МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
Національний аерокосмічний університет
«Харківський авіаційний інститут»

ЗАТВЕРДЖЕНО

Рішенням вченої ради Університету
Протокол № 2 від 24.09.2025

ВВЕДЕНО У ДІЮ

Наказ № 452 від 25.09.2025

В. о. ректора

Олексій ЛИТВИНОВ

ПОЛОЖЕННЯ

про Регіональний тренінговий центр інформаційних технологій, кібербезпеки та захисту інформації Національного аерокосмічного університету «Харківський авіаційний інститут»

СУЯ ХАІ-ЦЯО-РТЦ-П/001:2025

Дата введення «10» вересня 2025 р.

Редакція № 1

Харків 2025

1. ЗАГАЛЬНІ ПОЛОЖЕННЯ

1.1. Регіональний тренінговий центр інформаційних технологій, кібербезпеки та захисту інформації (далі – Центр, скорочена назва – РТЦ) є структурним підрозділом відділу післядипломної освіти Центру якості освіти, ліцензування та акредитації Національного аерокосмічного університету «Харківський авіаційний інститут» (далі – Університет).

1.2. Центр не є юридичною особою та здійснює свою діяльність на матеріально-технічній базі відділу післядипломної освіти Центру якості освіти, ліцензування та акредитації, кафедри комп'ютерних систем, мереж і кібербезпеки (№ 503), кафедри права (№ 702), а також може за погодженням використовувати ресурси інших структурних підрозділів Університету.

1.3. У своїй діяльності Центр керується Конституцією України, законами України «Про вищу освіту», «Про наукову і науково-технічну діяльність», «Про основні засади забезпечення кібербезпеки України», іншими нормативно-правовими актами, наказами та методичними рекомендаціями Міністерства освіти і науки України, Статутом Університету, внутрішніми нормативними документами Університету, цим Положенням, а також Меморандумом про співробітництво у сфері кібербезпеки та захисту інформації між Державною службою спеціального зв'язку та захисту інформації України і Університетом.

1.4. Центр функціонує як регіональна навчально-тренінгова платформа, орієнтована на профорієнтацію та перепідготовку молоді й фахівців у сфері кіберзахисту та інформаційних технологій, здійснює координацію діяльності освітніх установ і партнерських організацій, а також забезпечує реалізацію профорієнтаційних освітніх програм на національному та міжнародному рівнях.

2. МЕТА І ЗАВДАННЯ ЦЕНТРУ

2.1. Центр створено з метою організації професійної підготовки, перепідготовки та підвищення кваліфікації фахівців у сфері інформаційних технологій, кібербезпеки та захисту інформації, розвитку регіональної системи кіберзахисту, підвищення обізнаності населення та сприяння реалізації державної політики у сфері національної безпеки.

2.2. Завдання і функції Центру:

- забезпечення організації та проведення професійної підготовки, перепідготовки, підвищення кваліфікації фахівців у сфері інформаційних технологій, кібербезпеки та захисту інформації;

- забезпечення якісної підготовки слухачів до складання кваліфікаційних іспитів відповідно до професійних стандартів та кваліфікаційних вимог;
- розробка й упровадження навчальних програм, навчально-методичних матеріалів, тренінгів та спеціалізованих навчань у сфері інформаційної та функційної безпеки, технічного захисту інформації, криптографічного захисту, захисту критичної інформаційної інфраструктури;
- організація і проведення тренінгів, курсів підвищення кваліфікації, практичних семінарів, інших навчальних заходів із тем інформаційних технологій, кібербезпеки та захисту інформації;
- створення та розгортання кіберполігону, спеціалізованих лабораторій з кібербезпеки та функційної безпеки інформаційних та операційних технологій;
- розробка тестових завдань, практичних кейсів, симуляцій кібератак і кіберінцидентів;
- підготовка звітних матеріалів за підсумками тренінгів, практик, результатів тестувань;
- розробка та впровадження сучасних цифрових рішень, програмних засобів та інструментів моделювання кіберзагроз у навчальний процес;
- співпраця з державними установами, місцевими органами влади, навчальними закладами, міжнародними партнерами, юридичними особами публічного та приватного права у сфері підготовки фахівців з інформаційних технологій, кібербезпеки та захисту інформації;
- надання платних освітніх послуг з підготовки, перепідготовки та підвищення кваліфікації;
- формування регіональної мережі партнерства у сфері кіберзахисту та сприяння міжнародному співробітництву.

3. ОРГАНІЗАЦІЯ ДІЯЛЬНОСТІ ЦЕНТРУ

3.1. Організація діяльності Центру визначається залежно від обсягу робіт та їх фінансування, строками виконання завдань, а також потребами державних і регіональних програм розвитку у сфері інформаційних технологій, кібербезпеки та захисту інформації.

3.2. Керівництво Центром здійснює керівник Центру з наукової та навчально-методичної роботи, який визначає напрями діяльності та її координацію, а також відповідальний за організаційну роботу Центру, який здійснює безпосереднє керівництво роботою Центру. Керівник і відповідальний за роботу Центру призначаються наказом ректора Університету з числа науково-педагогічних працівників Університету.

3.3. **Керівник Центру з наукової та навчально-методичної роботи** здійснює стратегічне і науково-методичне керівництво Центром, зокрема:

- визначає стратегію розвитку Центру, формує його науково-методичну політику та напрями освітньої діяльності;
- координує підготовку та оновлення навчальних програм, курсів і тренінгів відповідно до державних стандартів та міжнародних практик;
- забезпечує якість навчально-методичного забезпечення та відповідність освітніх програм профілю підготовки;
- ініціює наукові дослідження, грантові та освітні проекти, фінансовані з державних та міжнародних джерел;
- представляє Центр у науково-методичних радах Університету та наукових організаціях.

3.4. **Відповідальний за організаційну діяльність Центру** здійснює загальне управління організаційними процесами та адміністративно-господарське забезпечення діяльності Центру, зокрема:

- організовує та контролює поточну роботу Центру, забезпечує виконання планів, наказів і розпоряджень ректора Університету;
- координує діяльність підрозділів та залучених фахівців, забезпечує належний рівень матеріально-технічної бази та ресурсного забезпечення;
- відповідає за організацію навчального процесу: формування навчальних груп, розклад занять, розподіл навантаження викладачів;
- здійснює організацію маркетингових та інформаційно-просвітницьких заходів у сфері кіберзахисту й інформаційних технологій на регіональному рівні;
- представляє Центр у відносинах з органами державної влади, органами місцевого самоврядування, підприємствами, установами й організаціями публічного та приватного права, у тому числі з міжнародними партнерами;
- забезпечує виконання вимог нормативних документів щодо ведення документації, укладання договорів та фінансової звітності Центру.

3.4. Для виконання мети і завдань, визначених цим Положенням, Центром залучаються науково-педагогічні та педагогічні працівники, співробітники, докторанти та аспіранти кафедр комп'ютерних систем, мереж і кібербезпеки (№ 503) та кафедри права (№702), а також інші науково-педагогічні, педагогічні працівники, співробітники, докторанти та аспіранти кафедр Університету.

3.5. Центр взаємодіє з кафедрами, лабораторіями, факультетами та іншими підрозділами Університету з питань надання освітніх послуг, проведення тренінгів, реалізації освітніх і науково-дослідних програм.

5. ПРИКІНЦЕВІ ПОЛОЖЕННЯ

5.1. Положення про Центр підписується проректором з науково-педагогічної роботи, директором Центру якості освіти, ліцензування та акредитації, начальником юридичного відділу Університету та затверджується ректором Університету.

5.2. Положення затверджується наказом ректора Університету і набирає чинності з моменту його підписання.

5.3. Зміни до цього Положення вносяться у встановленому порядку, підлягають погодженню відповідно до внутрішніх регламентів Університету та набирають чинності з моменту затвердження відповідним наказом.

Погоджено:

Проректор
з науково-педагогічної діяльності — Андрій ГУМЕННИЙ

Директорка Центра якості освіти,
ліцензування та акредитації — Елеонора ДАРМОФАЛ

Начальник юридичного відділу — Сергій ОРЛОВ

Додаток 1
Зразок оформлення заяви

В. о. ректора Національного аерокосмічного університету «Харківський авіаційний інститут»

Олексію ЛИТВИНОВУ

_____
П.І.Б.
який/яка зареєстрований/зареєстрована за адресою:
_____
_____
_____
тел. моб.: _____
e-mail: _____

ЗАЯВА

Прошу зарахувати мене слухачем/слухачкою Регіонального центру інформаційних технологій, кібербезпеки та захисту інформації Національного аерокосмічного університету «Харківський авіаційний інститут» та укласти зі мною договір на надання платних освітніх послуг для проходження навчання за програмою (необхідне позначити):

- ☐ Аудитор інформаційних технологій (з кібербезпеки)
- ☐ Фахівець з оцінки заходів захисту інформації (кібербезпеки)
- ☐ Фахівець з реагування на інциденти кібербезпеки
- ☐ Фахівець сфери захисту інформації

З умовами надання платної освітньої послуги Центром інформаційних технологій, кібербезпеки та захисту інформації Національного аерокосмічного університету «Харківський авіаційний інститут» ознайомлений/ознайомлена та зобов'зуюсь дотримуватись.

Оплату за надану освітню послугу на умовах договору гарантую.

До заяви додаю:

1. Копія паспорту (ID-картка, посвідка на постійне місце проживання, посвідчення біженця, посвідчення особи, яка потребує додаткового захисту тощо).
2. Копії документів про освіту з додатками (1 примірник).
3. Копія трудової книжки (1 примірник), усі сторінки із записами та помітками.
4. Лист роботодавця про направлення працівника на навчання (за наявності).
5. Фотокартка (1 одиниця) 3х4 см та графічний файл з фотокарткою у форматі .tif або .jpg розміром 3х4 см (роздільна здатність 300 пікселів/дюйм, не нижче), збережений у форматі .pdf.
6. Згода на оброблення персональних даних (за формою).
7. Інші документи, що підтверджують кваліфікацію та/або професійну компетентність.

«___» _____ 20__ року _____ /_____/

Додаток 2
програми підвищення кваліфікації, що реалізуються Регіональним тренінговим центром інформаційних технологій, кібербезпеки та захисту інформації

Всі програми підвищення кваліфікації, що реалізуються Центром, розроблені відповідно до вимог чинних професійних стандартів, нормативно-правових актів у сфері захисту інформації та кібербезпеки, а також рекомендацій Міністерства освіти і науки України щодо організації підвищення кваліфікації.

Типові навчальні програми:

1. **«Аудитор систем менеджменту інформаційної безпеки»** розроблена за професійним стандартом «Аудитор інформаційних технологій (з кібербезпеки)».

Обсяг програми: 180 годин, **6** кредитів ЄКТС

Форма навчання: змішана (офлайн/онлайн)

Мета: формування у здобувачів курсів системи професійних знань, вмінь та навичок щодо організації і супроводу процесів проведення внутрішнього та зовнішнього аудиту об'єктів інформатизації для надання об'єктивних якісних і кількісних оцінок про поточний стан інформаційної безпеки організації у відповідності з визначеними в нормативно-правовій базі критеріями та показниками безпеки. Формування рекомендацій, на основі наданих оцінок, для посилення системи менеджменту інформаційної безпеки (далі – СМІБ), підтримки планів стійкості, відновлення штатного функціонування інфраструктури організації після інцидентів та нештатних ситуацій.

Формування у здобувачів курсів системи спеціальних знань щодо організації та супроводу процесів моніторингу й аудиту кібернетичної безпеки у відповідності до критеріїв і показників якості безпеки, організації і контролю системи мінімізації ризиків, методів та засобів одержання об'єктивних оцінок про поточний стан інформаційної системи та інформаційної інфраструктури організації в цілому.

Завдання:

– використовувати на практиці нормативні документи в галузі аудиту кібернетичної безпеки;

– проводити аудит і сертифікацію (атестацію) систем, підсистем інформаційної безпеки та систем управління інформаційною безпекою;

– визначати рівень якості та проведення контролю інфраструктури на основі критеріїв оцінки, технологій і методологій оцінювання стану кібербезпеки, ефективності функцій захисту інформації та рівня гарантій та їх коректності;

– проводити аналіз та володіти базовими технологіям визначення рівня ефективності систем і процесів інформаційної та кібернетичної безпеки підприємств та організацій;

– формувати звіти по результатам аналізу, процедурам проведеного аудиту і моніторингу, надавати рекомендації й пропозиції щодо протидії кіберінцидентам, підвищенню якості функціонування кібернетичної безпеки, а також інфраструктури організації в цілому.

Програмні результати навчання у відповідності до трудових функцій професійного стандарту та визначеної кваліфікації (далі – ТФ):

ТФ А РН 1	Формування (підготовка), впровадження та виконання процедур внутрішнього аудиту інформаційних систем і технологій на основі визначення й прогнозування ризиків з метою забезпечення безпеки інформації та/або кібербезпеки інформаційних ресурсів, виконання стратегічних планів функціонування й розвитку інформаційної інфраструктури організації.
ТФ Б РН 2	Контроль та оцінювання ефективності поточного стану функціонування інформаційної системи, проведення незалежних оглядів (або/чи планових) для оцінювання ефективності сталих інформаційних процесів з метою підтвердження довіри до інформаційних систем і технологій та забезпечення встановленої стратегії і політик безпеки інформації та/або кібербезпеки організації.
ТФ Г РН 3	Розробка планів, впровадження та виконання процедур або/чи відповідних дій контролю для забезпечення управління інцидентами, безперервності сталих операційних процесів, підтримки планів стійкості, відновлення штатного функціонування інфраструктури організації після інцидентів та нештатних ситуацій викликаних реалізацією кібератак різного класу.
ТФ Є РН 4	Формування (підготовка), впровадження та виконання процедур внутрішнього аудиту та/або операційного аудиту систем менеджменту інформаційної безпеки організації, а також об'єктів критичної інфраструктури на основі чинного законодавства, вітчизняної та міжнародної системи стандартизації та кращих світових практик.
ТФ Ж РН 5	Контроль та оцінка ефективності поточного стану функціонування системи менеджменту інформаційної безпеки організації (в т.ч. об'єктів критичної інфраструктури), оцінювання ефективності сталих бізнес-операційних процесів з метою забезпечення встановленої мети, стратегії, політик безпеки різного рівня згідно з вітчизняними та міжнародними вимогами і стандартами.

2. «Фахівець з оцінки заходів захисту інформації (кібербезпеки)» розроблена за професійним стандартом «Фахівець з оцінки заходів захисту інформації (кібербезпеки)»
Обсяг програми: 180 годин, **6** кредитів ЄКТС
Форма навчання: змішана (офлайн/онлайн)

Мета: формування у здобувачів курсів системи професійних знань, вмінь та навичок щодо стратегічного управління кіберризиками, забезпечення стійкості та безперервності бізнес-процесів в умовах постійних кіберзагроз. Набуття здобувачами курсів системи теоретичних знань щодо теорії ризиків, нормативно-правової бази в сфері інформаційної безпеки, технічної експертизи. Формування практичних навичок аудиту та тестування, розвиток управлінських та аналітичних компетенцій.

Завдання:

- планувати та проводити огляди авторизації та безпеки;
- розробляти процеси відповідності безпеки та/або аудитів;
- проводити оцінку ефективності засобів контролю безпеки;
- оцінювати всі процеси управління конфігурацією, здійснювати моніторинг;

– виконувати перегляд та аналіз безпеки, визначати недоліки, формувати плани усунення вразливостей. рекомендації для зниження ризиків;

– формувати звіти по результатам аналізу, процедурам проведеного аудиту і моніторингу, надавати рекомендації й пропозиції щодо протидії кіберінцидентам, сприяти підвищенню якості функціонування кібернетичної безпеки, а також інфраструктури організації в цілому.

Програмні результати навчання у відповідності до трудових функцій професійного стандарту та визначеної кваліфікації:

ТФ А РН 1	Оцінювання ефективності засобів контролю безпеки, зокрема огляд авторизації безпеки та аудит зовнішніх послуг. Розробка кейсів впевненості та огляд авторизації безпеки.
ТФ Б РН 2	Оцінювання дотримання заходів забезпечення відповідності, у тому числі з аналізом процесів управління конфігураціями та дотриманням встановлених обмежень прикладного програмного забезпечення, мереж або систем.
ТФ Г РН 3	Виконання аналізу системи безпеки та її ризиків, перегляд безпеки архітектури, управління ризиками з наданням відповідних рекомендацій, даних та документів для включення в стратегію зниження ризиків та розробку плану управління ризиками.
ТФ Є РН 4	Нагляд за дотриманням належного опису, оновленню та документуванню діяльності, проектування та розвитку кібербезпеки, зокрема безпеки прикладної системи, системи та мережі, а також керування пакетами документів з акредитації.

3. «Фахівець сфери захисту інформації» розроблена за професійним стандартом «Фахівець сфери захисту інформації»

Обсяг програми: 180 годин, **6** кредитів ЄКТС

Форма навчання: змішана (офлайн/онлайн)

Мета: формування у здобувачів курсу комплексної системи професійних знань, вмінь та навичок, необхідних для практичного забезпечення захищеності (конфіденційності, цілісності, доступності) інформації, що обробляється та передається в сучасних інформаційних, електронних комунікаційних та інформаційно-комунікаційних системах. Програма готує фахівця, здатного ефективно протидіяти широкому спектру загроз, зокрема несанкціонованим діям з інформацією, її витоку технічними каналами та спеціальним впливам на засоби обробки. Окремим важливим завданням є формування навичок для захисту інформації, що озвучується на об'єктах інформаційної діяльності, через освоєння всього життєвого циклу комплексних систем захисту.

Завдання:

– аналізувати потреби та вимоги щодо захисту інформації, виявляти, досліджувати та системно аналізувати загрози для інформації, оцінювати ризики безпеки інформації та кібербезпеки, розробляти моделі загроз та порушників;

– формувати стратегію і політики безпеки інформації, аналізувати, розробляти та супроводжувати систему управління інформаційною безпекою підприємства/організації;

– проєктувати та впроваджувати комплексні системи захисту інформації, програмні та апаратні засоби технічного захисту інформації, адмініструвати системи безпеки інформації;

– проводити спеціальні дослідження засобів обробки інформації, технічних засобів та об'єктів інформаційної діяльності для виявлення технічних каналів витоку інформації;

– здійснювати оцінку відповідності (атестацію, державну експертизу) комплексних систем захисту інформації, комплексів технічного захисту інформації, програмних та апаратних засобів технічного та криптографічного захисту, систем управління інформаційною безпекою;

– забезпечувати експлуатацію та обслуговування систем і комплексів захисту інформації, підтримувати їх у робочому стані, оцінювати надійність та здійснювати контроль працездатності;

– здійснювати постійний моніторинг та аудит загроз для інформації, проводити процедури сканування вразливостей, контролювати стан технічного та криптографічного захисту інформації;

– розробляти технічну документацію, положення та інструкції щодо систем і комплексів захисту інформації.

Програмні результати навчання у відповідності до трудових функцій професійного стандарту та визначеної кваліфікації:

ТФ А РН 1	Впровадження систем та комплексів захисту інформації.
ТФ Б РН 2	Оцінювання відповідності систем, комплексів та засобів захисту інформації.
ТФ В РН 3	Експлуатація та обслуговування систем і комплексів захисту інформації, моніторинг та аудит загроз для інформації.
ТФ Г РН 4	Оцінювання відповідності програмних та апаратних засобів технічного та криптографічного захисту інформації.

4. **«Фахівець з реагування на інциденти кібербезпеки»** розроблена за професійним стандартом «Фахівець з реагування на інциденти кібербезпеки»

Обсяг програми: 180 годин, **6** кредитів ЄКТС

Форма навчання: змішана (офлайн/онлайн)

Мета: формування у здобувачів курсів системи професійних знань, вмінь та навичок щодо організації і супроводу процесів проведення аналізу, оцінки інцидентів кібербезпеки в рамках мережевого середовища та реагування на них. Усунення інцидентів кібербезпеки та пом'якшення їх наслідків. Відстеження, оцінка стану кібербезпеки систем та своєчасне повідомлення про інциденти кібербезпеки. Відновлення функціональності систем і процесів до робочого стану. Дослідження та аналіз заходів реагування, оцінка ефективності та покращення існуючих практик. Накопичення та проведення аналізу даних про кіберзагрози.

Завдання:

– використовувати на практиці нормативні документи в галузі реагування на інциденти кібербезпеки;

– відстежувати, збирати та документувати дані про інциденти кібербезпеки;

– проводити оцінку інцидентів кібербезпеки;

– обробляти інциденти кібербезпеки в режимі реального часу та вживати заходів щодо пом'якшення їх наслідків;

– здійснювати відновлення функціональності системи та процесів до робочого стану після інцидентів кібербезпеки;

– здійснювати моніторинг та оцінку поточного стану кібербезпеки;

– надавати експертну технічну підтримку з управління інцидентами кібербезпеки;

– досліджувати та аналізувати інциденти кібербезпеки.

Програмні результати навчання у відповідності до трудових функцій професійного стандарту та визначеної кваліфікації::

ТФ А РН 1	Відстеження, збір та документування даних про інциденти кібербезпеки з моменту їх виявлення до остаточної ідентифікації статусу події
ТФ Б РН 2	Проведення оцінки інцидентів кібербезпеки
ТФ В РН 3	Оброблення інцидентів кіберзахисту в режимі реального часу та вжиття заходів щодо пом'якшення наслідків кібербезпекових інцидентів, а також відновлення функціональності системи та процесів до робочого стану
ТФ Г РН 4	Моніторинг та оцінка поточного стану кібербезпеки
ТФ Д РН 5	Надання експертної технічної підтримки з управління кіберінцидентами
ТФ Е РН 6	Дослідження та аналіз кіберінцидентів

ЛИСТ ОБЛІКУ ОЗНАЙОМЛЕННЯ

З Положенням ознайомлений:

Прізвище, ініціали	Посада	Дата	Підпис

Розроблено:	Перевірено:	Дійсне з:
Вячеслав ХАРЧЕНКО Сергій ЛУКАШЕВИЧ	Сергій ОРЛОВ Елеонора ДАРМОФАЛ	10.09.2025

ЛИСТ ОБЛІКУ ВНЕСЕННЯ ЗМІН

Номер змін	Дата введення в дію	Номер пункту, що змінюється	Прізвище, ініціали особи, яка зробила запис

Розроблено:	Перевірено:	Дійсне з:
Вячеслав ХАРЧЕНКО Сергій ЛУКАШЕВИЧ	Сергій ОРЛОВ Елеонора ДАРМОФАЛ	10.09.2025