

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
Національний аерокосмічний університет ім. М.Є. Жуковського
«Харківський авіаційний інститут»

ЗАТВЕРДЖЕНО

вченою радою
Національного аерокосмічного
університету ім. М.Є. Жуковського
«Харківський авіаційний інститут»
19 квітня 2017 р., протокол № 13
наказ № 178 від 19.04.2017 р.

ОСВІТНЬО-ПРОФЕСІЙНА ПРОГРАМА

Безпека інформаційних і комунікаційних систем

Рівень вищої освіти – другий (магістерський)

за спеціальністю 125 Кібербезпека

галузі знань 12 Інформаційні технології

Кваліфікація: Магістр з кібербезпеки галузі знань інформаційні технології

(із змінами, внесеними згідно із рішеннями:
вченої ради ХАІ протокол №9 від 25.04.2018р.;
вченої ради ХАІ протокол №9 від 20.03.2019р.;
НМК № 2 НАУ «ХАІ» протокол № 1 від 31.08.2020 р.;
вченої ради «ХАІ» протокол № 9 від 28.04.2021р.;
вченої ради «ХАІ» протокол № 08 від 20.04.2022р.)

Освітня програма вводиться в дію
з «01» вересня 2022 р.

Ректор Національного
аерокосмічного університету
ім. М.Є. Жуковського «Харківський
авіаційний інститут»



М. В. Нечипорук
наказ № 117 від 21.04.2022 р.

Харків 2022 р.

ПЕРЕДМОВА

Освітньо-професійну програму «Безпека інформаційних і комунікаційних систем» для підготовки здобувачів другого (магістерського) рівня вищої освіти за спеціальністю 125 «Кібербезпека» в Національному аерокосмічному університеті ім. М. Є. Жуковського «Харківський авіаційний інститут» оновлено у зв'язку зі:

- перерозподілом кредитів ЄКТС між компонентами освітньо-професійної програми та оновленням її змісту опису (затверджено рішенням вченої ради ХАІ протокол № 9 від 25.04.2018 р.);

- перерозподілом кредитів ЄКТС між компонентами освітньо-професійної програми та оновленням її змісту опису (затверджено рішенням вченої ради ХАІ протокол № 9 від 20.03.2019 р.);

- зі зміною Національної рамки кваліфікацій (Постанова Кабінету Міністрів України від 25 червня 2020, № 519) (затверджено рішенням науково-методичної комісії 2 (НМК 2) ХАІ протокол № 1 від 31.08.2020);

- зі змінами відповідно до Стандарту МОН (наказ МОН № 330 від 18.03.2021 р.) та оновленням змісту опису освітньої програми (затверджено рішенням вченої ради ХАІ протокол № 9 від 28.04.2021 р.);

- перерозподілом кредитів ЄКТС між компонентами освітньо-професійної програми та оновленням її змісту опису (затверджено рішенням вченої ради ХАІ протокол № 08 від 20.04.2022 р.).

Оновлення освітньо-професійної програми «Безпека інформаційних і комунікаційних систем» проведено групою забезпечення ОПП ХАІ у складі:

1 Керівник

(гарант) освітньої Узун Д. Д.
програми

– канд. техн. наук, доцент кафедри комп'ютерних систем, мереж і кібербезпеки

2 Члени групи:

Морозова О.І.

– д-р техн. наук, професор, кафедри комп'ютерних систем, мереж і кібербезпеки

3

Ілляшенко О.О

– канд. техн. наук, доцент кафедри комп'ютерних систем, мереж і кібербезпеки

Рецензії-відгуки зовнішніх стейкхолдерів:

1. Одарущенко О.М - д-р техн. наук, доцент, провідний науковий співробітник ТОВ «НВП «Радій»»

2. Гаєвський В.В - канд. техн. наук, директор ТОВ «Залізничавтоматика»

Ця освітньо-професійна програма не може бути повністю або частково відтворена, тиражована та розповсюджена без дозволу Національного аерокосмічного університету ім. М. Є. Жуковського «Харківський авіаційний інститут»

ВСТУП

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 за спеціальністю 125 «Кібербезпека» для другого (магістерського) рівня вищої освіти (наказ МОН України № 332 від 18.03.2021 р.) і встановлює:

- обсяг та термін навчання магістрів;
- 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 магістрів за освітньо-професійною програмою «Безпека інформаційних і комунікаційних систем» зі спеціальності 125 «Кібербезпека»

Користувачі освітньо-професійної програми:

- здобувачі вищої освіти, які навчаються в Національному аерокосмічному університеті ім. М. Є. Жуковського «Харківський авіаційний інститут»;
- науково-педагогічні працівники, які здійснюють підготовку магістрів за освітньо-професійною програмою «Безпека інформаційних і комунікаційних систем» зі спеціальності 125 «Кібербезпека» Національного аерокосмічного університету ім. М. Є. Жуковського «Харківський авіаційний інститут»;
- екзаменаційна комісія спеціальності 125 «Кібербезпека»;
- приймальна комісія Національного аерокосмічного університету ім. М. Є. Жуковського «Харківський авіаційний інститут».

Освітньо-професійна програма поширюється на кафедри Університету, залучені для підготовки фахівців ступеня магістра за освітньо-професійною програмою «Безпека інформаційних і комунікаційних систем» зі спеціальності 125 «Кібербезпека»

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 «Кібербезпека» для другого (магістерського) рівня вищої освіти (наказ МОН України від 18.03.2021 № 332).
- 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.
- 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, (наказ МОН України № 600 від 01.06.2017 р.) схвалені сектором вищої освіти Науково-методичної Ради Міністерства освіти і науки України (зі змінами).
- 1.7 Положення «Про організацію освітнього процесу» Національного аерокосмічного університету ім. М. Є. Жуковського «Харківський авіаційний інститут» (зі змінами).
- 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.
- 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 Національний освітній глосарій: вища освіта / 2-е вид., перероб. І доп. / 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.
- 1.15 Стандарти і рекомендації щодо забезпечення якості в Європейському просторі вищої освіти. К. : Ленвіт, 2006. – 35 с. ISBN 966-7043-96-7.
- 1.16 Области образования и профессиональной подготовки 2013 (МСКО-О 2013): Сопроводительное руководство к Международной стандартной классификации образования 2011. – Институт статистики ЮНЕСКО, 2014. – Режим доступа: <http://www.uis.unesco.org/Library/Documents/iscfed-2013-fields-of-education-training-2014-rus.pdf>.

2 ПРОФІЛЬ ОСВІТНЬО-ПРОФЕСІЙНОЇ ПРОГРАМИ «БЕЗПЕКА ІНФОРМАЦІЙНИХ І КОМУНІКАЦІЙНИХ СИСТЕМ» ЗІ СПЕЦІАЛЬНОСТІ 125 «КІБЕРБЕЗПЕКА»

1 – Загальна інформація	
Повна назва ЗВО та структурного підрозділу	Національний аерокосмічний університет ім. М. Є. Жуковського «Харківський авіаційний інститут» Кафедра комп'ютерних систем, мереж і кібербезпеки
Ступінь вищої освіти та назва кваліфікації мовою оригіналу	Ступінь вищої освіти – магістр Кваліфікація: Магістр з кібербезпеки Master's Degree Qualification: Master's Degree of Cyber Security
Офіційна назва ОПП	Українською Безпека інформаційних і комунікаційних систем Англійською Security of information and communication systems
Тип диплому та обсяг ОПП	Диплом магістра, одиничний диплом, термін навчання 1 рік 4 місяці – на базі диплому освітнього рівня «бакалавр» – 90 кредитів ЄКТС.
Наявність акредитації	Сертифікат про акредитацію: Серія УД № 21005371, виданий 20.06.2018 р. на підставі наказу МОН України від 20.06.2018 р. № 662 Період акредитації: до 01.07.2023 р.
Цикл/рівень	НРК України - 7 рівень, FQ-EHEA – другий цикл, EQF-LLL – 7 рівень
Передумови	Особа має право здобувати ступінь магістра за умови наявності ступеня бакалавра
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.
Термін дії ОПП	Перегляд освітньої програми здійснюється не рідше ніж один раз на 5 років (відповідно положення) або за вимогою стейкхолдерів. З метою вдосконалення або модернізації гарант освітньої програми може вносити необхідні зміни або доповнення протягом цього терміну з урахуванням пропозицій різних груп стейкхолдерів
Інтернет-адреса постійного розміщення опису ОПП	https://khai.edu.ua/education/osvitni-programi-i-komponenti/osvitni-programi-magistriv/
2 – Мета освітньої програми	
1 Надати теоретичні знання та практичні уміння і навички, достатні для успішного виконання професійних обов'язків за освітньо-професійною програмою «Безпека інформаційних і комунікаційних систем», спеціальності 125 «Кібербезпека» та підготувати до успішного засвоєння складніших програм для наукових дослідників. 2 Формування особистості фахівця здатного використовувати професійно-профільні знання й практичні навички для вирішення інноваційних завдань в галузі з інформаційних технологій з урахуванням специфіки аерокосмічної галузі.	
3 – Характеристика освітньо-професійної програми	
Предметна область	Об'єктами професійної діяльності магістрів є: – сучасні процеси дослідження, аналізу, створення та забезпечення функціонування інформаційних систем і технологій, інших бізнес-операційних процесів на об'єктах інформаційної діяльності та критичних інфраструктур сфери інформаційної безпеки та/або кібербезпеки; – інформаційні системи (інформаційно-комунікаційні, інформаційно-телекомунікаційні, автоматизовані) та технології; – інфраструктура об'єктів інформаційної діяльності та критичних інфраструктур; – системи та комплекси створення, обробки, передачі, зберігання, знищення, захисту та відображення даних (інформаційних потоків); – інформаційні ресурси різних класів (в т.ч. державні інформаційні ресурси); – програмне та програмно-апаратне забезпечення (засоби) кіберзахисту; – системи управління інформаційною безпекою та/або кібербезпекою; – технології, методи, моделі та засоби інформаційної безпеки та/або кібербезпеки.

	Цілями навчання є підготовка фахівців, здатних розв'язувати задачі дослідницького та/або інноваційного характеру у сфері інформаційної та/або кібербезпеки. Теоретичний зміст предметної області Теоретичні засади наукоємних технологій, фізичні і математичні фундаментальні знання, теорії ідентифікації та прийняття рішень, системного аналізу, складних систем, моделювання та оптимізації процесів, теорія математичної статистики, криптографічного та технічного захисту інформації, теорії ризиків та інших міждисциплінарних теорій і практик у галузі інформаційної безпеки та/або кібербезпеки. Методи, методики та технології: Методи, моделі, методики та технології створення, обробки, передачі, приймання, знищення, відображення, захисту (кіберзахисту) інформаційних ресурсів у кіберпросторі, а також методи та моделі розробки та використання прикладного і спеціалізованого програмного забезпечення для вирішення професійних задач в галузі інформаційної безпеки та/або кібербезпеки. Технології, методи та моделі дослідження, аналізу, управління та забезпечення бізнес/операційних процесів із застосуванням сукупності нормативно-правових та організаційно-технічних методів і засобів захисту інформаційних ресурсів у кіберпросторі Інструменти та обладнання: Засоби, пристрої, мережне устаткування та середовище, прикладне та спеціалізоване програмне забезпечення, автоматизовані системи та комплекси проектування, моделювання, експлуатації, контролю, моніторингу, обробки, відображення та захисту даних (інформаційних потоків), а також методи і моделі теорії ризиків та управління інформаційними ресурсами при дослідженні і супроводженні об'єктів інформаційної діяльності у галузі інформаційної безпеки та/або кібербезпеки.
Орієнтація ОП	Освітньо-професійна
Основний фокус ОПП	Освітньо-професійна програма встановлює кваліфікаційні вимоги до соціально-виробничої діяльності випускників закладу вищої освіти зі спеціальності 125 «Кібербезпека» освітнього ступеня «магістр» і державні вимоги до властивостей та якостей особи, що здобула певний освітній рівень відповідного фахового спрямування за освітньо-професійною програмою «Безпека інформаційних і комунікаційних систем».
Особливості програми	Освітня програма вдосконалює знання принципів, методів і технологій розроблення, моделювання, моніторингу, аудиту та управління засобами забезпечення кібербезпеки інформаційних і комунікаційних систем і об'єктів критичної інфраструктури, а також оптимізацію засобів безпеки з урахуванням вимог стандартів і обмежень. Практика проводиться на підприємствах різних галузей промисловості.
4 – Придатність випускників до працевлаштування та подальшого навчання	
Придатність до працевлаштування	Проектна, виробнича, технологічна, управлінська, науково-дослідна; інноваційна, викладацька, експертна та консультативна діяльність у сфері комп'ютерної інженерії.
Подальше навчання	Випускники мають право продовжити навчання на третьому (освітньо-науковому) рівні вищої освіти та набувати додаткові кваліфікації 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 (дипломного проектування).

Оцінювання	Письмові іспити, звіти з практик, заліки, презентації, поточний (модульний) контроль, курсові проекти, кваліфікаційна робота (дипломне проєктування) та її захист.
6 – Програмні компетентності	
Інтегральна компетентність	Здатність особи розв'язувати задачі дослідницького та/або інноваційного характеру у сфері інформаційної безпеки та/або кібербезпеки.
Загальні компетентності	КЗ-1. Здатність застосовувати знання у практичних ситуаціях. КЗ-2. Здатність проводити дослідження на відповідному рівні. КЗ-3. Здатність до абстрактного мислення, аналізу та синтезу. КЗ-4. Здатність оцінювати та забезпечувати якість виконуваних робіт. КЗ-5. Здатність спілкуватися з представниками інших професійних груп різного рівня (з експертами з інших галузей знань / видів економічної діяльності).
Спеціальні (фахові) компетентності	КФ1. Здатність обґрунтовано застосовувати, інтегрувати, розробляти та удосконалювати сучасні інформаційні технології, фізичні та математичні моделі, а також технології створення та використання прикладного і спеціалізованого програмного забезпечення для вирішення професійних задач у сфері інформаційної безпеки та/або кібербезпеки. КФ2. Здатність розробляти, впроваджувати та аналізувати нормативні документи, положення, інструкції й вимогитехнічного та організаційного спрямування, а також інтегрувати, аналізувати і використовувати кращі світові практики, стандарти у професійній діяльності в сфері інформаційної безпеки та/або кібербезпеки. КФ3. Здатність досліджувати, розробляти і супроводжувати методи та засоби інформаційної безпеки та/або кібербезпеки на об'єктах інформаційної діяльності та критичної інфраструктури. КФ4. Здатність аналізувати, розробляти і супроводжувати систему управління інформаційною безпекою та/або кібербезпекою організації, формувати стратегію і політики інформаційної безпеки з урахуванням вітчизняних і міжнародних стандартів та вимог. КФ5. Здатність до дослідження, системного аналізу та забезпечення безперервності бізнес/операційних процесів з метою визначення вразливостей інформаційних систем та ресурсів, аналізу ризиків та визначення оцінки їх впливу у відповідності до встановленої стратегії і політики інформаційної безпеки та/або кібербезпеки організації. КФ6. Здатність аналізувати, контролювати та забезпечувати систему управління доступом до інформаційних ресурсів згідно встановленої стратегії і політики інформаційної безпеки та/або кібербезпеки організації. КФ7. Здатність досліджувати, розробляти та впроваджувати методи і заходи протидії кіберінцидентам, здійснювати процедури управління, контролю та розслідування, а також надавати рекомендації щодо попередження та аналізу кіберінцидентів в цілому. КФ8. Здатність досліджувати, розробляти, впроваджувати та супроводжувати методи і засоби криптографічного та технічного захисту інформації на об'єктах інформаційної діяльності та критичної інфраструктури, в інформаційних системах, а також здатність оцінювати ефективність їх використання, згідно встановленої стратегії і політики інформаційної безпеки та/або кібербезпеки організації. КФ9. Здатність аналізувати, розробляти і супроводжувати систему аудиту та моніторингу ефективності функціонування інформаційних систем і технологій, бізнес/операційних процесів в галузі інформаційної безпеки та/або кібербезпеки організації в цілому. КФ10. Здатність провадити науково-педагогічну діяльність, планувати навчання, контролювати і супроводжувати роботу з персоналом, а також приймати ефективні рішення з питань інформаційної безпеки та/або кібербезпеки. КФ11. Здатність аналізувати і розробляти методи і засоби оцінювання та забезпечення функційної безпечності інформаційно- керуючих систем. КФ12. Здатність аналізувати, розробляти і впроваджувати методи і засоби розгортання безпечних хмарних та інших ІТ-інфраструктур.

7 – Програмні результати навчання

- РН1. Вільно спілкуватись державною та іноземною мовами, усно і письмово для представлення і обговорення результатів досліджень та інновацій, забезпечення бізнес\операційних процесів та питань професійної діяльності в галузі інформаційної безпеки та/або кібербезпеки.
- РН2. Інтегрувати фундаментальні та спеціальні знання для розв'язування складних задач інформаційної безпеки та/або кібербезпеки у широких або мультидисциплінарних контекстах.
- РН3. Проводити дослідницьку та/або інноваційну діяльність в сфері інформаційної безпеки та/або кібербезпеки, а також в сфері технічного та криптографічного захисту інформації у кіберпросторі.
- РН4. Застосовувати, інтегрувати, розробляти, впроваджувати та удосконалювати сучасні інформаційні технології, фізичні та математичні методи і моделі в сфері інформаційної безпеки та/або кібербезпеки.
- РН5. Критично осмислювати проблеми інформаційної безпеки та/або кібербезпеки, у тому числі на міжгалузевому та міждисциплінарному рівні, зокрема на основі розуміння нових результатів інженерних і фізико-математичних наук, а також розвитку технологій створення та використання спеціалізованого програмного забезпечення.
- РН6. Аналізувати та оцінювати захищеність систем, комплексів та засобів кіберзахисту, технології створення та використання спеціалізованого програмного забезпечення.
- РН7. Обґрунтовувати використання, впроваджувати та аналізувати кращі світові стандарти, практики з метою розв'язання складних задач професійної діяльності в галузі інформаційної безпеки та/або кібербезпеки.
- РН8. Досліджувати, розробляти і супроводжувати системи та засоби інформаційної безпеки та/або кібербезпеки на об'єктах інформаційної діяльності та критичної інфраструктури.
- РН9. Аналізувати, розробляти і супроводжувати систему управління інформаційною безпекою та/або кібербезпекою організації на базі стратегії і політики інформаційної безпеки.
- РН10. Забезпечувати безперервність бізнес\операційних процесів, а також виявляти уразливості інформаційних систем та ресурсів, аналізувати та оцінювати ризики для інформаційної безпеки та/або кібербезпеки організації.
- РН11. Аналізувати, контролювати та забезпечувати ефективне функціонування системи управління доступом до інформаційних ресурсів відповідно до встановлених стратегії і політики інформаційної безпеки та/або кібербезпеки організації.
- РН12. Досліджувати, розробляти та впроваджувати методи і заходи протидії кіберінцидентам, здійснювати процедури управління, контролю та розслідування, а також надавати рекомендації щодо попередження та аналізу кіберінцидентів в цілому.
- РН13. Досліджувати, розробляти, впроваджувати та використовувати методи та засоби криптографічного та технічного захисту інформації бізнес\операційних процесів, а також аналізувати і надавати оцінку ефективності їх використання в інформаційних системах, на об'єктах інформаційної діяльності та критичної інфраструктури.
- РН14. Аналізувати, розробляти і супроводжувати систему аудиту та моніторингу ефективності функціонування інформаційних систем і технологій, бізнес\операційних процесів у сфері інформаційної та/або кібербезпеки в цілому.
- РН15. Зрозуміло і недвозначно доносити власні висновки з проблем інформаційної безпеки та/або кібербезпеки, а також знання та пояснення, що їх обґрунтовують до персоналу, партнерів та інших осіб.
- РН16. Приймати обґрунтовані рішення з організаційно-технічних питань інформаційної безпеки та/або кібербезпеки у складних і непередбачуваних умовах, у тому числі із застосуванням сучасних методів та засобів оптимізації, прогнозування та прийняття рішень.
- РН17. Мати навички автономного і самостійного навчання у сфері інформаційної безпеки та/або кібербезпеки і дотичних галузей знань, аналізувати власні освітні потреби та об'єктивно оцінювати результати навчання.
- РН18. Планувати навчання, а також супроводжувати та контролювати роботу з персоналом у напрямку інформаційної безпеки та/або кібербезпеки.
- РН19. Обирати, аналізувати і розробляти придатні типові аналітичні, розрахункові та

експериментальні методи кіберзахисту, розробляти, реалізовувати та супроводжувати проекти з захисту інформації у кіберпросторі, інноваційної діяльності та захисту інтелектуальної власності. РН20. Ставити та вирішувати складні інженерно-прикладні та наукові задачі інформаційної безпеки та/або кібербезпеки з урахуванням вимог вітчизняних та світових стандартів та кращих практик. РН21. Використовувати методи натурного, фізичного і комп'ютерного моделювання для дослідження процесів, які стосуються інформаційної безпеки та/або кібербезпеки. РН22. Планувати та виконувати експериментальні і теоретичні дослідження, висувати і перевіряти гіпотези, обирати для цього придатні методи та інструменти, здійснювати статистичну обробку даних, оцінювати достовірність результатів досліджень, аргументувати висновки. РН23. Обґрунтовувати вибір програмного забезпечення, устаткування та інструментів, інженерних технологій і процесів, а також обмежень щодо них в галузі інформаційної безпеки та/або кібербезпеки на основі сучасних знань у суміжних галузях, наукової, технічної та довідкової літератури та іншої доступної інформації. РН24. Аналізувати та оцінювати показники функційної безпечності інформаційно-керуючих систем та обґрунтовувати рекомендації щодо її забезпечення відповідно вимогам нормативних документів. РН25. Аналізувати, обґрунтовувати вибір, розробляти і впроваджувати методи і засоби розгортання безпечних хмарних та інших ІТ-інфраструктур.	
8 – Ресурсне забезпечення реалізації програми	
Кадрове забезпечення	Науково-педагогічні працівники, задіяні у викладанні професійно-орієнтованих дисциплін, мають наукові ступені та/або вчене звання та відповідають ліцензійним вимогам. Відповідає кадровим вимогам щодо забезпечення провадження освітньої діяльності у сфері вищої освіти згідно з діючим законодавством України (Постанова кабінету міністрів України «Про затвердження Ліцензійних умов провадження освітньої діяльності закладів освіти» від 30 грудня 2015 р. № 1187 (зі змінами)).
Матеріально-технічне забезпечення	Навчання здійснюється у навчальних лабораторіях, комп'ютерних класах, аудиторіях радіотехнічного корпусу Національного аерокосмічного університету ім. М.Є. Жуковського «ХАІ». Відповідає матеріально-технічним вимогам щодо забезпечення провадження освітньої діяльності у сфері вищої освіти згідно з діючим законодавством України (Постанова кабінету міністрів України «Про затвердження Ліцензійних умов провадження освітньої діяльності закладів освіти» від 30 грудня 2015 р. № 1187 (зі змінами)).
Інформаційне та навчально-методичне забезпечення	Використання віртуального навчального середовища Національного аерокосмічного університету ім. М. Є. Жуковського «Харківський авіаційний інститут» та авторських розробок науково-педагогічного складу. 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. Кафедра має робочі та навчальні програми власної розробки. Відповідає інформаційним та навчально-методичним вимогам щодо забезпечення провадження освітньої діяльності у сфері вищої освіти згідно з діючим законодавством України (Постанова кабінету міністрів України «Про затвердження Ліцензійних умов провадження освітньої діяльності закладів освіти» від 30 грудня 2015 р. № 1187 (зі змінами)).

9 – Академічна мобільність	
Національна кредитна мобільність	На основі двосторонніх договорів між Національним аерокосмічним університетом ім. М. Є. Жуковського «Харківський авіаційний інститут» і технічними закладами України, зокрема: Інститут кібернетики імені В.М. Глушкова НАН України, ТОВ «482.СОЛЮШНС», ТОВ «Sigma Software», ТЗОВ «SoftServe», ТОВ «Epm Systems», ТОВ «НВП «Радікс», RWA Railway Automatic (Залізничавтоматика).
Міжнародна кредитна мобільність	На основі двосторонніх договорів між Національним аерокосмічним університетом ім. М. Є. Жуковського «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); Університет Тренто (Італія) Програма мобільності. Erasmus+; Харбінський Політехнічний Університет Міжнародна літня школа «China Discovery Program»; Міжнародна літня школа у Пекінському університеті авіації та аеронавтики (BUAA), Пекін, КНР; Міжнародна літня школа для викладачів у Нанкінському університеті астронавтики та аеронавтики (NUAA), Нанкін, КНР; Короткострокові стажування для викладачів; Стипендіальні програми Німецької Служби Академічних обмінів DAAD; університет «Проф. д-р Златаров», м. Бургас, Болгарія, стажування науковців та викладачів, обмін здобувачами, наукова співпраця; Лундський Університет (Швеція) Стажування для викладачів; Стамбульський технічний університет Nanchang Hangkong university; Академічна мобільність з Магдебурзьким технічним університетом ім. Отто фон Геріке; Чеський Технічний Університет у Празі Стипендіальна програма Nikola Šohaj (1 семестр); Академічна мобільність з Ecole Centrale de Nantes (ECN), Франція ЄС; Академічна мобільність з Університетом Країни Басків, Іспанія.
Навчання іноземних здобувачів вищої освіти	Навчання іноземних громадян здійснюється державною або англійською мовами. Якщо навчання здійснюється державною мовою, то 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 ОП

Код КОП	Компоненти освітньої програми (навчальні дисципліни, курсові проекти (роботи), практики, кваліфікаційна робота)	Кількість кредитів	Форма підсумкового контролю
1	2	3	4
Обов'язкові компоненти ОП			
ОК1	Технології DevOps	4 (1)	іспит
ОК2	Організація наукових досліджень і захист інтелектуальної власності	4 (1)	залік
ОК3	Технології розроблення та забезпечення функційної безпечності ІКС	4 (1)	іспит
ОК4	Теорія та технології розроблення безпечних розподілених систем	4 (1)	іспит
ОК5	Методи моделювання та оптимізації безпечних комп'ютерних систем	4 (1)	залік
ОК6	Наукове-педагогічне стажування	5 (2)	залік
ОК7	Методи побудови та аналізу криптосистем	4 (2)	іспит
ОК8	Методи та технології кібербезпеки критичних інфраструктур	4 (2)	іспит
ОК9	Стандартизація і сертифікація систем кібербезпеки	4 (2)	іспит
ОК10	Переддипломна практика	10 (3)	диф. залік
ОК11	Кваліфікаційна робота (дипломне проектування)	20 (3)	захист
Загальний обсяг обов'язкових компонент:		67	
Вибіркові компоненти ОП*			
Гуманітарний блок (Soft skills)			
ВК1	Технічна іноземна мова	3 (2)	залік
Дисципліни індивідуального вибору**			
ВК2	Дисципліна індивідуального вибору 1	5 (1)	іспит
ВК3	Дисципліна індивідуального вибору 2	5 (1)	іспит
ВК4	Дисципліна індивідуального вибору 3	5 (2)	іспит
ВК5	Дисципліна індивідуального вибору 4	5 (2)	іспит
Загальний обсяг обов'язкових компонент:		23	
ЗАГАЛЬНИЙ ОБСЯГ ОСВІТНЬОЇ ПРОГРАМИ		90	

3.2 Структурно-логічна схема ОП

В основу розроблення освітньо-професійної програми покладено компетентний підхід з використанням ЄКТС, де для досягнення запланованих результатів навчання за освітньою програмою (навчальною дисципліною, модулем) передбачаються певні витрати часу студентом, тобто необхідний і достатній обсяг навчального навантаження здобувача, виражений у кількості кредитів ЄКТС (1 кредит ЄКТС дорівнює 30 годинам), 1 семестр – 30 кредитів ЄКТС, навчальний (академічний) рік – 60 кредитів ЄКТС.

Освітньо-професійна програма передбачає виділення дисциплін двох видів: обов'язкових дисциплін та дисциплін за вільним вибором здобувача. Структурно-логічна схема освітньої програми відображає послідовність вивчення її компонент і наведена у додатку А.

4 ФОРМА АТЕСТАЦІЇ ЗДОБУВАЧІВ ВИЩОЇ ОСВІТИ

Атестація випускників за освітньо-професійною програмою «Безпека інформаційних і комунікаційних систем» зі спеціальності 125 «Кібербезпека» проводиться у формі захисту кваліфікаційної магістерської роботи та завершується видачею документу встановленого зразка про присудження йому ступеня магістра із присвоєнням кваліфікації: магістр з кібербезпеки галузі знань інформаційні технології. Атестація здійснюється відкрито і публічно.

**5 МАТРИЦЯ
КОМПЕТЕНТНОСТЕЙ
ОСВІТНЬО-ПРОФЕСІЙНОЇ ПРОГРАМИ**

**ВІДПОВІДНОСТІ
ОБОВ'ЯЗКОВИМ**

**ПРОГРАМНИХ
КОМПОНЕНТАМ**

Програмні компетентності	Компоненти освітньої програми										
	ОК 1	ОК 2	ОК 3	ОК 4	ОК 5	ОК 6	ОК 7	ОК 8	ОК 9	ОК 10	ОК 11
КЗ1	+	+	+	+	+	+	+	+	+	+	+
КЗ2		+	+	+	+	+	+	+		+	+
КЗ3	+	+	+	+	+	+	+	+	+	+	+
КЗ4	+	+	+	+	+	+	+	+	+	+	+
КЗ5	+	+	+	+	+	+	+	+	+	+	+
КФ1	+		+	+	+		+	+		+	+
КФ2	+	+	+	+		+	+	+	+	+	+
КФ3			+	+			+	+	+	+	+
КФ4	+		+		+			+	+	+	+
КФ5			+	+	+			+	+		+
КФ6	+						+	+	+		+
КФ7							+	+	+		+
КФ8							+	+	+	+	+
КФ9			+					+	+		+
КФ10		+				+				+	+
КФ11			+	+				+		+	+
КФ12	+							+		+	+

**6 МАТРИЦЯ ВІДПОВІДНОСТІ ПРОГРАМНИХ РЕЗУЛЬТАТІВ
НАВЧАННЯ (ПРН) ОБОВ'ЯЗКОВИМ КОМПОНЕНТАМИ
ОСВІТНЬО-ПРОФЕСІЙНОЇ ПРОГРАМИ**

Програмні результати навчання	Компоненти освітньої програми										
	ОК 1	ОК 2	ОК 3	ОК 4	ОК 5	ОК 6	ОК 7	ОК 8	ОК 9	ОК 10	ОК 11
РН1	+	+	+	+	+	+	+	+	+	+	+
РН2	+	+	+		+		+	+		+	+
РН3		+					+	+		+	+
РН4	+		+	+	+						+
РН5	+		+		+		+	+	+	+	+
РН6	+		+				+		+	+	+
РН7	+	+	+	+		+	+	+	+		+
РН8	+		+				+	+			+
РН9							+	+	+	+	+
РН10	+		+	+				+	+	+	+
РН11	+						+	+	+		+
РН12			+				+	+	+	+	+
РН13					+		+	+	+	+	+
РН14							+		+		+
РН15	+		+		+		+	+	+		+
РН16	+	+			+			+			+
РН17	+	+	+	+	+	+	+	+	+	+	+
РН18	+	+	+	+	+	+	+	+	+	+	+
РН19	+	+	+	+	+	+	+	+	+	+	+
РН20	+	+	+	+	+	+	+	+	+	+	+
РН21			+		+		+	+		+	+
РН22			+	+	+		+	+		+	+
РН23	+	+	+	+	+		+	+		+	+
РН24			+					+	+	+	+
РН25	+			+				+		+	+

Додаток А
СТРУКТУРНО-ЛОГІЧНА СХЕМА ОСВІТНЬО-ПРОФЕСІЙНОЇ ПРОГРАМИ

