КИЇВСЬКИЙ СТОЛИЧНИЙ УНІВЕРСИТЕТ
ІМЕНІ БОРИСА ГРІНЧЕНКА

ЗАТВЕРДЖЕНО
Протокол засідання Вченої ради
Київського університету імені Бориса Грінченка
від 23.11.2017 р., протокол №11

ЗМІНИ ЗАТВЕРДЖЕНО
Протокол засідання Вченої ради
Факультету інформаційних технологій та управління
Київського університету імені Бориса Грінченка
від 27.08.2019 р., протокол №8

ЗМІНИ ЗАТВЕРДЖЕНО
Протокол засідання Вченої ради
Факультету інформаційних технологій та математики
Київського столичного університету
імені Бориса Грінченка
від 19.04.2023 р., протокол №3

ОСВІТНЬО-ПРОФЕСІЙНА ПРОГРАМА
125.00.01 Безпека інформаційних і комунікаційних систем

першого (бакалаврського) рівня вищої освіти

Галузь знань:	12 Інформаційні технології
Спеціальність:	125 Кібербезпека та захист інформації
Кваліфікація:	Бакалавр з кібербезпеки та захисту інформації

Введено в дію з 01.09.2023 р.
(наказ від 27.04.2023 р. № 233)

Київ – 2023 р.

2017, 2018 р

КИЇВСЬКИЙ УНІВЕРСИТЕТ ІМЕНІ БОРИСА ГРІНЧЕНКА

ЗАТВЕРДЖЕНО
Рішенням Вченої ради Київського
університету імені Бориса Грінченка
«23» жовтня 2017 р., протокол № 11
Голова вченої ради
_____ В. О. Огнев'юк

ОСВІТНЬО-ПРОФЕСІЙНА ПРОГРАМА
125.00.01 Безпека інформаційних і комунікаційних систем першого (бакалаврського) рівня вищої освіти

Галузь знань: 12 Інформаційні технології

Спеціальність: 125 Кібербезпека

Кваліфікація: бакалавр з кібербезпеки

3439 фахівець із організації інформаційної безпеки

Введено в дію з «01» вересня 2018 р.
(наказ від «24» листопада 2017 р. № 762)

Київ 2018

+Smart 3 2019 року

КИЇВСЬКИЙ УНІВЕРСИТЕТ ІМЕНІ БОРИСА ГРІНЧЕНКА

ЗАТВЕРДЖЕНО
Рішенням Вченої ради
Факультету інформаційних технологій
та управління
Київського університету імені Бориса Грінченка
«27» серпня 2019 р., протокол №8
Голова вченої ради, декан
_____ А.В. Михацька

ЗМІНИ ДО ОСВІТНЬО-ПРОФЕСІЙНОЇ ПРОГРАМИ
125.00.01 Безпека інформаційних і комунікаційних систем першого (бакалаврського) рівня вищої освіти

Галузь знань: **12 Інформаційні технології**

Спеціальність: **125 Кібербезпека**

Кваліфікація: **бакалавр з кібербезпеки**

3439 фахівець із організації інформаційної безпеки

Введено в дію з «01» вересня 2019 р.
(наказ від «30» серпня 2019 р. №509)

Київ 2019

КИЇВСЬКИЙ УНІВЕРСИТЕТ ІМЕНІ БОРИСА ГРІНЧЕНКА

«ЗАТВЕРДЖЕНО»
Рішенням Вченої ради Факультету
інформаційних технологій та математики
від 19 квітня 2023 р., протокол №3

Голова Вченої ради, декан
_____ Оксана ЛИТВИН

ЗМІНИ ДО ОСВІТНЬО-ПРОФЕСІЙНОЇ ПРОГРАМИ

125.00.01 Безпека інформаційних і комунікаційних систем

першого (бакалаврського) рівня вищої освіти

Галузь знань:	12 Інформаційні технології
Спеціальність:	125 Кібербезпека
Кваліфікація:	Бакалавр з кібербезпеки

Введено в дію з 01.09.2023
(наказ від 27.04.2023 № 223)

Київ – 2023

ЛИСТ-ПОГОДЖЕННЯ
змін до опису освітньо-професійної програми
«Безпека інформаційних і комунікаційних систем»
першого (бакалаврського) рівня вищої освіти

Кафедра інформаційної та кібернетичної безпеки
імені професора Володимира Бурячка
Протокол від 03.04. 2023 № 3
Завідувач кафедри _____ Павло СКЛАДАННИЙ

Вчена рада Факультету інформаційних технологій та математики
Протокол від 19.04. 2023 № 3
Голова Вченої ради _____ Оксана ЛИТВИН

Науково-методичний центр стандартизації та якості освіти
Завідувач _____ Євген АНТИПІН
17.04. 2023 р.

Проректор з науково-методичної та навчальної роботи
_____ Олексій ЖИЛЬЦОВ
17.04. 2023 р.

Погоджено робочою групою у складі:

Платоненко А.В. кандидат технічних наук, доцент, доцент кафедри інформаційної та кібернетичної безпеки імені професора Володимира Бурячка (керівник робочої групи);

Коршун Наталія Володимирівна, доктор технічних наук, професор, професор кафедри інформаційної та кібернетичної безпеки імені професора Володимира Бурячка;

Бессалов Анатолій Володимирович, доктор технічних наук, професор, професор кафедри інформаційної та кібернетичної безпеки імені професора Володимира Бурячка.

Актуалізовано:

Дата перегляду	27.08.2019	19.04.2023		
Підпис				
ПІБ гаранта ОП				

ПЕРЕДМОВА

Освітньо-професійна програма «Безпека інформаційних і комунікаційних систем» розроблена у відповідності до Стандарту вищої освіти України зі спеціальності 125 Кібербезпека першого (бакалаврського) рівня, затвердженого наказом Міністерства освіти і науки України від 04.10.2018 р. № 1074

Зміни до освітньо-професійної програми зумовлені необхідністю розширення компетентностей майбутніх фахівців в контексті сучасних SMART-технологій, загроз і викликів, побажаннями науково-педагогічних працівників, здобувачів вищої освіти, висловлених під час опитувань та обговорень в процесі реалізації освітньої програми в Університеті Грінченка. Також необхідність у вказаних змінах виявив аналіз відповідних публікацій та потреб громади та влади м. Києва у створенні комфортної та ефективної цифрової інфраструктури, консультацій з стейкхолдерами в різних галузях науки і економіки.

Зміни стосувались об’єктів вивчення та діяльності, змісту і назви окремих фахових дисциплін з метою приведення їх у відповідність до сучасного стану галузі.

Назву дисципліни «Безпека безпровідних, мобільних та хмарних технологій» змінено на «Безпека безпровідних, мобільних, хмарних та SMART- технологій». Змінено назву ВП.2.03 з «Переддипломної» практики на «Виробничу» та змінено кількість кредитів з 6 на 12.

На виконання наказу Міністерства освіти і науки України від 13.01.2022 року №26 «Про зміни, що вносяться до деяких стандартів вищої освіти» (п.1) змінено форму атестації: формою атестації здобувачів першого (бакалаврського) рівня вищої освіти зі спеціальності 125 Кібербезпека галузі знань 12 Інформаційні технології є Єдиний державний кваліфікаційний іспит (ЄДКІ).

У випадку неможливості технічного забезпечення складання ЄДКІ Міністерством освіти і науки України передбачено заміну цього іспиту на Комплексний іспит з кібербезпеки, організацію проведення якого бере на себе університет .

Не підлягали суттєвому перегляду програмні компетентності та результати навчання, ресурсне забезпечення, інші частини характеристик ОПП.

.

1. Профіль освітньої програми

1 – Загальна інформація	
Повна назва вищого навчального закладу та структурного підрозділу	Київський столичний університет імені Бориса Грінченка Факультет інформаційних технологій та математики Кафедра інформаційної та кібернетичної безпеки імені професора Володимира Бурячка
Ступінь вищої освіти та назва кваліфікації мовою оригіналу	Бакалавр з кібербезпеки та захисту інформації
Офіційна назва освітньої програми	125.00.01 Безпека інформаційних та комунікаційних систем
Тип диплому та обсяг освітньої програми	Диплом бакалавра, одиничний, 240 кредитів ЄКТС, термін навчання 3 роки 10 місяців
Наявність акредитації	Національне агентство забезпечення якості вищої освіти. Сертифікат про акредитацію освітньої програми №335 від 26.05.2020. Строк дії сертифікату до 26.05.2025 р.
Цикл/рівень	НРК України – 6 рівень, FQ-EHEA – перший цикл, EQF-LLL – 6 рівень
Передумови	Повна загальна середня освіта
Мова(и) викладання	Українська
Термін дії освітньої програми	Відповідно терміну акредитації
Інтернет-адреса постійного розміщення опису освітньої програми	kubg.edu.ua
2 – Мета освітньої програми	
Забезпечити студентам якісну теоретичну та практичну підготовку у вигляді знань, умінь та навичок за спеціальністю 125 Кібербезпека та захисту інформації для організації та забезпечення інформаційної безпеки на об’єктах інформаційної діяльності.	
3 - Характеристика освітньої програми	
Предметна область	Об’єкти професійної діяльності випускників: – об'єкти інформатизації, включаючи комп'ютерні, автоматизовані, телекомунікаційні, інформаційні, інформаційно-аналітичні, інформаційно-телекомунікаційні системи, інформаційні ресурси і технології; – технології кібербезпеки та захисту інформації; – процеси управління інформаційною та/або кібербезпекою об’єктів, що підлягають захисту; *Цілі навчання:* підготовка фахівців, здатних використовувати і впроваджувати технології інформаційної та/або кібербезпеки, розв’язувати складні задачі у галузі кібербезпеки та захисту інформації. *Теоретичний зміст предметної діяльності*. 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 застосування уразливостей в безпровідних, мобільних, хмарних та *SMART-технологіях* та способи боротьби з ними, методів організації захищеної передачі даних у незахищеному *SMART-середовищі,* засоби спеціального мережевого обладнання для забезпечення безпеки корпоративних мереж; – методів та засобів технічного та криптографічного захисту інформації – сучасних інформаційно-комунікаційних технологій; – сучасного програмно-апаратного забезпечення інформаційно-комунікаційних технологій; – автоматизованих систем проєктування. *Методи, методики та технології:* методи, методики інформаційно-комунікаційні та інші технології забезпечення інформаційної та/або кібербезпеки. *Інструменти та обладнання:* – системи розробки, забезпечення, моніторингу та контролю процесів інформаційної та/ або кібербезпеки; – сучасне програмно-апаратне забезпечення інформаційно-комунікаційних технологій. *Співвідношення обсягів загальної і професійної складових та вибіркової частини:* Обов'язкова частина (180 кредитів, 75 %): – цикл дисциплін гуманітарної та соціально-економічної підготовки (32 кредитів ЄКТС, 960 год.); – цикл дисциплін фундаментальної та природничо-наукової підготовки (28 кредитів ЄКТС, 840 год.); – цикл дисциплін професійної та практичної підготовки за спеціальністю (73 кредити ЄКТС, 2190 год.) та фаховою спеціалізацією (30 кредитів ЄКТС, 900 год.) з написанням 2 курсових робіт у 3 та 5 семестрах та Єдиного державного кваліфікаційного іспиту (ЄДКІ) / Комплексний іспит з кібербезпеки Частка виробничої (4 семестр), виробничої (технологічної) (6 семестр) та виробничої практик (8 семестр): 21 кредитів ЄКТС, 630 годин. Вибіркова частина (60 кредитів, 25 %). З них спеціалізований блок навчальних дисциплін – 60 кредитів ЄКТС, 1800 год.).
Орієнтація освітньої програми	Освітньо-професійна програма з прикладною спрямованістю за напрямком − безпека інформаційних і комунікаційних систем.
Основний фокус освітньої програми та спеціалізації	Загальна: дослідження в області практики та науки захисту інформації, організації та забезпечення інформаційної та/або кібербезпеки на об'єктах інформаційної діяльності.

Особливості програми	З метою підготовки до роботи в реальному середовищі майбутньої професійної діяльності та отримання випускниками освітньої кваліфікації бакалавр з кібербезпеки програма передбачає надання студентам: – системних теоретичних знань в галузі ІТ технологій із поглибленим вивченням спеціалізації безпека інформаційних і комунікаційних систем; – сучасних компетентностей та практичних навичок з програмування, розробки та управління базами даних, формування моделей захисту інформації та політик безпеки, технічного і криптографічного захисту інформації, побудови захищених IP і TCP мереж та обслуговування сертифікатів відкритих ключів, побудови комплексних систем захисту інформації (далі – КСЗІ) на об'єктах інформаційної діяльності та захисту автоматизованих систем від несанкціонованого доступу, тестування систем захисту інформаційно-комунікаційних систем (далі – ІКС) на проникнення, реалізації управління інформаційною та кібернетичною безпекою, адміністрування захищених ІКС, проведення їх моніторингу та аудиту тощо. З метою передачі передового досвіду майбутньому фахівцю, висвітлення в навчальному процесі останніх досягнень науки і техніки, правил ведення успішного бізнесу програма передбачає: – реалізацію процесного підходу при конструюванні змісту профільноорієнтованих навчальних дисциплін, студентської мобільності, академічної співпраці та молодіжних обмінів; – залучення до викладацької діяльності керівників та професіоналів, які працюють як в системі професійної освіти, так й на виробництві в галузі інформаційних технологій та телекомунікацій, а також представників бізнесу. –
4 – Придатність випускників до працевлаштування та подальшого навчання	
Придатність до працевлаштування	Випускники можуть працювати в державному та приватному секторах Києва, України та Європейського Союзу у таких сферах діяльності: 1) адміністрування ОС сімейства Windows/Linux, мережевого обладнання і технологій TCP/IP, DNS, DHCP, SSL/TLS, etc.; 2) застосування засобів антивірусного захисту (ESET, McAfee, Zilly, etc.), програмних, клієнт-серверних та хмарних технологій захисту інформації (систем веб фільтрації, систем запобігання вторгнень, систем захисту пошти від вірусів і спаму, etc.); 3) створення технічної, проектної та експлуатаційної документації ІКС) та систем захисту інформації (далі – СЗІ); 4) налагодження, експлуатації та проведення аналізу системних процесів функціонування мережевих, клієнт-серверних та хмарних технологій; 5) проведення моніторингу несанкціонованої активності в обчислювальних системах; 6) створення, впровадження та експлуатації КСЗІ) а також СЗІ в складі інформаційно телекомунікаційних (далі – ІТС) та обчислювальних систем; 7) формування політик та процесів у сфері ІТ безпеки, управління доступом до мережевих ресурсів ІТС та ризиками інформаційної безпеки; 8) проведення розслідувань інцидентів та забезпечення аудиту процесів інформаційної безпеки; 9) підтримка наукових досліджень, педагогічна діяльність тощо.

	Згідно з Національним класифікатором професій ДК 003:2010 фахівці, які здобули освіту за освітньою програмою «Безпека інформаційних і комунікаційних систем» можуть обіймати такі первинні посади, як: – програміст/тестувальник програмного забезпечення систем ІКБ; – адміністратор комп'ютерних систем і мереж; – адміністратор інформаційної та кібербезпеки; – аудитор безпеки інформаційно-комунікаційних систем; – розробник засобів захисту інформації; – інженер служби технічного захисту інформації тощо.
Подальше навчання	Можливість здобуття освіти на другому (магістерському) рівні за спеціальністю 125 «Кібербезпека та захист інформації» або іншими спорідненими (суміжними) спеціальностями галузі знань «Інформаційні технології», що узгоджуються з отриманим дипломом бакалавра, а також за іншими міждисциплінарними магістерськими програми з ІТ компонентою.
5 – Викладання та оцінювання	
Викладання та навчання	Ґрунтуються на принципах студентоцентризму та індивідуально-особистісного підходу; реалізуються через навчання на основі досліджень, посилення практичної орієнтованості та творчої спрямованості у формі комбінації лекцій, практичних занять, самостійної навчальної і дослідницької роботи з використанням елементів дистанційного навчання, розв'язування прикладних задач, виконання проєктів, навчальних та виробничих практик, курсових робіт, бакалаврської роботи.
Оцінювання	Накопичувальна бально-рейтингова система, що передбачає оцінювання студентів за усі види аудиторної та позааудиторної освітньої діяльності у вигляді вхідного, поточного, рубіжного та/або семестрового контролю, а також атестації.
6 - Програмні компетентності	
Інтегральна компетентність	Здатність розв'язувати складні спеціалізовані задачі та практичні проблеми у галузі забезпечення інформаційної безпеки і\або кібербезпеки, що характеризується комплексністю та неповною визначеністю умов.
Загальні компетентності (КЗ)	**ЗК 1.** Здатність застосовувати знання у практичних ситуаціях. **ЗК 2**. Знання та розуміння предметної області та розуміння професії. **ЗК 3.** Здатність професійно спілкуватися державною та іноземною мовами як усно, так і письмово. **ЗК 4.** Вміння виявляти, ставити та вирішувати проблеми за професійним спрямуванням. **ЗК 5.** Здатність до пошуку, оброблення та аналізу інформації. **ЗК 6.** Здатність реалізовувати 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. **ЗК 7.** Здатність зберігати та примножувати моральні, культурні, наукові цінності і досягнення суспільства на основі розуміння історії та закономірностей розвитку предметної області, її місця у загальній системі знань про природу і суспільство та у розвитку суспільства, техніки і технологій, використовувати різні види та форми рухової активності для активного відпочинку та ведення здорового способу життя. **ЗКу 8.** Вміння керувати проектами та вести підприємницьку діяльність.

Фахові компетентності спеціальності (КФ)	**ФК 1.** Здатність застосовувати законодавчу та нормативно-правову базу, а також державні та міжнародні вимоги, практики і стандарти з метою здійснення професійної діяльності в галузі інформаційної безпеки та/або кібербезпеки. **ФК 2.** Здатність до використання інформаційно-комунікаційних та *SMART-технологій,* сучасних методів і моделей інформаційної та/або кібербезпеки. **ФК 3.** Здатність до використання програмних та програмно-апаратних комплексів засобів захисту інформації в інформаційно-телекомунікаційних (автоматизованих) та *SMART-системах*. **ФК 4.** Здатність забезпечувати неперервність бізнесу згідно встановленої політики інформаційної та/або кібербезпеки. **ФК 5.** Здатність забезпечувати захист інформації, що обробляється в інформаційно-телекомунікаційних (автоматизованих) та *SMART-системах* з метою реалізації встановленої політики інформаційної та/або кібербезпеки. **ФК 6.** Здатність відновлювати штатне функціонування інформаційних, інформаційно-телекомунікаційних (автоматизованих) систем після реалізації загроз, здійснення кібератак, збоїв та відмов різних класів та походження. **ФК 7.** Здатність впроваджувати та забезпечувати функціонування комплексних систем захисту інформації (комплекси нормативно-правових, організаційних та технічних засобів і методів, процедур, практичних прийомів та ін.). **ФК 8**. Здатність здійснювати процедури управління інцидентами, проводити розслідування, надавати їм оцінку. **ФК 9.** Здатність здійснювати професійну діяльність на основі впровадженої системи управління інформаційною та/або кібербезпекою. **ФК 10.** Здатність застосовувати методи та засоби криптографічного та технічного захисту інформації на об'єктах інформаційної діяльності. **ФК 11.** Здатність виконувати моніторинг процесів функціонування інформаційних, інформаційно-телекомунікаційних (автоматизованих) згідно встановленої політики інформаційної та/або кібербезпеки. **ФК 12.** Здатність аналізувати, виявляти та оцінювати можливі загрози, уразливості та дестабілізуючі чинники інформаційному простору та інформаційним ресурсам згідно з встановленою політикою інформаційної та/або кібербезпеки. **ФКу 13.** Здатність контролювати та аналізувати доступ до ресурсів і процесів у IT та SMART-системах. **ФКу 14.** Здатність здійснювати конфігурування та адміністрування систем моніторингу IT та SMART-систем.
7 - Програмні результати навчання	
ПРН 1 Застосовувати знання державної та іноземних мов з метою забезпечення ефективності професійної комунікації.	
ПРН 2 Організовувати власну професійну діяльність, обирати оптимальні методи та способи розв'язування складних спеціалізованих задач та практичних проблем у професійній діяльності, оцінювати їхню ефективність.	
ПРН 3 Використовувати результати самостійного пошуку, аналізу та синтезу інформації з різних джерел для ефективного рішення спеціалізованих задач професійної діяльності.	

ПРН 4 Аналізувати, аргументувати, приймати рішення при розв'язанні складних спеціалізованих задач та практичних проблем у професійній діяльності, які характеризуються комплексністю та неповною визначеністю умов, відповідати за прийняті рішення.
ПРН 5 Адаптуватися в умовах частої зміни технологій професійної діяльності, прогнозувати кінцевий результат.
ПРН 6 Критично осмислювати основні теорії, принципи, методи і поняття у навчанні та професійній діяльності.
ПРН 7 Діяти на основі законодавчої та нормативно-правової бази України та вимог відповідних стандартів, у тому числі міжнародних в галузі інформаційної та /або кібербезпеки.
ПРН 8 Готувати пропозиції до нормативних актів щодо забезпечення інформаційної та /або кібербезпеки.
ПРН 9 Впроваджувати процеси, що базуються на національних та міжнародних стандартах, виявлення, ідентифікації, аналізу та реагування на інциденти інформаційної та/або кібербезпеки.
ПРН 10 Виконувати аналіз та декомпозицію інформаційно-телекомунікаційних систем.
ПРН 11 Виконувати аналіз зв'язків між інформаційними процесами на віддалених обчислювальних системах.
ПРН 12 Розробляти моделі загроз та порушника.
ПРН 13 Аналізувати проекти інформаційно-телекомунікаційних систем базуючись на стандартизованих технологіях та протоколах передачі даних.
ПРН 14 Вирішувати завдання захисту програм та інформації, що обробляється в інформаційно-телекомунікаційних системах програмно-апаратними засобами та давати оцінку результативності якості прийнятих рішень.
ПРН 15 Використовувати сучасне програмно-апаратне забезпечення інформаційно-комунікаційних технологій.
ПРН 16 Реалізовувати комплексні системи захисту інформації в автоматизованих системах (АС) організації (підприємства) відповідно до вимог нормативно-правових документів.
ПРН 17 Забезпечувати процеси захисту та функціонування інформаційно-телекомунікаційних (автоматизованих) систем на основі практик, навичок та знань, щодо структурних (структурно-логічних) схем, топології мережі, сучасних архітектур та моделей захисту електронних інформаційних ресурсів з відображенням взаємозв'язків та інформаційних потоків, процесів для внутрішніх і віддалених компонент.
ПРН 18 Використовувати програмні та програмно-апаратні комплекси захисту інформаційних ресурсів.
ПРН 19 Застосовувати теорії та методи захисту для забезпечення безпеки інформації в інформаційно-телекомунікаційних системах.

ПРН 20 Забезпечувати функціонування спеціального програмного забезпечення, щодо захисту інформації від руйнуючих програмних впливів, руйнуючих кодів в інформаційно-телекомунікаційних системах.
ПРН 21 Вирішувати задачі забезпечення та супроводу (в.т. числі: огляд, тестування, підзвітність) системи управління доступом згідно встановленої політики безпеки в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах.
ПРН 22 Вирішувати задачі управління процедурами ідентифікації, автентифікації, авторизації процесів і користувачів в інформаційно-телекомунікаційних системах згідно встановленої політики інформаційної і\або кібербезпеки.
ПРН 23 Реалізовувати заходи з протидії отриманню несанкціонованого доступу до інформаційних ресурсів і процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах.
ПРН 24 Вирішувати задачі управління доступом до інформаційних ресурсів та процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах на основі моделей управління доступом (мандатних, дискреційних, рольових).
ПРН 25 Забезпечувати введення підзвітності системи управління доступом до електронних інформаційних ресурсів і процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах з використанням журналів реєстрації подій, їх аналізу та встановлених процедур захисту.
ПРН 26 Впроваджувати заходи та забезпечувати реалізацію процесів попередження отриманню несанкціонованого доступу і захисту інформаційних, інформаційно-телекомунікаційних (автоматизованих) систем на основі еталонної моделі взаємодії відкритих систем.
ПРН 27 Вирішувати задачі захисту потоків даних в інформаційних, інформаційно-телекомунікаційних (автоматизованих) системах.
ПРН 28 Аналізувати та проводити оцінку ефективності та рівня захищеності ресурсів різних класів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах в ході проведення випробувань згідно встановленої політики інформаційної та\або кібербезпеки.
ПРН 29 Здійснювати оцінювання можливості реалізації потенційних загроз інформації, що обробляється в інформаційно-телекомунікаційних системах та ефективності використання комплексів засобів захисту в умовах реалізації загроз різних класів.
ПРН 30 Здійснювати оцінювання можливості несанкціонованого доступу до елементів інформаційно-телекомунікаційних систем.
ПРН 31 Застосовувати теорії та методи захисту для забезпечення безпеки елементів інформаційно-телекомунікаційних систем.
ПРН 32 Вирішувати задачі управління процесами відновлення штатного функціонування інформаційно-телекомунікаційних систем з використанням процедур резервування згідно встановленої політики безпеки.
ПРН 33 Вирішувати задачі забезпечення безперервності бізнес процесів організації на основі теорії ризиків.

ПРН 34 Приймати участь у розробці та впровадженні стратегії інформаційної безпеки та/або кібербезпеки відповідно до цілей і завдань організації.
ПРН 35 Вирішувати задачі забезпечення та супроводу комплексних систем захисту інформації, а також протидії несанкціонованому доступу до інформаційних ресурсів і процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах згідно встановленої політики інформаційної і\або кібербезпеки.
ПРН 36 Виявляти небезпечні сигнали технічних засобів.
ПРН 37 Вимірювати параметри небезпечних та завадових сигналів під час інструментального контролю процесів захисту інформації та визначати ефективність захисту інформації від витоку технічними каналами відповідно до вимог нормативних документів системи технічного захисту інформації.
ПРН 38 Інтерпретувати результати проведення спеціальних вимірювань з використанням технічних засобів, контролю характеристик інформаційно-телекомунікаційних систем відповідно до вимог нормативних документів системи технічного захисту інформації.
ПРН 39 Проводити атестацію (спираючись на облік та обстеження) режимних територій (зон), приміщень тощо в умовах додержання режиму секретності із фіксуванням результатів у відповідних документах.
ПРН 40 Інтерпретувати результати проведення спеціальних вимірювань з використанням технічних засобів, контролю характеристик ІТС відповідно до вимог нормативних документів системи технічного захисту інформації.
ПРН 41 Забезпечувати неперервність процесу ведення журналів реєстрації подій та інцидентів на основі автоматизованих процедур.
ПРН 42 Впроваджувати процеси виявлення, ідентифікації, аналізу та реагування на інциденти інформаційної і/або кібербезпеки.
ПРН 43 Застосовувати національні та міжнародні регулюючі акти в сфері інформаційної безпеки та/ або кібербезпеки для розслідування інцидентів.
ПРН 44 Вирішувати задачі забезпечення безперервності бізнес-процесів організації на основі теорії ризиків та встановленої системи управління інформаційною безпекою, згідно з вітчизняними та міжнародними вимогами та стандартами.
ПРН 45 Застосовувати ріні класи політик інформаційної безпеки та/ або кібербезпеки, що базуються на ризик-орієнтованому контролі доступу до інформаційних активів.
ПРН 46 Здійснювати аналіз та мінімізацію ризиків обробки інформації в інформаційно-телекомунікаційних системах.
ПРН 47 Вирішувати задачі захисту інформації, що обробляється в інформаційно-телекомунікаційних системах з використанням сучасних методів та засобів криптографічного захисту інформації.
ПРН 48 Виконувати впровадження та підтримку систем виявлення вторгнень та використовувати компоненти криптографічного захисту для забезпечення необхідного рівня захищеності інформації в інформаційно-телекомунікаційних системах.

ПРН 49 Забезпечувати належне функціонування системи моніторингу інформаційних ресурсів і процесів в інформаційно-телекомунікаційних системах.	
ПРН 50 Забезпечувати функціонування програмних та програмно-апаратних комплексів виявлення вторгнень різних рівнів та класів (статистичних, сигнатурних, статистично-сигнатурних);.	
ПРН 51 Підтримувати працездатність та забезпечувати конфігурування систем виявлення вторгнень в інформаційно-телекомунікаційних системах;	
ПРН 52 Використовувати інструментарій для моніторингу процесів в інформаційно-телекомунікаційних системах	
ПРН 53 Вирішувати задачі аналізу програмного коду на наявність можливих загроз.	
ПРН 54 Усвідомлювати цінності громадянського (вільного демократичного) суспільства та необхідність його сталого розвитку, верховенства права, прав і свобод людини і громадянина в Україні.	
ПРНу 55 Забезпечувати процеси моніторингу доступу до ресурсів і процесів ІТ та SMART-систем.	
ПРНу 56 Забезпечувати конфігурування та функціонування систем моніторингу ресурсів та процесів в ІТ та *SMART- системах.*	
8 - Ресурсне забезпечення реалізації програми	
Кадрове забезпечення	Кадрове забезпечення освітньо-професійної програми складається з професорсько-викладацького складу кафедри інформаційної та кібернетичної безпеки імені професора Володимира Бурячка та кафедри комп'ютерних наук і математики. До викладання окремих дисциплін відповідно до їх компетенції та досвіду залучений професорсько-викладацький склад інших кафедр університету. ОПП передбачає широку участь фахівців практиків, які відповідають напряму програми, що підсилює синергетичний зв'язок теоретичної та практичної підготовки. Кадрове забезпечення ОП відповідає вимогам, визначеним Ліцензійними умовами провадження освітньої діяльності.
Матеріально-технічне забезпечення	Основу матеріально-технічного забезпечення складають спеціалізовані комп'ютерні лабораторії із сучасними апаратними та програмними ресурсами, що забезпечують якісну підготовку бакалаврів за освітньою програмою «Безпека інформаційних і комунікаційних систем». Спеціально обладнані апаратно-програмним забезпеченням, наочними та методичними матеріалами центри розвитку компетентностей, а саме: 1) «Центр дослідження технологій функціонування й захисту інформаційно-комунікаційних систем та мереж» з: навчальною «Лабораторією комп'ютерних мереж та кібербезпеки», навчальною «Лабораторією безпеки інформаційно-комунікаційних систем» та навчальною «Лабораторією антивірусного захисту»; 2) «Центр дослідження технологій захисту інформаційних ресурсів» з: навчальною «Лабораторією безпеки інформаційних активів» (навчальний кіберполігон) та навчальною «Лабораторією систем технічного та криптографічного захисту інформації»; 3) «Центр моделювання та програмування»; 4) «Лабораторія вбудованих систем і 3Д моделювання» тощо.

Інформаційне та навчально-методичне забезпечення	Бібліотечні електронні ресурси, електронні наукові видання, електронні навчальні курси із можливістю дистанційного навчання та самостійної роботи, хмарні сервіси Microsoft.
9 - Академічна мобільність	
Національна кредитна мобільність	
Міжнародна кредитна мобільність	Укладено угоди, які передбачають студентську мобільність із університетами європейських країн та в рамках програми Еразмус+КА1. З них: Вільнюський університет (Литва), Університет Костянтина Філософа у Нітрі (Словаччина), Університет Естремадура (Іспанія), Сілезький університет в Катовіцах (Польща), Академія імені Яна Длугоша в Ченстохові (Польща), Університет Острави (Чехія), Університет Париж-Сорбонна (Франція), Лісабонський університет (Португалія) та інші.
Навчання іноземних здобувачів вищої освіти	Згідно ліцензії передбачається підготовка іноземців та осіб без громадянства. Процес навчання ведеться українською мовою, тому громадяни інших країн, що володіють українською мовою не нижче рівня В1 можуть отримувати освіту за даною освітньою програмою.

2. Перелік компонентів освітньо-професійної програми та їхня логічна послідовність

2.1. Перелік та розподіл кредитів – бакалавр, (240 кредитів ECTS - 3 роки 10 місяців)

Код	Компоненти освітньої програми (навчальні дисципліни, курсові проєкти (роботи), практики, ЄДКІ)	Кількість кредитів	Форма підсумкового контролю
Обов'язкова частина			
Навчальні дисципліни			
Формування загальних комптентностей			
ОДЗ.01	Університетські студії	**4**	залік
	Я - студент	1	
	Лідерство служіння	1	
	Вступ до спеціальності	2	
ОДЗ.02	Іноземна мова	**10**	екзамен, залік
ОДЗ.03	Фізичне виховання	**4**	залік
ОДЗ.04	Українські студії	**6**	екзамен
ОДЗ.05	Філософські студії	**4**	екзамен
ОДЗ.06	Групова динаміка і ділові комунікації	**4**	залік
	Всього	**32**	
Формування спеціальних (фахових, предметних) компетентностей			
ОДС.01	Фізика	**7**	екзамен, залік
ОДС.02	Вища математика	**10**	залік, екзамен
	Лінійна алгебра та аналітична геометрія	4	
	Математичний аналіз та чисельні методи	6	
ОДС.03	Основи інформаційної і кібербезпеки та захисту інформації	**4**	залік
ОДС.04	Теорія кіл і сигналів в інформаційному та кіберпросторах	**5**	екзамен
ОДС.05	Основи ОС та сучасних Інтернет-технологій	**4**	залік
ОДС.06	Технології безпечного програмування	**8**	екзамен, залік
КР.01	Курсова робота з ОДС.06	**1**	КР
ОДС.07	Теоретичні аспекти захищених інформаційно-комунікаційних технологій	**6**	екзамен, залік
ОДС.08	Компонентна база та елементи схемотехніки в системах захисту інформації	**4**	екзамен
ОДС.09	Кібернетичне право	**4**	залік
ОДС.10	Фізичні основи захисту інформації	**4**	екзамен
ОДС.11	Спеціальні методи в системах безпеки	**7**	екзамен
	Дискретна математика	4	
	Теорія ймовірностей та математична статистика	3	
ОДС.12	Захист інформації в інформаційно-комунікаційних системах	**8**	залік, екзамен
КР.02	Курсова робота з ОДС.12	**1**	КР
ОДС.13	Теорія інформації та кодування	**5**	екзамен
ОДС.14	Прийняття рішень в інформаційній та кібербезпеці	**5**	екзамен
ОДС.15	Теорія ризиків	**5**	залік
ОДС.16	Прикладна криптологія	**7**	залік екзамен,
ОДС.17	Безпека безпровідних, мобільних, хмарних та SMART- технологій	**4**	екзамен
ОДС.18	Безпека Web ресурсів	**4**	екзамен
ОДС.19	Прикладні аспекти аналізу та синтезу політик безпеки	**4**	екзамен

ОДС.20	Захист баз та сховищ даних	**4**	екзамен
ОДС.21	Криптомеханізми інформаційної та кібербезпеки	**5**	екзамен
ОДС.22	Методи та засоби протидії кіберзлочинності	**4**	екзамен
ОДС.23	Інфраструктура відкритих ключів	**6**	екзамен
	Всього	**127**	
Практика			
ВП.2.01	Виробнича	**3**	залік
ВП.2.02	Виробнича (технологічна)	**6**	залік
ВП.2.03	Виробнича	**12**	залік
	Всього	**21**	
Атестація			
ОА.01	Єдиний державний кваліфікаційний іспит (ЄДКІ)/ Комплексний іспит з кібербезпеки		
	Всього		
	Загальний обсяг обов'язкових компонет	**180**	
Вибіркова частина			
1. Спеціалізований блок 1			
ВДК.1.01	Стандарти інформаційної та кібербезпеки	**5**	залік
ВДК.1.02	Прикладні аспекти побудови КТЗІ	**5**	екзамен
ВДК.1.03	Основи безпеки телекомунікаційних технологій	**5**	екзамен
ВДК.1.04	Програмні комплекси захисту АС від НСД	**5**	екзамен
ВДК.1.05	Прикладні аспекти програмування в системах ІКБ	**5**	екзамен
ВДК.1.06	Основи захисту конфіденційних даних	**5**	екзамен
ВДК.1.07	Системи технічного захисту інформації	**4**	залік
ВДК.1.08	Методи та засоби управління інформаційною безпекою	**5**	залік
ВДК.1.09	КСЗІ: проєктування, впровадження, супровід	**6**	екзамен
ВКР.1.10	Курсова робота з ВДК.1.09	**1**	КР
ВДК.1.10	Управління інцидентами безпеки	**5**	залік
ВДК.1.11	Засади відкриття власного бізнесу	**5**	залік
ВДК.1.12	Інформаційна та кібербезпека сучасного підприємства	**4**	залік
	Всього	**60**	
2. Вибірковий блок 2 з Вибір з Каталогу вибіркових дисциплін			
	Всього	**60**	
	ЗАГАЛЬНИЙ ОБСЯГ ОСВІТНЬОЇ ПРОГРАМИ	**240**	

1 курс		2 курс		3 курс		4 курс	
1 семестр	*2 семестр*	*3 семестр*	*4 семестр*	*5 семестр*	*6 семестр*	*7 семестр*	*8 семестр*
Університетські студії (4)		Кібернетичне право (4)					
Іноземна мова (10)		Групова динаміка і ділові комунікації (4)					
Фізичне виховання (4)							
	Українські студії (6)		Філософські студії (4)				
Фізика (7)							
Вища математика (10)							
Основи інформаційної і кібербезпеки та захисту інформації (4)	Технології безпечного програмування (8)		Спеціальні методи в системах безпеки (7)	Теорія ризиків (5)			
Теорія кіл і сигналів в інформаційному та кіберпросторах (5)	Компонентна база та елементи схемотехніки в систем захисту інформації (4)	Курсова робота з Технологій безпечного програмування (1)	Теорія інформації та кодування (5)	Прийняття рішень в інформаційній та кібербезпеці (5)		Криптомеханізми інформаційної та кібербезпеки (5)	
Основи ОС та сучасних Інтернет-технологій (4)		Фізичні основи захисту інформації (4)	Захист інформації в інформаційно-комунікаційних системах (9)			Методи та засоби протидії кіберзлочинності (5)	Інфраструктура відкритих ключів (6)
	Теоретичні аспекти захищених інформаційно-комунікаційних технологій (6)			Курсова робота із Захисту інформації в інформаційно-комунікаційних системах (1)	Програмні комплекси захисту АС від НСД (5)	Прикладні аспекти програмування в системах ІКБ (5)	Основи захисту конфіденційних даних (5)
				Прикладна криптологія (7)			
				Безпека безпровідних, мобільних, хмарних та SMART-технологій (4)	Прикладні аспекти аналізу та синтезу політик безпеки (4)		
				Безпека Web ресурсів (4)	Захист баз та сховищ даних (4**)**	КСЗІ: проектування, впровадження, супровід (6)	
						Курсова робота з КСЗІ: проектування, впровадження, супровід (1)	
					Методи та засоби управління інформаційною безпекою (5)		
						Управління інцидентами безпеки (5)	
		Стандарти інформаційної та кібербезпеки (5)	Прикладні аспекти побудови КТЗІ (5)	Основи безпеки телекомунікаційних технологій (5)	Системи технічного захисту інформації (4)	Засади відкриття власного бізнесу (5)	Інформаційна та кібербезпека сучасного підприємства (4)
			Виробнича практика (3)		Виробнича практика (6)		Виробнича практика (12)
							Єдиний державний кваліфікаційний іспит (ЄДКІ)

3. Форма атестації здобувачів вищої освіти

Атестація здобувачів вищої освіти за освітньо-професійною програмою 125.00.01 Безпека інформаційних і комунікаційних систем спеціальності 125 «Кібербезпека та захист інформації» проводиться у формі Єдиного державного кваліфікаційного іспиту (ЄДКІ). Вимоги до Єдиного державного кваліфікаційного іспиту встановлюються законодавством.

У випадку неможливості технічного забезпечення складання ЄДКІ Міністерством освіти і науки України передбачено заміну цього іспиту на Комплексний іспит з кібербезпеки, організацію проведення якого бере на себе університет.

При складанні атестації видається документ державного зразка про присудження ступеня бакалавра із присвоєнням їй кваліфікації: «бакалавр з кібербезпеки».

МАТРИЦЯ ВІДПОВІДНОСТІ ПРОГРАМНИХ КОМПЕТЕНТНОСТЕЙ КОМПОНЕНТАМ ОСВІТНЬОЇ ПРОГРАМИ

	ЗК 1	ЗК 2	ЗК 3	ЗК 4	ЗК 5	ЗК 6	ЗК 7	ЗК 8	ФК 1	ФК 2	ФК 3	ФК 4	ФК 5	ФК 6	ФК 7	ФК 8	ФК 9	ФК 10	ФК 11	ФК 12	ФК 13	ФК 14
ОДЗ.01		+																		+		
ОДЗ.02			+				+		+													
ОДЗ.03							+															
ОДЗ.04						+	+															
ОДЗ.05						+	+															
ОДЗ.06			+			+	+															
ОДС.01	+		+												+							
ОДС.02		+			+															+		
ОДС.03	+	+				+					+						+					
ОДС.04	+												+									
ОДС.05		+															+					
ОДС.06					+				+	+												
ОДС.07				+									+					+				
ОДС.08		+		+										+	+							
ОДС.09		+				+		+	+								+					
ОДС.10					+								+									
ОДС.11					+											+						
ОДС.12	+			+					+		+		+		+		+					
ОДС.13					+								+						+			
ОДС.14		+						+								+	+			+		
ОДС.15		+		+				+								+	+			+		
ОДС.16		+		+					+	+					+			+				
ОДС.17		+			+														+		+	+
ОДС.18	+			+								+					+			+		
ОДС.19						+		+	+			+										

	ЗК 1	ЗК 2	ЗК 3	ЗК 4	ЗК 5	ЗК 6	ЗК 7	ЗК 8	ФК 1	ФК 2	ФК 3	ФК 4	ФК 5	ФК 6	ФК 7	ФК 8	ФК 9	ФК 10	ФК 11	ФК 12	ФК 13	ФК 14
ОДС.20		+			+									+							+	+
ОДС.21		+		+				+	+									+				
ОДС.22	+			+									+			+			+		+	+
ОДС.23		+		+		+			+			+		+	+		+	+	+	+		
ВП.2.01	+	+	+	+	+	+	+	+	+	+										+		
ВП.2.02	+	+	+	+	+	+		+	+	+	+	+	+	+	+	+					+	+
ВП.2.03	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+
ОА.01	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+
ВДК.1.01							+	+	+													
ВДК.1.02				+										+	+					+		
ВДК.1.03	+		+								+		+								+	+
ВДК.1.04				+				+	+			+					+					
ВДК.1.05	+		+		+			+			+				+	+	+	+		+		
ВДК.1.06	+																	+		+	+	+
ВДК.1.07		+		+				+	+			+			+							
ВДК.1.08	+			+					+			+				+	+					
ВДК.1.09		+		+	+			+				+	+		+		+			+	+	+
ВДК.1.10	+		+													+	+					
ВДК.1.11								+	+													
ВДК.1.12	+						+	+	+							+	+					

МАТРИЦЯ ВІДПОВІДНОСТІ ПРОГРАМНИХ КОМПЕТЕНТНОСТЕЙ КОМПОНЕНТАМ ОСВІТНЬОЇ ПРОГРАМИ

	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	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	ПРН 56
ОДЗ.01	+	+	+			+																																																
ОДЗ.02	+		+																																																		
ОДЗ.03																																																					
ОДЗ.04	+			+																																																	
ОДЗ.05	+		+	+		+																																															
ОДЗ.06	+			+	+																																															
ОДС.01																	+																		+	+																
ОДС.02		+	+																																																		
ОДС.03					+									+																		+																			
ОДС.04				+													+																		+	+	+		+													
ОДС.05						+					+																																				+						
ОДС.06			+		+										+																																					
ОДС.07														+								+																													+	
ОДС.08						+					+																																										
ОДС.09							+	+	+																								+									+										
ОДС.10											+						+							+					+	+	+							+	+		+											
ОДС.11				+																												+								+				+								
ОДС.12							+		+			+	+			+	+					+		+				+																	+				+				
ОДС.13																		+	+	+							+		+							+	+													+				
ОДС.14																							+	+	+	+	+	+	+	+				+						+		+		+		+						
ОДС.15																			+												+		+										+	+								
ОДС.16							+						+						+			+	+																													+		
ОДС.17																					+	+		+																												+	+
ОДС.18																	+		+	+			+			+				+																							
ОДС.19							+	+	+				+			+						+			+			+				+																				
ОДС.20										+							+					+	+	+	+	+	+																							+	+	+		+	+
ОДС.21																+			+																				+				+							+	+						+		
ОДС.22												+										+		+				+													+			+					+			+	+	+
ОДС.23							+	+	+				+			+	+		+		+				+	+																			+		+		+						
ВП.2.01	+	+	+	+	+	+	+						+					+	+			+	+																													+		
ВП.2.02		+	+	+						+															+						+			+		+				+			+					+	+	+	+				+	+
ВП.2.03	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+

	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	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	ПРН 56
МАТРИЦЯ ВІДПОВІДНОСТІ ПРОГРАМНИХ КОМПЕТЕНТНОСТЕЙ ВИБІРКОВИМ КОМПОНЕНТАМ ОСВІТНЬОЇ ПРОГРАМИ																																																									
ВДК. 1.01							+	+	+																							+					+				+		+									+	+	
ВДК. 1.02														+		+	+		+	+	+						+	+					+			+																		
ВДК. 1.03																+					+	+		+		+												+																
ВДК. 1.04							+	+	+					+	+					+			+			+				+					+																		
ВДК. 1.05				+								+		+	+	+	+	+	+	+								+	+			+														+				+			
ВДК. 1.06								+	+												+			+	+	+				+										+	+											+	+
ВДК. 1.07							+	+	+																										+	+	+		+														
ВДК. 1.08							+	+	+				+																				+										+										
ВДК. 1.09																+								+	+						+	+	+	+			+	+					+			+						+	+
ВДК. 1.10									+			+		+														+	+											+	+	+		+	+								
ВДК. 1.11					+	+	+																																			+											+		
ВДК.1.12													+			+																	+				+	+			+	+	+										