльності, прогнозувати кінцевий результат		ОК4 ОК5 ОК6 ОК7 ОК12 ОК16		ОК4 ОК5 ОК6 ОК7 ОК12 ОК16	ОК4 ОК5 ОК6 ОК7 ОК12 ОК16														

Результати навчання	Компетентності																		
	Загальні							Спеціальні (фахові)											
	КЗ 1	КЗ 2	КЗ 3	КЗ 4	КЗ 5	КЗ 6	КЗ 7	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 ОК21 ОК22 ОК24 ОК25 ОК27 ОК29 ОК30 ОК31 ОК32		ОК18 ОК21 ОК22 ОК24 ОК25 ОК27 ОК29 ОК30 ОК31 ОК32	ОК18 ОК21 ОК22 ОК24 ОК25 ОК27 ОК29 ОК30 ОК31 ОК32														
РН 6 – критично осмислювати основні теорії, принципи, методи і поняття у навчанні та професійній діяльності		ОК6 ОК7 ОК12 ОК16 ОК18 ОК21 ОК22 ОК25 ОК27 ОК29 ОК30 ОК31 ОК32																	
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		ОК5 ОК6 ОК7 ОК12 ОК16 ОК18 ОК21 ОК22 ОК24 ОК25 ОК27 ОК29 ОК30 ОК31 ОК32		ОК5 ОК6 ОК7 ОК12 ОК16 ОК18 ОК21 ОК22 ОК24 ОК25 ОК27 ОК29 ОК30 ОК31 ОК32				ОК5 ОК6 ОК7 ОК12 ОК16 ОК18 ОК21 ОК22 ОК24 ОК25 ОК27 ОК29 ОК30 ОК31 ОК32										
РН 8 – готувати пропозиції до нормативних актів щодо		ОК5		ОК5				ОК5											

Результати навчання	Компетентності																		
	Загальні							Спеціальні (фахові)											
	КЗ 1	**КЗ 2**	**КЗ 3**	**КЗ 4**	**КЗ 5**	**КЗ 6**	**КЗ 7**	**КФ 1**	**КФ 2**	**КФ 3**	**КФ 4**	**КФ 5**	**КФ 6**	**КФ 7**	**КФ 8**	**КФ 9**	**КФ 10**	**КФ 11**	**КФ 12**
забезпечення інформаційної та /або кібербезпеки		ОК6 ОК7 ОК12 ОК16 ОК18 ОК21 ОК22 ОК24 ОК25 ОК27 ОК29 ОК30 ОК31 ОК32		ОК6 ОК7 ОК12 ОК16 ОК18 ОК21 ОК22 ОК24 ОК25 ОК27 ОК29 ОК30 ОК31 ОК32				ОК6 ОК7 ОК12 ОК16 ОК18 ОК21 ОК22 ОК24 ОК25 ОК27 ОК29 ОК30 ОК31 ОК32											
РН 9 – впроваджувати процеси, що базуються на національних та міжнародних стандартах, виявлення, ідентифікації, аналізу та реагування на інциденти інформаційної та/або кібербезпеки					ОК4 ОК6 ОК7 ОК9 ОК8 ОК10 ОК11 ОК12 ОК13 ОК14 ОК15 ОК16 ОК18 ОК19 ОК20 ОК21 ОК22 ОК25 ОК27 ОК28 ОК29 ОК30 ОК31 ОК32			ОК4 ОК6 ОК7 ОК8 ОК9 ОК10 ОК11 ОК12 ОК13 ОК14 ОК15 ОК16 ОК18 ОК19 ОК20 ОК21 ОК22 ОК25 ОК27 ОК28 ОК29 ОК30 ОК31 ОК32		ОК4 ОК6 ОК7 ОК8 ОК9 ОК10 ОК11 ОК12 ОК13 ОК14 ОК15 ОК16 ОК18 ОК19 ОК20 ОК21 ОК22 ОК25 ОК27 ОК28 ОК29 ОК30 ОК31 ОК32	ОК4 ОК6 ОК7 ОК8 ОК9 ОК10 ОК11 ОК12 ОК13 ОК14 ОК15 ОК16 ОК18 ОК19 ОК20 ОК21 ОК22 ОК25 ОК27 ОК28 ОК29 ОК30 ОК31 ОК32	ОК4 ОК6 ОК7 ОК8 ОК9 ОК10 ОК11 ОК12 ОК13 ОК14 ОК15 ОК16 ОК18 ОК19 ОК20 ОК21 ОК22 ОК25 ОК27 ОК28 ОК29 ОК30 ОК31 ОК32		ОК4 ОК6 ОК7 ОК8 ОК9 ОК10 ОК11 ОК12 ОК13 ОК14 ОК15 ОК16 ОК18 ОК19 ОК20 ОК21 ОК22 ОК25 ОК27 ОК28 ОК29 ОК30 ОК31 ОК32	ОК4 ОК6 ОК7 ОК8 ОК9 ОК10 ОК11 ОК12 ОК13 ОК14 ОК15 ОК16 ОК18 ОК19 ОК20 ОК21 ОК22 ОК25 ОК27 ОК28 ОК29 ОК30 ОК31 ОК32	ОК4 ОК6 ОК7 ОК8 ОК9 ОК10 ОК11 ОК12 ОК13 ОК14 ОК15 ОК16 ОК18 ОК19 ОК20 ОК21 ОК22 ОК25 ОК27 ОК28 ОК29 ОК30 ОК31 ОК32		ОК4 ОК6 ОК7 ОК8 ОК9 ОК10 ОК11 ОК12 ОК13 ОК14 ОК15 ОК16 ОК18 ОК19 ОК20 ОК21 ОК22 ОК25 ОК27 ОК28 ОК29 ОК30 ОК31 ОК32	ОК4 ОК6 ОК7 ОК8 ОК9 ОК10 ОК11 ОК12 ОК13 ОК14 ОК15 ОК16 ОК18 ОК19 ОК20 ОК21 ОК22 ОК25 ОК27 ОК28 ОК29 ОК30 ОК31 ОК32

Результати навчання	Компетентності																	
	Загальні							Спеціальні (фахові)										
	КЗ 1	**КЗ 2**	**КЗ 3**	**КЗ 4**	**КЗ 5**	**КЗ 6**	**КЗ 7**	**КФ 1**	**КФ 2**	**КФ 3**	**КФ 4**	**КФ 5**	**КФ 6**	**КФ 7**	**КФ 8**	**КФ 9**	**КФ 10**	**КФ 11**	**КФ 12**
РН 10 – виконувати аналіз та декомпозицію інформаційно-телекомунікаційних систем	ОК1 ОК4 ОК5 ОК7 ОК9 ОК11 ОК12 ОК14 ОК16 ОК17 ОК20 ОК21 ОК22 ОК23 ОК24 ОК31 ОК32								ОК1 ОК4 ОК5 ОК9 ОК7 ОК11 ОК12 ОК14 ОК16 ОК17 ОК20 ОК21 ОК22 ОК23 ОК24 ОК31 ОК32									ОК1 ОК4 ОК5 ОК9 ОК7 ОК11 ОК12 ОК14 ОК16 ОК17 ОК20 ОК21 ОК22 ОК23 ОК24 ОК31 ОК32	
РН 11 – виконувати аналіз зв’язків між інформаційними процесами на віддалених обчислювальних системах	ОК1 ОК4 ОК5 ОК7 ОК9 ОК11 ОК12 ОК14 ОК16 ОК17 ОК20 ОК21 ОК22 ОК23 ОК24 ОК32								ОК1 ОК4 ОК5 ОК7 ОК9 ОК11 ОК12 ОК14 ОК16 ОК17 ОК20 ОК21 ОК22 ОК23 ОК24 ОК32									ОК1 ОК4 ОК5 ОК7 ОК9 ОК11 ОК12 ОК14 ОК16 ОК17 ОК20 ОК21 ОК22 ОК23 ОК24 ОК32	
РН 12 – розробляти моделі загроз та порушника														ОК8 ОК10 ОК11 ОК14 ОК15 ОК19					ОК8 ОК10 ОК11 ОК14 ОК15 ОК19

Результати навчання	Компетентності																		
	Загальні							Спеціальні (фахові)											
	КЗ 1	**КЗ 2**	**КЗ 3**	**КЗ 4**	**КЗ 5**	**КЗ 6**	**КЗ 7**	**КФ 1**	**КФ 2**	**КФ 3**	**КФ 4**	**КФ 5**	**КФ 6**	**КФ 7**	**КФ 8**	**КФ 9**	**КФ 10**	**КФ 11**	**КФ 12**
														ОК21 ОК22					ОК21 ОК22
РН 13 – аналізувати проекти інформаційно-телекомунікаційних систем базуючись на стандартизованих технологіях та протоколах передачі даних					ОК4 ОК7 ОК9 ОК11 ОК12 ОК13 ОК14 ОК16 ОК17 ОК19 ОК20 ОК21 ОК22 ОК30 ОК31 ОК32				ОК4 ОК7 ОК9 ОК11 ОК12 ОК13 ОК14 ОК16 ОК17 ОК19 ОК20 ОК21 ОК22 ОК30 ОК31 ОК32			ОК4 ОК7 ОК9 ОК11 ОК12 ОК13 ОК14 ОК16 ОК17 ОК19 ОК20 ОК21 ОК22 ОК30 ОК31 ОК32			ОК4 ОК7 ОК9 ОК11 ОК12 ОК13 ОК14 ОК16 ОК17 ОК19 ОК20 ОК21 ОК22 ОК30 ОК31 ОК32			ОК4 ОК7 ОК9 ОК11 ОК12 ОК13 ОК14 ОК16 ОК17 ОК19 ОК20 ОК21 ОК22 ОК30 ОК31 ОК32	ОК4 ОК7 ОК9 ОК11 ОК12 ОК13 ОК14 ОК16 ОК17 ОК19 ОК20 ОК21 ОК22 ОК30 ОК31 ОК32
РН 14 – вирішувати завдання захисту програм та інформації, що обробляється в інформаційно-телекомунікаційних системах програмно-апаратними засобами та давати оцінку результативності якості прийнятих рішень									ОК7 ОК9 ОК11 ОК12 ОК13 ОК14 ОК16 ОК17 ОК18 ОК19 ОК20 ОК21 ОК22 ОК23 ОК30 ОК31 ОК32	ОК7 ОК9 ОК11 ОК12 ОК13 ОК14 ОК16 ОК17 ОК18 ОК19 ОК20 ОК21 ОК22 ОК23 ОК30 ОК31 ОК32		ОК7 ОК9 ОК11 ОК12 ОК13 ОК14 ОК16 ОК17 ОК18 ОК19 ОК20 ОК21 ОК22 ОК23 ОК30 ОК31 ОК32			ОК7 ОК9 ОК11 ОК12 ОК13 ОК14 ОК16 ОК17 ОК18 ОК19 ОК20 ОК21 ОК22 ОК23 ОК30 ОК31 ОК32		ОК7 ОК9 ОК11 ОК12 ОК13 ОК14 ОК16 ОК17 ОК18 ОК19 ОК20 ОК21 ОК22 ОК23 ОК30 ОК31 ОК32	ОК7 ОК9 ОК11 ОК12 ОК13 ОК14 ОК16 ОК17 ОК18 ОК19 ОК20 ОК21 ОК22 ОК23 ОК30 ОК31 ОК32	
РН 15 – використовувати сучасне програмно-апаратне забезпечення інформаційно-комунікаційних технологій									ОК7 ОК9 ОК11 ОК12 ОК14	ОК7 ОК9 ОК11 ОК12 ОК14								ОК7 ОК9 ОК11 ОК12 ОК14	

Результати навчання	Компетентності																		
	Загальні							Спеціальні (фахові)											
	КЗ 1	**КЗ 2**	**КЗ 3**	**КЗ 4**	**КЗ 5**	**КЗ 6**	**КЗ 7**	**КФ 1**	**КФ 2**	**КФ 3**	**КФ 4**	**КФ 5**	**КФ 6**	**КФ 7**	**КФ 8**	**КФ 9**	**КФ 10**	**КФ 11**	**КФ 12**
									ОК16 ОК17 ОК18 ОК19 ОК20 ОК21 ОК22 ОК23	ОК16 ОК17 ОК18 ОК19 ОК20 ОК21 ОК22 ОК23								ОК16 ОК17 ОК18 ОК19 ОК20 ОК21 ОК22 ОК23	
РН 16 – реалізовувати комплексні системи захисту інформації в автоматизованих системах (АС) організації (підприємства) відповідно до вимог нормативно-правових документів								ОК7 ОК8 ОК9 ОК10 ОК11 ОК12 ОК14 ОК15 ОК16 ОК18 ОК19 ОК20 ОК22 ОК27 ОК29		ОК7 ОК8 ОК9 ОК10 ОК11 ОК12 ОК14 ОК15 ОК16 ОК18 ОК19 ОК20 ОК22 ОК27 ОК29				ОК7 ОК8 ОК9 ОК10 ОК11 ОК12 ОК14 ОК15 ОК16 ОК18 ОК19 ОК20 ОК22 ОК27 ОК29					ОК7 ОК8 ОК9 ОК10 ОК11 ОК12 ОК14 ОК15 ОК16 ОК18 ОК19 ОК20 ОК22 ОК27 ОК29
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,		ОК6 ОК7 ОК9 ОК10 ОК11 ОК12 ОК13 ОК14 ОК15 ОК16 ОК17 ОК18 ОК19 ОК20 ОК21 ОК22 ОК23							ОК6 ОК7 ОК9 ОК10 ОК11 ОК12 ОК13 ОК14 ОК15 ОК16 ОК17 ОК18 ОК19 ОК20 ОК21 ОК22 ОК23	ОК6 ОК7 ОК9 ОК10 ОК11 ОК12 ОК13 ОК14 ОК15 ОК16 ОК17 ОК18 ОК19 ОК20 ОК21 ОК22 ОК23	ОК6 ОК7 ОК9 ОК10 ОК11 ОК12 ОК13 ОК14 ОК15 ОК16 ОК17 ОК18 ОК19 ОК20 ОК21 ОК22 ОК23	ОК6 ОК7 ОК9 ОК10 ОК11 ОК12 ОК13 ОК14 ОК15 ОК16 ОК17 ОК18 ОК19 ОК20 ОК21 ОК22 ОК23	ОК6 ОК7 ОК9 ОК10 ОК11 ОК12 ОК13 ОК14 ОК15 ОК16 ОК17 ОК18 ОК19 ОК20 ОК21 ОК22 ОК23		ОК6 ОК7 ОК9 ОК10 ОК11 ОК12 ОК13 ОК14 ОК15 ОК16 ОК17 ОК18 ОК19 ОК20 ОК21 ОК22 ОК23			ОК6 ОК7 ОК9 ОК10 ОК11 ОК12 ОК13 ОК14 ОК15 ОК16 ОК17 ОК18 ОК19 ОК20 ОК21 ОК22 ОК23	

Результати навчання	Компетентності																		
	Загальні							Спеціальні (фахові)											
	КЗ 1	**КЗ 2**	**КЗ 3**	**КЗ 4**	**КЗ 5**	**КЗ 6**	**КЗ 7**	**КФ 1**	**КФ 2**	**КФ 3**	**КФ 4**	**КФ 5**	**КФ 6**	**КФ 7**	**КФ 8**	**КФ 9**	**КФ 10**	**КФ 11**	**КФ 12**
процесів для внутрішніх і віддалених компонент		ОК25 ОК27 ОК29 ОК30 ОК31 ОК32							ОК25 ОК27 ОК29 ОК30 ОК31 ОК32	ОК25 ОК27 ОК29 ОК30 ОК31 ОК32	ОК25 ОК27 ОК29 ОК30 ОК31 ОК32	ОК25 ОК27 ОК29 ОК30 ОК31 ОК32	ОК25 ОК27 ОК29 ОК30 ОК31 ОК32		ОК25 ОК27 ОК29 ОК30 ОК31 ОК32			ОК25 ОК27 ОК29 ОК30 ОК31 ОК32	
РН 18 – використовувати програмні та програмно-апаратні комплекси захисту інформаційних ресурсів	ОК1 ОК4 ОК5 ОК7 ОК9 ОК11 ОК12 ОК13 ОК14 ОК16 ОК17 ОК18 ОК19 ОК20 ОК21 ОК22 ОК23 ОК24 ОК31 ОК32								ОК1 ОК4 ОК5 ОК7 ОК9 ОК11 ОК12 ОК13 ОК14 ОК16 ОК17 ОК18 ОК19 ОК20 ОК21 ОК22 ОК23 ОК24 ОК31 ОК32	ОК1 ОК4 ОК5 ОК7 ОК9 ОК11 ОК12 ОК13 ОК14 ОК16 ОК17 ОК18 ОК19 ОК20 ОК21 ОК22 ОК23 ОК24 ОК31 ОК32		ОК1 ОК4 ОК5 ОК7 ОК9 ОК11 ОК12 ОК13 ОК14 ОК16 ОК17 ОК18 ОК19 ОК20 ОК21 ОК22 ОК23 ОК24 ОК31 ОК32					ОК1 ОК4 ОК5 ОК7 ОК9 ОК11 ОК12 ОК13 ОК14 ОК16 ОК17 ОК18 ОК19 ОК20 ОК21 ОК22 ОК23 ОК24 ОК31 ОК32	
РН 19 – застосовувати теорії та методи захисту для забезпечення безпеки інформації в інформаційно-телекомунікаційних системах	ОК1 ОК4 ОК5 ОК7 ОК9 ОК11 ОК12 ОК13 ОК14 ОК16 ОК17 ОК20 ОК21 ОК22								ОК1 ОК4 ОК5 ОК7 ОК9 ОК11 ОК12 ОК13 ОК14 ОК16 ОК17 ОК20 ОК21 ОК22			ОК1 ОК4 ОК5 ОК7 ОК9 ОК11 ОК12 ОК13 ОК14 ОК16 ОК17 ОК20 ОК21 ОК22			ОК1 ОК4 ОК5 ОК7 ОК9 ОК11 ОК12 ОК13 ОК14 ОК16 ОК17 ОК20 ОК21 ОК22			ОК1 ОК4 ОК5 ОК7 ОК9 ОК11 ОК12 ОК13 ОК14 ОК16 ОК17 ОК20 ОК21	

Результати навчання	Компетентності																		
	Загальні							Спеціальні (фахові)											
	КЗ 1	КЗ 2	КЗ 3	КЗ 4	КЗ 5	КЗ 6	КЗ 7	КФ 1	КФ 2	КФ 3	КФ 4	КФ 5	КФ 6	КФ 7	КФ 8	КФ 9	КФ 10	КФ 11	КФ 12
	ОК23 ОК24 ОК31 ОК32								ОК23 ОК24 ОК31 ОК32			ОК23 ОК24 ОК31 ОК32			ОК23 ОК24 ОК31 ОК32			ОК22 ОК23 ОК24 ОК31 ОК32	
РН 20 – забезпечувати функціонування спеціального програмного забезпечення, щодо захисту інформації від руйнуючих програмних впливів, руйнуючих кодів в інформаційно-телекомунікаційних системах	ОК1 ОК4 ОК5 ОК7 ОК9 ОК11 ОК12 ОК13 ОК14 ОК15 ОК16 ОК18 ОК19 ОК20 ОК21 ОК22 ОК23 ОК24 ОК30 ОК31 ОК32								ОК1 ОК4 ОК5 ОК7 ОК9 ОК11 ОК12 ОК13 ОК14 ОК15 ОК16 ОК18 ОК19 ОК20 ОК21 ОК22 ОК23 ОК24 ОК30 ОК31 ОК32	ОК1 ОК4 ОК5 ОК7 ОК9 ОК11 ОК12 ОК13 ОК14 ОК15 ОК16 ОК18 ОК19 ОК20 ОК21 ОК22 ОК23 ОК24 ОК30 ОК31 ОК32		ОК1 ОК4 ОК5 ОК7 ОК9 ОК11 ОК12 ОК13 ОК14 ОК15 ОК16 ОК18 ОК19 ОК20 ОК21 ОК22 ОК23 ОК24 ОК30 ОК31 ОК32	ОК1 ОК4 ОК5 ОК7 ОК9 ОК11 ОК12 ОК14 ОК16 ОК13 ОК15 ОК18 ОК19 ОК20 ОК21 ОК22 ОК23 ОК24 ОК30 ОК31 ОК32				ОК1 ОК4 ОК5 ОК7 ОК9 ОК11 ОК12 ОК14 ОК16 ОК13 ОК15 ОК18 ОК19 ОК20 ОК21 ОК22 ОК23 ОК24 ОК30 ОК31 ОК32		
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	ОК1 ОК4 ОК5 ОК7 ОК9 ОК12 ОК13 ОК16 ОК18 ОК20 ОК21 ОК22 ОК24 ОК27											ОК1 ОК4 ОК5 ОК7 ОК9 ОК12 ОК13 ОК16 ОК18 ОК20 ОК21 ОК22 ОК24 ОК27			ОК1 ОК4 ОК5 ОК7 ОК9 ОК12 ОК13 ОК16 ОК18 ОК20 ОК21 ОК22 ОК24 ОК27		ОК1 ОК4 ОК5 ОК7 ОК9 ОК12 ОК13 ОК16 ОК18 ОК20 ОК21 ОК22 ОК24 ОК27	

Результати навчання	Компетентності																		
	Загальні							Спеціальні (фахові)											
	КЗ 1	КЗ 2	КЗ 3	КЗ 4	КЗ 5	КЗ 6	КЗ 7	КФ 1	КФ 2	КФ 3	КФ 4	КФ 5	КФ 6	КФ 7	КФ 8	КФ 9	КФ 10	КФ 11	КФ 12
	ОК28 ОК31 ОК32											ОК28 ОК31 ОК32				ОК28 ОК31 ОК32		ОК28 ОК31 ОК32	
РН 22 – вирішувати задачі управління процедурами ідентифікації, автентифікації, авторизації процесів і користувачів в інформаційно-телекомунікаційних системах згідно встановленої політики інформаційної і\або кібербезпеки	ОК1 ОК4 ОК5 ОК7 ОК9 ОК12 ОК13 ОК16 ОК20 ОК24 ОК31 ОК32											ОК1 ОК4 ОК5 ОК7 ОК9 ОК12 ОК13 ОК16 ОК20 ОК24 ОК31 ОК32						ОК1 ОК4 ОК5 ОК7 ОК9 ОК12 ОК13 ОК16 ОК20 ОК24 ОК31 ОК32	
РН 23 – реалізовувати заходи з протидії отриманню несанкціонованого доступу до інформаційних ресурсів і процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах												ОК7 ОК9 ОК12 ОК13 ОК14 ОК15 ОК16 ОК17 ОК20 ОК21 ОК22	ОК7 ОК9 ОК12 ОК13 ОК14 ОК15 ОК16 ОК17 ОК20 ОК21 ОК22		ОК7 ОК9 ОК12 ОК13 ОК14 ОК15 ОК16 ОК17 ОК20 ОК21 ОК22			ОК7 ОК9 ОК12 ОК13 ОК14 ОК15 ОК16 ОК17 ОК20 ОК21 ОК22	
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)	ОК1 ОК4 ОК5 ОК6 ОК7 ОК9 ОК10 ОК11 ОК12 ОК13 ОК16 ОК18 ОК20 ОК21										ОК1 ОК4 ОК5 ОК6 ОК7 ОК9 ОК10 ОК11 ОК12 ОК13 ОК16 ОК18 ОК20 ОК21	ОК1 ОК4 ОК5 ОК6 ОК7 ОК9 ОК10 ОК11 ОК12 ОК13 ОК16 ОК18 ОК20 ОК21				ОК1 ОК4 ОК5 ОК6 ОК7 ОК9 ОК10 ОК11 ОК12 ОК13 ОК16 ОК18 ОК20 ОК21		ОК1 ОК4 ОК5 ОК6 ОК7 ОК9 ОК10 ОК11 ОК12 ОК13 ОК16 ОК18 ОК20 ОК21	

Результати навчання	Компетентності																		
	Загальні							Спеціальні (фахові)											
	КЗ 1	**КЗ 2**	**КЗ 3**	**КЗ 4**	**КЗ 5**	**КЗ 6**	**КЗ 7**	**КФ 1**	**КФ 2**	**КФ 3**	**КФ 4**	**КФ 5**	**КФ 6**	**КФ 7**	**КФ 8**	**КФ 9**	**КФ 10**	**КФ 11**	**КФ 12**
	ОК22 ОК24 ОК25 ОК27 ОК28 ОК29 ОК31 ОК32										ОК22 ОК24 ОК25 ОК27 ОК28 ОК29 ОК31 ОК32	ОК22 ОК24 ОК25 ОК27 ОК28 ОК29 ОК31 ОК32				ОК22 ОК24 ОК25 ОК27 ОК28 ОК29 ОК31 ОК32		ОК22 ОК24 ОК25 ОК27 ОК28 ОК29 ОК31 ОК32	
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												ОК7 ОК9 ОК12 ОК13 ОК16 ОК18 ОК20 ОК21 ОК22 ОК28 ОК32			ОК7 ОК9 ОК12 ОК13 ОК16 ОК18 ОК20 ОК21 ОК22 ОК28 ОК32	ОК7 ОК9 ОК12 ОК13 ОК16 ОК18 ОК20 ОК21 ОК22 ОК28 ОК32		ОК7 ОК9 ОК12 ОК13 ОК16 ОК18 ОК20 ОК21 ОК22 ОК28 ОК32	
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												ОК7 ОК9 ОК12 ОК13 ОК16 ОК20 ОК32						ОК7 ОК9 ОК12 ОК13 ОК16 ОК20 ОК32	
РН 27 – вирішувати задачі захисту потоків даних в інформаційних, інформаційно-	ОК1 ОК4 ОК5 ОК6 ОК10 ОК11										ОК1 ОК4 ОК5 ОК6 ОК10 ОК11	ОК1 ОК4 ОК5 ОК6 ОК10 ОК11	ОК1 ОК4 ОК5 ОК6 ОК10 ОК11						

Результати навчання	Компетентності																		
	Загальні							Спеціальні (фахові)											
	КЗ 1	**КЗ 2**	**КЗ 3**	**КЗ 4**	**КЗ 5**	**КЗ 6**	**КЗ 7**	**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	ОК12 ОК13 ОК14 ОК15 ОК16 ОК17 ОК20 ОК21 ОК22 ОК24 ОК25 ОК27 ОК29 ОК31 ОК32										ОК12 ОК13 ОК14 ОК15 ОК16 ОК17 ОК20 ОК21 ОК22 ОК24 ОК25 ОК27 ОК29 ОК31 ОК32	ОК12 ОК13 ОК14 ОК15 ОК16 ОК17 ОК20 ОК21 ОК22 ОК24 ОК25 ОК27 ОК29 ОК31 ОК32	ОК12 ОК13 ОК14 ОК15 ОК16 ОК17 ОК20 ОК21 ОК22 ОК24 ОК25 ОК27 ОК29 ОК31 ОК32						
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					ОК4 ОК7 ОК11 ОК12 ОК13 ОК14 ОК16 ОК18 ОК19 ОК20 ОК21 ОК22 ОК27 ОК28 ОК30 ОК31 ОК32							ОК4 ОК7 ОК11 ОК12 ОК13 ОК14 ОК16 ОК18 ОК19 ОК20 ОК21 ОК22 ОК27 ОК28 ОК30 ОК31 ОК32				ОК4 ОК7 ОК11 ОК12 ОК13 ОК14 ОК16 ОК18 ОК19 ОК20 ОК21 ОК22 ОК27 ОК28 ОК30 ОК31 ОК32			ОК7 ОК11 ОК12 ОК13 ОК14 ОК16 ОК18 ОК19 ОК20 ОК21 ОК22 ОК27 ОК28 ОК30 ОК31 ОК32
РН 29 – здійснювати оцінювання можливості реалізації потенційних загроз інформації, що обробляється в інформаційно-телекомунікаційних системах та ефективності										ОК6 ОК7 ОК9 ОК10 ОК11 ОК12 ОК13 ОК14	ОК6 ОК7 ОК9 ОК10 ОК11 ОК12 ОК13 ОК14	ОК6 ОК7 ОК9 ОК10 ОК11 ОК12 ОК13 ОК14			ОК6 ОК7 ОК9 ОК10 ОК11 ОК12 ОК13 ОК14	ОК6 ОК7 ОК9 ОК10 ОК11 ОК12 ОК13 ОК14			ОК6 ОК7 ОК9 ОК10 ОК11 ОК12 ОК13 ОК14

Результати навчання	Компетентності																		
	Загальні							Спеціальні (фахові)											
	КЗ 1	КЗ 2	КЗ 3	КЗ 4	КЗ 5	КЗ 6	КЗ 7	КФ 1	КФ 2	КФ 3	КФ 4	КФ 5	КФ 6	КФ 7	КФ 8	КФ 9	КФ 10	КФ 11	КФ 12
використання комплексів засобів захисту в умовах реалізації загроз різних класів										ОК16 ОК18 ОК19 ОК20 ОК21 ОК22 ОК25 ОК27 ОК28 ОК29 ОК32	ОК16 ОК18 ОК19 ОК20 ОК21 ОК22 ОК25 ОК27 ОК28 ОК29 ОК32	ОК16 ОК18 ОК19 ОК20 ОК21 ОК22 ОК25 ОК27 ОК28 ОК29 ОК32			ОК16 ОК18 ОК19 ОК20 ОК21 ОК22 ОК25 ОК27 ОК28 ОК29 ОК32	ОК16 ОК18 ОК19 ОК20 ОК21 ОК22 ОК25 ОК27 ОК28 ОК29 ОК32			ОК16 ОК18 ОК19 ОК20 ОК21 ОК22 ОК25 ОК27 ОК28 ОК29 ОК25
РН 30 – здійснювати оцінювання можливості несанкціонованого доступу до елементів інформаційно-телекомунікаційних систем																			ОК11 ОК14 ОК19 ОК22
РН 31 – застосовувати теорії та методи захисту для забезпечення безпеки елементів інформаційно-телекомунікаційних систем									ОК11 ОК12 ОК14 ОК15 ОК16 ОК17 ОК20 ОК21 ОК22 ОК23 ОК30 ОК31 ОК32				ОК11 ОК12 ОК14 ОК15 ОК16 ОК17 ОК20 ОК21 ОК22 ОК23 ОК30 ОК31 ОК32				ОК11 ОК12 ОК14 ОК15 ОК16 ОК17 ОК20 ОК21 ОК22 ОК23 ОК30 ОК31 ОК32			
РН 32 – вирішувати задачі управління процесами відновлення штатного функціонування інформаційно-телекомунікаційних систем з використанням процедур резервування згідно встановленої політики безпеки	ОК1 ОК4 ОК5 ОК6 ОК7 ОК9 ОК10 ОК11 ОК12 ОК13 ОК16										ОК1 ОК5 ОК4 ОК6 ОК7 ОК9 ОК10 ОК11 ОК12 ОК13 ОК16	ОК1 ОК4 ОК5 ОК6 ОК7 ОК9 ОК10 ОК11 ОК12 ОК13 ОК16			ОК1 ОК4 ОК5 ОК6 ОК7 ОК9 ОК10 ОК11 ОК12 ОК13 ОК16			ОК1 ОК4 ОК5 ОК6 ОК7 ОК9 ОК10 ОК11 ОК12 ОК13 ОК16	

Результати навчання	Компетентності																		
	Загальні							Спеціальні (фахові)											
	КЗ 1	**КЗ 2**	**КЗ 3**	**КЗ 4**	**КЗ 5**	**КЗ 6**	**КЗ 7**	**КФ 1**	**КФ 2**	**КФ 3**	**КФ 4**	**КФ 5**	**КФ 6**	**КФ 7**	**КФ 8**	**КФ 9**	**КФ 10**	**КФ 11**	**КФ 12**
	ОК20 ОК21 ОК22 ОК24 ОК25 ОК27 ОК29 ОК31 ОК32										ОК20 ОК21 ОК22 ОК25 ОК24 ОК27 ОК29 ОК31 ОК32	ОК20 ОК21 ОК22 ОК24 ОК25 ОК27 ОК29 ОК31 ОК32			ОК20 ОК21 ОК22 ОК24 ОК25 ОК27 ОК29 ОК31 ОК32			ОК20 ОК21 ОК22 ОК24 ОК25 ОК27 ОК29 ОК31 ОК32	
РН 33 – вирішувати задачі забезпечення безперервності бізнес процесів організації на основі теорії ризиків								ОК6 ОК7 ОК10 ОК11 ОК14 ОК18 ОК19 ОК21 ОК22 ОК25 ОК27 ОК28 ОК29 ОК32			ОК6 ОК7 ОК10 ОК11 ОК14 ОК18 ОК19 ОК21 ОК22 ОК25 ОК27 ОК28 ОК29 ОК32				ОК6 ОК7 ОК10 ОК11 ОК14 ОК18 ОК19 ОК21 ОК22 ОК25 ОК27 ОК28 ОК29 ОК32	ОК6 ОК7 ОК10 ОК11 ОК14 ОК18 ОК19 ОК21 ОК22 ОК25 ОК27 ОК28 ОК29 ОК32			ОК6 ОК7 ОК10 ОК11 ОК14 ОК18 ОК19 ОК21 ОК22 ОК25 ОК27 ОК28 ОК29 ОК32
РН 34 – приймати участь у розробці та впровадженні стратегії інформаційної безпеки та/або кібербезпеки відповідно до цілей і завдань організації								ОК6 ОК7 ОК10 ОК11 ОК12 ОК13 ОК14 ОК16 ОК18 ОК19 ОК20 ОК21 ОК22 ОК25 ОК27 ОК28			ОК6 ОК7 ОК10 ОК11 ОК12 ОК13 ОК14 ОК16 ОК18 ОК19 ОК20 ОК21 ОК22 ОК25 ОК27 ОК28	ОК6 ОК7 ОК10 ОК11 ОК12 ОК13 ОК14 ОК16 ОК18 ОК19 ОК20 ОК21 ОК22 ОК25 ОК27 ОК28			ОК6 ОК7 ОК10 ОК11 ОК12 ОК13 ОК14 ОК16 ОК18 ОК19 ОК20 ОК21 ОК22 ОК25 ОК27 ОК28	ОК6 ОК7 ОК10 ОК11 ОК12 ОК13 ОК14 ОК16 ОК18 ОК19 ОК20 ОК21 ОК22 ОК25 ОК27 ОК28			ОК6 ОК7 ОК10 ОК11 ОК12 ОК13 ОК14 ОК16 ОК18 ОК19 ОК20 ОК21 ОК22 ОК25 ОК27 ОК28

Результати навчання	Компетентності																		
	Загальні							Спеціальні (фахові)											
	КЗ 1	**КЗ 2**	**КЗ 3**	**КЗ 4**	**КЗ 5**	**КЗ 6**	**КЗ 7**	**КФ 1**	**КФ 2**	**КФ 3**	**КФ 4**	**КФ 5**	**КФ 6**	**КФ 7**	**КФ 8**	**КФ 9**	**КФ 10**	**КФ 11**	**КФ 12**
								ОК29 ОК32			ОК29 ОК32	ОК29 ОК32			ОК29 ОК32	ОК29 ОК32			ОК29 ОК32
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	ОК1 ОК4 ОК5 ОК6 ОК7 ОК8 ОК9 ОК10 ОК11 ОК12 ОК13 ОК14 ОК15 ОК16 ОК18 ОК19 ОК20 ОК21 ОК22 ОК24 ОК25 ОК27 ОК28 ОК29 ОК31 ОК32							ОК1 ОК4 ОК5 ОК6 ОК7 ОК8 ОК9 ОК10 ОК11 ОК12 ОК13 ОК14 ОК15 ОК16 ОК18 ОК19 ОК20 ОК21 ОК22 ОК24 ОК25 ОК27 ОК28 ОК29 ОК31 ОК32		ОК1 ОК4 ОК5 ОК6 ОК7 ОК8 ОК9 ОК10 ОК11 ОК12 ОК13 ОК14 ОК15 ОК16 ОК18 ОК19 ОК20 ОК21 ОК22 ОК24 ОК25 ОК27 ОК28 ОК29 ОК31 ОК32	ОК1 ОК4 ОК5 ОК6 ОК7 ОК8 ОК9 ОК10 ОК11 ОК12 ОК13 ОК14 ОК15 ОК16 ОК18 ОК19 ОК20 ОК21 ОК22 ОК24 ОК25 ОК27 ОК28 ОК29 ОК31 ОК32	ОК1 ОК4 ОК5 ОК6 ОК7 ОК8 ОК9 ОК10 ОК11 ОК12 ОК13 ОК14 ОК15 ОК16 ОК18 ОК19 ОК20 ОК21 ОК22 ОК24 ОК25 ОК27 ОК28 ОК29 ОК31 ОК32		ОК1 ОК4 ОК5 ОК6 ОК7 ОК8 ОК9 ОК10 ОК11 ОК12 ОК13 ОК14 ОК15 ОК16 ОК18 ОК19 ОК20 ОК21 ОК22 ОК24 ОК25 ОК27 ОК28 ОК29 ОК31 ОК32	ОК1 ОК4 ОК5 ОК6 ОК7 ОК8 ОК9 ОК10 ОК11 ОК12 ОК13 ОК14 ОК15 ОК16 ОК18 ОК19 ОК20 ОК21 ОК22 ОК24 ОК25 ОК27 ОК28 ОК29 ОК31 ОК32	ОК1 ОК4 ОК5 ОК6 ОК7 ОК8 ОК9 ОК10 ОК11 ОК12 ОК13 ОК14 ОК15 ОК16 ОК18 ОК19 ОК20 ОК21 ОК22 ОК24 ОК25 ОК27 ОК28 ОК29 ОК31 ОК32			ОК1 ОК4 ОК5 ОК6 ОК7 ОК8 ОК9 ОК10 ОК11 ОК12 ОК13 ОК14 ОК15 ОК16 ОК18 ОК19 ОК20 ОК21 ОК22 ОК24 ОК25 ОК27 ОК28 ОК29 ОК31 ОК32
РН 36 – виявляти небезпечні сигнали технічних засобів																	ОК30 ОК31		
РН 37 – вимірювати параметри небезпечних та завадових сигналів під час інструментального контролю процесів захисту інформації та визначати ефективність захисту інформації від витоку технічними каналами													ОК14 ОК15 ОК17 ОК21 ОК22 ОК30 ОК31 ОК32				ОК14 ОК15 ОК17 ОК21 ОК22 ОК30 ОК31 ОК32		

Результати навчання	Компетентності																		
	Загальні							Спеціальні (фахові)											
	КЗ 1	КЗ 2	КЗ 3	КЗ 4	КЗ 5	КЗ 6	КЗ 7	КФ 1	КФ 2	КФ 3	КФ 4	КФ 5	КФ 6	КФ 7	КФ 8	КФ 9	КФ 10	КФ 11	КФ 12
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													ОК14 ОК15 ОК17 ОК21 ОК22 ОК30 ОК31 ОК32				ОК14 ОК15 ОК17 ОК21 ОК22 ОК30 ОК31 ОК32		
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																	ОК30 ОК31		
РН 40 – інтерпретувати результати проведення спеціальних вимірювань з використанням технічних засобів, контролю характеристик ІТС відповідно до вимог нормативних документів системи технічного захисту інформації																	ОК30 ОК31		
РН 41 – забезпечувати неперервність процесу															ОК7 ОК9 ОК23			ОК7 ОК9 ОК23	

Результати навчання	Компетентності																		
	Загальні							Спеціальні (фахові)											
	КЗ 1	КЗ 2	КЗ 3	КЗ 4	КЗ 5	КЗ 6	КЗ 7	КФ 1	КФ 2	КФ 3	КФ 4	КФ 5	КФ 6	КФ 7	КФ 8	КФ 9	КФ 10	КФ 11	КФ 12
ведення журналів реєстрації подій та інцидентів на основі автоматизованих процедур															ОК31 ОК32			ОК31 ОК32	
РН 42 – впроваджувати процеси виявлення, ідентифікації, аналізу та реагування на інциденти інформаційної і/або кібербезпеки											ОК6 ОК7 ОК9 ОК10 ОК11 ОК12 ОК13 ОК14 ОК16 ОК18 ОК19 ОК20 ОК21 ОК22 ОК25 ОК27 ОК28 ОК29 ОК32	ОК6 ОК7 ОК9 ОК10 ОК11 ОК12 ОК13 ОК14 ОК16 ОК18 ОК19 ОК20 ОК21 ОК22 ОК25 ОК27 ОК28 ОК29 ОК32			ОК6 ОК7 ОК9 ОК10 ОК11 ОК12 ОК13 ОК14 ОК16 ОК18 ОК19 ОК20 ОК21 ОК22 ОК25 ОК27 ОК28 ОК29 ОК32	ОК6 ОК7 ОК9 ОК10 ОК11 ОК12 ОК13 ОК14 ОК16 ОК18 ОК19 ОК20 ОК21 ОК22 ОК25 ОК27 ОК28 ОК29 ОК32		ОК6 ОК7 ОК9 ОК10 ОК11 ОК12 ОК13 ОК14 ОК16 ОК18 ОК19 ОК20 ОК21 ОК22 ОК25 ОК27 ОК28 ОК29 ОК32	ОК6 ОК7 ОК9 ОК10 ОК11 ОК12 ОК13 ОК14 ОК16 ОК18 ОК19 ОК20 ОК21 ОК22 ОК25 ОК27 ОК28 ОК29 ОК32
РН 43 – застосовувати національні та міжнародні регулюючі акти в сфері інформаційної безпеки та/ або кібербезпеки для розслідування інцидентів		ОК6 ОК7 ОК9 ОК10 ОК11 ОК12 ОК13 ОК14 ОК16 ОК18 ОК19 ОК20 ОК21 ОК22 ОК25 ОК27 ОК28 ОК29						ОК6 ОК7 ОК9 ОК10 ОК11 ОК12 ОК13 ОК14 ОК16 ОК18 ОК19 ОК20 ОК21 ОК22 ОК25 ОК27 ОК28 ОК29			ОК6 ОК7 ОК9 ОК10 ОК11 ОК12 ОК13 ОК14 ОК16 ОК18 ОК19 ОК20 ОК21 ОК22 ОК25 ОК27 ОК28 ОК29	ОК6 ОК7 ОК9 ОК10 ОК11 ОК12 ОК13 ОК14 ОК16 ОК18 ОК19 ОК20 ОК21 ОК22 ОК25 ОК27 ОК28 ОК29			ОК6 ОК7 ОК9 ОК10 ОК11 ОК12 ОК13 ОК14 ОК16 ОК18 ОК19 ОК20 ОК21 ОК22 ОК25 ОК27 ОК28 ОК29	ОК6 ОК7 ОК9 ОК10 ОК11 ОК12 ОК13 ОК14 ОК16 ОК18 ОК19 ОК20 ОК21 ОК22 ОК25 ОК27 ОК28 ОК29

Результати навчання	Компетентності																		
	Загальні							Спеціальні (фахові)											
	КЗ 1	КЗ 2	КЗ 3	КЗ 4	КЗ 5	КЗ 6	КЗ 7	КФ 1	КФ 2	КФ 3	КФ 4	КФ 5	КФ 6	КФ 7	КФ 8	КФ 9	КФ 10	КФ 11	КФ 12
		ОК30 ОК31 ОК32						ОК30 ОК31 ОК32			ОК30 ОК31 ОК32	ОК30 ОК31 ОК32			ОК30 ОК31 ОК32	ОК30 ОК31 ОК32		ОК30 ОК31 ОК32	ОК30 ОК31 ОК32
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								ОК6 ОК7 ОК10 ОК11 ОК12 ОК13 ОК14 ОК16 ОК18 ОК19 ОК20 ОК21 ОК22 ОК25 ОК27 ОК28 ОК29 ОК32			ОК6 ОК7 ОК10 ОК11 ОК12 ОК13 ОК14 ОК16 ОК18 ОК19 ОК20 ОК21 ОК22 ОК25 ОК27 ОК28 ОК29 ОК32	ОК6 ОК7 ОК10 ОК11 ОК12 ОК13 ОК14 ОК16 ОК18 ОК19 ОК20 ОК21 ОК22 ОК25 ОК27 ОК28 ОК29 ОК32			ОК6 ОК7 ОК10 ОК11 ОК12 ОК13 ОК14 ОК16 ОК18 ОК19 ОК20 ОК21 ОК22 ОК25 ОК27 ОК28 ОК29 ОК32	ОК6 ОК7 ОК10 ОК11 ОК12 ОК13 ОК14 ОК16 ОК18 ОК19 ОК20 ОК21 ОК22 ОК25 ОК27 ОК28 ОК29 ОК32			ОК6 ОК7 ОК10 ОК11 ОК12 ОК13 ОК14 ОК16 ОК18 ОК19 ОК20 ОК21 ОК22 ОК25 ОК27 ОК28 ОК29 ОК32
РН 45 – застосовувати ріні класи політик інформаційної безпеки та/ або кібербезпеки, що базуються на ризик-орієнтованому контролі доступу до інформаційних активів											ОК6 ОК7 ОК10 ОК11 ОК12 ОК13 ОК14 ОК16 ОК18 ОК19 ОК20 ОК21 ОК22 ОК25 ОК27 ОК28 ОК29 ОК32	ОК6 ОК7 ОК10 ОК11 ОК12 ОК13 ОК14 ОК16 ОК18 ОК19 ОК20 ОК21 ОК22 ОК25 ОК27 ОК28 ОК29 ОК32			ОК6 ОК7 ОК10 ОК11 ОК12 ОК13 ОК14 ОК16 ОК18 ОК19 ОК20 ОК21 ОК22 ОК25 ОК27 ОК28 ОК29 ОК32	ОК6 ОК7 ОК10 ОК11 ОК12 ОК13 ОК14 ОК16 ОК18 ОК19 ОК20 ОК21 ОК22 ОК25 ОК27 ОК28 ОК29 ОК32			ОК6 ОК7 ОК10 ОК11 ОК12 ОК13 ОК14 ОК16 ОК18 ОК19 ОК20 ОК21 ОК22 ОК25 ОК27 ОК28 ОК29 ОК32

Результати навчання	Компетентності																			
	Загальні							Спеціальні (фахові)												
	КЗ 1	КЗ 2	КЗ 3	КЗ 4	КЗ 5	КЗ 6	КЗ 7	КФ 1	КФ 2	КФ 3	КФ 4	КФ 5	КФ 6	КФ 7	КФ 8	КФ 9	КФ 10	КФ 11	КФ 12
РН 46 – здійснювати аналіз та мінімізацію ризиків обробки інформації в інформаційно-телекомунікаційних системах											ОК6 ОК7 ОК10 ОК11 ОК12 ОК13 ОК14 ОК16 ОК18 ОК19 ОК20 ОК21 ОК22 ОК25 ОК27 ОК28 ОК29 ОК32	ОК6 ОК7 ОК10 ОК11 ОК12 ОК13 ОК14 ОК16 ОК18 ОК19 ОК20 ОК21 ОК22 ОК25 ОК27 ОК28 ОК29 ОК32			ОК6 ОК7 ОК10 ОК11 ОК12 ОК13 ОК14 ОК16 ОК18 ОК19 ОК20 ОК21 ОК22 ОК25 ОК27 ОК28 ОК29 ОК32	ОК6 ОК7 ОК10 ОК11 ОК12 ОК13 ОК14 ОК16 ОК18 ОК19 ОК20 ОК21 ОК22 ОК25 ОК27 ОК28 ОК29 ОК32			ОК6 ОК7 ОК10 ОК11 ОК12 ОК13 ОК14 ОК16 ОК18 ОК19 ОК20 ОК21 ОК22 ОК25 ОК27 ОК28 ОК29 ОК32
РН 47 – вирішувати задачі захисту інформації, що обробляється в інформаційно-телекомунікаційних системах з використанням сучасних методів та засобів криптографічного захисту інформації									ОК7 ОК9 ОК11 ОК12 ОК13 ОК14 ОК16 ОК17 ОК18 ОК19 ОК20 ОК21 ОК22 ОК30 ОК31 ОК32	ОК7 ОК9 ОК11 ОК12 ОК13 ОК14 ОК16 ОК17 ОК18 ОК19 ОК20 ОК21 ОК22 ОК30 ОК31 ОК32		ОК7 ОК9 ОК11 ОК12 ОК13 ОК14 ОК16 ОК17 ОК18 ОК19 ОК20 ОК21 ОК22 ОК30 ОК31 ОК32					ОК7 ОК9 ОК11 ОК12 ОК13 ОК14 ОК16 ОК17 ОК18 ОК19 ОК20 ОК21 ОК22 ОК30 ОК31 ОК32		
РН 48 – виконувати впровадження та підтримку систем виявлення вторгнень та використовувати компоненти криптографічного захисту												ОК7 ОК9 ОК12 ОК13 ОК14 ОК15	ОК7 ОК9 ОК12 ОК13 ОК14 ОК15		ОК7 ОК9 ОК12 ОК13 ОК14 ОК15		ОК7 ОК9 ОК12 ОК13 ОК14 ОК15	ОК7 ОК9 ОК12 ОК13 ОК14 ОК15	

Результати навчання	Компетентності																		
	Загальні							Спеціальні (фахові)											
	КЗ 1	КЗ 2	КЗ 3	КЗ 4	КЗ 5	КЗ 6	КЗ 7	КФ 1	КФ 2	КФ 3	КФ 4	КФ 5	КФ 6	КФ 7	КФ 8	КФ 9	КФ 10	КФ 11	КФ 12
для забезпечення необхідного рівня захищеності інформації в інформаційно-телекомунікаційних системах												ОК16 ОК17 ОК20 ОК21 ОК22 ОК30 ОК31 ОК32	ОК16 ОК17 ОК20 ОК21 ОК22 ОК30 ОК31 ОК32		ОК16 ОК17 ОК20 ОК21 ОК22 ОК30 ОК31 ОК32		ОК16 ОК17 ОК20 ОК21 ОК22 ОК30 ОК31 ОК32	ОК16 ОК17 ОК20 ОК21 ОК22 ОК30 ОК31 ОК32	
РН 49 – забезпечувати належне функціонування системи моніторингу інформаційних ресурсів і процесів в інформаційно-телекомунікаційних системах												ОК7 ОК9 ОК12 ОК13 ОК14 ОК15 ОК16 ОК17 ОК20 ОК21 ОК22 ОК32	ОК7 ОК9 ОК12 ОК13 ОК14 ОК15 ОК16 ОК17 ОК20 ОК21 ОК22 ОК32		ОК7 ОК9 ОК12 ОК13 ОК14 ОК15 ОК16 ОК17 ОК20 ОК21 ОК22 ОК32			ОК7 ОК9 ОК12 ОК13 ОК14 ОК15 ОК16 ОК17 ОК20 ОК21 ОК22 ОК32	
РН 50 – забезпечувати) функціонування програмних та програмно-апаратних комплексів виявлення вторгнень різних рівнів та класів (статистичних, сигнатурних, статистично-сигнатурних)										ОК7 ОК9 ОК12 ОК13 ОК14 ОК16 ОК18 ОК19 ОК20 ОК22 ОК32		ОК7 ОК9 ОК12 ОК13 ОК14 ОК16 ОК18 ОК19 ОК20 ОК22 ОК32			ОК7 ОК9 ОК12 ОК13 ОК14 ОК16 ОК18 ОК19 ОК20 ОК22 ОК32			ОК7 ОК9 ОК12 ОК13 ОК14 ОК16 ОК18 ОК19 ОК20 ОК22 ОК32	
РН 51 – підтримувати працездатність та забезпечувати конфігурування систем виявлення вторгнень в інформаційно-телекомунікаційних системах												ОК7 ОК9 ОК12 ОК13 ОК16 ОК20 ОК32			ОК7 ОК9 ОК12 ОК13 ОК16 ОК20 ОК32			ОК7 ОК9 ОК12 ОК13 ОК16 ОК20 ОК32	

Результати навчання	Компетентності																		
	Загальні							Спеціальні (фахові)											
	КЗ 1	КЗ 2	КЗ 3	КЗ 4	КЗ 5	КЗ 6	КЗ 7	КФ 1	КФ 2	КФ 3	КФ 4	КФ 5	КФ 6	КФ 7	КФ 8	КФ 9	КФ 10	КФ 11	КФ 12
РН 52 – використовувати інструментарій для моніторингу процесів в інформаційно-телекомунікаційних системах												ОК7 ОК9 ОК12 ОК13 ОК14 ОК15 ОК16 ОК17 ОК20 ОК21 ОК22 ОК32	ОК7 ОК9 ОК12 ОК13 ОК14 ОК15 ОК16 ОК17 ОК20 ОК21 ОК22 ОК32		ОК7 ОК9 ОК12 ОК13 ОК14 ОК15 ОК16 ОК17 ОК20 ОК21 ОК22 ОК32			ОК7 ОК9 ОК12 ОК13 ОК14 ОК15 ОК16 ОК17 ОК20 ОК21 ОК22 ОК32	
РН 53 – вирішувати задачі аналізу програмного коду на наявність можливих загроз	ОК1 ОК4 ОК5 ОК6 ОК7 ОК9 ОК10 ОК11 ОК12 ОК13 ОК14 ОК15 ОК16 ОК17 ОК18 ОК19 ОК20 ОК21 ОК22 ОК23 ОК24 ОК25 ОК27 ОК29 ОК31 ОК32			ОК1 ОК4 ОК5 ОК6 ОК7 ОК9 ОК10 ОК11 ОК12 ОК13 ОК14 ОК15 ОК16 ОК17 ОК18 ОК19 ОК20 ОК21 ОК22 ОК23 ОК24 ОК25 ОК27 ОК29 ОК31 ОК32					ОК1 ОК4 ОК5 ОК6 ОК7 ОК9 ОК10 ОК11 ОК12 ОК13 ОК14 ОК15 ОК16 ОК17 ОК18 ОК19 ОК20 ОК21 ОК22 ОК23 ОК24 ОК25 ОК27 ОК29 ОК31 ОК32	ОК1 ОК4 ОК5 ОК6 ОК7 ОК9 ОК10 ОК11 ОК12 ОК13 ОК14 ОК15 ОК16 ОК17 ОК18 ОК19 ОК20 ОК21 ОК22 ОК23 ОК24 ОК25 ОК27 ОК29 ОК31 ОК32	ОК1 ОК4 ОК5 ОК6 ОК7 ОК9 ОК10 ОК11 ОК12 ОК13 ОК14 ОК15 ОК16 ОК17 ОК18 ОК19 ОК20 ОК21 ОК22 ОК23 ОК24 ОК25 ОК27 ОК29 ОК31 ОК32	ОК1 ОК4 ОК5 ОК6 ОК7 ОК9 ОК10 ОК11 ОК12 ОК13 ОК14 ОК15 ОК16 ОК17 ОК18 ОК19 ОК20 ОК21 ОК22 ОК23 ОК24 ОК25 ОК27 ОК29 ОК31 ОК32	ОК1 ОК4 ОК5 ОК6 ОК7 ОК9 ОК10 ОК11 ОК12 ОК13 ОК14 ОК15 ОК16 ОК17 ОК18 ОК19 ОК20 ОК21 ОК22 ОК23 ОК24 ОК25 ОК27 ОК29 ОК31 ОК32		ОК1 ОК4 ОК5 ОК6 ОК7 ОК9 ОК10 ОК11 ОК12 ОК13 ОК14 ОК15 ОК16 ОК17 ОК18 ОК19 ОК20 ОК21 ОК22 ОК23 ОК24 ОК25 ОК27 ОК29 ОК31 ОК32			ОК1 ОК4 ОК5 ОК6 ОК7 ОК9 ОК10 ОК11 ОК12 ОК13 ОК14 ОК15 ОК16 ОК17 ОК18 ОК19 ОК20 ОК21 ОК22 ОК23 ОК24 ОК25 ОК27 ОК29 ОК31 ОК32	ОК1 ОК4 ОК5 ОК6 ОК7 ОК9 ОК10 ОК11 ОК12 ОК13 ОК14 ОК15 ОК16 ОК17 ОК18 ОК19 ОК20 ОК21 ОК22 ОК23 ОК24 ОК25 ОК27 ОК29 ОК31 ОК32
РН 54 – усвідомлювати цінності громадянського	ОК1 ОК3	ОК1 ОК3				ОК1 ОК3	ОК1 ОК3												

Результати навчання	Компетентності																	
	Загальні							Спеціальні (фахові)										
	КЗ 1	КЗ 2	КЗ 3	КЗ 4	КЗ 5	КЗ 6	КЗ 7	КФ 1	КФ 2	КФ 3	КФ 4	КФ 5	КФ 6	КФ 7	КФ 8	КФ 9	КФ 10	КФ 11	КФ 12
(вільного демократичного) суспільства та необхідність його сталого розвитку, верховенства права, прав і свобод людини і громадянина в Україні	ОК4 ОК5 ОК6 ОК7 ОК12 ОК16 ОК18 ОК21 ОК22 ОК24 ОК25 ОК27 ОК29 ОК30 ОК31 ОК32	ОК4 ОК5 ОК6 ОК7 ОК12 ОК16 ОК18 ОК21 ОК22 ОК24 ОК25 ОК27 ОК29 ОК30 ОК31 ОК32				ОК4 ОК5 ОК6 ОК7 ОК12 ОК16 ОК18 ОК21 ОК22 ОК24 ОК25 ОК27 ОК29 ОКЗО ОК31 ОК32	ОК4 ОК5 ОК6 ОК7 ОК12 ОК16 ОК18 ОК21 ОК22 ОК24 ОК25 ОК27 ОК29 ОКЗО ОК31 ОК32												

Гарант ОП *підписано* **Вячеслав ЛИМАРЕНКО**

ЛИСТ ПОГОДЖЕННЯ
освітньої програми «КІБЕРБЕЗПЕКА»

Назва структурного / функціонального підрозділу / посадова особа	**Дата, підпис**
1. Навчальний відділ	
2. Керівник відділу забезпечення якості освіти та інноваційного розвитку	
3. Завідувач кафедри кібербезпеки та інформаційних технологій	
4. Проректор з навчально-методичної роботи	

Громадська спілка "Харківський
кластер інформаційних технологій"
вул.Громадянська 11/13,
м.Харків, 61057 Україна
+38 (050) 658-88-46
olga.shapoval@it-kharkiv.com
www.it-kharkiv.com

Вих.№30/09-01
від 30.09.2020

РЕЦЕНЗІЯ-ВІДГУК

на освітньо-професійну програму «Кібербезпека»,
підготовлену кафедрою кібербезпеки та інформаційних технологій
Харківського національного економічного університету
імені Семена Кузнеця

Кібербезпека розглядає захист функціонування нової сутності – кіберпростору, середовища, що виникло в результаті взаємодії людей, програмного забезпечення, Інтернет сервісів з використанням технічних пристроїв і мережевих зв'язків.

Якщо раніше проблема безпеки в кіберпросторі стосувалася тільки окремих компаній, то з розвитком Інтернет і мобільного банкінгу, Інтернету речей та багатьох інших сучасних технологій – безпека в кіберпросторі стосується кожного з нас. Фахівці з кібербезпеки забезпечують захист життєво важливих інтересів людини і суспільства, своєчасне виявлення, запобігання і нейтралізацію реальних та потенційних загроз у сфері функціонування інформаційних, комп'ютерних та кіберфізичних систем.

Підготовка якісних спеціалістів у сфері захисту інформації (кіберпезпеки) є одним з найбільших викликів сьогодення через необхідність постійного оновлення змісту освіти. Освітня програма «Кібербезпека» сформована кафедрою кібербезпеки та інформаційних технологій Харківського національного економічного університету ім. С. Кузнеця, відповідно до останніх тенденцій розвитку спеціальності та повністю реалізує результати навчання передбачені стандартом вищої освіти за спеціальністю 125 Кібербезпека. Програма має чітко визначені цілі, які враховують основні її особливості - підготовки фахівця з інформаційної безпеки широкого профілю із знанням технологій програмування.

Однією з основних проблем реалізації освітнього процесу за спеціальністю 125 Кібербезпека є відсутність під час навчання можливості отримати знання та навички від професіоналів-практиків. В рамках викладання за освітньою програмою, що рецензується, залучено викладачів -практиків.

Вважаємо, що Освітньо-професійна програма «Кібербезпека», що складена та запропонована кафедрою кібербезпеки та інформаційних технологій Харківського національного економічного університету ім. С. Кузнеця, має всі необхідні компоненти для підготовки кваліфікованих фахівців які будуть впроваджені на ринку праці.

Громадська спілка
"Харківський кластер
інформаційних технологій"
Виконавчий директор

Шаповал О.С.

РЕЦЕНЗІЯ-ВІДГУК

на освітньо-професійну програму "Кібербезпека" першого (бакалаврського) рівня вищої освіти, яка підготовлена кафедрою кібербезпеки та інформаційних технологій Харківського національного економічного університету імені Семена Кузнеця

З урахуванням бурхливого розвитку та обчислювальних потужностей обчислювальної техніки актуальним завданням є захист життєво важливих інтересів людини і громадянина, суспільства та держави під час використання кіберпростору. У цих умовах фахівці з кібербезпеки повинні забезпечувати своєчасне виявлення, запобігання і нейтралізація реальних і потенційних загроз національній безпеці України у кіберпросторі. У зв'язку із складністю і трудомісткістю бізнес-процесів і методів захисту цифрового обладнання, інформації та комп'ютерних систем від ненавмисного чи несанкціонованого доступу вразливості комп'ютерних та інформаційних систем становлять значну проблему для користувачів, підприємств.

Підготовка якісних спеціалістів у сфері захисту інформації та кібербезпеки повинна відбуватися у відповідно до поступового трансформування навчальних програм та навчальних планів дисциплін пов'язаних з напрямком "Кібербезпека", що сформована кафедрою кібербезпеки та інформаційних технологій Харківського національного економічного університету ім. С. Кузнеця, відповідно до останніх тенденцій розвитку спеціальності, повністю реалізує результати навчання передбачені стандартом вищої освіти за спеціальністю 125 Кібербезпека. Програма має чітко визначені цілі, які враховують основні її особливості – підготовки фахівця з інформаційної безпеки широкого профілю із знанням технологій автоматизації бізнес-процесів, економічних завдань та повсякденної операційної діяльності підприємств з урахуванням технологічних можливостей держави, потреб бізнес-спільноти України та перспектив розвитку цифрової трансформації на державному рівні.

Сучасним трендом розвитку технологій розробки програмних продуктів є рішення, які надають можливість вирішувати завдання проєктування, програмування, налагодження, розгортання, супроводження, кібербезпеки, зберігання даних, організацію хмарних сервісів з мінімумом кодування. Однією з основних проблем реалізації освітнього процесу за спеціальністю

125 Кібербезпека є відсутність під час навчання можливості отримати знання та навички від професіоналів-практиків. В рамках викладання за освітньою програмою, що рецензується, залучено викладачів -практиків та вивчаються сучасні технології створення та керування безпекою у розгалужених хмарних вебдодатків для підтримання безперебійних бізнес-процесів, вчасного проведення фінансових операцій, прогнозування ланцюжків постачання сировини, надсилання готової продукції, та надання послуг клієнтам, партнерам.

Вважаємо, що Освітньо-професійна програма "Кібербезпека" першого (бакалаврського) рівня освіти, що складена та запропонована кафедрою кібербезпеки та інформаційних технологій Харківського національного економічного університету ім. С. Кузнеця, має всі необхідні компоненти для підготовки кваліфікованих фахівців, та забезпечує надбання ними відповідних компетенцій та спроможностей щодо вирішення актуальних завдань забезпечення безпеки автоматизації бізнес-процесів, економічних завдань, питань повсякденної операційної діяльності підприємств з урахуванням технологічних можливостей держави, потреб бізнес-спільноти України та перспектив розвитку технологій на державному рівні для успішного впровадження на ринку праці.

Консультант з інжинірингу
з напряму кібербезпеки,
ТОВ «ГлобалЛоджик Україна»

13.01.2021 _____ Олександр Адамов

Виконавчий директор
ГС «ХАРКІВСЬКИЙ КЛАСТЕР
ІНФОРМАЦІЙНИХ
ТЕХНОЛОГІЙ»

13.01.2021 _____ О.С. Шаповал

УКРАЇНА
ГРОМАДСЬКА СПІЛКА
"ХАРКІВСЬКИЙ КЛАСТЕР ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ"
№39887790
місто Харків

РЕЦЕНЗІЯ-ВІДГУК

на освітньо-професійну програму «Кібербезпека»,
підготовлену кафедрою кібербезпеки та інформаційних технологій
Харківського національного економічного університету
імені Семена Кузнеця

Сучасний стан розвитку інформаційного оточення яке охоплює майже усі сфери життєдіяльності людини і громадянина, суспільства та держави характеризується бурхливим збільшенням об'єму інформаційних потоків у віртуальному просторі, хмарних технологій збереження обчислення величезних об'ємів даних. Також суттєво зростає рівень контактних комунікації, які потребують верифікації, що є актуальним завданням щодо запобігання і нейтралізації реальних і потенційних загроз у кіберпросторі. Перспективнім напрямом теоретичної концепції та принципів використання блокчейн-технологій є криптовалюти, які зараз поширюють свій оберт у світовій фінансовій системі з капіталізацією понад декілька мільярдів долларів. Використання технології блокчейн дозволяє вирішувати питання забезпечення необхідного рівня кібербезпеки при заключенні контрактів у банківському секторі, інформаційного захисту користувачів у високотехнологічних системах хмарних мереж.

Кафедрою Харківського національного економічного університету ім. С. Кузнеця, відповідно до останніх тенденцій розвитку блокчейн-технологій розроблена навчальна програма «Кібербезпека», та навчальні плани дисциплін пов'язаних з напрямком "Блокчейн-технології" та повністю реалізує результати навчання передбачені стандартом вищої освіти за спеціальністю 125 Кібербезпека.

Програма враховують основні її особливості та має чітко визначені цілі - підготовки фахівця здатного забезпечити необхідний рівень кібербезпеки розгалуженої IT інфраструктури у високотехнологічних системах хмарних мереж за технологією блокчейн. Програма надає можливість майбутнім фахівцям здійснити освоєння принципів застосування криптографічних методів у блокчейн технологіях; надбати знання основних принципів криптовалют; вивчити основні обмеження та ризики створення та використання криптовалют; ознайомитись з методологічними основами розробки та функціонування блокчейн платформ. Студенти після проходження навчання за навчальною програмою «Кібербезпека» спроможного здійснювати аналіз, проектування та розробку систем, технологій і засобів інформаційної безпеки з використанням

криптографічних методів блокчейн-технологій у відповідності до законодавчої та нормативно-правової бази та вимог відповідних національних і міжнародних, стандартів й практик щодо здійснення професійної діяльності.

З метою формування практичних та науково-дослідницьких складових компетентностей на кафедрі кібербезпеки та інформаційних технологій розгорнуті Кіберполігон та Лабораторія блокчейн, яка дозволяє відтворити та відпрацювати навчальні питання забезпечення відповідного рівня кібербезпеки на практиці у режимі реального часу.

В рамках викладання за освітньою програмою, що рецензується, залучено спеціалістів-практиків від стейкхолдерів за напрямком блокчейн-технологій.

Вважаємо, що Освітньо-професійна програма «Кібербезпека», що складена та запропонована кафедрою кібербезпеки та інформаційних технологій Харківського національного економічного університету ім. С. Кузнеця, має всі необхідні компоненти для підготовки кваліфікованих фахівців, щодо забезпечення необхідного рівня кібербезпеки розгалуженої IT інфраструктури у високотехнологічних системах хмарних мереж за технологією блокчейн, спроможних здійснювати аналіз, проектування та розробку систем, технологій і засобів інформаційної безпеки, освоєння ними принципів застосування криптографічних методів у блокчейн технологіях та основних принципів криптовалют з урахуванням обмежень та ризиків створення та використання криптовалют у відповідності до методологічних основ розробки та функціонування блокчейн платформ, у межах законодавчої та нормативно-правової бази та вимог відповідних національних і міжнародних, стандартів щодо здійснення професійної діяльності для успішного впровадження на ринку праці.

Представник компанії Distributed Lab
Анастасія Сапожкова,
Блокчейн дослідник в Distributed Lab

САЙФЕР
Системи захисту інформації

ТОВ «САЙФЕР ІТ»
Адреса: 04107, Київ, вул. Нагірна, 25-27
Тел./Факс: (044) 484-46-17, 484-46-12, 483-03-22
E-mail: info@cipher.com.ua
http://www.cipher.com.ua

№ 05/20 від 25.09.2020 р.

РЕЦЕНЗІЯ-ВІДГУК

на освітньо-професійну програму «Кібербезпека»,

підготовлену кафедрою кібербезпеки та інформаційних технологій
Харківського національного економічного університету

імені Семена Кузнеця

Розвиток інформаційних і телекомунікаційних технологій призводить до проникнення їх проникнення у всі сфери діяльності людства. Збільшення обсягів даних їх інтенсивності і критичності призводить до необхідності захисту таких інформаційних потоків і ресурсів. Задачі захисту інформації і інформаційних ресурсів вирішуються в межах кібернетичної безпеки інформації (далі – кібербезпека).

Кібербезпека на сьогодні є спеціальністю, яка включає в себе декілька великих напрямів: підготовки (побудова архітектури безпеки, управління ризиками, використання промислових і індустріальних стандартів та методик, криптологія, технічний захист інформації тощо).

Таким чином підготовка фахівців з кібербезпеки за освітньо-професійною програмою «Кібербезпека» є актуальним напрямом освітньої діяльності.

Схема підготовки фахівців за освітньо-професійною програмою, що акредитується, є правильно побудованою: врахована необхідність отримання студентами знань з дисциплін професійного змісту, які повністю покривають результати навчання, що передбачені стандартом вищої освіти зі спеціальності 125 Кібербезпека.

В рамках освітньо-професійної програми, «Кібербезпека» складеною кафедрою кібербезпеки та інформаційних технологій Харківського національного економічного університету ім. С. Кузнеця, автори змогли досить органічно та логічно сформулювати схему підготовки майбутнього спеціаліста, яка, з одного боку, дозволяє освітній програмі забезпечувати реалізацію результатів навчання передбачених стандартом вищої освіти в повному обсязі, а, з іншого боку, завдяки акценту на технологіях програмування випускники мають можливість працевлаштовуватися не тільки за спеціальністю, але і в сфері інформаційних технологій.

Освітня програма «Кібербезпека» складена кафедрою кібербезпеки та інформаційних технологій Харківського національного економічного університету ім. С. Кузнеця, має всі необхідні компоненти для підготовки кваліфікованих спеціалістів, які будуть затребувані на ринку праці як за спеціальністю так і в цілому на ринку.

Директор ТОВ «САЙФЕР ІТ» В.Ю.Ковтун

САЙФЕР

Системи захисту інформації

ТОВ «САЙФЕР ІТ»
Адреса: 04107, Київ, вул. Нагірна, 25
Тел./Факс: (044) 484-46-17, 484-46-12, 483-03-22
E-mail: info@cipher.com.ua
https://cipher.com.ua

Вих. № 17/20 від 16.11.2020 року

Харківського національного
економічного університету
імені Семена Кузнеця
61166, Харків, просп. Науки, 9А

РЕЦЕНЗІЯ-ВІДГУК
на освітньо-професійну програму «Кібербезпека»,
підготовлену кафедрою кібербезпеки та інформаційних технологій
Харківського національного економічного університету
імені Семена Кузнеця

Стрімкий розвиток інформаційних технологій і швидке зростання глобальної мережі Інтернет призвели до формування інформаційного середовища, що впливає на всі сфери людської діяльності. Нові технологічні можливості полегшують поширення інформації, підвищують ефективність виробничих процесів, сприяють розширенню ділових операцій в процесі бізнесу.

Підприємства нового типу - це розгалужена мережа розподілених підрозділів, філій і груп, що взаємодіють один з одним. Розподілені корпоративні інформаційні системи стають сьогодні найважливішим засобом виробництва сучасної компанії, вони дозволяють перетворити традиційні форми бізнесу в електронний бізнес.

Електронний бізнес використовує глобальну мережу Інтернет і сучасні інформаційні технології для підвищення ефективності всіх сторін ділових відносин, включаючи продажі, маркетинг, платежі, фінансовий аналіз, пошук співробітників, підтримку клієнтів і партнерських відносин.

Однією з умов існування електронного бізнесу є інформаційна безпека, під якою розуміється захищеність інформації та підтримує інфраструктури від випадкових і навмисних впливів, здатних завдати шкоди власникам або користувачам інформації. Збиток від порушення інформаційної безпеки може привести до великих фінансових втрат і навіть до повного закриття компанії.

Незважаючи на інтенсивний розвиток комп'ютерних засобів і інформаційних технологій, вразливість сучасних інформаційних систем і комп'ютерних мереж, на жаль, не зменшується. Тому проблеми забезпечення інформаційної безпеки привертають пильну увагу як фахівців в області комп'ютерних систем і мереж, так і численних користувачів, включаючи компанії, що працюють в сфері електронного бізнесу.

Без знання і кваліфікованого застосування сучасних технологій, стандартів, протоколів і засобів захисту інформації неможливо досягти необхідного рівня інформаційної безпеки комп'ютерних систем і мереж.

Кафедрою кібербезпеки та інформаційних технологій Харківського національного економічного університету ім. С. Кузнеця розроблено навчальну програму «Кібербезпека», та навчальні плани дисциплін, пов'язаних з напрямком підготовки спеціаліста з інформаційної безпеки широкого профілю, яка формує широкий спектр компетентностей та забезпечує отримання результатів навчання, які передбачаються стандартом вищої освіти за спеціальністю 125 Кібербезпека.

Програма забезпечує підготовку спеціаліста, який здатен забезпечити необхідний рівень кібербезпеки систем різного призначення та природи, в першу чергу системи бізнес-процесів економічних систем, систем критичної інфраструктури, кібер-фізичних систем та інших, на будь якому рівні управлінської ієрархії, враховуючи принципи застосування криптографічних методів, сучасних технологій забезпечення кібербезпеки, інформаційної безпеки та безпеки інформації в межах національних і міжнародних стандартів й практик щодо здійснення професійної діяльності.

Навчальний процес освітньої програми організовано на базі сучасних інтегрованих середовищах розробки корпоративних додатків та систем збереження даних з санкціонованим доступом. Кожному студенту на період навчання безкоштовно надається ліцензований доступ до додатків та сервісів у аккаунті у порталу Microsoft 365. Більшість лабораторних та практичних робіт, а також курсового та дипломного проектування здійснюється з використанням апаратно-програмних засобів кіберполігону.

Вважаємо, що Освітньо-професійна програма «Кібербезпека», що запропонована та здійснюється кафедрою кібербезпеки та інформаційних технологій Харківського національного економічного університету ім. С. Кузнеця, має всі необхідні компоненти для підготовки кваліфікованих спеціалістів у відповідності до сучасних тенденцій на попит фахівців з кібербезпеки. Випускники цієї програми отримують всі необхідні знання та навички щодо забезпечення кібербезпеки економічної діяльності підприємств корпоративного рівня, спроможні здійснювати аналіз, проектування, програмування, розгортання та супроводження будь-яких сервісів, використовуючи сучасні технології.

Навчання за Освітньо-професійною програмою «Кібербезпека», забезпечує студентам надбання необхідних знать, компетенцій та навичок для успішної професійної діяльності у сфері впровадження та підтримки програмних рішень у корпоративному середовищі при дотриманні вимог відповідних національних і міжнародних, стандартів.

Директор ТОВ «Сайфер ІТ» В.Ю. Ковтун