ДЕРЖАВНИЙ УНІВЕРСИТЕТ
«КИЇВСЬКИЙ АВІАЦІЙНИЙ ІНСТИТУТ»
Кафедра «Цивільної та промислової безпеки
імені Героя України Чуба Олександра Сергійовича»
Центр безпеки та стійкості об'єктів критичної інфраструктури

ПОГОДЖЕНО
Заступник Міністра
розвитку громад і територій України

_____ Анатолій КОМІРНИЙ
«___» _____2024 р.

ЗАТВЕРДЖУЮ
Проректор з навчальної роботи

_____ Анатолій ПОЛУХІН
«___» _____2024 р.

Програма
підвищення кваліфікації персоналу за напрямом

«Підвищення безпеки та стійкості об'єктів критичної інфраструктури»

СМЯ КАІ ППК 10.03.01-2024

Київ 2024

1. Анотація

Програма «Підвищення безпеки та стійкості об'єктів критичної інфраструктури» ставить метою дати слухачам сукупності знань, що вдосконалюють і поглиблюють інженерну підготовку у операторів об'єктів критичної інфраструктури для забезпечення належного рівня державного регулювання діяльності у сфері захисту об'єктів критичної інфраструктури, та функціонування єдиної державної системи цивільного захисту України, формування у здобувачів здатності оцінювати особливості функціонування об'єктів критичної інфраструктури та розробляти заходи забезпечення їх безпеки та підвищення стійкості в сучасних умовах.

Програма курсів підвищення кваліфікації розрахована для фахівців, виробничі обов'язки яких пов'язані із забезпечення безпеки та стійкості критичної інфраструктури: організація захисту, забезпечення функціональності, цілісності і стійкості критичної інфраструктури, ефективного зниження та контролю за ризиками безпеки, можливості функціонувати у штатному режимі, адаптуватися до умов, що постійно змінюються, протистояти та швидко відновлюватися після впливу загроз.

Тривалість навчання – 44 навчальних годин.

Заняття проводяться в Центрі безпеки та стійкості об'єктів критичної інфраструктури кафедри «Цивільної та промислової безпеки ім. Героя України Чуба О.С.» КАІ. За домовленістю із замовником строк навчання може встановлюватися іншим, в залежності від освітнього рівня слухачів, досвіду їх практичної роботи та кваліфікації, яку визначає замовник навчання. Відповідно коригується навчальний план та програма навчання.

Після закінчення навчання слухачі одержують Сертифікат встановленого зразка.

Програма розроблена згідно із вимогами та рекомендаціями Ради національної безпеки та оборони України, Міністарства розвитку громад та територій України, Департаменту захисту критичної інфраструктури Держспецзв'язку України, Закону України «Про критичну інфраструктуру», інших нормативно-правових актах України.

Програма курсів орієнтована на підвищення кваліфікації:

- Експерта із захисту об'єктів критичної інфраструктури (за видами діяльності);
- Аналітика з оцінки ризиків, загроз та стану захищеності об'єктів критичної інфраструктури (за видами діяльності);
- Фахівця із захисту та стійкості об'єктів критичної інфраструктури.

Кваліфікаційні вимоги до слухачів, які пройшли підготовку

Слухачі повинні **мати**:

- достатні знання законодавства та інших нормативно-правових актах України в галузі забезпечення захисту критичної інфраструктури;
- усвідомлення функцій держави, функціональних, секторальних органів, форм реалізації цих функцій, правових основ захисту критичної інфраструктури.

Слухачі повинні **знати**:

- засади державної політики у сфері захисту критичної інфраструктури;
- специфіка спектру загроз об'єктів критичній інфраструктурі в Україні;
- системні аспекти при дослідженні ризику об'єктів критичної інфраструктури;
- методи оцінювання загроз та ризиків об'єктів критичної інфраструктури;
- оцінювання вразливості активів об'єктів критичної інфраструктури;
- принципи організації державно-приватного партнерства на об'єктах критичної інфраструктури;
- забезпечення стійкості об'єктів критичної інфраструктури в умовах прояву проєктних загроз;
- порядок проведення моніторингу рівня безпеки об'єктів критичної інфраструктури;

- порядок розроблення та погодження паспорта безпеки на об'єкт критичної інфраструктури.

Слухачі повинні **уміти**:

- виділяти основні загрози об'єкту критичної інфраструктурі;
- застосовувати методи оцінювання загроз та ризиків об'єкту критичної інфраструктурі;
- виділяти активи об'єктів критичної інфраструктури та оцінювати ризик для них;
- організувати і проводити навчанні співробітників об'єктів критичної інфраструктури з питань безпеки;
- організувати і реалізувати державно-приватне партнерство на об'єктах критичної інфраструктури;;
- планувати і реалізувати підвищення безпеки та стійкості об'єктів критичної інфраструктури;
- розробляти план захисту об'єкта критичної інфраструктури за проектною загрозою.

2. Тематичний план підвищення кваліфікації персоналу за напрямом «Підвищення безпеки та стійкості об'єктів критичної інфраструктури»

Навчальний план передбачає вивчення слухачами восьми тематичних модулів. У кожному модулі надається список рекомендованої літератури і перелік тестових питань.

2.1. Розрахунок навчального часу

Кількість навчальних годин 44 години
Тривалість навчального дня 4 - 8 годин (згідно розкладу проведення занять)

2.2. Розподіл навчальних годин

№	Тема	Лекції	Практ.	прим
1	**Вступ до курсу. Державна політика захисту критичної інфраструктури**	**2**	**2**	1.Закону України «Про критичну інфраструктуру» 2. Постанова Кабінету Міністрів України від 9 жовтня 2020 р. № 1109. 3. Проєкт Закону України «Про критичну інфраструктуру та її захист»
2	**Основні загрози критичній інфраструктурі**	**4**	**2**	1.OECD (2019), Належне врядування для забезпечення стійкості критичної інфраструктури, Огляди політики управління ризиками OECD, Публікація OECD, Париж. https://doi.org/10.1787/02f0e5a0-en 2. Метод оцінювання вразливості хімічних об'єктів США.
3	**Оцінка ризику об'єктів критичної інфраструктури**	**4**	**2**	1. Постанова Кабінету Міністрів України від 22 липня 2022 р. №

				821.
4	**Оцінювання ризику безпеки об'єктів критичної інфраструктури**	**4**	**2**	1. Посібник з питань ефективного реагування на надзвичайні ситуації в хімічній галузі. 2022 р. 2. Агентство з питань кібербезпеки і безпеки інфраструктури. Методологія оцінки стійкості регіональної інфраструктури. 2021 р. 3. Механізм планування стійкості інфраструктури (МПСІ). 2022 р.
5	**Організація навчання співробітників об'єктів критичної інфраструктури з питань безпеки**	**4**	**2**	1. Гарт С., Ремзі Дж. Д. (2011). Посібник з питань розроблення курсів із захисту фізичних об'єктів критичної інфраструктури для викладачів національної безпеки. Журнал Homeland Security Affairs, том 7(1). Завантажено з ресурсу https://commons.erau.edu/db-security-studies/14 2. Практичний посібник з питань методики навчання. 2014 р. 3. Пакет ситуаційних вправ АКЗІ.
6	**Інсайдерські загрози та захиститися від них**	**4**	**2**	1. Shevchenko, S., ZhdanovaY., Skladannyi, P., Boiko, S. (2022). Інсайдери та інсайдерська інформація: суть, загрози, діяльність та правова відповідальність. Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка», 3(15), 175-185. 2. Гулак, Г. М., Козачок, В. А., Складанний, П. М., Бондаренко, М. О., Вовкотруб, Б. В. (2017). Системи захисту персональних даних в сучасних інформаційно-телекомунікаційних системах. Сучасний захист інформації, 2, 65-71. 3. Walker-Roberts, S.; Hammoudeh, M.; Dehghantanha, A. A systematic review of the availability and efficacy of countermeasures to internal threats in healthcare critical infrastructure. IEEE Access 2018, 6, 25167–25177.
7	**Проєктна загроза та паспорти безпеки як ключові елементи**	**4**	**2**	1. Рекомендації з розроблення планів захисту за проєктною

	системи захисту критичної інфраструктури			загрозою національного рівня «Пожежі та вибухи» (наказ ДСНС від 23.07.2024 № 769) 2. Методичні рекомендації щодо розробки проєктних загроз критичній інфраструктурі секторального/об'єктового рівнів та оцінки загроз критичній інфраструктурі. 08.11.2023 р. Департамент захисту критичної інфраструктури. 3. Методичні рекомендації щодо розроблення планів локалізації і ліквідації аварій та їх наслідків (наказ ДСНС від 17.05.2022 № 253). 4. Постанова Кабінету Міністрів України від 9 серпня 2017 р. № 626. 5. Наказ Адміністрації Держспецзв'язку від 04 жовтня 2023 р. № 877 «Про затвердження форми Плану захисту об'єкту критичної інфраструктури за проєктною загрозою національного рівня «кібератака/ кіберінцидент». 6. Наказ Адміністрації Держспецзв'язку від 28 липня 2023 року № 219/ДСК «Про затвердження Проектних загроз критичній інфраструктурі національного рівня». 7. Рекомендації з розроблення плану захисту об'єкта критичної інфраструктури за проектною загрозою національного рівня «кібератака/кіберінцидент» (Наказ Адміністрації Держспецзв'язку від 01.12.2023 №1011).
8	**Паспорт безпеки об'єкта критичної інфраструктури**	**4**		1. Постанова Кабінету Міністрів України від 04 серпня 2023 р. № 818.
	Разом	**30**	**14**	

2.3 Зміст тематичних модулів

Тема № 1. Державна політика захисту критичної інфраструктури.

Зміст теми: Мета захисту критичної інфраструктури. Засади державної політики у сфері захисту критичної інфраструктури. Основні принципи побудови захисту критичної інфраструктури. Який вплив на бізнес закону про критичну інфраструктуру.

Тема № 2. Основні загрози критичній інфраструктурі.
Зміст теми: Основні категорії загроз критичній інфраструктурі у національних законодавствах провідних країн світу, виходячи з характеру їх походження. Специфіка спектру загроз критичній інфраструктурі в Україні. Загрози критичній інфраструктурі з точки зору виділення елементів критичній інфраструктурі, на які ці загрози спрямовані. Виділення спрямованості дії загроз та розробка планів протидії.

Тема № 3. Оцінка ризику об'єктів критичної інфраструктури.
Зміст теми: Системні аспекти при дослідженні ризику критичної інфраструктури. Сценарії і наслідки розвитку не сприятливих подій на об'єктах критичної інфраструктури. Загальна схема при управлінні безпекою об'єктів критичної інфраструктури. Задача оптимізації розподілу ресурсів для мінімізації інтегрального регіонального ризику. Обчислення інтегрального регіонального ризику. Методи оцінювання загроз та ризиків. Моніторинг загроз та ризиків. Методологічні основи ризик-менеджменту.

Тема № 4. Оцінювання ризику безпеки об'єктів критичної інфраструктури.
Зміст теми: Характеристика активів об'єктів критичної інфраструктури. Оцінювання загроз активам об'єктів критичної інфраструктури. Оцінювання вразливості активів об'єктів критичної інфраструктури. Оцінювання ризиків безпеки активів об'єктів критичної інфраструктури. Розробка заходів підвищення безпеки активів об'єктів критичної інфраструктури на основі проведеної оцінки ризиків.

Тема № 5. Організація навчання співробітників об'єктів критичної інфраструктури з питань безпеки.
Зміст теми: Цілі тренувань та навчань з безпеки. Типи тренувань і навчань. Розробка процесу планування та проведення навчань з безпеки. Кадрове забезпечення навчань. Проведення навчання і тренувань. Методологія оцінювання взаємодії між планами реагування на загрози безпеці та охорони. Оцінка результатів навчань виявлення сфер плану безпеки, плану дій у надзвичайних ситуаціях або засобів реагування, які потребують вдосконалення або посилення.

Тема № 6. Інсайдерські загрози та захисти від них.
Зміст теми: Характеристика інсайдерських загроз. У чому небезпека інсайдерських загроз. Моделі формалізації процесу виявлення інсайдерських кіберзагроз. Онтологічна модель формалізації процесу виявлення інсайдерських кіберзагроз. Правила та обмеження в онтологічній моделі для формалізації процесу виявлення інсайдерських кіберзагроз. Запровадження контролю доступу. Відстеження підозрілої діяльності персоналу. Перевірка репутації співробітників. Організація навчання персоналу з питань безпеки. Запобігання втраті даних.

Тема № 7. Проєктна загроза та паспорти безпеки як ключові елементи системи захисту критичної інфраструктури.
Зміст теми: Проблеми забезпечення стійкості об'єктів критичної інфраструктури. Режими функціонування об'єктів критичної інфраструктури. Забезпечення стійкості об'єктів критичної інфраструктури – основні нормативні документи. ДСНС: Методичні рекомендації ДСНС щодо розроблення планів ліквідації аварій та їх наслідків; Рекомендації з розроблення планів захисту

за проєктною загрозою національного рівня «Пожежі та вибухи»; План захисту із забезпечення цивільного захисту, пожежної та техногенної безпеки на об'єктах критичної інфраструктури та протидії проєктній загрозі національного рівня «Пожежі та вибухи».

Тема № 8. Паспорт безпеки об'єкта критичної інфраструктури.
Зміст теми: Порядок проведення моніторингу рівня безпеки об'єктів критичної інфраструктури (Постанова Кабінету Міністрів України від 22 липня 2022 р. № 821). Порядок розроблення та погодження паспорта безпеки на об'єкт критичної інфраструктури (Постанова Кабінету Міністрів України від 4 серпня 2023 р. № 818). Методичні рекомендації щодо розробки проєктних загроз критичної інфраструктури секторального/об'єктового рівнів та оцінки загроз критичної інфраструктури. Рекомендації з розроблення плану захисту об'єкта критичної інфраструктури за проектною загрозою національного рівня «кібератака/кіберінцидент». План захисту об'єкта критичної інфраструктури за проєктною загрозою національного рівня «кібератака/кіберінцидент».

3. Вимоги щодо кваліфікаційної перевірки у виробничих умовах.

Програмою навчання персоналу на курсах підвищення кваліфікації за напрямом «Підвищення безпеки та стійкості об'єктів критичної інфраструктури» передбачається проведення занять в Національному авіаційному університеті на базі досвіду роботи спеціалістів Центру безпеки та стійкості об'єктів критичної інфраструктури кафедри «Цивільної та промислової безпеки», яка є випусковою за спеціальністю К10 «Цивільна безпека» у співпраці з міжнародними фахівцями Фонду цивільних досліджень та розвитку США в Україні, Бюро міжнародної безпеки та нерозповсюдження, Державного департаменту США при сприянні Апарату Ради національної безпеки і оборони України, CISA Cybersecurity and Infrastructure security agency, AcuTech Consulting Group, CRDF GLOBAL.

Кваліфікаційна перевірка слухачів проводиться в процесі навчання з використанням інформаційних технологій. Кваліфікаційна перевірка та оцінювання слухачів здійснюється викладачем за даною програмою у процесі складання тестових завдань за темами.

4. Завдання поточного контролю, питання для самоконтролю, контрольні питання

В процесі навчання персоналу на курсах підвищення кваліфікації за напрямом «Підвищення безпеки та стійкості об'єктів критичної інфраструктури» передбачається проведення поточного контролю (та самоконтролю) за окремими темами. Тестові завдання, які використовуються для поточного контролю (можуть використовуватися слухачами також і для самоконтролю), наведено у Додатку 1 до цієї Програми.

5. Необхідне обладнання, комп'ютерні програми

В процесі навчання персоналу на курсах підвищення кваліфікації за напрямом «Підвищення безпеки та стійкості об'єктів критичної інфраструктури» передбачається використання комп'ютерного обладнання з доступом до мережі Internet, інформаційних (автоматизованих) систем, проектору для перегляду презентацій та навчальних відеоматеріалів. У процесі підготовки використовуються зразки документів, буклетів, рекламні проспекти.

6. Система оцінювання, екзаменаційні білети, тести

Всі слухачі, які пройшли навчання на курсах підвищення кваліфікації за напрямом «Підвищення безпеки та стійкості об'єктів критичної інфраструктури», мають скласти підсумковий тест.

Тестове завдання вважається успішно зданим за наявності не менше 70% правильних відповідей на поставлені питання. Тестове завдання наведено у Додатку 1. У випадку успішного складання тесту слухачеві видається відповідний Сертифікат. Зразок Сертифікату наведено Додатку 2.

Сертифікат про проходження навчання на курсах підвищення кваліфікації за напрямом «Підвищення безпеки та стійкості об'єктів критичної інфраструктури» видається на три роки.

7. Перелік навчальної літератури та нормативно-правових актів, які необхідні для підготовки

- Закону України «Про критичну інфраструктуру» від 16.11.2021 р. № 1882-IX (в редакції від 21.09.2024 р.).
- Постанова Кабінету Міністрів України від 9 серпня 2017 р. № 626, Про затвердження Порядку розроблення планів діяльності єдиної державної системи цивільного захисту (в редакції від 17.08.2024 р.).
- Постанова Кабінету Міністрів України від 9 жовтня 2020 р. № 1109, Деякі питання об'єктів критичної інфраструктури.
- Постанова Кабінету Міністрів України від 22 липня 2022 р. № 821, Про затвердження Порядку проведення моніторингу рівня безпеки об'єктів критичної інфраструктури.
- Постанова Кабінету Міністрів України від 04 серпня 2023 р. № 818, Деякі питання паспортизації об'єктів критичної інфраструктури.
- Методологія оцінки стійкості регіональної інфраструктури. Агентство з питань кібербезпеки і безпеки інфраструктури, 2021 р.
- Правила пожежної безпеки в Україні, затверджені наказом Міністерства внутрішніх справ України від 30.12.2014 № 1417, зареєстрованого в Міністерстві юстиції України від 05 березня 2015 року за № 252/26697.
- Рекомендації з розроблення планів захисту за проєктною загрозою національного рівня «Пожежі та вибухи» (наказ ДСНС від 23.07.2024 № 769).
- Методичні рекомендації щодо розробки проєктних загроз критичній інфраструктурі секторального/об'єктового рівнів та оцінки загроз критичній інфраструктурі. (08.11.2023 р. Департамент захисту критичної інфраструктури).
- Методичні рекомендації щодо розроблення планів локалізації і ліквідації аварій та їх наслідків (наказ ДСНС від 17.05.2022 № 253).
- Наказ Адміністрації Держспецзв'язку від 04 жовтня 2023 р. № 877 «Про затвердження форми Плану захисту об'єкту критичної інфраструктури за проєктною загрозою національного рівня «кібератака/ кіберінцидент».
- Наказ Адміністрації Держспецзв'язку від 28 липня 2023 року № 219/ДСК «Про затвердження Проектних загроз критичній інфраструктурі національного рівня».
- Гарт С., Ремзі Дж. Д. (2011). Посібник з питань розроблення курсів із захисту фізичних об'єктів критичної інфраструктури для викладачів національної безпеки. Журнал Homeland Security Affairs, том 7(1). – Режим доступу: https://commons.erau.edu/db-security-studies/14
- Shevchenko, S., ZhdanovaY., Skladannyi, P., Boiko, S. (2022). Інсайдери та інсайдерська інформація: суть, загрози, діяльність та правова відповідальність. Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка», 3(15), 175-185. https://doi.org/10.28925/2663-4023.2022.15.175185.

- Гулак, Г. М., Козачок, В. А., Складанний, П. М., Бондаренко, М. О., Вовкотруб, Б. В. (2017). Системи захисту персональних даних в сучасних інформаційно-телекомунікаційних системах. Сучасний захист інформації, 2, 65-71. http://nbuv.gov.ua/UJRN/szi_2017_2_12.
- 3. Walker-Roberts, S.; Hammoudeh, M.; Dehghantanha, A. A systematic review of the availability and efficacy of countermeasures to internal threats in healthcare critical infrastructure. IEEE Access 2018, 6, 25167–25177.
- National Strategy for Critical Infrastructure Protection (CIP Strategy) [Електронний ресурс]. – Режим доступу: http://ccpic. mai.gov.ro/docs/Germania_cip_stategy.pdf

Програму склали **О. Третьяков**
Б. Халмурадов

ДОДАТКИ

Додаток 1

ПІБ слухача_____ **Q1**

ТЕСТОВЕ ЗАВДАННЯ ДО ТЕМИ № 1

	Державна політика захисту критичної інфраструктури	**ОЦІНКА В БАЛАХ**
Q 01.1	**Засади державної політики у сфері захисту критичної інфраструктури.**	**40**
	Основні принципи побудови захисту критичної інфраструктури	**60**
	ЗАГАЛЬНА КІЛЬКІСТЬ БАЛІВ	**100%**
	ПРОХІДНИЙ БАЛ	**70%**

ПІБ слухача_____ **Q2**

ТЕСТОВЕ ЗАВДАННЯ ДО ТЕМИ № 1

	Основні загрози критичній інфраструктурі	**ОЦІНКА В БАЛАХ**
Q 02.1	**Надати характеристику основним категоріям загроз критичній інфраструктурі**	**25**
	_____	
Q 02.2	**Специфіка спектру загроз критичній інфраструктурі в Україні**	**25**
Q 02.3	**Загрози критичній інфраструктурі з точки зору виділення елементів критичній інфраструктурі, на які ці загрози спрямовані**	**25**
Q 02.4	**Виділення спрямованості дії загроз та розробка планів протидії**	**25**
	ЗАГАЛЬНА КІЛЬКІСТЬ БАЛІВ	**100%**
	ПРОХІДНИЙ БАЛ	**70%**

ПІБ слухача_____ **Q3**

ТЕСТОВЕ ЗАВДАННЯ ДО ТЕМИ № 3

	Оцінка ризику об'єктів критичної інфраструктури	ОЦІНКА В БАЛАХ
Q 03.1	**Сценарії і наслідки розвитку не сприятливих подій на об'єктах критичної інфраструктури**	**30**
		20
Q 03.2	**Загальна схема при управлінні безпекою об'єктів критичної інфраструктури**	
Q 03.3	**Методи оцінювання загроз та ризиків**	**30**
	Моніторинг загроз та ризиків	
Q 03.4	**Обчислення інтегрального регіонального ризику**	**20**
	ЗАГАЛЬНА КІЛЬКІСТЬ БАЛІВ	**100%**
	ПРОХІДНИЙ БАЛ	**70%**

ПІБ слухача_____ **Q4**

ТЕСТОВЕ ЗАВДАННЯ ДО ТЕМИ № 4

	Оцінювання ризику безпеки об'єктів критичної інфраструктури	ОЦІНКА В БАЛАХ
Q 04.1	**Характеристика активів об'єктів критичної інфраструктури**	**20**
		40
Q 04.2	**Оцінювання вразливості активів об'єктів критичної інфраструктури**	
	Оцінювання ризиків безпеки активів об'єктів критичної інфраструктури	
		40
Q 04.3	**Розробка заходів підвищення безпеки активів об'єктів критичної інфраструктури на основі проведеної оцінки ризиків**	
	ЗАГАЛЬНА КІЛЬКІСТЬ БАЛІВ	**100%**
	ПРОХІДНИЙ БАЛ	**70%**

ПІБ слухача_____ **Q5**

ТЕСТОВЕ ЗАВДАННЯ ДО ТЕМИ № 5

	Організація навчання співробітників об'єктів критичної інфраструктури з питань безпеки	ОЦІНКА В БАЛАХ
Q 05.1	**Типи тренувань і навчань з безпеки об'єктів критичної інфраструктури**	**30**
Q 05.2	**Планування та проведення навчань з безпеки об'єктів критичної інфраструктури**	**30**

Q 05.3	**Методологія оцінювання взаємодії між планами реагування на загрози безпеці та охорони**	**40**
	ЗАГАЛЬНА КІЛЬКІСТЬ БАЛІВ	**100%**
	ПРОХІДНИЙ БАЛ	**70%**

ПІБ слухача_____ **Q6**

ТЕСТОВЕ ЗАВДАННЯ ДО ТЕМИ № 6

	Інсайдерські загрози та захисти від них	**ОЦІНКА В БАЛАХ**
Q 06.1	**Моделі формалізації процесу виявлення інсайдерських кіберзагроз..**	**30**
Q 06.2	**Онтологічна модель формалізації процесу виявлення інсайдерських кіберзагроз**	**30**
Q 06.3	**Правила та обмеження в онтологічній моделі для формалізації процесу виявлення інсайдерських кіберзагроз**	**40**
	ЗАГАЛЬНА КІЛЬКІСТЬ БАЛІВ	**100%**
	ПРОХІДНИЙ БАЛ	**70%**

ПІБ слухача_____ **Q7**

ТЕСТОВЕ ЗАВДАННЯ ДО ТЕМИ № 7

	Проєктна загроза та паспорти безпеки як ключові елементи системи захисту критичної інфраструктури	**ОЦІНКА В БАЛАХ**
Q 07.1	**Проблеми забезпечення стійкості об'єктів критичної інфраструктури**	**100**
	Режими функціонування об'єктів критичної інфраструктури	
	Забезпечення стійкості об'єктів критичної інфраструктури	
	Розроблення планів захисту за проєктною загрозою національного рівня	
	План захисту із забезпечення цивільного захисту, пожежної та техногенної безпеки на об'єктах критичної інфраструктури	
	ЗАГАЛЬНА КІЛЬКІСТЬ БАЛІВ	**100%**
	ПРОХІДНИЙ БАЛ	**70%**

ПІБ слухача_____ **Q8**

ЗАКЛЮЧНЕ ТЕСТОВЕ ЗАВДАННЯ

	Паспорт безпеки об'єкта критичної інфраструктури	**ОЦІНКА В БАЛАХ**
Q 8.1	**Порядок проведення моніторингу рівня безпеки об'єктів критичної інфраструктури**	**100**
	Порядок розроблення та погодження паспорта безпеки на об'єкт критичної інфраструктури	

	Розроблення плану захисту об'єкта критичної інфраструктури за проектною загрозою національного рівня «кібератака/ кіберінцидент»	
	ЗАГАЛЬНА КІЛЬКІСТЬ БАЛІВ	**100%**
	ПРОХІДНИЙ БАЛ	**70%**

Додаток 2

ДАНІ ПРО ПРОФЕСОРСЬКО-ВИКЛАДАЦЬКИЙ СКЛАД

№	Прізвище, ім'я по батькові	Рік народ-ження	Стаж пед. роботи	Вчений ступінь, звання, посада	Підвищення кваліфікації, стажування (де, коли)
1	Халмурадов Батир Данатарович	1964	18	Професор, завідувач кафедри «Цивільної та промислової безпеки»	1. Центрально-європейський інститут освіти (м. Братислава, Словацька Республіка). Тема: Охорона здоров`я та система менеджменту безпеки (ISO 450001). 2018 (120 годин / 4 кредити ЄКТС). Документ: Сертифікат № SK 098-2018EA, 2018. 2. Європейський інститут безперервної освіти EIDV (м. Подхайска, Республіка Словаччина). 18.03.2021–19.03.2021 (15 годин/0,5 кредиту ЄКТС). Тема: участь у Міжнародній науковій конференції «Наука та освіта у світовому інформаційному просторі». Документ: Сертифікат про участь у Міжнародній науковій конференції. 3. Всеукраїнська Громадська організація «Інноваційний університет». 04.02.2022–20.05.2022 (240 годин / 8 кредитів ЄКТС). Програма: Науково-педагогічні працівники: особистісний розвиток, лідерство. Спеціальна тема: Дуальна освіта. Документ: Сертифікат, який засвідчує проходження підвищення кваліфікації. 4. Участь в семінарі «Безпека та стійкість критичної інфраструктури», який було організовано Національним координаційним центром кібербезпеки спільно з Фондом цивільних досліджень та розвитку США за підтримки Державного департаменту США. (семінар проходив у м.Варшава, Республіка Польща). 27.03.2023–30.03.2023 (40 годин / 1,3 кредиту ЄКТС). Тема: Безпека та стійкість критичної

					інфраструктури. Документ: Сертифікат про участь у семінарі. 5. Университет Саленто (м. Лечче, Італія) / University of Salento. 11.03.2024–14.03.2024 (40 годин / 1,3 кредиту ЄКТС). Тема: Розвиток університетських програм з безпеки та стійкості критичної інфраструктури / Development of University Programs in Critical Infrastructure and Resilience. Документ: Сертифікат, який засвідчує участь у семінарі.
2	Третьяков Олег Вальтерович	1954	33		1. Вища школа економіки в Бидгощі (м. Бидгощ, Республіка Польща). 08.09.2019–12.11.2019 (180 годин / 6 кредитів ЄКТС). Тема: Сучасні тенденції з рятування життя та здоров'я, екології та екологічної безпеки в процесі вищої освіти в університетах ЄС / Modern trends in lifesaving and health, ecology and environmental safety in the process of higher education at universities in the EU. Документ: Сертифікат про проходження науково-педагогічного стажування. 2. Товариство з обмеженою відповідальністю «АЛДИ-ТЕХ» (м. Харків). 01.06.2021–11.06.2021 (40 годин/1,33 кредиту ЄКТС). Тема: За програмою для викладачів вищих навчальних закладів з охорони праці, надання домедичної допомоги потерпілим, електробезпеки, пожежної безпеки, санітарного і гігієнічного забезпечення. Документ: Посвідчення про проходження навчання № 66/06/21-Н від 11.06.2021. 3. Державна служба України з питань праці. Головний навчально-методичний центр Держпраці. 4. . Университет Саленто (м. Лечче, Італія) / University of Salento. 11.03.2024–14.03.2024 (40 годин / 1,3 кредиту ЄКТС).

					Тема: Розвиток університетських програм з безпеки та стійкості критичної інфраструктури / Development of University Programs in Critical Infrastructure and Resilience. Документ: Сертифікат, який засвідчує участь у семінарі.

Додаток 3

Зразок Сертифікату про проходження курсу

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

ДЕРЖАВНИЙ УНІВЕРСИТЕТ
«КИЇВСЬКИЙ АВІАЦІЙНИЙ ІНСТИТУТ»

ЦЕНТР БЕЗПЕКИ ТА СТІЙКОСТІ
ОБ'ЄКТІВ КРИТИЧНОЇ ІНФРАСТРУКТУРИ

СЕРТИФІКАТ

Цим засвідчується, що ***ПЕТРЕНКО Олексій***

Успішно пройшов навчання за напрямом

«Підвищення безпеки та стійкості об’єктів критичної інфраструктури»

11.11 – 15.11.2024р

Для ефективної реалізації законодавчих та нормативних актів з безпеки та стійкості об’єктів критичної інфраструктури

(навчальна програма 44 годин /1,5 кредиту ECTS)

Дата видачі 14.11.2024 Строк дії сертифікату 3 роки м. Київ

Проректор ДУ КАІ Анатолій ПОЛУХІН

МП

Директор центру БСКІ Олег ТРЕТЬЯКОВ

Лист
реєстрації змін та доповнень
(Ревізія програми)

№ з/п	Розділ, тема	Номер сторінки			№ ревізії	Підпис відповідального	Дата
		зміненої	нової	анульованої			