

# 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 другого (магістерського) рівня вищої освіти**

**за спеціальністю: 125 Кібербезпека**  
**галузі знань: 12 Інформаційні технології**  
**освітньої кваліфікації: магістр з кібербезпеки**  
**професійної кваліфікації: не врегульована**

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

Київ 2019

**ЛИСТ ПОГОДЖЕННЯ**  
**змін до опису освітньо-професійної програми**

Розроблено і погоджено робочою групою у складі:

*БЕССАЛОВ* *Анатолій Володимирович*, доктор технічних наук,  
професор, професор кафедри інформаційної та кібернетичної  
безпеки Київського університету імені Бориса Грінченка



*СЕМКО* *Віктор Володимирович*, доктор технічних наук,  
доцент, професор кафедри інформаційної та кібернетичної  
безпеки Київського університету імені Бориса Грінченка



*КОРШУН* *Наталія Володимирівна*, доктор технічних наук,  
доцент, професор кафедри інформаційної та кібернетичної  
безпеки Київського університету імені Бориса Грінченка



Завідувач кафедри інформаційної  
та кібернетичної безпеки Київського  
університету імені Бориса Грінченка  
д.т.н., професор



В.Л. БУРЯЧОК

Вчена рада Факультету інформаційних технологій та управління Київського  
університету імені Бориса Грінченка

Протокол від "27" серпня 2019 р. №8

Голова Вченої ради



А.В. Михацька

Науково-методичний центр стандартизації та якості освіти

Завідувач



О.В. Леонтєва

"28" серпня 2019 р.

Проректор з науково-методичної та навчальної роботи



О.Б. Жильцов

"28" серпня 2019 р.

Зміни до освітньо-професійної програми (ОПП) зумовлені необхідністю розширення компетентностей майбутніх фахівців в контексті сучасних SMART-технологій. Потреба у вказаних вище компетентностях була виявлена при аналізі відповідних публікацій, консультацій з роботодавцями в різних галузях науки і економіки сучасного високотехнологічного інформаційного суспільства (влада, державний і бізнес сектора економіки держави, тощо), а також потреб громади та влади міста Києва у створенні комфортної та ефективної цифрової інфраструктури міста.

Ці зміни стосуються об'єктів вивчення та діяльності, змісту і назви фахових дисциплін з метою приведення їх у відповідність до сучасного стану галузі. Не підлягали суттєвому перегляду програмні компетентності та очікувані результати навчання, ресурсне забезпечення, форми підсумкової атестації чи інші частини характеристик ОПП.

Зокрема

1) уточнено **об'єкти вивчення та діяльності**:

– методи застосування уразливостей в телекомунікаційних технологіях і *SMART-інфраструктурі* та способи боротьби з ними, методи організації захищеної передачі даних у незахищеному *SMART-середовищі*, засоби спеціального мережевого обладнання для забезпечення безпеки корпоративних мереж;

– концепції проектування, побудови та експлуатації захищених проводових і *безпроводових телекомунікаційних та SMART-систем*;

2) уточнено **фахові компетентності**:

**ФК-1**: Здатність до застосування сучасних безпекових інформаційних та *SMART-технологій* у сфері захисту інформації;

**ФК-2**: Здатність до виявлення уразливостей та забезпечення безпеки *телекомунікаційних технологій і SMART-інфраструктури*, розслідування інцидентів інформаційної та/або кібербезпеки та протидії зловмисному програмному забезпеченню;

3) уточнено **програмні результати**:

**ПРН-2**:

– вміти виявляти і формулювати актуальні наукові проблеми, генерувати та інтегрувати нові ідеї та нові знання у сфері захисту інформації, інформаційної та/або кібербезпеки;

– вміти застосовувати спеціалізовані програмні пакети, сучасні інформаційні та/або безпекові технології у сфері захисту інформації;

– знати уразливості й методи їх застосування в різних телекомунікаційних технологіях та *SMART-інфраструктурі*;

– знати способи боротьби з даними уразливостями, а також спеціалізоване мережеве обладнання, що застосовується для забезпечення безпеки корпоративних мереж;

– вміти проектувати захищені (з урахуванням загроз) проводові і *безпроводові телекомунікаційні та SMART-системи*;

– знати методи організації захищеної передачі даних у незахищеному середовищі.

4) змінено *назву дисципліни* «Технології безпеки мережевої інфраструктури» змінено на «Технології безпеки мережевої та SMART- інфраструктури».

Таким чином, основні зміни стосувалися частини 1 «Профіль освітньої-професійної програми зі спеціальності 125 «Кібербезпека»» в сегментах 6 і 7, а також частини 2 ОПП в сегментах 2.1. «Перелік та розподіл кредитних обсягів дисциплін навчального плану підготовки здобувачів другого рівня вищої освіти – магістр» та 2.2. «Структурно-логічна схема ОПП».

Нові редакції цих частин освітньо-професійної програми містяться нижче.

## 1. Профіль освітньої-професійної програми зі спеціальності 125 «Кібербезпека»

6 – Компетентності випускника		
Фахові компетентності спеціальності (КФ)	ФК-1	Здатність до застосування сучасних безпекових інформаційних та SMART-технологій у сфері захисту інформації
	ФК-2	Здатність до виявлення уразливостей та забезпечення безпеки телекомунікаційних технологій і SMART-інфраструктури, розслідування інцидентів інформаційної та/або кібербезпеки та протидії злоякісному програмному забезпеченню
7 – Результати навчання		
Знання та розуміння	ПРН-2	<ul style="list-style-type: none"> <li>– вміти виявляти і формулювати актуальні наукові проблеми, генерувати та інтегрувати нові ідеї та нові знання у сфері захисту інформації, інформаційної та/або кібербезпеки;</li> <li>– вміти застосовувати спеціалізовані програмні пакети, сучасні інформаційні та/або безпекові технології у сфері захисту інформації;</li> <li>– знати уразливості й методи їх застосування в різних телекомунікаційних технологіях та SMART-інфраструктурі;</li> <li>– знати способи боротьби з даними уразливостями, а також спеціалізоване мережеве обладнання, що застосовується для забезпечення безпеки корпоративних мереж;</li> <li>– вміти проектувати захищені (з урахуванням загроз) проводові і безпроводові телекомунікаційні та SMART-системи;</li> <li>– знати методи організації захищеної передачі даних у незахищеному середовищі.</li> </ul>

## 2. Перелік компонентів освітньо-професійної програми та їх логічна послідовність

2.1. Перелік та розподіл кредитних обсягів дисциплін навчального плану підготовки здобувачів другого рівня вищої освіти – магістр, за спеціальністю – 125 «Кібербезпека» (90 кредитів ECTS - 1 рік 4 місяці)

Шифр н/д	Компоненти освітньої програми (навчальні дисципліни, курсові проекти (роботи), практики, кваліфікаційна робота)	Кількість кредитів ECTS / %	Розподіл годин на за курсами і семестрами			Форма підсумкового контролю
			5 курс		6 курс	
			9	10	11	
<b>I. ОBOB'ЯЗKOBA ЧACТИHA</b>						
<b>1. Навчальні дисципліни</b>						
<i>Формування спеціальних (фахових, предметних) компетентностей</i>						
ОДФ.01	Іноземна мова професійного спрямування	5	3	2		залік
ОДФ.02	Організація науки і наукових досліджень	4	4			залік
ОДФ.03	Прикладна загальна теорія систем безпеки	4	4			екзамен
ОДФ.04	Технології безпеки мережевої та SMART-інфраструктури	7	7			екзамен, КР
ОДФ.05	Технології безпеки безпроводових і мобільних мереж	7	7			залік
ОДФ.06	Технології безпеки Web-ресурсів	6		6		екзамен
ОДФ.07	Технології розслідування інцидентів безпеки	6		6		залік
ОДФ.08	Прикладні аспекти тестувань на проникнення та етичного хакінгу	6		4	2	залік, екзамен
<b>Всього</b>		<b>45</b>	<b>25</b>	<b>18</b>	<b>2</b>	

2. Практика						
ОП.01	Виробнича (технологічна) практика	3			3	залік
ОП.02	Науково-дослідницька практика	3			3	залік
ОП.03	Переддипломна практика	6			6	залік
		<b>Всього</b>	<b>12</b>	<b>0</b>	<b>12</b>	
3. Атестація						
ОА.1	Підготовка кваліфікаційної магістерської роботи	4,5			4,5	
	Захист кваліфікаційної магістерської роботи	1,5			1,5	
		<b>Всього</b>	<b>6</b>	<b>0</b>	<b>4,5</b>	<b>1,5</b>
<b>Загальний обсяг обов'язкової частини</b>		<b>63</b>	<b>25</b>	<b>22,5</b>	<b>15,5</b>	
2						
ВИБІРКОВА ЧАСТИНА						
4. Навчальні дисципліни						
4.1. Спеціалізований блок навчальних дисциплін						
ВДС.01	Моніторинг, аудит та адміністрування захищених ІТ систем і мереж	7	5	2		залік, екзамен
ВДС.02	Технології розробки і тестування ПЗ мережевої безпеки	6		6		екзамен
ВДС.03	Технології протидії злов'язісному програмному коду	6			6	екзамен
ВДС.04	Математичні методи криптографії	4		4		залік
ВДС.05	Методи побудови і аналізу криптосистем	4			4	залік
		<b>Всього</b>	<b>27</b>	<b>5</b>	<b>12</b>	<b>10</b>
4.2. Вибір дисциплін із каталогу (студент обирає дисципліни на відповідну кількість кредитів)						
ВД 1.01	Вибір з каталогу курсів	27	5	12	10	залік, екзамен
<b>Загальний обсяг вибіркової частини</b>		<b>27</b>				
<b>ЗАГАЛЬНИЙ ОБСЯГ ОСВІТНЬОЇ ПРОГРАМИ</b>		<b>90</b>	<b>30</b>	<b>34,5</b>	<b>25,5</b>	

## 2.2. Структурно-логічна схема ОПП

5 курс				6 курс			
9 семестр		10 семестр		11 семестр			
Іноземна мова за фаховим спрямуванням, 3+2= 5 кр., каф. ІМ				Методи побудови і аналізу криптосистем,			
Організація науки і наукових досліджень, наукові засади педагогічного процесу вищої школи методологія та засади наукового дослідження, організація та проведення наукових досліджень, організація навчально-наукового процесу у ВНЗ тощо 4 кр. каф. ПМД	Технології безпеки мережевої та SMART-інфраструктури уразливості ІТС, методи їх застосування та способи боротьби з ними, спеціалізовані засоби обладнання для забезпечення безпеки корпоративних мереж. Практичні навички проектування захищених проводних ІТС. Методи передачі захисту інф. в не захищеному середовищі тощо 7 кр., каф. ІКБ	Технології безпеки Web-ресурсів уразливості Web-ресурсів (url-код, брутфорс, xss тощо) та основні способи боротьби з ними на етапах розробки та в процесі експлуатації. Знання найбільш провідних безпечних Web-додатків тощо 6 кр., каф. ІКБ	Математичні методи криптографії, теорія чисел, теорія ймовірностей і математична статистика та теорія обчислювальної складовості в сучасній криптографії тощо 4 кр., каф. ІКБ	Виробнича (технологічна) практика, 3 кр.			
Примкладна загальна теорія систем безпеки поширення складних динамічних систем безпеки, основні моделювання процесів в системах безпеки, математичні методи оптимізації та системного аналізу, основні проєктування ІЗІ ІТС та реалізації таких проєктів, прийняття рішень при створенні і впровадженні систем безпеки, основні методи аналізу ризиків та управління ними тощо 4 кр., каф. ІКБ	Технології безпеки безпроводних і мобільних мереж уразливості безпроводних та мобільних мереж, виявлення задрів промислових або державних до них порушень. Знання спеціалізовані мережеві обладнання, що застосовуються для забезпечення безпеки таких мереж. Діагностика проєктування захищених без проводних мереж тощо 7 кр., каф. ІКБ	Технології розслідування інцидентів безпеки організація процесу розслідування інцидентів у відповідності зі стандартами ISO27001, ISO27037, ISO27031, NIST SP 800-6, тощо 6 кр., каф. ІКБ	Технології розробки і тестування ПЗ мережевої безпеки методи й способи розробки та тестування ПЗ з врахуванням та урахуванням захищеності, що застосовуються в ІТС – шифрування, фільтрація, сканери портів тощо 6 кр., каф. ІКБ	Науково-дослідницька практика, 3 кр.			
Моніторинг, аудит та адміністрування захищених ІТ систем і мереж, засоби і уразливості ІТС на основі аналізу на під системних, виявлення вторгнень та управління кваліфікованими системними задрями, стандарти в сфері моніторингу систем безпеки, організаційно-правові основи проведення аудиту безпеки, основні методи проєктування засобів захисту інформації та засоби забезпечення фізичної безпеки, структура та зміст аудиторського звіту, адміністрування у процесі проєктування та введення в експлуатацію захищених ІТС, технічна експлуатація та технічне обслуговування таких систем, надійність захищених ІТС 5+2= 7 кр., каф. ІКБ				Технології протидії злов'язісному програмному коду методи й способи системного аналізу файлів, аномалій злов'язісного ПЗ та моделювання його уразливостей, відновлення пошкодженої інформації тощо. 6 кр., каф. ІКБ		Переддипломна практика, 6 кр.	
				Прикладні аспекти тестування на провикнення та етичного хакінгу методи і способи використання мережевих ресурсів на наявність уразливостей безпеки та пошук шляхів щодо їх усунювання тощо 4+2=6 кр., каф. ІКБ		Підготовка магістерської роботи, 6 кр.	
30 кр.		30 кр.		30 кр.			
Цілевий дисципліни формування загальних компетентностей		Цілевий дисципліни формування фахових (предметних) компетентностей		Цілевий дисципліни поглиблення фахових компетентностей			
ОБОВ'ЯЗКОВІ	Дисципліни гуманітарної та соціально-економічної підготовки - 13 кр.	ОБОВ'ЯЗКОВІ	Дисципліни спеціальної підготовки - 20 кр. Дисципліни фахової спеціалізації - 12 кр.	ВИБІРКОВІ	Дисципліни курсової підготовки - 8 кр. Дисципліни спеціалізованого курсу - 19 кр.		

## Керівник проєктної групи (гарант освітньо-професійної програми)

Професор кафедри Інформаційних технологій та математичних дисциплін Факультету Інформаційних технологій та управління Київського університету імені Бориса Грінченка  
доктор технічних наук, професор



**В.Л. БУРЯЧОК**