Харківський національний економічний університет імені Семена Кузнеця
Кафедра кібербезпеки та інформаційних технологій

ЗАГАЛЬНА ПРОФЕСІЙНА (СЕРТИФІКАТНА) ПРОГРАМА
ПІДВИЩЕННЯ КВАЛІФІКАЦІЇ

ОРГАНІЗАЦІЙНЕ ЗАБЕЗПЕЧЕННЯ ЗАХИСТУ ІНФОРМАЦІЇ

(назва програми)

Шифр програми ЗП/2024/001

Рік запровадження програми 2024

Програму затверджено: Вченою радою Харківського національного економічного університету імені Семена Кузнеця від 23.02.2024 року № 2

Програму погоджено: наказ НАДС від 13 березня 2024 року № 46-24

ПРОФІЛЬ ПРОГРАМИ

1. Загальна інформація	
Назва програми	Організаційне забезпечення захисту інформації
Шифр програми	ЗП/2023/002
Тип програми за змістом	загальна професійна (сертифікатна) програма підвищення кваліфікації
Відомості про акредитацію для загальної професійної (сертифікатної) програми	
Форма навчання	дистанційна
Цільова група	державні службовці, які займають посади державної служби категорії «Б» та «В», посадові особи місцевого самоврядування, посади яких віднесено до 1-4 категорії посад органів місцевого самоврядування, депутати місцевих рад, що займаються обробленням інформації в інформаційно-комунікаційних системах
Передумови навчання за програмою	-
Найменування замовника освітніх послуг у сфері професійного навчання за програмою	-
Найменування партнера (партнерів) програми	-
Обсяг програми	2 кредити ЄКТС;
Тривалість програми та організація навчання	Тривалість програми становить 4 тижні (сесія 1 – перший тиждень, сесія 2 – другий тиждень, сесія 3, 4 – третій тиждень). Навчання відбувається три дні на тиждень з урахуванням запланованих годин для аудиторних та дистанційних занять
Мова(и) викладання	українська мова
Напрям(и) підвищення кваліфікації, який (які) охоплює програма	інформаційна безпека та захист персональних даних; кібербезпека
Перелік професійних компетентностей, на підвищення рівня яких спрямовано програму	знання законодавства у сфері забезпечення захисту інформації; професійні знання: знання стандартів Європейського Союзу у сфері забезпечення захисту інформації та заходів адаптації законодавства; знання принципів державної політики цифрового розвитку; знання засад і принципів державної політики у сфері інформаційної безпеки; знання інструментів та технологій комунікації; цифрова грамотність.
Укладач(і) програми	СТАРКОВА Ольга Володимирівна доктор технічних наук, професор, зав. кафедри кібербезпеки та інформаційних технологій, olha.starkova@hneu.net
2. Загальна мета	

отримання та удосконалення знань щодо проведення аналізу і оцінки загроз інформаційній безпеці об'єкта, оцінки збитків внаслідок протиправного розкриття інформації обмеженого доступу, організації і забезпечення режиму таємності, підбору, розстановки і роботи з кадрами	
3. Очікувані результати навчання	
За результатами навчання слухачі повинні демонструвати:	
знання	теоретичних основ законодавчої бази України та міжнародного суспільства в галузі національної та інформаційної безпеки, визначення основних вимог щодо формування підтримки та удосконалення систем управління інформаційної безпеки критичних інформаційно-комунікаційних систем.
уміння	впроваджувати процеси, що базуються на національних та міжнародних стандартах, виявлення, ідентифікації, аналізу та реагування на інциденти інформаційної та/або кібербезпеки; виконувати аналіз інформаційно-комунікаційних систем; вирішувати завдання захисту програм та інформації, що обробляється в інформаційно-комунікаційних системах та давати оцінку результативності якості прийнятих рішень; вирішувати задачі захисту інформації, що обробляється в інформаційно-комунікаційних системах, з використанням сучасних методів;
навички	здійснювати оцінювання можливості реалізації потенційних загроз інформації, що обробляється в інформаційно-комунікаційних системах та ефективності використання комплексів засобів захисту в умовах реалізації загроз різних класів; реалізовувати заходи з протидії отриманню несанкціонованого доступу до інформаційних ресурсів і процесів в інформаційних та інформаційно-комунікаційних (автоматизованих) системах; вирішувати задачі захисту потоків даних в інформаційних, інформаційно-комунікаційних (автоматизованих) системах; застосовувати теорії та методи захисту для забезпечення безпеки елементів інформаційно-комунікаційних систем; приймати участь у розробці та впровадженні стратегії інформаційної безпеки та/або кібербезпеки відповідно до цілей і завдань організації.
4. Викладання та навчання (методи навчання, форми проведення навчальних занять)	
Навчання здійснюється у дистанційному форматі у формі відеоконференцій, які включають проведення інтерактивних лекцій-презентацій, виконання індивідуально та в складі малих груп у окремих залах практичних завдань, дискусій у інтернет-чатах, самостійне вивчення нормативно-правової бази, що регулює цифрові процеси суспільства.	

5. Ресурсне забезпечення дистанційного навчання	
Назви вебплатформи, вебсайту, електронної системи навчання, через які здійснюватиметься дистанційне навчання із зазначенням посилання (вебадреси)	Платформа Moodle – сайт «Персональні навчальні системи» Харківського національного економічного університету ім. С. Кузнеця. Адреса: https://pns.hneu.edu.ua/ Платформа Zoom: https://zoom.us/
Назва дистанційного етапу/модуля	Відповідно до змісту програми
6. Оцінювання і форми поточного, підсумкового контролю	
Складові оцінювання та їх питома вага у підсумковій оцінці (%)	відвідування занять (дистанційно в синхронному режимі) – 10 %; поточний контроль – 60 %; підсумковий контроль – 30 %. Документ про підвищення кваліфікації видається за умови набрання учасником навчання не менше ніж 75 % обрахованих з урахуванням питомої ваги кожного із критеріїв оцінювання.
Форма та періодичність поточного контролю	комп'ютерне тестування після вивчення кожного модуля
Форма підсумкового контролю	комп'ютерне тестування

СТРУКТУРА ПРОГРАМИ

	Назва теми	Кількість годин				
		загальна кількість годин/ кредитів ЄКТС	у тому числі:			
			аудиторні заняття	дистанційні заняття	навчальні візити	самостійна робота слухачів
1	2	3	4	5	6	7
ОБОВ'ЯЗКОВІ МОДУЛІ ПРОГРАМИ (46 годин / 1,53 кредити ЄКТС)						
Сесія 1	Модуль 1. Роль організаційного забезпечення при здійсненні захисту інформації					
	Тема 1.1. Завдання організаційного забезпечення захисту інформації	9/0,3		7		2
	Тема 1.2. Організаційне забезпечення інформаційної безпеки	10/0,33		8		2
	Поточний контроль	1/0,03		1		
Сесія 2	Модуль 2. Заходи з організації забезпечення захисту інформації на підприємствах					
	Тема 2.1. Служба безпеки об'єкта	11/0,37		9		2
	Тема 2.2. Інформаційна безпека організації	14/0,47		12		2
	Поточний контроль	1/0,03		1		
ВИБІРКОВІ МОДУЛІ ПРОГРАМИ (вибирається один вибірковий модуль) (12 годин / 0,4 кредити ЄКТС)						
Сесія 3	Модуль 3. Ефективне управління інцидентами інформаційної безпеки за вимогами міжнародних стандартів					
	Тема 3.1. Менеджмент інциденту інформаційної безпеки	4/0,133		3		1
	Тема 3.2. Особливості менеджменту інцидентів за вимогами міжнародного стандарту ITIL	4/0,133		3		1
	Тема 3.3. Група реагування на інциденти інформаційної безпеки. Базові етапи створення груп CERT / CSIRT	3/0,1		2		1
	Поточний контроль	1/0,03		1		
	Модуль 4. Ризик-менеджмент інформаційної безпеки					
	Тема 4.1. Управління ризиками, міжнародні та державні стандарти	4/0,133		3		1
	Тема 4.2. Технології аналізу ризиків	4/0,133		3		1
	Тема 4.3. Інструментальні засоби аналізу ризиків. Аудит безпеки і аналіз ризиків	3/0,1		2		1
	Поточний контроль	1/0,03		1		
Сесія 4	Підсумковий контроль результатів навчання	2/0,07		2		
	РАЗОМ	60/2		49		11

ЗМІСТ ПРОГРАМИ

Обов'язкові модулі програми

Модуль 1. Роль організаційного забезпечення при здійсненні захисту інформації

Тема 1. Завдання організаційного забезпечення захисту інформації

Про концепцію інформаційної безпеки України. Основні задачі інформаційної безпеки. Джерела загроз інформаційній безпеці. Методи запобігання та ліквідації загроз інформаційній безпеці. Організаційні основи захисту інформації. Державна нормативно-правова база питань захисту інформації (Закони України «Про інформацію», «Про захист інформації в інформаційно-комунікаційних системах», «Про державну таємницю», «Про захист персональних даних»; Постанови Кабінету міністрів України «Про затвердження Правил забезпечення захисту інформації в інформаційних, електронних комунікаційних та інформаційно-комунікаційних системах», «Про затвердження Типової інструкції про порядок ведення обліку, зберігання, використання і знищення документів та інших матеріальних носіїв інформації, що містять службову інформацію»; нормативні документи в галузі технічного захисту інформації (НД ТЗІ) та державні стандарти України (ДСТУ) стосовно створення і функціонування КСЗІ).

Форми проведення навчальних занять та методи навчання, які дозволяють розкрити зміст теми: міні-лекція, тренінг, практична робота, тематична дискусія, аналіз ситуацій та розв'язання ситуаційних завдань.

Перелік питань, які виносяться на самостійну роботу:

Етапи розвитку засобів інформаційних комунікацій з урахуванням впливу на трансформацію ідей інформаційної безпеки. Типологія конфіденційності. Окремі аспекти інформаційної безпеки залежно від виду захисту інформації.

Тема 2. Організаційне забезпечення інформаційної безпеки

Суб'єкти інформаційного простору. Віднесення відомостей до різних видів конфіденційної інформації. Віднесення відомостей до комерційної таємниці. Віднесення відомостей до державної таємниці. Функції системи захисту інформації. Матриця розподілу доступу. Класичні моделі інформаційної безпеки. Модель розподілу інформаційних потоків. Організація системи інформаційної безпеки.

Форми проведення навчальних занять та методи навчання, які дозволяють розкрити зміст теми: міні-лекція, тренінг, практична робота, тематична дискусія, аналіз ситуацій та розв'язання ситуаційних завдань.

Перелік питань, які виносяться на самостійну роботу:

Управління паролями. Засоби збереження та доступу до паролів. Правила роботи з паролями.

Модуль 2. Заходи з організації забезпечення захисту інформації на підприємствах

Тема 1. Служба безпеки об'єкта

Організація доступу до таємної інформації. Захист службової інформації. Основні напрями захисту електронної інформації.

Форми проведення навчальних занять та методи навчання, які дозволяють розкрити зміст теми: міні-лекція, тренінг, практична робота, тематична дискусія, аналіз ситуацій та розв'язання ситуаційних завдань.

Перелік питань, які виносяться на самостійну роботу:

Захист інформації на мобільних телефонах. Огляд найпоширеніших мобільних вірусів та засобів боротьби з ними. Інформаційна безпека в соціальних мережах. Захист електронної пошти та власних акаунтів під час роботи в мережі.

Тема 2. Інформаційна безпека організації

Правила побудови системи інформаційної безпеки підприємства. Методи та засоби забезпечення інформаційної безпеки організації. Основи роботи з персоналом. Приймання на роботу нового співробітника. Робота з персоналом при звільнені. Навчання персоналу. Мотивація діяльності персоналу.

Форми проведення навчальних занять та методи навчання, які дозволяють розкрити зміст теми: міні-лекція, тренінг, практична робота, тематична дискусія, аналіз ситуацій та розв'язання ситуаційних завдань.

Перелік питань, які виносяться на самостійну роботу:

Забезпечення інформаційної безпеки підприємства/організації. Законодавчі вимоги і регулювання інформаційної безпеки.

Вибіркові модулі програми

Модуль 3. Ефективне управління інцидентами інформаційної безпеки за вимогами міжнародних стандартів

Тема 1. Менеджмент інциденту інформаційної безпеки

Короткий огляд проблеми управління ризиками. Етапи ефективного менеджменту інцидентів інформаційної безпеки за вимогами міжнародних стандартів ISO 27035 та ISO 18044.

Форми проведення навчальних занять та методи навчання, які дозволяють розкрити зміст теми: міні-лекція, тренінг, практична робота, тематична дискусія, аналіз ситуацій та розв'язання ситуаційних завдань.

Перелік питань, які виносяться на самостійну роботу:

Модель PDCA опису життєвого циклу процесів управління інцидентами інформаційної безпеки.

Тема 2. Особливості менеджменту інцидентів за вимогами міжнародного стандарту ITIL

Міжнародний стандарт ITIL. Менеджмент інцидентів відповідно до стандарту ITIL. Концепція побудови, структура та функціональні особливості ефективної системи менеджменту інцидентів ІБ.

Форми проведення навчальних занять та методи навчання, які дозволяють розкрити зміст теми: міні-лекція, тренінг, практична робота, тематична дискусія, аналіз ситуацій та розв'язання ситуаційних завдань.

Перелік питань, які виносяться на самостійну роботу:

Еволюція кіберзагроз. Критично важливі об'єкти інфраструктури України. Аналіз способів розгортання шкідливого ПЗ.

Тема 3. Група реагування на інциденти інформаційної безпеки. Базові етапи створення груп CERT / CSIRT

Поняття групи реагування на інциденти ІБ (CERT / CSIRT): історія розвитку та можливі вигоди підприємців. Узагальнена класифікація груп CERT / CSIRT: сфера діяльності, цілі та потенційні клієнти.

Інструменти для моніторингу та реєстрації інциденту. Інструменти для обробки інциденту. Інструменти для розслідування інциденту. Інструменти для контролю каналів зв'язку та веб-ресурсів.

Форми проведення навчальних занять та методи навчання, які дозволяють розкрити зміст теми: міні-лекція, тренінг, практична робота, тематична дискусія, аналіз ситуацій та розв'язання ситуаційних завдань.

Перелік питань, які виносяться на самостійну роботу:

Проблеми кібербезпеки в інтернеті речей. Основні причини кіберпорушень.

Модуль 4. Ризик-менеджмент інформаційної безпеки

Тема 1. Управління ризиками, міжнародні та державні стандарти

Міжнародний стандарт ISO 31000. Етапи процесу управління ризиками. Рамкова програма з кібербезпеки. Основні функції рамкової програми. Рівні впровадження рамкової програми. Встановлення або вдосконалення програми кібербезпеки. Серія стандартів ДСТУ ISO/IEC 270xx. Стандарт ДСТУ ISO/IEC 27005.

Форми проведення навчальних занять та методи навчання, які дозволяють розкрити зміст теми: міні-лекція, тренінг, практична робота, тематична дискусія, аналіз ситуацій та розв'язання ситуаційних завдань.

Перелік питань, які виносяться на самостійну роботу:

Система менеджменту інформаційної безпеки: орієнтовна послідовність дій при розробці, обов'язкові документи. Загальна політика інформаційної безпеки.

Тема 2. Технології аналізу ризиків

Аудит інформаційної безпеки. Дослідження стану інформаційно-комунікаційної системи. Дослідження інформаційного середовища інформаційно-комунікаційної системи. Дослідження фізичного середовища інформаційно-комунікаційної системи. Дослідження середовища користувачів. Тестування на уразливість інформаційно-комунікаційної системи. Методи оцінки ризиків. Практичний ризик-менеджмент.

Форми проведення навчальних занять та методи навчання, які дозволяють розкрити зміст теми: міні-лекція, тренінг, практична робота, тематична дискусія, аналіз ситуацій та розв'язання ситуаційних завдань.

Перелік питань, які виносяться на самостійну роботу:

Приклад структури (загальної і детальних) політик безпеки організації (для забезпечення мережевої безпеки). Приклад політики інформаційної безпеки. Приклади невдалих політик інформаційної безпеки. Фактори, що визначають ефективність політики безпеки.

Тема 3. Інструментальні засоби аналізу ризиків. Аудит безпеки і аналіз ризиків

Політика інформаційної безпеки. Ідентифікація та оцінка активів. Аналіз джерел проблем. Ролі та обов'язки щодо інформаційної безпеки. Якісна оцінка системи менеджменту інформаційної безпеки. Причини виникнення інцидентів. Специфічні питання управління інцидентами інформаційної безпеки. Політика розслідування інцидентів інформаційної безпеки.

Форми проведення навчальних занять та методи навчання, які дозволяють розкрити зміст теми: міні-лекція, тренінг, практична робота, тематична дискусія, аналіз ситуацій та розв'язання ситуаційних завдань.

Перелік питань, які виносяться на самостійну роботу:

Принципи ефективної політики реагування на інциденти.

ОЦІНЮВАННЯ РЕЗУЛЬТАТІВ НАВЧАННЯ

Оцінювання результатів навчання здійснюється за такими складовими:

відвідування дистанційних (в синхронному режимі) занять та активна участь під час таких занять (виступи, рефлексія, відповіді на запитання, швидке опитування тощо) – 10 %;

поточний контроль – 60 %;

підсумковий контроль – 30 %.

Підсумкова оцінка складається із суми всіх оцінок за кожною складовою оцінювання результатів навчання. Учасник професійного навчання отримує документ про підвищення кваліфікації, якщо набрав не менше 75 % від загального значення підсумкової оцінки.

Розподіл балів, які отримують слухачі курсу

Відвіду-вання занять	Поточне оцінювання							Комп'ютерне тестування	Сума
	Модуль 1		Модуль 2		Вибірковий модуль				
	Тема 1	Тема 2	Тема 1	Тема 2	Тема 1	Тема 2	Тема 3		
10	5	5	10	10	10	10	10	30	100

ЛІТЕРАТУРА, ІНФОРМАЦІЙНІ РЕСУРСИ, ОБОВ'ЯЗКОВІ ДЛЯ ОПРАЦЮВАННЯ8

1. Інформаційна безпека / за ред. Ю.Я. Бобала, І.В. Горбатого. Львів : Львівська політехніка, 2019. 580 с.
2. Хорошко В.О. Проектування комплексних систем захисту інформації. Львів : Львівська політехніка, 2020. 320 с.
3. Бурячок В.Л. Інформаційна та кібербезпека: соціотехнічний аспект : підручник. Львів: Магнолія, 2018. – 320 с.
4. Бурячок В. Л. Інформаційний та кіберпростори: проблеми безпеки, методи та засоби боротьби : підручник. Львів : Магнолія 2006, 2020. 448 с.
5. Лісовська Ю. П. Кібербезпека: ризики та заходи : навч. посіб. Київ : Кондор, 2021. 272 с.
6. Остапов С. Е. Кібербезпека: сучасні технології захисту : навч. посіб. Львів : Новий Світ-2000, 2021. 679 с.
7. Комаров М. Ю. Огляд кібератак на об'єкти критичної інфраструктури // Електронне моделювання. 2019. № 6. С. 91-106.
8. Розвиток моделей кібератак у площині інформаційної безпеки підприємства / Є. М. Галахов, В. В. Собчук // Комунікаційні та інформаційні технології. 2019. № 4. С. 12-24.