КИЇВСЬКИЙ УНІВЕРСИТЕТ ІМЕНІ БОРИСА ГРІНЧЕНКА

«ЗАТВЕРДЖЕНО»
Рішенням Вченої ради Факультету
інформаційних технологій та управління
16.09.2020 р., протокол № 7

Голова Вченої ради, декан
_____ Алла МИХАЦЬКА

ЗМІНИ ДО ОСВІТНЬО-НАУКОВОЇ ПРОГРАМИ
«Інформаційна безпека держави»
третього (освітньо-наукового) рівня вищої освіти

Галузь знань:	12 Інформаційні технології
Спеціальність:	125 Кібербезпека
Кваліфікація:	доктор філософії у галузі «Інформаційні технології» зі спеціальності «Кібербезпека»

наказ № 539 від 24.09.2020 р.

Київ – 2020

ЛИСТ-ПОГОДЖЕННЯ

змін до освітньо-наукової програми «Інформаційна безпека держави» третього (освітньо-наукового) рівня вищої освіти

Програму переглянуто у 2020 році.

Робоча група у складі:
БУРЯЧОК Володимир Леонідович, доктор технічних наук, професор, завідувач кафедри інформаційної та кібернетичної безпеки Факультету інформаційних технологій та управління (керівник робочої групи);
БЕССАЛОВ Анатолій Володимирович, доктор технічних наук, професор, професор кафедри інформаційної та кібернетичної безпеки Факультету інформаційних технологій та управління;
СЕМКО Віктор Володимирович, доктор технічних наук, доцент, доцент кафедри інформаційної та кібернетичної безпеки Факультету інформаційних технологій та управління.

Кафедра інформаційної та кібернетичної безпеки
Протокол від «03» вересня 2020 р. № 8
Завідувач кафедри _____ Володимир БУРЯЧОК
(підпис)

Вчена рада Факультету інформаційних технологій та управління
Протокол від 16.09. 2020 р. № 7
Голова Вченої ради _____ Алла МИХАЦЬКА
(підпис)

Завідувач аспірантури, докторантури
_____ Оксана ПЛЮЩИК
(підпис)
«16» 09 2020 р.

Проректор з наукової роботи
_____ Наталія ВІННІКОВА
(підпис)
«16» 09 2020 р.

Актуалізовано:

Дата перегляду ОНП/ внесення змін до ОНП	2020 р.		
Підпис			
ПІБ гаранта ОНП	Бурячок В.Л.		

ОБҐРУНТУВАННЯ

Зміни до освітньо-наукової програми (ОНП) «Інформаційна безпека держави» за спеціальністю 125 Кібербезпека за третім (освітньо-науковим) рівнем вищої освіти, затвердженої рішенням Вченої ради Київського університету імені Бориса Грінченка від 24.01.2019 р., протокол №1 (наказ від 29.01.2019 р. №37) зумовлені чинниками, які виявилися у процесі реалізації освітньо-наукової програми (навчального плану, розроблення робочих програм навчальних дисциплін та проведення практичної підготовки) протягом 2019-2020 навчального року.

Під час реалізації освітньо-наукової програми, у ході проведених опитувань, очних і дистанційних зустрічей та ін. група забезпечення отримала відгуки від здобувачів вищої освіти, академічної спільноти, роботодавців з побажаннями внести окремі зміни та уточнення до діючої освітньо-наукової програми. Провівши консультації, робочі наради, засідання, врахувавши відгуки стейкхолдерів та зміни в нормативній документації, погоджено зміни й уточнення до освітньо-наукової програми, які стосуються:

- ✓ уточнення загальної інформації про освітньо-наукову програму, зокрема рівня відповідності Національній рамці кваліфікацій в описі освітньо-наукової програми з дев'ятого на восьмий згідно з постановою Кабінету Міністрів України від 23.11.2011 № 1341 – у редакції постанови КМУ від 25.06.2020 № 519;
- ✓ перерозподілу кредитів між освітніми компонентами для посилення практичної складової освітньо-наукової програми (збільшення обсягу кредитів на науково-викладацьку практику з метою підготовки здобувачів до викладацької діяльності).

Цілі, програмні компетентності та програмні результати навчання не змінювалися.

Відповідно було внесено уточнення в такі розділи освітньо-наукової програми та їх сегменти:

I. 1. Загальна інформація

II. 2.1. Перелік компонентів ОНП

Вибіркову частину освітньо-наукової програми описано в Додатку 1.

1. Профіль освітньо-наукової програми «Інформаційна безпека держави» зі спеціальності 125 Кібербезпека

1 – Загальна інформація	
Повна назва закладу вищої освіти та структурного підрозділу	Київський університет імені Бориса Грінченка Факультет інформаційних технологій та управління
Ступінь вищої освіти та назва кваліфікації мовою оригіналу	доктор філософії, доктор філософії з кібернетичної безпеки
Офіційна назва освітньої-наукової програми	«Інформаційна безпека держави»
Тип диплому та обсяг освітньо-наукової програми	Диплом доктор філософії, одиничний, 60 кредитів ЄКТС (освітня складова – 60 кредитів). Термін навчання 4 роки
Наявність акредитації	Національне агентство забезпечення якості вищої освіти, Україна Термін подання програми на акредитацію – 2023 р.
Цикл/рівень	третій (освітньо-науковий) рівень FQ-EHEA – третій цикл, QF LLL – 8 рівень, НРК – 8 рівень
Передумови	Наявність ступеня магістра або освітньо-кваліфікаційного рівня спеціаліста
Мова(и) викладання	Українська
Інтернет-адреса постійного розміщення опису освітньої-наукової програми	https://kubg.edu.ua/informatsiya/aspirantam-i-doktorantam/aspirantura/spetsialnosti.html

ІІ. Перелік компонент освітньо-наукової програми та їх логічна послідовність.

2.1. Перелік компонент ОНП

Код	Компоненти освітньо-наукової програми (навчальні дисципліни, практики)	Кількість кредитів	Форма підсум-кового контролю
Обов'язкові компоненти ОНП			
Формування загальних компетентностей			
ОДЗ.01	**Філософія і методологія наукової діяльності**	**4**	екзамен
	Філософія науки	2	
	Загальнонаукова методологія	1	
	Наукова етика	1	
ОДЗ.02	**Стратегії наукових досліджень**	**6**	залік
	Нормативно-правова база наукових досліджень та наукової діяльності	1	
	Інтернаціоналізація науки	3	
	Сучасні технології інформаційної і кібербезпеки та захисту інформації	2	
ОДЗ.03	**Наукова комунікація іноземною мовою**	**8**	екзамен
	Всього	**18**	
Формування фахових компетентностей			
ОДС.01	**Інформаційно-аналітичні процеси в системах безпеки державних інформаційних ресурсів**	**3**	залік
ОДС.02	**Прикладні аспекти створення та застосування систем технічного захисту**	**4**	залік
ОДС.03	**Прикладні аспекти створення та застосування систем криптографічного захисту**	**4**	залік
ОДС.04	**Прикладні аспекти теорій ризиків, конфліктів і катастроф в системах безпеки**	**4**	залік
ОП.01	**Науково-викладацька практика**	**4**	залік
ОП.02	**Дослідницька практика**	**4**	залік
	Всього	**23**	
	Разом за обов'язковою частиною	**43**	
Вибіркова частина ОНП (Додаток 1)			
ВДК.01	**Системний аналіз та прийняття рішень в інформаційній і кібербезпеці**	4	залік
	Прикладні аспекти прогнозування і моделювання в сфері інформаційної діяльності		
ВДК.02	**Проектування і впровадження захищених інформаційно-комунікаційних систем**	4	залік
	Прикладні аспекти адміністрування та експлуатації захищених інформаційно-комунікаційних систем		
ВДК.03	**Організація захисту розподілених інформаційних ресурсів**	4	залік
	Прикладні аспекти моніторингу та аудиту захищених інформаційно-комунікаційних систем		
ВДК.04	**Забезпечення безпеки об'єктів критичної інфраструктури в умовах ведення кібердій і кіберконфліктів**	4	екзамен
	Прикладні аспекти управління інформаційною та кібербезпекою об'єктів критичної інфраструктури		
ВДК.05	**Технології безпеки складних соціотехнічних систем**	3	залік
	Прикладні аспекти протидії кібератакам в соціотехнічних системах		
	Всього	**19**	
	Разом за вибірковою частиною	**19**	
ЗАГАЛЬНИЙ ОБСЯГ ОСВІТНЬО-НАУКОВОЇ ПРОГРАМИ		**60**	

2.2. Структурно-логічна схема ОНП

<table>
<tr><th colspan="2">1 курс</th><th colspan="2">2 курс</th><th colspan="2">3 курс</th><th colspan="2">4 курс</th></tr>
<tr><td>1 семестр</td><td>2 семестр</td><td>3 семестр</td><td>4 семестр</td><td>5 семестр</td><td>6 семестр</td><td>7 семестр</td><td>8 семестр</td></tr>
<tr><td colspan="6">ОБОВ'ЯЗКОВА ЧАСТИНА</td><td rowspan="6" colspan="2">Завершення виконання наукової складової ОНП</td></tr>
<tr><td colspan="6">ФОРМУВАННЯ ЗАГАЛЬНИХ КОМПЕТЕНТНОСТЕЙ</td></tr>
<tr><td colspan="2">Філософія і методологія наукової діяльності</td><td colspan="4" rowspan="3"></td></tr>
<tr><td>Філософія науки - 2 кредити; Наукова етика - 1 кредит</td><td>Загальнонаукова методологія - 1 кредит</td></tr>
<tr><td colspan="3">Стратегії наукових досліджень</td><td colspan="3" rowspan="3"></td></tr>
<tr><td>Нормативно-правова база наукових досліджень та наукової діяльності 1 кредит</td><td>Інтернаціоналізація науки - 3 кредити</td><td>Сучасні технології інформаційної і кібербезпеки та захисту інформації – 2 кредити</td></tr>
<tr><td colspan="3">Наукова комунікація іноземною мовою</td></tr>
<tr><td>2 кредити</td><td>4 кредити</td><td>2 кредити</td><td colspan="4"></td></tr>
<tr><td colspan="8">ФОРМУВАННЯ ФАХОВИХ КОМПЕТЕНТНОСТЕЙ</td></tr>
<tr><td colspan="2" rowspan="4"></td><td colspan="2">Інформаційно-аналітичні процеси в системах безпеки державних інформаційних ресурсів 3 кредити</td><td colspan="4" rowspan="4"></td></tr>
<tr><td colspan="2" rowspan="2">Прикладні аспекти створення та застосування систем технічного захисту – 4 кредити
Прикладні аспекти створення та застосування систем криптографічного захисту – 4 кредити</td></tr>
<tr><td colspan="2">Прикладні аспекти теорій ризиків, конфліктів і катастроф в системах безпеки</td></tr>
<tr><td>2 кредити</td><td>2 кредити</td></tr>
<tr><td colspan="4"></td><td>Науково-викладацька практика – 4 кредити</td><td>Дослідницька практика – 4 кредити</td><td colspan="2"></td></tr>
</table>

ВИБІРКОВА ЧАСТИНА

Системний аналіз та прийняття рішень в інформаційній і кібербезпеці / Прикладні аспекти прогнозування і моделювання в сфері інформаційної діяльності			
2 кредити	*2 кредити*		
	Технології безпеки складних соціотехнічних систем / Прикладні аспекти протидії кібератакам в соціотехнічних системах – *3 кредити*		
		Проектування і впровадження захищених інформаційно-комунікаційних систем / Прикладні аспекти адміністрування та експлуатації захищених інформаційно-комунікаційних систем – *4 кредити*	
		Організація захисту розподілених інформаційних ресурсів / Прикладні аспекти моніторингу та аудиту захищених інформаційно-комунікаційних систем	
		2 кредити	*2 кредити*
			Забезпечення безпеки об'єктів критичної інфраструктури в умовах ведення кібердій і кіберконфліктів / Прикладні аспекти управління інформаційною та кібербезпекою об'єктів критичної інфраструктури – *4 кредити*

4. Матриця відповідності програмних компетентностей компонентам освітньо-наукової програми

	ЗК1	ЗК2	ЗК3	ЗК4	ФК1	ФК2	ФК3	ФК4	ФК5	ФК6	ФК7
ОДЗ.01				+	+						
ОДЗ.02		+	+	+	+						
ОДЗ.03	+										
ОДС.01				+		+		+			
ОДС.02							+		+	+	
ОДС.03							+		+	+	
ОДС.04							+			+	
ОП.01	+	+									
ОП.02	+	+	+	+	+	+	+	+	+	+	+

5. Матриця забезпечення програмних результатів навчання відповідними компонентами освітньо-наукової програми

	ПРН1	ПРН2	ПРН3	ПРН4	ПРН5	ПРН6	ПРН7
ОДЗ.01		+	+	+			
ОДЗ.02		+	+	+			
ОДЗ.03	+		+				
ОДС.01			+	+			
ОДС.02				+	+	+	
ОДС.03				+	+	+	
ОДС.04						+	
ОП.01	+	+	+	+			
ОП.02	+	+	+	+			

Додаток 1 – Вибіркова частина освітньо-наукової програми

Освітньо-наукова програма «Інформаційна безпека держави» забезпечує реалізацію аспірантами права на вільний вибір освітніх компонентів, передбаченого п. 15 частини І ст. 62 Закону України «Про вищу освіту», п. 26 Порядку підготовки здобувачів вищої освіти ступеня доктора філософії та доктора наук у закладах вищої освіти (наукових установах), затвердженого постановою Кабінету Міністрів України від 23.03.2016 р. №261 (зі змінами).

З наведеного переліку у вибірковій частині аспірант самостійно обирає одну дисципліну з кожного запропонованого блоку дисциплін. Вибір аспірантом запропонованих дисциплін створює умови для набуття знань і компетентностей у вузькій науковій спеціалізації, релевантній до тем напрямів досліджень, наукового напряму аспіранта. Здобувач може здійснювати вибір дисциплін з інших освітніх програм з урахуванням власних наукових інтересів, тематики дисертаційного дослідження та за погодженням з науковим керівником.

Дисципліна «Системний аналіз та прийняття рішень в інформаційній і кібербезпеці» передбачає вивчення основних понять, структури, основних завдань та методів системного аналізу і теорії прийняття рішень; технологій застосування системного аналізу та прийняття рішень в інформаційній безпеці; формування умінь та навичок із системного аналізу та системного підходу при прийнятті рішень достатніх для застосування і подальшого продовження самоосвіти у галузі інформаційної безпеки та захисту інформації; отримання кваліфікації як аналітика даних, спеціаліста аналізу даних, бізнес-аналітика ІКТ, Web-аналітика тощо (відповідно до «Проекту реєстру кваліфікацій: сфера ІТ та цифрові професії» від 03.09.2020 р.).

Дисципліна «Прикладні аспекти прогнозування і моделювання в сфері інформаційної діяльності» передбачає формування у здобувачів наукового ступеня «доктор філософії» професійних компетенцій та здатностей самостійно формувати обґрунтовані судження про можливий стан систем захисту та/або систем інформаційної і кібербезпеки в майбутньому та (або) про альтернативні шляхи і терміни їх реалізації. Головними функціями прогнозування перспектив розвитку систем захисту при цьому є: науковий аналіз процесів і тенденцій; дослідження об'єктивних зв'язків явищ в розвитку; оцінка об'єкта прогнозування (базується на поєднанні аспектів детермінованості (обмеження) і невизначеності; виявлення альтернатив розвитку; накопичення наукового матеріалу для обґрунтування вибору управлінських рішень.

Дисципліна «Проектування і впровадження захищених інформаційно-комунікаційних систем» передбачає вивчення технологій розробки захищених інформаційно-комунікаційних систем, а також проектування відповідних комплексів засобів захисту інформації в ІКС;

формування: умінь та навичок з розроблення систем захисту ІКС й визначення загальних принципів їх побудови; формування опису ІКС та середовища їх функціонування; визначення складу апаратного та програмного забезпечення; здійснення аналізу обчислювальних процесів та технологій; формування політик і правил забезпечення безпеки тощо; отримання: кваліфікації як фахівця з питань обслуговування мереж, фахівця з ІКТ безпеки, консультанта з питань ІКТ безпеки, тестувальника систем безпеки, експерта з кібернетики, тощо (відповідно до «Проекту реєстру кваліфікацій: сфера ІТ та цифрові професії» від 03.09.2020 року).

Дисципліна «Прикладні аспекти адміністрування та експлуатації захищених інформаційно-комунікаційних систем» передбачає формування у здобувачів наукового ступеня «доктор філософії» професійних компетенцій та здатностей самостійно оволодіти студентами сучасними технологіями адміністрування та захисту інформації в інформаційно-комунікаційних системах та мережах, особливостями їх реалізацій, принципами побудови та адміністрування програмних та програмно-апаратних засобів для захисту програмного забезпечення та іншої інформації в інформаційно-комунікаційних системах та мережах. Завдання дисципліни полягає у набутті студентами знань, умінь і здатностей (компетенцій) адміністрування в інформаційно-комунікаційних системах та мережах для ефективного вирішення завдань професійної діяльності.

Дисципліна «Організація захисту розподілених інформаційних ресурсів» передбачає вивчення технологій створення і принципів роботи розподілених файлових систем; технологій проектування систем захисту інформації в розподілених ІС (РІС); технологій оптимізації та пошуку і прийняття рішень при створенні систем захисту РІС; Технології обміну інформацією в РІС; формування умінь та навичок з вибору засобів ОС та програмно-апаратного забезпечення для розробки розподілених додатків; проектування і розробки РІС та систем їх захисту; підтримки працездатності РІС в заданих функціональних характеристиках та забезпечення їх відповідності заданим критеріям якості, тощо; отримання кваліфікації як фахівця з питань обслуговування мереж, розробника та інтегратора БД; адміністратора мережі ІКТ; директора з ІКТ безпеки; адміністратора Web-сайту; менеджера з розвитку Web-бізнесу; адміністратора безпеки ІКТ, тощо (відповідно до «Проекту реєстру кваліфікацій: сфера ІТ та цифрові професії» від 03.09.2020 року).

Дисципліна «Прикладні аспекти моніторингу та аудиту захищених інформаційно-комунікаційних систем» передбачає формування у здобувачів наукового ступеня «доктор філософії» професійних компетенцій та здатностей щодо створення системи моніторингу та аудиту стану інформаційної безпеки для забезпечення заданих показників захищеності інформації в розподілених обчислювальних системах. Завданнями навчальної дисципліни є формування

умінь із: обґрунтування варіантів побудови автоматизованої системи моніторингу та аудиту стану інформаційної безпеки для розподіленої обчислювальної системи та її основні складові: систему аналізу вразливостей, систему виявлення вторгнень, систему управління комплексною системою захисту інформації; застосування міждержавних та вітчизняних стандартів при створенні системи моніторингу та аудиту стану ІБ; створення перспективних систем моніторингу та аудиту стану ІБ.

Дисципліна «Забезпечення безпеки об'єктів критичної інфраструктури в умовах ведення кібердій і кіберконфліктів» передбачає вивчення способів формування вимог до систем безпеки об'єктів критичної інфраструктури (ОКІ); положення стандартів та нормативно-правових документів забезпечення їх захисту АСУ ОКІ від стороннього кібернетичного впливу; формування умінь та навичок з вибору стратегії дій на основі системного підходу використовуючи оброблену отриману інформацію; розробки неформалізованих моделей засобів, систем і процесів, що застосовуються в ОКІ та їх аналізу з точки зору ІКБ; забезпечення функціонування ОКІ в частині виконання вимог ІКБ; розробки планів і проведення заходів щодо організації захисту інформації (забезпечення кібербезпеки) ОКІ; побудови та перевірки моделей аналізу і синтезу інформаційно-комунікаційних систем та мереж; отримання кваліфікації як аналітика даних, Web-аналітика, ризик-менеджера, менеджера соціальних мереж, консультанта з питань ІКТ безпеки, експерта з кібернетики, директора з ІКТ безпеки; адміністратора безпеки ІКТ, тощо (відповідно до «Проекту реєстру кваліфікацій: сфера ІТ та цифрові професії» від 03.09.2020 року).

Дисципліна «Прикладні аспекти управління інформаційною та кібербезпекою об'єктів критичної інфраструктури» передбачає формування у здобувачів наукового ступеня «доктор філософії» професійних компетенцій та здатностей щодо створення комплексних систем захисту інформації (КСЗІ) в інформаційних, комунікаційних та ІТС, здійснення комплексу заходів, спрямованих на розроблення і впровадження інформаційних технологій, які забезпечують обробку інформації в ІТС згідно з вимогами, встановленими нормативно-правовими актами та нормативними документами у сфері захисту інформації. Завданнями дисципліни є формування умінь із побудови систем захисту інформації адміністрування систем захисту інформації.

Дисципліна «Технології безпеки складних соціотехнічних систем» передбачає вивчення сучасного стану проблеми безпеки в соціотехнічних системах (СТС), що є складною сукупністю взаємодій людини, інформаційної системи, навколишнього середовища в умовах впливу на них соціальних, економічних, політичних, природних, технічних та інших факторів; формування умінь та навичок з проведення оцінку безпеки СТС по заданому критерію; прогнозування можливих витоків повідомлень в СТС, моделювання систем захисту; імовірнісного аналізу помилок в повідомленні та сумарних

помилок на різних рівнях інформаційного взаємодії; отримання кваліфікації як аналітика клієнтського досвіду, менеджера з оптимізації пошукових систем, Web-розробника, ризик-менеджера, менеджера соціальних мереж, тощо (відповідно до «Проекту реєстру кваліфікацій: сфера ІТ та цифрові професії» від 03.09.2020 року).

Дисципліна «Прикладні аспекти протидії кібератакам в соціотехнічних системах» передбачає формування у здобувачів наукового ступеня «доктор філософії» професійних компетенцій та здатностей самостійної реалізації інформаційних операцій і атак в соціотехнічних системах, розробки організаційно-правових заходів захисту, необхідних для попередження атак в сфері управління ІБ. Завданнями дисципліни є формування умінь із реалізації інформаційних операцій і атак на соціотехнічні системи застосування механізмів оцінки та побудови заходів захисту від інформаційних операцій і атак в сфері управління інформаційною безпекою.

Матриця відповідності програмних компетентностей вибірковим компонентам освітньо-наукової програми

	ЗК3	ЗК4	ФК2	ФК3	ФК4	ФК5	ФК6	ФК7
ВДК.01	+	+	+		+			
ВДК.02				+		+	+	
ВДК.03			+					+
ВДК.04					+			+
ВДК.05						+	+	+

Матриця забезпечення програмних результатів навчання відповідними вибірковими компонентами освітньо-наукової програми

	ПР4	ПР5	ПР6	ПР7
ВДК.01	+			
ВДК.02	+	+	+	
ВДК.03	+			+
ВДК.04	+			+
ВДК.05		+	+	+