ID 60181

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»
20 квітня 2023 р., протокол № 09
наказ № 178 від 19.04.2017 р.

ОСВІТНЬО-ПРОФЕСІЙНА ПРОГРАМА

Безпека інформаційних і комунікаційних систем

Рівень вищої освіти – другий (магістерський)
галузі знань 12 Інформаційні технології
Спеціальність 125 Кібербезпека та захист інформації

Кваліфікація: Магістр з кібербезпеки та захисту інформації

(із змінами, внесеними згідно із рішенням
вченої ради «ХАІ» протокол № 10 від 17.04.2024р.)

Освітня програма вводиться в дію
з «01» вересня 2024 р.

В. о. ректора Національного
аерокосмічного університету
ім. М. Є. Жуковського «Харківський
авіаційний інститут»

_____ Олексій ЛИТВИНОВ
наказ № 172 від 18.04.2024 р.

Харків 2024 р.

ПЕРЕДМОВА

Освітньо-професійну програму «Безпека інформаційних і комунікаційних систем» для підготовки здобувачів другого (магістерського) рівня вищої освіти за спеціальністю 125 «Кібербезпека та захист інформації» в Національному аерокосмічному університеті ім. М. Є. Жуковського «Харківський авіаційний інститут» розроблено у зв'язку з внесенням змін до переліку галузей знань і спеціальностей, за якими здійснюється підготовка здобувачів вищої освіти (Постанова Кабінету Міністрів України від 16 грудня 2022 р., № 1392) на основі ОПП «Безпека інформаційних і комунікаційних систем» ХАІ (ID 208) другого (магістерського) рівня вищої освіти за спеціальністю 125 «Кібербезпека».

Освітньо-професійну програму (ОПП) «Безпека інформаційних і комунікаційних систем» для підготовки здобувачів другого (магістерського) рівня вищої освіти переглянуто у зв'язку із модернізацією структури компоненти освітньої програми й оновленням змісту її опису (затверджено рішенням вченої ради «ХАІ» протокол № 10 від 18.04.2024 р.) групою забезпечення ОПП Національного аерокосмічного університету ім. М. Є. Жуковського «Харківський авіаційний інститут» у складі:

1	Керівник (гарант) освітньої програми	Дмитро УЗУН	– канд. техн. наук, доцент, доцент кафедри комп'ютерних систем, мереж і кібербезпеки
2	Члени групи:	Ольга МОРОЗОВА	– д-р техн. наук, професор, професор кафедри комп'ютерних систем, мереж і кібербезпеки
3		Олег ІЛЛЯШЕНКО	– канд. техн. наук, доцент, доцент кафедри комп'ютерних систем, мереж і кібербезпеки

Рецензії-відгуки зовнішніх стейкхолдерів додаються

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), Стандарт вищої освіти за спеціальністю 125 «Кібербезпека» для другого (магістерського) рівня вищої освіти (наказ МОН № 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;

– вимоги до структури навчальних дисциплін.

Освітньо-професійна програма (ОПП) використовується для:

– складання навчальних планів та робочих навчальних планів;

– формування індивідуальних планів здобувачів;

– 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 та захист інформації".

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 спеціальності125 "Кібербезпека та захист інформації" Національного аерокосмічного університету ім. М. Є. Жуковського «Харківський авіаційний інститут»;

– екзаменаційна комісія спеціальності 125 «Кібербезпека та захист інформації»;

– 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 ОПП ««Безпека інформаційних і комунікаційних систем»» зі спеціальності 125 "Кібербезпека та захист інформації".

1 НОРМАТИВНІ ПОСИЛАННЯ

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

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

1.2 Стандарт вищої освіти за спеціальністю 125 «Кібербезпека» для другого (магістерського) рівня вищої освіти (наказ МОН № 332 від 18.03.2021 р.).

1.3 Постанова Кабінету Міністрів України «Про затвердження Національної рамки кваліфікацій» від 23.11.2011 р. № 1341.

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 Національний класифікатор України. Класифікатор професій ДК 003:2010, затверджений наказом Держспоживстандарту України від 28.07.2010 р.№ 327 (зі змінами).

1.7 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).

1.8 Положення «Про організацію освітнього процесу» Національного аерокосмічного університету ім. М. Є. Жуковського «Харківський авіаційний інститут», затверджене вченою радою університету.

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

1.10 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

1.11 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.

1.12 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.

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

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

1.15 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.

2 ПРОФІЛЬ ОСВІТНЬО-ПРОФЕСІЙНОЇ ПРОГРАМИ «СИСТЕМНЕ ПРОГРАМУВАННЯ» ЗІ СПЕЦІАЛЬНОСТІ 125 «Кібербезпека та захист інформації»

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 National Aerospace University «Kharkiv Aviation Institute» Department of Computer Systems, Networks and Cybersecurity
Ступінь вищої освіти	Ступінь вищої освіти – магістр Master's Degree
Галузь знань, спеціальність та назва кваліфікації	Галузь знань 12 Інформаційні технології Field of Study 12 Information Technologies Спеціальність 125 Кібербезпека та захист інформації Program Subject Area 125 Cybersecurity and Information Protection Кваліфікація: Магістр з кібербезпеки та захисту інформації Qualification: Master'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 магістра, одиничний, 90 кредитів ЄКТС / 1 рік 4 місяця
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 01.07.2025 р. Оновлення або модернізація освітньої програми здійснюється відповідно до розділу 5 Положення «Про розроблення та модернізацію освітніх програм в ХАІ».
Цикл/рівень	НРК України - 7 рівень, FQ-EHEA – другий цикл, EQF-LLL – 7 рівень
Передумови	Особа має право здобувати ступень 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 викладанняоднієї чи декількохдисциплін англійською та/або іншими іноземними мовами.
Інтернет-адреса постійного розміщення опису ОПП	https://khai.edu/ua/education/osvitni-programi-i-komponenti/osvitni-programi-magistriv/osvitno-profesiini-programi/
2 – Мета освітньої програми	
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 захист інформації». 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'єкт вивчення:** - 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.. - інформаційні процеси, технології, методи, способи та системи автоматизованого та автоматичного проектування; налагодження, виробництва й експлуатації, проектна документація, стандарти, процедури та засоби підтримки керування життєвим циклом вказаних програмно-технічних засобів. - методи та способи опрацювання інформації, математичні моделі обчислювальних процесів, технології виконання обчислень, в тому числі високопродуктивних, паралельних, розподілених, мобільних, веб-базованих та хмарних, зелених (енергоефективних), безпечних, автономних, адаптивних, інтелектуальних, розумних тощо, архітектура та організація функціонування відповідних програмно-технічних засобів. **Ціль навчання:** підготовка фахівців, здатних самостійно досліджувати, використовувати і впроваджувати технології інформаційної та/або кібербезпеки. **Теоретичний зміст предметної області:** поняття, концепції, принципи, методи, програмно-технічні засоби та технології досліджування, створення, використання та обслуговування комп'ютерних систем та мереж, вбудованих і розподілених обчислень. **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 програма
Основний фокус ОПП	Освітньо-професійна програма встановлює кваліфікаційні вимоги до соціально-виробничої діяльності випускників закладу вищої освіти зі спеціальності 125 «Кібербезпека та захист інформації» 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, комунікаційних та інформаційно-керуючих систем і об'єктів критичної інфраструктури з урахуванням рівнів інформаційних та операційних технологій, а також оптимізацію засобів безпеки з урахуванням вимог стандартів та існуючих обмежень. Практика проводиться на підприємствах різних галузей промисловості для підготовки конкурентноспроможних випускників на ринку праці. Особливість програми пов'язана з об'єктами аерокосмічної галузі у сфері інформаційних технологій, для яких необхідно здійснити збір, зберігання, оброблення інформації, її цілісність та захист від втручань.

4 – Придатність випускників до працевлаштування та подальшого навчання	
Придатність до працевлаштування	Проєктна, виробнича, технологічна, управлінська, науково-дослідна; інноваційна, викладацька, експертна та консультативна діяльність у сфері кібербезпеки та захисту інформації.
Подальше навчання	Особа має право продовжувати освіту за третім (освітньо-науковим) рівнем для отримання ступеня доктора філософії 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.
Оцінювання	Письмові іспити, звіти з практик, презентації, поточний (модульний) контроль, кваліфікаційна робота та її захист.
6 – Програмні компетентності	
Інтегральна компетентність	Здатність розв'язувати складні задачі та проблеми в галузі інформаційних технологій, що передбачає проведення досліджень та/або здійснення інновацій при застосуванні методів і принципів комп'ютерної інженерії для вирішення задачі розробки системних програм.
Загальні компетентності (ЗК)	ЗК1. Здатність до адаптації та дій в новій ситуації. ЗК2. Здатність до абстрактного мислення, аналізу і синтезу. ЗК3. Здатність проводити дослідження на відповідному рівні. ЗК4. Здатність до пошуку, оброблення та аналізу інформації з різних джерел. ЗК5. Здатність генерувати нові ідеї (креативність). ЗК6. Здатність виявляти, ставити та вирішувати проблеми. ЗК7. Здатність приймати обґрунтовані рішення. ЗК8. Здатність спілкуватися іноземною мовою.
Спеціальні (фахові) компетентності (ФК та/або СК – згідно Стандарту)	СК1. 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. СК2. Здатність розробляти, впроваджувати та аналізувати нормативні документи, положення, інструкції й вимоги технічного та організаційного спрямування, а також інтегрувати, аналізувати і використовувати кращі світові практики, стандарти у професійній діяльності в сфері інформаційної безпеки та/або кібербезпеки. СК3. Здатність досліджувати, розробляти і супроводжувати методи та засоби інформаційної безпеки та/або кібербезпеки на об'єктах інформаційної діяльності та критичної інфраструктури. СК4. 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. СК5. 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. СК6. Здатність аналізувати, контролювати та забезпечувати систему управління доступом до інформаційних ресурсів згідно встановленої стратегії і політики інформаційної безпеки та/або кібербезпеки організації. СК7. 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.

	СК8. 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. СК9. 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. СК10. 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. СК11. Здатність аналізувати і розробляти методи і засоби оцінювання та забезпечення функційної безпечності інформаційно-керуючих систем. СК12. Здатність аналізувати, розробляти і впроваджувати методи і засоби розгортання безпечних хмарних та інших ІТ-інфраструктур.
7 – Програмні результати навчання	
ПРН1. 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. ПРН2. Інтегрувати фундаментальні та спеціальні знання для розв'язування складних задач інформаційної безпеки та/або кібербезпеки у широких або мультидисциплінарних контекстах. ПРН3. Провадити дослідницьку та/або інноваційну діяльність в сфері інформаційної безпеки та/або кібербезпеки, а також в сфері технічного та криптографічного захисту інформації у кіберпросторі. ПРН4. Застосовувати, інтегрувати, розробляти, впроваджувати та удосконалювати сучасні інформаційні технології, фізичні та математичні методи і моделі в сфері інформаційної безпеки та/або кібербезпеки. ПРН5. 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. ПРН6. Аналізувати та оцінювати захищеність систем, комплексів та засобів кіберзахисту, технології створення та використання спеціалізованого програмного забезпечення. ПРН7. Обґрунтовувати використання, впроваджувати та аналізувати кращі світові стандарти, практики з метою розв'язання складних задач професійної діяльності в галузі інформаційної безпеки та/або кібербезпеки. ПРН8. Досліджувати, розробляти і супроводжувати системи та засоби інформаційної безпеки та/або кібербезпеки на об'єктах інформаційної діяльності та критичної інфраструктури. ПРН9. Аналізувати, розробляти і супроводжувати систему управління інформаційною безпекою та/або кібербезпекою організації на базі стратегії і політики інформаційної безпеки. ПРН10. Забезпечувати безперервність бізнес/операційних процесів, а також виявляти уразливості інформаційних систем та ресурсів, аналізувати та оцінювати ризики для інформаційної безпеки та/або кібербезпеки організації. ПРН11. Аналізувати, контролювати та забезпечувати ефективне функціонування системи управління доступом до інформаційних ресурсів відповідно до встановлених стратегії і політики інформаційної безпеки та/або кібербезпеки організації. ПРН12. Досліджувати, розробляти та впроваджувати методи і заходи протидії кіберінцидентам, здійснювати процедури управління, контролю та розслідування, а також надавати рекомендації щодо попередження та аналізу кібер. інцидентів в цілому. ПРН13. 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. ПРН14. 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.	

ПРН15. 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. ПРН16. 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. ПРН17. 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. ПРН18. Планувати навчання, а також супроводжувати та контролювати роботу з персоналом у напряму інформаційної безпеки та/або кібербезпеки. ПРН19. 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. ПРН20. Ставити та вирішувати складні інженерно-прикладні та наукові задачі інформаційної безпеки та/або кібербезпеки з урахуванням вимог вітчизняних та світових стандартів та кращих практик. ПРН21. Використовувати методи натурного, фізичного і комп'ютерного моделювання для дослідження процесів, які стосуються інформаційної безпеки та/або кібербезпеки. ПРН22. 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. ПРН23. 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. ПРН24. Аналізувати та оцінювати показники функційної безпечності інформаційно-керуючих систем та обґрунтовувати рекомендації щодо її забезпечення відповідно вимогам нормативних документів. ПРН25. Аналізувати, обґрунтовувати вибір, розробляти і впроваджувати методи і засоби розгортання безпечних хмарних та інших IT-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 здобувачів освіти 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 «Epam Systems», ТОВ «НВП «Радікс», ТОВ «НВП «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 ВО	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 ОПП

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 ОПП			
ОК1	Організація наукових досліджень і захист інтелектуальної власності	3(1)	залік
ОК2	Домени кібербезпеки. Теорія та практика	3 (1)	іспит
ОК3	Технології розроблення та забезпечення функційної безпечності ІКС	4 (1)	іспит
ОК4	Теорія та технології розроблення безпечних розподілених систем	4(1)	залік
ОК5	Методи моделювання та оптимізації безпечних комп'ютерних систем	3(1)	залік
ОК6	Наукове-педагогічне стажування	4 (2)	іспит
ОК7	Методи побудови та аналізу криптосистем	3 (2)	залік
ОК8	Методи та технології кібербезпеки критичних інфраструктур	3 (2)	іспит
ОК9	Стандартизація і сертифікація систем кібербезпеки	3 (2)	іспит
ОК10	Кваліфікаційна робота	20 (3)	захист
ОК11	Переддипломна практика	10 (3)	диф. залік
ОК12	Технології DevSecOps	4 (2)	іспит
ОК13	Scientific Foreign Language	3 (2)	залік
Загальний обсяг обов'язкових компонент:		**67**	
Вибіркові компоненти ОПП*			
ДІВ1	Дисципліна індивідуального вибору 1	5 (1)	іспит
ДІВ2	Дисципліна індивідуального вибору 2	5 (1)	іспит
ДІВ3	Дисципліна індивідуального вибору 3	5 (2)	іспит
ДІВ4	Дисципліна індивідуального вибору 4	5 (2)	іспит
ДІВ5	Технічна дисципліна за вибором	3 (1)	залік
Загальний обсяг вибіркових компонент		**23**	
ЗАГАЛЬНИЙ ОБСЯГ ОСВІТНЬО-ПРОФЕСІЙНОЇ ПРОГРАМИ		**90**	

*Здобувач обирає одну дисципліну із запропонованих у переліках освітніх компонент ДІВ1 – ДІВ5, 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 ДІВ1 – ДІВ5 можуть збільшуватися і оновлюватися за рішенням галузевої НМК.

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

Під час формування переліку дисциплін, практик та атестації враховано вимоги стандартів вищої освіти за спеціальністю 125 «Кібербезпека та захист інформації» для другого (магістерського) рівня вищої освіти, положення «Про організацію освітнього процесу у ХАІ» (https://khai.edu/ua/university/normativna-baza/polozheniya1/polozhennya-yaki-regulyuyut-poryadok-zdijsnennya-osvitnogo-procesu/polozhennya-pro-organizaciyu-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 освітньо-професійної програми

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 дисципліни за вільним вибором здобувача. Структурно-логічна схема освітньої програми відображає послідовність вивчення її компонент і наведена у додатку Б. Схема містить обов'язкову й вибіркову компоненту. Здобувачем вищої освіти обирається індивідуальна траєкторія навчання яка реалізується через обирання вибіркових компонент відповідно до Положення «Про забезпечення права студентів на вибір навчальних дисциплін».

4 ФОРМА АТЕСТАЦІЇ ЗДОБУВАЧІВ ВИЩОЇ ОСВІТИ

Атестація випускників за освітньо-професійною програмою «Системне програмування» зі спеціальності 125 «Кібербезпека та захист інформації» проводиться у формі захисту кваліфікаційної роботи та завершується видачею документу встановленого зразка про присудження ступеня магістра із присвоєнням кваліфікації: магістр з комп'ютерної інженерії галузі знань інформаційні технології.

Атестація здійснюється відкрито і публічно.

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

Програмні компетентності	Компоненти освітньої програми												
	ОК1	ОК2	ОК3	ОК4	ОК5	ОК6	ОК7	ОК8	ОК9	ОК10	ОК11	ОК12	ОК13
ЗК1	+	+	+	+	+	+	+	+	+	+	+	+	
ЗК2		+	+	+	+	+	+	+		+	+	+	
ЗК3	+	+	+	+	+	+	+	+	+	+	+	+	
ЗК4	+	+	+	+	+	+	+	+	+	+	+	+	
ЗК5	+	+	+	+	+	+	+	+	+	+	+	+	
ЗК6	+	+	+	+	+	+	+	+	+	+	+	+	
ЗК7	+	+	+	+	+	+	+	+	+	+	+	+	
ЗК8		+		+			+			+		+	+
СК1	+		+	+	+		+	+		+	+	+	
СК2	+	+	+	+		+	+	+	+	+	+		
СК3			+	+			+	+	+	+	+	+	
СК4	+		+		+			+	+	+	+	+	
СК5			+	+	+			+	+	+		+	
СК6	+						+	+	+	+		+	
СК7							+	+	+	+		+	
СК8							+	+	+	+	+		
СК9			+					+	+	+		+	
СК10		+				+				+	+		
СК11			+	+				+		+	+		
СК12	+							+		+	+	+	

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

Програмні результати навчання	Компоненти освітньої програми												
	ОК1	ОК2	ОК3	ОК4	ОК5	ОК6	ОК7	ОК8	ОК9	ОК10	ОК11	ОК12	ОК13
ПРН1	+	+	+	+	+	+	+	+	+	+	+	+	+
ПРН2	+	+	+		+		+	+		+	+	+	
ПРН3	+						+	+		+	+		
ПРН4		+	+	+	+					+		+	
ПРН5		+	+		+		+	+	+	+	+		
ПРН6		+	+				+		+	+	+	+	
ПРН7	+	+	+	+		+	+	+	+	+		+	
ПРН8		+	+				+	+		+		+	
ПРН9							+	+	+	+	+		
ПРН10		+	+	+				+	+	+	+	+	
ПРН11		+					+	+	+	+		+	
ПРН12			+				+	+	+	+	+		
ПРН13					+		+	+	+	+	+	+	
ПРН14		+					+		+	+		+	
ПРН15		+	+		+		+	+	+	+		+	
ПРН16	+	+			+			+		+		+	
ПРН17	+	+	+	+	+	+	+	+	+	+	+	+	
ПРН18	+	+	+	+	+	+	+	+	+	+	+	+	
ПРН19	+	+	+	+	+	+	+	+	+	+	+	+	
ПРН20	+	+	+	+	+	+	+	+	+	+	+	+	
ПРН21			+		+		+	+		+	+		
ПРН22			+	+	+		+	+		+	+		
ПРН23	+	+	+	+	+		+	+		+	+	+	
ПРН24			+					+	+	+	+		
ПРН25		+		+				+		+	+	+	

ДОДАТОК А

РОЗПОДІЛ ОСВІТНІХ КОМПОНЕНТ ОСВІТНЬОЇ ПРОГРАМИ (КОП) ЗА КУРСАМИ ТА СЕМЕСТРАМИ

1 курс				2 курс	
1 семестр		2 семестр		3 семестр	
КОП	кількість кредитів	КОП	кількість кредитів	КОП	кількість кредитів
ОК1	3	ОК6	4	ОК10	20
ОК2	3	ОК7	3	ОК11	10
ОК3	4	ОК8	3		
ОК4	4	ОК9	3		
ОК5	3	ОК12	4		
		ОК13	3		
ДІВ1	*5*	*ДІВ3*	*5*		
ДІВ2	*5*	*ДІВ4*	*5*		
ДІВ5	*3*				
30,0		30,0		30,0	
60				60	

Всі компоненти (обов'язкові та вибіркові), їх зміст, формування компетентностей (загальних, спеціальних (фахових)) та визначення результатів навчання представлено у робочих програмах дисциплін та/або силабусах 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» зі спеціальності 125 «Кібербезпека та захист інформації»

https://khai.edu/ua/education/osvitni-programi-i-komponenti/osvitni-programi-magistriv/osvitno-profesijni-programi88/bezpeka-informaciinih-i-komunikaciinih-sistem6/

Додаток Б

СТРУКТУРНО-ЛОГІЧНА СХЕМА ОСВІТНЬО-ПРОФЕСІЙНОЇ ПРОГРАМИ