

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 – 04 – 2021


Освітньо-професійна програма
затверджена Вченою радою Університету
Протокол № _____ від _____ 2021 р.

Вводиться в дію наказом ректора

Ректор
_____ М. Луцький

Наказ № _____ від _____ 2021 р.

КИЇВ

	<p align="center">Система менеджменту якості ОСВІТНЬО-ПРОФЕСІЙНА ПРОГРАМА «СИСТЕМИ ТЕХНІЧНОГО ЗАХИСТУ ІНФОРМАЦІЇ, АВТОМАТИЗАЦІЯ ЇЇ ОБРОБКИ»</p> <p>Спеціальність: <u>125 «Кібербезпека»</u> Галузь знань: <u>12 «Інформаційні технології»</u> Рівень вищої освіти - перший (бакалаврський)</p>	Шифр документа	СМЯ НАУ ОПП 09.01.10 – 04 - 2021
		стор. 2 з 31	

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 університету
протокол № _____

від «__» _____ 2021 р.

Голова НМР НАУ
проректор з навчальної роботи

_____ (Полухін А.В.)

ПОГОДЖЕНО

Вченою радою Факультету кібербезпеки,
комп'ютерної та програмної інженерії

протокол № _____

від «__» _____ 2021 р.

Голова Вченої ради факультету кібербезпеки,
комп'ютерної та програмної інженерії

_____ (_____)

ПОГОДЖЕНО

Кафедрою засобів захисту інформації

протокол засідання № _____

від «__» _____ 2021 р.

Завідувач кафедри

_____ (_____)

ПОГОДЖЕНО


Студентською радою факультету
кібербезпеки, комп'ютерної та
програмної інженерії

протокол № _____

від «__» _____ 2021 р.

Голова Студентської ради факультету
кібербезпеки, комп'ютерної та
програмної інженерії

_____ (_____)

	<p align="center">Система менеджменту якості ОСВІТНЬО-ПРОФЕСІЙНА ПРОГРАМА «СИСТЕМИ ТЕХНІЧНОГО ЗАХИСТУ ІНФОРМАЦІЇ, АВТОМАТИЗАЦІЯ ЇЇ ОБРОБКИ»</p> <p align="center">Спеціальність: <u>125 «Кібербезпека»</u> Галузь знань: <u>12 «Інформаційні технології»</u> Рівень вищої освіти - перший (бакалаврський)</p>	Шифр документа	СМЯ НАУ ОПІ 09.01.10 – 04 - 2021
		стор. 3 з 31	

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)

ВОЙТЕНКО С.Д. – к.т.н., доцент, доцент кафедри засобів захисту інформації Факультету кібербезпеки, комп'ютерної та програмної інженерії

_____ (підпис)

(П.І.Б. здобувача вищої освіти)

(підпис здобувача вищої освіти)

ЗОВНІШНІЙ СТЕЙКХОЛДЕР

Толюпа С.В. – д.т.н., професор, професор кафедри кібербезпеки та захисту інформації Факультету інформаційних технологій Київського національного університету імені Тараса Шевченка.

_____ (підпис)

Рецензії, відгуки зовнішніх стейкхолдерів (додаються).

Рівень документа – 3б

Плановий термін між ревізіями – 1 рік

Контрольний примірник



Система менеджменту якості
ОСВІТНЬО-ПРОФЕСІЙНА ПРОГРАМА
«СИСТЕМИ ТЕХНІЧНОГО ЗАХИСТУ ІНФОРМАЦІЇ,
АВТОМАТИЗАЦІЯ ЇЇ ОБРОБКИ»
Спеціальність: 125 «Кібербезпека»
Галузь знань: 12 «Інформаційні технології»
Рівень вищої освіти - перший (бакалаврський)

Шифр
документа

СМЯ НАУ ОПП
09.01.10 – 04 - 2021

стор. 4 з 31

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 18.01.2017 сертифікат серія НД-II № 1181256
1.6.	Період акредитації	До 01.07.2022 р.
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. 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). Умови вступу визначаються Правилами прийому до НАУ, затвердженими вченою радою Університету.
1.9.	Форма навчання	Інституційна з елементами дистанційної: очна, заочна.
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.	<p>Ціллю ОПП «Системи технічного захисту інформації, автоматизація її обробки» є підготовка висококваліфікованих 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.</p> <p>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.</p>
------	---

Розділ 3. Характеристика освітньо-професійної програми

3.1	Предметна область (об'єкт діяльності, теоретичний зміст)	<p>Об'єкт діяльності: системи та комплекси технічного захисту інформації на об'єктах інформаційної діяльності; системи та комплекси створення, обробки, передачі, зберігання, знищення, захисту та відображення даних (інформаційних потоків).</p> <p>Теоретичний зміст предметної області: методи та засоби технічного захисту інформації, технології створення, обробки, передачі, приймання, знищення, відображення, захисту (кіберзахисту) інформаційних ресурсів.</p>
3.2.	Орієнтація освітньо-професійної програми	<p>Програма має прикладну орієнтацію.</p> <p>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.</p>
3.3.	Основний фокус освітньо-професійної програми та спеціалізації (за наявності)	<p>Спеціальна освіта та професійна підготовка в галузі 12 – Інформаційні технології за спеціальністю 125 – Кібербезпека.</p> <p>Ключові слова: технічний захист інформації, інформаційна та/або кібербезпека, захист інформації.</p>
3.4.		<p>Освітньо-професійна програма передбачає:</p> <ul style="list-style-type: none">– обов'язкове проходження переддипломної практики;– застосування законодавчої, нормативно-



Особливості освітньо-професійної програми

правової бази України та вимог відповідних міжнародних стандартів і практик щодо здійснення професійної діяльності;

– застосування практичних навичок у сфері технічного захисту інформації;

– використання принципів супроводу систем та комплексів інформаційної та/або кібербезпеки;

– використання теорії, моделей та принципів управління доступом до інформаційних ресурсів;

– застосування теорії систем управління інформаційною та/або кібербезпекою;

– практичного використання методів та засобів виявлення закладних пристроїв, виявлення та локалізації каналів витоку інформації;

– застосування методів та засобів виявлення, управління та ідентифікації ризиків;

– методів та засобів оцінювання та забезпечення необхідного рівня захищеності інформації;

– практичного використання методів та засобів технічного та криптографічного захисту інформації;

– застосування сучасних інформаційно-комунікаційних технологій;

– використання сучасного програмно-апаратного забезпечення інформаційно-комунікаційних технологій;

– практичного використання автоматизованих систем проектування.

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)	<p><i>Методи, засоби та технології:</i> 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. Методи, методики, інформаційно-комунікаційні технології та інші технології забезпечення інформаційної та/або кібербезпеки. 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.</p> <p><i>Технології</i> 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.</p>
------	--	---



5.1.	Викладання та навчання (методи, методики, технології, інструменти та обладнання)	<i>Інструменти та обладнання:</i> матеріали, апаратно-програмні комплекси та засоби лінійного/просторового захисту інформації, комбіновані системи контролю та управління доступом, проектування систем технічного захисту інформації та контролю процесів інформаційної та/ або кібербезпеки; сучасне програмно-апаратне забезпечення інформаційно-комунікаційних технологій; 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 проєктів, 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 організувати 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)



6.2.	Загальні компетентності (ЗК)	<p>суспільства та необхідність його сталого розвитку, верховенства права, прав і свобод людини і громадянина в Україні.</p> <p>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.</p>
6.3.	Фахові компетентності (ФК)	<p>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.</p> <p>ФК2. Здатність до використання інформаційно-комунікаційних технологій, сучасних методів і моделей інформаційної та/або кібербезпеки.</p> <p>ФК3. Здатність до використання програмних, апаратних та програмно-апаратних комплексів засобів захисту інформації на об'єктах інформаційної діяльності та в інформаційно-телекомунікаційних (автоматизованих) системах.</p> <p>ФК4. Здатність забезпечувати неперервність бізнесу згідно встановленої політики інформаційної та/або кібербезпеки.</p> <p>ФК5. Здатність оцінювати захищеність інформації усіх видів, що циркулює на об'єктах інформаційної діяльності.</p> <p>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.</p> <p>ФК7. Здатність забезпечувати захист інформації, що обробляється в інформаційно-телекомунікаційних (автоматизованих) системах з метою реалізації встановленої політики інформаційної та/або кібербезпеки.</p> <p>ФК8. Здатність впроваджувати та забезпечувати функціонування комплексних систем захисту інформації (комплекси нормативно-правових,</p>



6.3.	Фахові компетентності (ФК)	<p>організаційних та технічних засобів і методів, процедур, практичних прийомів та ін.).</p> <p>ФК9. Здатність здійснювати процедури управління інцидентами, проводити розслідування, надавати їм оцінку.</p> <p>ФК10. Здатність застосовувати методи та засоби криптографічного та технічного захисту інформації на об'єктах інформаційної діяльності.</p> <p>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.</p> <p>ФК12. Здатність виявляти та блокувати канали витоку інформації, методи несанкціонованого доступу до інформації, джерел і способів дестабілізуючого впливу на інформацію, здійснювати пошук закладних пристроїв.</p> <p>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.</p> <p>ФК14. Здатність виконувати моніторинг процесів функціонування інформаційних, інформаційно-телекомунікаційних (автоматизованих) систем згідно встановленої політики інформаційної та/або кібербезпеки.</p> <p>ФК15. Здатність використовувати теоретичні знання та практичні навички з підготовки технічної документації.</p> <p>ФК16. Здатність здійснювати професійну діяльність на основі впровадженої системи управління інформаційною та/або кібербезпекою.</p>
Розділ 7. Програмні результати навчання		
7.1.	Програмні результати навчання (ПРН)	<p>ПРН1. Застосовувати знання державної та іноземних мов з метою забезпечення ефективності професійної комунікації.</p> <p>ПРН2. Організувати власну професійну діяльність, обирати оптимальні методи та способи розв'язування складних спеціалізованих задач та практичних проблем у професійній діяльності, оцінювати їхню ефективність.</p> <p>ПРН3. Використовувати результати самостійного пошуку, аналізу та синтезу інформації з різних джерел для ефективного рішення спеціалізованих</p>



	<p>7.1. Програмні результати навчання (ПРН)</p>	<p>задач професійної діяльності.</p> <p>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.</p> <p>ПРН5. Адаптуватися в умовах частотої зміни технологій професійної діяльності, прогнозувати кінцевий результат.</p> <p>ПРН6. Критично осмислювати основні теорії, принципи, методи і поняття у навчанні та професійній діяльності.</p> <p>ПРН7. Діяти на основі законодавчої та нормативно-правової бази України та вимог відповідних стандартів, у тому числі міжнародних в галузі інформаційної та /або кібербезпеки.</p> <p>ПРН8. Готувати пропозиції до нормативних актів щодо забезпечення інформаційної та /або кібербезпеки.</p> <p>ПРН9. Впроваджувати процеси, що базуються на національних та міжнародних стандартах, виявлення, ідентифікації, аналізу та реагування на інциденти інформаційної та/або кібербезпеки.</p> <p>ПРН10. Виконувати аналіз та декомпозицію інформаційно-телекомунікаційних систем.</p> <p>ПРН11. Виконувати аналіз зв'язків між інформаційними процесами на віддалених обчислювальних системах.</p> <p>ПРН12. Розробляти моделі загроз та порушника.</p> <p>ПРН13. Аналізувати проекти інформаційно-телекомунікаційних систем базуючись на стандартизованих технологіях та протоколах передачі даних.</p> <p>ПРН14. Вирішувати завдання захисту програм та інформації, що обробляється в інформаційно-телекомунікаційних системах програмно-апаратними засобами та давати оцінку результативності якості прийнятих рішень.</p> <p>ПРН15. Використовувати сучасне програмно-апаратне забезпечення інформаційно-комунікаційних технологій.</p> <p>ПРН16. Реалізовувати комплексні системи захисту інформації в автоматизованих системах (АС) організації (підприємства) відповідно до вимог нормативно-правових документів.</p> <p>ПРН17. Забезпечувати процеси захисту та функціонування інформаційно-телекомунікаційних (автоматизованих) систем на</p>
--	---	---



7.1.	Програмні результати навчання (ПРН)	<p>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.</p> <p>ПРН18. Використовувати програмні та програмно-апаратні комплекси захисту інформаційних ресурсів.</p> <p>ПРН19. Застосовувати теорії та методи захисту для забезпечення безпеки інформації в інформаційно-телекомунікаційних системах.</p> <p>ПРН20. Забезпечувати функціонування спеціального програмного забезпечення, щодо захисту інформації від руйнуючих програмних впливів, руйнуючих кодів в інформаційно-телекомунікаційних системах.</p> <p>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.</p> <p>ПРН22. Вирішувати задачі управління процедурами ідентифікації, автентифікації, авторизації процесів і користувачів в інформаційно телекомунікаційних системах згідно встановленої політики інформаційної і/або кібербезпеки.</p> <p>ПРН23. Реалізовувати заходи з протидії отриманню несанкціонованого доступу до інформаційних ресурсів і процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах.</p> <p>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).</p> <p>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.</p> <p>ПРН26. Впроваджувати заходи та забезпечувати</p>
------	-------------------------------------	---



7.1.	Програмні результати навчання (ПРН)	<p>реалізацію процесів попередження отриманню несанкціонованого доступу і захисту інформаційних, інформаційно-телекомунікаційних (автоматизованих) систем на основі еталонної моделі взаємодії відкритих систем.</p> <p>ПРН27. Вирішувати задачі захисту потоків даних в інформаційних, інформаційно-телекомунікаційних (автоматизованих) системах.</p> <p>ПРН28. 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.</p> <p>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.</p> <p>ПРН30. Здійснювати оцінювання можливості несанкціонованого доступу до елементів інформаційно-телекомунікаційних систем.</p> <p>ПРН31. Застосовувати теорії та методи захисту для забезпечення безпеки елементів інформаційно-телекомунікаційних систем.</p> <p>ПРН32. Вирішувати задачі управління процесами відновлення штатного функціонування інформаційно-телекомунікаційних систем з використанням процедур резервування згідно встановленої політики безпеки.</p> <p>ПРН33. Вирішувати задачі забезпечення безперервності бізнес процесів організації на основі теорії ризиків.</p> <p>ПРН34. Приймати участь у розробці та впровадженні стратегії інформаційної безпеки та\або кібербезпеки відповідно до цілей і завдань організації.</p> <p>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.</p> <p>ПРН36. Виявляти небезпечні сигнали технічних засобів.</p> <p>ПРН37. Вимірювати параметри небезпечних та</p>
------	-------------------------------------	--



7.1.	Програмні результати навчання (ПРН)	<p>задає 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.</p> <p>ПРН38. Інтерпретувати результати проведення спеціальних вимірювань з використанням технічних засобів, контролю характеристик інформаційно-телекомунікаційних систем відповідно до вимог нормативних документів системи технічного захисту інформації.</p> <p>ПРН39. Проводити атестацію (спираючись на облік та обстеження) режимних територій (зон), приміщень тощо в умовах додержання режиму секретності із фіксуванням результатів у відповідних документах.</p> <p>ПРН40. Виявляти закладні пристрої несанкціонованого отримання інформації.</p> <p>ПРН41. Забезпечувати неперервність процесу ведення журналів реєстрації подій та інцидентів на основі автоматизованих процедур.</p> <p>ПРН42. Впроваджувати процеси виявлення, ідентифікації, аналізу та реагування на інциденти інформаційної і/або кібербезпеки.</p> <p>ПРН43. Застосовувати національні та міжнародні регулюючі акти в сфері інформаційної безпеки та/або кібербезпеки для розслідування інцидентів.</p> <p>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.</p> <p>ПРН45. Застосовувати різні класи політик інформаційної безпеки та/або кібербезпеки, що базуються на ризик-орієнтованому контролі доступу до інформаційних активів.</p> <p>ПРН46. Здійснювати аналіз та мінімізацію ризиків обробки інформації в інформаційно-телекомунікаційних системах.</p> <p>ПРН47. Вирішувати задачі захисту інформації, що обробляється в інформаційно-телекомунікаційних системах з використанням сучасних методів та засобів криптографічного захисту інформації.</p> <p>ПРН48. Виконувати впровадження та підтримку систем виявлення вторгнень та використовувати компоненти криптографічного захисту для</p>
------	-------------------------------------	--




7.1.	Програмні результати навчання (ПРН)	<p>забезпечення необхідного рівня захищеності інформації в інформаційно-телекомунікаційних системах.</p> <p>ПРН49. Забезпечувати належне функціонування системи моніторингу інформаційних ресурсів і процесів в інформаційно-телекомунікаційних системах.</p> <p>ПРН50. Забезпечувати функціонування програмних та програмно-апаратних комплексів виявлення вторгнень різних рівнів та класів (статистичних, сигнатурних, статистично-сигнатурних).</p> <p>ПРН51. Підтримувати працездатність та забезпечувати конфігурування систем виявлення вторгнень в інформаційно-телекомунікаційних системах.</p> <p>ПРН52. Використовувати інструментарій для моніторингу процесів в інформаційно-телекомунікаційних системах.</p> <p>ПРН53. Вирішувати задачі аналізу програмного коду на наявність можливих загроз.</p> <p>ПРН54. Усвідомлювати цінності громадянського (вільного демократичного) суспільства та необхідність його сталого розвитку, верховенства права, прав і свобод людини і громадянина в Україні.</p> <p>ПРН55. Визначати відомості, які відносяться до інформації з обмеженим доступом, організувати допуск та доступ персоналу до інформації з обмеженим доступом згідно чинного законодавства та встановленої політики інформаційної та/або кібербезпеки.</p> <p>ПРН56. Організувати внутрішньо-об'єктовий та пропускний режими на підприємстві.</p> <p>ПРН57. Вирішувати задачі забезпечення та супроводу комплексу технічного захисту інформації на об'єкті інформаційної діяльності.</p> <p>ПРН58. Оцінювати захищеність інформації на об'єктах інформаційної діяльності.</p> <p>ПРН59. Скласти звітність та вести технічну документацію.</p>
Розділ 8. Ресурсне забезпечення реалізації програми		
8.1.	Кадрове забезпечення	<p>Кадрове забезпечення відповідає ліцензійним вимогам.</p> <p>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</p>



8.1.		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	<p>Матеріально-технічна база випускової кафедри засобів захисту інформації дозволяє забезпечити підготовку фахівців на першому (бакалаврському) рівні вищої освіти за ОПП:</p> <ul style="list-style-type: none">– забезпеченість комп'ютерними робочими місцями та прикладними комп'ютерними 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). <p>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.</p>
8.3.	Інформаційне та навчально-методичне забезпечення	<p>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.</p> <p>Всі студенти забезпечені підручниками та навчальними посібниками з компонентів ОПП.</p> <p>Відповідне інформаційне та навчально-методичне забезпечення розташоване на освітніх платформах Google Classroom, Moodle (Modular</p>



8.3.	Інформаційне та навчально-методичне забезпечення	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 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+K1 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.

	<p align="center">Система менеджменту якості ОСВІТНЬО-ПРОФЕСІЙНА ПРОГРАМА «СИСТЕМИ ТЕХНІЧНОГО ЗАХИСТУ ІНФОРМАЦІЇ, АВТОМАТИЗАЦІЯ ЇЇ ОБРОБКИ» Спеціальність: <u>125 «Кібербезпека»</u> Галузь знань: <u>12 «Інформаційні технології»</u> Рівень вищої освіти - перший (бакалаврський)</p>	Шифр документа	СМЯ НАУ ОПП 09.01.10 – 04 - 2021
		стор. 18 з 31	

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				
OK1.	Історія української державності та культури	3.0	Екзамен	1
OK2.	Ділова українська мова	3.0	Екзамен	2
OK3.	Філософія	3.5	Екзамен	4
OK4.	Фахова іноземна мова	4.5	Залік, екзамен	1, 2
OK5.	Фізичне виховання та самовдосконалення	3.0	Залік	2
OK6.	Вища математика	14.0	Залік, екзамен	1, 2, 3
OK7.	Фізика	10.5	Залік, екзамен	1, 2
OK8.	Інформаційні технології	11.5	Залік, екзамен	1, 2
OK9.	Основи автоматизованої обробки інформації	6.5	Залік	1, 2
OK10.	Основи кібербезпеки	4.5	Залік	1
OK11.	Апаратне забезпечення інформаційних систем	5.0	Залік, екзамен	3, 4
OK12.	Курсова робота з Апаратного забезпечення інформаційних систем	1.0	Залік	3
OK13.	Виявлення закладних пристроїв на об'єктах інформаційної діяльності	4.0	Екзамен	3
OK14.	Основи теорії кіл, сигналів та процесів в системах технічного захисту інформації	6.5	Залік, екзамен	3, 4
OK15.	Курсова робота з Основ теорії кіл, сигналів та процесів в системах технічного захисту інформації	1.0	Залік	4
OK16.	Компонентна база засобів технічного захисту інформації	4.0	Екзамен	3
OK17.	Безпека інформаційно-комунікаційних систем	4.0	Залік	4
OK18.	Схемотехніка пристроїв технічного захисту інформації	4.5	Залік	4
OK19.	Засоби передавання сигналів в системах технічного захисту інформації	4.5	Екзамен	5
OK20.	Курсова робота з Засобів передавання сигналів в системах технічного захисту інформації	1.0	Залік	5




Система менеджменту якості
ОСВІТНЬО-ПРОФЕСІЙНА ПРОГРАМА
«СИСТЕМИ ТЕХНІЧНОГО ЗАХИСТУ ІНФОРМАЦІЇ,
АВТОМАТИЗАЦІЯ ЇЇ ОБРОБКИ»
Спеціальність: 125 «Кібербезпека»
Галузь знань: 12 «Інформаційні технології»
Рівень вищої освіти - перший (бакалаврський)

Шифр
документа

СМЯ НАУ ОПП
09.01.10 – 04 - 2021


стор. 19 з 31

1	2	3	4	5
OK21.	Авіаційна безпека та кібербезпека авіаційних інформаційних систем	10.5	Залік, екзамен	5, 6, 7
OK22.	Поля і хвилі в системах технічного захисту інформації	4.5	Екзамен	5
OK23.	Захищені комп'ютерні системи та мережі**	8.0	Залік, екзамен	5, 6
OK24.	Управління інформаційною безпекою	3.0	Екзамен	6
OK25.	Курсова робота з Управління інформаційною безпекою	1.0	Залік	6
OK26.	Прикладна криптологія	7.5	Екзамен	6, 7
OK27.	Курсова робота з Прикладної криптології	1.0	Залік	7
OK28.	Операційні системи та технології їх захисту***	7.0	Залік, екзамен	6, 7
OK29.	Системи технічного захисту інформації	3.5	Екзамен	7
OK30.	Засоби приймання та обробки сигналів в системах технічного захисту інформації	3.5	Залік	7
OK31.	Комплексні системи захисту інформації	4.0	Екзамен	8
OK32.	Методи та засоби технічного захисту інформації	4.5	Екзамен	8
OK33.	Проектування систем технічного захисту інформації	3.0	Екзамен	8
OK34.	Цифрова обробка сигналів	3.0	Екзамен	8
OK35.	Фахова ознайомлювальна практика	3.0	Залік	2
OK36.	Комп'ютерна практика	3.0	Залік	4
OK37.	Технологічна практика	3.0	Залік	6
OK38.	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 вибірових компонент*		60 кредитів ЄКТС		
Загальний обсяг освітньо-професійної програми		240 кредитів ЄКТС		

	<p align="center">Система менеджменту якості ОСВІТНЬО-ПРОФЕСІЙНА ПРОГРАМА «СИСТЕМИ ТЕХНІЧНОГО ЗАХИСТУ ІНФОРМАЦІЇ, АВТОМАТИЗАЦІЯ ЇЇ ОБРОБКИ» Спеціальність: <u>125 «Кібербезпека»</u> Галузь знань: <u>12 «Інформаційні технології»</u> Рівень вищої освіти - перший (бакалаврський)</p>	Шифр документа	СМЯ НАУ ОПП 09.01.10 – 04 - 2021
		стор. 20 з 31	

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				
ОК3.	Філософія	3.5	Екзамен	2
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	4.0	Екзамен	1
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

	Система менеджменту якості ОСВІТНЬО-ПРОФЕСІЙНА ПРОГРАМА «СИСТЕМИ ТЕХНІЧНОГО ЗАХИСТУ ІНФОРМАЦІЇ, АВТОМАТИЗАЦІЯ ЇЇ ОБРОБКИ» Спеціальність: <u>125 «Кібербезпека»</u> Галузь знань: <u>12 «Інформаційні технології»</u> Рівень вищої освіти - перший (бакалаврський)	Шифр документа	СМЯ НАУ ОПП 09.01.10 – 04 - 2021
		стор. 21 з 31	

1	2	3	4	5
OK28.	Операційні системи та технології їх захисту***	7.0	Залік, екзамен	4, 5
OK29.	Системи технічного захисту інформації	3.5	Екзамен	5
OK30.	Засоби приймання та обробки сигналів в системах технічного захисту інформації	3.5	Залік	5
OK31.	Комплексні системи захисту інформації	4.0	Екзамен	6
OK32.	Методи та засоби технічного захисту інформації	4.5	Екзамен	6
OK33.	Проектування систем технічного захисту інформації	3.0	Екзамен	6
OK34.	Цифрова обробка сигналів	3.0	Екзамен	6
<i>Практична підготовка</i>				
OK36.	Комп'ютерна практика	3.0	Залік	2
OK37.	Технологічна практика	3.0	Залік	4
OK38.	Кваліфікаційна робота	7.5	Захист	6
Загальний обсяг обов'язкових компонент:		120 кредитів ЄКТС		
Вибіркові компоненти*				
BK1.		4.0	Залік	
BK2.		4.0	Залік	
BK3.		4.0	Залік	
---	----	---	---	---
BK15.		4.0	Залік	
Загальний обсяг вибірових 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.

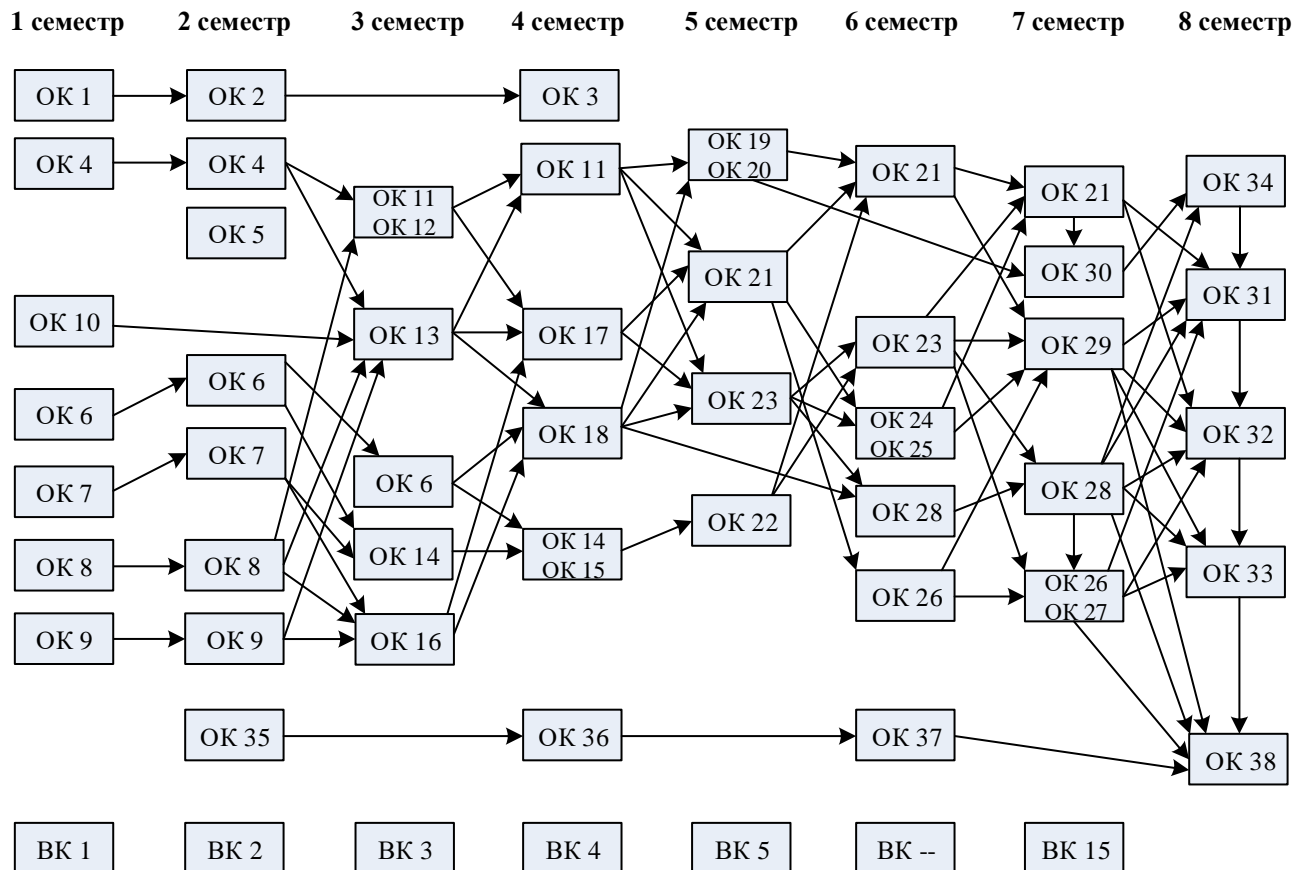
Вибіркові компоненти обираються здобувачами вищої освіти із каталогів рекомендованих та альтернативних вибірових дисциплін.


** Офіційний сертифікований курс Cisco Networking Academy.

*** Офіційний сертифікований курс Network Development Group.



2.3. Структурно-логічна схема освітньо-професійної програми



	<p align="center">Система менеджменту якості ОСВІТНЬО-ПРОФЕСІЙНА ПРОГРАМА «СИСТЕМИ ТЕХНІЧНОГО ЗАХИСТУ ІНФОРМАЦІЇ, АВТОМАТИЗАЦІЯ ЇЇ ОБРОБКИ»</p> <p>Спеціальність: <u>125 «Кібербезпека»</u> Галузь знань: <u>12 «Інформаційні технології»</u> Рівень вищої освіти - перший (бакалаврський)</p>	Шифр документа	СМЯ НАУ ОПП 09.01.10 – 04 - 2021
		стор. 23 з 31	

3. Форма атестації здобувачів вищої освіти

Форми атестації здобувачів вищої освіти	Атестація здобувачів ОС «Бакалавр» здійснюється у формі публічного захисту кваліфікаційної роботи і завершується видачею документу встановленого зразку про присудження їм освітнього ступеня «Бакалавр» із присвоєнням освітньої кваліфікації: Бакалавр з кібербезпеки, за спеціальністю 125 «Кібербезпека».
Вимоги до кваліфікаційної роботи	<p>Кваліфікаційна робота бакалавра повинна бути самостійною логічно завершеною теоретичною або експериментальною науково-дослідною роботою, пов'язаною з вирішенням актуальної науково-технічної або іншої проблеми у сфері Кібербезпеки.</p> <p>Кваліфікаційна робота бакалавра не повинна містити академічного плагіату, у тому числі некоректних текстових запозичень, фабрикації та фальсифікації.</p> <p>Кваліфікаційна робота має бути оприлюднена на офіційному сайті Університету або його структурного підрозділу, або у репозитарії.</p> <p>Оприлюднення кваліфікаційних робіт, що містять інформацію з обмеженим доступом, здійснювати відповідно до вимог законодавства.</p>
Вимоги до публічного захисту (демонстрації)	<p>Публічний захист кваліфікаційної бакалаврської роботи відбувається на засіданні екзаменаційної комісії.</p> <p>Порядок захисту передбачає представлення здобувача й поданих документів; виступ здобувача; відповіді здобувача на запитання членів екзаменаційної комісії та присутніх. Виступ здобувача має супроводжуватись презентацією.</p>



Система менеджменту якості
ОСВІТНЬО-ПРОФЕСІЙНА ПРОГРАМА
«СИСТЕМИ ТЕХНІЧНОГО ЗАХИСТУ ІНФОРМАЦІЇ,
АВТОМАТИЗАЦІЯ ЇЇ ОБРОБКИ»
Спеціальність: 125 «Кібербезпека»
Галузь знань: 12 «Інформаційні технології»
Рівень вищої освіти - перший (бакалаврський)

Шифр
документа

СМЯ НАУ ОПП
09.01.10 – 04 - 2021

стор. 24 з 31

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	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	ОК 34	ОК 35	ОК 36	ОК 37	ОК 38	БК 1*	БК 2*	БК --	БК 15*			
	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			
ПК1	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+		
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			



Система менеджменту якості
 ОСВІТНЬО-ПРОФЕСІЙНА ПРОГРАМА
 «СИСТЕМИ ТЕХНІЧНОГО ЗАХИСТУ ІНФОРМАЦІЇ,
 АВТОМАТИЗАЦІЯ ЇЇ ОБРОБКИ»
 Спеціальність: 125 «Кібербезпека»
 Галузь знань: 12 «Інформаційні технології»
 Рівень вищої освіти - перший (бакалаврський)

Шифр
 документа

СМЯ НАУ ОПП
09.01.10 – 04 - 2021

стор. 25 з 31

ФК14			+	+				+	+	+	+				+			+	+			+	+		+	+	+	+	+							
ФК15		+	+			+	+	+	+	+	+	+	+	+	+	+	+	+			+	+	+	+	+		+	+	+	+						
ФК16								+		+					+			+			+	+														

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



Система менеджменту якості
ОСВІТНЬО-ПРОФЕСІЙНА ПРОГРАМА
«СИСТЕМИ ТЕХНІЧНОГО ЗАХИСТУ ІНФОРМАЦІЇ,
АВТОМАТИЗАЦІЯ ЇЇ ОБРОБКИ»
Спеціальність: 125 «Кібербезпека»
Галузь знань: 12 «Інформаційні технології»
Рівень вищої освіти - перший (бакалаврський)

Шифр
документа

СМЯ НАУ ОПП
09.01.10 – 04 - 2021

стор. 26 з 31

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	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	ОК 34	ОК 35	ОК 36	ОК 37	ОК 38	ВК 1*	ВК 2*	ВК --	ВК 15*													
	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								+	+	+					+		+	+	+		+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+				



Система менеджменту якості
 ОСВІТНЬО-ПРОФЕСІЙНА ПРОГРАМА
 «СИСТЕМИ ТЕХНІЧНОГО ЗАХИСТУ ІНФОРМАЦІЇ,
 АВТОМАТИЗАЦІЯ ЇЇ ОБРОБКИ»
 Спеціальність: 125 «Кібербезпека»
 Галузь знань: 12 «Інформаційні технології»
 Рівень вищої освіти - перший (бакалаврський)


Шифр
 документа

СМЯ НАУ ОПП
09.01.10 – 04 - 2021

стор. 28 з 31

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 вибірових дисциплін Університету мають також забезпечувати визначені програмні результати навчання (ПРН). Кількість вибірових компонент визначається виходячи із загального обсягу вибірових компонент (кредитів) освітньої програми.


	<p align="center">Система менеджменту якості ОСВІТНЬО-ПРОФЕСІЙНА ПРОГРАМА «СИСТЕМИ ТЕХНІЧНОГО ЗАХИСТУ ІНФОРМАЦІЇ АВТОМАТИЗАЦІЯ ЇЇ ОБРОБКИ» - Спеціальність: <u>125 «Кібербезпека»</u> Галузь знань: <u>12 «Інформаційні технології»</u> Рівень вищої освіти - перший (бакалаврський)</p>	Шифр документа	СМЯ НАУ ОПП 09.01.10 – 01 - 2020
		стор. 29 з 31	

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.

	<p align="center">Система менеджменту якості ОСВІТНЬО-ПРОФЕСІЙНА ПРОГРАМА «СИСТЕМИ ТЕХНІЧНОГО ЗАХИСТУ ІНФОРМАЦІЇ, АВТОМАТИЗАЦІЯ ЇЇ ОБРОБКИ» - Спеціальність: <u>125 «Кібербезпека»</u> - Галузь знань: <u>12 «Інформаційні технології»</u> Рівень вищої освіти - перший (бакалаврський)</p>	Шифр документа	СМЯ НАУ ОПП 09.01.10 – 01 - 202
		стор. 31 з 31	

(Ф 03.02 – 04)

АРКУШ РЕЄСТРАЦІЇ РЕВІЗІЇ

№ пор.	Прізвище ім'я по-батькові	Дата ревізії	Підпис	Висновок щодо адекватності

(Ф 03.02 – 03)

АРКУШ ОБЛІКУ ЗМІН

№ зміни	№ листа (сторінки)				Підпис особи, яка внесла зміну	Дата внесення зміни	Дата введення зміни
	Зміненого	Заміненого	Нового	Анульованого			

(Ф 03.02 – 32)

УЗГОДЖЕННЯ ЗМІН

	Підпис	Ініціали, прізвище	Посада	Дата
Розробник				
Узгоджено				
Узгоджено				
Узгоджено				
Узгоджено				