ID 60173

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»
22 червня 2023 р., протокол № 11

ОСВІТНЬО-ПРОФЕСІЙНА ПРОГРАМА

Безпека інформаційних і комунікаційних систем

Рівень вищої освіти – перший (бакалаврський)
галузі знань 12 Інформаційні технології
спеціальність 125 Кібербезпека та захист інформації

Кваліфікація: Бакалавр з кібербезпеки та захисту інформації
галузі знань інформаційні технології

Освітня програма вводиться в дію
«01» вересня 2023 р.

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

_____ Микола НЕЧИПОРУК
наказ №152 від «26» 06.2023 р.

Харків 2023 р.

ПЕРЕДМОВА

Освітньо-професійну програму (ОПП) «Безпека інформаційних і комунікаційних систем» для підготовки здобувачів першого (бакалаврського) рівня вищої освіти за спеціальністю 125 «Кібербезпека та захист інформації» в Національному аерокосмічному університеті ім. М. Є. Жуковського «Харківський авіаційний інститут» (далі – ХАІ) 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 1740) першого (бакалаврського) рівня вищої освіти за спеціальністю 125 «Кібербезпека» з урахуванням:

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

– стандарту вищої освіти за спеціальністю 125 «Кібербезпека» першого (бакалаврського) рівня вищої освіти (наказ МОН України № 1074 від 04.10.2018 р.).

Розроблення освітньо-професійної програми «Безпека інформаційних і комунікаційних систем» проведено групою забезпечення ОПП Національного аерокосмічного університету ім. М. Є. Жуковського «Харківський авіаційний інститут» у складі:

1	Керівник (гарант) освітньої програми	Ілляшенко О.О.	– канд. техн. наук, доцент, доцент кафедри комп'ютерних систем, мереж і кібербезпеки
2	Члени групи:	Морозова О.І.	– д-р техн. наук, доцент, професор кафедри комп'ютерних систем, мереж і кібербезпеки
3		Узун Д.Д.	– канд. техн. наук, доцент кафедри комп'ютерних систем, мереж і кібербезпеки

Рецензії-відгуки зовнішніх стейкхолдерів:

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.
3		

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 та захист інформації (наказ МОН України № 1074 від «04» жовтня 2018 р.) і встановлює:

– 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 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 бакалаврів 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 ХАІ;

– науково-педагогічні працівники, які здійснюють підготовку здобувачів за освітньо-професійною програмою «Безпека інформаційних і комунікаційних систем» зі спеціальності 125 Кібербезпека та захист інформації;

– екзаменаційна комісія спеціальності 125 Кібербезпека та захист інформації;

– приймальна комісія ХАІ.

Кафедри ХАІ, які залучені для підготовки фахівців ступеня бакалавра за освітньо-професійною програмою «Безпека інформаційних і комунікаційних систем» зі спеціальності 125 Кібербезпека 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-VII 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 123 Комп'ютерна інженерія для першого (бакалаврського) рівня вищої освіти (наказ МОН України від №1262 від «19» листопада 2018 р.).

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, (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».

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. 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.

ПРОФІЛЬ ОСВІТНЬО-ПРОФЕСІЙНОЇ ПРОГРАМИ 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 Computer Systems, Networks and Cybersecurity
Ступінь вищої освіти	Ступінь вищої освіти – бакалавр Bachelor`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 Specialty 125 Cyber Security and Information Protection Кваліфікація: бакалавр з кібербезпеки та захисту інформації галузі знань інформаційні технології Qualification: Bachelor`s Degree in Cyber Security and Information Protection of Area of knowledge Information Technology
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 ступеня «молодший бакалавр» (освітньо-кваліфікаційного рівня «молодший спеціаліст», ступеня «фаховий молодший бакалавр» – 240 кредитів ЄКТС. ХАІ визнає та перезараховує: • не більше ніж 120 кредитів ЄКТС, отриманих в межах попередньої освітньої програми підготовки молодшого бакалавра (молодшого спеціаліста); • не більше ніж 60 кредитів ЄКТС, отриманих за попередньою освітньою програмою фахової передвищої освіти
Наявність акредитації	Впроваджено у 2023 році Оновлення або модернізація освітньої програми здійснюється відповідно до розділу 5 Положення «Про розроблення та модернізацію освітніх програм в ХАІ».
Цикл/рівень	НРК України – 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 на базі освітнього ступеня «молодший бакалавр» (освітньо-кваліфікаційного рівня «молодший спеціаліст»), ступеня «фаховий молодший бакалавр».
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/ua/education/osvitni-programi-i-komponenti/osvitni-programi-bakalavriv/
2 – Мета освітньої програми	
Підготовка висококваліфікованих фахівців (бакалаврів) у галузі інформаційних технологій зі спеціальності 125 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, енергетичний та суміжних галузях згідно до стратегії розвитку Національного аерокосмічного університету ім. М. Є. Жуковського «Харківський авіаційний інститут» на 2020-2030 роки.	

3 – Характеристика освітньо-професійної програми	
Предметна область	Об’єкт вивчення: – об'єкти інформатизації, включаючи комп'ютерні, автоматизовані, телекомунікаційні, інформаційні, інформаційно-аналітичні, інформаційно-телекомунікаційні системи, інформаційні ресурси і технології; – технології забезпечення безпеки інформації; – процеси управління інформаційною та/або кібербезпекою об’єктів, що підлягають захисту. Ціль навчання: підготовка фахівців, здатних використовувати і впроваджувати технології інформаційної безпеки та/або кібербезпеки. Теоретичний зміст предметної області Знання: – законодавчої, нормативно-правової бази України та вимог відповідних міжнародних стандартів і практик щодо здійснення професійної діяльності; – принципів супроводу систем та комплексів інформаційної та/або кібербезпеки; – теорії, моделей та принципів управління доступом до інформаційних ресурсів; – теорії систем управління інформаційною та/або кібербезпекою; – методів та засобів виявлення, управління та ідентифікації ризиків; – методів та засобів оцінювання та забезпечення необхідного рівня захищеності інформації; – методів та засобів технічного та криптографічного захисту інформації; – сучасних інформаційно-комунікаційних технологій; – сучасного програмно-апаратного забезпечення інформаційно-комунікаційних технологій; – автоматизованих систем проектування. Методи, методики та технології: Методи, методики, інформаційно-комунікаційні технології та інші технології забезпечення інформаційної та/ або кібербезпеки. Інструменти та обладнання: – системи розробки, забезпечення, моніторингу та контролю процесів інформаційної та/ або кібербезпеки; – сучасне програмно-апаратне забезпечення інформаційно-комунікаційних технологій.
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 125 «Кібербезпека та захист інформації» освітнього ступеня «бакалавр з кібербезпеки» 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, енергетичний 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 мережевих 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 компенетностей. 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	Бакалавр може обіймати на підприємствах в галузі інформаційних технологій наступні первинні посади: розробника систем захисту інформації; адміністратора мереж і систем; аналітика загроз безпеки; аналітика систем захисту інформації та оцінки вразливостей; аналітик з безпеки інформаційно-телекомунікаційних систем; фахівця з криптографічного захисту інформації; фахівця з питань безпеки (інформаційно-комунікаційні технології); фахівця з підтримки інфраструктури кіберзахисту; фахівця із організації інформаційної безпеки; фахівця з технічного захисту інформації; фахівця сфери захисту інформації. Місця працевлаштування: науково-дослідні, проектно-конструкторські, виробничі, державні та приватні підприємства (фахівці ІТ-підрозділів або ІТ-підприємств), навчальні заклади.
Подальше навчання	Можливість навчання за програмою другого циклу вищої освіти. Набуття додаткових кваліфікацій в системі післядипломної освіти.
5 – Викладання та оцінювання	
Викладання та навчання	Студентське-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.
6 – Програмні компетентності	
Інтегральна компетентність	Здатність розв’язувати складні спеціалізовані задачі та практичні проблеми у галузі забезпечення інформаційної безпеки і\або кібербезпеки, що характеризується комплексністю та неповною визначеністю умов.
Загальні компетентності (ЗК)	КЗ 1. Здатність застосовувати знання у практичних ситуаціях. КЗ 2. Знання та розуміння предметної області та розуміння професії. КЗ 3. Здатність професійно спілкуватися державною та іноземною мовами як усно, так і письмово. КЗ 4. Вміння виявляти, ставити та вирішувати проблеми за професійним спрямуванням. КЗ 5. Здатність до пошуку, оброблення та аналізу інформації. КЗ 6. Здатність реалізувати свої права і обов’язки як члена суспільства, усвідомлювати цінності громадянського (вільного демократичного) суспільства та необхідність його сталого розвитку, верховенства права, прав і свобод людини і громадянина в Україні. КЗ 7. 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.

Фахові компетентності спеціальності (ФК)	КФ 1. Здатність застосовувати законодавчу та нормативно-правову базу, а також державні та міжнародні вимоги, практики і стандарти з метою здійснення професійної діяльності в галузі інформаційної та/або кібербезпеки. КФ 2. Здатність до використання інформаційно-комунікаційних технологій, сучасних методів і моделей інформаційної безпеки та/або кібербезпеки. КФ 3. Здатність до використання програмних та програмно-апаратних комплексів засобів захисту інформації в інформаційно-телекомунікаційних (автоматизованих) системах. КФ 4. Здатність забезпечувати неперервність бізнесу згідно встановленої політики інформаційної та/або кібербезпеки. КФ 5. Здатність забезпечувати захист інформації, що обробляється в інформаційно-телекомунікаційних (автоматизованих) системах з метою реалізації встановленої політики інформаційної та/або кібербезпеки. КФ 6. Здатність відновлювати штатне функціонування інформаційних, інформаційно-телекомунікаційних (автоматизованих) систем після реалізації загроз , здійснення кібератак, збоїв та відмов різних класів та походження. КФ 7. Здатність впроваджувати та забезпечувати функціонування комплексних систем захисту інформації (комплекси нормативно-правових, організаційних та технічних засобів і методів, процедур, практичних прийомів та ін.). КФ 8. Здатність здійснювати процедури управління інцидентами, проводити розслідування, надавати їм оцінку. КФ 9. Здатність здійснювати професійну діяльність на основі впровадженої системи управління інформаційною та/або кібербезпеки. КФ 10. Здатність застосовувати методи та засоби криптографічного та технічного захисту інформації на об'єктах інформаційної діяльності. КФ 11. Здатність виконувати моніторинг процесів функціонування інформаційних, інформаційно-телекомунікаційних (автоматизованих) систем згідно встановленої політики інформаційної та/або кібербезпеки. КФ 12. Здатність аналізувати, виявляти та оцінювати можливі загрози, уразливості та дестабілізуючі чинники інформаційному простору та інформаційним ресурсам згідно з встановленою політикою інформаційної та/або кібербезпеки.
7 – Результати навчання (визначені нормативним змістом підготовки здобувача вищої освіти)	
ПРН 1. Застосовувати знання державної та іноземних мов з метою забезпечення ефективності професійної комунікації. ПРН 2. Організовувати власну професійну діяльність, обирати оптимальні методи та способи розв'язування складних спеціалізованих задач та практичних проблем у професійній діяльності, оцінювати їхню ефективність. ПРН 3. Використовувати результати самостійного пошуку, аналізу та синтезу інформації з різних джерел для ефективного рішення спеціалізованих задач професійної діяльності. ПРН 4. Аналізувати, аргументувати, приймати рішення при розв'язанні складних спеціалізованих задач та практичних проблем у професійній діяльності, які характеризуються комплексністю та неповною визначеністю умов, відповідати за прийняті рішення. ПРН 5. Адаптуватися в умовах частої зміни технологій професійної діяльності, прогнозувати кінцевий результат. ПРН 6. Критично осмислювати основні теорії, принципи, методи і поняття у навчанні та професійній діяльності. ПРН 7. Діяти на основі законодавчої та нормативно-правової бази України та вимог відповідних стандартів, у тому числі міжнародних в галузі інформаційної та /або кібербезпеки. ПРН 8. Готувати пропозиції до нормативних актів щодо забезпечення інформаційної та /або кібербезпеки. ПРН 9. Впроваджувати процеси, що базуються на національних та міжнародних стандартах, виявлення, ідентифікації, аналізу та реагування на інциденти інформаційної та/або кібербезпеки. ПРН 10. Виконувати аналіз та декомпозицію інформаційно-телекомунікаційних систем. ПРН 11. Виконувати аналіз зв'язків між інформаційними процесами на віддалених обчислювальних системах.	

ПРН 12. Розробляти моделі загроз та порушника.
ПРН 13. Аналізувати проекти інформаційно-телекомунікаційних систем базуючись на стандартизованих технологіях та протоколах передачі даних.
ПРН 14. Вирішувати завдання захисту програм та інформації, що обробляється в інформаційно-телекомунікаційних системах програмно-апаратними засобами та давати оцінку результативності якості прийнятих рішень.
ПРН 15. Використовувати сучасне програмно-апаратне забезпечення інформаційно-комунікаційних технологій.
ПРН 16. Реалізовувати комплексні системи захисту інформації в автоматизованих системах (АС) організації (підприємства) відповідно до вимог нормативно-правових документів.
ПРН 17. Забезпечувати процеси захисту та функціонування інформаційно-телекомунікаційних (автоматизованих) систем на основі практик, навичок та знань, щодо структурних (структурно-логічних) схем, топології мережі, сучасних архітектур та моделей захисту електронних інформаційних ресурсів з відображенням взаємозв'язків та інформаційних потоків, процесів для внутрішніх і віддалених компонент.
ПРН 18. Використовувати програмні та програмно-апаратні комплекси захисту інформаційних ресурсів.
ПРН 19. Застосовувати теорії та методи захисту для забезпечення безпеки інформації в інформаційно-телекомунікаційних системах.
ПРН 20. Забезпечувати функціонування спеціального програмного забезпечення, щодо захисту інформації від руйнуючих програмних впливів, руйнуючих кодів в інформаційно-телекомунікаційних системах.
ПРН 21. Вирішувати задачі забезпечення та супроводу (в.т. числі: огляд, тестування, підзвітність) системи управління доступом згідно встановленої політики безпеки в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах.
ПРН 22. Вирішувати задачі управління процедурами ідентифікації, автентифікації, авторизації процесів і користувачів в інформаційно-телекомунікаційних системах згідно встановленої політики інформаційної і\або кібербезпеки.
ПРН 23. Реалізовувати заходи з протидії отриманню несанкціонованого доступу до інформаційних ресурсів і процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах.
ПРН 24. Вирішувати задачі управління доступом до інформаційних ресурсів та процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах на основі моделей управління доступом (мандатних, дискреційних, рольових).
ПНР 25. Забезпечувати введення підзвітності системи управління доступом до електронних інформаційних ресурсів і процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах з використанням журналів реєстрації подій, їх аналізу та встановлених процедур захисту.
ПРН 26. Впроваджувати заходи та забезпечувати реалізацію процесів попередження отриманню несанкціонованого доступу і захисту інформаційних, інформаційно-телекомунікаційних (автоматизованих) систем на основі еталонної моделі взаємодії відкритих систем.
ПРН 27. Вирішувати задачі захисту потоків даних в інформаційних, інформаційно-телекомунікаційних (автоматизованих) системах.
ПРН 28. Аналізувати та проводити оцінку ефективності та рівня захищеності ресурсів різних класів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах в ході проведення випробувань згідно встановленої політики інформаційної та\або кібербезпеки.
ПРН 29. Здійснювати оцінювання можливості реалізації потенційних загроз інформації, що обробляється в інформаційно-телекомунікаційних системах та ефективності використання комплексів засобів захисту в умовах реалізації загроз різних класів.
ПРН 30. Здійснювати оцінювання можливості несанкціонованого доступу до елементів інформаційно-телекомунікаційних систем.
ПРН 31. Застосовувати теорії та методи захисту для забезпечення безпеки елементів інформаційно-телекомунікаційних систем.
ПРН 32. Вирішувати задачі управління процесами відновлення штатного функціонування інформаційно-телекомунікаційних систем з використанням процедур резервування згідно встановленої політики безпеки.
ПРН 33. Вирішувати задачі забезпечення безперервності бізнес процесів організації на основі теорії ризиків.

ПРН 34. Приймати участь у розробці та впровадженні стратегії інформаційної безпеки та/або кібербезпеки відповідно до цілей і завдань організації. ПРН 35. Вирішувати задачі забезпечення та супроводу комплексних систем захисту інформації, а також протидії несанкціонованому доступу до інформаційних ресурсів і процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах згідно встановленої політики інформаційної і\або кібербезпеки. ПРН 36. Виявляти небезпечні сигнали технічних засобів. ПРН 37. Вимірювати параметри небезпечних та завадових сигналів під час інструментального контролю процесів захисту інформації та визначати ефективність захисту інформації від витоку технічними каналами відповідно до вимог нормативних документів системи технічного захисту інформації. ПРН 38. Інтерпретувати результати проведення спеціальних вимірювань з використанням технічних засобів, контролю характеристик інформаційно-телекомунікаційних систем відповідно до вимог нормативних документів системи технічного захисту інформації. ПРН 39. Проводити атестацію (спираючись на облік та обстеження) режимних територій (зон), приміщень тощо в умовах додержання режиму секретності із фіксуванням результатів у відповідних документах. ПРН 40. Інтерпретувати результати проведення спеціальних вимірювань з використанням технічних засобів, контролю характеристик ІТС відповідно до вимог нормативних документів системи технічного захисту інформації. ПРН 41. Забезпечувати неперервність процесу ведення журналів реєстрації подій та інцидентів на основі автоматизованих процедур. ПРН 42. Впроваджувати процеси виявлення, ідентифікації, аналізу та реагування на інциденти інформаційної і/або кібербезпеки. ПРН 43. Застосовувати національні та міжнародні регулюючі акти в сфері інформаційної безпеки та/ або кібербезпеки для розслідування інцидентів. ПРН 44. Вирішувати задачі забезпечення безперервності бізнес-процесів організації на основі теорії ризиків та встановленої системи управління інформаційною безпекою, згідно з вітчизняними та міжнародними вимогами та стандартами. ПРН 45. Застосовувати різні класи політик інформаційної безпеки та/ або кібербезпеки, що базуються на ризик-орієнтованому контролі доступу до інформаційних активів. ПРН 46. Здійснювати аналіз та мінімізацію ризиків обробки інформації в інформаційно-телекомунікаційних системах. ПРН 47. Вирішувати задачі захисту інформації, що обробляється в інформаційно-телекомунікаційних системах з використанням сучасних методів та засобів криптографічного захисту інформації. ПРН 48. Виконувати впровадження та підтримку систем виявлення вторгнень та використовувати компоненти криптографічного захисту для забезпечення необхідного рівня захищеності інформації в інформаційно-телекомунікаційних системах. ПРН 49. Забезпечувати належне функціонування системи моніторингу інформаційних ресурсів і процесів в інформаційно-телекомунікаційних системах. ПРН 50. Забезпечувати функціонування програмних та програмно-апаратних комплексів виявлення вторгнень різних рівнів та класів (статистичних, сигнатурних, статистично-сигнатурних). ПРН 51. Підтримувати працездатність та забезпечувати конфігурування систем виявлення вторгнень в інформаційно-телекомунікаційних системах. ПРН 52. Використовувати інструментарій для моніторингу процесів в інформаційно-телекомунікаційних системах. ПРН 53. Вирішувати задачі аналізу програмного коду на наявність можливих загроз. ПРН 54. Усвідомлювати цінності громадянського (вільного демократичного) суспільства та необхідність його сталого розвитку, верховенства права, прав і свобод людини і громадянина в Україні.

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 ім. М. Є. Жуковського «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 КМУ «Про затвердження Ліцензійних умов провадження освітньої діяльності закладів освіти» від 30.12.2015 р. № 1187 зі змінами).
Матеріально-технічне забезпечення	Матеріально-технічне забезпечення відповідає вимогам Ліцензійних умов провадження освітньої діяльності у сфері вищої освіти згідно з діючим законодавством України (Постанова КМУ «Про затвердження Ліцензійних умов провадження освітньої діяльності закладів освіти» від 30.12.2015 р. № 1187 зі 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 м^2. Навчальна площа на якій здійснюється освітній процес, складає 792,8 м^2. 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 м^2, 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'ютингу (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 «Про затвердження Ліцензійних умов провадження освітньої діяльності закладів освіти» від 30 грудня 2015 р. № 1187 зі змінами) включає в себе бібліотечні ресурси, електронні навчальні ресурси, сайт Національного аерокосмічного університету ім. М. Є. Жуковського «Харківський авіаційний інститут» 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 ім. М. Є. Жуковського «Харківський авіаційний інститут»; – MENTOR – система підтримки дистанційного навчання Національного аерокосмічного університету ім. М. Є. Жуковського «Харківський авіаційний інститут»; – rSmart® SakaiCLE і 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 ім. М. Є. Жуковського "Харківський авіаційний інститут". 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 ім. М. Є. Жуковського «Харківський авіаційний інститут» і технічними закладами України, зокрема: Інститут кібернетики імені В.М. Глушкова НАН України, ТОВ «482.СОЛЮШНС», ТОВ «SigmaSoftware», ТЗОВ «SoftServe», ТОВ «EpamSystems», 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); – 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 Centralede 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.

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

2.1 Перелік компонент освітньої програми

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	Вища математика	5 (1)	іспит
		5 (2)	іспит
		5 (3)	іспит
ОК2	Дискретна математика	4,5 (1)	іспит
		4 (2)	іспит
ОК3	Основи функціонування комп'ютерів	5 (1)	іспит
ОК4	Технології програмування	5 (1)	іспит
		4,5 (2)	іспит
ОК5	Основи професійної україномовної комунікації	3 (1)	залік
ОК13	Технології безпечного програмування	4 (3)	іспит
ОК6	Фізика	5 (2)	залік
ОК7	Комп'ютерна електроніка	4 (2)	іспит
ОК8	Іноземна мова	3 (2)	диф. залік
ОК9	Архітектура комп'ютерів	4 (3)	іспит
ОК12	Системи технічного захисту інформації	4 (3)	залік
		4,5 (4)	іспит
ОК11	Моделі та структури даних	4,5 (3)	іспит
ОК10	Схемотехніка засобів безпеки	4 (3)	іспит
ОК14	Апаратні та програмні засоби захисту інформації	4,5 (4)	іспит
ОК15	Операційні системи	4,5 (4)	іспит
ОК16	Теоретичні основи криптології	4,5 (4)	іспит
ОК17	Технології безпечного програмування (КП)	2 (4)	диф. залік
ОК18	Web-технології	4 (5)	іспит
ОК19	Безпека засобів штучного інтелекту	4 (5)	іспит
ОК20	Теорія інформації та кодування	3,5 (5)	залік
ОК21	Інформаційно-комунікаційні системи	4 (5)	іспит
ОК23	Прикладна криптологія	4 (5)	іспит
		4,5 (6)	іспит
ОК22	Безпечні вбудовані системи	4 (5)	іспит
ОК24	Організація та безпека баз даних	4 (6)	іспит
ОК26	Побудова та кібербезпека інтернету речей	4 (6)	іспит
ОК25	Нормативно-правове забезпечення інформаційної безпеки	4 (6)	іспит
ОК29	Управління інформаційною безпекою	4 (7)	залік
		4 (8)	залік
ОК30	Функційна безпечність та надійність комп'ютерних систем	4 (7)	іспит
ОК27	Захист інформації в інформаційно-комунікаційних системах	4,5 (7)	іспит
		4 (8)	іспит
ОК28	Комплексні системи захисту інформації: проектування, впровадження, супровід	4 (7)	іспит
		4 (8)	іспит
ОК31	Навчальна практика	3 (2)	залік
ОК32	Ознайомча практика	3 (4)	залік
ОК33	Виробнича практика	3 (6)	залік
ОК34	Кваліфікаційна робота бакалавра	9 (8)	іспит
	Єдиний державний кваліфікаційний іспит (ЄДКІ)	-	Атестація
Загальний обсяг обов'язкових компонент:		**180**	
Вибіркові компоненти ОП*			
Гуманітарний блок (Soft skills)			
ВК1	Правова компетентність	3 (1)	залік

Код КОП	Компоненти освітньої програми (навчальні дисципліни, курсові проекти (роботи), практики, кваліфікаційна робота)	Кількість кредитів	Форма підсумкового контролю
1	2	3	4
ВК2	Мовні компетентності (іноземна мова)	3 (1)	залік
ВК3	Економічна дисципліна за вибором	3 (4)	залік
ВК4	Формування системного наукового світогляду	3 (2)	залік
ВК5	Соціально-гуманітарна дисципліна за вибором	3 (3)	залік
ВК6	Математично-технічний блок на вибір	5,5 (4)	залік
Блок дисциплін професійного спрямування MINOR**			
ВК7	Minor. Дисципліна 1	5 (5)	іспит
ВК8	Minor. Дисципліна 2	5 (5)	іспит
ВК9	Minor. Дисципліна 3	5 (7)	іспит
ВК10	Minor. Дисципліна 4	5 (8)	іспит
Окремі вибіркові дисципліни***			
ВК11	Дисципліна індивідуального вибору 1	5 (6)	іспит
ВК12	Дисципліна індивідуального вибору 2	5 (7)	іспит
ВК13	Дисципліна індивідуального вибору 3	5,5 (8)	іспит
ВК14	Дисципліна із циклу за вибором кафедри 503 (КП1)	2 (6)	диф. залік
ВК15	Дисципліна із циклу за вибором кафедри 503 (КП2)	2 (7)	диф. залік
Загальний обсяг вибіркових компонент:		**60**	
ЗАГАЛЬНИЙ ОБСЯГ ОСВІТНЬОЇ ПРОГРАМИ		**240**	

*Здобувач обирає одну дисципліну із запропонованих у переліках/блоках освітніх компонент ВК1 – ВК15, тим самим забезпечує опанування і поглиблення загальних компетентностей та результатів навчання, що направлені на здобуття соціальних навичок відповідно до вимог стандарту спеціальності. Переліки складових освітніх компонент ВК1 – ВК15 може збільшуватися і оновлюватися за рішенням галузевої НМК.
**Здобувач може обрати будь-який блок дисциплін компетентного спрямування MINOR. Блоки дисциплін компетентного спрямування MINOR можуть збільшуватися і оновлюватися за рішенням галузевої НМК.
*** Загальноуніверситетський блок, в якому дисципліни для вибору пропонують кафедри Університету або інші підрозділи відповідно до напрямів своєї діяльності або наукових напрямів/шкіл.

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

Здобувач, який зарахований на базі освітнього ступеня «молодший бакалавр» (освітньо-кваліфікаційного рівня «молодший спеціаліст»), ступеня «фаховий молодший бакалавр» виконує освітньо-професійну програму в обсязі – 240 кредитів ЄКТС. ХАІ визнає та перезараховує не більше ніж 120 кредитів ЄКТС, отриманих в межах попередньої освітньої програми підготовки молодшого бакалавра (молодшого спеціаліста); не більше ніж 60 кредитів ЄКТС, отриманих за попередньою освітньою програмою фахової передвищої освіти.

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 перезарахування навчальних дисциплін і визначення академічної різниці в Національному аерокосмічному університеті ім. М. Є. Жуковського «Харківський авіаційний інститут»» (https://khai.edu/ua/university/normativna-baza/polozheniya1/polozhennya-yaki-regulyuyut-poryadok-zdijsnennya-osvitnogo-procesu/polozhennya-pro-poryadok-perezarahuvannya/) шляхом порівняння: відповідності змісту дисципліни освітньо-професійної програми (ОПП); запланованих результатів навчання з відповідної дисципліни; загального обсягу у годинах і кредитах ЄКТС; форм підсумкового контролю тощо.

2.2 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 першого (бакалаврського) 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.

2.3 Структурно-логічна схема освітньої програми

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

3 ФОРМА АТЕСТАЦІЇ ЗДОБУВАЧІВ ВИЩОЇ ОСВІТИ

Атестація випускників за освітньо-професійною програмою «Безпека інформаційних і комунікаційних систем» зі спеціальності 125 «Кібербезпека та захист інформації» здійснюється у формі захисту кваліфікаційної роботи бакалавра та єдиного державного кваліфікаційного іспиту.

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

Єдиний державний кваліфікаційний іспит передбачає оцінювання досягнень результатів навчання, визначених цим стандартом та освітньою програмою.
Атестація здійснюється відкрито і публічно.

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

Програмні компетентності	Компоненти освітньої програми																																
	ОК 1	ОК 2	ОК 3	ОК 4	ОК 5	ОК 6	ОК 7	ОК8	ОК 9	ОК 10	ОК 11	ОК 12	ОК 13	ОК 14	ОК 15	ОК 16	ОК 17	ОК 18	ОК 19	ОК 20	ОК 21	ОК 22	ОК 23	ОК 24	ОК 25	ОК 26	ОК 27	ОК 28	ОК 29	ОК 30	ОК 31	ОК 32	ОК 33	ОК 34
ЗК1	+	+		+	+	+	+	+	+	+	+	+	+	+	+	+	+	+		+	+	+	+	+	+	+	+	+	+	+	+	+	+	+
ЗК2	+	+		+	+	+		+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+
ЗК3			+	+	+		+	+				+	+	+	+		+	+	+		+	+	+	+	+	+	+	+	+			+	+
ЗК4	+	+		+		+	+		+	+	+	+	+	+	+	+	+	+		+	+	+	+	+	+	+	+	+	+	+	+	+	+	+
ЗК5	+	+		+		+	+		+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+
ЗК6			+		+														+															+
ЗК7								+																					+					+
ФК1																+	+						+		+				+	+	+	+	+	+
ФК2	+	+		+									+					+		+	+								+	+				+
ФК3				+					+	+		+	+	+			+	+			+	+				+			+	+	+	+	+	+
ФК4											+	+		+	+	+							+	+			+	+	+	+				+
ФК5				+							+	+	+	+						+		+				+	+	+			+		+	+
ФК6		+		+		+	+		+	+			+		+			+		+		+					+	+		+			+
ФК7	+	+		+		+	+			+	+	+	+	+	+	+		+		+		+	+	+	+	+	+	+	+	+				+
ФК8																									+		+	+	+					+
ФК9																									+		+	+	+					+
ФК10	+	+		+									+	+		+						+	+	+				+						+
ФК11			+						+	+	+	+			+				+					+	+		+	+	+					+
ФК12	+	+		+			+		+		+	+	+	+		+	+					+	+	+	+	+	+	+	+	+	+	+	+	+

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

Програмні результати навчання	Компоненти освітньої програми																																	
	ОК 1	ОК 2	ОК 3	ОК 4	ОК 5	ОК 6	ОК 7	ОК8	ОК 9	ОК 10	ОК 11	ОК 12	ОК 13	ОК 14	ОК 15	ОК 16	ОК 17	ОК 18	ОК 19	ОК 20	ОК 21	ОК 22	ОК 23	ОК 24	ОК 25	ОК 26	ОК 27	ОК 28	ОК 29	ОК 30	ОК 31	ОК 32	ОК 33	ОК 34
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															+										+				+					+
ПРН26																					+				+			+	+					+
ПРН27				+									+				+		+		+						+							+
ПРН28																					+				+		+							+
ПРН29																					+				+			+						+
ПРН30																												+	+	+				+

Програмні результати навчання	Компоненти освітньої програми																																	
	ОК 1	ОК 2	ОК 3	ОК 4	ОК 5	ОК 6	ОК 7	ОК8	ОК 9	ОК 10	ОК 11	ОК 12	ОК 13	ОК 14	ОК 15	ОК 16	ОК 17	ОК 18	ОК 19	ОК 20	ОК 21	ОК 22	ОК 23	ОК 24	ОК 25	ОК 26	ОК 27	ОК 28	ОК 29	ОК 30	ОК 31	ОК 32	ОК 33	ОК 34
ПРН31																+					+						+	+					+	+
ПРН32																											+		+	+				+
ПРН33																											+	+	+					+
ПРН34																											+	+	+					+
ПРН35																											+	+	+					+
ПРН36										+		+																				+		+
ПРН37												+													+							+		+
ПРН38												+									+				+							+	+	+
ПРН40												+									+				+							+	+	+
ПРН41																											+	+	+					+
ПРН42																									+		+		+					+
ПРН43																									+		+		+					+
ПРН44																									+			+	+					+
ПРН45																											+	+	+					+
ПРН46																					+						+		+					+
ПРН47																+					+		+										+	+
ПРН48														+		+					+	+	+											+
ПРН49															+														+			+		+
ПРН50														+													+					+	+	+
ПРН51														+													+					+	+	+
ПРН52														+							+								+					+
ПРН53				+										+										+			+							+
ПРН54					+			+					+						+						+							+	+	+

Додаток А

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

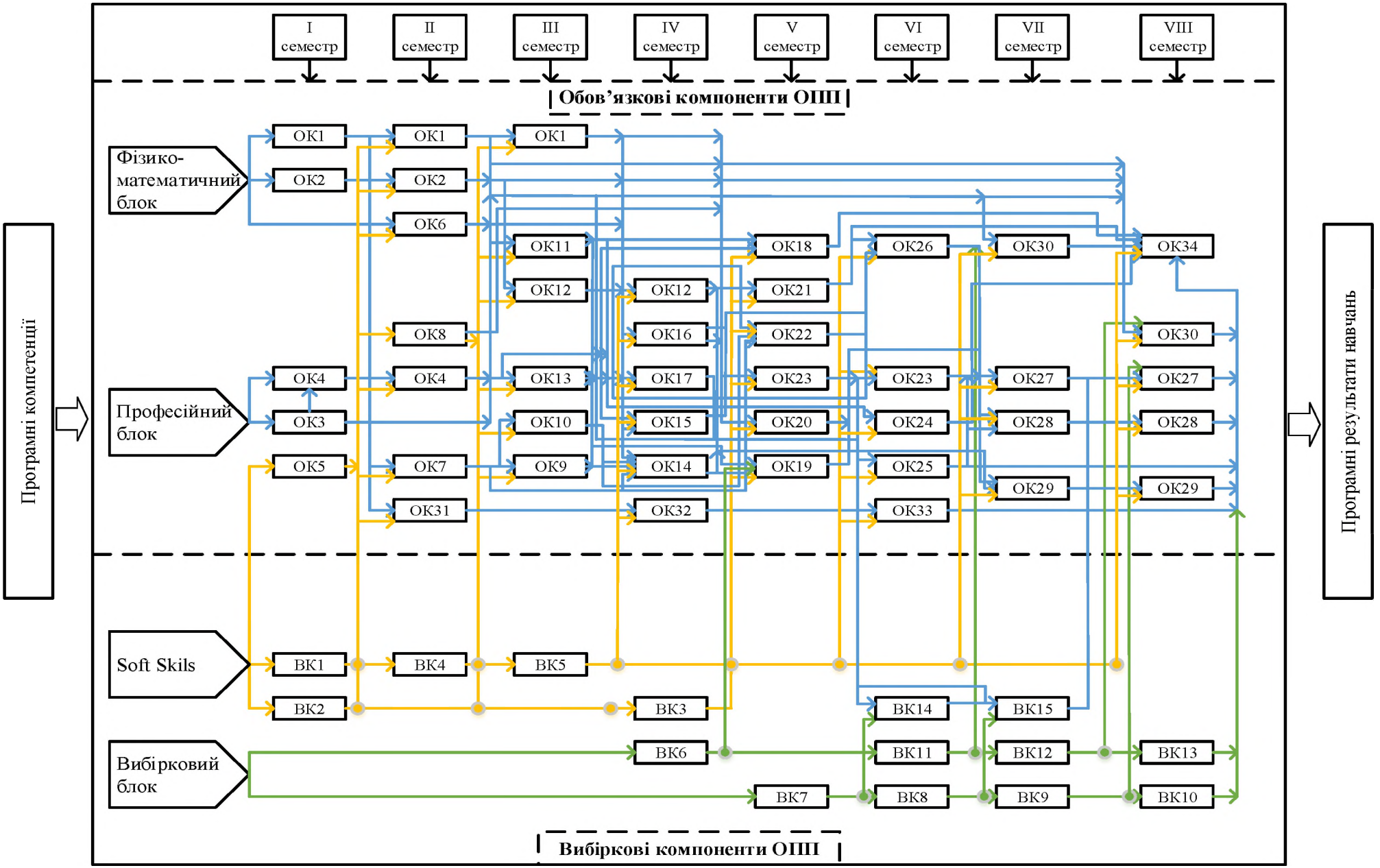
1 курс				2 курс				3 курс				4 курс			
1 семестр		2 семестр		3семестр		4 семестр		5 семестр		6 семестр		7 семестр		8 семестр	
КОП	кількість кредитів	КОП	кількість кредитів	КОП	кількість кредитів	КОП	кількість кредитів	КОП	кількість кредитів	КОП	кількість кредитів	КОП	кількість кредитів	КОП	кількість кредитів
ОК1	5	ОК1	5	ОК1	5	ОК14	4.5	ОК18	4	ОК24	4	ОК27	4.5	ОК27	4
ОК2	4.5	ОК6	5	ОК9	4	ОК15	4.5	ОК21	4	ОК25	4	ОК28	4	ОК28	4
ОК3	5	ОК2	4	ОК10	4	ОК12	4.5	ОК22	4	ОК23	4.5	ОК30	4	ОК29	4
ОК4	5	ОК7	4	ОК11	4.5	ОК16	4.5	ОК23	4	ОК26	4	ОК29	4	ОК34	9
ОК5	3	ОК4	4.5	ОК12	4	ОК17	2	ОК19	4	ОК33	3				
		ОК8	3	ОК13	4	ОК32	3	ОК21	3.5						
		ОК31	3												
ВК1	3	ВК4	3	ВК5	3	ВК3	3	ВК7	5	ВК8	5	ВК9	5	ВК10	5
ВК2	3					ВК6	5.5			ВК11	5	ВК12	5	ВК13	5.5
										ВК14	2	ВК15	2		
28,5		31,5		28,5		31,5		28,5		31,5		28,5		31,5	
60				60				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" спеціальності 125 «Кіберезпека та захист інформації».

https://khai.edu/ua/education/osvitni-programi-i-komponenti/osvitni-programi-bakalavriv/bezpeka-informacijnih-i-komunikacijnih-sistem/

Додаток Б

СТРУКТУРНО-ЛОГІЧНА СХЕМА ОСВІТНЬО-ПРОФЕСІЙНОЇ ПРОГРАМИ



ЛИСТ ОБЛІКУ ВНЕСЕННЯ ЗМІН

Номер зміни	Дата введення в дію	Пояснення до змін
1.	2 вересня 2024 р.	Затвердити зміни до освітньо-професійної програми «Безпека інформаційних і комунікаційних систем» спеціальності 125 «Кібербезпека та захист інформації» першого (бакалаврського) рівня вищої освіти для здобувачів усіх курсів та форм навчання, які на ній навчаються. (Додаток А). Підстава: 1) Наказ МОН України від 13.06.2024 № 842 «Про внесення змін до деяких стандартів вищої освіти»; 2) Рішення галузевої навчально-методичної комісії № 2 (протокол №1 від 30.08.2024).

ДОДАТОК А

Затверджені зміни у

освітньо-професійній програмі «Безпека інформаційних і комунікаційних систем»
спеціальності 125 «Кібербезпека та захист інформації»
галузі знань 12 «Інформаційні технології»
першого (бакалаврського) рівня вищої освіти
викладено у такій редакції:

2 ПРОФІЛЬ ОСВІТНЬО-ПРОФЕСІЙНОЇ ПРОГРАМИ «Безпека інформаційних і комунікаційних систем» зі спеціальності 125 «Кібербезпека та захист інформації»

Позицію «Загальні компетентності» пункту 6 – Програмні компетентності доповнити ЗК8 такого змісту:

ЗК8. Здатність ухвалювати рішення та діяти, дотримуючись принципу неприпустимості корупції та будь-яких інших проявів недоброчесності.

5 МАТРИЦЯ ВІДПОВІДНОСТІ ПРОГРАМНИХ КОМПЕТЕНТНОСТЕЙ КОМПОНЕНТАМ ОСВІТНЬО-ПРОФЕСІЙНОЇ ПРОГРАМИ

Ввести до всіх компонент освітньо-професійній програмі «Безпека інформаційних і комунікаційних систем» спеціальності 125 «Кібербезпека та захист інформації» першого (бакалаврського) рівня вищої освіти, для здобувачів усіх курсів та форм навчання, які на ній навчаються загальну компетентність ЗК8. Здатність ухвалювати рішення та діяти, дотримуючись принципу неприпустимості корупції та будь-яких інших проявів не доброчесності.