(Ф 03.02 – 107)

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

Національний авіаційний університет

ОСВІТНЬО – ПРОФЕСІЙНА ПРОГРАМА

«Системи технічного захисту інформації, автоматизація її обробки»
(найменування освітньо-професійної програми)

Першого (бакалаврського) рівня вищої освіти

за спеціальністю 125 Кібербезпека
(шифр та найменування спеціальності)

галузі знань 12 Інформаційні технології
(шифр та найменування галузі)

СМЯ НАУ ОПП 09.01.10 – 01 – 2021

Освітньо-професійна програма
затверджена Вченою радою Університету
Протокол № 4 від 21.04.2021 р.

Вводиться в дію наказом ректора
Ректор
М. Нижник
Наказ № 246/од від 29.04.2021 р.

КИЇВ

Стандарт вищої освіти України: перший (бакалаврський) рівень
галузь знань 12 «Інформаційні технології»
спеціальність 125 «Кібербезпека»
Стандарт вищої освіти затверджено і введено в дію наказом Міністерства освіти і науки України від «04» жовтня 2018 р. № 1074

ЛИСТ ПОГОДЖЕННЯ
освітньо-професійної програми

ПОГОДЖЕНО

Науково-методичною радою
Національного авіаційного університету
протокол № 3
від «20» 04 2021 р.
Голова Науково-методичної ради
проректор з навчальної роботи
_____ А. Полухін

ПОГОДЖЕНО

Вченою радою Факультету кібербезпеки, комп'ютерної та програмної інженерії
протокол № 5
від «15» квітня 2021 р.
Голова Вченої ради факультету
_____ К. Нестеренко

ПОГОДЖЕНО

Кафедрою засобів захисту інформації
протокол засідання № 8
від «14» квітня 2021 р.
Завідувач кафедри
_____ В. Козловський

ПОГОДЖЕНО

Студентською радою Факультету кібербезпеки, комп'ютерної та програмної інженерії
протокол № 214-а-ЗЗ
від «14» квітня 2021 р.
Голова студентською ради
_____ В. Прощаваєв

ПЕРЕДМОВА

РОЗРОБЛЕНО РОБОЧОЮ ГРУПОЮ ОСВІТНЬО-ПРОФЕСІЙНОЇ ПРОГРАМИ (спеціальності 125 «Кібербезпека») у складі:

ГАРАНТ ОСВІТНЬОЇ ПРОГРАМИ:

ТЕМНІКОВ В.О. – д.т.н., доцент, професор кафедри засобів захисту інформації Факультету кібербезпеки, комп'ютерної та програмної інженерії

(підпис)

ЧЛЕНИ РОБОЧОЇ ГРУПИ:

КОЗЛОВСЬКИЙ В.В. – д.т.н., професор, завідувач кафедри засобів захисту інформації Факультету кібербезпеки, комп'ютерної та програмної інженерії

(підпис)

ЛАЗАРЕНКО С.В. – д.т.н., доцент, професор кафедри засобів захисту інформації Факультету кібербезпеки, комп'ютерної та програмної інженерії

(підпис)

ШВЕЦЬ В.А. – к.т.н., доцент, доцент кафедри засобів захисту інформації Факультету кібербезпеки, комп'ютерної та програмної інженерії

(підпис)

МАРТИНЮК Г.В. – (к.т.н., доцент, доцент кафедри засобів захисту інформації Факультету кібербезпеки, комп'ютерної та програмної інженерії)

(підпис)

Федченко Єлизавета Сергіївна

(П.І.Б. здобувача вищої освіти)

(підпис здобувача вищої освіти)

ЗОВНІШНІ СТЕЙКХОЛДЕРИ

Савченко В.А. – д.т.н., професор, директор Навчально-наукового інституту захисту інформації Державного університету телекомунікацій

(підпис)

Рецензії, відгуки зовнішніх стейкхолдерів (додаються).

Рівень документа – 3б
Плановий термін між ревізіями – 1 рік
Контрольний примірник

1. Профіль освітньо-професійної програми

Розділ 1. Загальна інформація		
1.1.	Повна назва закладу вищої освіти та структурного підрозділу	Національний авіаційний університет Факультет кібербезпеки, комп'ютерної та програмної інженерії Кафедра засобів захисту інформації
1.2.	Ступінь вищої освіти та назва кваліфікації мовою оригіналу	Бакалавр, Бакалавр з кібербезпеки
1.3.	Офіційна назва освітньо-професійної програми та спеціалізації (за наявності)	Системи технічного захисту інформації, автоматизація її обробки
1.4.	Тип диплому та обсяг освітньо-професійної програми	Диплом бакалавра, одиничний, 240 кредитів ЄКТС, термін навчання 3 роки 10 місяців (денна форма навчання) / 4 роки 6 місяців (заочна форма навчання)
1.5.	Акредитаційна інституція	Міністерство освіти і науки України, рішення Акредитаційної комісії від 31.10.2017 сертифікат серія НД № 1193809
1.6.	Період акредитації	До 01.07.2027 р., чергова
1.7.	Цикл/рівень	6 рівень Національної рамки кваліфікацій України (НРК України), перший цикл Європейського простору вищої освіти (FQ-EHEA), 6 рівень Європейської рамки кваліфікацій для навчання впродовж життя (EQF-LLL).
1.8.	Передумови	Вступ на навчання на освітню програму обсягом 240 кредитів ЄКТС здійснюється на базі повної загальної середньої освіти при наявності атестату. Для здобуття освітнього ступеня бакалавра на базі ступеня «молодший бакалавр» (освітньо-кваліфікаційного рівня «молодший спеціаліст») заклад вищої освіти має право визнати та перезарахувати не більше ніж 120 кредитів ЄКТС, отриманих в межах попередньої освітньої програми підготовки молодшого бакалавра (молодшого спеціаліста), а також навчання осіб, які мають диплом про вищу освіту (ОС бакалавр, ОКР спеціаліст, ОС магістр) за будь-якою іншою спеціальністю, якщо академічна різниця із змістом попередньої освіти не перевищує 30 кредитів. Умови вступу визначаються Правилами прийому до НАУ, затвердженими вченою радою Університету.
1.9.	Форма навчання	Інституційна з елементами дистанційної: очна, заочна, мережева.

1.10.	Мова(и) викладання	Українська
1.11.	Інтернет-адреса постійного розміщення опису освітньо-професійної програми	http://www.nau.edu.ua http://www.kzzi.nau.edu.ua
Розділ 2. Ціль освітньо-професійної програми		
2.1.	Ціллю ОПП «Системи технічного захисту інформації, автоматизація її обробки» є підготовка кваліфікованих фахівців, які володіють сучасними загально-науковими й спеціальними знаннями та технологіями інформаційної та/або кібербезпеки, здатних використовувати і впроваджувати технології інформаційної та/або кібербезпеки. Опанування специфічних знань особливостей професійної діяльності в авіаційному секторі, застосування яких дозволяє вирішувати практичні завдання підвищення рівня безпеки в авіації. ОПП «Системи технічного захисту інформації, автоматизація її обробки» відповідає місії НАУ, у якій наголошується, щодо внеску НАУ у розвиток суспільства на національному та міжнародному рівнях через генерацію нових знань та інноваційних ідей на основі інтеграції та інтернаціоналізації освіти, досліджень і практики, так і надання високоякісних освітніх та науково-дослідних послуг громадянам України та іноземцям при підготовці фахівців з Кібербезпеки в авіаційно-космічній галузі.	
Розділ 3. Характеристика освітньо-професійної програми		
3.1	Предметна область (об'єкт діяльності, теоретичний зміст)	Об'єкт діяльності: – об'єкти інформатизації, включаючи комп'ютерні, автоматизовані, телекомунікаційні, інформаційні, інформаційно-аналітичні, інформаційно-телекомунікаційні системи, інформаційні ресурси і технології; – технології забезпечення безпеки інформації, системи та комплекси технічного захисту інформації на об'єктах інформаційної діяльності; – процеси управління інформаційною та/або кібербезпекою об'єктів, що підлягають захисту. Теоретичний зміст предметної області: методи та засоби технічного захисту інформації, технології створення, обробки, передачі, приймання, знищення, відображення, захисту (кіберзахисту) інформаційних ресурсів.
3.2.	Орієнтація освітньо-професійної програми	Програма має прикладну орієнтацію. Базується на загальновідомих положеннях, результатах сучасних наукових досліджень та нових знаннях в галузі інформаційних технологій, необхідних для майбутньої професійної діяльності бакалаврів з Кібербезпеки, здатних вирішувати певні проблеми і задачі за умови оволодіння системою загальних та фахових компетентностей.

3.3.	Основний фокус освітньо-професійної програми та спеціалізації (за наявності)	Спеціальна освіта та професійна підготовка в галузі 12 – Інформаційні технології за спеціальністю 125 – Кібербезпека. Ключові слова: технічний захист інформації, інформаційна та/або кібербезпека, захист інформації.
3.4.	Особливості освітньо-професійної програми	Освітньо-професійна програма передбачає 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; – методів та засобів виявлення закладних пристроїв, виявлення та локалізації каналів витоку інформації. На відміну від інших освітніх програм увага приділяється автоматизованим системам та комплексам технічного захисту інформації.
Розділ 4. Придатність випускників до працевлаштування та подальшого навчання		
4.1.	Придатність до працевлаштування	Випускники отримують можливість працевлаштування до підприємств (організацій, установ) різних форм власності в галузі «Інформаційних технологій» за спеціальністю «Кібербезпека» на відповідні посади та обіймати посади в інших секторах економіки при наявності сертифікатів про опанування відповідних програм підготовки.
4.2.	Подальше навчання	Можливість продовження навчання за програмами другого (магістерського) циклу вищої освіти (НРК України - 7 рівень, FQ-EHEA - другий цикл, EQF LLL - 7 рівень).

Розділ 5. Викладання та оцінювання		
5.1.	Викладання та навчання (методи, методики, технології, інструменти та обладнання)	*Методи, методики та технології:* Методи, методики, інформаційно-комунікаційні технології та інші технології забезпечення інформаційної та/ або кібербезпеки. Проблемно-орієнтоване навчання, яке передбачає формулювання та вирішення проблеми під час лекцій, розв`язання ситуативних задач на семінарах, практичних заняттях, дослідження проблеми під час самостійної роботи здобувачів вищої освіти. Практико-орієнтоване навчання через різні види практик на підприємствах, установах та організаціях різних форм власності на підставі договорів про проходження практики, організація якої здійснюється за принципом неперервності. Виконання практичних та лабораторних робіт в умовах виробництва. *Технології* дистанційного навчання, що реалізуються за допомогою комп'ютерної техніки, шляхом проведення занять з використанням чат-технологій; дистанційних занять, конференцій, семінарів, ділових ігор, лабораторних робіт, практикумів й інших форм навчальних занять, які проводяться за допомогою засобів телекомунікацій з використанням веб-технологій. Інформаційні технології навчання: робота здобувачів вищої освіти у спеціалізованих кабінетах облаштованих мультимедійними комплексами, що забезпечує можливість проведення інтерактивних лекцій та віртуальних лабораторних робіт, застосування пошукової методики здобуття нових знань, організації проектної роботи, проведення комп'ютеризованого тестового контролю якості знань. *Інструменти та обладнання:* – системи розробки, забезпечення, моніторингу та контролю процесів інформаційної та/ або кібербезпеки; – сучасне програмно-апаратне забезпечення інформаційно-комунікаційних технологій; – апаратно-програмні комплекси та засоби лінійного/просторового захисту інформації; – комбіновані системи контролю та управління доступом; – засоби технологічного, інформаційного, інструментального, метрологічного та організаційного забезпечення освітнього процесу.

5.2.	Оцінювання	Усні, письмові, творчі, тестові та комбіновані екзамени, диференційовані заліки, лабораторні звіти, звіти із практичних робіт та практик, реферати, захист курсових проектів, презентації, поточний контроль, захист кваліфікаційної роботи.
Розділ 6. Програмні компетентності		
6.1.	Інтегральна компетентність (ІК)	ІК1. Здатність розв'язувати складні спеціалізовані задачі та практичні проблеми у галузі забезпечення інформаційної безпеки та/або кібербезпеки, що характеризується комплексністю та неповною визначеністю умов.
6.2.	Загальні компетентності (ЗК)	ЗК1. Здатність застосовувати знання у практичних ситуаціях. ЗК2. Знання та розуміння предметної області та розуміння професії. ЗК3. Здатність професійною спілкуватися державною та іноземною мовами як усно, так і письмово. ЗК4. Вміння виявляти, ставити та вирішувати проблеми за професійним спрямуванням. ЗК5. Здатність до пошуку, оброблення та аналізу інформації. ЗК6. Здатність використовувати технічні засоби захисту та охорони інформаційних ресурсів і баз даних обмеженого доступу. ЗК7. Здатність організовувати функціонування системи організаційно-службових і спеціальних (охоронних) заходів із забезпечення інформаційної та/або кібербезпеки установ, підприємств, організацій. ЗК8. 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. ЗК9. 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.
6.3.	Фахові компетентності (ФК)	ФК1. 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. ФК2. Здатність до використання інформаційно-комунікаційних технологій, сучасних методів і моделей інформаційної та/або кібербезпеки. ФК3. Здатність до використання програмних, апаратних та програмно-апаратних комплексів засобів захисту інформації на об'єктах інформаційної діяльності та в інформаційно-телекомунікаційних (автоматизованих) системах. ФК4. Здатність забезпечувати неперервність бізнесу згідно встановленої політики інформаційної та/або кібербезпеки. ФК5. Здатність оцінювати захищеність інформації усіх видів, що циркулює на об'єктах інформаційної діяльності. ФК6. Здатність відновлювати штатне функціонування інформаційних, інформаційно-телекомунікаційних (автоматизованих) систем та комплексів технічного захисту інформації після реалізації загроз, здійснення кібератак, збоїв та відмов різних класів та походження. ФК7. Здатність забезпечувати захист інформації, що обробляється в інформаційно-телекомунікаційних (автоматизованих) системах з метою реалізації встановленої політики інформаційної та/або кібербезпеки. ФК8. Здатність впроваджувати та забезпечувати функціонування комплексних систем захисту інформації (комплекси нормативно-правових, організаційних та технічних засобів і методів, процедур, практичних прийомів та ін.). ФК9. Здатність здійснювати процедури управління інцидентами, проводити розслідування, надавати їм оцінку. ФК10. Здатність застосовувати методи та засоби криптографічного та технічного захисту інформації на об'єктах інформаційної діяльності. ФК11. Здатність аналізувати, виявляти та оцінювати можливі загрози, уразливості та дестабілізуючі чинники інформаційному простору та інформаційним ресурсам згідно з встановленою політикою інформаційної та/або кібербезпеки.

6.3.	Фахові компетентності (ФК)	ФК12. Здатність виявляти та блокувати канали витоку інформації, методи несанкціонованого доступу до інформації, джерел і способів дестабілізуючого впливу на інформацію, здійснювати пошук закладних пристроїв. ФК13. Здатність оцінювати та визначати фізичні процеси, які висвітлюють характеристики та параметри напівпровідникових активних елементів, а також проводити лінійний та нелінійний аналіз електричних схем, схемотехніки різноманітних підсилювальних каскадів, операційних підсилювачів та елементів логіки. ФК14. Здатність виконувати моніторинг процесів функціонування інформаційних, інформаційно-телекомунікаційних (автоматизованих) систем згідно встановленої політики інформаційної та/або кібербезпеки. ФК15. Здатність використовувати теоретичні знання та практичні навички з підготовки технічної документації. ФК16. Здатність здійснювати професійну діяльність на основі впровадженої системи управління інформаційною та/або кібербезпекою.
Розділ 7. Програмні результати навчання		
7.1.	Програмні результати навчання (ПРН)	ПРН1. Застосовувати знання державної та іноземних мов з метою забезпечення ефективності професійної комунікації. ПРН2. Організовувати власну професійну діяльність, обирати оптимальні методи та способи розв'язування складних спеціалізованих задач та практичних проблем у професійній діяльності, оцінювати їхню ефективність. ПРН3. Використовувати результати самостійного пошуку, аналізу та синтезу інформації з різних джерел для ефективного рішення спеціалізованих задач професійної діяльності. ПРН4. 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. ПРН5. Адаптуватися в умовах частої зміни технологій професійної діяльності, прогнозувати кінцевий результат. ПРН6. Критично осмислювати основні теорії, принципи, методи і поняття у навчанні та професійній діяльності.

7.1.	Програмні результати навчання (ПРН)	ПРН7. Діяти на основі законодавчої та нормативно-правової бази України та вимог відповідних стандартів, у тому числі міжнародних в галузі інформаційної та /або кібербезпеки. ПРН8. Готувати пропозиції до нормативних актів щодо забезпечення інформаційної та /або кібербезпеки. ПРН9. Впроваджувати процеси, що базуються на національних та міжнародних стандартах, виявлення, ідентифікації, аналізу та реагування на інциденти інформаційної та/або кібербезпеки. ПРН10. Виконувати аналіз та декомпозицію інформаційно-телекомунікаційних систем. ПРН11. Виконувати аналіз зв'язків між інформаційними процесами на віддалених обчислювальних системах. ПРН12. Розробляти моделі загроз та порушника. ПРН13. Аналізувати проекти інформаційно-телекомунікаційних систем базуючись на стандартизованих технологіях та протоколах передачі даних. ПРН14. Вирішувати завдання захисту програм та інформації, що обробляється в інформаційно-телекомунікаційних системах програмно-апаратними засобами та давати оцінку результативності якості прийнятих рішень. ПРН15. Використовувати сучасне програмно-апаратне забезпечення інформаційно-комунікаційних технологій. ПРН16. Реалізовувати комплексні системи захисту інформації в автоматизованих системах (АС) організації (підприємства) відповідно до вимог нормативно-правових документів. ПРН17. 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. ПРН18. Використовувати програмні та програмно-апаратні комплекси захисту інформаційних ресурсів. ПРН19. Застосовувати теорії та методи захисту для забезпечення безпеки інформації в інформаційно-телекомунікаційних системах.

7.1.	Програмні результати навчання (ПРН)	ПРН20. Забезпечувати функціонування спеціального програмного забезпечення, щодо захисту інформації від руйнуючих програмних впливів, руйнуючих кодів в інформаційно-телекомунікаційних системах. ПРН21. 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. ПРН22. Вирішувати задачі управління процедурами ідентифікації, автентифікації, авторизації процесів і користувачів в інформаційно телекомунікаційних системах згідно встановленої політики інформаційної і\або кібербезпеки. ПРН23. Реалізовувати заходи з протидії отриманню несанкціонованого доступу до інформаційних ресурсів і процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах. ПРН24. Вирішувати задачі управління доступом до інформаційних ресурсів та процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах на основі моделей управління доступом (мандатних, дискреційних, рольових). ПРН25. 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. ПРН26. Впроваджувати заходи та забезпечувати реалізацію процесів попередження отриманню несанкціонованого доступу і захисту інформаційних, інформаційно-телекомунікаційних (автоматизованих) систем на основі еталонної моделі взаємодії відкритих систем. ПРН27. Вирішувати задачі захисту потоків даних в інформаційних, інформаційно-телекомунікаційних (автоматизованих) системах. ПРН28. Аналізувати та проводити оцінку ефективності та рівня захищеності ресурсів різних класів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах в

7.1.	Програмні результати навчання (ПРН)	ході проведення випробувань згідно встановленої політики інформаційної та\або кібербезпеки. ПРН29. 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. ПРН30. Здійснювати оцінювання можливості несанкціонованого доступу до елементів інформаційно-телекомунікаційних систем. ПРН31. Застосовувати теорії та методи захисту для забезпечення безпеки елементів інформаційно-телекомунікаційних систем. ПРН32. Вирішувати задачі управління процесами відновлення штатного функціонування інформаційно-телекомунікаційних систем з використанням процедур резервування згідно встановленої політики безпеки. ПРН33. Вирішувати задачі забезпечення безперервності бізнес процесів організації на основі теорії ризиків. ПРН34. Приймати участь у розробці та впровадженні стратегії інформаційної безпеки та/або кібербезпеки відповідно до цілей і завдань організації. ПРН35. 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 та\або кібербезпеки. ПРН36. Виявляти небезпечні сигнали технічних засобів. ПРН37. 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. ПРН38. Інтерпретувати результати проведення спеціальних вимірювань з використанням технічних засобів, контролю характеристик інформаційно-телекомунікаційних систем відповідно до вимог нормативних документів системи технічного захисту інформації.

7.1.	Програмні результати навчання (ПРН)	ПРН39. Проводити атестацію (спираючись на облік та обстеження) режимних територій (зон), приміщень тощо в умовах додержання режиму секретності із фіксуванням результатів у відповідних документах. ПРН40. Виявляти закладні пристрої несанкціонованого отримання інформації. ПРН41. Забезпечувати неперервність процесу ведення журналів реєстрації подій та інцидентів на основі автоматизованих процедур. ПРН42. Впроваджувати процеси виявлення, ідентифікації, аналізу та реагування на інциденти інформаційної і/або кібербезпеки. ПРН43. Застосовувати національні та міжнародні регулюючі акти в сфері інформаційної безпеки та/ або кібербезпеки для розслідування інцидентів. ПРН44. 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. ПРН45. Застосовувати різні класи політик інформаційної безпеки та/або кібербезпеки, що базуються на ризик-орієнтованому контролі доступу до інформаційних активів. ПРН46. Здійснювати аналіз та мінімізацію ризиків обробки інформації в інформаційно-телекомунікаційних системах. ПРН47. Вирішувати задачі захисту інформації, що обробляється в інформаційно-телекомунікаційних системах з використанням сучасних методів та засобів криптографічного захисту інформації. ПРН48. Виконувати впровадження та підтримку систем виявлення вторгнень та використовувати компоненти криптографічного захисту для забезпечення необхідного рівня захищеності інформації в інформаційно-телекомунікаційних системах. ПРН49. Забезпечувати належне функціонування системи моніторингу інформаційних ресурсів і процесів в інформаційно-телекомунікаційних системах. ПРН50. Забезпечувати функціонування програмних та програмно-апаратних комплексів виявлення вторгнень різних рівнів та класів (статистичних, сигнатурних, статистично-сигнатурних).

7.1.	Програмні результати навчання (ПРН)	ПРН51. Підтримувати працездатність та забезпечувати конфігурування систем виявлення вторгнень в інформаційно-телекомунікаційних системах. ПРН52. Використовувати інструментарій для моніторингу процесів в інформаційно-телекомунікаційних системах. ПРН53. Вирішувати задачі аналізу програмного коду на наявність можливих загроз. ПРН54. Усвідомлювати цінності громадянського (вільного демократичного) суспільства та необхідність його сталого розвитку, верховенства права, прав і свобод людини і громадянина в Україні. ПРН55. Визначати відомості, які відносяться до інформації з обмеженим доступом, організовувати допуск та доступ персоналу до інформації з обмеженим доступом згідно чинного законодавства та встановленої політики інформаційної та/або кібербезпеки. ПРН56. Організовувати внутрішньо-об'єктовий та пропускний режими на підприємстві. ПРН57. Вирішувати задачі забезпечення та супроводу комплексу технічного захисту інформації на об'єкті інформаційної діяльності. ПРН58. Оцінювати захищеність інформації на об'єктах інформаційної діяльності. ПРН59. Складати звітність та вести технічну документацію.
Розділ 8. Ресурсне забезпечення реалізації програми		
8.1.	Кадрове забезпечення	Кадрове забезпечення відповідає ліцензійним вимогам. В освітньому процесі беруть участь доктори та кандидати наук, професори та доценти, старші викладачі й асистенти за спеціальністю 125 Кібербезпека та за іншими спеціальностями, які забезпечують підготовку бакалаврів з Кібербезпеки. До організації навчального процесу залучаються професіонали з досвідом наукової, педагогічної, дослідницької, управлінської, інноваційної, творчої та фахової роботи, іноземні лектори.
8.2.	Матеріально-технічне забезпечення	Матеріально-технічна база випускової кафедри засобів захисту інформації дозволяє забезпечити підготовку фахівців на першому (бакалаврському) рівні вищої освіти за ОПП: – забезпеченість комп'ютерними робочими місцями та прикладними комп'ютерними

8.2.	Матеріально-технічне забезпечення	програмами достатнє для виконання навчальних планів; – усі комп'ютери кафедри під'єднані до локальної мережі університету з можливістю виходу в глобальну мережу Інтернет; – для ведення документації та забезпечення навчально-методичними матеріалами освітнього процесу кафедра в достатній кількості забезпечена оргтехнікою (принтерами, МФУ, сканерами); – навчальні лабораторії оснащені технічними засобами та спеціалізованим програмним забезпеченням, необхідними приладами та обладнанням (охоронними системами відеоспостереження, засобами та комплексами виявлення закладних пристроїв, засобами просторового та мережевого захисту інформації). Усі приміщення відповідають будівельним та санітарним нормам, гуртожитками забезпечені усі потребуючі, наявна соціальна інфраструктура включає спортивний комплекс, пункти харчування, центр творчості, медпункт і базу відпочинку.
8.3.	Інформаційне та навчально-методичне забезпечення	Забезпечення навчальною та навчально-методичною літературою, доступ до фахових періодичних видань професійного спрямування, упровадження електронного каталогу та можливість роботи з електронними підручниками здійснюється за рахунок фондів Науково-технічної бібліотеки НАУ. Всі студенти забезпечені підручниками та навчальними посібниками з компонентів ОПП. Відповідне інформаційне та навчально-методичне забезпечення розташоване на освітніх платформах Google Classroom, Moodle (Modular Object-Oriented Dynamic Learning Environment). Всі ресурси науково-технічної бібліотеки доступні через сайт університету: http://www.lib.nau.edu.ua Читальний зал забезпечений бездротовим доступом до мережі Інтернет. Електронний репозитарій наукової бібліотеки НАУ: http://er.nau.edu.ua
Розділ 9. Академічна мобільність		
9.1.	Національна кредитна мобільність	Національна кредитна мобільність здобувачів вищої освіти, наукових і науково-педагогічних працівників, у т.ч. навчання, стажування, проведення наукових досліджень, викладання та

9.1.	Національна кредитна мобільність	підвищення кваліфікації організовується на підставі партнерських угод про співпрацю між Національним авіаційним університетом та закладами вищої освіти в Україні: – Національним технічним університетом України «Київським політехнічним інститутом імені Ігоря Сікорського»; – Харківським національним університетом радіоелектроніки.
9.2.	Міжнародна кредитна мобільність	У рамках Еразмус+К1 договір про співробітництво між Національним авіаційним університетом та навчальними закладами ЕС.
9.3.	Навчання іноземних здобувачів вищої освіти	**Іноземці та особи без громадянства,** які проживають в Україні на законних підставах, мають право на здобуття вищої освіти за освітньо-професійною програмою нарівні з громадянами України. Умовою зарахування іноземців на навчання для отримання певного освітнього ступеня є володіння ними мовою навчання на рівні, достатньому для засвоєння навчального матеріалу. Іноземці зараховуються на навчання за освітньо-професійною програмою до НАУ за результатами співбесіди.

2. Перелік компонент освітньо-професійної програми та їх логічна послідовність

2.1. Перелік освітніх компонент ОПП, 240 кредитів ЄКТС

Код н/д	Компоненти освітньо-професійної програми (навчальні дисципліни, курсові проекти (роботи), практики, кваліфікаційна робота)	Кількість кредитів	Форма підсумкового контролю	Семестр
1	2	3	4	5
Обов'язкові компоненти				
Ядро програми (Core), (soft-skills)				
ОК1.	Історія української державності та культури	3.0	Екзамен	1
ОК2.	Ділова українська мова	3.0	Екзамен	2
ОК3.	Філософія	3.5	Екзамен	4
ОК4.	Фахова іноземна мова	4.5	Залік, екзамен	1, 2
ОК5.	Фізичне виховання та самовдосконалення	3.0	Залік	2
Професійно-практична підготовка (Major)				
ОК6.	Вища математика	14.0	Залік, Екзамен	1, 2, 3

1	2	3	4	5
ОК7.	Фізика	10.5	Залік, екзамен	1, 2
ОК8.	Інформаційні технології	11.5	Залік, екзамен	1, 2
ОК9.	Основи автоматизованої обробки інформації	6.5	Залік	1, 2
ОК10.	Основи кібербезпеки	4.5	Залік	1
ОК11.	Апаратне забезпечення інформаційних систем	5.0	Залік, екзамен	3, 4
ОК12.	Курсова робота з Апаратного забезпечення інформаційних систем	1.0	Залік	3
ОК13.	Виявлення закладних пристроїв на об'єктах інформаційної діяльності	4.0	Екзамен	3
ОК14.	Основи теорії кіл, сигналів та процесів в системах технічного захисту інформації	6.5	Залік, екзамен	3, 4
ОК15.	Курсова робота з Основ теорії кіл, сигналів та процесів в системах технічного захисту інформації	1.0	Залік	4
ОК16.	Компонентна база засобів технічного захисту інформації	4.0	Екзамен	3
ОК17.	Безпека інформаційно-комунікаційних систем	4.0	Залік	4
ОК18.	Схемотехніка пристроїв технічного захисту інформації	4.5	Залік	4
ОК19.	Засоби передавання сигналів в системах технічного захисту інформації	4.5	Екзамен	5
ОК20.	Курсова робота з Засобів передавання сигналів в системах технічного захисту інформації	1.0	Залік	5
ОК21.	Авіаційна безпека та кібербезпека авіаційних інформаційних систем	10.5	Залік, екзамен	5, 6, 7
ОК22.	Поля і хвилі в системах технічного захисту інформації	4.5	Екзамен	5
ОК23.	Захищені комп'ютерні системи та мережі**	8.0	Залік, екзамен	5, 6
ОК24.	Управління інформаційною безпекою	3.0	Екзамен	6
ОК25.	Курсова робота з Управління інформаційною безпекою	1.0	Залік	6
ОК26.	Прикладна криптологія	7.5	Екзамен	6, 7
ОК27.	Курсова робота з Прикладної криптології	1.0	Залік	7
ОК28.	Операційні системи та технології їх захисту***	7.0	Залік, екзамен	6, 7
ОК29.	Системи технічного захисту інформації	3.5	Екзамен	7
ОК30.	Засоби приймання та обробки сигналів в системах технічного захисту інформації	3.5	Залік	7

1	2	3	4	5
ОК31.	Комплексні системи захисту інформації	4.0	Екзамен	8
ОК32.	Методи та засоби технічного захисту інформації	4.5	Екзамен	8
ОК33.	Проектування систем технічного захисту інформації	3.0	Екзамен	8
ОК34.	Цифрова обробка сигналів	3.0	Екзамен	8
Практична підготовка				
ОК35.	Фахова ознайомлювальна практика	3.0	Залік	2
ОК36.	Комп'ютерна практика	3.0	Залік	4
ОК37.	Технологічна практика	3.0	Залік	6
ОК38.	Кваліфікаційна робота	7.5	Захист	8
Загальний обсяг обов'язкових компонент:		180 кредитів ЄКТС		
Вибіркові компоненти*				
ВК1.		4.0	Залік	
ВК2.		4.0	Залік	
ВК3.		4.0	Залік	
---	----	---	---	---
ВК15.		4.0	Залік	
Загальний обсяг вибіркових компонент*		60 кредитів ЄКТС		
Загальний обсяг освітньо-професійної програми		240 кредитів ЄКТС		

2.2. Перелік освітніх компонент для скороченого терміну навчання, 180 кредитів ЄКТС

Код н/д	Компоненти освітньо-професійної програми (навчальні дисципліни, курсові проекти (роботи), практики, кваліфікаційна робота)	Кількість кредитів	Форма підсумкового контролю	Семестр
1	2	3	4	5
Обов'язкові компоненти				
Ядро програми (Core), (soft-skills)				
ОК3.	Філософія	3.5	Екзамен	2
Професійно-практична підготовка (Major)				
ОК6.	Вища математика	14.0	Екзамен	1
ОК11.	Апаратне забезпечення інформаційних систем	5.0	Залік, екзамен	1, 2
ОК12.	Курсова робота з Апаратного забезпечення інформаційних систем	1.0	Залік	1
ОК13.	Виявлення закладних пристроїв на об'єктах інформаційної діяльності	4.0	Екзамен	1

1	2	3	4	5
ОК14.	Основи теорії кіл, сигналів та процесів в системах технічного захисту інформації	6.5	Залік, екзамен	1, 2
ОК15.	Курсова робота з Основ теорії кіл, сигналів та процесів в системах технічного захисту інформації	1.0	Залік	2
ОК16.	Компонентна база засобів технічного захисту інформації	4.0	Екзамен	1
ОК17.	Безпека інформаційно-комунікаційних систем	4.0	Залік	2
ОК18.	Схемотехніка пристроїв технічного захисту інформації	4.5	Залік	2
ОК19.	Засоби передавання сигналів в системах технічного захисту інформації	4.5	Екзамен	3
ОК20.	Курсова робота з Засобів передавання сигналів в системах технічного захисту інформації	1.0	Залік	3
ОК21.	Авіаційна безпека та кібербезпека авіаційних інформаційних систем	10.5	Залік, екзамен	3, 4, 5
ОК22.	Поля і хвилі в системах технічного захисту інформації	4.5	Екзамен	3
ОК23.	Захищені комп'ютерні системи та мережі**	8.0	Залік, екзамен	3, 4
ОК24.	Управління інформаційною безпекою	3.0	Екзамен	4
ОК25.	Курсова робота з Управління інформаційною безпекою	1.0	Залік	4
ОК26.	Прикладна криптологія	7.5	Залік, екзамен	4, 5
ОК27.	Курсова робота з Прикладної криптології	1.0	Залік	5
ОК28.	Операційні системи та технології їх захисту***	7.0	Залік, екзамен	4, 5
ОК29.	Системи технічного захисту інформації	3.5	Екзамен	5
ОК30.	Засоби приймання та обробки сигналів в системах технічного захисту інформації	3.5	Залік	5
ОК31.	Комплексні системи захисту інформації	4.0	Екзамен	6
ОК32.	Методи та засоби технічного захисту інформації	4.5	Екзамен	6
ОК33.	Проектування систем технічного захисту інформації	3.0	Екзамен	6
ОК34.	Цифрова обробка сигналів	3.0	Екзамен	6
Практична підготовка				
ОК36.	Комп'ютерна практика	3.0	Залік	2
ОК37.	Технологічна практика	3.0	Залік	4
ОК38.	Кваліфікаційна робота	7.5	Захист	6
Загальний обсяг обов'язкових компонент:		120 кредитів ЄКТС		

1	2	3	4	5
Вибіркові компоненти*				
ВК1.		4.0	Залік	
ВК2.		4.0	Залік	
ВК3.		4.0	Залік	
---	----	---	---	---
ВК15.		4.0	Залік	
Загальний обсяг вибіркових компонент*		60 кредитів ЄКТС		
Загальний обсяг освітньо-професійної програми		180 кредитів ЄКТС		

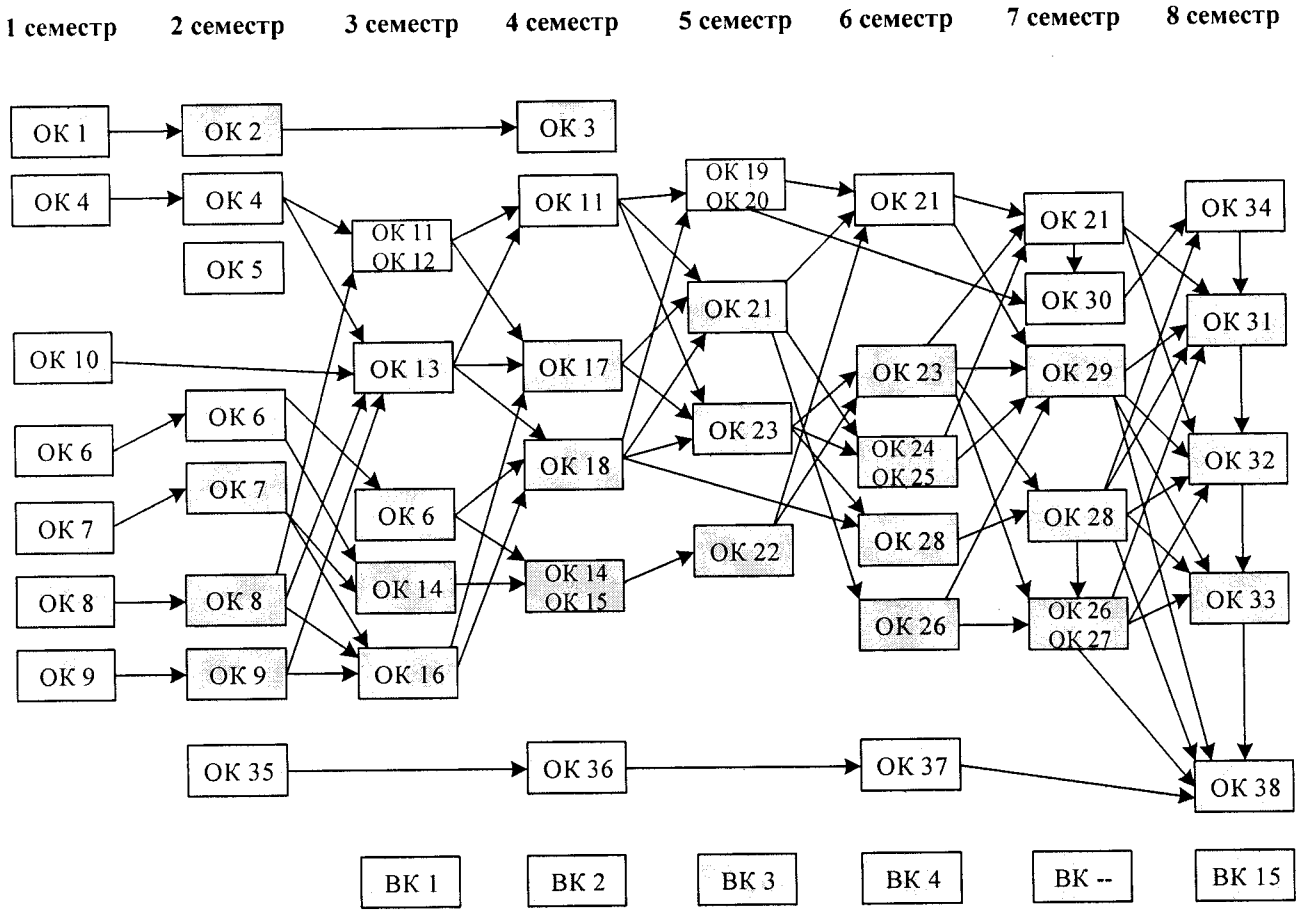
* *Реалізація права здобувачів вищої освіти на вільний вибір навчальних дисциплін та створення індивідуальної освітньої траєкторії регламентується законом України «Про вищу освіту» та внутрішніми нормативними актами НАУ.*

Вибіркові компоненти обираються здобувачами вищої освіти із каталогів рекомендованих та альтернативних вибіркових дисциплін.

** *Офіційний сертифікований курс Cisco Networking Academy.*

*** *Офіційний сертифікований курс Network Development Group.*

2.3. Структурно-логічна схема освітньо-професійної програми



3. Форма атестації здобувачів вищої освіти

Форми атестації здобувачів вищої освіти	Атестація здобувачів ОС «Бакалавр» здійснюється у формі публічного захисту кваліфікаційної бакалаврської роботи і завершується видачею документу встановленого зразку про присудження їм освітнього ступеня «Бакалавр» із присвоєнням освітньої кваліфікації: Бакалавр з кібербезпеки, за спеціальністю 125 «Кібербезпека». На атестацію виноситься сукупність знань, умінь, навичок, інших компетентностей, набутих студентами у процесі навчання. До атестації допускаються студенти, які виконали всі вимоги програми підготовки.

Вимоги до кваліфікаційної роботи	Кваліфікаційна робота бакалавра повинна бути самостійною логічно завершеною теоретичною або експериментальною (дослідною) роботою, пов'язаною з розв'язанням спеціалізованої задачі в галузі інформаційної та/або кібербезпеки. Кваліфікаційна робота бакалавра не повинна містити академічного плагіату, у тому числі некоректних текстових запозичень, фабрикації та фальсифікації. Кваліфікаційна робота має бути оприлюднена на офіційному сайті Університету або його структурного підрозділу, або у репозитарії. Оприлюднення кваліфікаційних робіт, що містять інформацію з обмеженим доступом, здійснювати відповідно до вимог законодавства.
Вимоги до публічного захисту (демонстрації)	Публічний захист кваліфікаційної бакалаврської роботи відбувається на засіданні екзаменаційної комісії. Порядок захисту передбачає представлення здобувача й поданих документів; виступ здобувача; відповіді здобувача на запитання членів екзаменаційної комісії та присутніх. Виступ здобувача має супроводжуватись презентацією.

4. Матриця відповідності програмних компетентностей компонентам освітньо-професійної програми

Компоненти / Компетентності	ОК 1	ОК 2	ОК 3	ОК 4	ОК 5	ОК 6	ОК 7	ОК8	ОК 9	ОК 10	ОК11, ОК12	ОК 13	ОК14, ОК15	ОК 16	ОК 17	ОК 18	ОК19, ОК20	ОК 21	ОК 22	ОК 23	ОК24, ОК25	ОК26, ОК27	ОК 28	ОК 29	ОК 30	ОК 31	ОК 32	ОК 33	ОК 34	ОК 35	ОК 36	ОК 37	ОК 38	ВК 1*	ВК 2*	ВК --	ВК 15*
1	2	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36	37	38	39
ІК1	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+				
ЗК1	+	+	+	+		+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+				
ЗК2	+	+					+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+				
ЗК3		+		+																										+	+	+	+				
ЗК4		+				+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+				
ЗК5	+	+	+	+		+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+				
ЗК6								+	+	+	+	+		+	+			+		+	+	+	+	+		+	+	+		+	+	+	+				
ЗК7					+					+	+	+		+		+	+	+						+	+	+	+	+		+	+	+	+				
ЗК8	+	+	+																											+	+	+	+				
ЗК9	+	+	+	+	+	+		+																						+	+	+	+				
ФК1		+		+					+	+		+			+			+			+			+		+	+	+		+	+	+	+				
ФК2				+				+	+	+	+			+	+			+		+	+	+	+	+		+	+	+	+	+	+	+				
ФК3								+		+	+	+		+	+	+		+		+	+	+	+	+		+	+	+		+	+	+				
ФК4								+	+	+	+	+		+	+					+	+		+	+		+	+	+		+	+	+				
ФК5							+			+		+	+					+	+		+			+		+	+			+	+	+				
ФК6								+	+	+	+			+		+				+	+		+	+		+	+	+		+	+	+				
ФК7								+	+	+	+			+	+			+		+	+	+	+	+		+	+	+	+	+	+	+				
ФК8								+	+	+	+	+		+	+		+	+		+	+		+	+	+	+	+		+	+	+	+				
ФК9								+		+		+			+			+			+			+		+	+			+	+	+				
ФК10						+				+				+	+							+		+		+	+	+		+	+	+				
ФК11								+	+	+		+	+		+			+	+	+	+		+	+		+	+			+	+	+				
ФК12							+			+		+	+		+		+		+		+			+	+	+	+	+		+	+	+				
ФК13						+	+						+	+		+	+								+				+	+	+	+				

1	2	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36	37	38	39
ФК14			+	+				+	+	+	+				+			+		+	+		+	+		+	+		+	+	+	+	+				
ФК15		+	+			+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+			+	+	+	+	+		+	+	+	+				
ФК16								+		+					+			+			+			+		+	+										

** Вибіркові компоненти обрані із каталогів рекомендованих та альтернативних вибіркових дисциплін Університету мають також забезпечувати визначені компетентності. Кількість вибіркових компонент визначається виходячи із загального обсягу вибіркових компонент (кредитів) освітньої програми.*

5. Матриця забезпечення програмних результатів навчання (ПРН) відповідними компонентами освітньо-професійної програми

Компоненти / Програмні результати навчання	ОК 1	ОК 2	ОК 3	ОК 4	ОК 5	ОК 6	ОК 7	ОК8	ОК 9	ОК 10	ОК11, ОК12	ОК 13	ОК14, ОК15	ОК 16	ОК 17	ОК 18	ОК19, ОК20	ОК 21	ОК 22	ОК 23	ОК24, ОК25	ОК26, ОК27	ОК 28	ОК 29	ОК 30	ОК 31	ОК 32	ОК 33	ОК 34	ОК 35	ОК 36	ОК 37	ОК 38	ВК 1*	ВК 2*	ВК --	ВК 15*
1	2	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36	37	38	39
ПРН 1		+		+				+	+	+					+			+		+	+	+	+	+		+	+		+	+	+	+	+			
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								+	+	+					+			+		+	+		+			+	+			+	+	+	+			

1	2	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36	37	38	39
ПРН 23								+	+	+					+			+		+	+		+	+		+	+			+	+	+	+				
ПРН 24								+		+					+			+		+	+		+			+	+			+	+	+	+				
ПРН 25								+	+	+					+			+		+	+		+			+	+			+	+	+	+				
ПРН 26								+		+					+			+		+	+		+			+	+			+	+	+	+				
ПРН 27								+	+	+					+			+		+			+			+	+			+	+	+	+				
ПРН 28							+	+	+	+		+	+		+			+	+	+	+			+		+	+	+		+	+	+	+				
ПРН 29									+	+		+	+		+			+	+		+			+		+	+	+		+	+	+	+				
ПРН 30									+	+		+	+		+			+	+		+			+		+	+	+		+	+	+	+				
ПРН 31								+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+		+	+	+	+	+	+	+	+				
ПРН 32								+		+	+				+			+			+		+			+	+			+	+	+	+				
ПРН 33								+	+	+	+				+			+			+		+			+	+			+	+	+	+				
ПРН 34										+					+			+			+			+		+	+			+	+	+	+				
ПРН 35								+	+	+	+	+		+	+	+	+	+		+	+		+	+	+	+	+	+		+	+	+	+				
ПРН 36							+			+			+				+	+	+						+	+		+		+	+	+	+				
ПРН 37						+	+						+				+	+	+						+			+		+	+	+	+				
ПРН 38						+	+		+				+						+						+			+		+	+	+	+				
ПРН 39									+	+					+			+			+			+		+	+			+	+	+	+				
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	+	+	+		+	+	+	+	+	+		+			+			+		+	+		+	+		+	+	+		+	+	+	+				
ПРН 55								+	+	+					+			+			+	+	+	+		+	+			+	+	+	+				

1	2	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36	37	38	39
ПРН 56								+		+	+							+			+		+	+		+	+			+	+	+	+				
ПРН 57									+	+		+	+	+	+	+	+	+	+	+	+			+	+		+	+	+	+	+	+	+				
ПРН 58							+	+	+	+		+	+		+			+	+	+	+			+		+	+	+		+	+	+	+				
ПРН 59		+				+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+				

** Вибіркові компоненти обрані із каталогів рекомендованих та альтернативних вибіркових дисциплін Університету мають також забезпечувати визначені програмні результати навчання (ПРН). Кількість вибіркових компонент визначається виходячи із загального обсягу вибіркових компонент (кредитів) освітньої програми.*

6. Система внутрішнього забезпечення якості вищої освіти НАУ

Якість освітньо-професійної програми визначається внутрішньою системою забезпечення якості вищої освіти та освітньої діяльності НАУ, яка функціонує згідно з Положенням про систему забезпечення якості вищої освіти та освітньої діяльності, затвердженого рішенням вченої ради Університету від 28.11.2018 (протокол № 8) та відповідає вимогам Закону України «Про вищу освіту» від 01.07.2014 № 1556-VII (Розділ V Забезпечення якості вищої освіти, ст.16).

7. Перелік нормативних документів, на яких базується освітньо-професійна програма

1. «Про освіту»: Закон України від 05.09.2017 № 2145-VIII [Електронний ресурс]. – режим доступу: http://zakon.rada.gov.ua/laws/show/2145-19
2. «Про вищу освіту»: Закон України від 01.07.2014 № 1556-VII [Електронний ресурс]. – режим доступу: http://zakon4.rada.gov.ua/laws/show/1556-18
3. Постанова Кабінету Міністрів України від 25.06.2020 р. № 519 «Про внесення змін у додаток до постанови Кабінету Міністрів України від 23 листопада 2011 р. № 1341».
4. Про затвердження переліку галузей знань і спеціальностей, за якими здійснюється підготовка здобувачів вищої освіти: Постанова Кабінету Міністрів України від 29.04.2015 р. № 266 [Електронний ресурс]. – режим доступу: http://zakon2.rada.gov.ua/laws/show/266-2015-%D0%BF
5. Класифікація видів економічної діяльності : ДК 009:2010. – На заміну ДК 009:2005; Чинний від 2012-01-01. – (Національний класифікатор України).
6. Класифікатор професій ДК 003:2010. – На заміну ДК 003:2005; Чинний від 2010-11-01. –(Національний класифікатор України).
7. Стандарт вищої освіти України: перший (бакалаврський) рівень, галузь знань 12 «Інформаційні технології», спеціальність 125 «Кібербезпека». Стандарт вищої освіти затверджено і введено в дію наказом Міністерства освіти і науки України від 04.10.2018 № 1074.
8. Стратегія кібербезпеки України, затверджена Указом Президента України від 15.03.2016 № 96/2016.
9. Положення про освітні програми Національного авіаційного університету, погоджено Радою з якості НАУ (протокол від 28.04.2020 № 2) та уведено в дію наказом ректора від 07.05.2020 № 148/од.

РЕЦЕНЗІЯ
Освітньо-професійної програми
«Системи технічного захисту інформації, автоматизація її обробки»
першого (бакалаврського) рівня вищої освіти
за спеціальністю 125 «Кібербезпека»
Національного авіаційного університету

Аналіз представленої на рецензію освітньо-професійної програми «Системи технічного захисту інформації, автоматизація її обробки» (далі – ОПП) першого (бакалаврського) рівня вищої освіти свідчить про її направленість на підготовку висококваліфікованих фахівців зі спеціальності 125 «Кібербезпека».

Слід зазначити, що рецензована ОПП за освітнім ступенем «Бакалавр» скорегована у напрямку посилення професійної орієнтації фахівців у сфері забезпечення інформаційної та/або кібербезпеки. Об'єктивна необхідність ОПП зумовлена формуванням у студентів фундаментальних знань, вмінь та навичок майбутніх фахівців, здатних використовувати і впроваджувати технології інформаційної та/або кібербезпеки.

Представлена програма регламентує мету, очікувані результати навчання, зміст, умови і технологію реалізації освітнього процесу, оцінку якості підготовки здобувачів першого (бакалаврського) рівня за даною спеціальністю і включає в себе: загальну інформацію, мету і характеристику освітньої програми, здатність випускників до подальшого навчання та працевлаштування, викладання та оцінювання, компетентності та програмні результати навчання, ресурсне забезпечення реалізації програми, академічну мобільність, перелік обов'язкових і блок вибіркових компонентів та їх логічну послідовність, структурно-логічну схему освітньої програми, форму атестації здобувачів вищої освіти, матрицю відповідності компетентностей та програмних результатів навчання.

Компоненти освітньої програми дозволяють повною мірою сформувати знання, практичні уміння і навички, необхідні сучасному фахівцеві. У доборі цих компонент витримано баланс між циклами гуманітарної підготовки і циклами професійної та практичної підготовки, теорією і практикою.

У структуру ОПП включені обов'язкові та блок вибіркових компонент підготовки здобувачів вищої освіти, сформульовані у термінах результатів навчання: знання, уміння, комунікація, автономія та відповідальність. Наявність в освітній програмі блоку вільного вибору передбачає можливість реалізації особистісного потенціалу здобувача освіти, враховуючи його здібності, інтереси, потреби, мотивацію, можливості та ґрунтується на виборі здобувачем освіти видів, форм і темпу здобуття освіти, навчальних дисциплін і рівня їх складності, методів і засобів навчання, формуючи індивідуальну освітню траєкторію підготовки.

Розроблена ОПП заслуговує на увагу ще й тому, що логічно витримана її загальна структура, до якої привнесені відповідні корективи та сутнісні зміни щодо компетенцій, отриманих завдяки вивченню низки окремих навчальних дисциплін, дає змогу підсилити фахову та професійну підготовку випускників з подальшою можливістю їх працевлаштування.

В цілому, представлена на рецензію ОПП, враховує новітні тенденції та проблеми розвитку освітянської галузі й сприятиме підготовці висококваліфікованих фахівців та інтеграції України в європейський загальноосвітній та науковий простір.

Враховуючи викладене зазначаю, що освітньо-професійна програма «Системи технічного захисту інформації, автоматизація її обробки» підготовки здобувачів першого (бакалаврського) рівня вищої освіти відповідає Стандарту вищої освіти України і може використовуватися для підготовки фахівців спеціальності 125 «Кібербезпека».

Директор Навчально-наукового інституту захисту інформації
Державного університету телекомунікацій
д.т.н., професор Савченко В.А.

Підпис Савченка В.А.
засвідчую
Учений секретар О.В. Пожар

РЕЦЕНЗІЯ-ВІДГУК
на освітньо-професійну програму
«Системи технічного захисту інформації, автоматизація її обробки»
першого (бакалаврського) рівня вищої освіти
за спеціальністю 125 «Кібербезпека»
Національного авіаційного університету

Сучасний рівень глобалізації та інформатизації суспільства ставить нові вимоги перед роботодавцями, що потребують підвищення рівня безпеки та захисту інформації, що має обіг на підприємствах (установах, організаціях тощо).

У рамках тенденцій сьогодення було розглянуто та опрацьовано надану освітньо-професійну програму «Системи технічного захисту інформації, автоматизація її обробки» (далі - ОПП) першого (бакалаврського) рівня вищої освіти за спеціальністю 125 «Кібербезпека».

Розроблена ОПП надає можливість підготовки фахівців, здатних розв'язувати складні спеціалізовані завдання та прикладні проблеми, які характеризуються комплексністю та певною невизначеністю умов в галузі Кібербезпеки.

Представлена на розгляд ОПП відповідає Стандарту вищої освіти України за спеціальністю 125 «Кібербезпека» для першого (бакалаврського) рівня вищої освіти. Поставлені цілі враховують стратегію та місію Національного авіаційного університету, відповідають рівню розвитку інноваційних технологій в напрямку забезпечення інформаційної та/або кібербезпеки.

У процесі роботи над проектом ОПП було виявлено та виправлено ряд зауважень, що позитивно вплинуло на актуальність програми та її відповідність вимогам ринку праці.

Підготовлена ОПП має логічну послідовність вивчення дисциплін для отримання відповідних компетентностей. Перелік та обсяг обов'язкових та вибіркових компонент відповідає структурно-логічній схемі підготовки здобувачів вищої освіти за спеціальністю 125 «Кібербезпека». Дисципліни, наведені в ОПП, відображають актуальні для інформаційної та/або кібербезпеки теми.

З представленої ОПП можна зробити висновок, що вона має високий рівень забезпеченості навчально-методичною документацією та матеріалами, сприяє відповідності програмних результатів навчання запитам потенційних роботодавців.

З урахуванням вищевикладеного, вважаємо, що надану для рецензування освітньо-професійну програму «Системи технічного захисту інформації, автоматизація її обробки» варто рекомендувати для підготовки студентів за спеціальністю 125 «Кібербезпека» першого (бакалаврського) рівня вищої освіти.

Директор Товариства з обмеженою відповідальністю
«Світ інформаційно-телекомунікаційних рішень» А. Рудевич

РЕЦЕНЗІЯ-ВІДГУК
на освітньо-професійну програму
«Системи технічного захисту інформації, автоматизація її обробки»
першого (бакалаврського) рівня вищої освіти
за спеціальністю 125 «Кібербезпека»
Національного авіаційного університету

Аналіз представленої на розгляд освітньо-професійної програми «Системи технічного захисту інформації, автоматизація її обробки» (далі – ОПП) освітнього ступеня «Бакалавр» свідчить про її відповідність до вимог Стандарту вищої освіти України за спеціальністю 125 «Кібербезпека» для першого (бакалаврського) рівня вищої освіти.

Слід зазначити, що рецензована ОПП за освітнім ступенем «Бакалавр» скорегована у напрямку посилення професійної орієнтації фахівців у сфері забезпечення інформаційної та/або кібербезпеки. Об'єктивна необхідність ОПП зумовлена формуванням у студентів фундаментальних знань, вмінь та навичок майбутніх кваліфікованих, конкурентоспроможних фахівців.

У структуру ОПП включені обов'язкові дисципліни, дисципліни професійної та практичної підготовки. Також включено блок дисциплін вільного вибору студента. Зазначені дисципліни у повному обсязі забезпечують інтегральні, загальні та фахові компетентності випускників Національного авіаційного університету.

У розробленій ОПП логічно витримана загальна структура, до якої привнесені відповідні корективи та сутнісні зміни щодо компетенцій, отриманих завдяки вивченню низки окремих навчальних дисциплін, що дає змогу підсилити фахову та професійну підготовку випускників з подальшою можливістю їх працевлаштування.

В цілому, представлена на розгляд та рецензію ОПП, враховує новітні тенденції та проблеми розвитку освітянської галузі й сприятиме підготовці висококваліфікованих фахівців та інтеграції України в європейський загальноосвітній та науковий простір.

Враховуючи викладене вважаємо, що надану для рецензування освітньо-професійну програму «Системи технічного захисту інформації, автоматизація її обробки» доцільно використовувати для підготовки студентів за спеціальністю 125 «Кібербезпека» першого (бакалаврського) рівня вищої освіти.

Директор Товариства з обмеженою відповідальністю
«Українські технології безпеки» Є. Кисельов