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

УХВАЛЕНО
Рішенням Вченої ради
Харківського національного
економічного університету
імені Семена Кузнеця
від 24.06.2026 р. протокол № 8

ВВЕДЕНО В ДІЮ
Наказом ректора Харківського
національного економічного університету
імені Семена Кузнеця
від 24.06.2026 р. № 197

_____ Тетяна ШТАЛЬ

ОСВІТНЬО-ПРОФЕСІЙНА ПРОГРАМА
«КІБЕРБЕЗПЕКА»

РІВЕНЬ ВИЩОЇ ОСВІТИ	**Перший (бакалаврський)**
СТУПІНЬ ВИЩОЇ ОСВІТИ	**Бакалавр**
ГАЛУЗЬ ЗНАНЬ	**F Інформаційні технології**
СПЕЦІАЛЬНІСТЬ	**F5 Кібербезпека та захист інформації**

Харків, 2026

ПРЕАМБУЛА

Робоча група освітньо-професійної програми «Кібербезпека»:

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

Солодовник Ганна Валеріївна, доцент кафедри кібербезпеки та інформаційних технологій, кандидат технічних наук, доцент.

Тютюник Вадим Володимирович, професор кафедри кібербезпеки та інформаційних технологій, доктор технічних наук, професор

Голубничий Дмитро Юрійович, доцент кафедри інформаційних систем, кандидат технічних наук, доцент

Бойко Софія Олегівна, здобувач вищої освіти.

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

Розглянуто на засіданні кафедри кібербезпеки та інформаційних технологій, протокол № 14 від 13.05.2026 року.

Розглянуто вченою радою навчально-наукового інституту інформаційних технологій, протокол № 11 від 23.06.2026 р.

ОП розроблена/оновлена на підставі:

1. Законодавчих та нормативних актів: Законів України «Про освіту», «Про вищу освіту», Національної рамки кваліфікації, Національного класифікатору України.
2. Стандарту вищої освіти за спеціальністю 125 «Кібербезпека» галузі знань 12 «Інформаційні технології» для першого (бакалаврського) рівня вищої освіти, затвердженого наказом Міністерства освіти і науки України від 29.10.2024 р. № 1547.
3. *На виконання Закону України «Про основи національного спротиву» від 16.07.2021 р. № 1702-IX.
4. Аналізу ринку праці, з урахуванням регіонального контексту.
5. Вивчення вітчизняного та зарубіжного досвіду.
6. Пропозицій роботодавців.
7. Рекомендації після процедур акредитації освітньої програми Національним агентством із забезпечення якості вищої освіти, протокол № 7 (50) від 27 квітня 2021 року.

Рецензії-відгуки зовнішніх стейкхолдерів (додаються).

І. ЗАГАЛЬНА ХАРАКТЕРИСТИКА

Рівень вищої освіти	Перший (бакалаврський) рівень
Ступінь вищої освіти	Бакалавр
Галузі знань	F Інформаційні технології
Спеціальності	F5 Кібербезпека та захист інформації
Спеціалізація	-
Освітня програма	Кібербезпека / Cybersecurity
Форми здобуття освіти, обсяг освітньої програми в кредитах ЄКТС та розрахункові строки виконання освітньої програми	На базі повної загальної середньої освіти: денна форма – 240 кредитів, 3 роки 10 місяців На базі ступеня «молодший бакалавр» (освітньо-кваліфікаційного рівня «молодший спеціаліст»): очна (денна) форма – 240 кредитів, 2 роки 10 місяців.
Наявність акредитації	Сертифікат про акредитацію освітньої програми НАЗЯВО № 18572, дійсний до 31.12.2027 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)	Фахівець сфери захисту інформації (трудові функції А, Б, В, Г) https://register.nqa.gov.ua/uploads/0/439-profesijnij_standart_fahivec_sferi_zahistu_informacii.pdf
Кваліфікація в дипломі	Ступінь вищої освіти Бакалавр Спеціальність F5 Кібербезпека та захист інформації Освітня програма Кібербезпека
Мета освітньої програми	Підготовка фахівців, здатних використовувати і впроваджувати технології інформаційної та/або кібербезпеки, а також технологій цифрової економіки.
Фокус та особливості (унікальність) програми	Особливістю ОПП Кібербезпека є орієнтація на сучасні вимоги до фахівців в галузі інформаційних технологій, та набуття здобувачами вищої освіти конкурентоспроможних компетентностей на основі синергізму отримання результатів навчання з інформаційної та/або кібербезпеки та програмування.
Опис предметної області	**Об’єкти вивчення:** технології кібербезпеки та захисту інформації; процеси управління кібербезпекою та захистом інформації; об'єкти інформаційної діяльності, в тому числі інформаційні та Інформаційно-комунікаційні системи, інформаційні ресурси і технології.

	Цілі навчання: підготовка фахівців, здатних використовувати і впроваджувати технології кібербезпеки та захисту інформації та розв'язувати складні задачі у галузі кібербезпеки та захисту інформації. **Теоретичний зміст предметної області: п**ринципи, концепції, теорії захисту життєво важливих інтересів людини, суспільства, держави під час використання кіберпростору, за якого забезпечуються сталий розвиток інформаційного суспільства та цифрового комунікативного середовища, своєчасне виявлення, запобігання і нейтралізація реальних і потенційних загроз національній безпеці України у кіберпросторі. **Методи, методики та технології:** методи, методики та технології розв'язання теоретичних і практичних задач кібербезпеки та захисту інформації. **Інструменти та обладнання:** засоби, пристрої, мережне устаткування, прикладне та спеціалізоване програмне забезпечення, інформаційні системи та комплекси проектування, моделювання, контролю, моніторингу, зберігання, обробки, відображення та захисту даних (інформаційних потоків), спеціалізований клас (кіберполігон).
Академічна мобільність	-
Академічні права	Мають право на здобуття освіти на другому (магістерському) рівні вищої освіти. Здобуття або вдосконалення освіти та професійної підготовки в системі освіти дорослих.
Професійні права	Право професійної діяльності відповідно до отриманої освітньої та професійної кваліфікації
Працевлаштування випускників	Професії, на підготовку з яких спрямована ОП (згідно з чинною редакцією Національного класифікатора України: Класифікатор професій ДК 003:2010): адміністратор безпеки мереж і систем, 2139.2; фахівець сфери захисту інформації, 2139.2; фахівець з питань безпеки (Інформаційно-комунікаційні технології), 2139.2; конструктор систем кібербезпеки, 2132.2; фахівець з підтримки інфраструктури кіберзахисту, 2139.2; фахівець з реагування на інциденти кібербезпеки, 2139.2; фахівець з криптографічного захисту інформації, 2139.2; фахівець з технічного захисту інформації, 2139.2; фахівець з тестування систем захисту інформації, 2139.2; аудитор інформаційних технологій (з кібербезпеки), 2139.2; фахівець з оцінки заходів захисту інформації (кібербезпеки), 2139.2. А також на посади у структурних підрозділах установ/підприємств/організацій, які передбачають наявність вищої освіти зі спеціальності 125 Кібербезпека та захист інформації
Силабуси освітніх компонентів	https://hneu.edu.ua/informatsijnyj-paket-bakalavr-kiberbezpeka-2026

ІІ – ПЕРЕЛІК КОМПЕТЕНТНОСТЕЙ ВИПУСКНИКА

Інтегральна компетентність	Здатність розв'язувати складні спеціалізовані задачі і практичні завдання у галузі кібербезпеки та захисту інформації.
Загальні компетентності	**ЗК1.** Здатність застосовувати знання у практичних ситуаціях. **ЗК2.** Знання та розуміння предметної області і розуміння професійної діяльності. **ЗК3.** Здатність спілкуватися державною мовою як усно, так і письмово. **ЗК4.** Здатність спілкуватися іноземною мовою. **ЗК5.** Здатність вчитися і оволодівати сучасними знаннями. **ЗК6.** Здатність реалізувати свої права і обов'язки як члена суспільства, усвідомлювати цінності громадянського (вільного демократичного) суспільства та необхідність його сталого розвитку, верховенства права, прав та свобод людини і громадянина в Україні. **ЗК7.** Здатність ухвалювати рішення й діяти дотримуючись принципу неприпустимості корупції та будь-яких інших проявів недоброчесності. **ЗК8.** Здатність зберігати та примножувати моральні, культурні, наукові цінності і досягнення суспільства на основі розуміння історії та закономірностей розвитку предметної області, її місця у загальній системі знань про природу і суспільство та у розвитку суспільства, техніки і технологій, використовувати різні види та форми рухової активності для активного відпочинку та ведення здорового способу життя. **ЗК15.** Здатність виконувати конституційний обов'язок щодо захисту Вітчизни, незалежності та територіальної цілісності України.
Спеціальні (фахові, предметні) компетентності	**СК1.** Здатність застосовувати законодавчу та нормативно-правову базу, а також державні і міжнародні вимоги, практики і стандарти у професійній діяльності. **СК2.** Здатність використовувати інформаційні технології, сучасні методи і моделі кібербезпеки та системи захисту інформації. **СК3.** Здатність забезпечувати неперервність бізнес-процесів згідно встановленої політики кібербезпеки та захисту інформації. **СК4.** Здатність забезпечувати захист Інформації в інформаційних та інформаційно-комунікаційних системах згідно встановленої політики кібербезпеки й захисту інформації. **СК5.** Здатність відновлювати функціонування Інформаційних та інформаційно-комунікаційних систем після реалізації загроз, здійснення кібератак, збоїв і відмов різних класів та походження. **СК6.** Здатність впроваджувати та забезпечувати функціонування комплексних систем захисту інформації (комплекси нормативно-правових, організаційних та технічних засобів і методів, процедур, практичних прийомів тощо). **СК7.** Здатність здійснювати професійну діяльність на основі

	впровадженої системи управління інформаційною та кібербезпекою. **СК8.** Здатність застосовувати методи та засоби криптографічного захисту інформації на об'єктах інформаційної діяльності. **СК9.** Здатність застосовувати методи та засоби технічного захисту Інформації на об'єктах інформаційної діяльності. **СК10.** Здатність виконувати моніторинг інформаційних процесів, аналізувати, виявляти, оцінювати можливі вразливості та загрози інформаційному простору й інформаційним ресурсам згідно з встановленою політикою інформаційної безпеки.

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

ІІІ – НОРМАТИВНИЙ ЗМІСТ ПІДГОТОВКИ ЗДОБУВАЧІВ ВИЩОЇ ОСВІТИ, СФОРМУЛЬОВАНИЙ У ТЕРМІНАХ РЕЗУЛЬТАТІВ НАВЧАННЯ ЗА СПЕЦІАЛЬНІСТЮ F5 КІБЕРБЕЗПЕКА ТА ЗАХИСТ ІНФОРМАЦІЇ ОПП «КІБЕРБЕЗПЕКА»

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

РН21. Виконувати впровадження, підтримку, аналіз ефективності систем виявлення несанкціонованого доступу, дій з інформацією в інформаційній системі, вразливостей, можливих загроз інформаційному

простору й інформаційним ресурсам та використовувати комплекси захисту для забезпечення необхідного рівня захищеності інформації в інформаційних системах.

РН22. Формування національно-патріотичної свідомості, громадянської стійкості щодо захисту Вітчизни, незалежності та територіальної цілісності України.

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)	8	Залік, Екзамен
ОК 3	Історія української культури	4	Залік
ОК 4	Філософія	5	Екзамен
ОК 5	Основи здорового способу життя, безпека життєдіяльності та охорона праці	3	Залік
ОК 27	Основи національного спротиву (формування національного патріотизму)*	5	Залік
ВИБІРКОВІ ОСВІТНІ КОМПОНЕНТИ			
ВК 1	Навчальна дисципліна правового спрямування	5	Залік
ВК 2	Майнор або вільний майнор	5	Залік
ВК 3	Майнор або вільний майнор	5	Залік
ВК 4	Майнор або вільний майнор	5	Залік
ВК 5	Майнор або вільний майнор	5	Залік
ЦИКЛ ПРОФЕСІЙНОЇ ПІДГОТОВКИ			
ОБОВ'ЯЗКОВІ ОСВІТНІ КОМПОНЕНТИ			
ОК 6	Вступ до фаху	6	Залік
ОК 7	Основи алгоритмізації	6	Екзамен
ОК 8	Вища математика	15	Залік, екзамен
ОК 9	Програмування	10	Екзамен, екзамен
ОК 10	Дискретна математика	5	Залік
ОК 11	Математичні основи криптології	4	Залік

ОК 12	Основи побудови та захисту сучасних операційних систем	5	Екзамен
ОК 13	Введення в мережі	5	Екзамен
ОК 14	Технології програмування	12	Залік, Екзамен
ОК 15	Основи криптографічного захисту	5	Екзамен
ОК 16	Основи побудови та захисту мікропроцесорних систем	4	Залік
ОК 17	Організаційне забезпечення захисту інформації	5	Екзамен
ОК 18	Основи математичного моделювання	4	Залік
ОК 19	Розробка захищених мобільних застосунків	4	Залік
ОК 20	Курсова робота: розробка захищених мобільних застосунків	1	Курсова робота
ОК 21	Безпека в інформаційно-комунікаційних системах	5	Екзамен
ОК 22	Інформаційні системи та інтернет технології	12	Екзамен, екзамен
ОК 23	Безпека інтернет-речей	6	Екзамен
ОК 24	Виробнича практика	3	Звіт
ОК 25	Розробка захищених клієнт-серверних застосунків	4	Залік
ОК 26	Курсова робота: розробка захищених клієнт-серверних застосунків	1	Курсова робота
ОК 28	Комплексний курсовий проєкт	2	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	Кваліфікаційна робота	9	Кваліфікаційна робота
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

* ОСНОВИ НАЦІОНАЛЬНОГО СПРОТИВУ - обов’язково для громадяни України, які навчаються за денною або дуальною формою здобуття освіти; ФОРМУВАННЯ НАЦІОНАЛЬНОГО ПАТРІОТИЗМУ - обов’язково для іноземних громадян денної форми навчання, та всіх, хто навчаються за заочною формою здобуття освіти.

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.

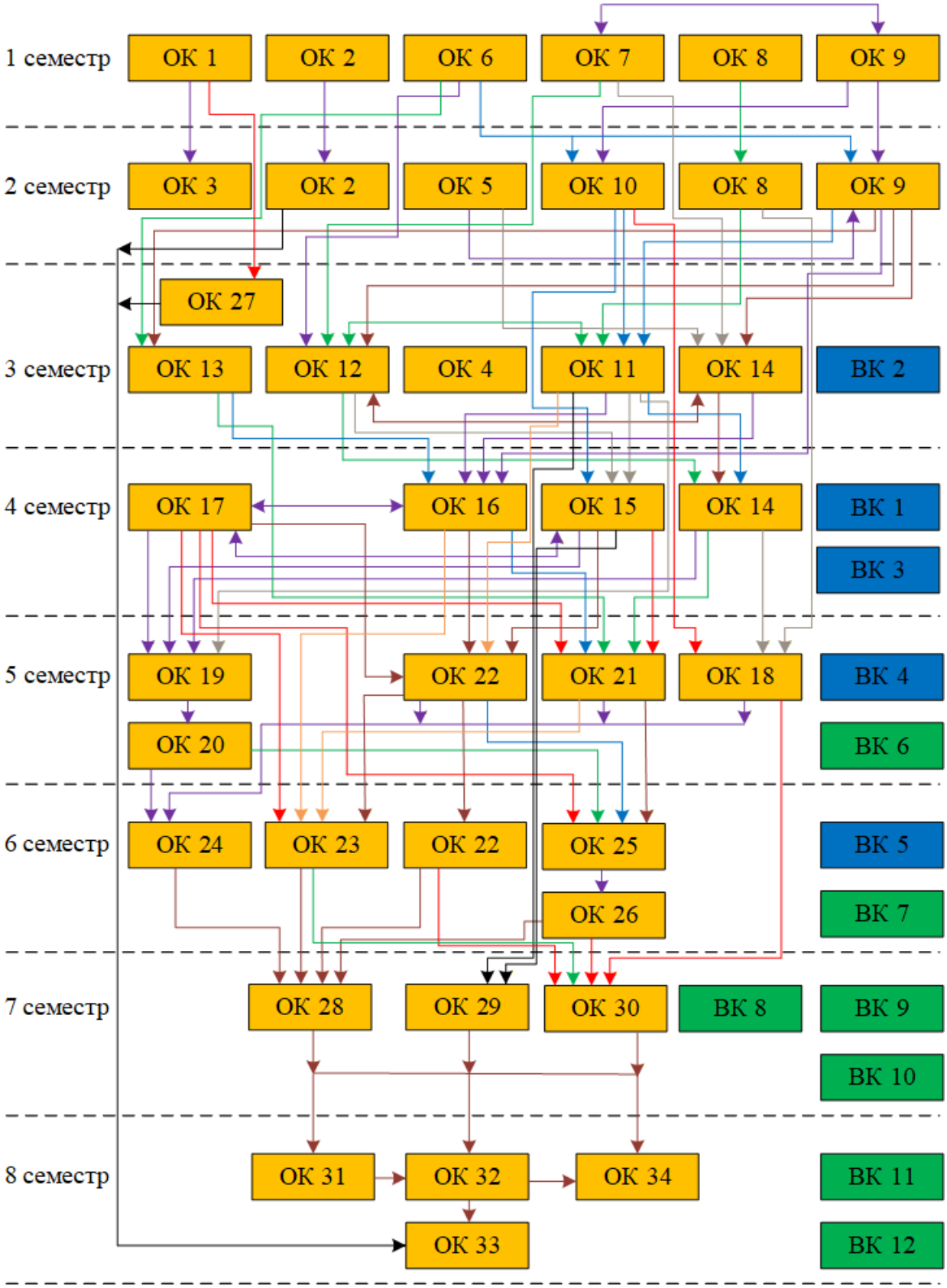
Здобувачеві вищої освіти пропонується обирати 1 дисципліну правового спрямування. Обсяг кожної вибіркової навчальної дисципліни за спрямуванням – 5 кредитів ЄКТС.

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



V. ФОРМИ АТЕСТАЦІЇ ЗДОБУВАЧІВ ВИЩОЇ ОСВІТИ

Форми атестації здобувачів вищої освіти	Атестація здійснюється у формі публічного захисту кваліфікаційної роботи та єдиного державного кваліфікаційного іспиту. Атестація здійснюється екзаменаційною комісією відповідно до вимог стандарту вищої освіти після виконання здобувачем вищої освіти навчального плану у формі публічного захисту кваліфікаційної роботи бакалавра за спеціальністю F5 Кібербезпека та захист інформації. До атестації допускаються здобувачі вищої освіти, які виконали всі вимоги освітньої програми та навчального плану.
Вимоги до кваліфікаційної роботи	ХНЕУ ім. С. Кузнеця розробляє та затверджує: Положення про атестацію здобувачів вищої освіти ХНЕУ ім. С. Кузнеця; Регламент перевірки на унікальність академічних текстів здобувачів вищої освіти та науково-педагогічних працівників ХНЕУ ім. С. Кузнеця навчально-методичним відділом. Кафедрою кібербезпеки та інформаційних технологій затверджуються нормативи унікальності текстів кваліфікаційних робіт. Кваліфікаційна робота має передбачати розв'язання спеціалізованого завдання теоретичного або практичного спрямування в галузі кібербезпеки та захисту інформації проблеми. Кваліфікаційна робота – це навчально-наукова робота здобувача вищої освіти, яка виконується на завершальному етапі здобуття кваліфікації бакалавра для встановлення відповідності отриманих здобувачами вищої освіти результатів навчання (компетентностей) вимогам стандартів вищої освіти. Вона є кваліфікаційним документом, на підставі якого Екзаменаційна комісія визначає рівень теоретичної підготовки випускника, його готовність до самостійної роботи за фахом і приймає рішення щодо присвоєння відповідної кваліфікації та видачі документа про вищу освіту. Атестація осіб, які здобувають ступінь бакалавра, здійснюється ЕК, до складу якої можуть включатися представники роботодавців та їх об'єднань. Атестація здійснюється відкрито і публічно. У кваліфікаційній роботі не повинно бути академічного поагіату, фальсифікації та фабрикації. Кваліфікаційні роботи допущені до захисту на кафедрі мають бути підписані кваліфікованим електронним підписом здобувача вищої освіти, оприлюднені до їх захисту у машинозчитувальному форматі, на постійній основі, з наданням вільного доступу до них без проходження автентифікації та з дотриманням інших вимог, визначених законодавством, зокрема положенням про Національний репозитарій академічних текстів, затвердженим Кабінетом Міністрів України.
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. Ухвалення екзаменаційною комісією рішення про присудження ступеня бакалавра з кібербезпеки та захисту інформації та видачу диплома бакалавра за результатами атестації здобувача вищої освіти оголошується після оформлення в установленому порядку протоколів засідань екзаменаційної комісії.
Вимоги до єдиного державного кваліфікаційного іспиту	Єдиний державний кваліфікаційний іспит передбачає оцінювання досягнень результатів навчання, визначених стандартом вищої освіти.
Вимоги до присвоєння професійної кваліфікації	Присвоєння професійної кваліфікації відбувається відповідно до Порядку присвоєння / підтвердження професійної кваліфікації кваліфікаційним центром Харківського національного економічного університету імені Семена Кузнеця.

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. Перевірка наукових праць науково-педагогічних працівників Університету та здобувачів вищої освіти здійснюється за допомогою інтернетсервісів на основі відкритих інтернет-ресурсів та системи StrikePlagiarism.com, що діє на підставі Ліцензійного Договору про надання права користування антиплагіатним програмним забезпеченням. Нормативними документами в ХНЕУ ім. С.Кузнеця щодо регламентації є такі документи: 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; Політика використання штучного інтелекту в

	освітньому процесі та наукових дослідженнях. Використання ШІ-інструментів у навчанні та дослідженнях дозволене як допоміжний засіб за умови обов'язкового декларування їх застосування та критичної оцінки отриманих результатів. Неприйнятними є видавання ШІ-контенту за власний рахунок, використання ШІ під час контрольних заходів без дозволу, а також застосування ШІ для маніпуляцій та фальсифікацій. Кваліфікаційні роботи (дипломні роботи / проєкти), підписуються кваліфікованим електронним підписом, оприлюднюються до їх захисту у машинозчитувальному форматі, на постійній основі, з наданням вільного доступу до них без проходження автентифікації та з дотриманням інших вимог.

ПОЯСНЮВАЛЬНА ЗАПИСКА

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

Таблиця 1

Матриця відповідності визначених компетентностей дескрипторам НРК

Класифікація компетентностей за НРК	Знання	Уміння	Комунікація	Автономія та відповідальність
ЗАГАЛЬНІ КОМПЕТЕНТНОСТІ				
ЗК1. Здатність застосовувати знання у практичних ситуаціях.	+	+		
ЗК2. Знання та розуміння предметної області і розуміння професійної діяльності.	+	+	+	
ЗК3. Здатність спілкуватися державною мовою як усно, так і письмово.			+	
ЗК4. Здатність спілкуватися іноземною мовою.			+	+
ЗК5. Здатність вчитися і оволодівати сучасними знаннями.	+	+	+	+
ЗК6. Здатність реалізувати свої права і обов'язки як члена суспільства, усвідомлювати цінності громадянського (вільного демократичного) суспільства та необхідність його сталого розвитку, верховенства права, прав та свобод людини і громадянина в Україні.	+		+	+
ЗК7. Здатність ухвалювати рішення й діяти дотримуючись принципу неприпустимості корупції та будь-яких інших проявів недоброчесності.			+	+
ЗК8. Здатність зберігати та примножувати моральні, культурні, наукові цінності і досягнення суспільства на основі розуміння історії та закономірностей розвитку предметної області, її місця у загальній системі знань про природу і суспільство та у розвитку суспільства, техніки і технологій, використовувати різні види та форми рухової активності для активного відпочинку та ведення здорового способу життя.	+		+	+
ЗК9 Здатність виконувати конституційний обов'язок щодо захисту Вітчизни, незалежності та територіальної цілісності України.	+	+	+	+
СПЕЦІАЛЬНІ (ФАХОВІ) КОМПЕТЕНТНОСТІ				
СК1. Здатність застосовувати законодавчу та нормативно- правову базу, а також державні і міжнародні вимоги, практики і стандарти у професійній діяльності.	+	+	+	
СК2. Здатність використовувати інформаційні технології, сучасні методи і моделі кібербезпеки та системи захисту інформації.	+	+	+	
СК3. Здатність забезпечувати неперервність бізнес-процесів згідно встановленої політики кібербезпеки та захисту інформації.		+		+

СК4. Здатність забезпечувати захист Інформації в інформаційних та інформаційно-комунікаційних системах згідно встановленої політики кібербезпеки й захисту інформації.		+		+
СК5. Здатність відновлювати функціонування Інформаційних та інформаційно-комунікаційних систем після реалізації загроз, здійснення кібератак, збоїв і відмов різних класів та походження.		+	+	+
СК6. Здатність впроваджувати та забезпечувати функціонування комплексних систем захисту інформації (комплекси нормативно-правових, організаційних та технічних засобів і методів, процедур, практичних прийомів тощо).		+	+	+
СК7. Здатність здійснювати професійну діяльність на основі впровадженої системи управління інформаційною та кібербезпекою.		+	+	+
СК8. Здатність застосовувати методи та засоби криптографічного захисту інформації на об’єктах інформаційної діяльності.	+	+		
СК9. Здатність застосовувати методи та засоби технічного захисту Інформації на об’єктах інформаційної діяльності.	+	+		
СК10. Здатність виконувати моніторинг інформаційних процесів, аналізувати, виявляти, оцінювати можливі вразливості та загрози інформаційному простору й інформаційним ресурсам згідно з встановленою політикою інформаційної безпеки.		+	+	+

Таблиця 2

Матриця відповідності визначених результатів навчання, компетентностей та освітніх компонентів

Результати навчання	Компетентності																	
	Загальні									Спеціальні (фахові)								
	ЗК1	ЗК2	ЗК3	ЗК4	ЗК5	ЗК6	ЗК7	ЗК8	ЗК9	СК1	СК2	СК3	СК4	СК5	СК6	СК7	СК8	СК9	СК10
РН1. Вільно спілкуватися державною мовою усно та письмово при виконанні професійних обов'язків.	ОК1 ОК3 ОК4		ОК1 ОК3 ОК4		ОК1 ОК3 ОК4			ОК3 ОК5		ОК3 ОК5									
РН2. Спілкуватися іноземною мовою з метою забезпечення ефективності професійної комунікації.		ОК2 ОК27		ОК2 ОК27				ОК2 ОК27		ОК2 ОК27									
РН3. Застосовувати принцип неприпустимості корупції та будь-яких інших проявів недоброчесності у професійній діяльності.						ОК6 ОК17 ОК21 ОК23 ОК28	ОК6 ОК17 ОК21 ОК23 ОК28			ОК6 ОК17 ОК21 ОК23 ОК28									
РН4. Організовувати власну професійну діяльність, обирати і використовувати оптимальні методи та способи розв'язання складних спеціалізованих задач і практичних проблем у професійній діяльності, оцінювати їхню ефективність.	ОК5 ОК12 ОК13 ОК16 ОК19 ОК20 ОК25 ОК26	ОК5 ОК6 ОК12 ОК13 ОК25 ОК26			ОК25 ОК26					ОК5 ОК21	ОК12 ОК13 ОК25 ОК26								
РН5. Аналізувати, аргументувати, приймати рішення при розв'язанні складних спеціалізованих задач і практичних завдань у професійній діяльності, які характеризуються комплексністю та неповною визначеністю умов, відповідати за прийняті рішення.					ОК7 ОК9 ОК30						ОК9 ОК30		ОК9 ОК15 ОК17		ОК7 ОК1 ОК21				ОК14 ОК30
РН6. Адаптуватися до нових умов і технологій професійної діяльності, прогнозувати кінцевий результат.		ОК21 ОК22			ОК17 ОК30						ОК22 ОК30		ОК21 ОК22	ОК21 ОК22	ОК21 ОК22	ОК21 ОК22		ОК21 ОК22	
РН7. Застосовувати й адаптувати теорії інформації та кодування, математичної статистики, чисел, криптографії та стеганографії, оброблення і передачі сигналів тощо, принципи, методи, поняття кібербезпеки та захисту інформації у навчанні та професійній діяльності.					ОК8 ОК10						ОК16 ОК29	ОК16 ОК29			ОК16 ОК29	ОК7 ОК10 ОК11	ОК8 ОК10 ОК11 ОК29		
РН8. Застосовувати знання й розуміння математики та фізики в професійній діяльності, формалізувати задачі предметної галузі кібербезпеки та захисту					ОК8 ОК10						ОК18 ОК29				ОК8 ОК10		ОК8 ОК10 ОК11		

Результати навчання	Компетентності																		
	Загальні									Спеціальні (фахові)									
	ЗК1	ЗК2	ЗК3	ЗК4	ЗК5	ЗК6	ЗК7	ЗК8	ЗК9	СК1	СК2	СК3	СК4	СК5	СК6	СК7	СК8	СК9	СК10
інформації, формулювати їх математичну постановку та обирати раціональний метод вирішення.																			
РН9. Знати та застосовувати законодавство України та міжнародні вимоги, практики і стандарти з метою здійснення професійної діяльності в галузі кібербезпеки та захисту інформації.						ОК6 ОК17 ОК21 ОК23 ОК28	ОК6 ОК17 ОК21 ОК23 ОК28			ОК6 ОК17 ОК21 ОК23 ОК28	ОК6 ОК17 ОК21 ОК23 ОК28								
РН10. Використовувати сучасні інформаційні технології, методи і моделі кібербезпеки та систем захисту інформації для здійснення професійної діяльності.	ОК12 ОК13 ОК19 ОК20 ОК22 ОК25 ОК26 ОК30	ОК12 ОК13 ОК19 ОК20 ОК21 ОК22 ОК25 ОК26 ОК30									ОК6 ОК12 ОК13 ОК19 ОК20 ОК21 ОК22 ОК25 ОК26 ОК30		ОК15 ОК19 ОК20 ОК21 ОК22 ОК30	ОК22 ОК29	ОК21 ОК30	ОК15 ОК19 ОК20 ОК22		ОК22 ОК29	ОК13 ОК30
РН11. Планувати підготовку та забезпечувати неперервність бізнес-процесів в організаціях згідно зі встановленою політикою кібербезпеки з урахування вимог до захисту інформації.		ОК22 ОК30 ОК13									ОК17 ОК30	ОК6 Ок17	ОК17 ОК21						
РН12. Застосовувати методи та засоби захисту інформації в інформаційних та інформаційно-комунікаційних системах відповідно до встановленої політики інформаційної безпеки.	ОК22 ОК30	ОК12 ОК19 ОК20 ОК22 ОК30									ОК12 ОК22 ОК30 ОК31		ОК31 ОК21 ОК22 ОК30 ОК12 ОК19 ОК20	ОК21 ОК22	ОК21 ОК30	ОК22 ОК30		ОК22 ОК30	
РН13. Впроваджувати, налаштовувати, супроводжувати та підтримувати функціонування програмних і програмно-апаратних комплексів і систем кібербезпеки та захисту інформації як необхідні процедури для функціонування інформаційних й Інформаційно-комунікаційних систем та\або інфраструктури організації в цілому.	ОК22 ОК30 ОК13	ОК22 ОК30 ОК13									ОК12 ОК13 ОК19 ОК20 ОК25 ОК26		ОК21 ОК22 ОК30 ОК12	ОК16 ОК21	ОК21 ОК29	ОК19 ОК20 ОК25 ОК26		ОК22 ОК30	ОК12 ОК19 ОК20 ОК25 ОК26 ОК30
РН14. Вирішувати задачі управління процесами відновлення штатного функціонування інформаційних та інформаційно-комунікаційних систем з використанням процедур											ОК12 ОК30		ОК17 ОК21	ОК21 Ок30	ОК13 ОК17 ОК21				ОК17 ОК19

Результати навчання	Компетентності																		
	Загальні									Спеціальні (фахові)									
	ЗК1	ЗК2	ЗК3	ЗК4	ЗК5	ЗК6	ЗК7	ЗК8	ЗК9	СК1	СК2	СК3	СК4	СК5	СК6	СК7	СК8	СК9	СК10
резервування згідно встановленої політики безпеки і забезпечувати функціонування спеціального програмного забезпечення щодо захисту та відновлення інформації.																			
РН15. Збирати, обробляти, зберігати, аналізувати критичні дані для доказу реалізації кіберзагроз, проводити аналіз та дослідження кіберінциденту з метою оперативного відновлення функціонування інформаційної системи.											ОК13 ОК30		ОК17 ОК21	ОК21 ОК22	ОК17 ОК21				ОК14 ОК17
РН16. Вирішувати задачі впровадження та супроводу комплексних систем захисту інформації в інформаційних системах.	ОК22 ОК30	ОК22 ОК30								ОК24 ОК32	ОК22 ОК30	ОК22 ОК30	ОК21 ОК24 ОК32	ОК21 ОК24 ОК32	ОК21 ОК24 ОК32			ОК22 ОК30	ОК22 ОК30
РН17. Забезпечувати функціонування системи управління кібербезпекою і захистом інформації організації, включаючи персонал та управління наслідками реалізації загроз інформаційній безпеці в кризових ситуаціях, на основі здійснення процедур кількісної і якісної оцінки ризиків.		ОК13 ОК17											ОК17 ОК21	ОК21 ОК22	ОК17 ОК21				ОК17 ОК22
РН18. Аналізувати, застосовувати методи та засоби криптографічного захисту інформації на об'єктах інформаційної діяльності.					ОК24 ОК32								ОК15 ОК24 ОК32				ОК15 ОК24 ОК32	ОК22 ОК24 ОК32	ОК22 ОК24 ОК32
РН19. Вирішувати задачі щодо організації та контролю стану криптографічного захисту інформації, зокрема відповідно до вимог нормативних документів.					ОК8 ОК10 ОК11 ОК12 ОК15								ОК8 ОК10 ОК11 ОК12 ОК15				ОК8 ОК10 ОК11 ОК12 ОК15		
РН20. Визначати загрози створення технічних каналів витоку інформації на об'єктах інформаційної діяльності; впроваджувати засоби і заходи технічного захисту інформації від витоку технічними каналами, проводити обслуговування і контроль стану апаратних засобів захисту інформації та комплексів технічного захисту інформації.		ОК13 ОК16 ОК17 ОК21 ОК23											ОК13 ОК16 ОК17 ОК21 ОК23	ОК13 ОК16 ОК17 ОК21 ОК23	ОК13 ОК16 ОК17 ОК21 ОК23				ОК13 ОК16 ОК17 ОК21 ОК23
РН21. Виконувати впровадження, підтримку, аналіз ефективності											ОК12 ОК21				ОК21 ОК30	ОК19 ОК20			ОК17 ОК21

Результати навчання	Компетентності																		
	Загальні									Спеціальні (фахові)									
	ЗК1	ЗК2	ЗК3	ЗК4	ЗК5	ЗК6	ЗК7	ЗК8	ЗК9	СК1	СК2	СК3	СК4	СК5	СК6	СК7	СК8	СК9	СК10
систем виявлення несанкціонованого доступу, дій з інформацією в інформаційній системі, вразливостей, можливих загроз інформаційному простору й інформаційним ресурсам та використовувати комплекси захисту для забезпечення необхідного рівня захищеності інформації в інформаційних системах.											ОК25 ОК26					ОК25 ОК26			
РН22. Формування національно-патріотичної свідомості, громадянської стійкості щодо захисту Вітчизни, незалежності та територіальної цілісності України.									ОК27										

Таблиця 3

Матриця формування трудових функцій визначених для професійної кваліфікації «Фахівець сфери захисту інформації» та освітніх компонентів ОП «Кібербезпека»

Трудові функції	Компетентності	Знання	ОК	Уміння та навички	ОК	Комунікація	ОК	Відповідальність і автономія	ОК
А. Впровадження систем та комплексів захисту інформації	Здатність аналізувати потреби та вимоги користувачів (замовників) щодо захисту інформації та кіберзахисту з метою впровадження систем та комплексів захисту інформації	А1.З1. Поняття та класифікація інформації з обмеженим доступом, державні інформаційні ресурси	ОК 6	А1.У1. Визначати (формулювати) потреби щодо захисту інформації в інформаційних, електронних комунікаційних та інформаційно-комунікаційних системах користувачів (замовників)	ОК 12	А1.К1. Пояснювати користувачам та замовникам вимоги щодо оброблення й захисту інформації з обмеженим доступом	ОК 17	А1.В1. Нести відповідальність за правильність визначення категорій інформації та дотримання вимог її захисту	ОК 21
		А1.З2. Поняття технічного та криптографічного захисту інформації	ОК 11	А1.У2. Визначати (формулювати) потреби щодо захисту інформації, що озвучується на об'єктах інформаційної діяльності підприємства (організації)	ОК 17	А1.К2. Узгоджувати із замовниками вимоги до технічного та криптографічного захисту інформації на об’єктах інформаційної діяльності	ОК 15	А1.В2. Нести відповідальність за обґрунтований вибір засобів технічного та криптографічного захисту інформації відповідно до встановлених вимог безпеки	ОК 15
		А1.З3. Концепції і протоколи комп'ютерних мереж, методологія забезпечення мережевої безпеки та захисту інформації в автоматизованих системах і на об'єктах інформаційної діяльності	ОК 13	А1.У3. Визначати (формулювати) потреби до кібербезпеки в електронних комунікаційних та інформаційно-комунікаційних системах користувачів (замовників)	ОК 22	А1.К3. Взаємодіяти із замовниками та технічними фахівцями щодо визначення вимог до мережевої безпеки та кіберзахисту інформаційно-комунікаційних систем	ОК 22	А1.В3. Самостійно приймати рішення щодо визначення потреб до кібербезпеки та відповідати за обґрунтованість запропонованих заходів захисту мережевої інфраструктури	ОК 22
		А1.З4. Методи та процеси управління ризиками (методи оцінки та зниження ризиків)	ОК 30	А1.У4. Визначати та аналізувати вимоги щодо захисту інформації та кіберзахисту в інформаційно-	ОК 30	А1.К4. Обговорювати із замовниками та керівництвом результати	ОК 30	А1.В4. Нести відповідальність за обґрунтованість аналізу ризиків та самостійно	ОК 30

Трудові функції	Компетентності	Знання	ОК	Уміння та навички	ОК	Комунікація	ОК	Відповідальність і автономія	ОК
				комунікаційних системах та на об'єктах інформаційної діяльності підприємства (організації)		оцінювання ризиків і вимоги щодо захисту інформації та кіберзахисту		визначати заходи щодо їх мінімізації в інформаційно-комунікаційних системах	
		А1.З5. Закони, нормативні акти, нормативні документи, що визначають вимоги із захисту інформації та кіберзахисту	ОК 17	А1.У5. Здійснювати попередню оцінку достатності потреб і вимог користувачів для забезпечення необхідного рівня захисту інформації та кіберзахисту	ОК 17	А1.К5. Надавати роз’яснення користувачам та замовникам щодо нормативних вимог у сфері захисту інформації та кіберзахисту	ОК 17	А1.В5. Самостійно оцінювати достатність вимог до захисту інформації та нести відповідальність за їх відповідність чинним нормативним документам	ОК 17
		А1.З6. Політики та етичні норми приватності стосовно безпеки інформації та кібербезпеки	ОК 17	А1.У6. Застосовувати політики безпеки для досягнення цілей безпеки системи	ОК 17	А1.К6. Доводити до користувачів вимоги політик безпеки та етичних норм поводження з інформацією	ОК 17	А1.В6. Нести відповідальність за дотримання та впровадження політик безпеки для забезпечення необхідного рівня захисту інформації та кібербезпеки	ОК 17
		А1.З7. Принципи та способи захисту інформації, кібербезпеки та приватності	ОК 25	А1.У7. Аналізувати потреби та вимоги користувачів з метою планування і проведення розробки системи безпеки	ОК 25	А1.К7. Узгоджувати з користувачами та замовниками вимоги до системи захисту інформації, кібербезпеки та приватності	ОК 25	А1.В7. Самостійно аналізувати потреби користувачів і нести відповідальність за обґрунтованість рішень під час планування системи безпеки	ОК 25
		А1.З8. Класифікація операційних наслідків у результаті помилок із захисту інформації та кібербезпеки	ОК 17	А1.У8. Використовувати моделі та симуляції інформаційних, електронних комунікаційних та інформаційно-комунікаційних систем для аналізу вразливості та прогнозування	ОК 18	А1.К8. Інформувати користувачів та керівництво про можливі наслідки вразливостей і помилок у системах захисту інформації та кібербезпеки	ОК 17	А1.В8. Самостійно застосовувати моделі та симуляції для аналізу вразливостей і нести відповідальність за достовірність прогнозування рівня захищеності та	ОК 18

Трудові функції	Компетентності	Знання	ОК	Уміння та навички	ОК	Комунікація	ОК	Відповідальність і автономія	ОК
				продуктивності				продуктивності систем	
		А1.39. Політики, вимоги та процедури безпеки ланцюжка постачання інформаційних технологій та управління ризиками ланцюжка постачання	ОК 18						
		А1.310. Поняття комплексних систем захисту інформації та комплексів технічного захисту інформації, їх склад і призначення	ОК 19						
		А1.311. Моделі та симуляції інформаційних, електронних комунікаційних та інформаційно-комунікаційних систем, призначених для аналізу вразливості та прогнозування продуктивності	ОК 18						
	Здатність виявляти, досліджувати (оцінювати), системно аналізувати загрози для інформації, аналізувати ризики безпеки інформації та кібербезпеки у разі реалізації загроз	А2.31. Класифікація загроз для інформації та кіберзагроз (загрози від несанкціонованих дій з інформацією, технічні канали витоку інформації, спеціальні впливи на засоби обробки інформації)	ОК 16	А2.У1. Виявляти загрози для інформації та кіберзагрози в інформаційних, електронних комунікаційних та інформаційно-комунікаційних системах	ОК 17	А2.К1. Взаємодіяти з користувачами та технічними фахівцями щодо виявлення й обговорення загроз для інформації та кіберзагроз	ОК 17	А2.В1. Самостійно здійснювати виявлення та аналіз загроз для інформації й нести відповідальність за достовірність результатів оцінювання рівня безпеки систем	ОК 17
		А2.32. Методи (способи) та методики виявлення, дослідження та системного аналізу загроз для інформації та кіберзагроз	ОК 21	А2.У2. Виявляти загрози для інформації, що озвучується на об'єктах інформаційної діяльності (обґрунтовувати можливість створення певних технічних каналів витоку інформації)	ОК 21	А2.К2. Обговорювати з фахівцями та замовниками результати виявлення технічних каналів витоку інформації	ОК 21	А2.В2. Самостійно застосовувати методики аналізу загроз і нести відповідальність за обґрунтованість висновків щодо можливості витоку	ОК 21

Трудові функції	Компетентності	Знання	ОК	Уміння та навички	ОК	Комунікація	ОК	Відповідальність і автономія	ОК
						та потенційних загроз		інформації	
		А2.33. Форми та зміст моделей загроз для інформації, моделі порушника інформації; порядок їх розробки	ОК 12	А2.У3. Досліджувати (оцінювати) та системно аналізувати загрози для інформації та вразливості комп'ютерної системи (систем) для розробки профілю безпеки	ОК 12	А2.К3. Узгоджувати з користувачами та фахівцями результати аналізу загроз і формування профілю безпеки комп’ютерних систем	ОК 12	А2.В3. Самостійно розробляти моделі загроз і порушника та нести відповідальність за повноту й обґрунтованість оцінювання вразливостей систем	ОК 12
		А2.34. Поняття ризиків безпеки інформації та кібербезпеки	ОК 12	А2.У4. Оцінювати та аналізувати ризики безпеки інформації та кібербезпеки	ОК 12	А2.К4. Надавати керівництву та користувачам інформацію щодо рівня ризиків безпеки інформації та кібербезпеки	ОК 12	А2.В4.Самостійно здійснювати оцінювання ризиків і нести відповідальність за обґрунтованість результатів аналізу безпеки інформаційних систем	ОК 12
		А2.35. Підходи, методи (способи) оцінки та аналізу ризиків безпеки інформації та кібербезпеки	ОК 21	А2.У5. Розробляти модель загроз для інформації від несанкціонованих дій та модель порушника інформації	ОК 21	А2.К5. Обговорювати із замовниками та фахівцями результати оцінювання ризиків і побудови моделей загроз та порушника	ОК 21	А2.В5. Самостійно обирати методи аналізу ризиків і нести відповідальність за коректність розроблення моделей загроз та порушника інформації	ОК 21
		А2.36. Класифікація операційних наслідків, спричинених помилками в системі кібербезпеки	ОК 21	А2.У6. Розробляти модель загроз для інформації від витоку технічними каналами	ОК 23	А2.К6. Інформувати користувачів та керівництво про можливі наслідки витоку інформації через технічні канали	ОК 23	А2.В6. Самостійно розробляти моделі загроз витоку інформації технічними каналами та нести відповідальність за достовірність оцінки можливих наслідків	ОК 23
		А2.37. Поняття спеціальних	Ок	А2.У7. Розробляти модель	Ок	А2.К7.	Ок	А2.В7. Самостійно	Ок

Трудові функції	Компетентності	Знання	ОК	Уміння та навички	ОК	Комунікація	ОК	Відповідальність і автономія	ОК
		впливів на засоби обробки інформації з метою знищення (спотворення), блокування інформації	16	загроз для інформації від спеціальних впливів на засоби обробки інформації	16	Взаємодіяти з технічними фахівцями та керівництвом щодо оцінювання загроз спеціальних впливів на засоби обробки інформації	16	розробляти моделі загроз від спеціальних впливів та нести відповідальність за обґрунтованість визначених заходів захисту інформації	16
	Здатність формувати стратегію і політики безпеки інформації в інформаційно-комунікаційних системах	А3.З1. Поняття стратегії і політики безпеки інформації в інформаційних, електронних комунікаційних та інформаційно-комунікаційних системах	ОК 21	А3.У1. Обґрунтовувати та розробляти політику безпеки інформації в інформаційних, електронних комунікаційних та інформаційно-комунікаційних системах	ОК 21	А3.К1. Узгоджувати із замовниками та керівництвом вимоги до стратегії і політики безпеки інформації в інформаційно-комунікаційних системах	ОК 21	А3.В1. Самостійно обґрунтовувати та розробляти політику безпеки інформації й нести відповідальність за її відповідність цілям та вимогам кібербезпеки	ОК 21
		А3.З2. Концепції архітектури безпеки мережі, включаючи топологію, протоколи, компоненти і принципи ешелонованого захисту	ОК 13	А3.У2. Ураховувати методи управління мережевими системами при обґрунтуванні концепції безпеки інформації	ОК 13	А3.К2. Взаємодіяти з адміністраторами мереж та замовниками щодо формування концепції безпеки мережевої інфраструктури	ОК 13	А3.В2. Самостійно враховувати методи управління мережевими системами та нести відповідальність за обґрунтованість архітектурних рішень у сфері безпеки інформації	ОК 13
		А3.З3. Принципи, моделі, інструменти та методи управління мережевими системами (наскрізний моніторинг продуктивності систем)	ОК 21	А3.У3. Ураховувати методи управління ризиками при обґрунтуванні концепції безпеки інформації	ОК 21	А3.К3. Обговорювати з технічними фахівцями результати моніторингу мережевих систем та їх вплив на безпеку інформації	ОК 21	А3.В3. Самостійно враховувати методи управління ризиками під час обґрунтування концепції безпеки інформації та нести відповідальність за ефективність запропонованих рішень	ОК 21
		А3.З4. Зміст і порядок розробки політики безпеки інформації в інформаційних,	ОК 21	А3.У4. Визначати (розробляти, обґрунтовувати) профіль	ОК 21	А3.К4. Узгоджувати з користувачами та керівництвом	ОК 21	А3.В4. Самостійно розробляти та обґрунтовувати	ОК 21

Трудові функції	Компетентності	Знання	ОК	Уміння та навички	ОК	Комунікація	ОК	Відповідальність і автономія	ОК
		електронних комунікаційних та інформаційно-комунікаційних системах		безпеки інформації в автоматизованих системах різного класу		вимоги до профілю безпеки інформації в автоматизованих системах		профіль безпеки інформації й нести відповідальність за його відповідність політиці безпеки та вимогам захисту інформації	
		А3.35. Поняття профілю безпеки інформації та функціональних послуг безпеки	ОК 21	А3.У5. Розробляти групові політики та переліки контролю доступу для забезпечення відповідності стандартам організації, бізнес-правилам і потребам	ОК 21	А3.К5. Взаємодіяти з адміністраторами та користувачами щодо впровадження групових політик і механізмів контролю доступу	ОК 21	А3.В5. Самостійно розробляти групові політики та переліки контролю доступу й нести відповідальність за їх відповідність вимогам безпеки та стандартам організації	ОК 21
		А3.36. Поняття рівня гарантій реалізації функціональних послуг безпеки	ОК 21	А3.У6. Застосовувати політики безпеки інформації в інформаційно-комунікаційних системах для досягнення цілей безпеки системи	ОК 21	А3.К6. Пояснювати користувачам та адміністраторам вимоги політик безпеки і рівні гарантій реалізації функціональних послуг безпеки	ОК 21	А3.В6. Самостійно застосовувати політики безпеки інформації та нести відповідальність за досягнення встановлених цілей безпеки інформаційно-комунікаційних систем	ОК 21
	Здатність аналізувати, розробляти та супроводжувати систему управління інформаційною безпекою підприємства/організації	А4.31. Поняття системи управління інформаційною безпекою підприємства/організації	ОК 22	А4.У1. Визначати сферу та межі дії системи управління інформаційною безпекою підприємства/організації (далі – СУІБ)	ОК 22	А4.К1. Взаємодіяти з керівництвом та структурними підрозділами щодо визначення сфери та меж дії системи управління інформаційною безпекою	ОК 22	А4.В1. Самостійно визначати сферу та межі дії СУІБ та нести відповідальність за коректність їх встановлення відповідно до потреб організації	ОК 22
		А4.32. Принципи створення систем управління інформаційною безпекою	ОК 22	А4.У2. Розробляти (брати участь у розробці) СУІБ	ОК 22	А4.К2. Координувати взаємодію між підрозділами під час	ОК 22	А4.В2. Самостійно брати участь у розробленні СУІБ та нести	ОК 22

Трудові функції	Компетентності	Знання	ОК	Уміння та навички	ОК	Комунікація	ОК	Відповідальність і автономія	ОК
						розроблення системи управління інформаційною безпекою		відповідальність за відповідність її структури принципам управління інформаційною безпекою	
		А4.З3. Принципи створення систем інформаційної безпеки (NIST SP 800-160)	ОК 22	А4.У3. Впроваджувати (брати участь у впровадженні) СУІБ	ОК 22	А4.К3. Взаємодіяти з технічними фахівцями та керівництвом щодо впровадження системи управління інформаційною безпекою відповідно до сучасних стандартів	ОК 22	А4.В3. Самостійно впроваджувати або брати участь у впровадженні СУІБ та нести відповідальність за дотримання принципів побудови систем інформаційної безпеки	ОК 22
				А4.У4. Здійснювати моніторинг та аналіз (брати участь у моніторингу та аналізуванні) СУІБ	ОК 22	А4.К4. Взаємодіяти з відповідальними підрозділами та керівництвом щодо результатів моніторингу й аналізу системи управління інформаційною безпекою	ОК 22	А4.В4. Самостійно здійснювати моніторинг та аналіз СУІБ і нести відповідальність за достовірність результатів оцінювання ефективності системи	ОК 22
				А4.У5. Здійснювати підтримку та вдосконалення (брати участь у здійсненні підтримки та вдосконаленні) СУІБ	ОК 22	А4.К5. Координувати взаємодію між підрозділами під час підтримки та вдосконалення системи управління інформаційною безпекою	ОК 22	А4.В5. Самостійно здійснювати підтримку та вдосконалення СУІБ і нести відповідальність за підвищення ефективності функціонування системи	ОК 22
				А4.У6. Створювати системи (брати участь у створенні систем)	ОК 22	А4.К6. Взаємодіяти з технічними фахівцями та	ОК 22	А4.В6. Самостійно створювати або брати участь у	ОК 22

Трудові функції	Компетентності	Знання	ОК	Уміння та навички	ОК	Комунікація	ОК	Відповідальність і автономія	ОК
				інформаційної безпеки		замовниками під час створення систем інформаційної безпеки		створенні систем інформаційної безпеки та нести відповідальність за відповідність систем вимогам безпеки	
				А4.У7. Застосовувати сервіс-орієнтовані принципи архітектури безпеки, щоб задовольнити вимоги конфіденційності, цілісності та доступності організації	ОК 22	А4.К7. Узгоджувати архітектурні рішення із зацікавленими сторонами щодо забезпечення конфіденційності, цілісності та доступності інформації	ОК 22	А4.В7. Самостійно застосовувати сервіс-орієнтовані принципи архітектури безпеки та нести відповідальність за досягнення цілей інформаційної безпеки організації	ОК 22
	Здатність виконувати передпроєктні роботи щодо систем та комплексів захисту інформації	А5.31. Середовища функціонування автоматизованих систем	ОК 23	А5.У1. Здійснювати категоріювання об'єктів інформаційної діяльності (об'єктів електронно-обчислювальної техніки)	ОК 23	А5.К1. Взаємодіяти із замовниками та технічними фахівцями щодо визначення особливостей середовища функціонування автоматизованих систем	ОК 23	А5.В1. Самостійно здійснювати категоріювання об’єктів інформаційної діяльності та нести відповідальність за правильність визначення їх характеристик і умов функціонування	ОК 23
		А5.32. Загальний порядок створення комплексних систем захисту інформації та комплексів технічного захисту інформації	ОК 23	А5.У2. Здійснювати обстеження середовищ функціонування автоматизованих систем	ОК 23	А5.К2. Узгоджувати з технічними фахівцями та замовниками результати обстеження середовищ функціонування автоматизованих систем	ОК 23	А5.В2. Самостійно здійснювати обстеження середовищ функціонування автоматизованих систем та нести відповідальність за повноту зібраних даних для створення систем захисту інформації	ОК 23
		А5.33. Порядок	ОК	А5.У3. Здійснювати	ОК	А5.К3. Взаємодіяти	ОК	А5.В3. Самостійно	ОК

Трудові функції	Компетентності	Знання	ОК	Уміння та навички	ОК	Комунікація	ОК	Відповідальність і автономія	ОК
		категоріювання об'єктів	23	обстеження об'єктів інформаційної діяльності	23	з відповідальними особами під час проведення обстеження об’єктів інформаційної діяльності	23	здійснювати обстеження об’єктів інформаційної діяльності та нести відповідальність за коректність визначення їх категорії й умов захисту інформації	23
		А5.34. Порядок і методи (способи) обстеження середовищ функціонування автоматизованих систем та об'єктів інформаційної діяльності	ОК 23	А5.У4. Розробляти моделі загроз для інформації	ОК 23	А5.К4. Обговорювати з технічними фахівцями результати обстеження та виявлені загрози для інформації	ОК 23	А5.В4. Самостійно проводити обстеження середовищ функціонування систем та нести відповідальність за обґрунтованість розроблених моделей загроз	ОК 23
		А5.35. Порядок розробки моделей загроз для інформації	ОК 23	А5.У5. Розробляти технічні завдання на створення комплексних систем захисту інформації	ОК 23	А5.К5. Узгоджувати із замовниками вимоги до технічного завдання на створення комплексної системи захисту інформації	ОК 23	А5.В5. Самостійно розробляти технічні завдання на створення комплексних систем захисту інформації та нести відповідальність за їх відповідність встановленим вимогам безпеки	ОК 23
		А5.36. Порядок розробки та зміст технічних завдань на створення комплексних систем захисту інформації та комплексів технічного захисту інформації	ОК 23	А5.У6. Розробляти технічні завдання на створення комплексів технічного захисту інформації	ОК 23	А5.К6. Узгоджувати із замовниками та технічними фахівцями вимоги до технічних завдань на створення комплексів технічного захисту інформації	ОК 23	А5.В6. Самостійно розробляти технічні завдання та нести відповідальність за їх відповідність нормативним вимогам і потребам захисту інформації	ОК 23

Трудові функції	Компетентності	Знання	ОК	Уміння та навички	ОК	Комунікація	ОК	Відповідальність і автономія	ОК
				А5.У7. Розробляти проєкти комплексних систем захисту інформації та комплексів технічного захисту інформації багаторівневими вимогами безпеки	ОК 23	А5.К7. Взаємодіяти з усіма зацікавленими сторонами під час проєктування комплексних систем захисту інформації	ОК 23	А5.В7. Самостійно розробляти проєкти комплексних систем захисту інформації та нести відповідальність за реалізацію багаторівневих вимог безпеки	ОК 23
	Здатність проводити спеціальні дослідження засобів обробки інформації, технічних засобів та об'єктів інформаційної діяльності	А6.31. Поняття спеціальних досліджень засобів обробки інформації, технічних засобів	ОК 16	А6.У1. Проводити спеціальні дослідження засобів обробки інформації, технічних засобів (визначати складові та режими роботи, визначати тестові сигнали, складати схеми спеціальних досліджень, виявляти та вимірювати небезпечні (тестові) електричні, електромагнітні та оптичні сигнали, визначати показники захищеності інформації та можливість (неможливість) створення технічних каналів витоку інформації)	ОК 16	А6.К1. Взаємодіяти з технічними фахівцями та відповідальними особами під час проведення спеціальних досліджень засобів обробки інформації	ОК 16	А6.В1. Самостійно проводити спеціальні дослідження технічних засобів та нести відповідальність за достовірність визначення показників захищеності інформації і виявлення технічних каналів витоку інформації	ОК 16
		А6.32. Поняття спеціальних досліджень об'єктів інформаційної діяльності	ОК 16	А6.У2. Проводити спеціальні дослідження об'єктів інформаційної діяльності (складати схеми спеціальних досліджень, виявляти та вимірювати небезпечні (тестові) акустичні, віброакустичні, акустоелектричні, акустоелектромагнітні, лазерні сигнали,	ОК 16	А2.К2. Взаємодіяти з відповідальними особами та технічними фахівцями під час проведення спеціальних досліджень об’єктів інформаційної діяльності	ОК 16	А6.В2. Самостійно проводити спеціальні дослідження об’єктів інформаційної діяльності та нести відповідальність за достовірність оцінювання показників захищеності мовної	ОК 16

Трудові функції	Компетентності	Знання	ОК	Уміння та навички	ОК	Комунікація	ОК	Відповідальність і автономія	ОК
				визначати показники захищеності мовної інформації)				інформації	
		А6.33. Архітектура комп'ютера, принципи дії складових електронно-обчислювальної машини, комп'ютерні мережі, класи автоматизованих систем	ОК 16	А6.У3. Визначати вимоги до показників (характеристик) апаратних засобів технічного захисту інформації, які необхідні для забезпечення захищеності інформації	ОК 16	А2.К3. Узгоджувати з технічними спеціалістами вимоги до характеристик апаратних засобів технічного захисту інформації	ОК 16	А6.В3. Самостійно визначати вимоги до показників апаратних засобів захисту інформації та нести відповідальність за їх відповідність вимогам захищеності інформації	ОК 16
		А6.34. Поняття об'єкта інформаційної діяльності	ОК 16	А6.У4. Складати протоколи спеціальних досліджень	ОК 16	А2.К4. Оформлювати та погоджувати результати спеціальних досліджень із відповідальними особами та технічними фахівцями	ОК 16	А6.В4. Самостійно складати протоколи спеціальних досліджень та нести відповідальність за повноту і достовірність зафіксованих результатів	ОК 16
		А6.35. Поняття показників захищеності інформації засобів обробки інформації та технічних засобів	ОК 16	А6.У5. Складати приписи на експлуатацію засобів обробки інформації та об'єктів інформаційної діяльності	ОК 16	А2.К5. Надавати відповідальним особам рекомендації щодо безпечної експлуатації засобів обробки інформації та об’єктів інформаційної діяльності	ОК 16	А6.В5. Самостійно складати приписи на експлуатацію засобів обробки інформації та нести відповідальність за обґрунтованість установлених вимог захисту інформації	ОК 16
		А6.36. Методи вимірювання фізичних величин і принципи роботи сучасних засобів вимірювальної техніки (спектроаналізаторів, осцилографів, частотомірів,	ОК 16						

Трудові функції	Компетентності	Знання	ОК	Уміння та навички	ОК	Комунікація	ОК	Відповідальність і автономія	ОК
		вольтметрів, омметрів)							
		А6.37. Методики спеціальних досліджень засобів обробки інформації та об'єктів інформаційної діяльності	ОК 16						
		А6.38. Теорія електромагнітного поля (в частині, необхідній для виконання професійних функцій)	ОК 16						
		А6.39. Теорія акустики (в частині, необхідній для виконання професійних функцій)	ОК 16						
		А6.310. Пристрої електротехніки (в частині, що складають архітектуру комп'ютера: друковані плати, мікросхеми, процесори, елементи пам'яті)	ОК 16						
		А6.311. Теорія радіотехнічних ланцюгів і сигналів (у частині, необхідній для виконання професійних функцій)	ОК 16						
		А6.312. Спектри сигналів і методи спектрального аналізу	ОК 16						
		А6.313. Загальні положення теорії інформації та методи кодування	ОК 29						
		А6.314. Загальні положення теорії ймовірностей і нечітких множин	ОК 10						
		А6.315. Статистична радіотехніка (прийом звісних сигналів на фоні шумів, оцінка параметрів сигналів)	ОК 23						

Трудові функції	Компетентності	Знання	ОК	Уміння та навички	ОК	Комунікація	ОК	Відповідальність і автономія	ОК
		А6.316. Методи цифрової обробки зображень та сигналів	ОК 23						
		А6.317. Математика логарифмів, тригонометрія, лінійна алгебра, математичний аналіз, операційний аналіз, статистика	ОК 18						
		А6.318. Концепції і протоколи комп'ютерних мереж	ОК 13						
		А6.319. Технології передачі голосу по IP (VoIP)	ОК 13						
	Здатність впроваджувати (активізувати) програмні та апаратні засоби захисту інформації в системах і на об'єктах	А7.31. Принципи, методи, засоби забезпечення безпеки інформації та інформаційних технологій (програмні засоби (механізми) захисту інформації, мережеві екрани, шифрування)	ОК 9	А7.У1. Використовувати методи комп'ютерного проєктування та моделювання систем для розробки технічних проєктів комплексних систем захисту інформації	ОК 9	А7.К1. Взаємодіяти з розробниками та адміністраторами систем під час проєктування комплексних систем захисту інформації	ОК 9	А7.В1. Самостійно застосовувати методи комп’ютерного проєктування та моделювання й нести відповідальність за обґрунтованість технічних рішень у системах захисту інформації	ОК 9
		А7.32. Методології забезпечення мережевої безпеки	ОК 13	А7.У2. Визначати та групувати за пріоритетами основні системні функції або підсистеми, необхідні для підтримки основних можливостей або бізнес-функцій з метою відновлення або поновлення після відмови системи	ОК 13	А7.К2. Взаємодіяти з адміністраторами мереж та керівництвом щодо визначення пріоритетних функцій і підсистем для забезпечення безперервності роботи систем	ОК 13	А7.В2. Самостійно визначати пріоритети системних функцій та нести відповідальність за обґрунтованість рішень щодо відновлення і забезпечення стійкості інформаційних систем	ОК 13
		А7.33. Способи та апаратні засоби захисту інформації,	ОК 16	А7.У3. Аналізувати проєктні обмеження та	ОК 16	А7.К3. Узгоджувати з розробниками та	ОК 16	А7.В3. Самостійно аналізувати проєктні	ОК 16

Трудові функції	Компетентності	Знання	ОК	Уміння та навички	ОК	Комунікація	ОК	Відповідальність і автономія	ОК
		методи автентифікації, авторизації та контролю доступу		можливі компроміси системи безпеки інформації (комплексної системи захисту інформації)		замовниками проєктні обмеження і вимоги до засобів автентифікації, авторизації та контролю доступу		обмеження та нести відповідальність за обґрунтованість компромісів у системі безпеки інформації	
		А7.З4. Методологічні та математичні основи комп'ютерного проєктування та моделювання систем	ОК 18	А7.У4. Проєктувати, розробляти та модифікувати програмні системи, використовуючи науковий аналіз і математичні моделі для прогнозування та вимірювання результатів та наслідків проєкту	ОК 14	А7.К4. Взаємодіяти з учасниками проєкту щодо результатів моделювання та прогнозування ефективності систем захисту інформації	ОК 14	А7.В4. Самостійно проєктувати та модифікувати програмні системи й нести відповідальність за достовірність результатів аналізу та ефективність запропонованих рішень	ОК 14
		А7.З5. Мови програмування мікроконтролерів і контролерів відповідно до норм IEC 61131-3	ОК 16	А7.У5. Розробляти проєкти з кібербезпеки	ОК 14	А7.К5. Взаємодіяти з розробниками та технічними спеціалістами під час розроблення проєктів з кібербезпеки для автоматизованих систем і контролерів	ОК 14	А7.В5. Самостійно розробляти проєкти з кібербезпеки та нести відповідальність за їх відповідність технічним і нормативним вимогам	ОК 14
		А7.З6. Порядок розробки та зміст технічних проєктів комплексних систем захисту інформації та комплексів технічного захисту інформації	ОК 16	А7.У6. Проєктувати функції управління ключами стосовно сфери кібербезпеки	ОК 14	А7.К6. Узгоджувати із замовниками та адміністраторами вимоги до функцій управління криптографічними ключами в системах кібербезпеки	ОК 14	А7.В6. Самостійно проєктувати функції управління ключами та нести відповідальність за надійність і безпечність реалізації криптографічного захисту інформації	ОК 14
		А7.З7. Методи техніко-економічного аналізу та обґрунтування проєктних рішень	ОК 16	А7.У7. Активізувати (налаштовувати) програмні механізми захисту інформації в	ОК 14	А7.К7. Узгоджувати з користувачами та адміністраторами параметри	ОК 14	А7.В7. Самостійно налаштовувати програмні механізми захисту інформації	ОК 14

Трудові функції	Компетентності	Знання	ОК	Уміння та навички	ОК	Комунікація	ОК	Відповідальність і автономія	ОК
				інформаційних системах, електронних комунікаційних та інформаційно-комунікаційних системах (програмні фільтри, антивірусні програми, антишпигунське програмне забезпечення)		налаштування програмних механізмів захисту інформації		та нести відповідальність за ефективність і коректність їх функціонування	
		А7.38. Процедури активізації (настроювання) програмних механізмів захисту інформації в інформаційних системах	ОК 14	А7.У8. Впроваджувати (налаштовувати) програмно-апаратні засоби захисту інформації в інформаційних системах, електронних комунікаційних та інформаційно-комунікаційних системах	ОК 14	А7.К8. Взаємодіяти з технічними фахівцями під час впровадження та налаштування програмно-апаратних засобів захисту інформації	ОК 14	А7.В8. Самостійно впроваджувати та налаштовувати програмно-апаратні засоби захисту інформації й нести відповідальність за забезпечення належного рівня кібербезпеки систем	ОК 14
		А7.39. Процедури підключення до локальної мережі підприємства (організації) та до глобальних мереж; процедури активізації (настроювання) програмних мережевих механізмів захисту інформації	ОК 13	А7.У9. Впроваджувати (налаштовувати) програмні та програмно-апаратні засоби захисту мережевих комунікацій	ОК 13	А7.К9. Взаємодіяти з мережевими адміністраторами та користувачами під час налаштування засобів захисту мережевих комунікацій	ОК 13	А7.В9. Самостійно впроваджувати та налаштовувати засоби захисту мережевих комунікацій і нести відповідальність за безпечність мережевої взаємодії	ОК 13
		А7.310. Концепції управління послугами для мереж і відповідних стандартів (бібліотека інфраструктури інформаційних технологій (ITIL))	ОК 13	А7.У10. Впроваджувати (налаштовувати) апаратні засоби захисту інформації на об'єктах інформаційної діяльності	ОК 13	А7.К10. Координувати роботи з технічними підрозділами під час впровадження апаратних засобів захисту інформації	ОК 13	А7.В10. Самостійно впроваджувати та налаштовувати апаратні засоби захисту інформації й нести відповідальність за їх відповідність вимогам безпеки та стандартам управління ІТ-послугами	ОК 13
		А7.311. Способи	ОК	А7.У11. Оцінювати якість	ОК	А7.К11. Надавати	ОК	А7.В11. Самостійно	ОК

Трудові функції	Компетентності	Знання	ОК	Уміння та навички	ОК	Комунікація	ОК	Відповідальність і автономія	ОК
		провадження апаратних засобів захисту інформації	23	виконаних робіт з впровадження програмних та апаратних засобів захисту інформації в системах і на об'єктах	23	керівництву та замовникам результати оцінювання якості впровадження засобів захисту інформації	23	оцінювати якість виконаних робіт та нести відповідальність за достовірність результатів контролю ефективності засобів захисту інформації	23
	Здатність адмініструвати системи, мережі та системи безпеки інформації	А8.31. Концепції адміністрування систем, мереж і систем безпеки інформації	ОК 21	А8.У1. Розробляти та документувати стандартні операційні процедури адміністрування систем, мереж і систем безпеки інформації	ОК 21	А8.К1. Взаємодіяти з адміністраторами та користувачами під час розроблення і впровадження процедур адміністрування систем та мереж	ОК 21	А8.В1. Самостійно розробляти й документувати стандартні операційні процедури та нести відповідальність за їх відповідність вимогам інформаційної безпеки	ОК 21
		А8.32. Методики адміністрування систем, мереж і систем безпеки інформації	ОК 21	А8.У2. Координувати свої дії з аналітиками системи захисту кіберпростору для управління та адміністрування оновлень правил і сигнатур для спеціалізованих прикладних програм у сфері кіберзахисту та захисту інформації	ОК 21	А8.К2. Координувати взаємодію з аналітиками та адміністраторами під час оновлення правил і сигнатур засобів кіберзахисту	ОК 21	А8.В2. Самостійно виконувати адміністрування систем захисту інформації та нести відповідальність за актуальність і коректність налаштувань засобів кіберзахисту	ОК 21
		А8.33. Політики адміністрування даних	ОК 21	А8.У3. Здійснювати системне адміністрування операційних систем і спеціалізованих прикладних програм кіберзахисту та захисту інформації, систем (антивірусне програмне забезпечення, засоби аудиту та відновлення) та пристроїв VPN	ОК 21	А8.К3. Взаємодіяти з користувачами та технічними фахівцями щодо експлуатації та підтримки систем кіберзахисту	ОК 21	А8.В3. Самостійно здійснювати системне адміністрування ОС і засобів кіберзахисту та нести відповідальність за стабільність і безпеку їх роботи	ОК 21

Трудові функції	Компетентності	Знання	ОК	Уміння та навички	ОК	Комунікація	ОК	Відповідальність і автономія	ОК
		А8.34. Принципи, концепції і методи адміністрування серверів	ОК 26	А8.У4. Здійснювати адміністрування серверів	ОК 26	А8.К4. Координувати дії з іншими адміністраторами та користувачами під час експлуатації серверної інфраструктури	ОК 26	А8.В4. Самостійно адмініструвати сервери та нести відповідальність за їх доступність, продуктивність і захищеність	ОК 26
				А8.У5. Дотримуватись стандартних операційних процедур адміністрування систем організації	ОК 21	А8.К5. Взаємодіяти з адміністраторами та відповідальними підрозділами щодо виконання стандартних операційних процедур	ОК 21	А8.В5. Самостійно дотримуватись стандартних операційних процедур адміністрування систем і нести відповідальність за коректність і своєчасність виконання регламентованих дій	ОК 21
				А8.У6. Управляти системними/серверними ресурсами, включаючи продуктивність, ємність, доступність, ремонтопридатність і здатність відновлюватись	ОК 21	А8.К6. Координувати дії з технічними фахівцями щодо оптимізації та підтримки ресурсів систем і серверів	ОК 21	А8.В6. Самостійно управляти системними/серверними ресурсами та нести відповідальність за їх ефективність, стабільність і здатність до відновлення	ОК 21
	Здатність розробляти, впроваджувати та аналізувати технічні документи, положення, інструкції щодо систем і комплексів захисту інформації	А9.31. Систему технічних документів щодо систем і комплексів захисту інформації	ОК 17	А9.У1. Формувати (брати участь у формуванні) вимог до захисту інформації в інформаційно-комунікаційних системах і на об'єктах інформаційної діяльності	ОК 17	А9.К1. Взаємодіяти із замовниками та технічними фахівцями під час формування вимог до захисту інформації	ОК 17	А9.В1.Самостійно формувати вимоги до захисту інформації та нести відповідальність за їх повноту, узгодженість і відповідність потребам системи	ОК 17
		А9.32. Вимоги до структури та змісту технічних	ОК 17	А9.У2. Розроблювати (брати участь у розробці)	ОК 17	А9.К2. Узгоджувати з керівництвом та	ОК 17	А9.В2. Самостійно розробляти політики	ОК 17

Трудові функції	Компетентності	Знання	ОК	Уміння та навички	ОК	Комунікація	ОК	Відповідальність і автономія	ОК
		документів щодо систем і комплексів захисту інформації		політики безпеки інформації в інформаційно-комунікаційних системах		зацікавленими сторонами зміст політик безпеки інформації		безпеки інформації та нести відповідальність за їх відповідність нормативним вимогам і цілям захисту інформації	
		А9.33. Вимоги та підходи до розроблення технічних документів положень, інструкцій, методичних матеріалів щодо систем і комплексів захисту інформації	ОК 17	А9.У3. Розроблювати (брати участь у розробці) технічної та експлуатаційної документації щодо створення, державної експертизи, (атестації), ведення в експлуатацію, експлуатації систем і комплексів захисту інформації	ОК 17	А9.К3. Взаємодіяти із замовниками, експертами та технічними фахівцями під час підготовки та погодження технічної й експлуатаційної документації	ОК 17	А9.В3. Самостійно розробляти технічну та експлуатаційну документацію та нести відповідальність за її повноту, коректність і відповідність вимогам нормативних документів	ОК 17
		А9.34. Сучасні підходи до формування вимог до захисту інформації в інформаційно-комунікаційних системах і на об'єктах інформаційної діяльності	ОК 17	А9.У4. Застосовувати інструменти, методи та техніки проєктування систем, включаючи інструменти автоматизованого аналізу та проєктування систем	ОК 18	А9.К4. Координувати взаємодію з учасниками проєкту під час застосування інструментів проєктування та формування вимог до систем захисту інформації	ОК 17	А9.В4. Самостійно застосовувати інструменти та методи проєктування систем і нести відповідальність за обґрунтованість і якість розроблених рішень	ОК 17
		А9.35. Інструменти, методи та техніки проєктування систем, включаючи інструменти автоматизованого аналізу та проєктування систем	ОК 18	А9.У5. Розроблювати плани аварійного відновлення та безперервності операцій в інформаційних, електронних комунікаційних та інформаційно-комунікаційних системах	ОК 18	А9.К5. Взаємодіяти з адміністраторами та керівництвом щодо узгодження вимог до аварійного відновлення та безперервності бізнес-процесів	ОК 18	А9.В5. Самостійно розробляти плани аварійного відновлення та безперервності операцій і нести відповідальність за їх ефективність та відповідність вимогам організації	ОК 18
Б. Оцінювання відповідності систем, комплексів та засобів	Здатність проводити оцінку відповідності (атестацію) комплексів	Б1.31. Поняття атестації комплексів технічного захисту інформації	ОК 16	Б1.У1. Складати програму та методику атестації комплексу технічного	ОК 16	Б1.К1. Взаємодіяти з замовниками, експертами та	ОК 16	Б1.В1. Самостійно складати програму та методику	ОК 16

Трудові функції	Компетентності	Знання	ОК	Уміння та навички	ОК	Комунікація	ОК	Відповідальність і автономія	ОК
захисту інформації	технічного захисту інформації			захисту інформації (ТЗІ)		технічними фахівцями під час узгодження програми та методики атестації комплексу ТЗІ		атестації комплексів ТЗІ та нести відповідальність за її відповідність нормативним вимогам і об'єктивність оцінювання	
		Б1.32. Порядок, умови та організація проведення атестації комплексів технічного захисту інформації	ОК 16	Б1.У2. Здійснювати перевірку повноти і відповідності реалізованих заходів із захисту інформації вимогам технічного завдання на створення комплексу ТЗІ, нормативно-правових актів і нормативних документів системи ТЗІ	ОК 16	Б1.К2. Взаємодіяти з замовниками та експертами щодо результатів перевірки реалізованих заходів захисту інформації	ОК 16	Б1.В2. Самостійно здійснювати перевірку відповідності заходів ТЗІ та нести відповідальність за обґрунтованість висновків щодо їх повноти та відповідності	ОК 16
		Б1.33. Поняття та загальний зміст програми та методики проведення атестації комплексів технічного захисту інформації	ОК 16	Б1.У3. Здійснювати інструментальний контроль захищеності інформації на об'єкті інформаційної діяльності від витоку технічними каналами	ОК 16	Б1.К3. Координувати дії з технічними фахівцями під час проведення інструментального контролю захищеності інформації	ОК 16	Б1.В3. Самостійно здійснювати інструментальний контроль та нести відповідальність за достовірність результатів вимірювань захищеності інформації	ОК 16
		Б1.34. Техніко-технологічне, комп'ютерне, програмне та інше забезпечення атестації комплексів технічного захисту інформації	ОК 16	Б1.У4. Робити висновки щодо відповідності комплексу ТЗІ вимогам технічного завдання та нормативних документів системи ТЗІ	ОК 16	Б1.К4. Узгоджувати з експертами та замовниками результати оцінювання відповідності комплексу ТЗІ	ОК 16	Б1.В4. Самостійно формувати висновки щодо відповідності комплексу ТЗІ та нести відповідальність за їх обґрунтованість	ОК 16
		Б1.35. Засоби вимірювальної техніки та методики вимірювань оцінюваних показників комплексів	ОК 23	Б1.У5. Оформлювати протоколи інструментального контролю захищеності	ОК 23	Б1.К5. Взаємодіяти з членами атестаційної групи щодо оформлення	ОК 23	Б1.В5. Самостійно оформлювати протоколи інструментального	ОК 23

Трудові функції	Компетентності	Знання	ОК	Уміння та навички	ОК	Комунікація	ОК	Відповідальність і автономія	ОК
		технічного захисту інформації		інформації на об'єкті інформаційної діяльності		результатів інструментального контролю		контролю та нести відповідальність за точність і повноту зафіксованих результатів	
		Б1.З6. Документи, що оформлюються за результатами атестації комплексів технічного захисту інформації	ОК 23	Б1.У6. Оформлювати акти атестації комплексів ТЗІ та організовувати їх затвердження і реєстрацію	ОК 23	Б1.К6. Взаємодіяти з керівництвом та регуляторними органами щодо затвердження та реєстрації актів атестації	ОК 23	Б1.В6. Самостійно оформлювати акти атестації комплексів ТЗІ та нести відповідальність за їх відповідність вимогам нормативних документів і результатам оцінювання	ОК 23
	Здатність проводити оцінку відповідності (державну експертизу) комплексних систем захисту інформації та засобів технічного захисту інформації	Б2.З1. Поняття та шляхи проведення державної експертизи комплексних систем захисту інформації та засобів технічного захисту інформації	ОК 23	Б2.У1. Складати програму та методику проведення державної експертизи комплексних систем захисту інформації	ОК 23	Б2.К1. Взаємодіяти з експертами, замовниками та уповноваженими органами під час узгодження програми та методики державної експертизи КСЗІ	ОК 23	Б2.В1.Самостійно розробляти програму та методику державної експертизи КСЗІ та нести відповідальність за її відповідність нормативним вимогам і об’єктивність результатів оцінювання	ОК 23
		Б2.З2. Порядок, умови та організація проведення державної експертизи комплексних систем захисту інформації та засобів технічного захисту інформації	ОК 23	Б2.У2. Проводити попереднє ознайомлення з об'єктом експертизи та поглиблене обстеження об'єкта експертизи	ОК 23	Б2.К2.Взаємодіяти з власниками об’єктів та експертами під час проведення обстеження та підготовки до державної експертизи	ОК 23	Б2.В2. Самостійно проводити обстеження об’єкта експертизи та нести відповідальність за повноту зібраних даних для експертного оцінювання	ОК 23
		Б2.З3. Поняття та загальний зміст програми та методики проведення державної	ОК 23	Б2.У3. Проводити експертні випробування та дослідження	ОК 23	Б2.К3. Координувати взаємодію з	ОК 23	Б2.В3. Самостійно проводити експертні випробування КСЗІ	ОК 23

Трудові функції	Компетентності	Знання	ОК	Уміння та навички	ОК	Комунікація	ОК	Відповідальність і автономія	ОК
		експертизи комплексних систем захисту інформації та засобів технічного захисту інформації		комплексних систем захисту інформації (оцінювати функціональні послуги безпеки, оцінювати рівні гарантій коректності реалізації функціональних послуг безпеки)		експертною групою та технічними фахівцями під час проведення експертних випробувань		та нести відповідальність за об’єктивність оцінки функціональних послуг безпеки	
		Б2.34. Методи тестування та оцінки захищеності систем	ОК 21	Б2.У4. Оформлювати протоколи експертних випробувань та атестів відповідності комплексних систем захисту інформації	ОК 21	Б2.К4. Взаємодіяти з членами експертної комісії щодо погодження результатів випробувань та оформлення документації	ОК 21	Б2.В4. Самостійно оформлювати протоколи та атестати відповідності й нести відповідальність за точність і повноту експертних результатів	ОК 21
		Б2.35. Техніко-технологічне, комп'ютерне, програмне та інше забезпечення оцінювання відповідності комплексних систем захисту інформації	ОК 21	Б2.У5. Здійснювати експертизу комплексних систем захисту інформації шляхом декларування, оформлювати декларації відповідності та організовувати їх затвердження та реєстрацію	ОК 21	Б2.К5. Узгоджувати з регуляторними органами та замовниками результати експертизи та оформлення декларацій відповідності	ОК 21	Б2.В5. Самостійно здійснювати експертизу шляхом декларування та нести відповідальність за правомірність і обґрунтованість висновків відповідності	ОК 21
		Б2.36. Засоби вимірювальної техніки та методики вимірювань оцінюваних показників комплексних систем захисту інформації та характеристик засобів технічного захисту інформації	ОК 23	Б2.У6. Здійснювати експертизу засобів технічного захисту інформації, оформлювати протоколи експертних випробувань та експертні висновки на засоби ТЗІ, організовувати затвердження і реєстрацію експертних висновків	ОК 23	Б2.К6. Взаємодіяти з виробниками, експертами та замовниками під час проведення експертизи засобів технічного захисту інформації	ОК 23	Б2.В6. Самостійно здійснювати експертизу засобів ТЗІ та нести відповідальність за достовірність експертних висновків і протоколів випробувань	ОК 23
		Б2.37. Документи, що оформлюються за результатами державної	ОК 23						

Трудові функції	Компетентності	Знання	ОК	Уміння та навички	ОК	Комунікація	ОК	Відповідальність і автономія	ОК
		експертизи комплексних систем захисту інформації та засобів технічного захисту інформації							
	Здатність проводити оцінку відповідності систем управління інформаційною безпекою	Б3.31. Поняття оцінки відповідності систем управління інформаційною безпекою	ОК 21	Б3.У1. Здійснювати оцінку відповідності (брати участь в оцінці відповідності) систем управління інформаційною безпекою відповідно до стандартів ДСТУ ISO/IEC серії 27k	ОК 21	Б3.К1. Взаємодіяти з аудиторами, керівництвом та відповідальними підрозділами під час проведення оцінки відповідності СУІБ	ОК 21	Б3.В1. Самостійно або у складі команди здійснювати оцінку відповідності СУІБ та нести відповідальність за об’єктивність і коректність висновків відповідно до стандартів ДСТУ ISO/IEC 27k	ОК 21
		Б3.32. Порядок, умови та організація проведення оцінки відповідності систем управління інформаційною безпекою	ОК 21	Б3.У2. Аналізувати політику та конфігурації систем управління інформаційною безпекою організації та оцінювати її відповідність нормативним актам і документам з питань безпеки інформації та кібербезпеки	ОК 21	Б3.К2. Взаємодіяти з керівництвом та відповідальними підрозділами під час аналізу політик і конфігурацій СУІБ та узгодження результатів оцінювання відповідності	ОК 21	Б3.В2. Самостійно аналізувати політики та конфігурації СУІБ і нести відповідальність за обґрунтованість висновків щодо відповідності нормативним вимогам	ОК 21
		Б3.33. Документи, що оформлюються за результатами оцінки відповідності систем управління інформаційною безпекою	ОК 21	Б3.У3. Аналізувати проєктні обмеження, компроміси та детальний проєкт системи управління інформаційною безпекою організації	ОК 21	Б3.К3. Координувати взаємодію з проєктними командами та керівництвом щодо аналізу обмежень і компромісів СУІБ	ОК 21	Б3.В3. Самостійно аналізувати проєкт СУІБ та нести відповідальність за обґрунтованість оцінки проєктних рішень і компромісів	ОК 21
				Б3.У4. Оцінювати ефективність заходів із захисту інформації, заходів з режиму та	ОК 21	Б3.К4. Взаємодіяти з відповідальними підрозділами щодо результатів оцінки	ОК 21	Б3.В4. Самостійно оцінювати ефективність заходів захисту інформації	м

Трудові функції	Компетентності	Знання	ОК	Уміння та навички	ОК	Комунікація	ОК	Відповідальність і автономія	ОК
				управління доступом, заходів з кібербезпеки, які використовуються системою управління інформаційною безпекою організації		ефективності заходів безпеки		та нести відповідальність за об'єктивність результатів оцінювання	
				Б3.У5. Переконуватися, що усі операції з безпеки та їх технічна підтримка належним чином задокументовані та оновлюються в разі необхідності	ОК 22	Б3.К5. Координувати дії з адміністраторами та власниками процесів для забезпечення актуальності документації з безпеки	ОК 22	Б3.В5. Самостійно контролювати повноту та актуальність документації операцій безпеки і нести відповідальність за її відповідність вимогам СУІБ	ОК 22
				Б3.У6. Переконуватися, що вимоги із захисту інформації та кібербезпеки інтегровані в планування безперервного функціонування системи та/або організації	ОК 22	Б3.К6. Взаємодіяти з керівництвом та підрозділами бізнес-неперервності щодо інтеграції вимог кібербезпеки у плани відновлення	ОК 22	Б3.В6. Самостійно перевіряти інтеграцію вимог безпеки в плани безперервності та нести відповідальність за їх повноту й узгодженість	ОК 22
				Б3.У7. Здійснювати точну технічну оцінку програмного забезпечення прикладних програм, СУІБ чи мережі, а також реалізованих заходів із кіберзахисту вимогам кібербезпеки та можливим вразливостям	ОК 22	Б3.К7. Координувати взаємодію з технічними фахівцями під час проведення технічної оцінки систем і засобів кіберзахисту	ОК 22	Б3.В7. Самостійно здійснювати технічну оцінку систем і нести відповідальність за точність виявлення вразливостей та відповідність вимогам кібербезпеки	ОК 22
				Б3.У8. Оформлювати документи за результатами оцінки відповідності систем управління інформаційною безпекою	ОК 22	Б3.К8. Взаємодіяти з аудиторами та керівництвом щодо узгодження результатів оцінки відповідності СУІБ	ОК 22	Б3.В8. Самостійно оформлювати звітні документи за результатами оцінки відповідності та нести	ОК 22

Трудові функції	Компетентності	Знання	ОК	Уміння та навички	ОК	Комунікація	ОК	Відповідальність і автономія	ОК
								відповідальність за їх повноту і достовірність	
В. Експлуатація та обслуговування систем і комплексів захисту інформації, моніторинг та аудит загроз для інформації	Здатність підтримувати системи та комплекси захисту інформації у робочому стані, оцінювати їх надійність та здійснювати контроль їх працездатності та виявлення місць відмов та інцидентів	В1.З1. Принципи взаємодії «людина-комп'ютер»	ОК 14	В1.У1. Здійснювати контроль працездатності комп'ютерних систем, систем і комплексів захисту інформації	ОК 21	В1.К1. Взаємодіяти з користувачами та технічними фахівцями щодо виявлених збоїв і стану працездатності систем захисту інформації	ОК 21	В1.В1. Самостійно здійснювати контроль працездатності систем і комплексів захисту інформації та нести відповідальність за своєчасне виявлення відмов і порушень їх роботи	ОК 21
		В1.З2. Загальні положення теорії надійності, методи діагностики працездатності та виявлення місця відмов у комп'ютерних системах, системах і комплексах захисту інформації	ОК 23	В1.У2. Діагностувати несправне апаратне забезпечення системи/сервера	ОК 23	В1.К2. Взаємодіяти з адміністраторами та технічним персоналом щодо результатів діагностики та стану апаратного забезпечення	ОК 23	В1.В2. Самостійно проводити діагностику несправного апаратного забезпечення та нести відповідальність за точність визначення причин відмов	ОК 23
		В1.З3. Принципи стійкості та надмірності в комп'ютерних системах і комплексах захисту інформації	ОК 23	В1.У3. Застосовувати засоби контролю працездатності та виявлення місця відмов	ОК 23	В1.К3. Координувати дії з технічними фахівцями під час застосування засобів моніторингу та контролю працездатності систем	ОК 23	В1.В3. Самостійно застосовувати засоби контролю працездатності та нести відповідальність за своєчасне виявлення відмов у системах	ОК 23
				В1.У4. Виявляти місця відмов у комп'ютерних системах, системах і комплексах захисту інформації	ОК 23	В1.К4. Взаємодіяти з адміністраторами систем для уточнення причин та локалізації відмов	ОК 23	В1.В4. Самостійно визначати місця відмов у системах і нести відповідальність за достовірність результатів діагностики	ОК 23

Трудові функції	Компетентності	Знання	ОК	Уміння та навички	ОК	Комунікація	ОК	Відповідальність і автономія	ОК
				В1.У5. Організовувати (проводити) ремонт апаратних засобів захисту інформації зі складу комплексних систем захисту інформації та комплексів технічного захисту інформації	ОК 23	В1.К5. Координувати роботи з ремонтними підрозділами та технічними фахівцями під час відновлення працездатності апаратних засобів	ОК 23	В1.В5. Самостійно організовувати або проводити ремонт апаратних засобів захисту інформації та нести відповідальність за відновлення їх працездатності	ОК 23
	Здатність проводити періодичне обслуговування інформаційних систем та мереж, комплексних систем захисту інформації та комплексів технічного захисту інформації	В2.31. Типи та періодичність планової підтримки апаратного забезпечення, періодичність підтримки та оновлення програмного забезпечення	ОК 22	В2.У1. Проводити чищення систем і мереж (фізичне й електронне), здійснювати перевірку дисків і завантажувальних програм, ізолювати та видаляти шкідливе програмне забезпечення	ОК 22	В2.К1. Взаємодіяти з користувачами та адміністраторами систем щодо проведення планового обслуговування та усунення виявлених загроз	ОК 22	В2.В1. Самостійно виконувати періодичне обслуговування систем і мереж та нести відповідальність за їх працездатність і безпеку під час проведення профілактичних робіт	ОК 22
		В2.32. Підходи щодо забезпечення безпеки віртуальних приватних мереж (VPN)	ОК 22	В2.У2. Виправляти фізичні та технічні проблеми, що впливають на роботу системи/сервера	ОК 22	В2.К2. Взаємодіяти з адміністраторами мереж та користувачами для уточнення технічних проблем і погодження дій з відновлення працездатності систем	ОК 22	В2.В2. Самостійно усувати фізичні та технічні несправності систем/серверів і нести відповідальність за відновлення їх стабільної роботи	ОК 22
				В2.У3. Встановлювати оновлення системи та компонентів (серверів, пристроїв, мережевих пристроїв)	ОК 22	В2.К3. Координувати оновлення з іншими адміністраторами та користувачами для мінімізації впливу на роботу системи	ОК 22	В2.В3. Самостійно встановлювати оновлення компонентів системи та нести відповідальність за їх коректність і безпеку	ОК 22

Трудові функції	Компетентності	Знання	ОК	Уміння та навички	ОК	Комунікація	ОК	Відповідальність і автономія	ОК
				В2.У4. Моніторити та оптимізувати роботу системи/сервера	ОК 22	В2.К4. Взаємодіяти з технічними фахівцями щодо результатів моніторингу та показників продуктивності систем	ОК 22	В2.В4. Самостійно здійснювати моніторинг та оптимізацію систем/серверів і нести відповідальність за їх продуктивність і стабільність	ОК 22
				В2.У5. Відновлювати системи/сервери після виявленого збою (програмне забезпечення для відновлення, відмовостійкі кластери, дублювання/«зеркалювання»)	ОК 22	В2.К5. Координувати дії з адміністраторами та підрозділами ІТ під час відновлення систем після збоїв	ОК 22	Самостійно відновлювати системи/сервери після збоїв і нести відповідальність за мінімізацію простоїв та втрат даних	ОК 22
				В2.У6. Здійснювати оновлення баз даних антивірусних програм, програмних механізмів захисту інформації	ОК 22	В2.К6. Взаємодіяти з користувачами та службами безпеки щодо оновлення засобів захисту та реагування на загрози	ОК 22	В2.В5. Самостійно оновлювати антивірусні бази та механізми захисту і нести відповідальність за актуальність засобів кіберзахисту	ОК 22
				В2.У7. Проводити періодичне обслуговування апаратних засобів захисту інформації зі складу комплексних систем захисту інформації та комплексів технічного захисту інформації	ОК 30	В2.К7. Координувати роботи з технічним персоналом під час профілактичного обслуговування апаратних засобів захисту	ОК 30	В2.В6. Самостійно виконувати періодичне обслуговування апаратних засобів захисту і нести відповідальність за їх працездатність та надійність	ОК 30
				В2.У8. Документувати та приводити у відповідність інформаційну безпеку організації, архітектуру кібербезпеки та вимоги техніки безпеки системи протягом всього	ОК 30	В2.К8. Координувати роботи з технічним персоналом під час профілактичного обслуговування апаратних засобів	ОК 30	В2.В7. Самостійно виконувати періодичне обслуговування апаратних засобів захисту і нести відповідальність за	ОК 30

Трудові функції	Компетентності	Знання	ОК	Уміння та навички	ОК	Комунікація	ОК	Відповідальність і автономія	ОК
				життєвого циклу системи		захисту		їх працездатність та надійність	
	Здатність виконувати попередній нескладний ремонт несправного апаратного забезпечення системи/сервера	В3.31. Методи (способи) тестування, оцінки та ремонту комп'ютерних систем, систем і комплексів захисту інформації	ОК 23	В3.У1. Здійснювати заходи з тестування елементів систем безпеки та ІКС	ОК 23	В3.К1. Взаємодіяти з адміністраторами та технічними фахівцями щодо результатів тестування та виявлених несправностей елементів систем безпеки	ОК 23	В3.В1. Самостійно проводити тестування елементів систем безпеки та ІКС і нести відповідальність за точність виявлення несправностей та коректність результатів перевірок	ОК 23
		В3.32. Інструменти діагностики систем і методик визначення несправностей	ОК 23	В3.У2. Діагностувати проблеми з підключенням	ОК 23	В3.К2. Взаємодіяти з користувачами та адміністраторами мереж для уточнення причин проблем з підключенням і узгодження шляхів їх усунення	ОК 23	В3.В2. Самостійно діагностувати проблеми з підключенням та нести відповідальність за точність визначення причин збоїв у мережевій взаємодії	ОК 23
		В3.33. Засоби та діагностики систем/серверів, методики визначення несправностей	ОК 21	В3.У3. Здійснювати інтегроване тестування системи безпеки та інформаційно-комп'ютерних систем	ОК 21	В3.К3. Координувати дії з технічними фахівцями під час проведення інтегрованого тестування систем безпеки	ОК 21	В3.В3. Самостійно здійснювати інтегроване тестування систем безпеки та ІКС і нести відповідальність за об’єктивність результатів перевірки	ОК 21
		В3.34. Види попереднього нескладного ремонту несправного апаратного забезпечення системи/сервера	ОК 21	В3.У4. Виконувати попередній нескладний ремонт несправного апаратного забезпечення системи/сервера	ОК 21	В3.К4. Взаємодіяти з адміністраторами та технічним персоналом щодо виявлених несправностей і виконаного ремонту	ОК 21	В3.В4. Самостійно виконувати попередній нескладний ремонт апаратного забезпечення та нести	ОК 21

Трудові функції	Компетентності	Знання	ОК	Уміння та навички	ОК	Комунікація	ОК	Відповідальність і автономія	ОК
						апаратного забезпечення		відповідальність за відновлення його працездатності	
		В3.35. Технічні регламенти та специфікації відповідного ремонту	ОК 21	В3.У5. Виконувати ремонт систем і комплексів захисту інформації	ОК 21	В3.К5. Узгоджувати з технічними фахівцями та відповідальними особами порядок і результати ремонту систем захисту інформації	ОК 21	В3.В5. Самостійно виконувати ремонт систем і комплексів захисту інформації та нести відповідальність за їх подальшу працездатність і відповідність технічним регламентам	ОК 21
		В3.36. Прилади та інструменти, програмне забезпечення, необхідні для проведення попереднього нескладного ремонту несправного апаратного забезпечення системи/сервера, апаратних засобів захисту інформації	ОК 21	В3.У6. Здійснювати усунення неполадок і діагностування аномалій функціонування інфраструктури системи безпеки на основі її аналізу	ОК 21	В3.К6. Взаємодіяти з адміністраторами систем і фахівцями з кібербезпеки для аналізу та усунення інфраструктурних збоїв	ОК 21	В3.В6. Самостійно здійснювати діагностику та усунення аномалій інфраструктури системи безпеки і нести відповідальність за стабільність її функціонування	ОК 21
	Здатність здійснювати контроль за станом технічного та криптографічного захисту інформації	В4.31. Поняття та зміст контролю за станом технічного та криптографічного захисту інформації	ОК 15	В4.У1. Організовувати (приймати участь в організації) контроль за станом технічного та криптографічного захисту інформації	ОК 15	В4.К1. Взаємодіяти з адміністраторами, фахівцями з ТЗІ та криптографічного захисту, а також керівництвом щодо планування та проведення контрольних заходів	ОК 15	В4.В1. Самостійно або в складі групи організовувати контроль стану технічного та криптографічного захисту інформації та нести відповідальність за повноту та своєчасність проведення контрольних процедур	ОК 15
		В4.32. Методи контролю за станом технічного та криптографічного захисту	ОК 15	В4.У2. Перевіряти виконання вимог нормативно-правових	ОК 15	В4.К2. Взаємодіяти з відповідальними підрозділами та	ОК 15	В4.В2. Самостійно перевіряти виконання вимог	ОК 15

Трудові функції	Компетентності	Знання	ОК	Уміння та навички	ОК	Комунікація	ОК	Відповідальність і автономія	ОК
		інформації		актів і нормативних документів з технічного та криптографічного захисту інформації на підприємстві/в організації		посадовими особами щодо результатів перевірки дотримання вимог нормативних документів		нормативно-правових актів і нести відповідальність за об'єктивність і точність результатів контролю	
		В4.33. Організація та порядок здійснення контролю за станом технічного та криптографічного захисту інформації	ОК 15	В4.У3. Застосовувати засоби контролю захищеності інформації	ОК 15	В4.К3. Координувати дії з технічними фахівцями під час застосування засобів контролю захищеності інформації	ОК 15	В4.В3. Самостійно застосовувати засоби контролю захищеності інформації та нести відповідальність за коректність отриманих результатів	ОК 15
		В4.34. Інструментарій контролю за станом технічного та криптографічного захисту інформації	ОК 15	В4.У4. Користуватися інструментарієм контролю за станом технічного та криптографічного захисту інформації	ОК 15	В4.К4. Взаємодіяти з адміністраторами та фахівцями з безпеки щодо використання інструментарію контролю та інтерпретації результатів	ОК 15	В4.В4. Самостійно використовувати інструментарій контролю та нести відповідальність за точність вимірювань і результатів перевірки	ОК 15
				В4.У5. Визначати стан технічного та криптографічного захисту інформації на підприємстві/в організації	ОК 15	В4.К5. Узгоджувати з керівництвом та відповідальними підрозділами висновки щодо стану захисту інформації	ОК 15	В4.В5. Самостійно визначати стан технічного та криптографічного захисту інформації та нести відповідальність за обґрунтованість висновків	ОК 15
				В4.У6. Оформлювати документи за результатами контролю стану технічного та криптографічного захисту інформації на підприємстві/в організації	ОК 15	В4.К6. Взаємодіяти з керівництвом і службами безпеки щодо узгодження та затвердження документів за результатами	ОК 15	В4.В6. Самостійно оформлювати результати контролю та нести відповідальність за повноту, точність і відповідність	ОК 15

Трудові функції	Компетентності	Знання	ОК	Уміння та навички	ОК	Комунікація	ОК	Відповідальність і автономія	ОК
						контролю		документів нормативним вимогам	
	Здатність здійснювати постійний моніторинг та аудит загроз для інформації та відповідну модернізацію (доробку) систем і комплексів захисту інформації	В5.31. Методи та технології моніторингу та аудиту загроз для конфіденційності, цілісності та доступності інформації	ОК 30	В5.У1. Здійснювати моніторинг та аудит загроз для інформації в інформаційних системах та мережах та оцінку ризиків безпеки інформації	ОК 30	В5.К1. Взаємодіяти з адміністраторами систем, аналітиками кібербезпеки та керівництвом щодо результатів моніторингу, аудиту та оцінки ризиків	ОК 30	В5.В1. Самостійно здійснювати моніторинг та аудит загроз для інформації і нести відповідальність за своєчасність виявлення ризиків та обґрунтованість їх оцінки	ОК 30
		В5.32. Методи, засоби та інформаційні технології виявлення несанкціонованого доступу до інформації на різних ієрархічних рівнях інформаційно-комунікаційної системи	ОК 30	В5.У2. Здійснювати моніторинг та аудит загроз для інформації, що озвучується	ОК 30	В5.К2. Взаємодіяти з користувачами та відповідальними особами щодо фіксації та аналізу загроз для інформації, що озвучується, та можливих інцидентів	ОК 30	В5.В2. Самостійно здійснювати моніторинг та аудит загроз і нести відповідальність за виявлення несанкціонованого доступу та коректність оцінки загроз	ОК 30
		В5.33. Класифікація контрзаходів для виявлених ризиків безпеки інформації	ОК 30	В5.У3. Використовувати інструменти та технології безперервного моніторингу з метою оцінки ризиків, користуватися прикладними програмами моніторингу та аудиту загроз для інформації в інформаційних системах та мережах	ОК 30	В5.К3. Координувати дії з аналітиками кібербезпеки та адміністраторами систем під час використання інструментів моніторингу та оцінки ризиків	ОК 30	В5.В3. Самостійно застосовувати інструменти безперервного моніторингу та нести відповідальність за своєчасність виявлення та оцінки ризиків	ОК 30
		В5.34. Інструментарій (прикладні програми) моніторингу (аудиту) загроз для інформації в інформаційних системах та мережах	ОК 30	В5.У4. Проводити аудити/огляди систем і комплексів захисту інформації (систем безпеки інформації) та інформаційно-комунікаційних систем	ОК 30	В5.К4. Взаємодіяти з технічними фахівцями та керівництвом щодо результатів аудитів і оглядів систем захисту інформації	ОК 30	В5.В4. Самостійно проводити аудити та огляди систем безпеки і нести відповідальність за об’єктивність і повноту висновків	ОК 30

Трудові функції	Компетентності	Знання	ОК	Уміння та навички	ОК	Комунікація	ОК	Відповідальність і автономія	ОК
		В5.35. Способи модернізації (доробки) систем і комплексів ОК 30захисту інформації відповідно до виявлених актуальних загроз для інформації		В5.У5. Здійснювати модернізацію (доробку) систем і комплексів захисту інформації відповідно до виявлених актуальних загроз для інформації	ОК 30	В5.К5. Узгоджувати з розробниками та адміністраторами напрямки модернізації систем захисту інформації відповідно до виявлених загроз	ОК 30	В5.В5. Самостійно здійснювати модернізацію систем захисту інформації та нести відповідальність за їх актуальність і ефективність проти загроз	м
				В5.У6. Використовувати відповідні інструменти для відновлення програмного, апаратного та периферійного обладнання системи	ОК 13	В5.К6. Координувати дії з адміністраторами під час відновлення працездатності системного обладнання	ОК 13	В5.В6. Самостійно застосовувати інструменти відновлення та нести відповідальність за відновлення працездатності системи	ОК 13
				В5.У7. Здійснювати визначення, модифікацію та маніпулювання з відповідними системними компонентами у ОС Windows, Unix або Linux (паролі, облікові записи користувачів, файли)	ОК 13	В5.К7. Взаємодіяти з адміністраторами систем та фахівцями з безпеки щодо налаштування облікових записів і системних компонентів	ОК 13	В5.В7. Самостійно виконувати модифікацію системних компонентів та нести відповідальність за безпеку та коректність налаштувань ОС	ОК 13
				В5.У8. Співпрацювати із системними аналітиками, інженерами, програмістами, з метою отримання інформації про обмеження та можливості системи, вимог до продуктивності та інтерфейсів, шляхів модернізації систем і комплексів захисту інформації	ОК 13	В5.К8. Активно взаємодіяти з міждисциплінарним и командами для отримання вимог, обмежень і технічних рішень щодо модернізації систем	ОК 13	В5.В8. Самостійно брати участь у процесах модернізації та нести відповідальність за врахування технічних вимог і обмежень при розвитку систем захисту інформації	ОК 13
	Здатність проводити процедури сканування	В6.31. Інструментарій сканування та розпізнавання	ОК 30	В6.У1. Проводити сканування вразливостей і	ОК 30	В6.К1. Взаємодіяти з адміністраторами	ОК 30	В6.В1. Самостійно проводити	ОК 30

Трудові функції	Компетентності	Знання	ОК	Уміння та навички	ОК	Комунікація	ОК	Відповідальність і автономія	ОК
	вразливостей і розпізнавання вразливостей в системах безпеки	вразливостей у системах безпеки для інформації в інформаційних системах і мережах		розпізнання вразливостей в ІКС і системах безпеки		систем та фахівцями з кібербезпеки щодо проведення сканування та аналізу виявлених вразливостей		сканування та розпізнавання вразливостей і нести відповідальність за достовірність результатів аналізу безпеки систем	
		В6.32. Способи сканування розпізнавання вразливостей у системах безпеки для інформації в інформаційних системах і мережах	ОК 30	В6.У2. Виявляти проблеми кібербезпеки, безпеки інформації і приватності, які виникають при з'єднаннях внутрішніх і зовнішніх замовників та організацій-партнерів на основі аналізу даних вразливостей і конфігурації інформаційно-комунікаційних систем і мереж	ОК 30	В6.К2. Координувати взаємодію з внутрішніми та зовнішніми партнерами щодо усунення виявлених проблем кібербезпеки та конфігураційних недоліків	ОК 30	В6.В2. Самостійно виявляти проблеми кібербезпеки та нести відповідальність за обґрунтованість висновків щодо ризиків взаємодії інформаційних систем і мереж	ОК 30
Г. Оцінювання відповідності програмних та апаратних засобів технічного та криптографічного захисту інформації	Здатність проводити оцінку відповідності (державну експертизу) програмних засобів технічного та криптографічного захисту інформації	Г1.31. Загальні способи оцінювання відповідності програмних засобів технічного захисту інформації	ОК 23	Г1.У1. Складати програму та методику проведення державної експертизи програмних засобів технічного захисту інформації	ОК 23	Г1.К1. Взаємодіяти з експертами, розробниками та замовниками під час підготовки та погодження програми і методики державної експертизи програмних засобів ТЗІ	ОК 23	Г1.В1.Самостійно складати програму та методику державної експертизи програмних засобів ТЗІ та нести відповідальність за їх відповідність нормативним вимогам і повноту оцінювання	ОК 23
		Г1.32. Поняття державної експертизи програмних засобів технічного захисту інформації	ОК 23	Г1.У2. Проводити експертні випробування та дослідження програмних засобів технічного захисту інформації (оцінювати функціональні послуги	ОК 23	Г1.К2. Взаємодіяти з експертами та розробниками програмних засобів під час проведення випробувань і оцінювання	ОК 23	Г1.В2. Самостійно проводити експертні випробування програмних засобів ТЗІ та нести відповідальність за об’єктивність оцінки	ОК 23

Трудові функції	Компетентності	Знання	ОК	Уміння та навички	ОК	Комунікація	ОК	Відповідальність і автономія	ОК
				безпеки, оцінювати рівні гарантій коректності реалізації функціональних послуг безпеки)		функціональних послуг безпеки		рівнів гарантій безпеки	
		Г1.33. Порядок та організація проведення державної експертизи програмних засобів технічного захисту інформації	ОК 9	Г1.У3. Оцінювати відповідність програмних засобів технічного захисту інформації задекларованим характеристикам та вимогам нормативних документів системи технічного захисту інформації	ОК 9	Г1.К3. Координувати взаємодію з замовниками та експертними групами щодо результатів оцінки відповідності програмних засобів ТЗІ	ОК 9	Г1.В3. Самостійно оцінювати відповідність програмних засобів ТЗІ та нести відповідальність за достовірність експертних висновків	ОК 9
		Г1.34. Поняття та загальний зміст програми та методики проведення державної експертизи програмних засобів технічного захисту інформації	ОК 9	Г1.У4. Виконувати безпечне тестування, огляд та/або оцінку програм, щоб виявити потенційні недоліки в кодах і пом'якшити вразливості	ОК 9	Г1.К4. Взаємодіяти з розробниками програмного забезпечення щодо результатів тестування та рекомендацій із усунення вразливостей	ОК 9	Г1.В4. Самостійно проводити безпечне тестування програмних засобів та нести відповідальність за коректність виявлення вразливостей і недоліків коду	ОК 9
		Г1.35. Техніко-технологічне, комп'ютерне, програмне та інше забезпечення оцінювання відповідності програмних засобів технічного захисту інформації	ОК 9	Г1.У5. Оформлювати протоколи експертних випробувань та експертні висновки за результатами державної експертизи та організовувати їх затвердження і реєстрацію	ОК 9	Г1.К5. Взаємодіяти з експертними органами та керівництвом щодо погодження, затвердження та реєстрації експертних висновків	ОК 9	Г1.В5. Самостійно оформлювати протоколи та експертні висновки й нести відповідальність за їх повноту, точність і відповідність нормативним вимогам	ОК 9
		Г1.36. Документи, що оформлюються за результатами державної експертизи програмних засобів технічного захисту інформації	ОК 9						
	Здатність проводити	Г2.31. Загальні способи	ОК	Г2.У1. Складати програму	ОК	Г2.К1. Взаємодіяти	ОК	Г2.В1. Самостійно	ОК

Трудові функції	Компетентності	Знання	ОК	Уміння та навички	ОК	Комунікація	ОК	Відповідальність і автономія	ОК
	оцінку відповідності (державну експертизу, сертифікацію) апаратних засобів технічного та криптографічного захисту інформації	оцінювання відповідності апаратних засобів технічного та криптографічного захисту інформації	15	та методику проведення державної експертизи апаратних засобів технічного захисту інформації	15	з експертами, виробниками та замовниками під час підготовки та погодження програми і методики державної експертизи апаратних засобів ТЗІ	15	складати програму та методику державної експертизи апаратних засобів ТЗІ та нести відповідальність за їх відповідність нормативним вимогам і повноту оцінювання	15
		Г2.32. Поняття державної експертизи апаратних засобів технічного та криптографічного захисту інформації	ОК 15	Г2.У2. Проводити експертні випробування та дослідження апаратних засобів технічного захисту інформації (склади схеми вимірювань характеристик засобів, вимірювати (визначати) функціональні характеристики засобів)	ОК 15	Г2.К2. Взаємодіяти з експертами та технічними спеціалістами під час проведення випробувань і вимірювання характеристик апаратних засобів ТЗІ	ОК 15	Г2.В2. Самостійно проводити експертні випробування апаратних засобів ТЗІ та нести відповідальність за точність вимірювань і достовірність результатів досліджень	ОК 15
		Г2.33. Порядок, умови та організація проведення державної експертизи апаратних засобів технічного та криптографічного захисту інформації	ОК 15	Г2.У3. Оцінювати відповідність апаратних засобів технічного захисту інформації задекларованим характеристикам та вимогам нормативних документів системи технічного захисту інформації	ОК 15	Г2.К3. Координувати взаємодію з виробниками, замовниками та експертними органами щодо оцінки відповідності апаратних засобів ТЗІ	ОК 15	Г2.В3. Самостійно оцінювати відповідність апаратних засобів ТЗІ та нести відповідальність за обґрунтованість експертних висновків	ОК 15
		Г2.34. Поняття та загальний зміст програми та методики проведення державної експертизи апаратних засобів технічного та криптографічного захисту інформації	ОК 15	Г2.У4. Оформлювати протоколи експертних випробувань та експертні висновки за результатами державної експертизи та організовувати їх затвердження і реєстрацію	ОК 15	Г2.К4. Взаємодіяти з експертними органами та відповідальними особами щодо погодження, затвердження та реєстрації експертних	ОК 15	Г2.В4. Самостійно оформлювати протоколи експертних випробувань та експертні висновки і нести відповідальність за їх повноту, точність	ОК 15

Трудові функції	Компетентності	Знання	ОК	Уміння та навички	ОК	Комунікація	ОК	Відповідальність і автономія	ОК
						висновків		та відповідність нормативним вимогам	
		Г2.35. Техніко-технологічне, комп'ютерне, програмне та інше забезпечення оцінювання відповідності апаратних засобів технічного та криптографічного захисту інформації	ОК 15						
		Г2.36. Засоби вимірювальної техніки та методики вимірювань оцінюваних показників апаратних засобів технічного та криптографічного захисту інформації	ОК 15						
		Г2.37. Документи, що оформлюються за результатами державної експертизи апаратних засобів технічного та криптографічного захисту інформації	ОК 15						
		Г2.38. Загальні поняття сертифікації апаратних засобів технічного та криптографічного захисту інформації	ОК 15						

Гарант ОП *підписано* **Вячеслав ЛИМАРЕНКО**

ЛИСТ ПОГОДЖЕННЯ
Освітньо-професійної програми «Кібербезпека»

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

uken Uniwersytet Komisji Edukacji Narodowej w Krakowie

РЕЦЕНЗІЯ
на освітньо-професійну програму «Кібербезпека»
першого (бакалаврського) рівня вищої освіти
за спеціальністю F5 - Кібербезпека
галузі знань F - Інформаційні технології
Харківського національного економічного університету ім. Семена Кузнеця

У сучасних умовах цифровізації зростає потреба у фахівцях з кібербезпеки, які володіють фундаментальними знаннями та практичними навичками. Представлена ОПП «Кібербезпека» бакалаврського рівня Харківського національного економічного університету ім. Семена Кузнеця орієнтована на формування базових компетенцій, необхідних для роботи в ІТ-безпеці.

Програма охоплює такі ключові напрями:

- основи інформаційної безпеки та захисту даних;
- адміністрування комп'ютерних мереж і виявлення вразливостей;
- базові принципи криптографії та захисту програмного забезпечення.

Навчальний план включає як теоретичні дисципліни, так і практичні модулі, що сприяє засвоєнню знань та формуванню професійних навичок.

ОПП «Кібербезпека» відповідає сучасним стандартам освіти та забезпечує необхідний рівень підготовки для подальшого навчання або роботи в галузі кібербезпеки.

ОПП містить перелік навчальних компонентів та опис їх логічних зв'язків, матрицю забезпечення результатів навчання компонентами ОПП, визначення форми атестації здобувачів. Це дозволяє зробити висновок про зміст навчання за ОПП.

ОПП «Кібербезпека» першого (бакалаврського) рівня вищої освіти за спеціальністю F5-Кібербезпека галузі знань F-Інформаційні технології Харківського національного економічного університету ім. Семена Кузнеця є актуальною, відповідає вимогам підготовки здобувача вищої освіти рівня бакалавр.

Професор кафедри комп'ютерної інженерії та кібербезпеки
Університет комісії Національної світи в Кракові (Польща)

д.т.н. Анна КОРЧЕНКО

Pełnomocnik Rektora
ds. Rozwoju Dyscypliny
Informatyka Techniczna i Telekomunikacja
dr hab. Serhii Semenov

ТОВ «Спарта РобоТек»
Україна, 61072, Харківська обл.,
м. Харків,
вул. Олеся Олександра, б. 10
к.т. +38067-972-7000
spartarobotech@gmail.com

РЕЦЕНЗІЯ-ВІДГУК
на освітньо-професійну програму «Кібербезпека» спеціальності F5 Кібербезпека та захист інформації першого (бакалаврського) рівня вищої освіти у Харківському національному економічному університеті ім. С. Кузнеця

Кібербезпека – це сукупність процесів, технологій і практик, спрямованих на захист комп'ютерних систем, мереж, програм, пристроїв і даних від несанкціонованого доступу, кібератак, пошкоджень або знищення. Кібербезпека є критично важливою для державних установ, підприємств, банків, медичних закладів та будь-яких організацій, які працюють з конфіденційною інформацією. В умовах війни, яка ведеться проти нашої держави втому числі і на інформаційному фронті, важко переоцінити важливість кібербезпеки, як напрямку підготовки ІТ-спеціалістів.

Освітня програма «Кібербезпека», що реалізується на кафедрі Кібербезпеки та інформаційних технологій Харківського національного економічного університету імені Семена Кузнеця, є однією з найсильніших у регіоні за глибиною, практичною цінністю та сучасністю змісту.

Програма повністю відповідає викликам часу й орієнтована на підготовку висококваліфікованих фахівців, здатних ефективно працювати в умовах зростаючих кіберзагроз як у державному, так і в приватному секторі.

Особливо варто відзначити:

– комплексний підхід до навчання – студенти отримують знання з технічного захисту інформації, криптографії, управління інформаційною безпекою, кіберрозвідки, цифрової криміналістики та інших важливих напрямів;

– високий рівень викладацького складу – викладачі кафедри мають глибокі наукові знання, практичний досвід та тісні зв'язки з ІТ-індустрією й безпековими структурами;

– сучасна матеріально-технічна база – навчальні лабораторії оснащені всім необхідним для моделювання кіберінцидентів, аналізу загроз та проведення практичних занять;

– практична орієнтованість – студенти залучаються до участі в хакатонах, наукових конференціях, проходять стажування в ІТ-компаніях і профільних установах, зокрема у сфері державної безпеки.

Програма не лише формує ґрунтовні технічні компетентності, а й розвиває критичне мислення, навички командної роботи та аналітичного підходу до вирішення проблем.

Рекомендуємо освітню програму «Кібербезпека» спеціальності F5 Кібербезпека та захист інформації першого (бакалаврського) рівня вищої освіти, що провадиться на кафедрі Кібербезпеки та інформаційних технологій ХНЕУ ім. С. Кузнеця, всім, хто прагне здобути актуальну професію з великим майбутнім і зробити свій внесок у безпеку цифрового суспільства.

Директор ТОВ
«Спарта РобоТек» Наталія ХИЖНЯК

KHARKIV IT CLUSTER

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

Рецензія

на освітньо-професійну програму «Кібербезпека» за спеціальністю F5 «Кібербезпека та захист інформації» першого (бакалаврського) рівня вищої освіти в Харківському національному економічному університеті імені Семена Кузнеця

Ознайомившись з поданою на рецензування освітньо-професійною програмою «Кібербезпека» першого (бакалаврського) рівня вищої освіти в Харківському національному економічному університеті імені Семена Кузнеця можемо відзначити, що наповнення ОП відповідає визначеній цілі навчання щодо «підготовки фахівців, здатних використовувати й впроваджувати технології інформаційної та/або кібербезпеки, а також технологій цифрової економіки». Це чітко відповідає очікуванням ІТ-галузі щодо поєднання технічних компетенцій і цифрової грамотності.

Унікальність програми полягає в інтегруванні курсів з програмування та кібербезпеки, що формує конкурентоспроможні компетентності випускника, а можливість обирати майнор чи вільні майнори дозволяє студентам поглиблювати знання у суміжних галузях.

Позитивними сторонами освітньої програми є комплексність фундаментальної підготовки, що забезпечується такими освітніми компонентами , як математика, алгоритми, структури даних і програмування. Це створює міцний базис для розуміння алгоритмічних та криптографічних методів захисту даних. А також тим, що ОП охоплює класичні напрямки кібербезпеки (мережі, операційні системи, аудит безпеки, криптографія, управління інцидентами), що відповідає потребам найбільших ІТ-підприємств і державних структур. Наявність кіберполігону, курсових проєктів, переддипломної й виробничої практик забезпечує студентам безпосередній досвід застосування інструментів захисту інформації.

Тож, дана освітня програма вже має міцну основу, проте для її вдосконалення рекомендуємо розглянути певні напрями покращення. Це підвищить привабливість освітньої програми університету та сприятиме формуванню сильної школи кібербезпеки у Харкові.

Рекомендації щодо вдосконалення:

1. Впровадити курс «Методи машинного навчання в кібербезпеці» із практичними лабораторіями з аналізу аномалій та поведінкового виявлення загроз.
2. Посилити блок пентестингу та форензіки окремим практикумом «Етичний хакінг» і «Цифрова криміналістика» з використанням Kali Linux, Metasploit та інструментів збору доказів.
3. Розвинути soft skills та підприємницькі компетенції через курс «Командна робота й ділова комунікація в ІТ», що включатиме презентаційні тренінги, переговорні кейси та основи кіберстартапів.

Загалом, програма «Кібербезпека» першого (бакалаврського) рівня вищої освіти в Харківському національному економічному університеті імені Семена Кузнеця має міцну фундаментальну базу, актуальні профільні дисципліни та добре організовану практичну підготовку, що відповідає вимогам ІТ-галузі та державних структур. Інтеграція програмування з курсами з кібербезпеки й можливість обирати майнори забезпечують конкурентоздатні компетенції випускників. Водночас впровадження курсів з машинного навчання в кібербезпеці, поглиблення навичок етичного хакінгу і цифрової криміналістики, а також розвиток soft skills і підприємницьких компетенцій зроблять програму ще більш привабливою та сучасною. Реалізація цих рекомендацій сприятиме подальшому зміцненню позицій ХНЕУ ім. С. Кузнеця як провідного центру у підготовці фахівців з кібербезпеки в регіоні.

Виконавчий директор
ГС «Харківський кластер
інформаційних технологій» Ольга ШАПОВАЛ

2026 рік

РЕЦЕНЗІЯ
НА ОСВІТНЬО-ПРОФЕСІЙНУ ПРОГРАМУ
«КІБЕРБЕЗПЕКА»
ПЕРШОГО (БАКАЛАВРСЬКОГО) РІВНЯ ВИЩОЇ ОСВІТИ
ЗА СПЕЦІАЛЬНІСТЮ «*F5 КІБЕРБЕЗПЕКА ТА ЗАХИСТ ІНФОРМАЦІЇ*»
«ХАРКІВСЬКОГО НАЦІОНАЛЬНОГО ЕКОНОМІЧНОГО УНІВЕРСИТЕТУ
ім.. СЕМЕНА КУЗНЕЦЯ»

Компанія EPAM є найбільшою та найвідомішою IT-компанією України. Вона впевнено очолює різні рейтинги за кількістю та якістю фахівців, які співпрацюють з компанією (понад 14 тис. фахівців). В той же час, в останні роки спостерігається тренд збільшення кількості та складності проектів, до яких долучаються фахівці компанії, що в свою чергу збільшує попит компанії на підготовку якісних фахівців. Рішення цього завдання компанія бачить у активній співпраці з навчальними закладами. З цього погляду підготовка якісних фахівців на кафедрі кібербезпеки та інформаційних технологій Харківського Національного Економічного Університету ім. Семена Кузнеця є актуальним завданням, що потребує тісної співпраці університету та компанії.

Можливості кафедри кібербезпеки та інформаційних технологій Харківського Національного Економічного Університету ім. Семена Кузнеця у підготовці якісних фахівців підкреслюються наявністю висококваліфікованого викладацького складу, серед яких можливо окремо виділити:

7 викладачів, що мають фаховий досвід співробітництва з провідними IT-компаніями або стартапами;

10 викладачів, що пройшли стажування у провідних IT-компаніях, та отримали відповідні сертифікати;

2 викладачів є сертифікованими фахівцями таких компаній як Microsoft, Google, Cisco, Oracle, AWS.

Харківський Національний Економічний Університет ім. Семена Кузнеця має відповідний досвід, розуміння культури інновацій, потужний кадровий потенціал та матеріально-технічну базу для виконання завдання підготовки IT-фахівців за обраним фокусом.

Проаналізувавши структуру програми та освітні компоненти, можна відзначити таке:

структура програми відповідає вимогам стандарту освіти у рамках спеціальності «F5 Кібербезпека та захист інформації;

структурно-логічна схема підготовки здобувачів вищої освіти пройшла спільну верифікацію представниками кафедри та спеціалістами компанії EPAM, що зафіксовано у відповідному протоколі засідання кафедри;

крім основних, стандартних форм навчання (лекції, практичні та лабораторні роботи, самостійна робота та ін.) у структурі програми передбачені інноваційні форми навчання, такі як самостійне та групове проектне навчання, комплексний

тренінг, ІТ-марафон.

Позитивною стороною освітньо-професійної програми є те що її розробка виконувалась співробітниками університету у співпраці з фахівцями компанії та ІТ-співтовариства:

зміст робочих програм та силабусів навчальних компонент «Технології програмування», «Основи стеганографічного захисту інформації» було верифіковано фахівцями компанії ЕРАМ, що зафіксовано у протоколі засідання кафедри;

побажання фахівців компанії щодо структурної та змістовної складових ОПП враховані та реалізовані у відповідних пунктах 4.1 та 4.3.

Висновки:

Зважаючи на позитивний досвід університету у підготовці фахівців, серед яких декілька осіб на поточний момент співпрацюють з компанією ЕРАМ та спираючись на результати рецензування вважаємо, що освітньо-професійна програма «КІБЕРБЕЗПЕКА» першого (бакалаврського) рівня вищої освіти за спеціальністю «F5 КІБЕРБЕЗПЕКА ТА ЗАХИСТ ІНФОРМАЦІЇ» ХАРКІВСЬКОГО НАЦІОНАЛЬНОГО ЕКОНОМІЧНОГО УНІВЕРСИТЕТУ ім. СЕМЕНА КУЗНЕЦЯ відповідає сучасним вимогам підготовки ІТ-фахівців та рекомендується до продовження терміну акредитації.

Заступник генерального директора
ТОВ "ЕПАМ СИСТЕМЗ" Надія БАБЕЙКО