ID 1740

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 – перший (бакалаврський)
за спеціальністю 125Кібербезпека
галузі знань 12 Інформаційні технології
Кваліфікація: Бакалавр з кібербезпеки галузі знань інформаційні технології

(із змінами, внесеними згідно із рішеннями:
вченої ради ХАІ протокол № 5 від 26.12.2018 р.
вченої ради ХАІ протокол № 9 від 20.03.2019 р.
науково-методичної ради (НМК) 2, протокол №1 від 31.08.2020р.)

Освітня програма вводиться в дію
з «01» вересня 2020 р.

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

М. В. Нечипорук
Наказ № 383 від 01.09. 2020 р.

Харків 2020 р.

ПЕРЕДМОВА

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

– зі змінами відповідно до Стандарту МОН (наказ МОН № 1074 від 04.10.2018 р.) (затверджено рішенням вченої ради, протокол № 5 від 26.12.2018);

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

– зі зміною Національної рамки кваліфікацій (Постанова Кабінету міністрів України від 25 червня 2020, № 519) та модернізацією структури вибіркової компоненти освітньої програми й оновленням змісту її опису (затверджено рішенням науково-методичної комісії 2 (НМК 2) ХАІ протокол № 1 від 31.08.2020 р.).

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

1	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 (за наявності):

1

2

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

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

Освітньо-професійна програма використовується для:

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

Кафедри ХАІ, які залучені для підготовки фахівців ступеня бакалавра за освітньо-професійною програмою «Безпека інформаційних і комунікаційних систем» зі спеціальності 125 «Кібербезпека» 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 125 «Кібербезпека» для першого (бакалаврського) рівня вищої освіти (наказ МОН України від №1074 від «04» жовтня 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.

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», затверджене вченою радою університету.

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

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

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

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

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.

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

1 – Загальна інформація	
Повна назва вищого навчального закладу та структурного підрозділу	Національний аерокосмічний університет ім. М. Є. Жуковського «Харківський авіаційний інститут» Кафедра комп'ютерних систем, мереж і кібербезпеки
Ступінь вищої освіти	Бакалавр
Ступінь вищої освіти та назва кваліфікації мовою оригіналу	Ступінь вищої освіти – бакалавр Кваліфікація – бакалавр з кібербезпеки галузі знань інформаційні технології Degree of higher education – bachelor Qualification – Bachelor of Cyber Security of Areas of knowledge Information Technologies
Офіційна назва освітньо-професійної програми	Безпека інформаційних і комунікаційних систем Security of Information and Communication Systems
Тип диплому та обсяг освітньо-професійної програми	Диплом бакалавра, одиничний, термін навчання 3 роки 10 місяців: – на базі повної загальної середньої освіти – 240 кредитів ЄКТС; – на базі ступеня «молодший бакалавр» (освітньо-кваліфікаційного рівня «молодший спеціаліст») – 240 кредитів ЄКТС. ХАІ визнає та перезараховує не більше ніж 120 кредитів ЄКТС, отриманих в межах попередньої освітньої програми підготовки молодшого бакалавра (молодшого спеціаліста).
Наявність акредитації	Сертифікат про акредитацію: Серія УД № 21008326 від 25.01.2019 р. відповідно до рішення Акредитаційної комісії від 16 червня 2016 р. протокол № 121 (наказ МОН України від 21.06.2016 № 79-А). Період акредитації: до 01 липня 2021 р.
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 початкового рівня (короткого циклу) вищої освіти (молодший бакалавр), фаховий молодший бакалавр у порядку, визначеному законодавством
Мова(и) викладання	Мовою викладання є державна мова. З метою створення умов для міжнародної академічної мобільності може бути прийнято рішення про викладання однієї чи декількох дисциплін англійською та/або іншими іноземними мовами
Термін дії освітньо-професійної програми	Перегляд освітньої програми здійснюється не рідше ніж один раз на 5 років 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 стейхолдерів.
Інтернет-адреса постійного розміщення опису ОПП	https://khai.edu/ua/education/osvitni-programi-i-komponenti/osvitni-programi-bakalavriv/
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» за спеціальністю 125 «Кібербезпека». 2 Формування особистості фахівця здатного використовувати професійно-профільні знання й практичні навички для вирішення складних спеціалізованих задач та практичних проблем у галузі інформаційних технологій з урахуванням специфіки аерокосмічної галузі.	

3 – Характеристика освітньо-професійної програми	
Предметна область	**Об’єктом вивчення :** − об'єкти інформатизації, включаючи комп'ютерні, автоматизовані, екомунікаційні, інформаційні, інформаційно-аналітичні, інформаційно-екомунікаційні системи, інформаційні ресурси і технології; − технології забезпечення безпеки інформації; − процеси управління інформаційною та/або кібербезпекою об’єктів, що лягають захисту. **Ціль навчання:** підготовка фахівців, здатних використовувати і впроваджувати технології інформаційної безпеки та/або кібербезпеки. **Теоретичний зміст предметної області:** − законодавчої, нормативно-правової бази України та вимог відповідних народних стандартів і практик щодо здійснення професійної діяльності; − принципів супроводу систем та комплексів інформаційної та/або ербезпеки; − теорії, моделей та принципів управління доступом до інформаційних урсів; − теорії систем управління інформаційною та/або кібербезпекою; − методів та засобів виявлення, управління та ідентифікації ризиків; − методів та засобів оцінювання та забезпечення необхідного рівня ищеності інформації; − методів та засобів технічного та криптографічного захисту інформації; − сучасних інформаційно-комунікаційних технологій; − сучасного програмно-апаратного забезпечення ормаційно-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 ормаційної та/ або кібербезпеки; − сучасне програмно-апаратне забезпечення інформаційно-тунікаційних технологій.
Орієнтація ОПП	Освітньо-професійна програма підготовки бакалавра розроблена для студентів, які прагнуть стати фахівцями у галузі інформаційних технологій.
Основний фокус ОПП (спеціалізації)	Освітньо-професійна програма встановлює кваліфікаційні вимоги до соціально-виробничої діяльності випускників закладу вищої освіти зі спеціальності 125 «Кібербезпеки» освітнього ступеня «бакалавр» 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 спрямована на вивчення систем та мов програмування, які сприятимуть реалізації напряму наскрізного підходу до систем забезпечення інформаційною та/або кібербезпекою в інформаційно-комунікаційних системах з урахуванням специфіки аерокосмічної галузі, що починається з побудови моделі загроз і закінчується побудовою системи захисту. Практика проводиться на підприємствах різних галузей промисловості.
4 – Придатність випускників до працевлаштування та подальшого навчання	
Придатність до працевлаштування	Випускники можуть працювати за професіями згідно з Національним класифікатором професій ДК 003:2010: фахівець з інформаційних технологій; фахівець з розробки та тестування програмного забезпечення; фахівець із організації захисту інформації з обмеженим доступом; фахівець із організації інформаційної безпеки. Місця працевлаштування: навчальні заклади; науково-дослідні, проектно-конструкторські, виробничі, державні та приватні підприємства (фахівці ІТ-підрозділів, ІТ-підприємств або підрозділів з захисту інформації).
Подальше навчання	Можливість продовжити навчання за освітньою програмою ступеня магістра.
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 (дипломний проект) 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	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	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 – Програмні результати навчання	
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	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).
Матеріально-технічне забезпечення	Загальна площа, на якій розміщені приміщення кафедри комп'ютерних систем та мереж 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 та мереж 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'ютинга (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.). 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)..
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).
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.
Міжнародна кредитна мобільність	На основі двосторонніх договорів між Національним аерокосмічним університетом ім. М. Є. Жуковського «Харківський авіаційний інститут» і навчальними закладами країн-партнерів. ERASMUS+ .
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	Семестр
1	2	3	4	5
Обов'язкові компоненти ОП				
ОК1	Вища математика	15		1,2,3
ОК2	Дискретна математика	8,5	іспити	1,2
ОК3	Основи функціонування комп'ютерів	5	іспит	1
ОК4	Технології програмування	18	іспити	1,2,3,4
ОК5	Фізика	5	залік	2
ОК6	Комп'ютерна електроніка	4	іспит	2
ОК7	Архітектура комп'ютерів	4	іспит	3
ОК8	Системи технічного захисту інформації	9	залік, іспит	3,4
ОК9	Моделі та структури даних	4,5	іспит	3
ОК10	Комп'ютерна схемотехніка	4	іспит	3
ОК11	Апаратні та програмні засоби захисту інформації	4,5	іспит	4
ОК12	Операційні системи	4,5	іспит	4
ОК13	Технології програмування (КП)	2	диф. залік	4
ОК14	Теорія інформації та кодування	3,5	залік	5
ОК15	Інформаційно-комунікаційні системи	4	іспит	5
ОК16	Прикладна криптологія	8,5	іспити	5,6
ОК17	Вбудовані системи	4	іспит	5
ОК18	Web-технології	4	іспит	5
ОК19	Програмування засобів штучного інтелекту на Python	4	залік	5
ОК20	Бази даних	4	іспит	6
ОК21	Програмування систем IoT	4	іспит	6
ОК22	Прикладна криптологія (КП)	2	диф. залік	6
ОК23	Нормативно-правове забезпечення інформаційної безпеки	4	іспит	6
ОК24	Управління інформаційною безпекою	4	залік	7
ОК25	Захист інформації в інформаційно-комунікаційних системах (КП)	2	диф. залік	7
ОК26	Надійність та функціональна безпека інформаційно-управляючих систем	4,5	іспит	7
ОК27	Захист інформації в інформаційно-комунікаційних системах	8	іспити	7,8
ОК28	Комплексні системи захисту інформації: проектування, впровадження, супровід	8,5	іспити	7,8
ОК29	Тестування та забезпечення якості	4	іспит	8
ОК30	Навчальна практика	3	залік	2
ОК31	Ознайомча практика	3	залік	4
ОК32	Виробнича практика	3	залік	6
ОК33	Кваліфікаційна робота бакалавра	9	атестація	
Загальний обсяг обов'язкових компонент:		**179**		
Вибіркові компоненти ОП*				
Гуманітарний блок (Soft skills)				
ВК1	Правова компетентність	3	залік	2
ВК2	Українські студії	3	залік	1
ВК3	Мовні компетентності (іноземна мова)	6	залік, диф. залік	1,2
ВК4	Математично-технічний блок на вибір	5	залік	4
ВК5	Гуманітарна або економічна дисципліна за вибором	3	залік	1
ВК6	Компетентності, спрямовані на формування системного наукового світогляду	3	залік	3
ВК7	Компетентності загального культурного кругозору та розвитку комунікацій	3	залік	4

Код КОП	Компоненти освітньої програми (навчальні дисципліни, курсові проекти (роботи), практики, кваліфікаційна робота)	Кількість кредитів	Форма підсумкового контролю	Семестр
1	2	3	4	5
Блок дисциплін професійного спрямування MINOR**				
ВК8	Minor. Дисципліна 1	5	іспит	5
ВК9	Minor. Дисципліна 2	5	іспит	6
ВК10	Minor. Дисципліна 3	5	іспит	7
ВК11	Minor. Дисципліна 4	5	іспит	8
Окремі вибіркові дисципліни***				
ВК12	Дисципліна індивідуального вибору 1	5	іспит	6
ВК13	Дисципліна індивідуального вибору 2	5	іспит	7
ВК14	Дисципліна індивідуального вибору 3	5	іспит	8
Загальний обсяг вибіркових компонент:		**61**		
ЗАГАЛЬНИЙ ОБСЯГ ОСВІТНЬОЇ ПРОГРАМИ		**240**		

*Здобувач обирає одну дисципліну із запропонованих у переліках/блоках освітніх компонент ВК1 – ВК7, 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 – ВК7 може збільшуватися і оновлюватися за рішенням галузевої НМК.

**Здобувач може обрати будь-який блок дисциплін професійного спрямування MINOR. Блоки дисциплін професійного 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 ступеня «молодший бакалавр» (освітньо-кваліфікаційного рівня «молодший спеціаліст»), виконує освітньо-професійну програму в обсязі 240 кредитів ЄКТС. При цьому ХАІ визнає та перезараховує не більше ніж 120 кредитів ЄКТС, отриманих в межах попередньої освітньої програми підготовки молодшого бакалавра (молодшого спеціаліста).

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.

3.2 Структурно-логічна схема ОП

Структурно-логічна схема (додаток А) 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 на підставі Положення «Про забезпечення права студентів на вибір навчальних дисциплін».

3.3 Формування компетентностей (фахових, спеціальних) та програмних результатів навчання обов’язкової компоненти

№ з/п	Код КОП	Назва компонента ОП	Мета та завдання компонента ОП	Формування компетентностей		Програмні результати навчання
				загальні	фахові	
1.	ОК1	Вища математика	**Мета**: глибоке засвоєння знань щодо основних методів вищої математики, що забезпечать логіку математичного мислення студентів. **Завдання**: вивчення основних методів вищої математики для подальшого використання в дисциплінах, пов’язаних з математичними моделями та методами оптимізації; знати загальну теорію побудови математичних моделей робочих процесів та їх реалізацію.	КЗ 1 КЗ 2 КЗ 4 КЗ 5	КФ 2 КФ 5 КФ 6 КФ 7 КФ 10 КФ 11 КФ 12	ПРН1 ПРН2 ПРН3 ПРН4 ПРН5
2.	ОК2	Дискретна математика	**Мета**: надання бакалаврам теоретичного фундаменту для коректної постановки, формального подання та обґрунтування методу рішення теоретичних та практичних задач в області алгоритмізації, проектування та побудови інформаційних систем. **Завдання**: формування у студентів базових понять і навичок для побудови та визначення властивостей основних об’єктів дискретної математики – множин, алгебр, комбінаторних об’єктів, логічних висловлювань, графів, дерев – для вирішення відповідних задач при розробці та аналізі інформаційних систем для використання у професійній діяльності.	КЗ 1 КЗ 2 КЗ 4 КЗ 5	КФ 2 КФ 6 КФ 7 КФ 10 КФ 12	ПРН1 ПРН3 ПРН4 ПРН5 ПРН11
3.	ОК3	Основи функціонування комп'ютерів	**Мета**: надати знання методів збору, аналізу, класифікації, представлення і оброблення інформації у комп'ютері, а також базовими принципами побудови та функціонування сучасних комп'ютерів **Завдання**: аналізувати інформацію із навколишнього середовища з метою вибору придатного типу і формату даних для її представлення, зберігання та перетворення; застосовувати принципи кодування аналогової та цифрової інформації, та методи оброблення цифрової інформації, представленої у базових кодах; аналізувати та критикувати властивості комп'ютерів та їх складових для класифікації комп'ютерів з метою оцінки та співвіднесення їх до певної архітектури; застосовувати знання архітектури комп'ютерів для розроблення алгоритму, кодування, тестування програми у машинних кодах для виконання у середовищі учбового комп'ютера ToyCom.	КЗ 1 КЗ 4	КФ 3 КФ 6 КФ 11 КФ 12	ПРН1 ПРН2 ПРН3 ПРН5 ПРН6
4.	ОК4	Технології програмування	**Мета**: вивчення програмного забезпечення персональних комп’ютерів (ПК), загального синтаксису мови програмування С++, типових алгоритмів вирішення задач системи автоматизованого проектування (САПР).	КЗ 1 КЗ 2 КЗ 3 КЗ 4	КФ 2 КФ 3 КФ 5 КФ 6	ПРН1 ПРН5 ПРН14 ПРН15

№ з/п	Код КОП	Назва компонента ОП	Мета та завдання компонента ОП	Формування компетентностей		Програмні результати навчання
				загальні	фахові	
			Завдання: вивчення загальних операторів роботи з командним рядком, інтегрованого середовища розробки програм Microsoft VisualStudio, базових алгоритмів опрацювання даних, типів даних мови С++ та операції над ними, функції, структурні типи даних та їх використання; отримання навичок тестування і налагодження програм, розв'язання типових задач опрацювання даних.	КЗ 5	КФ 7 КФ 10 КФ 12	ПРН20 ПРН21 ПРН27
5.	ОК5	Фізика	**Мета**: сформувати у студентів уявлення про сучасну фізичну картину світу, надати знання про найбільш важливі принципи та закони, що визначають будову і найпростіші форми руху матерії, підготувавши тим самим їх до якісного вивчення загально технічних та спеціальних дисциплін. **Завдання**: вивчення основних закономірностей, методів та моделей для подальшого використання в дисциплінах спеціальності.	КЗ 1 КЗ 2 КЗ 4 КЗ 5	КФ 6 КФ 7	ПРН1 ПРН3 ПРН4 ПРН5
6.	ОК6	Комп'ютерна електроніка	**Мета**: сформувати у студентів уявлення про сучасну теорію електричних кіл і застосування системи теоретичних знань і практичних навичок , отриманих у процесі всього періоду навчання відповідно до вимог стандартів вищої освіти. **Завдання**: виконувати розрахунок стандартних цифрових вузлів (генераторів, формувачів імпульсів, допоміжних схем, тощо) з врахуванням особливостей елементної бази, що використовується; виконувати розрахунки усталеного та перехідного режиму в лінійному електричному колі, в якому діють джерела постійних, синусоїдальних або несинусоїдальних сигналів; виконувати розрахунки характеристик сигналів при проходженні їх через електричні кола, використовуючи спектральний метод аналізу.	КЗ 1 КЗ 3 КЗ 4 КЗ 5	КФ 6 КФ 7 КФ 12	ПРН1 ПРН2 ПРН4 ПРН6 ПРН17
7.	ОК7	Архітектура комп'ютерів	**Мета**: навчити студентів методам розроблення програм на мові асемблер на основі знань про архітектуру процесора **Завдання**: аналізувати інформацію про архітектуру процесорів для їх класифікації і виділення складових з метою розуміння можливостей процесорів при програмуванні на мові асемблер та розробленні операційних систем; застосовувати знання архітектури процесора, системи команд та режимів адресації для розроблення, налагодження та тестування програм; вміти оцінювати архітектуру для аргументованого вибору процесорів задля вирішення потрібних задач.	КЗ 1 КЗ 2 КЗ 4 КЗ 5	КФ 3 КФ 6 КФ 11 КФ 12	ПРН1 ПРН2 ПРН4 ПРН6 ПРН17
8.	ОК8	Системи технічного захисту інформації	**Мета**: діяльності на основі застосування системи теоретичних знань, практичних навичок обґрунтування, вибору та аналізу систем технічного захисту інформації.	КЗ 1 КЗ 2 КЗ 3	КФ 3 КФ 4 КФ 5	ПРН1,ПРН2 ПРН4,ПРН6 ПРН7 ПРН17

№ з/п	Код КОП	Назва компонента ОП	Мета та завдання компонента ОП	Формування компетентностей		Програмні результати навчання
				загальні	фахові	
			Завдання: здійснювати порівняльний аналіз систем технічного захисту інформації та оцінку їх ефективності; здійснювати розрахунок та вибір конкретних датчиків та мереж охорони, обмеження доступу, сигналізації.	КЗ 4 КЗ 5	КФ 7 КФ 11 КФ 12	ПРН36 ПРН37 ПРН38 ПРН40
9.	ОК9	Моделі та структури даних	**Мета**: здатність використання моделей та структур даних, а також аналізу та синтезу алгоритмів вирішення завдань кібербезпеки. **Завдання**: здійснювати вибір моделей та структур даних, а також аналізу та синтезу алгоритмів вирішення завдань кібербезпеки; здатність аналізувати і синтезувати алгоритми рішення задач кібербезпеки; застосовувати знання і розуміння для розв'язування задач вибору моделей та структур даних, синтезу та аналізу алгоритмів в сфері кібербезпеки; формувати уміння вирішувати проблеми та приймати рішення кількома способами	КЗ 1 КЗ 2 КЗ 4 КЗ 5	КФ 4 КФ 5 КФ 7 КФ 11 КФ 12	ПРН1 ПРН3 ПРН4
10.	ОК10	Комп'ютерна схемотехніка	**Мета**: навчити студентів аналізувати та розробляти різного рівня складності апаратні рішення обчислювальних (комп'ютерних) систем та їх модулів з використанням сучасних методів та засобів проектування, в тому числі з урахуванням сучасних викликів в галузі забезпечення кібербезпеки **Завдання**: володіти інформацією щодо існуючого стану речей в галузі розробки обчислювальних (комп'ютерних) систем; розробляти та визначати шляхи оптимізації проектних рішень за різними критеріями (швидкість обчислень, ресурсомісткість, захищеність даних з точки зору кібербезпеки тощо).	КЗ 1 КЗ 2 КЗ 4 КЗ 5	КФ 3 КФ 6 КФ 7 КФ 11	ПРН1 ПРН4 ПРН17
11.	ОК11	Апаратні та програмні засоби захисту інформації	**Мета**: діяльності на основі застосування системи теоретичних знань і практичних навичок, отриманих у процесі всього періоду навчання відповідно до вимог стандартів вищої освіти. **Завдання**: вивчення основних закономірностей, методів та моделей засоби захисту інформації; можливість їх використання щодо захисту інформації; реалізація сучасних крипто алгоритмів.	КЗ 1 КЗ 2 КЗ 3 КЗ 4 КЗ 5	КФ 3 КФ 4 КФ 5 КФ 7 КФ 10 КФ 11 КФ 12	ПРН1 ПРН2 ПРН3 ПРН4 ПРН10 ПРН14 ПРН15 ПРН16 ПРН17 ПРН18 ПРН20 ПРН50 ПРН51

№ з/п	Код КОП	Назва компонента ОП	Мета та завдання компонента ОП	Формування компетентностей		Програмні результати навчання
				загальні	фахові	
12.	ОК12	Операційні системи	**Мета**: надання студентам знання і навичок у галузі фундаментальних концепцій і практичних рішень, які є основою сучасних операційних систем, використання можливостей операційної системи; ознайомлення з функціями, структурою, принципами побудови, методами розробки, основами функціонування і використання операційних систем різного рівня складності і їх компонентів. **Завдання**: визначати способи і варіанти установки, конфігурування й налаштування операційних систем; використовувати принципи пошуку й усунення несправностей, конфліктів і збоїв в ОС та відновлення інформації; аналізувати можливості засобів діагностики, оптимізації й відновлення системи.	КЗ 1 КЗ 2 КЗ 3 КЗ 4 КЗ 5	КФ 4 КФ 6 КФ 7 КФ 11	ПРН1 ПРН3 ПРН6 ПРН14 ПРН25 ПРН49
13.	ОК13	Технології програмування (КП)	**Мета**: визначення рівня підготовленості студента до розв'язання комплексу сучасних наукових і прикладних завдань відповідно до технології програмування. **Завдання**: систематизація, закріплення і розширення теоретичних знань; розвиток навичок самостійної роботи, оволодіння методикою досліджень і експериментування використання сучасних інформаційних технологій у процесі розв'язання задач, які передбачені завданням на курсову роботу	КЗ 1 КЗ 2 КЗ 3 КЗ 4 КЗ 5	КФ 1 КФ 3 КФ 12	ПРН1,ПРН2 ПРН6,ПРН14 ПРН15 ПРН20 ПРН21 ПРН26 ПРН27
14.	ОК14	Теорія інформації та кодування	**Мета**: опанування навичок з розрахунку ентропії та інших характеристик простих дискретних систем інформації; кодування повідомлення за методами ефективного та перешкодостійкого кодування; побудови кодів стиснення інформації. **Завдання**: вивчення принципи оптимального і перешкодостійкого кодування; застосовувати методи та засоби перешкодостійкого кодування; застосувати базові принципи кодування інформації з метою її захисту від перетворень та несанкціонованого доступу в інформаційних і комунікаційних системах.	КЗ 1 КЗ 2 КЗ 4 КЗ 5	КФ 2 КФ 5 КФ 6 КФ 7	ПРН1 ПРН2 ПРН3 ПРН4 ПРН5 ПРН6 ПРН13 ПРН19
15.	ОК15	Інформаційно-комунікаційні системи	**Мета**: вивчення можливостей та технологій сучасних інформаційно-комунікаційні мереж (ІКМ), основ їх побудови, супроводу і адміністрування. **Завдання**: вивчення основних принципів побудови ІКМ; вивчення локальних ІКМ; вивчення мережевих архітектурних рішень; вивчення протоколів нижнього рівня ІКМ; вивчення питань проектування ІКМ; вивчення протоколів середнього і верхнього рівня ІКМ; вивчення способів адміністрування ІКМ.	КЗ 1 КЗ 2 КЗ 3 КЗ 4 КЗ 5	КФ 2 КФ 3	ПРН1,ПРН2 ПРН3,ПРН4 ПРН8,ПРН10 ПРН11,ПРН13 ПРН14,ПРН15 ПРН17,ПРН22 ПРН23,ПРН24 ПРН26,ПРН27 ПРН31,ПРН38 ПРН40,ПРН47

№ з/п	Код КОП	Назва компонента ОП	Мета та завдання компонента ОП	Формування компетентностей		Програмні результати навчання
				загальні	фахові	
16.	ОК16	Прикладна криптологія	**Мета**: володіння науковими методами обґрунтування, вибору та аналізу криптографічних алгоритмів і протоколів. **Завдання**: здійснювати порівняльний аналіз криптографічних алгоритмів та оцінку їх криптографічної стійкості; здійснювати розрахунок та вибір конкретних параметрів криптографічних алгоритмів і протоколів; використовувати спеціалізоване програмне забезпечення та розробляти на базі мов програмування високого рівня програмне забезпечення для вирішення задач криптозахисту даних	КЗ 1 КЗ 2 КЗ 3 КЗ 4 КЗ 5	КФ 1 КФ 4 КФ 7 КФ 10 КФ 12	ПРН1,ПРН2 ПРН3,ПРН6 ПРН7,ПРН8 ПРН9 ПРН13 ПРН19 ПРН22 ПРН47 ПРН48
17.	ОК17	Вбудовані системи	**Мета**: надбання студентами знань і навичок з проектування мікропроцесорних систем **Завдання**: володіти базовими навичками побудови сучасних мікропроцесорних систем на мікропроцесорах та мікроконтролерах; знати принципи функціонування та вміти використовувати сучасні мікросхеми постійних запам'ятовуючих приладів та оперативних запам'ятовуючих приладів; знати принципи функціонування та вміти використовувати сучасні мікросхеми інтерфейсів периферійних пристроїв.	КЗ 1 КЗ 2 КЗ 3 КЗ 4 КЗ 5	КФ 3 КФ 5 КФ 6 КФ 7 КФ 10 КФ 12	ПРН1 ПРН6 ПРН14
18.	ОК18	Web-технології	**Мета**: надбання студентами знань про Web-програмування; проектування архітектури front-end інтерфейсу і архитектури back-end частині веб-додатки; застосування типових шаблонів (патернів) при створенні програмних модулів; використанню засобів налагодження програмного коду веб-додатків. **Завдання**: вивчення способів розробки WEB-сторінок з використанням мови розмітки сторінок HTML, технології CSS; застосування знань з веб-програмування для правильного вибору мов і технологій в кожному конкретних проекті; аналізувати поставлену задачу і оптимально вибирати формати обміну між веб-сервісами.	КЗ 1 КЗ 2 КЗ 3 КЗ 4 КЗ 5	КФ 2 КФ 3 КФ 6 КФ 7	ПРН1 ПРН3 ПРН10 ПРН11 ПРН15
19.	ОК19	Програмування засобів штучного інтелекту на Python	**Мета**: надбання навичок з проектування та розробки програмного забезпечення. **Завдання**: отримання навичок програмування, тестування і налагодження програм, використовувати принципи об'єктно-орієнтованого програмування для вирішення практичних задач; роз'яснювати і представляти проекти / розробки програмного забезпечення замовникам; розпізнавати та використовувати на практиці інформацію з новітніх підходів до проектування та розробки програмного забезпечення	КЗ 2 КЗ 3 КЗ 5 КЗ 6	КФ 11 КФ 12	ПРН1 ПРН15 ПРН21 ПРН27

№ з/п	Код КОП	Назва компонента ОП	Мета та завдання компонента ОП	Формування компетентностей		Програмні результати навчання
				загальні	фахові	
20.	ОК20	Бази даних	**Мета**: надання слухачам знань, уміння, навичок та методичних прийомів, що необхідні для проектування сучасних баз даних (БД). **Завдання**: вивчення основних принципів побудови реляційних БД; вивчення архітектурних рішень і моделей систем управління БД (СУБД); вивчення реляційної моделі БД; вивчення основ проектування БД з використанням нормальних форм; вивчення основ створення БД з використанням СУБД MySQL	КЗ 1 КЗ 2 КЗ 3 КЗ 4 КЗ 5	КФ 4 КФ 7 КФ 10 КФ 11 КФ 12	ПРН1 ПРН2
21.	ОК21	Програмування систем IoT	**Мета**: надбання студентами знань і навичок з проектування мікропроцесорних систем захисту інформації, систем контролю доступом, систем аутентифікації. **Завдання**: Володіти базовими навичками побудови сучасних мікропроцесорних систем захисту інформації на мікропроцесорах та мікроконтролерах; здійснювати розрахунок та вибір конкретних пристроїв для виконання криптографічних алгоритмів і протоколів; використовувати спеціалізоване програмне забезпечення та розробляти системи аутентифікації особи для вирішення задач криптозахисту даних та побудови систем управління контролю доступом до об’єктів та інформації	КЗ 1 КЗ 2 КЗ 3 КЗ 4 КЗ 5	КФ 3 КФ 5 КФ 7 КФ 12	ПРН1
22.	ОК22	Прикладна криптологія (КП)	**Мета**: визначення рівня підготовленості студента до розв'язання комплексу сучасних наукових і прикладних завдань відповідно до прикладної криптології . **Завдання**: систематизація, закріплення і розширення теоретичних знань; розвиток навичок самостійної роботи, оволодіння методикою досліджень і експериментування використання сучасних інформаційних технологій у процесі розв'язання задач, які передбачені завданням на курсове проектування	КЗ 1 КЗ 2 КЗ 3 КЗ 4 КЗ 5	КФ 1 КФ 3 КФ 10 КФ 12	ПРН1 ПРН47 ПРН48
23.	ОК23	Нормативно-правове забезпечення інформаційної безпеки	**Мета**: здатність аналізувати сучасні стандарти та формувати загальні вимоги до інформаційної безпеки комп’ютерних систем і мереж. **Завдання**: знати систему міжнародних і національних стандартів у галузі кібербезпеки; знати структуру нормативно-правового забезпечення кібербезпеки інформаційно- комунікаційних систем і мереж організацій і підприємств; знати методику оцінювання інформаційної безпеки на відповідність вимогам стандартів.	КЗ 1 КЗ 2 КЗ 3 КЗ 4 КЗ 5	КФ 1 КФ 7 КФ 8 КФ 9 КФ 11 КФ 12	ПРН1,ПРН2 ПРН7,ПРН8 ПРН12,ПРН16 ПРН21,ПРН22 ПРН23,ПРН24 ПРН25,ПРН26 ПРН28,ПРН29 ПРН 37,ПРН38 ПРН40,ПРН42 ПРН43,ПРН44
24.	ОК24	Управління інформаційною безпекою	**Мета**: діяльності на основі застосування системи теоретичних знань і практичних навичок, з: формування комплексу засобів (правил, процедур, тощо) щодо управління інформаційною безпекою; застосування комплексного підходу з забезпечення інформаційної безпеки в різних сферах діяльності (критичні системи та додатки).	КЗ 1 КЗ 2 КЗ 3 КЗ 4 КЗ 5	КФ 1 КФ 2 КФ 3 КФ 4 КФ 7	ПРН1 ПРН2 ПРН3 ПРН4 ПРН5

№ з/п	Код КОП	Назва компонента ОП	Мета та завдання компонента ОП	Формування компетентностей		Програмні результати навчання
				загальні	фахові	
			Завдання: знати структуру нормативних актів та стандартів в сфері управління інформаційної безпекою; систему термінів та понять; організовувати основні процеси реалізації систем ІБ, а саме, планування, ризик-аналізу, вибору контрзаходів, тощо; вміти використовувати сучасні інформаційні технології при оцінювання ризиків критичної інфраструктури; визначати шляхи зниження ризиків, практично застосовувати методи забезпечення безпеки.	КЗ 7	КФ 8 КФ 9 КФ 11 КФ 12	ПРН7,ПРН8 ПРН9,ПРН21 ПРН22,ПРН23 ПРН24,ПРН25 ПРН26,ПРН 30 ПРН32,ПРН33 ПРН34,ПРН41 ПРН42,ПРН43 ПРН44,ПРН45 ПРН46,ПРН49 ПРН52
25.	ОК25	Захист інформації в інформаційно-комунікаційних системах (КП)	**Мета**: визначення рівня підготовленості студента до розв'язання комплексу сучасних наукових і прикладних завдань відповідно до захисту інформації в інформаційно-комунікаційних системах. **Завдання**: систематизація, закріплення і розширення теоретичних знань; розвиток навичок самостійної роботи, оволодіння методикою досліджень і експериментування використання сучасних інформаційних технологій у процесі розв'язання задач, які передбачені завданням на курсове проектування	КЗ 1 КЗ 2 КЗ 3 КЗ 4 КЗ 5	КФ 1 КФ 3 КФ 12	ПРН1,ПРН8 ПРН14 ПРН19 ПРН30 ПРН31 ПРН34 ПРН50 ПРН51
26.	ОК26	Надійність та функціональна безпека інформаційно-управляючих систем	**Мета**: здатність аналізувати надійність та функціональну безпеку типових компонентів та систем кібербезпеки та володіти навичками оцінювання та забезпечення показників надійності та безпеки відповідно до вимог. **Завдання**: знати основні поняття та показники та вимоги до надійності та функціональної безпеки систем кібербезпеки відповідно до міжнародних і національних стандартів; знати та застосувати методики та засоби аналізу та оцінювання надійності та функціональної безпеки систем кібербезпеки; знати та застосувати методики та засоби підвищення надійності та функціональної безпеки систем кібербезпеки з урахуванням ресурсних обмежень.	КЗ 1 КЗ 2 КЗ 3 КЗ 4 КЗ 5	КФ 1 КФ 2 КФ 3 КФ 4 КФ 6 КФ 7 КФ 12	ПРН1 ПРН3 ПРН4 ПРН5 ПРН7 ПРН8 ПРН14 ПРН19 ПРН30 ПРН32
27.	ОК27	Захист інформації в інформаційно-комунікаційних системах	**Мета**: здатність аналізувати методологію створення, основні напрями, методи, алгоритми реалізації функцій захисту інформації в інформаційно-комунікаційних системах, засоби забезпечення основних вимог інформаційної безпеки. **Завдання**: знати сучасні міжнародні та вітчизняні стандарти з інформаційної безпеки; знати загальні аспекти проблематики в галузі інформаційної безпеки, а також тенденції і перспективи створення механізмів захисту інформації та засобів подолання цих	КЗ 1 КЗ 2 КЗ 3 КЗ 4 КЗ 5	КФ 4 КФ 5 КФ 6 КФ 7 КФ 8 КФ 9 КФ 11 КФ 12	ПРН1,ПРН2 ПРН3,ПРН4 ПРН5,ПРН7 ПРН8,ПРН9 ПРН10 ПРН11 ПРН12 ПРН14 ПРН18

№ з/п	Код КОП	Назва компонента ОП	Мета та завдання компонента ОП	Формування компетентностей		Програмні результати навчання
				загальні	фахові	
			механізмів; розуміти властивостіі інформаційних ресурсів та технологій, як об'єктів кібербезпеки, та вміння здійснювати класифікацію загроз безпеці інформаційних ресурсів, класифікацію та ранжирування джерел загроз і уразливостей безпеці, застосовуючи системний підхід та знання основ теорії інформаційної безпеки; - розуміти принципи і методи теорії захищених систем, основних механізми захисту, які реалізовані в сучасних операційних системах та системах управління базами даних, видів і прийомів використання шкідливого програмного забезпечення та методів його нейтралізації.			ПРН19 ПРН20 ПРН27 ПРН31 ПРН34 ПРН50 ПРН51 ПРН53
28.	ОК28	Комплексні системи захисту інформації: проектування, впровадження, супровід	**Мета**: діяльності на основі застосування системи теоретичних знань і практичних навичок з виявлення способів порушення інформаційної безпеки при роботі комп'ютерних систем обробки інформації; вирішення задач захисту програм та даних програмно-апаратними засобами; застосування системного підходу до забезпечення інформаційної безпеки, включаючи комплекс організаційних заходів. **Завдання**: застосовувати знання до вирішення задач інформаційної безпеки; обирати потрібні організаційні та інженерно-технічні заходи, засоби і методи захисту інформації; аналізувати вхідні данні та обирати методи оцінки якості систем та моделей	КЗ 1 КЗ 2 КЗ 3 КЗ 4 КЗ 5	КФ 4 КФ 5 КФ 6 КФ 7 КФ 8 КФ 9 КФ 10 КФ 11 КФ 12	ПРН1,ПРН2 ПРН3,ПРН4 ПРН5,ПРН6 ПРН7,ПРН8 ПРН9,ПРН10 ПРН12,ПРН13 ПРН14,ПРН16 ПРН17,ПРН19 ПРН21,ПРН23 ПРН24,ПРН26 ПРН29,ПРН30 ПРН 31,ПРН33 ПРН34,ПРН35
29.	ОК29	Тестування та забезпечення якості	**Мета**: діяльність на основі застосування системи теоретичних знань і практичних навичок, щодо використання сучасних методів тестування та забезпечення якості інформаційно-комунікаційних системах. **Завдання**: оволодіти основами сучасних технологій тестування програмного та технічного забезпечення інформаційно-комунікаційних систем; методами їх використання; знати склад та основні принципи роботи мережного обладнання; розробляти конфігурації мережного обладнання з метою забезпечення якості системи; використовувати принципи пошуку й усунення несправностей для вирішення практичних задач.	КЗ 1 КЗ 2 КЗ 3 КЗ 4 КЗ 5	КФ 2 КФ 3	ПРН1 ПРН5 ПРН8 ПРН9 ПРН10 ПРН14 ПРН20 ПРН28 ПРН29
30.	ОК30	Навчальна практика	**Мета**: підготовка спеціалістів з кібербезпеки до виконання робіт з розроблення програмного забезпечення щодо захисту інформації з використанням принципів та методів об'єктно-орієнтованого програмування. **Завдання**: вивчення засобів розробки програмного продукту щодо забезпечення кібербезпеки під керівництвом ОС Windows з	КЗ 1 КЗ 2 КЗ 4 КЗ 5	КФ 1 КФ 3 КФ 5 КФ 12	ПРН1 ПРН2 ПРН3 ПРН5 ПРН6

№ з/п	Код КОП	Назва компонента ОП	Мета та завдання компонента ОП	Формування компетентностей		Програмні результати навчання
				загальні	фахові	
			широким використанням можливостей об'єктно-орієнтованого програмування, правила будування програмних засобів в середовищах візуального програмування та відлагодження налаштувань Windows.			ПРН17
31.	ОК31	Ознайомча практика	**Мета**: ознайомлення студентів зі специфікою майбутнього фаху, отримання ними первинних професійних умінь і навичок, а також відповідної робітничої професії. **Завдання**: закріплення знань, які одержано студентами в процесі навчання; знайомство з місцем практичної підготовки; знайомство з умовами праці; адаптація до умов роботи організації; знайомство з організацією праці та управління; розвиток у студентів практичних навичок й послідовне їх закріплення для реальної взаємодії з робочим оточенням, в яке він потрапить після закінчення навчання в учбовому закладі; налагоджування зв'язків, уміння адаптуватися із зовнішнім, не завжди звичним робочим оточенням; підвищення рівня практичної та загальної підготовки спеціалістів.	КЗ 1 КЗ 2 КЗ 4 КЗ 5	КФ 1 КФ 3 КФ 12	ПРН1,ПРН2 ПРН3,ПРН4 ПРН6,ПРН8 ПРН14,ПРН15 ПРН16,ПРН17 ПРН18,ПРН36 ПРН37 ПРН38 ПРН40 ПРН49 ПРН50 ПРН51
32.	ОК32	Виробнича практика	**Мета**: використовувати знання зі створення комп'ютерних систем методами комп'ютерних наук в практиці проектування комп'ютерних систем на виробництві. **Завдання**: отримати навички та уміння при створенні комп'ютерних систем обробки інформації та управління на реальних підприємствах.	КЗ 1 КЗ 2 КЗ 3 КЗ 4 КЗ 5	КФ 1 КФ 3 КФ 5 КФ 12	ПРН1,ПРН2 ПРН3,ПРН4 ПРН6,ПРН7 ПРН8,ПРН9 ПРН11,ПРН13 ПРН15,ПРН19 ПРН22,ПРН31 ПРН38,ПРН40 ПРН47,ПРН50 ПРН51
33.	ОК33	Кваліфікаційна робота бакалавра	**Мета**: визначення рівня підготовленості студента до розв'язання комплексу сучасних наукових і прикладних завдань відповідно до узагальненого об'єкта діяльності на основі застосування системи теоретичних знань і практичних навичок, отриманих у процесі всього періоду навчання відповідно до вимог стандартів вищої освіти. **Завдання**: систематизація, закріплення і розширення теоретичних знань, отриманих у процесі навчання за освітньо-професійною програмою підготовки фахівця певного освітнього ступеня, і їх практичне використання при вирішенні конкретних наукових, прикладних, інженерних, економіко-соціальних і виробничих питань у певній галузі професійної діяльності; розвиток навичок самостійної роботи, оволодіння методикою досліджень і експериментування, фізичного або математичного моделювання, використання сучасних інформаційних технологій у процесі	КЗ 1 КЗ 2 КЗ 3 КЗ 4 КЗ 5 КЗ 6 КЗ 7	КФ 1 КФ 2 КФ 3 КФ 4 КФ 5 КФ 6 КФ 7 КФ 8 КФ 9 КФ 10 КФ 11 КФ 12	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

№ з/п	Код КОП	Назва компонента ОП	Мета та завдання компонента ОП	Формування компетентностей		Програмні результати навчання
				загальні	фахові	
			розв'язання задач, які передбачені завданням на дипломне проектування; визначення відповідності рівня підготовки випускника вимогам освітніх ступенів характеристики фахівця, його готовності та спроможності до самостійної роботи в умовах ринкової економіки, сучасного виробництва, прогресу науки, техніки і культури.			ПРН31,ПРН32 ПРН33,ПРН34 ПРН35,ПРН36 ПРН37,ПРН38 ПРН39,ПРН40 ПРН41,ПРН42 ПРН43,ПРН44 ПРН45,ПРН46 ПРН47,ПРН48 ПРН49,ПРН50 ПРН51,ПРН52 ПРН53,ПРН54

Вибіркові компоненти, їх зміст, формування компетентностей (фахових, спеціальних) та визначення програмних результатів навчання представлено у робочих програмах дисциплін та силабусах на сайті в розділі «Короткий опис, структура і освітні компоненти освітніх програми і компонентів» освітньо-професійної програми «Безпека інформаційних і комунікаційних систем» спеціальності 125 «Кібербезпека».

4 ФОРМА АТЕСТАЦІЇ ЗДОБУВАЧІВ ВИЩОЇ ОСВІТИ

Атестація випускників за освітньо-професійною програмою «Безпека інформаційних і комунікаційних систем» за спеціальністю 125 «Кібербезпека» проводиться у формі захисту кваліфікаційної роботи бакалавра та завершується видачою документу встановленого зразка про присудження йому ступеня бакалавра із присвоєнням освітньої кваліфікації: Бакалавр з кібербезпеки галузі знань інформаційні технології.

Атестація здійснюється відкрито і публічно.

5. МАТРИЦЯ ВІДПОВІДНОСТІ ПРОГРАМНИХ КОМПЕТЕНТНОСТЕЙ КОМПОНЕНТАМ ОСВІТНЬО-ПРОФЕСІЙНОЇ ПРОГРАМИ

КОП	Програмні компетентності																		
	К31	К32	К33	К34	К35	К36	К37	КФ1	КФ2	КФ3	КФ4	КФ5	КФ6	КФ7	КФ8	КФ9	КФ10	КФ11	КФ12
ОК 1	+	+		+	+				+					+			+		+
ОК 2	+	+		+	+				+				+	+			+		+
ОК 3			+										+					+	+
ОК 4	+	+	+	+	+				+	+		+	+	+			+		+
ОК 5	+	+		+	+								+	+					
ОК 6	+		+	+	+								+	+					+
ОК 7	+	+		+	+					+			+					+	+
ОК 8	+	+	+	+	+					+	+	+		+				+	+
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	+	+	+	+	+			+		+		+							+
ОК33	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+

6. МАТРИЦЯ ВІДПОВІДНОСТІ ПРОГРАМНИХ РЕЗУЛЬТАТІВ НАВЧАННЯ (ПРН) ВІДПОВІДНИМИ КОМПОНЕНТАМИ ОСВІТНЬО-ПРОФЕСІЙНОЇ ПРОГРАМИ

КОП	Програмні результати навчання																										
	ПРН1	ПРН 2	ПРН 3	ПРН 4	ПРН 5	ПРН 6	ПРН 7	ПРН 8	ПРН 9	ПРН 10	ПРН 11	ПРН 12	ПРН 13	ПРН 14	ПРН 15	ПРН 16	ПРН 17	ПРН 18	ПРН 19	ПРН 20	ПРН 21	ПРН 22	ПРН 23	ПРН 24	ПРН 25	ПРН 26	ПРН 27
ОК 1	+	+	+	+	+																						
ОК 2	+		+	+	+						+																
ОК 3	+	+	+		+	+																					
ОК 4	+				+									+	+					+	+						+
ОК 5	+		+	+	+																						
ОК 6	+	+		+		+											+										
ОК 7	+	+		+		+											+										
ОК 8	+	+		+		+		+									+										
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	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+

КОП	ПРН 28	ПРН 29	ПРН 30	ПРН 31	ПРН 32	ПРН 33	ПРН 34	ПРН 35	ПРН 36	ПРН 37	ПРН 38	ПРН 40	ПРН 41	ПРН 42	ПРН 43	ПРН 44	ПРН 45	ПРН 46	ПРН 47	ПРН 48	ПРН 49	ПРН 50	ПРН 51	ПРН 52	ПРН 53	ПРН 54
ОК 1																										
ОК 2																										
ОК 3																										
ОК 4																										
ОК 5																										
ОК 6																										
ОК 7																										
ОК 8									+	+	+	+														
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	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+

Додаток А

СТРУКТУРНО-ЛОГІЧНА СХЕМА ОСВІТНЬО-ПРОФЕСІЙНОЇ ПРОГРАМИ

Код КОП	Назва компонента ОП
I семестр	
ОК1	Вища математика
ОК2	Дискретна математика
ОК3	Основи функціонування комп'ютерів
ОК4	Технології програмування
ВК2	*Українські студії*
ВК3	*Мовні компетентності (іноземна мова)*
ВК5	*Гуманітарна або економічна дисципліна за вибором*
II семестр	
ОК1	Вища математика
ОК2	Дискретна математика
ОК4	Технології програмування
ОК5	Фізика
ОК6	Комп'ютерна електроніка
ОК30	Навчальна практика
ВК1	*Правова компетентність*
ВК3	*Мовні компетентності (іноземна мова)*

Код КОП	Назва компонента ОП
III семестр	
ОК1	Вища математика Теорія ймовірностей та математична статистика
ОК4	Технології програмування
ОК7	Архітектура комп'ютерів
ОК8	Системи технічного захисту інформації
ОК9	Моделі та структури даних
ОК10	Комп'ютерна схемотехніка
ВК6	*Компетентності, спрямовані на формування системного наукового світогляду*
IV семестр	
ОК4	Технології програмування
ОК8	Системи технічного захисту інформації
ОК11	Апаратні та програмні засоби захисту інформації
ОК12	Операційні системи
ОК13	Технології програмування (КП)
ОК31	Ознайомча практика
ВК4	*Математично-технічний блок на вибір*
ВК7	*Компетентності загального культурного кругозору та розвитку комунікацій*

Код КОП	Назва компонента ОП
V семестр	
ОК14	Теорія інформації та кодування
ОК15	Інформаційно-комунікаційні системи
ОК16	Прикладна криптологія
ОК17	Вбудовані системи
ОК18	Web-технології
ОК19	Програмування засобів штучного інтелекту на Python
ВК8	*Minor. Дисципліна 1*
VI семестр	
ОК16	Прикладна криптологія
ОК20	Бази даних
ОК21	Програмування систем IoT
ОК22	Прикладна криптологія (КП)
ОК27	Виробнича практика
ОК33	Нормативно-правове забезпечення інформаційної безпеки
ВК9	*Minor. Дисципліна 2*
ВК12	*Дисципліна індивідуального вибору 1*

Код КОП	Назва компонента ОП
VII семестр	
ОК24	Управління інформаційною безпекою
ОК25	Захист інформації в інформаційно-комунікаційних системах (КП).
ОК26	Надійність та функціональна безпека інформаційно-управляючих систем
ОК27	Захист інформації в інформаційно-комунікаційних системах .
ОК28	Комплексні системи захисту інформації: проектування, впровадження, супровід
ВК10	*Minor. Дисципліна 3*
ВК13	*Дисципліна індивідуального вибору 2*
VIII семестр	
ОК27	Захист інформації в інформаційно-комунікаційних системах
ОК28	Комплексні системи захисту інформації: проектування, впровадження, супровід
ОК29	Тестування та забезпечення якості
ВК11	Minor. Дисципліна 4
ВК14	Дисципліна індивідуального вибору 3
ОК33	**Кваліфікаційна робота бакалавра (атестація)**

Таблиця входів/виходів структурно-логічної схеми освітньо-професійної програми

Код КОП	Компоненти освітньої програми	Входи	Виходи
1	2	3	4
ОК1	Вища математика		Для усіх дисциплін
ОК2	Дискретна математика		ОК4, ОК6, ОК7, ОК8, ОК9, ОК10, ОК12, ОК14, ОК15, ОК20, ОК25, ОК27, ОК33, ВК4
ОК3	Основи функціонування комп'ютерів		ОК6, ОК7, ОК8, ОК10, ОК11, ОК17, ОК30
ОК4	Технології програмування	ОК2	ОК9, ОК11, ОК12, ОК13, ОК16, ОК18, ОК21, ОК31, ОК33
ОК5	Фізика		ОК8, ОК11, ОК15, ОК17, ОК25, ОК27, ОК28, ОК33
ОК6	Комп'ютерна електроніка	ОК2, ОК3	ОК7, ОК8, ОК10, ОК17, ОК30, ОК33
ОК7	Архітектура комп’ютерів	ОК2, ОК3, ОК6	ОК11, ОК17, ОК21, ОК25, ОК 26, ОК31, ОК33
ОК8	Системи технічного захисту інформації	ОК2, ОК3, ОК5	ОК11, ОК17, ОК21, ОК25, ОК26, ОК27, ОК31, ОК33
ОК9	Моделі та структури даних	ОК2	ОК12, ОК20, ОК21, ОК25, ОК27, ОК33
ОК10	Комп'ютерна схемотехніка	ОК2, ОК3, ОК6	ОК11, ОК17, ОК21, ОК31, ОК33
ОК11	Апаратні та програмні засоби захисту інформації	ОК3, ОК4, ОК5, ОК7, ОК7, ОК8, ОК10	ОК12, ОК15, ОК17, ОК18, ОК20, ОК25, ОК27. ОК28. ОК33
ОК12	Операційні системи	ОК2, ОК4, ОК9, ОК11	ОК15, ОК17, ОК18, ОК20, ОК24, ОК25, ОК27, ОК31, ОК33
ОК13	Технології програмування (КП)	ОК4	ОК16, ОК18, ОК21, ОК31, ОК33
ОК14	Теорія інформації та кодування	ОК2	ОК15, ОК25, ОК27, ОК33
ОК15	Інформаційно-комунікаційні системи	ОК2, ОК5, ОК11, ОК12, ОК14	ОК18, ОК25, ОК27, ОК28, ОК32, ОК33
ОК16	Прикладна криптологія	ОК4, ОК13, ОК19	ОК22, ОК25, ОК27, ОК32, ОК33
ОК17	Вбудовані системи	ОК3, ОК5, ОК6, ОК8, ОК10, ОК11, ОК12	ОК26, ОК27, ОК28, ОК33
ОК17	Web-технології	ОК4, ОК11, ОК12, ОК13, ОК15	ОК21, ОК25, ОК27, ОК28, ОК29, ОК33.
ОК19	Програмування засобів штучного інтелекту на Python		ОК16, ОК21, ОК22, ОК29, ОК33
ОК20	Бази даних	ОК2, ОК9, ОК11, ОК12	ОК24, ОК25, ОК26, ОК27, ОК29, ОК 32, ОК33
ОК21	Програмування систем IoT	ОК4, ОК7, ОК8, О,К9, ОК10, ОК13, ОК17, ОК19	ОК27, ОК28, ОК32, ОК33
ОК22	Прикладна криптологія (КП)	ОК16	ОК25, ОК27, ОК28, ОК32, ОК33
ОК23	Нормативно-правове забезпечення інформаційної безпеки		ОК24, ОК25, ОК26, ОК27, ОК28, ОК29, ОК33
ОК24	Управління інформаційною безпекою	ОК12, ОК23	ОК25, ОК26, ОК27, ОК28, ОК33.
ОК25	Захист інформації в інформаційно-комунікаційних системах (КП)	ОК2, ОК5, ОК7, ОК8, ОК9, ОК11, ОК12, ОК14, ОК15, ОК16, ОК17, ОК21, ОК22, ОК23, ОК24	ОК33

Код КОП	Компоненти освітньої програми	Входи	Виходи
1	2	3	4
ОК26	Надійність та функціональна безпека інформаційно-управляючих систем	ОК7, ОК8, ОК17, ОК23, ОК24	ОК33
ОК27	Захист інформації в інформаційно-комунікаційних системах	ОК2, ОК5, ОК8, ОК9, ОК11, ОК12, ОК14, ОК15, ОК16, ОК17, ОК19, ОК20, ОК21, ОК22, ОК23, ОК24	ОК33
ОК28	Комплексні системи захисту інформації: проектування, впровадження, супровід	ОК5, ОК11, ОК15, ОК17, ОК20, ОК21, ОК22, ОК23, ОК24	ОК33
ОК29	Тестування та забезпечення якості	ОК17, ОК23	ОК33
ОК30	Навчальна практика	ОК3, ОК6	ОК4, ОК33.
ОК31	Ознайомча практика	ОК4, ОК7, ОК8, ОК10, ОК12, ОК13	
ОК32	Виробнича практика	ОК15, ОК16, ОК19, ОК20, ОК21, ОК22	
ОК33	Кваліфікаційна робота бакалавра	З усіх дисциплін	
ВК1	Правова компетентність		Для усіх дисциплін
ВК2	Українські студії		Для усіх дисциплін
ВК3	Мовні компетентності (іноземна мова)		Для усіх дисциплін
ВК4	Математично-технічний блок на вибір	ОК2	Для усіх дисциплін
ВК5	Гуманітарна або економічна дисципліна за вибором		Для усіх дисциплін
ВК6	Компетентності, спрямовані на формування системного наукового світогляду		Для усіх дисциплін
ВК7	Компетентності загального культурного кругозору та розвитку комунікацій		Для усіх дисциплін

ЛИСТ ОБЛІКУ ВНЕСЕННЯ ЗМІН

Номер зміни	Дата введення в дію	Пояснення до змін
1.	01 вересня 2022 р.	Затвердити оновлення змісту опису освітньо-професійної програми «Безпека інформаційних і комунікаційних систем» спеціальності 125 «Кібербезпека» першого (бакалаврського) рівня вищої освіти, для здобувачів усіх курсів та форм навчання, які на ній навчаються (Додаток А). Підстава: наказ МОН України від 13.01.2022, № 26 «Про внесення змін до деяких стандартів вищої освіти»; протокол засідання Вченої ради № 8 від 20.04.2022 року; Положення про організацію освітнього процесу (п.8.2); Положення про розроблення та модернізацію освітніх програм (п.5.1)
2.	01 вересня 2023 р.	Затвердити оновлену модернізовану освітньо-професійну програму «Безпека інформаційних і комунікаційних систем» спеціальності 125 «Кібербезпека» першого (бакалаврського) рівня вищої освіти, для здобувачів усіх курсів та форм навчання, які на ній навчаються у зв'язку з модернізацією структури освітньої програми. (Додаток Б) Підстава: Протокол засідання Вченої ради № 11 від 22.06.2023 року; Положення про організацію освітнього процесу (п.8.2); Положення про розроблення та модернізацію освітніх програм (п.5.1) Пропозиції та рекомендації експертної групи та Галузевої експертної ради Національного агентства із забезпечення якості освіти з подальшого удосконалення освітньої програми після проходження нею акредитаційної експертизи.

ДОДАТОК А

Затверджені зміни у освітньо-професійній програмі «Безпека інформаційних і комунікаційних систем» спеціальності 125 «Кібербезпека» першого (бакалаврського) рівня вищої освіти у такій редакції:

3 – Характеристика освітньо-професійної програми	
Оцінювання	Письмові іспити, звіти з практик, презентації, поточний (модульний) контроль, кваліфікаційна робота (дипломний проект) бакалавра та її захист, атестаційний екзамен.

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

3.1 Перелік компонент ОП (доповнити)

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			
ОК34	Атестаційний екзамен	0	атестація

3.3 Структура навчального плану за семестрами та зміст компонентів ОП (доповнити)

Код КОП	Назва компонента ОП	Мета та завдання компонента ОП	Формування компетентностей	
			загальні	фахові
ОК34	Атестаційний екзамен	**Мета:** контроль та оцінка рівня знань, отриманих в процесі вивчення певного переліку теоретичних дисциплін, практичних навичок, відпрацювання вмінь і навичок з спеціальності та готовності працювати за фахом відповідно до програмних результати навчання. **Завдання:** визначення ступеня сформованості компетентностей та результатів навчання здобувача вищої освіти першого (бакалаврського) рівня вищої освіти	Згідно з ст. 6 Закону України «Про вищу освіту»: «Атестація – це встановлення відповідності результатів навчання здобувачів вищої освіти вимогам освітньої програми»	

4 ФОРМА АТЕСТАЦІЇ ЗДОБУВАЧІВ ВИЩОЇ ОСВІТИ

Атестація випускників за освітньо-професійною програмою «Безпека інформаційних і комунікаційних систем» за спеціальністю 125 «Кібербезпека» проводиться у формі захисту кваліфікаційної роботи бакалавра й атестаційного екзамену та завершується видачою документу встановленого зразка про присудження йому ступеня бакалавра із присвоєнням освітньої кваліфікації: Бакалавр з кібербезпеки галузі знань інформаційні технології.

Атестація здійснюється відкрито і публічно.

5 МАТРИЦЯ ВІДПОВІДНОСТІ ПРОГРАМНИХ КОМПЕТЕНТНОСТЕЙ КОМПОНЕНТАМ ОСВІТНЬО-ПРОФЕСІЙНОЇ ПРОГРАМИ

Доповнити

Примітка.

1. Матриця відображає набуття компетентностей через освітні компоненти.
2. Компонент «ОК34. Атестаційний екзамен», який належить до атестаційної процедури, відсутній в Матриці. Згідно з ст. 6 Закону України «Про вищу освіту»: «Атестація – це встановлення відповідності результатів навчання здобувачів вищої освіти вимогам освітньої програми».

6 МАТРИЦЯ ВІДПОВІДНОСТІ ПРОГРАМНИХ РЕЗУЛЬТАТІВ НАВЧАННЯ (ПРН) ВІДПОВІДНИМИ КОМПОНЕНТАМИ ОСВІТНЬО-ПРОФЕСІЙНОЇ ПРОГРАМИ

Примітка.

1. Матриця відображає набуття програмних результатів через освітні компоненти.
2. Компонент «ОК34. Атестаційний екзамен», який належить до атестаційної процедури, відсутній в Матриці. Згідно з ст. 6 Закону України «Про вищу освіту»: «Атестація – це встановлення відповідності результатів навчання здобувачів вищої освіти вимогам освітньої програми».

СТРУКТУРНО-ЛОГІЧНА СХЕМА ОСВІТНЬО-ПРОФЕСІЙНОЇ ПРОГРАМИ (доповнити)

Код КОП	Назва компонента ОП
VIII семестр	
ОК34	Атестаційний екзамен (атестація)

ДОДАТОК Б

Затверджені зміни

у освітньо-професійній програмі «Безпека інформаційних і комунікаційних систем» спеціальності 125 «Кібербезпека» першого (бакалаврського) рівня вищої освіти викладено у такій редакції:

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

Ввести зміни та вважати:

1 – Загальна інформація	
Наявність акредитації	Сертифікат про акредитацію освітньої програми: 0, виданий 25.04.2023 р. на підставі рішення Національного агентства із забезпечення якості освіти (протокол № 6 від 25.04.2023 р.) Період акредитації: до 25.04.2024 р.

3 ПЕРЕЛІК КОМПОНЕНТІВ ОСВІТНЬО-ПРОФЕСІЙНОЇ ПРОГРАМИ ТА ЇХ ЛОГІЧНА ПОСЛІДОВНІСТЬ

3.1. Перелік компонент ОП*

Ввести зміни в ОК24, ОК27, ВК13, ВК14 та вважати:

Код КОП	**Компоненти освітньо-професійної програми (навчальні дисципліни, курсові проекти (роботи), практики, атестація (кваліфікаційна робота, атестаційний іспит)**	**Кількість кредитів**	**Форма підсумкового контролю**	**Семестр**
1	**2**	**3**	**4**	**5**
1. Обов'язкові компоненти ОПП				
ОК27	Захист інформації в інформаційно-комунікаційних системах	4,5	іспит	7
ОК29	Управління інформаційною безпекою	4,5	залік	8
ВК13	Дисципліна індивідуального вибору 2	4,5	іспит	7
ВК14	Дисципліна індивідуального вибору 3	4,5	іспит	8
Загальний обсяг обов'язкових компонент:		**180**		
Загальний обсяг вибіркових компонент:		**60**		

*Зміни внесено у виконання Розділу ІІІ. «Обсяг кредитів ЄКТС, необхідний для здобуття відповідного ступеня вищої освіти» Стандарту вищої освіти за спеціальністю 125 «Кібербезпека» першого (бакалаврського) рівня вищої освіти (наказ МОН України від 04.10.2018 р., № 1074 (зі змінами)) у вимогі: мінімум 75% обсягу освітньої програми має бути спрямовано на забезпечення загальних та спеціальних (фахових) компетентностей за спеціальністю визначеною стандартом вищої освіти.

6. МАТРИЦЯ ВІДПОВІДНОСТІ ПРОГРАМНИХ РЕЗУЛЬТАТІВ НАВЧАННЯ (ПРН) ВІДПОВІДНИМИ КОМПОНЕНТАМИ ОСВІТНЬО-ПРОФЕСІЙНОЇ ПРОГРАМИ

Ввести зміни та вважати:

КОП	Програмні результати навчання																										
	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
ОК 21	+		+							+	+				+												

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» 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»
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»

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» 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.