

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

Національний аерокосмічний університет
«Харківський авіаційний інститут»

ЗАТВЕРДЖЕНО

вченою радою

Національного аерокосмічного
університету

«Харківський авіаційний інститут»

«21» травня 2025 р., протокол № 11

наказ № 235 від «22» травня 2025 р.

ОСВІТНЬО-ПРОФЕСІЙНА ПРОГРАМА

БЕЗПЕКА ІНФОРМАЦІЙНИХ І КОМУНІКАЦІЙНИХ СИСТЕМ

Рівень вищої освіти	перший (бакалаврський)
галузі знань	F «Інформаційні технології»
спеціальність	F5 «Кібербезпека та захист інформації»
кваліфікація	Бакалавр з кібербезпеки та захисту інформації

(із змінами, внесеними згідно із рішеннями
вченої ради ХАІ протокол № 11 від 27.05.2026 р.,
вченої ради ХАІ протокол № 01 від 19.08.2026 р.)

Освітня програма вводиться в дію
з «01» вересня 2026 р.

Ректор Національного аерокосмічного
університету
«Харківський авіаційний інститут»

Олексій ЛИТВИНОВ
наказ № 321 від «25» серпня 2026 р.



Харків 2026

ПЕРЕДМОВА

Освітньо-професійну програму «Безпека інформаційних і комунікаційних систем» для підготовки здобувачів першого (бакалаврського) рівня вищої освіти спеціальності F5 «Кібербезпека та захист інформації» галузі знань F «Інформаційні технології» в Національному аерокосмічному університеті «Харківський авіаційний інститут» (далі – ХАІ) започатковано з метою продовження реалізації освітньо-професійної програми «Безпека інформаційних і комунікаційних систем» (ID 60173) першого (бакалаврського) рівня вищої освіти спеціальності 125 «Кібербезпека та захист інформації» галузі знань 12 «Інформаційні технології» у зв'язку зі змінами у переліку галузей знань і спеціальностей, за якими здійснюється підготовка здобувачів вищої освіти відповідно до постанови Кабінету Міністрів України від 29 квітня 2015 р. № 266 (в редакції постанови Кабінету Міністрів України 30 серпня 2024 р. № 1021) «Перелік галузей знань і спеціальностей, за якими здійснюється підготовка здобувачів вищої та фахової передвищої освіти» з урахуванням:

- Національної рамки кваліфікацій (Постанова Кабінету Міністрів України від 23 грудня 2011 р., № 1341 (зі змінами));

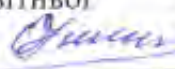
- стандарту вищої освіти зі спеціальності 125 «Кібербезпека та захист інформації» першого (бакалаврського) рівня вищої освіти (наказ МОН України від 29.10.2024 р. № 1547).

За освітньо-професійною програмою «Безпека інформаційних і комунікаційних систем» спеціальності F5 «Кібербезпека» першого (бакалаврського) рівня вищої освіти проведено модернізацію/оновлення структури компонент освітньої програми та змісту її опису у зв'язку:

- з введенням в дію Закону України «Про внесення змін до деяких законів України щодо окремих питань підготовки громадян України до національного спротиву» від 25.03.2026 р. №4826-IX (затверджено рішенням вченої ради від 27.05.2026 р., протокол № 11);

- зі змінами у Законі України «Про внесення змін до деяких законів України щодо окремих питань підготовки громадян України до національного спротиву» від 25.03.2026 р. №4826-IX (затверджено рішенням вченої ради від 19.08.2026 р., протокол № 01).

Модернізацію/оновлення освітньо-професійної програми «Безпека інформаційних і комунікаційних систем» (затверджено рішенням вченої ради від 27.05.2026 р., протокол № 11) проведено групою забезпечення ОПІ Національного аерокосмічного університету «Харківський авіаційний інститут» у складі:

- | | | |
|---|--|--|
| 1 | Гарант освітньої програми  ОЛЕГ ІЛЛЯШЕНКО | – кандидат технічних наук, доцент, доцент кафедри кібербезпеки та інтелектуальних інформаційних технологій |
| 2 | Члени групи:  ОЛЬГА МОРОЗОВА | – доктор технічних наук, доцент, професор кафедри кібербезпеки та інтелектуальних інформаційних технологій |
| 3 |  ДМИТРО УЗУН | – канд. техн. наук, професор кафедри кібербезпеки та інтелектуальних інформаційних технологій |
| 4 |  АНДРІЙ КАРПЕНКО | – доктор філософії, старший викладач кафедри кібербезпеки та інтелектуальних інформаційних технологій |

Рецензії-відгуки зовнішніх стейкхолдерів:

На освітню програму було отримано рецензії від керівників провідних підприємств аерокосмічної галузі України. Оригінали рецензій зберігаються на кафедрі кібербезпеки та інтелектуальних інформаційних технологій Національного аерокосмічного університету «Харківський авіаційний інститут». В електронному вигляді рецензії розміщено на сайті в розділі «Освітні програми і компоненти для бакалаврів» освітньо-професійної програми «Безпека інформаційних і комунікаційних систем» спеціальності F5 «Кібербезпека»

- | | | |
|---|---------------------------------|--|
| 1 | ТОВ НВП
«Залізничавтоматика» | Генеральний директор, к.т.н. Гаєвський В.В. |
| 2 | ТОВ НВП «Радікс» | Провідний науковий співробітник, д.т.н.,
проф., Одарущенко О.М. |

ВСТУП

Освітню програму розроблено відповідно до існуючої в Україні нормативно-правової бази та наявних стандартів, які регулюють питання запровадження та подальшого провадження освітньої діяльності.

Також розглянуто та опрацьовано вимоги з ESCO. Проаналізовано переліки обов'язкових та допоміжних навичок та компетентностей, а також переліки основних/обов'язкових знань та допоміжних знань. Зазначений підхід дозволяє гармонізувати освітню програму з вимогами європейського ринку праці та європейського простору вищої освіти.

Відповідно до ст. 1 «Основні терміни та їх визначення» Закону України «Про вищу освіту» від 01.07.2014 р. № 1556-VII (зі змінами) освітня програма – система освітніх компонентів на відповідному рівні вищої освіти в межах спеціальності, що визначає вимоги до рівня освіти осіб, які можуть розпочати навчання за цією програмою, перелік навчальних дисциплін і логічну послідовність їх вивчення, кількість кредитів ЄКТС, необхідних для виконання цієї програми, а також очікувані результати навчання (компетентності), якими повинен оволодіти здобувач відповідного ступеня вищої освіти.

Освітня програма використовується під час:

- акредитації освітньої програми, інспектування освітньої діяльності за спеціальністю та спеціалізацією;

- розроблення навчального плану, програм навчальних дисциплін і практик;
- розроблення засобів діагностики якості вищої освіти;
- визначення змісту навчання в системі перепідготовки та підвищення кваліфікації;
- професійної орієнтації здобувачів фаху.

Освітньо-професійна програма враховує вимоги Закону України «Про вищу освіту» від 01.07.2014 р. № 1556-VII (зі змінами), Постанову Кабінету Міністрів України «Про затвердження Національної рамки кваліфікацій» від 23.11.2011 р. № 1341 (зі змінами), стандарту вищої освіти зі спеціальності 125 «Кибербезпека та захист інформації» для першого (бакалаврського) рівня вищої освіти (наказ МОН України від 29.10.2024 р., № 1547) і встановлює:

- обсяг та термін навчання бакалаврів;
- загальні компетентності;
- фахові компетентності;
- програмні результати навчання;
- перелік та обсяг навчальних дисциплін для опанування компетентностей освітньо-професійної програми;
- вимоги до структури навчальних дисциплін.

Освітньо-професійна програма використовується для:

- складання навчальних планів та робочих навчальних планів;
- формування індивідуальних планів студентів;
- формування робочих програм навчальних дисциплін, практик;
- визначення інформаційної бази для формування засобів діагностики;
- акредитації освітньо-професійної програми;
- внутрішнього і зовнішнього контролю якості підготовки фахівців;
- атестації бакалаврів за освітньо-професійною програмою «Безпека інформаційних і комунікаційних систем» зі спеціальності F5 «Кибербезпека та захист інформації».

Користувачі освітньо-професійної програми:

- здобувачі вищої освіти, які навчаються в Національному аерокосмічному університеті «Харківський авіаційний інститут»;
- науково-педагогічні працівники, які здійснюють підготовку здобувачів за освітньо-професійною програмою «Безпека інформаційних і комунікаційних систем» зі спеціальності F5 «Кибербезпека та захист інформації»;
- екзаменаційна комісія спеціальності F5 «Кибербезпека та захист інформації»;
- приймальна комісія Національного аерокосмічного університету «Харківський авіаційний інститут».

Кафедри ХАІ, які залучені для підготовки фахівців ступеня бакалавра за освітньо-професійною програмою «Безпека інформаційних і комунікаційних систем» зі спеціальності F5 «Кибербезпека та захист інформації» керуються цією програмою для складання НМКД, навчальних планів, тощо.

1 НОРМАТИВНІ ПОСИЛАННЯ

Освітньо-професійна програма розроблена на основі таких нормативних документів і рекомендацій:

1.1 Закон України «Про вищу освіту». № 1556-УІІ від 01.07.2014 (зі змінами).

1.2 Постанова Кабінету Міністрів України «Про затвердження Національної рамки кваліфікацій» від 23.11.2011 р. № 1341 (зі змінами).

1.3 Стандарт вищої освіти за спеціальністю 125 «Кибербезпека та захист інформації» для першого (бакалаврського) рівня вищої освіти (наказ МОН України від 29.10.2024 р., № 1547).

1.4 Постанова Кабінету Міністрів України «Про затвердження переліку галузей знань і спеціальностей, за якими здійснюється підготовка здобувачів вищої освіти» від 29.04.2015 № 266 (зі змінами).

1.5 Постанова Кабінету Міністрів України «Про затвердження Положення про порядок реалізації права на академічну мобільність» від 12.08.2015 р. № 579.

1.6 Методичні рекомендації щодо розроблення стандартів вищої освіти, затверджені наказом Міністерства освіти і науки України від 27.03.2025 р. № 515 (розроблених членами сектору вищої освіти Науково-методичної ради Міністерства освіти і науки України та Національним агентством із забезпечення якості вищої освіти): <https://mon.gov.ua/static-objects/mon/sites/1/vishcha-osvita/2025/03/27/nakaz-mon-512-vid-27-03-2025.pdf>.

1.7 Положення «Про організацію освітнього процесу» Національного аерокосмічного університету «Харківський авіаційний інститут», затверджене вченою радою університету.

1.8 A Tuning Guide to Formulating Degree Programme Profiles Including Programme Competences and Programme Learning Outcomes. – Bilbao, Groningen and The Hague, 2010.

1.9 A TUNING-AHELO conceptual framework of expected/desired learning outcomes in engineering. OECD Education Working Papers, No. 60, OECD Publishing 2011. <http://dx.doi.org/10.1787/5kghtchn8mbn-en>.

1.10 Розроблення освітніх програм. Методичні рекомендації / Авт.: В.М. Захарченко, В.І. Луговий, Ю.М. Рашкевич, Ж.В. Таланова / За ред. В.Г. Кременя. – К. : ДП «НВЦ «Пріоритети», 2014. – 120 с.

1.11 Наказ МОН України «Про особливості запровадження переліку галузей знань і спеціальностей, за якими здійснюється підготовка здобувачів вищої освіти, затвердженого постановою Кабінету Міністрів України від 29 квітня 2015 року № 266» від 06.11.2015 № 1151 (зі змінами).

1.12 Класифікація видів економічної діяльності: ДК 009:2010. – Чинний від 01.01.2012. – (Національний класифікатор України).

1.13 Класифікатор професій: ДК 003:2010. – Чинний від 01.11.2010. – (Національний класифікатор України).

1.14 ESCO (European Skills, Competences, Qualifications and Occupations) — європейська багатомовна класифікація навичок, компетенцій і професій. Проєкт Європейської Комісії // Генеральний директорат із питань зайнятості, соціальних питань та інклюзії (DGEMPL).

1.15 Національний освітній глосарій: вища освіта / 2-е вид., перероб. ідоп. / Авт.-уклад.: В. М. Захарченко, С. А. Калашнікова, В. І. Луговий, А. В. Ставицький, Ю. М. Рашкевич, Ж. В. Таланова / За ред. В. Г. Кременя. – К.: ТОВ «Видавничий дім «Плеяди», 2014. – 100 с.

1.16 Закон України «Про внесення змін до деяких законів України щодо окремих питань підготовки громадян України до національного спротиву» від 25.03.2026 р. № 4826-ІХ.

2 ПРОФІЛЬ ОСВІТНЬО-ПРОФЕСІЙНОЇ ПРОГРАМИ
«БЕЗПЕКА ІНФОРМАЦІЙНИХ І КОМУНІКАЦІЙНИХ СИСТЕМ»
ЗІ СПЕЦІАЛЬНОСТІ F5 «КІБЕРБЕЗПЕКА ТА ЗАХИСТ ІНФОРМАЦІЇ»

1 – Загальна інформація	
Повна назва ЗВО та структурного підрозділу	Національний аерокосмічний університет «Харківський авіаційний інститут» Кафедра кібербезпеки та інтелектуальних інформаційних технологій National Aerospace University «Kharkiv Aviation Institute» Department of Cybersecurity and Intelligent Information Technologies
Ступінь вищої освіти	Бакалавр Bachelor's Degree
Галузь знань, спеціальність та назва кваліфікації	Галузь знань F Інформаційні технології Field of Study F Information Technologies Спеціальність F5 Кібербезпека та захист інформації Specialty F5 Cyber Security and Information Protection Кваліфікація: бакалавр з кібербезпеки та захисту інформації Qualification: Bachelor's Degree in Cyber Security and Information Protection
Офіційна назва ОПП	Безпека інформаційних і комунікаційних систем Security of Information and Communication Systems
Тип диплому та обсяг ОПП	Диплом бакалавра, одиничний, термін навчання 3 роки 10 місяців: – на базі повної загальної середньої освіти становить 240 кредитів ЄКТС; – на базі здобутих освітніх ступенів молодшого бакалавра, фахового молодшого бакалавра (освітньо-кваліфікаційного рівня молодшого спеціаліста) – 240 кредитів ЄКТС. При цьому ХАІ визнає та перераховує не більше ніж 60 кредитів ЄКТС, отриманих в межах попередньої освітньої програми підготовки фахівців.
Наявність акредитації	Започатковано провадження освітньої діяльності з 2025 р. Оновлення або модернізація освітньої програми здійснюється відповідно до розділу 5 Положення «Про розроблення та модернізацію освітніх програм в ХАІ».
Цикл/рівень	НРК Україна – 6 рівень, FQ-EHEA – перший цикл, EQF-LLL – 6 рівень
Передумови	Особа має право здобувати ступень бакалавра за умови наявності повної загальної середньої освіти та/або ступеня молодшого бакалавра, фахового молодшого бакалавра або освітньо-кваліфікаційного рівня молодшого спеціаліста в порядку, визначеному законодавством.
Мова(и) викладання	Мовою викладання є державна мова. З метою створення умов для міжнародної академічної мобільності може бути прийнято рішення про викладання однієї чи декількох дисциплін англійською та/або іншими іноземними мовами.
Інтернет-адреса постійного розміщення опису ОПП	https://khai.edu/profil-id-77301
2 – Мета освітньої програми	
Підготовка висококваліфікованих фахівців (бакалаврів) у галузі інформаційних технологій зі спеціальності F5 «Кібербезпека та захист інформації», компетентності яких відповідають сучасним вимогам роботодавців та перспективі розвитку ринку праці цифровізації та кібербезпеки с сфері інформаційних технологій, в аерокосмічній, машинобудівній, енергетичній та суміжних галузях згідно до стратегії розвитку Національного аерокосмічного університету «Харківський авіаційний інститут» на 2020-2030 роки.	

3 – Характеристика освітньо-професійної програми	
Предметна область	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: принципи, 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).
Орієнтація освітньої програми	Освітньо-професійна програма.
Основний фокус ОПП	Освітньо-професійна програма встановлює кваліфікаційні вимоги до соціально-виробничої діяльності випускників закладу вищої освіти зі спеціальності F5 «Кібербезпека та захист інформації» освітнього ступеня «бакалавр з кібербезпеки та захисту інформації» і державні вимоги до властивостей та якостей особи, що здобула освітній рівень відповідного фахового спрямування за освітньо-професійною програмою «Безпека інформаційних і комунікаційних систем». Базовий фокус – системи та процеси кіберпростору, засоби та заходи захисту. Програма містить дисципліни загальної та професійної підготовки, що мають інтегральний характер, змістовно спрямовані навчальні дисципліни обов’язкового і вільного вибору здобувачів для забезпечення підготовки фахівців у сфері сучасних методів розроблення, впровадження і супровіду автоматизованих систем кібербезпеки у сферах інформаційних технологій, в аерокосмічній, машинобудівній, енергетичній та суміжних галузях.
Особливості програми	Програма забезпечує розвиток аерокосмічної та інших високотехнологічних галузей в Україні та світі шляхом ґрунтовної фундаментальної підготовки фахівців з кібербезпеки та захисту інформації, здатних виконувати розроблення апаратних, програмних і мережних рішень для аналізу, оцінювання та забезпечення кібербезпеки шляхом власного розроблення, або на основі готових компонент, а також здатних здійснювати комплексний захист та управління інформаційною та/або кібербезпекою, у поєднанні із сучасною професійною підготовкою, яка дозволяє проводити інноваційну діяльність і працювати з наукоємними та бізнес-орієнтовними технологіями кібербезпеки, що передбачає формування потрібних знань та компетентностей. Освітня програма спрямована на вивчення професійних та соціальних навичок, які сприятимуть реалізації напряму наскрізного підходу до систем забезпечення інформаційною та/або кібербезпекою в інформаційно-комунікаційних системах, що починається з побудови моделі загроз і закінчується побудовою системи захисту з урахуванням специфіки сфер інформаційних технологій, аерокосмічної, машинобудівної, енергетичної та суміжних галузей. Практика проводиться на підприємствах різних галузей промисловості.

4 – Придатність випускників до працевлаштування та подальшого навчання	
Придатність до працевлаштування	На посади у структурних підрозділах установ/підприємств/організацій, які передбачають наявність вищої освіти зі спеціальності 125 «Кібербезпека та захист інформації».
Подальше навчання	Мають право на здобуття освіти на другому (магістерському) рівні вищої освіти. Здобуття або вдосконалення освіти та професійної підготовки в системі освіти дорослих.
5 – Викладання та оцінювання	
Викладання та навчання	Студентсько-центроване навчання, самонавчання, проблемно-орієнтоване навчання спрямоване на розвиток критичного і творчого мислення, навчання через лабораторну практику, дуальну, дистанційну освіту тощо. Лекції, мультимедійні лекції, лабораторні роботи, семінари, практичні заняття в малих групах, самостійна робота на основі підручників та конспектів, консультації із викладачами, підготовка кваліфікаційної роботи бакалавра.
Оцінювання	Письмові іспити, звіти з практик, презентації, поточний (модульний) контроль, кваліфікаційна робота бакалавра та її захист, Єдиний державний кваліфікаційний іспит (ЄДКІ) або атестаційний екзамен за спеціальністю в установленому порядку.
6 – Програмні компетентності	
Інтегральна компетентність	Здатність розв'язувати складні спеціалізовані задачі і практичні завдання у галузі кібербезпеки та захисту інформації.
Загальні компетентності (ЗК)	Компетентності визначені стандартом вищої освіти ЗК1. Здатність застосовувати знання у практичних ситуаціях. Еквівалент в ESCO – develop strategy to solve problems Uri: http://data.europa.eu/esco/skill/7a8fb784-67fa-41e9-a75c-6b491d91f800 ЗК2. Знання та розуміння предметної області і розуміння професійної діяльності. Еквівалент в ESCO – cyber security Uri: http://data.europa.eu/esco/skill/8088750d-8388-4170-a76f-48354c469c44 Еквівалент в ESCO – information security strategy Uri: http://data.europa.eu/esco/skill/11eebd42-44ab-401d-8a2c-bdb9fc9beb5 ЗК3. Здатність спілкуватися державною мовою як усно, так і письмово. Еквівалент в ESCO – interact verbally in Ukrainian Uri: http://data.europa.eu/esco/skill/cda53197-9c99-404a-ac8a-d8c8550ca98d Еквівалент в ESCO – write Ukrainian Uri: http://data.europa.eu/esco/skill/0e91219a-e74a-46e6-bcf9-9e14da031343 ЗК4. Здатність спілкуватися іноземною мовою. Еквівалент в ESCO – using foreign languages Uri: http://data.europa.eu/esco/skill/03961960-e729-4768-ab0a-49886132f17a ЗК5. Здатність вчитися і оволодівати сучасними знаннями. Еквівалент в ESCO – manage personal professional development URI: http://data.europa.eu/esco/skill/a8d24a95-47b3-4f88-92e7-06600bcd3612 Еквівалент в ESCO – demonstrate willingness to learn URI: http://data.europa.eu/esco/skill/9bf266a6-188b-4d17-a22f-2f266d76832b 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. Еквівалент в ESCO – promote human rights implementation URI: http://data.europa.eu/esco/skill/5ff0df56-48a7-4f84-937f-ba9a88182f3f Еквівалент в ESCO – international human rights law URI: http://data.europa.eu/esco/skill/24e4b3c9-286f-423f-ac43-54c9b8d92c5e Еквівалент в ESCO – promote sustainability URI: http://data.europa.eu/esco/skill/469e19ed-a0bd-445a-ae2d-4ba9430e296b ЗК7. Здатність ухвалювати рішення й діяти дотримуючись принципу неприпустимості корупції та будь-яких інших проявів недоброчесності. Еквівалент в ESCO – following ethical code of conduct

	URI: http://data.europa.eu/esco/skill/925af2b5-2f4d-4cce-92cc-79e1ff887c7d Еквівалент в ESCO – apply research ethics and scientific integrity principles in research activities URI: http://data.europa.eu/esco/skill/833289fa-3646-4010-9d9e-93ba8c9ef2d8 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. Еквівалент в ESCO – morality URI: http://data.europa.eu/esco/skill/7cf2762d-32e1-4b21-8ef8-574e40310c18 Еквівалент в ESCO – cultural history URI: http://data.europa.eu/esco/skill/d51ca82a-1a70-449d-91b3-9465f7ba905c Еквівалент в ESCO – promote healthy lifestyle URI: http://data.europa.eu/esco/skill/988c06ea-7ab9-4ee4-a64b-9e93f2527c6d <i>Додаткові компетенції:</i> ЗК9. Здатність забезпечувати особисту та колективну безпеку, діяти відповідально в умовах воєнних загроз і кризових ситуацій, застосовуючи базові знання та практичні навички національного спротиву, психологічної та домедичної допомоги, інформаційної та мінної безпеки, сучасних технологій і засобів комунікації.
Спеціальні (фахові предметні) компетентності (СК)	СК1. Здатність застосовувати законодавчу та нормативно-правову базу, а також державні і міжнародні вимоги, практики і стандарти у професійній діяльності. Еквівалент в ESCO – ICT security legislation URI: http://data.europa.eu/esco/skill/7814e88f-c133-4c3b-b27f-857afa145d42 Еквівалент в ESCO – ICT security standards URI: http://data.europa.eu/esco/skill/3ff589b7-68df-4ea5-ae41-b395bdb2378f Еквівалент в ESCO – manage IT security compliances URI: http://data.europa.eu/esco/skill/06358891-8424-43c5-891e-d40f226bef40 СК2. Здатність використовувати інформаційні технології, сучасні методи і моделі кібербезпеки та системи захисту інформації. Еквівалент в ESCO – cyber security URI: http://data.europa.eu/esco/skill/8088750d-8388-4170-a76f-48354c469c44 Еквівалент в ESCO – manage system security URI: http://data.europa.eu/esco/skill/2a3a96a3-709e-4d60-81f6-d247d6933f13 СК3. Здатність забезпечувати неперервність бізнес-процесів згідно встановленої політики кібербезпеки та захисту інформації. Еквівалент в ESCO – maintain plan for continuity of operations URI: http://data.europa.eu/esco/skill/909a28ce-d4b6-4567-9b74-d111f1ed9633 Еквівалент в ESCO – apply information security policies URI: http://data.europa.eu/esco/skill/86d2e2ea-1ba2-4aa6-b465-8a1f9abc81b8 СК4. Здатність забезпечувати захист інформації в інформаційних та інформаційно-комунікаційних системах згідно встановленої політики кібербезпеки й захисту інформації. Еквівалент в ESCO – apply information security policies URI: http://data.europa.eu/esco/skill/86d2e2ea-1ba2-4aa6-b465-8a1f9abc81b8 Еквівалент в ESCO – manage system security URI: http://data.europa.eu/esco/skill/2a3a96a3-709e-4d60-81f6-d247d6933f13 СК5. Здатність відновлювати функціонування інформаційних та інформаційно-комунікаційних систем після реалізації загроз, здійснення кібератак, збоїв і відмов різних класів та походження. Еквівалент в ESCO – implement ICT recovery system URI: http://data.europa.eu/esco/skill/fc2f1d4f-a46f-471e-a618-cbd4d0496a53

	Еквівалент в ESCO – manage disaster recovery plans URI: http://data.europa.eu/esco/skill/64852ade-6ae1-4760-ba4a-976bf07ca255 СК6. Здатність впроваджувати та забезпечувати функціонування комплексних систем захисту інформації (комплексні нормативно-правових, організаційних та технічних засобів і методів, процедур, практичних прийомів тощо). Еквівалент в ESCO – apply information security policies URI: http://data.europa.eu/esco/skill/86d2e2ea-1ba2-4aa6-b465-8a1f9abc81b8 Еквівалент в ESCO – integrate system components URI: http://data.europa.eu/esco/skill/ed8de897-adbe-4f0e-b4d2-534953e64c72 Еквівалент в ESCO – manage system security URI: http://data.europa.eu/esco/skill/2a3a96a3-709e-4d60-81f6-d247d6933f13 СК7. Здатність здійснювати професійну діяльність на основі впровадженої системи управління інформаційною та кібербезпекою. Еквівалент в ESCO – develop information security strategy URI: http://data.europa.eu/esco/skill/3579208e-49b3-4ce4-98e7-20e41b1ce8d4 Еквівалент в ESCO – implement ICT risk management URI: http://data.europa.eu/esco/skill/69cfc5ed-6569-4aca-a4cc-fd782ba51d9c Еквівалент в ESCO – manage IT security compliances URI: http://data.europa.eu/esco/skill/06358891-8424-43c5-891e-d40f226bef40 СК8. Здатність застосовувати методи та засоби криптографічного захисту інформації на об'єктах інформаційної діяльності. Еквівалент в ESCO – ICT encryption URI: http://data.europa.eu/esco/skill/d32db06e-bd06-4415-a7ab-1b0ee68caa9a СК9. Здатність застосовувати методи та засоби технічного захисту інформації на об'єктах інформаційної діяльності. Еквівалент в ESCO – manage technical security systems URI: http://data.europa.eu/esco/skill/1ebc1454-b6cb-4e45-a96a-17399961ad39 Еквівалент в ESCO – information confidentiality URI: http://data.europa.eu/esco/skill/a56dec32-05ef-45de-a256-ee6741f356db СК10. Здатність виконувати моніторинг інформаційних процесів, аналізувати, виявляти, оцінювати можливі вразливості та загрози інформаційному простору й інформаційним ресурсам згідно з встановленою політикою інформаційної безпеки. Еквівалент в ESCO – identify ICT security risks URI: http://data.europa.eu/esco/skill/felc2b32-7fe9-4668-affa-07ff658a68cf Еквівалент в ESCO – identify ICT system weaknesses URI: http://data.europa.eu/esco/skill/dad7e408-162f-46a4-8567-db560e19e2fc Еквівалент в ESCO – perform ICT security testing URI: http://data.europa.eu/esco/skill/f4a85869-1855-45d5-a43c-7ee8cd451996
7 – Результати навчання	
Результати навчання визначені стандартом вищої освіти	
PH1. Вільно спілкуватися державною мовою усно та письмово при виконанні професійних обов'язків.	
Еквівалент в ESCO – interact verbally in Ukrainian	
URI: http://data.europa.eu/esco/skill/cda53197-9c99-404a-ac8a-d8c8550ca98d	
Еквівалент в ESCO – write Ukrainian	
URI: http://data.europa.eu/esco/skill/0e91219a-e74a-46e6-bcf9-9e14da031343	
PH2. Спілкуватися іноземною мовою з метою забезпечення ефективності професійної комунікації.	
Еквівалент в ESCO – communicate commercial and technical issues in foreign languages	
URI: http://data.europa.eu/esco/skill/6bc57b80-37c8-4c9a-be7b-960d2e44fb77	
Еквівалент в ESCO – using foreign languages	
URI: http://data.europa.eu/esco/skill/03961960-e729-4768-ab0a-49886132f17a	

PH3. Застосовувати принцип неприпустимості корупції та будь-яких інших проявів недобросовісності у професійній діяльності.

Еквівалент в ESCO – following ethical code of conduct

URI: <http://data.europa.eu/esco/skill/925af2b5-2f4d-4cce-92cc-79e1ff887c7d>

PH4. 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.

Еквівалент в ESCO – develop strategy to solve problems

URI: <http://data.europa.eu/esco/skill/7a8fb784-67fa-41e9-a75c-6b491d91f800>

Еквівалент в ESCO – evaluate information

URI: <http://data.europa.eu/esco/skill/7dd94ad3-13d6-43fe-8b94-51fcbf67ced9>

PH5. 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.

Еквівалент в ESCO – address problems critically

URI: <http://data.europa.eu/esco/skill/b9f16465-56a9-426b-a047-0f9f1f95ec92>

Еквівалент в ESCO – make decisions

URI: <http://data.europa.eu/esco/skill/d62d2b4c-a6f8-439e-8a1b-4f29ab5f2c47>

Еквівалент в ESCO – show responsibility

URI: <http://data.europa.eu/esco/skill/199f7919-5114-41b6-b6a5-41e0e4896ec1>

PH6. Адаптуватися до нових умов і технологій професійної діяльності, прогнозувати кінцевий результат.

Еквівалент в ESCO – adapt to change

URI: <http://data.europa.eu/esco/skill/49de9958-2aa4-4eef-a89d-fe5d5bcd28c4>

Еквівалент в ESCO – monitor technology trends

URI: <http://data.europa.eu/esco/skill/7a17d7ce-01a2-4746-bbcc-22ffe22fa16e>

PH7. 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.

Еквівалент в ESCO – statistics

URI: <http://data.europa.eu/esco/skill/7ee4c2ea-b349-4bd2-81a3-ec31475d4833>

Еквівалент в ESCO – ICT encryption

URI: <http://data.europa.eu/esco/skill/d32db06e-bd06-4415-a7ab-1b0ee68caa9a>

Еквівалент в ESCO – signal processing

URI: <http://data.europa.eu/esco/skill/cfa2be0d-96d5-4017-a866-962efb9c5070>

Еквівалент в ESCO – cyber security

URI: <http://data.europa.eu/esco/skill/8088750d-8388-4170-a76f-48354c469c44>

PH8. 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.

Еквівалент в ESCO — mathematics

URI: <http://data.europa.eu/esco/skill/4339176e-3acd-4f7f-a5d9-445bee3d23f2>

Еквівалент в ESCO — physics

URI: <http://data.europa.eu/esco/skill/692ace70-7f97-4214-92bd-88f7637d8a44>

Еквівалент в ESCO — execute analytical mathematical calculations

URI: <http://data.europa.eu/esco/skill/31c69100-b612-4a61-8db5-fd314318854c>

PH9. Знати та застосовувати законодавство України та міжнародні вимоги, практики і стандарти з метою здійснення професійної діяльності в галузі кібербезпеки та захисту інформації.

Еквівалент в ESCO — ICT security legislation

URI: <http://data.europa.eu/esco/skill/7814e88f-c133-4c3b-b27f-857afa145d42>

Еквівалент в ESCO — ICT security standards

URI: <http://data.europa.eu/esco/skill/3ff589b7-68df-4ea5-ae41-b395bdb2378f>

Еквівалент в ESCO — manage IT security compliances

URI: <http://data.europa.eu/esco/skill/06358891-8424-43c5-891e-d40f226bef40>

PH10. Використовувати сучасні інформаційні технології, методи і моделі кібербезпеки та систем захисту інформації для здійснення професійної діяльності.

Еквівалент в ESCO – cyber security

URI: <http://data.europa.eu/esco/skill/8088750d-8388-4170-a76f-48354c469c44>

Еквівалент в ESCO – manage system security

URI: <http://data.europa.eu/esco/skill/2a3a96a3-709e-4d60-81f6-d247d6933f13>

PH11. Планувати підготовку та забезпечувати неперервність бізнес-процесів в організаціях згідно зі встановленою політикою кібербезпеки з урахування вимог до захисту інформації.

Еквівалент в ESCO – maintain plan for continuity of operations

URI: <http://data.europa.eu/esco/skill/909a28ce-d4b6-4567-9b74-d111f1ed9633>

Еквівалент в ESCO – apply information security policies

URI: <http://data.europa.eu/esco/skill/86d2e2ea-1ba2-4aa6-b465-8a1f9abc81b8>

PH12. Застосовувати методи та засоби захисту інформації в інформаційних та інформаційно-комунікаційних системах відповідно до встановленої політики інформаційної безпеки.

Еквівалент в ESCO – apply information security policies

URI: <http://data.europa.eu/esco/skill/86d2e2ea-1ba2-4aa6-b465-8a1f9abc81b8>

Еквівалент в ESCO – manage system security

URI: <http://data.europa.eu/esco/skill/2a3a96a3-709e-4d60-81f6-d247d6933f13>

PH13. 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.

Еквівалент в ESCO – install software

URI: <http://data.europa.eu/esco/skill/c8de8023-ab8a-402b-a828-b2b57cd3b2f7>

Еквівалент в ESCO – configure ICT system

URI: <http://data.europa.eu/esco/skill/b3c8eada-b0a8-4b61-968b-b354fbfb6874>

Еквівалент в ESCO – integrate system components

URI: <http://data.europa.eu/esco/skill/ed8de897-adbe-4f0e-b4d2-534953e64c72>

Еквівалент в ESCO – maintain ICT system

URI: <http://data.europa.eu/esco/skill/fbbcb9ab-4b95-4e57-a756-30d08b7da7a5>

PH14. 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.

Еквівалент в ESCO – implement ICT recovery system

URI: <http://data.europa.eu/esco/skill/fc2f1d4f-a46f-471e-a618-cbd4d0496a53>

Еквівалент в ESCO – perform backups

URI: <http://data.europa.eu/esco/skill/cf3e976d-2c3e-495c-a874-f9e8a66d3b48>

Еквівалент в ESCO — system backup best practice

URI: <http://data.europa.eu/esco/skill/47ca0da1-cae5-4395-ae6b-fd97b9ff48d3>

PH15. Збирати, обробляти, зберігати, аналізувати критичні дані для доказу реалізації кіберзагроз, проводити аналіз та дослідження кіберінциденту з метою оперативного відновлення функціонування інформаційної системи.

Еквівалент в ESCO — computer forensics

URI: <http://data.europa.eu/esco/skill/118a9b27-1c5a-4214-b685-1a4d9e6365ea>

Еквівалент в ESCO — gather data for forensic purposes

URI: <http://data.europa.eu/esco/skill/0c766ca3-9364-4203-916b-fed16e4814c1>

Еквівалент в ESCO — perform forensic preservations of digital devices

URI: <http://data.europa.eu/esco/skill/28a0fe16-4e03-4d5e-8f0e-5198309e77a9>

Еквівалент в ESCO — evaluate forensic data

URI: <http://data.europa.eu/esco/skill/9e136617-1cd1-4f71-af3e-9deda4c75bea>

Еквівалент в ESCO – implement ICT recovery system

URI: <http://data.europa.eu/esco/skill/fc2f1d4f-a46f-471e-a618-cbd4d0496a53>

PH16. Вирішувати задачі впровадження та супроводу комплексних систем захисту інформації в інформаційних системах.

Еквівалент в ESCO – apply information security policies

URI: <http://data.europa.eu/esco/skill/86d2e2ea-1ba2-4aa6-b465-8a1f9abc81b8>

Еквівалент в ESCO – integrate system components

URI: <http://data.europa.eu/esco/skill/ed8de897-adbe-4f0e-b4d2-534953e64c72>

Еквівалент в ESCO – manage system security

URI: <http://data.europa.eu/esco/skill/2a3a96a3-709e-4d60-81f6-d247d6933f13>

Еквівалент в ESCO – maintain ICT system

URI: <http://data.europa.eu/esco/skill/fbbcb9ab-4b95-4e57-a756-30d08b7da7a5>

PH17. 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.

Еквівалент в ESCO – develop information security strategy

URI: <http://data.europa.eu/esco/skill/3579208e-49b3-4ce4-98e7-20e41b1ce8d4>

Еквівалент в ESCO – implement ICT risk management

URI: <http://data.europa.eu/esco/skill/69cfc5ed-6569-4aca-a4cc-fd782ba51d9c>

Еквівалент в ESCO – apply crisis management

URI: <http://data.europa.eu/esco/skill/f780a6ad-b01e-4c35-9746-af8fc0c5ad06>

Еквівалент в ESCO – train employees

URI: <http://data.europa.eu/esco/skill/e54ff029-1ce9-447d-a5b2-eb7283a23e6e>

PH18. Аналізувати, застосовувати методи та засоби криптографічного захисту інформації на об'єктах інформаційної діяльності.

Еквівалент в ESCO – ICT encryption

URI: <http://data.europa.eu/esco/skill/d32db06e-bd06-4415-a7ab-1b0ee68caa9a>

PH19. Вирішувати задачі щодо організації та контролю стану криптографічного захисту інформації, зокрема відповідно до вимог нормативних документів.

Еквівалент в ESCO – ICT encryption

URI: <http://data.europa.eu/esco/skill/d32db06e-bd06-4415-a7ab-1b0ee68caa9a>

Еквівалент в ESCO – manage IT security compliances

URI: <http://data.europa.eu/esco/skill/06358891-8424-43c5-891e-d40f226bef40>

PH20. 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.

Еквівалент в ESCO – identify surveillance devices

URI: <http://data.europa.eu/esco/skill/15f97982-d453-453e-83d0-8037773f921d>

Еквівалент в ESCO — manage technical security systems

URI: <http://data.europa.eu/esco/skill/1ebc1454-b6cb-4e45-a96a-17399961ad39>

Еквівалент в ESCO — information confidentiality

URI: <http://data.europa.eu/esco/skill/a56dec32-05ef-45de-a256-ee6741f356db>

Еквівалент в ESCO — maintain computer hardware

URI: <http://data.europa.eu/esco/skill/c77db25e-bb51-4a10-b2ad-99b48b1b4a37>

PH21. 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.

Еквівалент в ESCO — use access control software

URI: <http://data.europa.eu/esco/skill/5da73370-f6b9-417d-a94c-09bf01f84aa2>

Еквівалент в ESCO — identify ICT system weaknesses

URI: <http://data.europa.eu/esco/skill/dad7e408-162f-46a4-8567-db560e19e2fc>

Еквівалент в ESCO – perform security vulnerability assessments

URI: <http://data.europa.eu/esco/skill/f4a85869-1855-45d5-a43c-7ee8cd451996>

Еквівалент в ESCO – manage system security

URI: <http://data.europa.eu/esco/skill/2a3a96a3-709e-4d60-81f6-d247d6933f13>

Додаткові програмні результати навчання

РН22. Застосовувати знання з основ національного спротиву, міжнародного гуманітарного права, тактичної медицини, мінної безпеки, навігації та інформаційної безпеки для збереження життя і здоров'я людей, протидії загрозам та ефективних дій в умовах воєнного стану, надзвичайних і кризових ситуацій.

8 – Ресурсне забезпечення реалізації програми

Кадрове забезпечення	Кадрове забезпечення формується, в основному за рахунок науково-педагогічних працівників кафедри комп'ютерних систем, мереж та кібербезпеки, професорсько-викладацький склад якої складається з достатньої кількості докторів технічних наук, професорів, кандидатів технічних наук та доцентів. До викладання дисциплін залучаються також інші кафедри Національного аерокосмічного університету «Харківський авіаційний інститут». Науково-педагогічні працівники, залучені до реалізації освітньої програми, відповідають вимогам щодо забезпечення провадження освітньої діяльності у сфері вищої освіти згідно з діючим законодавством України (Постанова Кабінету Міністрів України від 30 грудня 2015 р. № 1187 «Про затвердження Ліцензійних умов провадження освітньої діяльності» (із змінами)).
Матеріально-технічне забезпечення	Матеріально-технічне забезпечення відповідає вимогам Ліцензійних умов провадження освітньої діяльності у сфері вищої освіти згідно з діючим законодавством України (Постанова Кабінету Міністрів України від 30 грудня 2015 р. № 1187 «Про затвердження Ліцензійних умов провадження освітньої діяльності» (із змінами)) і забезпечує проведення всіх видів навчальних занять та практик, передбачених навчальним планом. Навчання здійснюється у навчальних лабораторіях, комп'ютерних класах кафедри комп'ютерних систем, мереж і кібербезпеки. Загальна площа, на якій розміщені приміщення кафедри складає 967,2 м². Навчальна площа на якій здійснюється освітній процес, складає 792,8 м². Територіально приміщення кафедри розташовані у двох навчальних корпусах. В усіх приміщеннях забезпечуються комфортні умови для навчання здобувачів та роботи викладачів. Кафедра комп'ютерних систем, мереж і кібербезпеки має власні комп'ютерні класи, площею 485,6 м², що обладнані 111 комп'ютерами, 9 мультимедійними проекторами, 1 мультимедійною дошкою для здобувачів вищої освіти. Навчання здійснюється у навчальних лабораторіях, комп'ютерних класах: - лабораторія системного програмування (ауд. 118 р.к.); - лабораторія якості програмних систем (ауд. 123 р.к.); - лабораторія критичного комп'ютерного (ауд. 132 р.к.); - лабораторія гарантоздатних розподілених обчислень (ауд. 135р.к.); - лабораторія мікропроцесорних засобів (ауд. 136-а р.к.); - лабораторія мережених технологій (ауд. 136-в р.к.); - лабораторія безпеки інформаційно-комунікаційних систем (ауд. 232б р.к.); - лабораторія проблем кібербезпеки (ауд. 229 р.к.); - лабораторія смартсистем і технічного захисту інформації (ауд. 230 р.к.)
Інформаційне та навчально-методичне забезпечення	Відповідно до вимог Ліцензійних умов провадження освітньої діяльності у сфері вищої освіти згідно з діючим законодавством України (Постанова Кабінету Міністрів України від 30 грудня 2015 р. № 1187 «Про затвердження Ліцензійних умов провадження освітньої діяльності» (із змінами)) включає в себе бібліотечні ресурси, електронні навчальні ресурси,

	сайт Національного аерокосмічного університету «ХАІ» та сайт кафедри комп'ютерних систем, мереж і кібербезпеки, на яких розміщена основна інформація щодо освітньої діяльності за ОПП. Зокрема, навчальне середовище містить такі системи інформаційного та навчально-методичного забезпечення: – навчально-методичні матеріали, які розміщені у бібліотеці і доступні через сайт бібліотеки Національного аерокосмічного університету ХАІ; – MENTOR – система підтримки дистанційного навчання Національного аерокосмічного університету «ХАІ»; – rSmart® SakaiCLE i Moodle – системи підтримки дистанційного навчання; – Google Classroom – система підтримки дистанційного навчання; – Google Cloud – хмарне сховище, на якому зберігаються кафедральна документація і кваліфікаційні роботи здобувачів; матеріали доступні публічно за умов дотримання встановлених правил безпеки; – UNICHECK – система перевірки на плагіат; – електронні системи PILOT, які використовуються для організації та керування освітнім процесом в Національному аерокосмічному університету "ХАІ". Для самостійної роботи студентів на кафедрі з кожної навчальної дисципліни розроблені контрольні завдання з чіткою вказівкою тем та необхідною літературою для їх виконання. Дисципліни, які вивчаються, забезпечені навчальними та робочими програмами, планами семінарських та практичних занять, методичними вказівками з їх виконання, пакетами контрольних завдань для комплексної перевірки з дисциплін фахової підготовки. Підготовлені методичні вказівки з написання курсових та дипломних робіт. Викладачі кафедри використовують авторські розробки та навчальні програми власної розробки для проведення навчальних занять.
9 – Академічна мобільність	
Національна кредитна мобільність	На основі двосторонніх договорів між Національним аерокосмічним університетом «Харківський авіаційний інститут» і технічними закладами України, зокрема: Інститут кібернетики імені В.М. Глушкова НАН України, ТОВ «482.СОЛЮШНС», ТОВ «SigmaSoftware», ТЗОВ «SoftServe», ТОВ «EramSystems», ТОВ «НВП «Радікс», ТОВ НВП «Залізничавтоматика».
Міжнародна кредитна мобільність	На основі двосторонніх договорів між Національним аерокосмічним університетом «Харківський авіаційний інститут» і навчальними закладами країн-партнерів: – меморандум про обмін співробітниками та здобувачами вищої освіти та про обмін технологіями та сумісне проведення наукових досліджень з Tallinn University of Technology (Естонія); – партнерська угода про наукову співпрацю з TALLINNA TEHNIKAULIKOOL (Естонія); – партнерська угода про наукову співпрацю з University of Newcastle upon Tyne (Великобританія); – Програма мобільності Erasmus+, Університет Тренто (Італія); – Стипендіальні програми Німецької Служби Академічних обмінів DAAD; – Лундський Університет (Швеція), стажування для викладачів; – Стамбульський технічний університет; – Академічна мобільність з Магдебурзьким технічним університетом ім. Отто фон Геріке; – Чеський Технічний Університет у м. Прага Стипендіальна програма Nikola Šohaj; – Академічна мобільність з Ecole Centrale de Nantes (ECN), Франція; – Академічна мобільність з Університетом Країни Басків, Іспанія.
Навчання іноземних здобувачів ВО	Навчання здійснюється державною мовою. У певних випадках може бути прийнято рішення про викладання однієї чи декількох дисциплін англійською та/або іншими іноземними мовами.

3 ПЕРЕЛІК КОМПОНЕНТ ОСВІТНЬО-ПРОФЕСІЙНОЇ ПРОГРАМИ (КОП) ТА ЇХ ЛОГІЧНА ПОСЛІДОВНІСТЬ

3.1 Перелік компонент освітньої програми

Код КОП	Компоненти освітньої програми (навчальні дисципліни, курсові проекти (роботи), практики, кваліфікаційна робота)	Кількість кредитів (семестр)	Форма підсумкового контролю
1	2	3	4
Обов'язкові компоненти ОП			
OK1	Вища математика	5 (1)	іспит
		5 (2)	іспит
OK2	Іноземна мова	3 (1)	залік
		3 (2)	диф. залік
OK3	Основи права	2 (1)	залік
OK4	Українська мова за професійним спрямуванням	2 (1)	залік
OK5	Дискретна математика	5,5 (1)	іспит
		4 (2)	іспит
OK6	Основи функціонування комп'ютерів	5,5 (1)	іспит
OK7	Технології програмування	5,5 (1)	іспит
		4,5 (2)	іспит
OK8	Фізика	5 (2)	залік
OK10	Комп'ютерна електроніка і схемотехніка	4 (2)	іспит
OK9	Філософія	3 (3)	залік
OK11	Архітектура комп'ютерів і квантових процесорів	3,5 (3)	іспит
OK12	Програмовні засоби безпеки	3,5 (3)	залік
OK13	Моделі та структури даних	3,5 (3)	іспит
OK14	Основи національного спротиву	3 (2)	диф. залік
		2 (3)	диф. залік
OK15	Технології безпечного програмування	3 (3)	залік
OK16	Апаратні та програмні засоби захисту інформації	3 (4)	іспит
OK17	Операційні системи	3,5 (4)	іспит
OK18	Системи технічного захисту інформації	3,5 (4)	залік
		3 (5)	іспит
OK19	Теоретичні основи криптології	3,5 (4)	іспит
OK20	Теорія інформації та кодування	3 (4)	залік
OK21	Технології безпечного програмування (КП)	2 (4)	диф. залік
OK22	Web-технології	3,5 (5)	залік
OK23	Інформаційно-комунікаційні системи	3 (5)	іспит
OK24	Безпечні вбудовані системи	3 (5)	залік
OK25	Прикладна криптологія	3 (5)	іспит
		3,5 (6)	іспит
OK26	Безпека засобів штучного інтелекту	3 (5)	залік
		3 (6)	іспит
OK27	Організація та безпека баз і сховищ даних	3,5 (6)	залік
OK28	Нормативно-правове забезпечення інформаційної безпеки	3,5 (6)	іспит
OK29	Побудова та кібербезпека інтернету речей	3 (6)	залік
OK30	Курсовий проєкт 1 (КП)	2 (6)	диф. залік
OK31	Економіка ІТ-проєктів	3 (7)	залік
OK32	Захист інформації в інформаційно-комунікаційних системах	3,5 (7)	іспит
		4 (8)	іспит
OK33	Комплексні системи захисту інформації: проектування, впровадження, супровід	3 (7)	іспит
		4,5 (8)	іспит
OK34	Управління інформаційною безпекою	3 (7)	залік
		4 (8)	залік
OK35	Функційна безпечність та надійність комп'ютерних систем	4 (7)	іспит
OK36	Курсовий проєкт 2 (КП)	2 (7)	диф. залік
OK37	Комплексні системи кібербезпеки	4,5 (8)	диф. залік
OK38	Навчальна практика	3 (2)	залік
OK39	Ознайомча практика	3 (4)	залік
OK40	Виробнича практика	3 (6)	залік
OK41	Комплексний курсовий проєкт (КП)	4,5 (8)	диф. залік
	Єдиний державний кваліфікаційний іспит/Атестаційний екзаме́н	-	Атестація
Загальний обсяг обов'язкових компонент:		180	

Код КОП	Компоненти освітньої програми (навчальні дисципліни, курсові проекти (роботи), практики, кваліфікаційна робота)	Кількість кредитів (семестр)	Форма підсумкового контролю
1	2	3	4
Вибіркові компоненти ОП			
Вибірковий блок дисциплін MINOR*			
BK1	Minor. Дисципліна 1	5 (5)	іспит
BK2	Minor. Дисципліна 2	5 (6)	іспит
BK3	Minor. Дисципліна 3	5 (7)	іспит
BK4	Minor. Дисципліна 4	5 (8)	іспит
Окремі вибіркові дисципліни			
BK5	Математично-технічний блок на вибір**	5 (4)	іспит
BK6	Дисципліна індивідуального вибору 1**	5 (6)	іспит
BK7	Дисципліна індивідуального вибору 2**	5 (7)	іспит
BK8	Дисципліна індивідуального вибору 3**	5 (8)	іспит
BK9	Дисципліна індивідуального вибору за фахом 1***	5 (3)	іспит
BK10	Дисципліна індивідуального вибору за фахом 2***	5 (3)	іспит
BK11	Дисципліна індивідуального вибору за фахом 3***	5 (4)	іспит
BK12	Дисципліна індивідуального вибору за фахом 4***	5 (5)	іспит
Загальний обсяг вибіркових компонент:		60	
ЗАГАЛЬНИЙ ОБСЯГ ОСВІТНЬОЇ ПРОГРАМИ:		240	

*Загальноуніверситетський блок, в якому блоки дисциплін для вибору пропонують кафедри Університету, що направлені на опанування і поглиблення певних компетентностей та результатів навчання, які можуть передбачати здобуття часткової професійної кваліфікації. До складу кожного блоку Minor входять чотири послідовних освітніх компоненти обсягом п'ять кредитів кожна. Здобувач може обрати будь-який блок дисциплін Minor. Блоки дисциплін Minor можуть оновлюватися за рішенням галузевої НМК.

** Здобувач обирає одну дисципліну із запропонованих у переліках освітніх компонент BK5-BK8, які пропонують кафедри Університету відповідно до напрямів своєї діяльності у рамках науково-методичних комісій Університету, що направлені на опанування і поглиблення певних компетентностей та результатів навчання. Переліки складових освітніх компонент BK5-BK89 можуть збільшуватися і оновлюватися за рішенням галузевої НМК.

***Здобувач обирає одну дисципліну із запропонованих у переліках освітніх компонент BK9-BK12, які пропонують кафедри Університету відповідно до напрямів своєї діяльності у рамках науково-методичних комісій Університету, які забезпечують опанування і поглиблення компетентностей та результатів навчання, що направлені на здобуття фахових навичок відповідно до вимог стандарту спеціальності. Переліки складових освітніх компонент BK9-BK12 можуть збільшуватися і оновлюватися за рішенням галузевої НМК.

Здобувач, який зарахований на базі повної загальної середньої освіти, виконує освітньо-професійну програму в обсязі 240 кредитів ЄКТС.

Здобувач, який зарахований на базі освітніх ступенів молодшого бакалавра, фахового молодшого бакалавра (освітньо-кваліфікаційного рівня молодшого спеціаліста) виконує освітньо-професійну програму в обсязі – 240 кредитів ЄКТС. При цьому ХАІ визнає та перераховує не більше ніж 60 кредитів ЄКТС, отриманих в межах попередньої освітньої програми підготовки фахівців.

Згідно з принципами компетентнісного підходу до здобуття вищої освіти перезарахування результатів раніше складених претендентом дисциплін відповідно до індивідуального навчального плану здійснюється за заявою претендента на підставі Положення «Про порядок перезарахування навчальних дисциплін і визначення академічної різниці в Національному аерокосмічному університеті «Харківський авіаційний інститут»» (<https://khai.edu/polozenna-pro-poradok-perezarahuvanna-navchalnih-disciplin-i-viznacenna-akademicnoi-riznici>) шляхом порівняння: відповідності змісту дисциплін освітньо-професійної програми (ОПП); запланованих результатів навчання з відповідної дисципліни; загального обсягу у годинах і кредитах ЄКТС; форм підсумкового контролю тощо.

3.2 Розподіл освітніх компонент освітньої програми (КОП) за курсами та семестрами

Під час формування переліку дисциплін, практик та атестації враховано вимоги Національної рамки кваліфікацій України, стандарту вищої освіти зі спеціальності F5 «Кибербезпека та захист інформації» для першого (бакалаврського) рівня вищої освіти, положення «Про організацію освітнього процесу у ХАІ» (<https://khai.edu/polozenna-pro-organizaciu-osvitnogo-procesu>) та відповідних нормативних документів.

Практики та/або стажування (за всіма видами) входять до складу обов'язкових навчальних дисциплін. Кількість форм контролю на навчальний рік не перевищує шістнадцять. Аудиторне навантаження становить від 1/3 до 2/3 загального обсягу навантаження.

Розподіл освітніх компонент освітньої програми (КОП) за курсами та семестрами надано у додатку А.

3.3 Структурно-логічна схема освітньої програми

Структурно-логічна схема (додаток Б) освітньої програми відображає послідовність вивчення її компонент, як обов'язкових, так і вибірових. Здобувачем вищої освіти обирається індивідуальна траєкторія навчання яка реалізується через обирання вибірових компонент згідно Положення «Про забезпечення права студентів на вибір навчальних дисциплін».

4 ФОРМА АТЕСТАЦІЇ ЗДОБУВАЧІВ ВИЩОЇ ОСВІТИ

Атестація здобувачів за освітньо-професійною програмою «Безпека інформаційних і комунікаційних систем» зі спеціальності F5 «Кибербезпека та захист інформації» здійснюється у формі Єдиного державного кваліфікаційного іспиту (ЄДКІ) або атестаційного екзамену відповідно до Постанови КМ України від 19 травня 2021 р. № 497.

Атестація завершується видачею документу встановленого зразка про присудження випускникам ступеня бакалавра із присвоєнням кваліфікації: бакалавр з кібербезпеки та захисту інформації.

Атестація здійснюється відкрито і публічно.

5 МАТРИЦЯ ВІДПОВІДНОСТІ ПРОГРАМНИХ КОМПЕТЕНТНОСТЕЙ ОБОВ'ЯЗКОВИМ КОМПОНЕНТАМ ОСВІТНЬО-ПРОФЕСІЙНОЇ ПРОГРАМИ

Програмні компетентності	Компоненти освітньої програми																																											
	OK 1	OK 2	OK 3	OK 4	OK 5	OK 6	OK 7	OK 8	OK 9	OK 10	OK 11	OK 12	OK 13	OK 14	OK 15	OK 16	OK 17	OK 18	OK 19	OK 20	OK 21	OK 22	OK 23	OK 24	OK 25	OK 26	OK 27	OK 28	OK 29	OK 30	OK 31	OK 32	OK 33	OK 34	OK 35	OK 36	OK 37	OK 38	OK 39	OK 40	OK 41			
ЗК1	+	+	+	+	+	+	+	+	+	+	+	+	+		+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+		
ЗК2	+	+		+	+		+	+			+	+	+		+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	
ЗК3			+	+		+	+		+	+	+	+	+		+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+		+	+	+	+	+	+	+	+	+	+	+	
ЗК4	+	+			+	+		+		+	+	+	+		+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+		+	+	+	+	+	+	+	+	+	+	+	+
ЗК5	+		+		+	+	+	+	+	+	+	+	+		+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+
ЗК6			+	+		+									+	+	+	+	+	+	+	+	+	+	+	+	+																+	
ЗК7			+																										+			+											+	
ЗК8		+						+																										+			+					+		
ЗК9														+																													+	
СК1			+												+	+		+	+		+			+	+			+		+	+	+	+	+	+	+	+	+	+	+	+	+	+	
СК2							+					+			+	+		+		+	+	+	+	+	+	+					+			+	+		+	+					+	
СК3													+			+	+	+	+	+	+						+			+		+	+	+	+	+	+	+	+				+	
СК4							+						+		+	+		+		+				+	+				+	+		+	+	+	+			+	+			+	+	
СК5					+		+	+		+	+	+			+		+					+		+										+	+		+						+	
СК6	+				+		+	+		+		+	+		+	+	+	+	+	+		+		+				+	+	+	+		+	+	+	+	+	+	+	+				+
СК7																									+				+					+	+	+			+				+	
СК8	+				+										+	+			+					+	+		+						+			+	+					+		
СК9												+			+	+		+							+					+							+	+	+	+	+	+	+	
СК10										+		+	+		+	+	+	+	+		+			+		+	+	+	+	+			+	+	+	+	+	+	+	+	+	+	+	+

6 МАТРИЦЯ ВІДПОВІДНОСТІ РЕЗУЛЬТАТІВ НАВЧАННЯ ОБОВ'ЯЗКОВИМ КОМПОНЕНТАМ ОСВІТНЬО-ПРОФЕСІЙНОЇ ПРОГРАМИ

[illegible]

Додаток А

Розподіл освітніх компонент освітньої програми (КОП) за курсами та семестрами

1 курс				2 курс				3 курс				4 курс			
1 семестр		2 семестр		3 семестр		4 семестр		5 семестр		6 семестр		7 семестр		8 семестр	
КОП	кількість кредитів	КОП	кількість кредитів	КОП	кількість кредитів	КОП	кількість кредитів	КОП	кількість кредитів	КОП	кількість кредитів	КОП	кількість кредитів	КОП	кількість кредитів
ОК1	5	ОК1	5	ОК9	3	ОК16	3	ОК18	3	ОК25	3,5	ОК31	3	ОК32	4
ОК2	3	ОК2	3	ОК11	3,5	ОК17	3,5	ОК22	3,5	ОК26	3	ОК32	3,5	ОК33	4,5
ОК3	2	ОК5	4	ОК12	3,5	ОК18	3,5	ОК23	3	ОК27	3,5	ОК33	3	ОК34	4
ОК4	2	ОК7	4,5	ОК13	3,5	ОК19	3,5	ОК24	3	ОК28	3,5	ОК34	3	ОК37	4,5
ОК5	5,5	ОК8	5	ОК14	2	ОК20	3	ОК25	3	ОК29	3	ОК35	4	ОК41	4,5
ОК6	5,5	ОК10	4	ОК15	3	ОК21	2	ОК26	3	ОК30	2	ОК36	2		
ОК7	5,5	ОК14	3			ОК39	3			ОК40	3				
		ОК38	3												
				БК9	5	БК5	5	БК1	5	БК2	5	БК3	5	БК4	5
				БК10	5	БК11	5	БК12	5	БК6	5	БК7	5	БК8	5
28,5		31,5		28,5		31,5		28,5		31,5		28,5		31,5	
60				60				60				60			

Усі компоненти (обов'язкові та вибіркові), їх зміст, формування компетентностей (загальних, спеціальних(фахових)) та визначення результатів навчання представлено у силабусах навчальних дисциплін на сайті в розділі «Короткий опис, структура і освітні компоненти освітніх програми і компонентів» (окремо за кожним курсом навчання) освітньо-професійної програми «Безпека інформаційних і комунікаційних систем» спеціальності F5 «Кібербезпека та захист інформації»:

<https://khai.edu/profil-id-77301>

Додаток Б **СТРУКТУРНО-ЛОГІЧНА СХЕМА ОСВІТНЬО-ПРОФЕСІЙНОЇ ПРОГРАМИ**

