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

ЛИСТ ПОГОДЖЕННЯ

змін до опису освітньо-професійної програми

Розроблено і погоджено робочою групою у складі:

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

БЕССАЛОВ Анатолій Володимирович, доктор технічних наук, професор, 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. Леонтьєва
"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 безпровідних, мобільних, хмарних та *SMART-технологіях* та способи боротьби з ними, методи організації захищеної передачі даних у незахищеному *SMART-середовищі*, засоби спеціального мережевого обладнання для забезпечення безпеки корпоративних мереж;

2) уточнено ***фахові компетентності***:

КФ-2: Здатність до використання інформаційно-комунікаційних та *SMART-технологій*, сучасних методів і моделей інформаційної та/або кібербезпеки;

КФ-3: Здатність до використання програмних та програмно-апаратних комплексів засобів захисту інформації в інформаційно-телекомунікаційних (автоматизованих) та *SMART-системах*;

КФ-5: Здатність забезпечувати захист інформації, що обробляється в інформаційно-телекомунікаційних (автоматизованих) та *SMART-системах* з метою реалізації встановленої політики інформаційної та/або кібербезпеки.;

КФ-6: Здатність відновлювати штатне функціонування інформаційних, інформаційно-телекомунікаційних (автоматизованих) та *SMART-систем* після реалізації загроз, здійснення кібератак, збоїв та відмов різних класів та походження;

КФ-11: Здатність виконувати моніторинг процесів функціонування інформаційних, інформаційно-телекомунікаційних (автоматизованих) та *SMART-систем* згідно встановленої політики інформаційної та/або кібербезпеки;

3) уточнено ***програмні результати***:

ПРз-1: - готувати пропозиції до нормативних актів і документів з метою забезпечення встановленої політики інформаційної та/або кібербезпеки;

- розробляти проектну документацію, щодо програмних та програмно-апаратних комплексів захисту інформаційних, інформаційно-телекомунікаційних (автоматизованих) та *SMART-систем*;

- виконувати аналіз реалізації прийнятої політики інформаційної та/або кібербезпеки;

ПРз-2: - здійснювати професійну діяльність на основі знань сучасних інформаційно-комунікаційних та *SMART-технологій*;

- розробляти та аналізувати проекти *IT* та *SMART-систем* базуючись на стандартизованих технологіях та протоколах передачі даних;

- застосовувати в професійній діяльності знання, навички та практики, щодо структур сучасних обчислювальних систем, методів і засобів обробки інформації, архітектур операційних систем;

- здійснювати захист ресурсів і процесів в ІТС на основі моделей безпеки (кінцевих автоматів, управління потоками, Bell-LaPadula, Biba, Clark-Wilson, та інші), а також встановлених режимів безпечного функціонування *IT* та *SMART-системах*;

ПРз-3: - забезпечувати процеси захисту інформаційно-телекомунікаційних (автоматизованих) та *SMART-систем* шляхом встановлення та коректної експлуатації програмних та програмно-апаратних комплексів засобів захисту;

- забезпечувати функціонування спеціального програмного забезпечення, щодо захисту даних від руйнуючих програмних впливів, руйнуючих кодів в інформаційних, інформаційно-телекомунікаційних (автоматизованих) та *SMART-системах*;

- виконувати розробку експлуатаційної документації на КЗЗ;

ПРз-4: - вирішувати задачі супроводу (в.т. числі: огляд, тестування, підзвітність) системи управління доступом згідно принципів, критеріїв доступу та встановленої політики безпеки в інформаційних та інформаційно-телекомунікаційних (автоматизованих) та *SMART-системах*;

- реалізовувати заходи з протидії отриманню несанкціонованого доступу до інформаційних ресурсів і процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) та *SMART-системах*;

- вирішувати задачі управління доступом до інформаційних ресурсів та процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) та *SMART-системах* на основі моделей управління доступом (мандатних, дискриційних, рольових);

- вирішувати задачі централізованого і децентралізованого адміністрування доступом до інформаційних ресурсів і процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) та *SMART-системах*;

- забезпечувати введення підзвітності системи управління доступом інформаційних ресурсів і процесів в *IT* та *SMART-системах*;

ПРз-5: - обирати основні методи та засоби захисту інформації відповідно до вимог сучасних стандартів інформаційної і кібербезпеки, та критеріїв безпеки інформаційних технологій, застосовуючи системний підхід та знання основ теорії захисту інформації;

- вирішувати задачі управління процедурами ідентифікації, автентифікації, авторизації, користувачів і процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) та *SMART-системах;*

- проектувати та реалізувати комплексні системи захисту інформації в АС організації (підприємства) відповідно до вимог нормативних документів системи технічного захисту інформації;

- вирішувати задачі захисту потоків даних в інформаційних, інформаційно-телекомунікаційних (автоматизованих) та *SMART-системах*;

- визначати рівень захищеності інформаційних ресурсів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) та *SMART-системах*;

- використовувати інструментальні засоби оцінювання можливості реалізації потенційних загроз інформації, що обробляється в інформаційно-телекомунікаційних (автоматизованих) та *SMART-системах*;

ПРз-7: - вирішувати задачі супроводу та впровадження комплексних систем захисту інформації, а також протидії несанкціонованому доступу до ресурсів і процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) та *SMART-системах*;

- здійснювати оцінку рівня захищеності інформації що обробляється в *IT* та *SMART-системах* використовувати інструментальні засоби оцінювання наявності потенційних вразливостей;

- вирішувати задачі управління комплексною системою захисту інформації в інформаційних та інформаційно-телекомунікаційних (автоматизованих) та *SMART-системах*;

- вирішувати задачі експертизи, випробування КСЗІ;

ПРз-8: - вирішувати задачі попередження та виявлення, ідентифікації, аналізу та реагування на інциденти в інформаційних, інформаційно-телекомунікаційних (автоматизованих) та *SMART-системах*;

- проводити розслідування інцидентів інформаційної та/або кібербезпеки базуючись на національних та міжнародних регулюючих актах, процедурах та положеннях в сфері інформаційної та/або кібербезпеки;

- забезпечувати дотримання політики ведення журналів реєстрації подій та інцидентів з встановленим рівнем деталізації;

ПРз-10: - аналізувати та визначати можливість застосування технологій, методів та засобів криптографічного захисту інформації;

- аналізувати та визначати можливість застосування технологій, методів та засобів технічного захисту інформації;

- виявляти небезпечні сигнали технічних засобів;

- вимірювати параметри небезпечних та завадових сигналів під час інструментального контролю захищеності інформації від витоку технічними каналами;

- визначати ефективність захисту інформації від витоку технічними каналами відповідно до вимог нормативних документів системи технічного захисту інформації;

- інтерпретувати результати проведення спеціальних вимірювань з використанням технічних засобів, контролю характеристик *IT* та *SMART-систем* відповідно до вимог нормативних документів системи технічного захисту інформації;

- обґрунтовувати можливість створення технічних каналів витоку інформації на об'єктах інформаційної діяльності;

- впроваджувати заходи та засоби технічного захисту інформації від витоку технічними каналами;

ПРз-11: - забезпечувати процеси моніторингу доступу до ресурсів і процесів *IT* та *SMART-систем*;

- забезпечувати конфігурування та функціонування систем моніторингу ресурсів та процесів в *IT* та *SMART-системах*;

ПРз-12: - виконувати впровадження та підтримку систем виявлення вторгнень та використовувати комплекси захисту для забезпечення необхідного рівня захищеності інформації в інформаційних, інформаційно-телекомунікаційних (автоматизованих) та *SMART-системах*;

- аналізувати ефективність систем виявлення та протидії несанкціонованому доступу до ресурсів і процесів в *IT* та *SMART-системах*;

- аналізувати та впроваджувати системи захисту від зловмисних програмних кодів.

4) змінено ***назву дисципліни*** «Безпека безпровідних, мобільних та хмарних технологій» змінено на «Безпека безпровідних, мобільних, хмарних та SMART- технологій».

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)	**КФ -2**	Здатність до використання інформаційно-комунікаційних та *SMART-технологій*, сучасних методів і моделей інформаційної та/або кібербезпеки.
	КФ -3	Здатність до використання програмних та програмно-апаратних комплексів засобів захисту інформації в інформаційно-телекомунікаційних (автоматизованих) *SMART-системах.*
	К Ф-5	Здатність забезпечувати захист інформації, що обробляється в інформаційно-телекомунікаційних (автоматизованих) та *SMART-системах* з метою реалізації встановленої політики інформаційної та/або кібербезпеки.
	КФ -6	Здатність відновлювати штатне функціонування інформаційних, інформаційно-телекомунікаційних (автоматизованих) та *SMART-систем* після реалізації загроз, здійснення кібератак, збоїв та відмов різних класів та походження.
	КФ -11	Здатність виконувати моніторинг процесів функціонування інформаційних, інформаційно-телекомунікаційних (автоматизованих) та *SMART-систем* згідно встановленої політики інформаційної та/або кібербезпеки.
7 – Результати навчання		
Знання та розуміння	**ПРз-1**	- готувати пропозиції до нормативних актів і документів з метою забезпечення встановленої політики інформаційної та/або кібербезпеки; - розробляти проектну документацію, щодо програмних та програмно-апаратних комплексів захисту інформаційних, інформаційно-телекомунікаційних (автоматизованих) та *SMART-систем*; - виконувати аналіз реалізації прийнятої політики інформаційної та/або кібербезпеки;
	ПРз-2	- здійснювати професійну діяльність на основі знань сучасних інформаційно-комунікаційних та *SMART-технологій*; - розробляти та аналізувати проекти *IT* та *SMART-систем* базуючись на стандартизованих технологіях та протоколах передачі даних; - застосовувати в професійній діяльності знання, навички та практики, щодо структур сучасних обчислювальних систем, методів і засобів обробки інформації, архітектур операційних систем; - здійснювати захист ресурсів і процесів в ІТС на основі моделей безпеки (кінцевих автоматів, управління потоками, Bell-LaPadula, Biba, Clark-Wilson, та інші), а також встановлених режимів безпечного функціонування *IT* та *SMART-системах*; - виконувати аналіз програмного забезпечення з метою оцінки на відповідність встановленим вимогам інформаційної та/або кібербезпеки в *IT* та *SMART-системах*;
	ПРз-3	- забезпечувати процеси захисту інформаційно-телекомунікаційних (автоматизованих) та *SMART-систем* шляхом встановлення та коректної експлуатації програмних та програмно-апаратних комплексів засобів захисту; - забезпечувати функціонування спеціального програмного забезпечення, щодо захисту даних від руйнуючих програмних впливів, руйнуючих кодів в інформаційних, інформаційно-телекомунікаційних (автоматизованих) та *SMART-системах*; - виконувати розробку експлуатаційної документації на КЗЗ;
	ПРз-4	- вирішувати задачі супроводу (в.т. числі: огляд, тестування, підзвітність) системи управління доступом згідно принципів, критеріїв доступу та встановленої політики безпеки в інформаційних та інформаційно-телекомунікаційних (автоматизованих) та *SMART-системах*; - реалізовувати заходи з протидії отриманню несанкціонованого доступу до інформаційних ресурсів і процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) та *SMART-системах*; - вирішувати задачі управління доступом до інформаційних ресурсів та процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) та *SMART-системах* на основі моделей управління доступом (мандатних, дискреційних, рольових); - вирішувати задачі централізованого і децентралізованого адміністрування доступом до інформаційних ресурсів і процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) та *SMART-системах*;

		- забезпечувати введення підзвітності системи управління доступом інформаційних ресурсів і процесів в *IT* та *SMART-системах*;
	ПРз-5	- обирати основні методи та засоби захисту інформації відповідно до вимог сучасних стандартів інформаційної і кібербезпеки, та критеріїв безпеки інформаційних технологій, застосовуючи системний підхід та знання основ теорії захисту інформації; - вирішувати задачі управління процедурами ідентифікації, автентифікації, авторизації, користувачів і процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) та *SMART-системах;* - проектувати та реалізувати комплексні системи захисту інформації в АС організації (підприємства) відповідно до вимог нормативних документів системи технічного захисту інформації; - вирішувати задачі захисту потоків даних в інформаційних, інформаційно-телекомунікаційних (автоматизованих) та *SMART-системах*; - визначати рівень захищеності інформаційних ресурсів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) та *SMART-системах*; - використовувати інструментальні засоби оцінювання можливості реалізації потенційних загроз інформації, що обробляється в інформаційно-телекомунікаційних (автоматизованих) та *SMART-системах*;
	ПРз-7	- вирішувати задачі супроводу та впровадження комплексних систем захисту інформації, а також протидії несанкціонованому доступу до ресурсів і процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) та *SMART-системах*; - здійснювати оцінку рівня захищеності інформації що обробляється в *IT* та *SMART-системах* використовувати інструментальні засоби оцінювання наявності потенційних вразливостей; - вирішувати задачі управління комплексною системою захисту інформації в інформаційних та інформаційно-телекомунікаційних (автоматизованих) та *SMART-системах*; - вирішувати задачі експертизи, випробування КСЗІ;
	ПРз-8	- вирішувати задачі попередження та виявлення, ідентифікації, аналізу та реагування на інциденти в інформаційних, інформаційно-телекомунікаційних (автоматизованих) та *SMART-системах*; - проводити розслідування інцидентів інформаційної та/або кібербезпеки базуючись на національних та міжнародних регулюючих актах, процедурах та положеннях в сфері інформаційної та/або кібербезпеки; - забезпечувати дотримання політики ведення журналів реєстрації подій та інцидентів з встановленим рівнем деталізації;
	ПРз-10	- аналізувати та визначати можливість застосування технологій, методів та засобів криптографічного захисту інформації; - аналізувати та визначати можливість застосування технологій, методів та засобів технічного захисту інформації; - виявляти небезпечні сигнали технічних засобів; - вимірювати параметри небезпечних та завадових сигналів під час інструменттального контролю захищеності інформації від витоку технічними каналами; - визначати ефективність захисту інформації від витоку технічними каналами відповідно до вимог нормативних документів системи технічного захисту інформації; - інтерпретувати результати проведення спеціальних вимірювань з використанням технічних засобів, контролю характеристик *IT* та *SMART-систем* відповідно до вимог нормативних документів системи технічного захисту інформації; - обгрунтовувати можливість створення технічних каналів витоку інформації на об'єктах інформаційної діяльності; - впроваджувати заходи та засоби технічного захисту інформації від витоку технічними каналами;
	ПРз-11	- забезпечувати процеси моніторингу доступу до ресурсів і процесів *IT* та *SMART-систем*; - забезпечувати конфігурування та функціонування систем моніторингу ресурсів та процесів в *IT* та *SMART-системах*;
	ПРз-12	- виконувати впровадження та підтримку систем виявлення вторгнень та використовувати комплекси захисту для забезпечення необхідного рівня захищеності інформації в інформаційних, інформаційно-телекомунікаційних (автоматизованих) та *SMART-системах*; - аналізувати ефективність систем виявлення та протидії несанкціонованому доступу до ресурсів і процесів в *IT* та *SMART-системах*; - аналізувати та впроваджувати системи захисту від зловмисних програмних кодів.

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

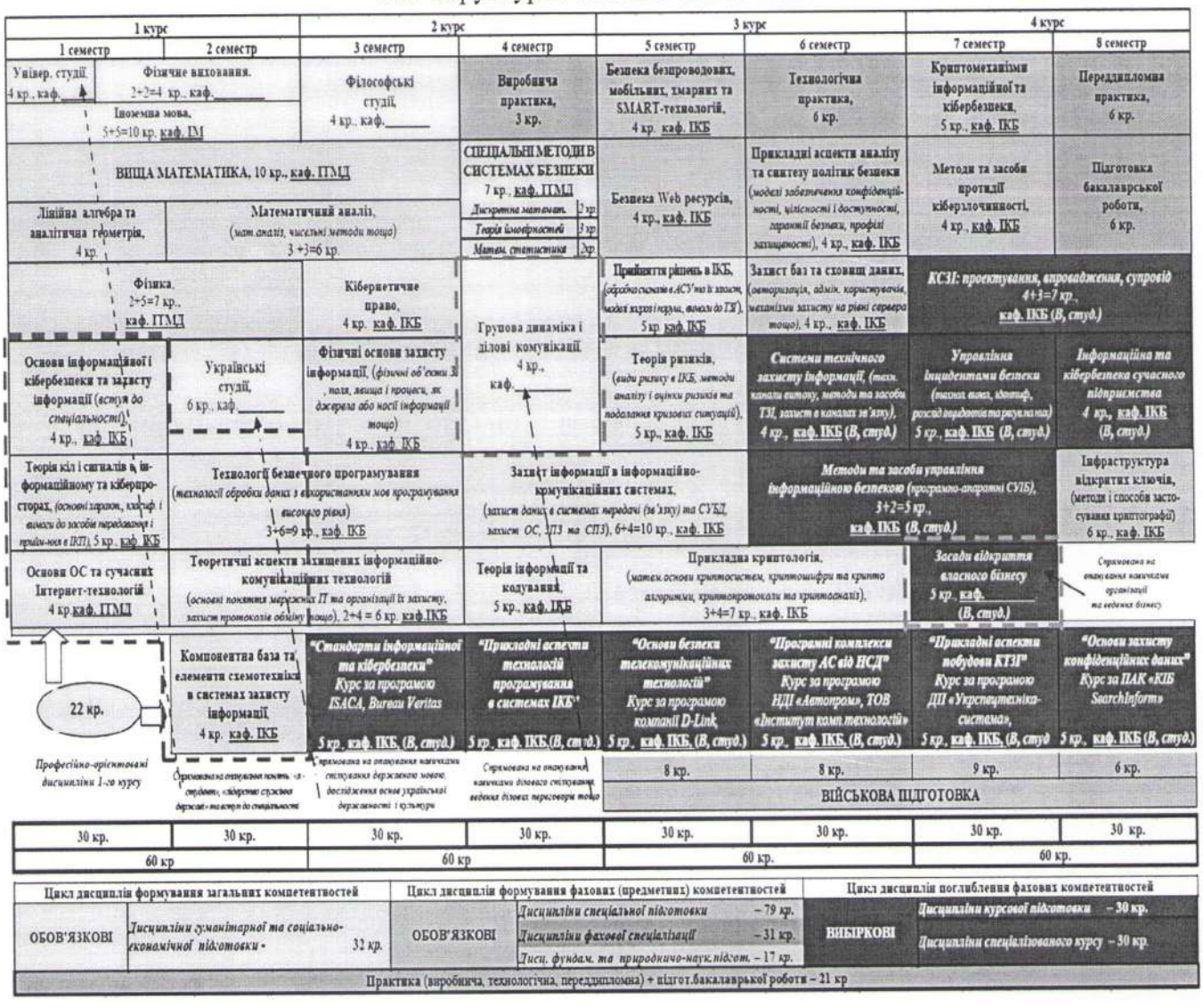
2.1. Перелік та розподіл кредитних обсягів дисциплін навчального плану підготовки здобувачів першого рівня вищої освіти – бакалавр, за спеціальністю – 125 «Кібербезпека» (240 кредитів ECTS - 3 роки 10 місяців)

Код	Компоненти освітньої програми (навчальні дисципліни, курсові проекти (роботи), практики, кваліфікаційна робота)	кредитів	Розподіл аудиторних годин за курсами і семестрами								Форма підсумкового контролю
			1 курс		2 курс		3 курс		4 курс		
			1	2	3	4	5	6	7	8	
І. Обов'язкова частина											
1. Навчальні дисципліни											
Формування загальних компетентностей											
ОДЗ.01	Університетські студії	**4**	4								залік

	Я - студент	1	*								
	Лідерство служіння	1	*								
	Вступ до спеціальності	2	*								
ОДЗ.02	Іноземна мова	**10**	5	5							екзамен, залік
ОДЗ.03	Фізичне виховання	**4**	2	2							залік
ОДЗ.04	Українські студії	**6**		6							екзамен
ОДЗ.05	Філософські студії	**4**			4						екзамен
ОДЗ.06	Групова динаміка і ділові комунікації	**4**				4					залік
	Всього	**32**	**11**	**13**	**4**	**4**	**0**	**0**	**0**	**0**	
Формування спеціальних (фахових, предметних) компетентностей											
ОДС.01	Фізика	**7**	2	5							екзамен, залік
ОДС.02	Вища математика	**10**	4	3	3						залік, екзамен
	Лінійна алгебра та аналітична геометрія	4	*								
	Математичний аналіз та чисельні методи	6		*	*						
ОДС.03	Основи інформаційної і кібербезпеки та захисту інформації	**4**	4								залік
ОДС.04	Теорія кіл і сигналів в інформаційному та кіберпросторах	**5**	5								екзамен
ОДС.05	Основи ОС та сучасних Інтернет-технологій	**4**	4								залік
ОДС.06	Технології безпечного програмування	**9**		3	6						екзамен, залік, КР
ОДС.07	Теоретичні аспекти захищених інформаційно-комунікаційних технологій	**6**		2	4						екзамен, залік
ОДС.08	Компонентна база та елементи схемотехніки в сист.захисту інформації	**4**		4							екзамен
ОДС.09	Кібернетичне право	**4**			4						залік
ОДС.10	Фізичні основи захисту інформації	**4**			4						екзамен
ОДС.11	Спеціальні методи в системах безпеки	**7**				7					екзамен
	Дискретна математика	4				*					
	Теорія ймовірностей та математична статистика	3				*					
ОДС.12	Захист інформації в інформаційно-комунікаційних системах	**10**				6	4				екзамен, залік, КР
ОДС.13	Теорія інформації та кодування	**5**				5					екзамен
ОДС.14	Прийняття рішень в інформаційній та кібербезпеці	**5**					5				екзамен
ОДС.15	Теорія ризиків	**5**					5				залік
ОДС.16	Прикладна криптологія	**7**					3	4			екзамен, залік
ОДС.17	Безпека безпроводових, мобільних, хмарних та *SMART*-технологій	**4**					4				екзамен
ОДС.18	Безпека Web ресурсів	**4**					4				екзамен
ОДС.19	Прикладні аспекти аналізу та синтезу політик безпеки	**4**						4			екзамен
ОДС.20	Захист баз та сховищ даних	**4**						4			екзамен
ОДС.21	Криптомеханізми інформаційної та кібербезпеки	**5**							5		екзамен
ОДС.22	Методи та засоби протидії кіберзлочинності	**4**							4		екзамен
ОДС.23	Інфраструктура відкритих ключів	**6**								6	екзамен
	Всього	**127**	**19**	**17**	**21**	**18**	**25**	**12**	**9**	**6**	
2. Практика											
ВП.2.01	Виробнича	**3**				3					залік
ВП.2.02	Виробнича (технологічна)	**6**						6			залік
ВП.2.03	Переддипломна	**6**								6	залік
	Всього	**15**	**0**	**0**	**0**	**3**	**0**	**6**	**0**	**6**	
3. Атестація											
ОА.01	Підготовка бакалаврської роботи	**4,5**								4,5	
	Захист бакалаврської роботи	**1,5**								1,5	
Всього		**6**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**6**	
	Разом за обов'язковою частиною	**180**	**30**	**30**	**25**	**25**	**25**	**18**	**9**	**18**	
ІІ. Вибіркова частина											
4. Навчальні дисципліни											
4.1. Спеціалізований блок навчальних дисциплін											
ВДК.1.01	Стандарти інформаційної та кібербезпеки	**5**			5						залік
ВДК.1.02	Прикладні аспекти побудови КТЗІ	**5**				5					екзамен
ВДК.1.03	Основи безпеки телекомунікаційних технологій	**5**					5				екзамен
ВДК.1.04	Програмні комплекси захисту АС від НСД	**5**						5			екзамен
ВДК.1.05	Прикладні аспекти програмування в системах ІКБ	**5**							5		екзамен

ВДК.1.06	Основи захисту конфіденційних даних	5								5	екзамен
ВДК.1.07	Системи технічного захисту інформації	4						4			залік
ВДК.1.08	Методи та засоби управління інформаційною безпекою	5						3	2		залік
ВДК.1.09	КСЗІ: проектування, впровадження, супровід	7							4	3	екзамен ,КР
ВДК.1.10	Управління інцидентами безпеки	5							5		залік
ВДК.1.11	Засади відкриття власного бізнесу	5							5		залік
ВДК.1.12	Інформаційна та кібербезпека сучасного підприємства	4								4	залік
Всього		60	0	0	5	5	5	12	21	12	
4.2. Вибір дисциплін з каталогу (студент обирає дисципліни на відповідну кількість кредитів)											
ВД 1.01	Вибір з каталогу курсів	60			5	5	5	12	21	12	екзамен, залік, КР
Разом за вибірковою частиною		60	0	0	5	5	5	12	21	12	
ЗАГАЛЬНИЙ ОБСЯГ ОСВІТНЬОЇ ПРОГРАМИ		240	30	30	30	30	30	30	30	30	

2.2. Структурно-логічна схема ОПП



Керівник проектної групи (гарант освітньо-професійної програми)
доцент кафедри управління Факультету інформаційних технологій та управління Київського університету імені Бориса Грінченка,
доктор технічних наук, доцент **В.В. СЕМКО**