МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

МАРІУПОЛЬСЬКИЙ ДЕРЖАВНИЙ УНІВЕРСИТЕТ

ЗАТВЕРДЖУЮ

Ректор

_____ К.В. Балабанов

«_26_»_____12_____ 2018 р.

ОСВІТНЬО-ПРОФЕСІЙНА ПРОГРАМА

РІВЕНЬ ВИЩОЇ ОСВІТИ Перший (бакалаврський) рівень
(назва рівня вищої освіти)

СТУПІНЬ ВИЩОЇ ОСВІТИ Бакалавр
(назва ступеня вищої освіти)

ГАЛУЗЬ ЗНАНЬ 12 Інформаційні технології
(шифр та назва галузі знань)

СПЕЦІАЛЬНІСТЬ 125 Кібербезпека
(код та найменування спеціальності)

Кібербезпека

Назва освітньо-професійної програми

Спеціалізація (за необхідністю)_____

СХВАЛЕНО

Протокол засідання Вченої ради МДУ
від 26.12.2018 № 5

Освітня програма вводиться в дію з 01 вересня 2018 р.
Ректор _____ К.В. Балабанов

(наказ № 3 від 08.01. 2019 р.)

«08» 01 2019 р.

І Преамбула

1. Розроблено і внесено кафедрою математичних методів та системного аналізу Маріупольського державного університету згідно стандарту вищої освіти за спеціальністю 125 «Кібербезпека» галузі знань 12 «Інформаційні технології» першого (бакалаврського) рівня, затвердженого і введеного в дію наказом Міністерства освіти і науки України від 04.10.2018 р. № 1047.
2. Затверджено та надано чинності рішенням Вченої ради МДУ від 26. 12 2018 р. протокол № 5 .
3. Розробники програми:
   Меркулова Катерина Володимірівна, к.т.н., доц., доцент кафедри математичних методів та системного аналізу МДУ.
   Коляда Юрій Євгенович, д.ф.-м.н., проф., завідувач кафедри математичних методів та системного аналізу МДУ.
   Зайцева Еліна Євгенівна, к.т.н., доцент кафедри математичних методів та системного аналізу МДУ.
   Крівенко Сергій Вікторович, к.т.н., доцент кафедри математичних методів та системного аналізу МДУ.
   Толюпа Сергій Васильович, д.т.н., проф, професор кафедри кібербезпеки та захисту інформації Київського національного університету імені Тараса Шевченка, професор кафедри математичних методів та системного аналізу МДУ (за сум).
   Неласа Ганна Вікторівна, к.т.н., доц., доцент кафедри математичних методів та системного аналізу МДУ.
4. Рецензії-відгуки зовнішніх стейкхолдерів:
   Крижановський Володимир Григорович, д.т.н., професор, професор кафедри радіофізики та кібербезпеки Донецького національного університету імені Василя Стуса, Гарант освітньої програми «Кібербезпека».
   Зінченко Сергій Георгійович, к.е.н., начальник відділу системи управління якістю ДП «Маріупольський морський торговельний порт».
   Ціон Павло Олександрович, заступник начальника Управління – начальник відділу протидії кіберзлочинам Донецької області Донецького Управління кіберполіції Департаменту кіберполіції Національної поліції України, капітан поліції.

ІІ Загальна характеристика

Рівень вищої освіти	Перший (бакалаврський) рівень
Ступінь вищої освіти	Бакалавр
Галузь знань	12 Інформаційні технології
Спеціальність	125 Кібербезпека
Обмеження щодо форм навчання	Денна, заочна
Освітня кваліфікація	Бакалавр з кібербезпеки \ Bachelor in Cyber Security.
Професійна(і) кваліфікація(ї) (тільки для регульованих професій)	
Кваліфікація в дипломі	Ступінь вищої освіти – Бакалавр Спеціальність – 125 Кібербезпека

	Освітня програма - Кібербезпека
Опис предметної області	Об’єкти професійної діяльності випускників: - об’єкти інформатизації, включаючи комп’ютерні, автоматизовані, телекомунікаційні, інформаційні, інформаційно-аналітичні, інформаційно-телекомунікаційні системи, інформаційні ресурси й технології; - технології забезпечення безпеки 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. Теоретичний зміст предметної області 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 та засобів технічного та криптографічного захисту інформації; - сучасних інформаційно-комунікаційних технологій; - сучасного програмно-апаратного забезпечення інформаційно-комунікаційних технологій; - автоматизованих систем проектування. Методи, методики та технології: Методи, методики, інформаційно-комунікаційні технології 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.
Фокус програми: загальна/ спеціальна	Здобуття вищої освіти в галузі інформаційних технологій із спеціальності 125 Кібербезпека. Акцент на здатності організовувати й підтримувати комплекс заходів щодо забезпечення інформаційної безпеки з урахуванням їхньої правової обґрунтованості, адміністративно-управлінської й технічної реалізуємості, економічної доцільності, можливих зовнішніх впливів, імовірних загроз і рівня розвитку технологій захисту інформації.
Орієнтація програми	Орієнтація на отримання теоретичних та практичних навичок використання методів та засобів ідентифікації вразливостей та загроз інформаційній безпеці на об’єктах інформаційної діяльності; методів та засобів забезпечення відповідного рівня захищеності інформації.
Академічні права випускників	Можливість продовжити навчання за освітньою програмою ступеня магістра
Працевлаштування	Бакалавр з кібербезпеки здатний виконувати професійні види робіт згідно з Національною рамкою кваліфікацій та Національним класифікатором

випускників (для регульованих професій обов'язково)	України: Класифікатор професій ДК 003:2010.

Код КП	Професійна назва роботи
3439	Інспектор з організації захисту секретної інформації
3119	Технік (сфера захисту інформації)
2149.2	Фахівець (сфера захисту інформації)
3439	Фахівець із організації захисту інформації з обмеженим доступом
2131.2	Адміністратор бази даних
2132.2	Програміст (база даних)
2132.2	Програміст прикладний
2132.2	Програміст системний
1495	Менеджер (управитель) систем з інформаційної безпеки
3121	Фахівець з інформаційних технологій
3439	Фахівець із організації інформаційної безпеки
2131.2	Інженер з програмного забезпечення комп'ютерів
2132.2	Інженер-програміст
2132.2	Програміст (база даних)
2132.2	Програміст прикладний
2132.2	Програміст системний
3121	Технік-програміст
3121	Фахівець з розроблення комп'ютерних програм
2131.2	Аналітик операційного та прикладного програмного забезпечення

III Обсяг кредитів ЄКТС, необхідний для здобуття відповідного ступеня вищої освіти. Тип диплома.

Обсяг освітньої програми бакалавра становить 240 кредитів ЄКТС, 100 % обсягу освітньої програми спрямовано на забезпечення загальних та спеціальних (фахових) компетентностей за спеціальністю, визначених стандартом вищої освіти за спеціальністю 125 «Кібербезпека». Для здобуття ступеня бакалавра на основі ступеня «молодшого бакалавра» МДУ визнаються та перезараховуються не більше ніж 120 кредитів ЄКТС, отриманих в межах попередньої освітньої програми підготовки молодшого бакалавра (молодшого спеціаліста), з дотриманням вимог Інструкції про порядок визначення академічної різниці та перезарахування навчальних дисциплін у Маріупольському державному університеті.

Тип диплома: одиничний ступінь.

IV Перелік компетентностей випускника

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 1. Здатність застосовувати знання у практичних ситуаціях.
	КЗ 2. Знання та розуміння предметної області та розуміння професії.
	КЗ 3.Здатність професійно спілкуватися державною та іноземною мовами як усно, так і письмово.
	КЗ 4. Вміння виявляти, ставити та вирішувати проблеми за професійним спрямуванням.

	КЗ 5. Здатність до пошуку, оброблення та аналізу інформації.
	КЗ 6. Здатність реалізувати 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.
	КЗ 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.
Фахові компетентності	КФ 1. Здатність використовувати законодавчу та нормативно-правову бази, а також державні та міжнародні вимоги, практики і стандарти з метою здійснення професійної діяльності в галузі інформаційної та/або кібербезпеки.
	КФ 2. Здатність до використання інформаційно-комунікаційних технологій, сучасних методів і моделей інформаційної безпеки та/або кібербезпеки.
	КФ 3. Здатність до використання програмних та програмно-апаратних комплексів засобів захисту інформації в інформаційно-телекомунікаційних (автоматизованих) системах.
	КФ 4. Здатність забезпечувати неперервність бізнесу згідно встановленої політики інформаційної та /або кібербезпеки.
	КФ 5. Здатність забезпечувати захист інформації, що обробляється в інформаційно-телекомунікаційних (автоматизованих) системах з метою реалізації встановленої політики інформаційної та /або кібербезпеки.
	КФ 6. Здатність відновлювати штатне функціонування інформаційних, інформаційно-телекомунікаційних (автоматизованих) систем після реалізації загроз, здійснення кібератак, збоїв та відмов різних класів та походження.
	КФ 7. Здатність впроваджувати та забезпечувати функціонування комплексних систем захисту інформації (комплекси нормативно-правових, організаційних та технічних засобів і методів, процедур, практичних прийомів та ін.).
	КФ 8. Здатність здійснювати процедури управління інцидентами, проводити розслідування, надавати їм оцінку.
	КФ 9. Здатність здійснювати професійну діяльність на основі впровадженої системи управління інформаційною та /або кібербезпекою.
	КФ 10. Здатність застосовувати методи та засоби криптографічного та технічного захисту інформації на об'єктах інформаційної діяльності.
	КФ 11. Здатність виконувати моніторинг процесів функціонування інформаційних, інформаційно-телекомунікаційних (автоматизованих) систем згідно встановленої політики інформаційної та /або кібербезпеки.
	КФ 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.

V Нормативний зміст підготовки здобувачів вищої освіти, сформульований у термінах результатів навчання

Кінцеві, підсумкові та інтегровані результати навчання, що визначають нормативний зміст підготовки і корелюються з визначеним вище переліком загальних і спеціальних компетентностей, подано нижче.

	Результати навчання
1.	застосувати знання державної та іноземних мов з метою забезпечення ефективності професійної комунікації;
2.	організувати власну професійну діяльність, обирати оптимальні методи та способи розв'язування складних спеціалізованих задач та практичних проблем у професійній діяльності, оцінювати їхню ефективність;
3.	використовувати результати самостійного пошуку, аналізу та синтезу інформації з різних джерел для ефективного рішення спеціалізованих задач професійної діяльності;
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;
5.	адаптуватися в умовах частої зміни технологій професійної діяльності, прогнозувати кінцевий результат;
6.	критично осмислювати основні теорії, принципи, методи і поняття у навчанні та професійній діяльності.
7.	діяти на основі законодавчої та нормативно-правової бази України та вимог відповідних стандартів, у тому числі міжнародних в галузі інформаційної та /або кібербезпеки;
8.	готувати пропозиції до нормативних актів щодо забезпечення інформаційної та /або кібербезпеки;
9.	впроваджувати процеси, що базуються на національних та міжнародних стандартах, виявлення, ідентифікації, аналізу та реагування на інциденти інформаційної та /або кібербезпеки;
10.	виконувати аналіз та декомпозицію інформаційно-телекомунікаційних систем;
11.	виконувати аналіз зв'язків між інформаційними процесами на віддалених обчислювальних системах;
12	розробляти моделі загроз та порушника;
13	аналізувати проекти інформаційно-телекомунікаційних систем базуючись на стандартизованих технологіях та протоколах передачі даних;
14	вирішувати завдання захисту програм та інформації, що обробляється в інформаційно-телекомунікаційних системах програмно-апаратними засобами та давати оцінку результативності якості прийнятих рішень;
15	використовувати сучасне програмно-апаратне забезпечення інформаційно-телекомунікаційних технологій;
16	реалізовувати комплексні системи захисту інформації в автоматизованих системах (АС) організації (підприємства) відповідно до вимог нормативно-правових документів;
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;
18	використовувати програмні та програмно-апаратні комплекси захисту інформаційних ресурсів;
19	застосовувати теорії та методи захисту для забезпечення безпеки інформації в інформаційно-телекомунікаційних системах;
20	забезпечувати функціонування спеціального програмного забезпечення, щодо захисту інформації від руйнуючих програмних впливів, руйнуючих кодів в інформаційно-телекомунікаційних системах;
21	вирішувати задачі забезпечення та супроводу (в.т. числі: огляд, тестування, підзвітність) системи управління доступом згідно встановленої політики безпеки в інформаційно- телекомунікаційних (автоматизованих) системах;
22	вирішувати задачі управління процедурами ідентифікації, автентифікації, авторизації процесів і користувачів в інформаційно-телекомунікаційних системах згідно встановленої політики інформаційної та /або кібербезпеки;
23	реалізовувати заходи з протидії отриманню несанкціонованого доступу до інформаційних ресурсів і процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах;
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);
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;
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;
27	вирішувати задачі захисту потоків даних в інформаційних, інформаційно-телекомунікаційних (автоматизованих) системах;
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;
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;
30	здійснювати оцінювання можливості несанкціонованого доступу до елементів інформаційно-телекомунікаційних систем;
31	застосовувати теорії та методи захисту для забезпечення безпеки елементів інформаційно-телекомунікаційних систем;
32	вирішувати задачі управління процесами відновлення штатного функціонування інформаційно-телекомунікаційних систем з використанням процедур резервування згідно встановленої політики безпеки;
33	вирішувати задачі забезпечення безперервності бізнес процесів організації на основі теорії ризиків;
34	приймати участь у розробці та впровадженні стратегії інформаційної безпеки та/або кібербезпеки відповідно до цілей і завдань організації;
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;
36	виявляти небезпечні сигнали технічних засобів;
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;
38	інтерпретувати результати проведення спеціальних вимірювань з використанням технічних засобів, контролю характеристик інформаційно-телекомунікаційних систем відповідно до вимог нормативних документів системи технічного захисту інформації;
39	проводити атестацію (спираючись на облік та обстеження) режимних територій (зон), приміщень тощо в умовах додержання режиму секретності із фіксуванням результатів у відповідних документах;
40	інтерпретувати результати проведення спеціальних вимірювань з використанням технічних засобів, контролю характеристик ІТС відповідно до вимог нормативних документів системи технічного захисту інформації;
41	забезпечувати безперервність процесу ведення журналів реєстрації подій та інцидентів на основі автоматизованих процедур;
42	впроваджувати процеси виявлення, ідентифікації, аналізу та реагування на інциденти інформаційної і/або кібербезпеки;
43	застосовувати національні та міжнародні регулюючі акти в сфері інформаційної безпеки та/ або кібербезпеки для розслідування інцидентів;
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;
45	застосовувати різні класи політик інформаційної безпеки та/ або кібербезпеки, що базуються на ризик-орієнтованому контролі доступу до інформаційних активів;
46	здійснювати аналіз та мінімізацію ризиків обробки інформації в інформаційно-телекомунікаційних системах;
47	вирішувати задачі захисту інформації, що обробляється в інформаційно-телекомунікаційних системах з використанням сучасних методів та засобів криптографічного захисту інформації;
48	впровадження та підтримку систем виявлення вторгнень та використовувати компоненти криптографічного захисту для забезпечення необхідного рівня захищеності інформації в інформаційно-телекомунікаційних системах;
49	забезпечувати належне функціонування системи моніторингу інформаційних ресурсів і процесів в інформаційно-телекомунікаційних системах;
50	забезпечувати функціонування програмних та програмно-апаратних комплексів виявлення вторгнень різних рівнів та класів (статистичних, сигнатурних, статистично-сигнатурних);
51	підтримувати працездатність та забезпечувати конфігурування систем виявлення вторгнень в інформаційно-телекомунікаційних системах;
52	використовувати інструментарій для моніторингу процесів в інформаційно-телекомунікаційних системах;
53	вирішувати задачі аналізу програмного коду на наявність можливих загроз
54	усвідомлювати цінності громадянського (вільного демократичного) суспільства та необхідність його сталого розвитку, верховенства права, прав і свобод і громадянина в Україні.

2. Стиль та методика навчання

А) *Підходи до викладання та навчання*	Лекційні курси поєднуються з практично-лабораторною діяльністю. Навчання переважно проблемно-орієнтоване, з використанням самонавчання.
Б) *Система оцінювання*	Письмові екзамени, захист практичних та лабораторних робот в обсязі, необхідному для успішного засвоєння теоретичних та прикладних питань з інформаційної безпеки. Виконання курсових робіт та індивідуальних проектних завдань. Кваліфікаційний комплексний іспит з професійних дисциплін.

3. Рекомендований перелік навчальних дисциплін і практик.

Обсяг освітньої складової освітньо-професійної програми підготовки бакалавра з кібербезпеки становить 240 кредитів ЄКТС.

Розподіл змісту освітньої складової програми за циклами дисциплін та критеріями нормативності і вибірковості наведено у табл. 2.

Таблиця 2

Розподіл змісту освітньої складової за критеріями нормативності та вибірковості

Цикл дисциплін	Загальна кількість кредитів	У тому числі:	
		нормативні дисципліни, кредитів	вибіркові дисципліни, кредитів
Загальна підготовка	51 (21%)	39 (16%)	12 (20%)
Професійна підготовка	189 (79%)	141 (59%)	48(80%)
Усього для ступеня бакалавра	**240 (100%)**	**180 (75%)**	**60 (25%)**

Теоретичне навчання здійснюється на основі поєднання лекційних та семінарських (практичних) занять з самостійною роботою. Практична підготовка передбачає проходження різних видів практики.

Формами підсумкового контролю з навчальних дисциплін є екзамени, заліки, а також диференційовані заліки, які проводяться для оцінювання якості навчання.

Таблиця 3

Перелік компонент ООП

Код н/д	**Шифр дисципліни за навчальним планом**	**Компоненти освітньої програма (навчальні дисципліни, курсові роботи, практики, кваліфікаційна робота)**	**Кількість кредитів**	**Форма підсумкового контролю**
Обов'язкові компоненти ОПП				
Дисципліни загальної підготовки				
ОК 1.	НДЗП 1.1.1.	Українська мова (за професійним спрямуванням)	3	екзамен

ОК 2.	НДЗП 1.1.2.	Історія України	3	екзамен
ОК 3.	НДЗП 1.1.3.	Історія української культури	3	екзамен
ОК 4.	НДЗП 1.1.4.	Іноземна мова	6	залік, екзамен
ОК 5.	НДЗП 1.1.5.	Філософія	3	екзамен
ОК 6.	НДЗП 1.1.6.	Політологія	3	екзамен
ОК 7.	НДЗП 1.1.7.	Основи психології	3	екзамен
ОК 8.	НДЗП 1.1.8.	Основи економічної теорії	3	екзамен
ОК 9.	НДЗП 1.1.9.	Безпека життєдіяльності	3	д. залік
ОК 10.	НДЗП 1.1.10.	Основи правознавства	3	екзамен
ОК 11.	НДЗП 1.1.11.	Основи криптографічного захисту інформації	3	залік
ОК 12.	НДЗП 1.1.12.	Фізичне виховання	3	д. залік
Дисципліни професійної підготовки				
ОК 13.	НДПП 1.2.1.	Вища математика	19	екзамен, екзамен,
ОК 14.	НДПП 1.2.2.	Дискретна математика	6	екзамен
ОК 15.	НДПП 1.2.3.	Теорія ймовірностей та математична статистика	6	екзамен
ОК 16.	НДПП 1.2.4.	Фізика	5	екзамен
ОК 17.	НДПП 1.2.5.	Прикладна криптологія	3	залік
ОК 18.	НДПП 1.2.6.	Теорія інформації та кодування	5	екзамен
ОК 19.	НДПП 1.2.7.	Алгоритми та структури даних	5	екзамен
ОК 20.	НДПП 1.2.8.	Нормативно-правове забезпечення інформаційної безпеки	5	екзамен
ОК 21.	НДПП 1.2.9.	Комп'ютерні мережі	4	екзамен
ОК 22.	НДПП 1.2.10.	Програмування	16	д. залік, д. залік, екзамен (курсова робота)
ОК 23.	НДПП 1.2.11.	Інформаційні технології та системи	4	екзамен
ОК 24.	НДПП 1.2.12.	Основи теорії кіл, сигналів та процесів в електроніці	5	екзамен
ОК 25.	НДПП 1.2.13.	Управління інформаційною безпекою	5	екзамен
ОК 26.	НДПП 1.2.14.	Електроніка	5	екзамен
ОК 27.	НДПП 1.2.15.	Архітектура комп'ютерних систем	6	екзамен
ОК 28.	НДПП 1.2.16.	Захист інформації в комп’ютерних системах та мережах	8	екзамен
ОК 29.	НДПП 1.2.17.	Комплексні системи захисту інформації	5	екзамен

ОК 30.	НДПП 1.2.18.	Комп'ютерна графіка та моделювання	6	екзамен
ОК 31.	НДПП 1.2.19.	Теорія і практика інфраструктури відкритих ключів	5	екзамен
ОК 32.	НДПП 1.2.20.	Виконання кваліфікаційної роботи	6	екзамен
ОК 33.	НДПП 1.2.21.	**Практична підготовка**		
		Навчальна практика	6	д.залік, д. залік
		Виробнича (навчально-виробнича практика)	3	д. залік
		Виробнича практика	3	д. залік
Вибіркові компоненти ОПП				
Дисципліни загальної підготовки				
ВК 1.	ВДЗП 2.1.1.	Дисц. вільного вибору №1 (Маркетинг/ Безпекознавство)	3	залік
ВК 2.	ВДЗП 2.1.2.	Дисц. вільного вибору №2 (Правове супроводження ІТ-технологій/Правові основи охорони здоров’я людини)	3	залік
ВК 3.	ВДЗП 2.1.3.	Дисц. вільного вибору №3 (Міжнародна інформація / Конфліктологія та теорія переговорів)	3	залік
ВК 4.	ВДЗП 2.1.4.	Дисц. вільного вибору №4 (Психологія спілкування/Психологія управління)	3	залік
Дисципліни професійної підготовки				
ВК 5.	ВДПП 2.2.1.	Дисц. вільного вибору №1 (Математичні перетворення в криптосистемах / Методи оптимізації та дослідження операцій)	6	залік
ВК 6.	ВДПП 2.2.2.	Дисц. вільного вибору №2 (Організація баз даних та знань / Інформаційні управляючі системи)	6	екзамен, курсова робота
ВК 7.	ВДПП 2.2.3.	Дисц. вільного вибору №3 (Системи штучного інтелекту / Захищені банківські технології)	4	залік
ВК 8.	ВДПП 2.2.4.	Дисц. вільного вибору №4 (Захист операційних систем та баз даних / Основи системного аналізу та прийняття рішень)	6	екзамен
ВК 9.	ВДПП 2.2.5.	Дисц. вільного вибору №5 (Моделювання інформаційної безпеки / Інформаційна безпека держави)	5	залік
ВК 10.	ВДПП 2.2.6.	Дисц. вільного вибору №6 (Економічна безпека / Адміністрування комп’ютерних систем та мереж)	4	залік

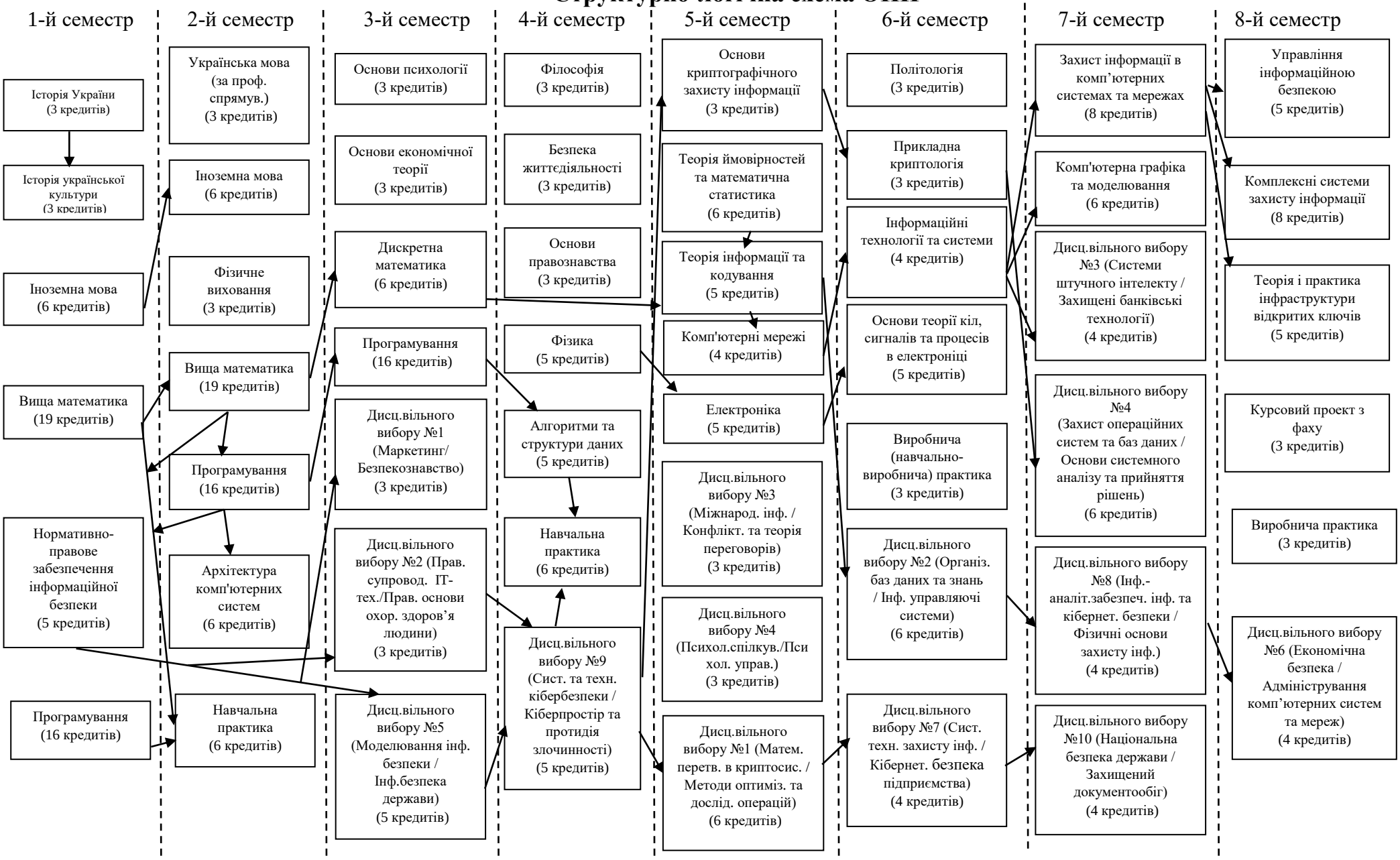
ВК 11	ВДПП 2.2.7.	Дисц. вільного вибору №7 (Системи технічного захисту інформації / Кібернетична безпека підприємства)	4	Залік
ВК 12.	ВДПП 2.2.8.	Дисц. вільного вибору №8 (Інформаційно-аналітичне забезпечення інформаційної та кібернетичної безпеки / Фізичні основи захисту інформації)	4	Залік
ВК 13.	ВДПП 2.2.9.	Дисц. вільного вибору №9 (Системи та технології кібербезпеки / Кіберпростір та протидія злочинності)	5	Залік
ВК 14.	ВДПП 2.2.10.	Дисц. вільного вибору №10 (Національна безпека держави / Захищений документообіг)	4	Залік

Схематично співвідношення між результатами навчання та компетентностями представлено у вигляді матриці (Таблиця 4), рядки якої містять результати навчання (РН) за окремими дисциплінами освітньої програми, а стовпці – компетентності (К), які студент набуває в результаті успішного навчання за даною освітньою програмою.

Опис нормативних та вибіркових навчальних дисциплін наведено в Додатку А та Додатку Б

Таблиця 4

Структурно-логічна схема ОПП



Таблиця 5

Матриця відповідності фахових компетентностей та результатів навчання

Програмні результати навчання / Навчальна дисципліна		Компетентності																				
		ІК	Загальні							Фахові												
			КЗ1	КЗ2	КЗ3	КЗ4	КЗ5	КЗ6	КЗ7	КФ1	КФ2	КФ3	КФ4	КФ5	КФ6	КФ7	КФ8	КФ9	КФ10	КФ11	КФ12
РН1	застосувати знання державної та іноземних мов з метою забезпечення ефективності професійної комунікації;	Здатність розв'язувати складні спеціалізовані задачі та практичні проблеми у галузі забезпечення інформаційної безпеки і/або кібербезпеки, що характеризується комплексністю та неповною визначеністю умов.		+	+		+		+	+	+										
РН2	організувати власну професійну діяльність, обирати оптимальні методи та способи розв'язування складних спеціалізованих задач та практичних проблем у професійній діяльності, оцінювати їхню ефективність;		+	+		+	+			+	+	+			+			+	+	+	+
РН3	використовувати результати самостійного пошуку, аналізу та синтезу інформації з різних джерел для ефективного рішення спеціалізованих задач професійної діяльності;		+	+	+	+	+		+		+			+						+	+
РН4	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;		+	+		+	+				+		+		+		+	+			+
РН5	адаптуватися в умовах частої зміни технологій професійної діяльності, прогнозувати кінцевий результат;		+	+	+				+		+										
РН6	критично осмислювати основні теорії, принципи, методи і поняття у навчанні та професійній діяльності.																					
РН7	діяти на основі законодавчої та нормативно-правової бази України та вимог відповідних стандартів, у тому числі міжнародних в галузі інформаційної та /або кібербезпеки;				+			+		+			+	+							+
РН8	готувати пропозиції до нормативних актів щодо забезпечення інформаційної та /або кібербезпеки;				+	+		+	+	+			+								+
РН9	впроваджувати процеси, що базуються на національних та міжнародних стандартах, виявлення, ідентифікації, аналізу та реагування на інциденти інформаційної та /або кібербезпеки;		+		+		+			+	+					+					+
РН10	виконувати аналіз та декомпозицію інформаційно-телекомунікаційних систем;					+					+				+	+		+	+		+
РН11	виконувати аналіз зв'язків між інформаційними процесами на віддалених обчислювальних системах;					+					+	+	+		+	+	+	+	+		

Програмні результати навчання / Навчальна дисципліна		ІК	Компетентності																			
			Загальні							Фахові												
			КЗ1	КЗ2	КЗ3	КЗ4	КЗ5	КЗ6	КЗ7	КФ1	КФ2	КФ3	КФ4	КФ5	КФ6	КФ7	КФ8	КФ9	КФ10	КФ11	КФ12
РН12	розробляти моделі загроз та порушника;		+								+										+
РН13	аналізувати проекти інформаційно-телекомунікаційних систем базуючись на стандартизованих технологіях та протоколах передачі даних;									+	+		+	+						+	+
РН14	вирішувати завдання захисту програм та інформації, що обробляється в інформаційно-телекомунікаційних системах програмно-апаратними засобами та давати оцінку результативності якості прийнятих рішень;		+			+									+				+		
РН15	використовувати сучасне програмно-апаратне забезпечення інформаційно-телекомунікаційних технологій;				+										+	+			+	+	
РН16	реалізовувати комплексні системи захисту інформації в автоматизованих системах організації (підприємства) відповідно до вимог нормативно-правових документів;		+			+										+		+	+		
РН17	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;		+								+	+	+	+				+	+	+	
РН18	використовувати програмні та програмно-апаратні комплекси захисту інформаційних ресурсів;											+									
РН19	застосовувати теорії та методи захисту для забезпечення безпеки інформації в інформаційно-телекомунікаційних системах;		+	+								+		+				+	+		+
РН20	забезпечувати функціонування спеціального програмного забезпечення, щодо захисту інформації від руйнуючих програмних впливів, руйнуючих кодів в інформаційно-телекомунікаційних системах;											+	+		+						
РН21	вирішувати задачі забезпечення та супроводу (в.т. числі: огляд, тестування, підзвітність) системи управління доступом згідно встановленої політики безпеки в інформаційно-телекомунікаційних (автоматизованих) системах;										+	+	+	+	+				+	+	+

Програмні результати навчання / Навчальна дисципліна		**Компетентності**																		
		ІК	Загальні							Фахові										
			КЗ1	КЗ2	КЗ3	КЗ4	КЗ5	КЗ6	КЗ7	КФ1	КФ2	КФ3	КФ4	КФ5	КФ6	КФ7	КФ8	КФ9	КФ10	КФ11	КФ12
РН22	вирішувати задачі управління процедурами ідентифікації, автентифікації, авторизації процесів і користувачів в інформаційно-телекомунікаційних системах згідно встановленої політики інформаційної та /або кібербезпеки;											+	+	+		+		+		
РН23	реалізовувати заходи з протидії отриманню несанкціонованого доступу до інформаційних ресурсів і процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах;											+	+	+		+		+		
РН24	вирішувати задачі управління доступом до інформаційних ресурсів та процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах на основі моделей управління доступом (мандатних, дискреційних, рольових);										+	+	+	+		+		+	+		
РН25	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;									+			+	+		+	+	+		+	
РН26	впроваджувати заходи та забезпечувати реалізацію процесів попередження отриманню несанкціонованого доступу і захисту інформаційних, інформаційно-телекомунікаційних (автоматизованих) систем на основі еталонної моделі взаємодії відкритих систем;									+			+	+		+	+	+		+	
РН27	вирішувати задачі захисту потоків даних в інформаційних, інформаційно-телекомунікаційних (автоматизованих) системах;		+								+	+		+		+					
РН28	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;											+								+	+
РН29	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;																+			+	+
РН30	здійснювати оцінювання можливості несанкціонованого доступу до																+			+	+

Програмні результати навчання / Навчальна дисципліна		ІК	Компетентності																		
			Загальні							Фахові											
			КЗ1	КЗ2	КЗ3	КЗ4	КЗ5	КЗ6	КЗ7	КФ1	КФ2	КФ3	КФ4	КФ5	КФ6	КФ7	КФ8	КФ9	КФ10	КФ11	КФ12
	елементів інформаційно-телекомунікаційних систем;																				
РН31	застосовувати теорії та методи захисту для забезпечення безпеки елементів інформаційно-телекомунікаційних систем;		+								+										
РН32	вирішувати задачі управління процесами відновлення штатного функціонування інформаційно-телекомунікаційних систем з використанням процедур резервування згідно встановленої політики безпеки;														+			+			
РН33	вирішувати задачі забезпечення безперервності бізнес процесів організації на основі теорії ризиків;																				
РН34	приймати участь у розробці та впровадженні стратегії інформаційної безпеки та/або кібербезпеки відповідно до цілей і завдань організації;									+		+		+							+
РН35	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;										+	+		+	+	+		+	+		+
РН36	виявляти небезпечні сигнали технічних засобів;		+				+					+			+	+					
РН37	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;										+	+				+					
РН38	інтерпретувати результати проведення спеціальних вимірювань з використанням технічних засобів, контролю характеристик інформаційно-телекомунікаційних систем відповідно до вимог нормативних документів системи технічного захисту інформації;													+						+	+
РН39	проводити атестацію (спираючись на облік та обстеження) режимних територій (зон), приміщень тощо в умовах додержання режиму секретності із фіксуванням результатів у відповідних документах;									+	+			+			+		+		+
РН40	інтерпретувати результати проведення спеціальних вимірювань з використанням технічних засобів, контролю характеристик ІТС відповідно до вимог нормативних документів системи технічного захисту інформації;		+									+									+
РН41	забезпечувати безперервність процесу ведення журналів реєстрації подій та												+				+	+		+	+

Програмні результати навчання / Навчальна дисципліна		Компетентності																			
		ІК	Загальні							Фахові											
			КЗ1	КЗ2	КЗ3	КЗ4	КЗ5	КЗ6	КЗ7	КФ1	КФ2	КФ3	КФ4	КФ5	КФ6	КФ7	КФ8	КФ9	КФ10	КФ11	КФ12
	інцидентів на основі автоматизованих процедур;																				
РН42	впроваджувати процеси виявлення, ідентифікації, аналізу та реагування на інциденти інформаційної і/або кібербезпеки;												+			+	+	+		+	+
РН43	застосовувати національні та міжнародні регулюючі акти в сфері інформаційної безпеки та/ або кібербезпеки для розслідування інцидентів;							+		+											
РН44	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;									+	+		+								
РН45	застосовувати різні класи політик інформаційної безпеки та/ або кібербезпеки, що базуються на ризик-орієнтованому контролі доступу до інформаційних активів;										+										+
РН46	здійснювати аналіз та мінімізацію ризиків обробки інформації в інформаційно-телекомунікаційних системах;		+								+									+	+
РН47	вирішувати задачі захисту інформації, що обробляється в інформаційно-телекомунікаційних системах з використанням сучасних методів та засобів криптографічного захисту інформації;											+						+	+		
РН48	виконувати впровадження та підтримку систем виявлення вторгнень та використовувати компоненти криптографічного захисту для забезпечення необхідного рівня захищеності інформації в інформаційно-телекомунікаційних системах;											+						+	+		
РН49	забезпечувати належне функціонування системи моніторингу інформаційних ресурсів і процесів в інформаційно-телекомунікаційних системах;										+	+						+		+	+
РН50	забезпечувати функціонування програмних та програмно-апаратних комплексів виявлення вторгнень різних рівнів та класів (статистичних, сигнатурних, статистично-сигнатурних);		+								+	+						+			
РН51	підтримувати працездатність та забезпечувати конфігурування систем виявлення вторгнень в інформаційно-телекомунікаційних системах;															+	+				+
РН52	використовувати інструментарій для моніторингу процесів в інформаційно-телекомунікаційних системах;											+								+	+
РН53	вирішувати задачі аналізу програмного коду на наявність можливих загроз																				
РН54	усвідомлювати цінності громадянського (вільного демократичного) суспільства та необхідність його сталого розвитку, верховенства права, прав і свобод і громадянина в Україні.				+			+	+	+											

Таблиця 6

Матриця відповідності фахових компетентностей та результатів навчання

Програмні результати навчання / Навчальна дисципліна	Компетентності																				
	ІК	Загальні							Фахові												
		КЗ1	КЗ2	КЗ3	КЗ4	КЗ5	КЗ6	КЗ7	КФ1	КФ2	КФ3	КФ4	КФ5	КФ6	КФ7	КФ8	КФ9	КФ10	КФ11	КФ12
РН1/ ОК1, ОК2, ОК3, ОК4	Здатність розв'язувати складні спеціалізовані задачі та практичні проблеми у галузі забезпечення інформаційної безпеки і/або кібербезпеки, що характеризується комплексністю та неповною визначеністю умов.		+	+		+		+	+	+											
РН2 / ОК5, ОК7, ОК8, ОК9, ОК12, ОК20, ОК25, ОК13, ОК15, ОК16, ОК24, ОК26, ОК18, ОК21, ОК23, ОК28, ОК31, ОК29, ОК 33, ОК 32, ОК33, ОК30		+	+		+	+			+	+	+			+			+	+	+	+
РН 3 / ОК5, ОК7, ОК13, ОК15, ОК 33, ОК 32, ОК33		+	+	+	+	+		+		+			+						+	+
РН 4 / ОК5, ОК7, ОК8, ОК13, ОК15, ОК18, ОК21, ОК23, ОК28, ОК29, ОК31, ОК 32, ОК 33		+	+		+	+				+		+		+		+	+			+
РН 5 / ОК13, ОК15, ОК8		+	+	+				+		+											
РН 6 / ОК5, ОК11, ОК33																					
РН 7 / ОК10, ОК20, ОК25				+			+		+			+	+								+
РН 8 / ОК9, ОК20, ОК25				+	+		+	+	+			+									+
РН 9 / ОК9, ОК20, ОК25		+		+		+			+	+					+						+
РН 10 / ОК21, ОК23, ОК29, ОК33					+					+				+	+		+	+			+
РН 11 / ОК21, ОК23, ОК28, ОК31, ОК29, ОК18					+					+	+	+		+	+	+	+	+			
РН 12 / ОК13, ОК15, ОК14, ОК19, ОК22, ОК27, ОК18		+								+											+
РН 13 / ОК21, ОК23, ОК28									+	+		+	+							+	+
РН 14 / ОК 33, ОК11, ОК17, ОК13, ОК15, ОК14, ОК19, ОК22, ОК27, ОК16, ОК24, ОК26		+			+									+				+			
РН 15 / ОК29, ОК32, ОК33, ОК11, ОК17, ОК14, ОК19, ОК22, ОК27, ОК16, ОК24, ОК26				+										+	+			+	+		
РН 16 / ОК21, ОК23, ОК29, ОК11, ОК17		+			+										+		+	+			
РН 17 / ОК18, ОК21, ОК23, ОК29		+								+	+	+	+				+	+	+		

Програмні результати навчання / Навчальна дисципліна	**Компетентності**																			
	ІК	Загальні							Фахові											
		КЗ1	КЗ2	КЗ3	КЗ4	КЗ5	КЗ6	КЗ7	КФ1	КФ2	КФ3	КФ4	КФ5	КФ6	КФ7	КФ8	КФ9	КФ10	КФ11	КФ12
РН 18 / ОК32, ОК33, ОК11, ОК17, ОК16, ОК24, ОК26, ОК21, ОК23, ОК29											+									
РН 19 / ОК11, ОК17, ОК14, ОК19, ОК22, ОК27, ОК16, ОК24, ОК26, ОК28, ОК31		+	+								+		+				+	+		+
РН 20 / ОК30, ОК14, ОК19, ОК22, ОК27											+	+		+						
РН 21 / ОК28, ОК31, ОК29										+	+	+	+	+				+	+	+
РН 22 / ОК30, ОК28, ОК31											+	+	+		+		+			
РН 23 / ОК28, ОК30, ОК29											+	+	+		+		+			
РН 24 / ОК21, ОК28, ОК31										+	+	+	+		+		+	+		
РН 25 / ОК29, ОК13, ОК15									+			+	+		+	+	+		+	
РН 26 / ОК28, ОК29, ОК31									+			+	+		+	+	+		+	
РН 27 / ОК31, ОК29, ОК11, ОК17, ОК14, ОК19, ОК22, ОК27, ОК16, ОК24, ОК26, ОК18, ОК21, ОК23, ОК28,		+								+	+		+		+					
РН 28 / ОК 33, ОК 32, ОК 33, ОК13, ОК15											+								+	+
РН 29 / ОК13, ОК15, ОК18, ОК21, ОК23																+			+	+
РН 30 / ОК 33, ОК13, ОК15																+			+	+
РН 31 / ОК14, ОК19, ОК22, ОК27, ОК18, ОК28, ОК31, ОК11, ОК17		+								+										
РН 32 / ОК21, ОК23, ОК28, ОК20, ОК25														+			+			
РН 33 / ОК25, ОК29, ОК28																				
РН 34 / ОК20, ОК25, ОК29, ОК5, ОК7									+		+		+							+
РН 35 / ОК20, ОК25, ОК11, ОК17, ОК28, ОК31, ОК29, ОК 32, ОК33										+	+		+	+	+		+	+		+
РН 36 / ОК16, ОК24, ОК26, ОК18, ОК21		+				+					+			+	+					
РН 37 / ОК16, ОК24, ОК26, ОК18										+	+				+					
РН 38 / ОК13, ОК15, ОК16, ОК24, ОК26													+						+	+

Програмні результати навчання / Навчальна дисципліна	**Компетентності**																			
	ІК	Загальні							Фахові											
		КЗ1	КЗ2	КЗ3	КЗ4	КЗ5	КЗ6	КЗ7	КФ1	КФ2	КФ3	КФ4	КФ5	КФ6	КФ7	КФ8	КФ9	КФ10	КФ11	КФ12
РН 39 / ОК21, ОК20, ОК25									+	+			+			+		+		+
РН 40 / ОК18, ОК24, ОК30		+									+									+
РН 41 / ОК21, ОК20, ОК25, ОК11, ОК17												+				+	+		+	+
РН 42 / ОК 32, ОК 33												+			+	+	+		+	+
РН 43 / ОК20. ОК25, ОК29							+		+											
РН 44 / ОК25, ОК29, ОК28									+	+		+								
РН 45 / ОК25, ОК29, ОК28										+										+
РН 46 / ОК13, ОК15, ОК28, ОК31, ОК32, ОК33		+								+									+	+
РН 47 / ОК14, ОК19, ОК22, ОК27, ОК32, ОК33, ОК11, ОК17											+						+	+		
РН 48 / ОК11, ОК17, ОК25											+						+	+		
РН 49 / ОК23, ОК25, ОК29										+	+						+		+	+
РН 50 / ОК20, ОК25, ОК14, ОК19, ОК22, ОК27		+								+	+						+			
РН 51 / ОК18, ОК21, ОК23															+	+				+
РН 52 / ОК 23, ОК 28, ОК29											+								+	+
РН 53 / ОК14, ОК19, ОК22, ОК27																				
РН 54 / ОК1, ОК2, ОК3, ОК4, ОК5, ОК7 ОК8, ОК9, ОК12, ОК6, ОК10, ОК20, ОК25				+			+	+	+											

VI Форми атестації здобувачів вищої освіти

Форми атестації здобувачів вищої освіти	Атестація здійснюється у формі публічного захисту кваліфікаційної роботи. На атестацію виноситься сукупність знань, умінь, навичок, інших компетентностей, набутих особою у процесі навчання. До атестації допускаються студенти, які виконали всі вимоги програми підготовки.
Вимоги до кваліфікаційної роботи/проекту	Кваліфікаційна робота передбачає розв'язання спеціалізованої задачі в галузі інформаційної та/або кібербезпеки. Кваліфікаційна робота перевіряється на плагіат та розміщується в репозиторії кваліфікаційних робіт МДУ має потреби

VII. Вимоги до наявності системи внутрішнього забезпечення якості вищої освіти

У МДУ функціонує система забезпечення закладом вищої освіти якості освітньої діяльності та якості вищої освіти (система внутрішнього забезпечення якості), яка передбачає здійснення таких процедур і заходів:

1) визначення принципів та процедур забезпечення якості вищої освіти;

2) здійснення моніторингу та періодичного перегляду освітніх програм;

3) щорічне оцінювання здобувачів вищої освіти, науково-педагогічних і педагогічних працівників вищого навчального закладу та регулярне оприлюднення результатів таких оцінювань на офіційному веб-сайті закладу вищої освіти, на інформаційних стендах та в будь-який інший спосіб

4) забезпечення підвищення кваліфікації педагогічних, наукових і науково-педагогічних працівників;

5) забезпечення наявності необхідних ресурсів для організації освітнього процесу, у тому числі самостійної роботи студентів, за кожною освітньою програмою чи спеціальністю;

6) забезпечення наявності інформаційних систем для ефективного управління освітнім процесом;

7) забезпечення публічності інформації про освітні програми, ступені вищої освіти та кваліфікації;

8) забезпечення ефективної системи запобігання та виявлення академічного плагіату у наукових працях працівників закладів вищої освіти і здобувачів вищої освіти;

9) інших процедур і заходів.

Система забезпечення закладом вищої освіти якості освітньої діяльності та якості вищої освіти (система внутрішнього забезпечення якості) за поданням ВНЗ оцінюється Національним агентством із забезпечення якості вищої освіти або акредитованими ним незалежними установами оцінювання та забезпечення якості вищої освіти на предмет її відповідності вимогам до системи забезпечення якості вищої освіти, що затверджуються Національним

агентством із забезпечення якості вищої освіти, та міжнародним стандартам і рекомендаціям щодо забезпечення якості вищої освіти.

Додаток А

ОПИС НОРМАТИВНИХ НАВЧАЛЬНИХ ДИСЦИПЛІН

1.1. Дисципліни загальної підготовки

НДЗП 1.1.1. Українська мова (за професійним спрямуванням)

Мета вивчення курсу: підвищення рівня теоретичних знань та розвиток практичних навичок студентів щодо мовних умінь і навичок у професійній сфері; практичне опанування студентами умінь ділового мовлення на рівні, достатньому для професійної діяльності; формування комунікативної компетентності студентів.

Завдання курсу: підвищення загального рівня грамотності студентів; засвоєння основних відомостей про українську мову як багатоаспектну лінгвістичну систему; формування, розвиток та закріплення навичок та вмінь правильного використання усталених мовностилістичних засобів української мови; докладне вивчення зразків оформлення різних видів документів; формування вмінь культури мовлення у професійній діяльності.

Змістові модулі:

1. Основи культури української мови
2. Ділові папери як засіб писемної професійної комунікації
3. Усна форма спілкування як інструмент професійної діяльності

НДЗП 1.1.2. Історія України

Мета вивчення курсу: формування знань про заселення українських земель, формування української нації та розвиток інших етнічних спільнот, історію української державності, соціально-економічні, політичні, культурні процеси, що складають змістовий пласт історії України від найдавніших часів до початку XXI ст.

Завдання курсу: виховання у студентів на фактах історії України почуття національної гідності, патріотизму, почуття відповідальності за вивчення історії України, як основи для засвоєння широкої системи історичних знань, вивчення історичного процесу за принципом історизму, об'єктивності та науковості, формування нового історичного мислення шляхом співставлення полярних точок зору і різних фактів, розвинення вміння аналізувати історичний матеріал, робити ґрунтовні висновки, використовуючи різні типи історичних джерел, навчити розрізняти історичний факт від історичного міфу, викривати стереотипи, упередженість, необ'єктивність, розвити вміння робити виважені висновки та самостійні оцінки історичних подій, явищ, толерантно сприймати багатоетнічні, полікультурні явища національної та світової історії, розглядати історію України у європейському та світовому контекстах, формувати національну самобутність і почуття патріотизму.

Змістові модулі:

1. Українські землі від найдавніших часів до початку XX ст.
2. Українські землі у першій половині XX ст.
3. Україна у другій половині XX – на початку XXI ст.

НДЗП 1.1.3. Історія української культури

Мета вивчення курсу: формування у студентів системи знань про унікальність української культури, її роль та місце в світовому культурному просторі.

Завдання курсу: формування у студентів розуміння унікальності національного культурного простору на основі з'ясування проблеми культурогенезу; познайомити з основними досягненнями української культури в її діахронному вимірі; виявити детермінованість та закономірності культурного процесу, оцінити історичний розвиток культури на основі порівняння української культури з європейською та світовою; оцінити еволюцію мистецького розвитку в контексті проблеми співвідношення традиції і новаторства

Змістові модулі:

1. Концептуальні засади вивчення української культури
2. Етапи формування та розвитку української культури
3. Українська культура в умовах євроінтеграції

НДЗП 1.1. 4. Іноземна мова

НДЗП 1.1.4 (1.) Іноземна мова (англійська)

Мета вивчення курсу: : формування навичок креативного усного та писемного мовлення; формування навичок монологічного і діалогічного непідготовленого мовлення на основі активно засвоєного лексичного, граматичного та стилістичного матеріалів; засвоєння лексичних одиниць та мовленнєвих моделей на матеріалі текстів підручників, розмовних тем, суспільно-політичних текстів, комунікативних ситуацій, текстів позалекційного читання; посилення самостійної пошукової, творчої роботи; підвищення рівня лінгвістичної компетенції через втілення знань стилістичних прийомів та виразних засобів в ґрунтовний аналіз англомовного тексту; підвищення рівня мовної компетенції студентів, вдосконалення їхніх мовних навичок через розвиток таких вмінь як читання, аудіювання, усне та письмове мовлення, а також розвиток точності граматичної побудови мовлення.

Завдання курсу поповнити словниковий запас студентів для посилення їх висловлювальних можливостей; активізувати пасивний вокабуляр, а також поповнити активний словник, що має розширити висловлювальні можливості студентів; забезпечити знаннями практичної граматики у ході побудови монологічного та діалогічного мовлення; вдосконалити вміння студентів щодо глибокого філологічного (зокрема, лінгвостилістичного) аналізу тексту на англійській мові; покращити вміння студентів сприймати текст на слух (з опорою та без опори на друкований текст) та стимулювати активне обговорення сприйнятої інформації в аудиторії; сформувати навички письма з метою підвищення ефективності письмової комунікації; логічно структурувати та правильно виконувати словесне оформлення письмового тексту на задану тему; актуалізувати знання практичної граматики у ході побудови монологічного та діалогічного мовлення; ознайомити студентів з сучасними тенденціями англійської розмовної мови; вдосконалити навички усних доповідей/презентацій на англійській мові.

Змістовні модулі:

1. Формування та поглиблення навичок базової мовної та мовленнєвої компетенції
2. Удосконалення базових навичок мовної та мовленнєвої компетенції
3. Формування граматичної компетенції, аудіокомпетенції

НДЗП 1.1.4. (2). Іноземна мова (німецька/ французька)

Мета вивчення курсу: формування комунікативної компетенції, яка складається з мовної, мовленнєвої, лінгвосоціокультурної та навчально-стратегічної та дозволяє вільно спілкуватися іноземною мовою з опорою на словниковий запас та граматику. В процесі вивчення мови студенти вчаться читати, перекладати з іноземної мови на рідну та з рідної на іноземну, писати, розуміти мову. У студентів формуються навички для подальшого вдосконалення своїх знань у галузі іноземної мови.

Завдання курсу: вдосконалення лексичної, граматичної та фонетичної компетенцій студентів; розвиток навичок та вмінь усного та писемного мовлення; розвиток навичок та вмінь аудіювання з подальшою репродукцією як рідною так і іноземною мовами; формування вмінь монологічного та діалогічного мовлення у межах заданих тем, а також у процесі усного непідготовленого мовлення; оволодіння країнознавчими знаннями щодо культурного простору країн виучуваної мови у межах комунікативних сфер, тем та ситуацій; розвиток соціокультурної компетенції студентів.

Змістові модулі:

1. Знайомство. Перші контакти.
2. Вивчення іноземної мови.

3. Студентське життя. Мій університет.
4. Родина. День народження.
5. Моя квартира. Житло в Німеччині (Франції) та в Україні.

НДЗП 1.1.5. Філософія

Мета вивчення курсу: набуття студентами знань про генезис, розвиток і зазначення філософських ідей у всесвітній культурі, знайомство із сучасною філософією, опанування філософськими методами, аналізом та вирішенням філософських проблем сучасності; формуванні світогляду, свідомості та самосвідомості студентів.

Завдання курсу: залучення до історії людської думки; формування критичного мислення, розвиток вміння висловлювати свої думки, виступати публічно, аргументувати і доводити свою точку зору, шанобливо ставитися до інших точок зору; вироблення здатності аналізувати та інтерпретувати інформацію, працювати з різними джерелами, класифікувати, обробляти філософську і будь-яку гуманітарну інформацію; знайомство і прилучення до загальнолюдських цінностей, вироблення навичок культури соціальних відносин, здатності до соціальної адаптації.

Змістові модулі:

1. Антична та середньовічна філософія.
2. Філософія нового часу.
3. Сучасна філософія.

НДЗП 1.1.6. Політологія

Мета вивчення курсу: складання у майбутніх фахівців глибокого та всебічного розуміння політичної реальності та її осмислення політичною наукою. Сформувати базові уявлення про взаємодію суб'єктів політики між собою та з суспільством, виокремити основні політичні інститути, процеси та явища. Застосовувати політичні знання при аналізі політичних процесів сучасності. Сформувати політичну культуру, особисту позицію.

Завдання курсу: методології політичної науки; систематизація та структуризація знань про політику; понятійно-категоріального апарату; сутності політичної системи суспільства, її функціонування та взаємодію з середовищем.

Змістові модулі:

1.Політологія як навчальна дисципліна.
2. Держава як політичний інститут.
3. Громадянське суспільство та політичні партії як складові політичної системи.

НДЗП 1.1.7. Основи психології

Мета вивчення: формування прагнення до самопізнання та самовдосконалення, комунікативної компетентності студентів; підвищення рівня теоретичних знань; розвиток творчого мислення і вмінь підходити до рішення професійних та життєвих задач з урахуванням основних закономірностей функціонування психіки людини.

Завдання курсу: допомога в осмисленні значущості основ психології для майбутнього професіонала в будь-який галузі життєдіяльності; ознайомлення студентів з історією, сучасним станом, основними категоріями, методами; галузями психологічної науки; формування знань про сутність, зміст, структуру, джерела психіки людини та соціальної групи; формування професійного бачення психологічних закономірностей протікання та розвитку психічних процесів, станів та властивостей особистості; окреслення онтогенетичного шляху людини як соціального індивіда й особистості, розкриття зв'язку закономірностей психічного розвитку з вихованням і навчанням; розвиток у студентів комунікативних компетенцій, оволодіння технологіями міжособистісного спілкування; формування практичних навичок вправного застосування різних методів вивчення пізнавальної сфери особистості, психічних станів та індивідуально-типологічних

особливостей особистості; заохочування студентів до пошуку зв'язків теоретичних положень науки з практикою.

Змістові модулі:

1. Вступ у психологію.
2. Психологія пізнання.
3. Проблема особистості в психології.

НДЗП 1.1.8. Основи економічної теорії

Мета вивчення курсу: набуття ґрунтовних економічних знань, формування логіки економічного мислення і економічної культури, навчання базовим методам пізнання і аналізу економічних процесів.

Завдання курсу: набуття навичок раціональної економічної поведінки, виходячи з концептуальних основ ринкової економіки; розуміння особливостей функціонування сучасних ринків, формування агрегованих показників, визначення чинників і наслідків макроекономічного розвитку господарських систем; формування вмінь загального аналізу основних економічних подій у своїй країні та за її межами, пошуку й використання інформації, необхідної для орієнтування в основних поточних проблемах економіки.

Змістові модулі:

1. Загальні основи соціально-економічного розвитку.
2. Теоретичні основи мікроекономіки.
3. Теоретичні основи макроекономіки. Закономірності розвитку світового господарства.

НДЗП 1.1. 9. Безпека життєдіяльності

Мета вивчення курсу: набуття студентом компетенцій, знань, умінь і навичок для здійснення професійної діяльності за спеціальністю з урахуванням ризику виникнення техногенних аварій й природних небезпек, які можуть спричинити надзвичайні ситуації та привести до несприятливих наслідків на об'єктах господарювання, а також формування у студентів відповідальності за особисту та колективну безпеку; формуванні у студентів здатності творчо мислити, вирішувати складні проблеми інноваційного характеру й приймати продуктивні рішення у сфері цивільного захисту, з урахуванням особливостей майбутньої професійної діяльності випускників, а також досягнень науково-технічного прогресу; наданні знань, умінь, здатностей (компетенцій) для здійснення ефективної професійної діяльності шляхом забезпечення оптимального управління охороною праці на підприємствах (об'єктах господарської, економічної та науково-освітньої діяльності), формуванні у студентів відповідальності за особисту та колективну безпеку і усвідомлення необхідності обов'язкового виконання в повному обсязі всіх заходів гарантування безпеки праці на робочих місцях.

Завдання курсу: опанувати знання, вміння та навички вирішувати професійні завдання з обов'язковим урахуванням галузевих вимог щодо забезпечення безпеки персоналу та захисту населення в небезпечних та надзвичайних ситуаціях і формування мотивації щодо посилення особистої відповідальності за забезпечення гарантованого рівня безпеки функціонування об'єктів галузі, матеріальних та культурних цінностей в межах науково-обґрунтованих критеріїв прийнятного ризику; засвоєння студентами новітніх теорій, методів і технологій з прогнозування НС, визначення рівня ризику та обґрунтування комплексу заходів, спрямованих на відвернення НС, захисту персоналу, населення, матеріальних та культурних цінностей в умовах НС, локалізації та ліквідації їхніх наслідків; набуття студентами знань, умінь і здатностей (компетенцій) ефективно вирішувати завдання професійної діяльності з обов'язковим урахуванням вимог охорони праці та гарантуванням збереження життя, здоров'я та працездатності працівників у різних сферах професійної діяльності.

Змістовні модулі:

1. Теоретичні основи безпеки життєдіяльності. Безпека у надзвичайних ситуаціях

2. Загальна підготовка та профільна підготовка з питань цивільного захисту
3. Загальні питання охорони праці. Основи виробничої безпеки

НДЗП 1.1.10. Основи правознавства

Мета вивчення курсу: набуття студентами ґрунтовних знань з теорії правознавства, оволодіння системою основних понять правознавства, засвоєння найважливіших положень окремих правових галузей та вироблення навичок їх застосування на практиці.

Завдання курсу: вивчення теорії правознавства; закономірностей та специфіки розвитку держави та права; основних положень Конституції України, які стосуються регламентування діяльності держави та організації суспільного життя, прав і обов'язків громадянина; ознайомлення з базовими положеннями основних галузей права України та їх застосуванням у практичних завданнях; ознайомлення студентів із перспективами розвитку правової системи України у зв'язку із євроінтеграційними процесами.

Змістові модулі:

1. Теоретичні засади держави та права.
2. Публічно-правові галузі права.
3. Приватно-правові галузі права.

НДЗП 1.1.11. Основи криптографічного захисту інформації

Мета вивчення курсу: формування сучасного рівня культури з інформаційної безпеки; набуття практичних навичок з основ застосування сучасних методів забезпечення захисту інформації в комп'ютерних системах, починаючи з криптографічних методів захисту інформації; формуванні у студентів розуміння основ інформаційної безпеки, вміння застосовувати криптографічні методи шифрування, вміння проектувати підсистеми захисту комп'ютерних систем, вміння застосовувати методи шифрування інформації для передачі у мережі, вміння розробляти парольні захищенні системи, ознайомлення зі шляхами використовування управління доступом різними методами; ознайомлення студентів з актуальними питаннями впливу комп'ютерних вірусів і шкідливих програм на безпеку комп'ютерних систем та методам протидії цьому, ознайомлення з методами захисту мережевої інформації.

Завдання курсу: надання основних відомостей з принципів протидії спробам несанкціонованого доступу до інформації з боку сторонніх осіб; придбання знань в області захисту інформації в комп'ютерних системах та мережах з урахуванням сучасного стану та прогнозу розвитку методів; освоєння засобів аналізу погроз інформаційній безпеці; вивчення принципів використання основних методів, принципів, алгоритмів, систем та засобів здійснення захисту інформації у системах та мережах.

Змістові модулі:

1. Основи криптографії.
2. Методи і засоби криптографічного захисту інформації в комп'ютерних системах.

НДЗП 1.1.12. Фізичне виховання

Мета вивчення курсу: формування всебічно розвинених особистостей, підготовка студентів до високоякісної праці за обраних фахом, збереження та зміцнення здоров'я.

Завдання курсу: збереження та зміцнення здоров'я, загартування організму, прищеплення навичок здорового способу життя, підвищення фізичної і розумової працездатності; виховання у студентів потреби до систематичних занять фізичними вправами, прагнення до фізичного вдосконалення; оволодіння системою спеціальних знань з основ теорії і методики, організації фізичного виховання; набуття необхідних знань у галузі гігієни праці, харчування спорту; формування життєво важливих вмінь і навичок, розвиток фізичних здібностей

Змістові модулі:

1. Розвиток загальних фізичних якостей, подальший розвиток витривалості.
2. Основи методики розвитку силових здібностей.
3. Основи методики розвитку швидкісно-силових здібностей.
4. Розвиток швидкісних якостей та складно координаційних здібностей.

1.2 Дисципліни професійної підготовки

НДПП 1.2.1. Вища математика

Мета вивчення курсу: формування у студентів фундаментальних понять алгебраїчного та геометричного характеру, а також умінь застосування цих понять до розв'язання практичних задач, забезпечення теоретичною підготовкою та фундаментальною базою успішного вивчення дисциплін професійної та практичної підготовки, які передбачені навчальними планами; оволодіння основними методами дослідження і вирішення математичних завдань, вироблення вміння самостійно розширювати математичні знання і проводити математичний аналіз прикладних задач.

Завдання курсу: навчання студентів теоретичним основам і методам теорії лінійної алгебри, векторної алгебри та аналітичної геометрії і застосуванню цих методів для розв’язання різноманітних задач теоретичного та практичного характеру, формування у студентів ключових і міждисциплінарних компетенцій, що забезпечують успішне проходження ними дисциплін практичного, спеціального і професійного спрямування.

Змістові модулі:

1. Вступ до вищої алгебри.
2. Векторна алгебра.
3. Аналітична геометрія на площині та у просторі.
4. Многочлени від одного невідомого.
5. Лінійна алгебра.
6. Лінії та поверхні другого порядку .
7. Елементи теорії множин, дійсних чисел і числові послідовності.
8. Границя функції, диференціювання функцій однієї змінної, дослідження функцій.
9. Функції багатьох змінних.
10. Інтегральне числення. Неозначений інтеграл, означений, невласні та кратні інтеграли.
11. Теорія поля.
12. Числові ряди.
13. Функціональні та степеневі ряди.
14. Ряди Фур’є.

НДПП 1.2.2. Дискретна математика

Мета вивчення курсу: надання майбутнім фахівцям базових знань з теорії множин, математичної логіки та теорії алгоритмів, теоретичних і практичних знань в області проектування систем з застосуванням дискретного аналізу.

Завдання курсу: навчання студентів теоретичним основам і методам теорії множин, математичної логіки і дискретної математики та застосуванню цих методів для розв’язання різноманітних задач теоретичного та практичного характеру.

Змістові модулі:

1. Теорія множин і математична логіка.
2. Теорія алгоритмів.
3. Основи теорії множин.
4. Елементи комбінаторного аналізу.
5. Теорія графів.
6. Дерева.
7. Мережі.

НДПП 1.2. 3. Теорія ймовірностей та математична статистика

Мета вивчення курсу: отримання базових знань і основних навичок по теорії ймовірності, випадкових процесів та математичної статистики для розв'язування задач, які виникають в математичному забезпеченні прикладної діяльності, вироблення ймовірнісно-статистичного мислення та інтуїції, формування навичок побудови ймовірнісних моделей дослідження та розв'язування відповідних задач.

Завдання курсу: формування у студентів системи математичних знань, необхідних для побудови ймовірних моделей явищ, уміння відображати та аналізувати результати експериментів та спостережень.

Змістові модулі:

1. Вступ до теорії ймовірностей.
2. Випадкові величини.
3. Випадкові процеси.
4. Математична статистика.

НДПП 1.2. 4. Фізика

Мета вивчення курсу: освоєння фундаментальних фізичних законів і понять, теорій, методів класичної і сучасної фізики.

Завдання курсу: формування наукового мислення і наукового світогляду; формування навичок володіння основними прийомами і методами вирішення науково-технічних завдань; ознайомлення з сучасною науково-дослідної апаратурою і вимірювальними приладами; ознайомлення з історією фізики і її розвитком, а також з основними напрямами і тенденціями розвитку сучасної фізики; формування навичок проведення наукових досліджень; формування культури мислення, усної та письмової мови, розвиток здатності до узагальнення, аналізу, сприйняття інформації, постановці мети та вибору шляхів її досягнення.

Змістові модулі:

1. Механіка і молекулярна фізика.
2. Електрика і фізика коливань.
3. Квантова фізика.

НДПП 1.2.5. Прикладна криптологія

Мета вивчення курсу: формуванні у студентів розуміння основ прикладної криптології, вміння застосовувати криптографічні методи дешифрування, вміння застосовувати методи зламу інформації, ознайомлення студентів з актуальними питаннями впливу шкідливих програм на безпеку комп'ютерних систем та методам протидії цьому.

Завдання курсу: придбання знань в області криптології з урахуванням сучасного стану та прогнозу розвитку методів захисту за зламу; вивчення принципів використання основних методів, принципів, алгоритмів, систем та засобів здійснення захисту інформації у системах та мережах.

Змістові модулі:

1. Основи криптології.
2. Методи та засоби криптології.

НДПП 1.2.6. Теорія інформації та кодування

Мета вивчення курсу: є надання студентам знань з теорії інформації та кодування для розуміння функціонування комп'ютерних систем, а також розвитку у студентів навичок самостійної роботи для освоєння методів формування і кодування повідомлень при їх передачі по трактах зі значним рівнем завад. Формування у студентів вмінь кількісно

оцінювати інформацію у повідомленнях для дискретних і неперервних ансамблів та джерел, а також кодувати повідомлення у дискретних і неперервних каналах.

Завдання курсу: придбання і закріплення основних засобів оцінки кількості інформації, освоєння сучасних методів та алгоритмів кодування для джерел повідомлень і передачі даних по каналам зв'язку; знати принципи побудови завадостійких кодів та їх використання в сучасних комп'ютерних інформаційних системах; вміти використовувати основні принципи кодування інформації з метою підвищення ефективності вводу, збереження, обробки та передачі інформації в сучасних інформаційних технологіях.

Змістові модулі:

1. Інформація та інформаційні процеси.
2. Кодування в дискретних і неперервних каналах.
3. Стиснення та кодування даних у комп'ютерних інформаційних технологіях.
4. Коди, що виявляють та виправляють помилки.

НДПП 1.2.7. Алгоритми та структури даних

Мета вивчення курсу: формування системи знань в області алгоритмізації та структур даних, а також вмінь і навичок складання алгоритмів та вибору типів структур, необхідних для вирішення поставлених задач фахового спрямування.

Завдання курсу: оволодіння основами алгоритмізації на рівні, достатньому для опрацьовування задач системного аналізу, пов'язаних з подальшою практичною діяльністю фахівця в області моделювання об'єктів і процесів, напрацювання навичок самостійної роботи з науковою літературою, розглядання методів дослідження та розв'язання прикладних задач.

Змістові модулі:

1. Аналіз алгоритмів.
2. Структури даних (поняття структури даних, структурні та лінійні типи даних, хешування даних, нелінійні структури даних).
3. Алгоритми пошуку та сортування.

НДПП 1.2.8. Нормативно-правове забезпечення інформаційної безпеки

Мета вивчення курсу: вивчення сучасних понять нормативно-правового забезпечення інформаційної безпеки, як однієї з найважливіших сфер діяльності в умовах входження держави в інформаційне суспільство та алгоритмів необхідних в подальшому при розробці систем захисту інформації в комп'ютерних системах та мережах.

Завдання курсу: формування у студентів певних знань та вмінь з основ нормативно-правового забезпечення інформаційної безпеки держави. Визначити основні терміни, поняття та категорії нормативно-правового забезпечення інформаційної безпеки на рівні тлумачення та відтворення, підзаконні нормативні акти із захисту інформації, основні положення нормативно-правового забезпечення інформаційної безпеки держави для їх практичного застосування та втілення у процесі фахової діяльності майбутнього спеціаліста з інформаційної безпеки, вільно орієнтуватися в питаннях інформаційної безпеки держави, самостійно давати характеристику стану законодавчої бази у сфері нормативно-правового забезпечення інформаційної безпеки.

Змістові модулі:

1. Загальна нормативно правова база інформаційної безпеки. Основні поняття та положення.
2. Спеціалізована нормативно-правова база інформаційної безпеки.
3. Забезпечення функціонування Національної системи конфіденційного зв'язку.
4. Міжнародні норми та положення щодо сфери інформатизації і захисту інформатизації.

НДПП 1.2.9. Комп'ютерні мережі

Мета: придбання знань в області теорії комп'ютерних мереж, а також навичок проектування корпоративних комп'ютерних мереж і їхнього використання для пошуку, обробки й аналізу даних, необхідних для прийняття ефективних управлінських рішень.

Завдання: ознайомити студентів з основами побудови комп'ютерних мереж, засобами комунікаційної техніки, концепціями побудови локальних і глобальних комп'ютерних мереж; вивчити сучасні комп'ютерні технології й основні засоби забезпечення їх працездатності; ознайомитися із програмним забезпеченням мережевих технологій і тенденціями їх розвитку на сучасному етапі; надати практичних навичок проектування корпоративної комп'ютерної мережі стосовно до умов конкретного об'єкта.

Змістові модулі

1. Принципи побудови та організації взаємодії в комп'ютерних мережах. Локальні мережі.
2. Глобальні комп'ютерні мережі. Програмне забезпечення комп'ютерних мереж.

НДПП 1.2.10. Програмування

Мета вивчення курсу: набуття студентами знань, вмінь та навичок, необхідних для ефективного використання мов програмування при розробці прикладного і системного програмного забезпечення, розв'язування практичних обчислювальних задач за допомогою персонального комп'ютеру; ознайомлення студентів з сучасною мовою програмування С++ та оволодіння основними можливостями цієї мови, навичками хорошого стилю програмування, методами проектування та створення програм згідно сучасних технологій програмування; формуванні у студентів розуміння основ теоретичних концепцій, принципів та понять сучасного, зокрема композиційного, програмування, методів формалізації мов програмування та доведення коректності програм.

Завдання курсу: набуття компетенцій, знань, умінь та навиків на рівні новітніх досягнень у теорії програмування відповідно до кваліфікації.

Змістові модулі:

1. Підготовка задач к розрахунку на ПК .
2. Базові поняття програмування та їх реалізація засобами мови С++.
3. Функціональне програмування.
4. Об'єктно- орієнтоване програмування.

НДПП 1.2.11. Інформаційні технології та системи

Мета вивчення курсу: формування у студентів теоретичних знань та практичних навичок, необхідних безпосередньо для проектування та використання інформаційних технологій для створення комп'ютерних систем та забезпечення їх роботи; ознайомлення студентів з теоретичними положеннями та практичними навиками, що створюють основи побудови складних корпоративних інформаційних систем та їх складових частин – автоматизованих робочих місць фахівців та керівних осіб.

Завдання курсу: надання студентам знань, щодо структури та основних методів створення і використання інформаційних технологій та систем, які містять інформацію про стан об'єктів дослідження або управління, а також економічні й технологічні показники виробничої та інших сторін діяльності підприємств та установ, функціонування технічних засобів, набуття студентами практичних навичок із створення персонального інформаційного середовища фахівця будь-якого обраного профілю на базі сучасних комп'ютерних технологій, а також вмінню використовувати інформаційні системи для вирішення прикладних задач відповідно до їх професійній спрямованості; закріплення у студентів практичних навичок роботи з складними інформаційними технологіями при вирішенні прикладних задач.

Змістові модулі:

1. Сучасні інформаційні технології проектування комп'ютерних систем.
2. Аналіз і етапи проектування інформаційних систем.
3. Особливості проектування інтерфейсів інформаційних систем.

НДПП 1.2.12. Основи теорії кіл, сигналів та процесів в електроніці

Мета вивчення курсу: навчити студентів методам кількісного аналізу усталених та перехідних явищ та процесів, що відбуваються в лінійних та нелінійних колах постійного та змінного струмів.

Завдання курсу: надання студентам знань щодо основних фізичних понять електромагнітних явищ; методів розрахунку та аналізу лінійних електричних та магнітних кіл; методів розрахунку нелінійних кіл постійного та змінного струму; суті процесів, що відбуваються при перехідних режимах роботи схеми та методи розрахунку таких кіл; явищ, що відбуваються в колах з розподіленими параметрами, методи розрахунку таких кіл; методів синтезу реактивних багатополюсників.

Змістові модулі:

1. Основні поняття теорій електричних кіл. Розрахунок кіл методом еквівалентного генератора.
2. Використання синусоїдного струму в радіотехніці.
3. Основи теорії багатополюсників.
4. Багатоелементні двополюсники, їх властивості та характеристики.
5. Основи теорії чотириполюсників.
6. Перехідні процеси.
7. Загальна характеристика нелінійних кіл та методів їх розрахунку.
8. Основи теорії кіл з розподіленими параметрами.

НДПП 1.2.13. Управління інформаційною безпекою

Мета вивчення курсу: надати студентам знання, основні рекомендації та загальні принципи щодо здійснення, підтримки і поліпшення системи управління інформаційною безпекою підприємства на базі міжнародних стандартів серії ISO/IEC, що забезпечують загальне керівництво безпекою інформації на загальноприйнятих показниках.

Завдання курсу: забезпечити розуміння концепції менеджменту інформаційної безпеки на базі міжнародних стандартів серії ISO/IEC; надати знань щодо порядку створення системи менеджменту інформаційної безпеки (СМІБ); загальних вимог забезпечення документацією СМІБ; обов'язків керівників СМІБ; порядку проведення внутрішніх та зовнішніх аудитів коректності реалізації СМІБ; цілей управління СМІБ; засобів управління СМІБ; основних понять і визначення моделі оцінки ризику.

Змістові модулі:

1. Основні положення системи управління інформаційною безпекою
2. Використання моделі PDCA при організації СМІБ на базі міжнародного стандарту ISO / IEC 27001
3. Базові правила управління інформаційною безпекою

НДПП 1.2.14. Електроніка

Мета вивчення курсу: оволодіння студентами теоретичними навичками аналізувати, розраховувати, синтезувати та проектувати електроні аналогові та цифрові пристрої, які використовуються в системах захисту інформації

Завдання курсу: надання студентам знань щодо основних типів цифрових та аналогових електронних пристроїв, а також розумінню їх роботи та характеристик; набуття практичних навичок щодо використання елементів та пристроїв при проектуванні електронних систем.

Змістові модулі:

1. Напівпровідникові та мікроелектронні прилади.
2. Аналогові та імпульсні електронні пристрої.

2.1.Підсилювальні пристрої.

2.2.Операційний підсилювач

2.3.Елементи імпульсних пристроїв.

2.4.Тригерні і генераторні пристрої.
2.5.Джерела вторинного електроживлення.
3. Основи цифрової техніки.
3.1.Логічні функції і логічний пристрій.
3.2.Логічні елементи.
3.3.Елементи пам'яті на тригерах.
3.4.Комбінаційні логічні пристрої.
3.5.Комбінаційні цифрові пристрої.
3.6.Запам'ятовуючі пристрої.
3.7.Аналогово-цифрові та цифро аналогові перетворювачі.

НДПП 1.2.15. Архітектура комп'ютерних систем

Мета вивчення курсу: ознайомлення студентів з побудовою апаратної частини комп'ютерів та освоєння основ програмування на низькому рівні, тобто програмування мовою ASSEMBLER; вивчення і засвоєння принципів роботи з наступними програмами і пакетами програм: ОС DOS, Windows, Linux, файловим менеджером Far-manager, математичним пакетом MatLAB, програмами пакету Microsoft Office 2010: табличним процесором (EXCEL), текстовим редактором (WORD).

Завдання курсу: надання студентам системного уявлення про архітектуру сучасних CPU та комп'ютерних систем, організація адресного простору пам'яті в реальному та захищеному режимах, організація низькорівневої взаємодії периферійних приладів ПК, основи мови програмування ASSEMBLER.

Змістові модулі:

1.Апаратна архітектура обчислювальних систем.
2.Основи програмування низького рівня комп'ютерів.
3.Системне програмне забезпечення.
4.Програмне забезпечення MatLAB.

НДПП 1.2.16. Захист інформації в комп'ютерних системах та мережах

Мета вивчення курсу: закласти термінологічний фундамент, навчити студентів правильно проводити аналіз погроз інформаційній безпеці, основним методам, принципам, алгоритмам захисту інформації в комп'ютерних системах та мережах з урахуванням сучасного стану та прогнозу розвитку методів, систем та засобів здійснення погроз зі сторони потенційних порушників.

Завдання курсу: формування у студентів певних знань та вмінь з теорії та практики захисту інформації, за результатами яких студенти повинні знати сучасні погрози безпеці інформаційним системам; технічні методи і засоби захисту інформації; програмні методи і засоби захисту; методи захисту інформації в розподілених інформаційних системах; організаційно-правове забезпечення захисту інформації; а також вміти аналізувати можливості несанкціонованого здобуття інформації потенційними порушниками; аналізувати вплив комп'ютерних вірусів і шкідливих програм на безпеку комп'ютерних систем; виявляти дії вірусу в ОС Windows за допомогою аналізу процесів, що протікають, за допомогою аналізу кодів підозрілих програм, за допомогою антивірусних програм; організовувати та виконувати практичні дій посадових осіб відділу захисту інформації відповідно до інструкцій і обов'язків.

Змістові модулі:

1. Основи безпеки інформації.
2. Захист інформації в комп'ютерних системах від випадкових погроз.
3. Технічні методи і засоби захисту інформації.
4. Програмні методи і засоби захисту.
5. Захист інформації в розподілених інформаційних системах.
6. Організаційно-правове забезпечення захисту інформації.

НДПП 1.2.17. Комплексні системи захисту інформації

Мета вивчення курсу: оволодіння студентами комплексом знань у галузі захисту інформації, системами й методами визначення захищеності програмних продуктів, пристроїв; комп'ютерних мереж, їх складових та набуття на основі цих знань практичних навичок та теоретичних знань, необхідних для творчого підходу в питанні сучасного та майбутнього оперативного захисту комп'ютерної техніки й інформації; оволодіння студентами алгоритмами створення сучасних програм захисту, алгоритмами кодування, сучасними методами, технологією, комп'ютерними програмними, технічними засобами у галузі безпеки: операційних систем, текстових редакторів, табличних процесорів, систем управління базами даних, конфіденціальної інформації тощо; набуття на основі вказаних знань практичних навичок, необхідних для розробки систем захисту, керування розробкою систем захисту, а на основі вказаного, нормального забезпечення роботи організацій, зі збереженням характеристик трафіку, швидкості санкціонованого доступу тощо; опанування концептуальними моделями розробки, розподілення, обробки, використання та зберігання конфіденціальних документів; стратегією вибору систем виявлення атак, навичками роботи з пристроями безпеки в локальних та глобальних комп'ютерних мережах із метою використання їх, можливостей для покращання показників безпеки в них.

Завдання курсу: студенти повинні здобути знань та практичних навичок щодо засобів дії загроз на об'єкти інформаційної безпеки установ, про правові і нормативні акти, які визначають систему захисту інформації в державі; керівні документи, що визначають ступінь захищеності комп'ютерних систем; методи проведення аналізу надійності системи захисту інформації в комп'ютерних системах; основні методи, технологію, принципи і правила побудови захисту комп'ютерних систем, в тому числі, персональних комп'ютерів, їх елементів і об'єктів комп'ютерних мереж; мати достатньо повне уявлення про алгоритми створення сучасних програм, алгоритми кодування та застосування стандартного програмного забезпечення захисту; методи та технологію захисту операційних систем, текстових редакторів, табличних процесорів, системи управління базами даних, у локальних, корпоративних та глобальних комп'ютерних мережах установ, на основі вивчених алгоритмів вміти розробляти нові програмні складові захисту в майбутньому; здобути практичні навички роботи з концептуальними моделями розробки, розподілення, обробки, використання та зберігання конфіденціальних документів; роботи з системами й методами визначення захищеності носіїв інформації; створення засобами стандартного програмного забезпечення елементів захисту інформації; формулювати завдання щодо питань захисту інформації та, формалізуючи їх, вказувати шляхи вирішення.

Змістові модулі:

1. Основні категорії інформаційної безпеки.
2. Безпека інформаційних систем.
3. Законодавча база в галузі захисту інформації.
4. Комплексні системи захисту.

НДПП 1.2.18. Комп'ютерна графіка та моделювання

Мета вивчення курсу: формування у майбутніх фахівців сучасного рівня інформаційної культури у галузі комп'ютерної графіки; ознайомлення з основними методами і алгоритмами теорії обробки зображень; набуття практичних навичок з основ застосування сучасних технологій обробки зображень за допомогою сучасних комп'ютерних засобів та спеціалізованих пакетів роботи із графікою; формування у студентів розуміння основ комп'ютеризації сучасних методів обробки графічної інформації, а також інформаційного забезпечення, системи знань та вмінь, зорієнтованих на проведенні інформаційної та інформаційно-аналітичної роботи з використанням спеціалізованого прикладного програмного забезпечення для роботи з зображеннями; ознайомлення студентів з актуальними питаннями використання засобів для роботи з комп'ютерною графікою та обробки зображень.

Завдання курсу: придбання і закріплення знань студентами в області використання інформаційних технологій для роботи з комп'ютерною графікою; вивчення пакетів програм; придбання знань в області обробки зображень за допомогою методів та алгоритмів комп'ютерної графіки; освоєння методики і технологій обробки зображень, зокрема фільтрації, сегментації та ін.

Змістові модулі:

1. Види графіки.
2. Методи та алгоритми обробки зображень.
3. Сучасні комп'ютерні системи моделювання та пакети для роботи з графічною інформацією.

НДПП 1.2.19. Теорія і практика інфраструктури відкритих ключів

Мета вивчення курсу: навчання студентів принципам побудови комплексних систем захисту інформації, розробки, дослідженню та застосуванню механізмів захисту інформації, що засновані на використанні алгоритмів традиційної (симетричної) криптографії та криптографії з відкритим ключем для забезпечення безпеки програмного забезпечення, вивчення студентами основ стеганографічного захисту інформації та особливості побудови інфраструктури відкритих ключів.

Завдання курсу: формування у студентів володіння принципами побудови комплексних систем захисту інформації; вміння розробляти, проводити дослідження та застосовувати механізми щодо забезпечення автентичності, цілісності та конфіденційності в програмно-апаратних, програмних засобах; володіння основами стеганографічного захисту інформації, принципами захисту програмного коду від зламу/модифікації; вміння побудови інфраструктури відкритих ключів.

Змістові модулі:

1. Принципи безпеки та захисту інформації в програмному забезпеченні.
2. Основи технології інфраструктури відкритих ключів.

Додаток Б

ОПИС ВИБІРКОВИХ НАВЧАЛЬНИХ ДИСЦИПЛІН

2.1 Дисципліни загальної підготовки

ВДЗП 2.1.1. (1). Маркетинг

Мета вивчення курсу: формування системи знань про сутність і зміст маркетингу як філософію підприємницької діяльності в умовах ринкової економіки і конкуренції, розгляд проблем реалізації його основних політик - товарної, цінової, політики комунікацій та розподілу.

Завдання курсу: вивчення основних понять, систем і алгоритмів маркетингу; набуття практичних навичок розв'язання конкретних маркетингових завдань; формування вмінь творчого пошуку резервів удосконалення маркетингової діяльності підприємства.

Змістові модулі:

1. Основи маркетингу.
2. Інформаційне забезпечення систем маркетингу.

ВДЗП 2.1.1. (2). Безпекознавство

Мета вивчення курсу: ознайомити студентів із проблемами формування національної безпеки України; основними формами й видами безпеки в сучасному багатополюсному світі.

Завдання курсу: комплексне вивчення основних теоретичних та практичних аспектів формування національної безпеки України та інших розвинених країн світу.

Змістові модулі:

1. Теоретично – методологічне підґрунтя вивчення проблеми національної безпеки. Правова, політична, економічна, воєнна безпека України.
2. Екологічна, інформаційна, міжнародна безпека України.

ВДЗП 2.1.2. (1). Правове супроводження ІТ-технологій

Мета вивчення курсу: засвоєння національно-правових і міжнародно-правових стандартів визначення та регламентації суспільних інформаційних відносин, провідним предметом яких є інформація як продукт та сукупність відомостей; визначення та аналіз форм і методів сучасної інформаційної діяльності, правових режимів практичного застосування інформації у різних сферах суспільної діяльності.

Завдання курсу: формування у студентів певних знань з теорії права, а саме з понять національно-правових і міжнародно-правових стандартів визначення та регламентації суспільних інформаційних відносин; ознайомити студентів з правовим забезпеченням сучасного розвитку інформаційних технологій, правовими режимами електронного обігу інформації та регулювання мережі Інтернет.

Змістові модулі:

1. Загальні засади правового регулювання інформаційних технологій.
2. Правове регулювання відносин, пов’язаних з обігом відкритої інформації та інформації з обмеженим доступом в інформаційних (національно-правові і міжнародно-правові стандарти визначення та регламентації).

ВДЗП 2.1.2. (2). Правові основи охорони здоров’я людини

Мета вивчення курсу: сформувати у студентів систему уявлень про основи організації охорони здоров’я в Україні, що мали б змогу оволодіти системою теоретичних знань, набути практичних навичок застосування законодавства з охорони здоров’я в різних сферах суспільного життя.

Завдання курсу: проаналізувати національні основи законодавства з охорони здоров’я, висвітлити правовий статус суб’єктів медичних правовідносин, з’ясувати форми, способи і засоби захисту прав суб’єктів медичних правовідносин.

Змістові модулі:

1. Історико-правовий огляд нормативного регулювання охорони здоров'я. Права людини у сфері охорони здоров'я. Захист прав пацієнтів.
2. Медичне страхування. Правове регулювання надання платних медичних послуг. Правове регулювання експертної діяльності у сфері охорони здоров'я в Україні. Дефекти надання медичної допомоги: юридична оцінка.

ВДЗП 2.1.3. (1). Міжнародна інформація

Мета вивчення курсу: ознайомити студентів із становленням і сучасним розвитком поширення інформації у світі, а також із системою її використання; висвітлити еволюцію ставлення міжнародних організацій до проблем інформації і комунікації, нові економічні і правові аспекти; навчити студентів визначати зміни в міжнародних інформаційних структурах і процесах поширення інформації.

Завдання курсу: набуття студентами теоретичних знань з питань визначення системи інформації на загальносвітовому рівні, її значення для розвитку політичних процесів; розуміння студентами сучасних тенденцій та актуальних проблем міжнародної комунікації та інформації; розуміння змісту основних положень права особи на інформацію, використання новітніх технологій; придбання практичних навичок застосовувати здобуті знання.

Змістові модулі:

1. Основні поняття міжнародної комунікації та інформації.
2. Історія розвитку та поширення інформації.
3. Інформаційне суспільство.
4. Перші спроби використання інформації в політичних цілях. Політичні процеси в сучасних умовах та роль інформації.
5. Новітні технології та їх використання в політичних процесах.
6. Національне та міжнародне інформаційне право.
7. Діяльність міжнародних організацій в міжнародній інформаційній сфері.
8. Міжнародні стандарти свободи слова.
9. Захист особистих даних.
10. Інформаційна безпека та інформаційні війни.
11. Світовий ринок інформаційних технологій.

ВДЗП 2.1.3. (2). Конфліктологія та теорія переговорів

Мета вивчення курсу: ознайомлення студентів із загальною теорією конфлікту як соціального феномену, з поняттями, методами, концепціями теоретичної конфліктології, формування вмінь діагностувати, прогнозувати, регулювати конфлікти, а також вміння позитивно сприймати конфлікт та прагматично його використовувати.

Завдання курсу: вивчення студентами теоретичних та практичних основ з питань сутності конфліктології як системи знань; розвитку конфліктологічної думки; загальної теорію конфлікту; змісту процесу управління конфліктом; переговорів як способу вирішення конфліктів.

Змістові модулі:

1. Загальна теорія конфлікту.
2. Управління конфліктом.

ВДЗП 2.1.4. (1). Психологія спілкування

Мета вивчення курсу: засвоєння студентами основних теоретичних підходів до вивчення проблем комунікації та спілкування, формування навиків аналізу смислів та змісту комунікаційних актів, навиків розпізнання невербальної сигналізації та емоцій співбесідника, навиків збереження комунікативної рівноваги та ефективності комунікації.

Завдання курсу: оволодіння студентами та подальше вільне оперування професійною термінологією, використовуваною в даній сфері практичної діяльності; набуття теоретичних знань та вмінь розкрити взаємозв'язки міжособистісного спілкування з іншими формами комунікативних процесів, характеризувати міжособистісну комунікативну взаємодію у зв'язку с цілями та мотивами комунікантів, ставленням один до одного, сценаріями спілкування, характеризувати особливості розуміння комунікантами один одного; формування у студентів навичок аналізу смислів за змісту повідомлень та діалогів у комунікативних актах; набуття вмінь розкрити особливості використання психологічних знань про комунікативні процеси у формуванні комунікативної компетентності, навичок рефлексії та емпатії, ефективної комунікації.

Змістові модулі:

1. Сприймання та розуміння у комунікації.
2. Спілкування як взаємодія.

ВДЗП 2.1.4. (2). Психологія управління

Мета вивчення курсу: розкрити психологічні закономірності управлінської діяльності, дати студентам знання, що застосовуються при вирішенні проблеми управління організацією та її членами.

Завдання курсу: розкрити теоретичні поняття і положення психології управління, сучасні підходи до розуміння управління соціальними системами, структуру та категоріальний апарат психології управління, психологічні закономірності управлінської діяльності, методи психологічних досліджень в управлінні; навчити студентів використовувати одержані знання для забезпечення ефективної управлінської діяльності, реалізовувати основні напрями роботи практичного психолога в управлінській практиці.

Змістові модулі:

1. Місце психології управління в системі наукового знання.
2. Психологія управлінської діяльності.
3. Психологія особистості керівника.
4. Психологія організації в управлінні.

2.2 Дисципліни професійної підготовки

ВДПП 2.2.1. (1). Математичні перетворення в криптосистемах

Мета вивчення курсу: закласти математичний та термінологічний фундамент в галузі криптології, навчити студентів правильно проводити аналіз погроз безпеці інформації, основним методам, механізмам, алгоритмам та протоколам криптографічного захисту інформації в інформаційно – комунікаційних системах з урахуванням сучасного стану та прогнозу розвитку методів, систем та засобів здійснення погроз та проведення криптографічного аналізу зі сторони потенційних порушників.

Завдання курсу: формування у студентів певних професійних компетенцій, знань та вмінь з теорії та практики криптографічного захисту інформації та криптографічного аналізу.

Змістові модулі:

1. Математичні методи та симетричні криптографічні перетворення .
2. Асиметричні криптосистеми та методи автентифікації
3. Криптографічні механізми та протоколи

ВДПП 2.2.1. (2). Методи оптимізації та дослідження операцій

Мета вивчення курсу: формування у студентів системи знань з методології та інструментарію побудови і використання різних типів економіко-математичних моделей.

Завдання курсу: набуття студентами знань з основних принципів та інструментарію постановки задач, побудови економіко-математичних моделей, методів їх розв'язування та аналізу: вивчення теоретичних основ та методів математичного програмування (лінійного,

цілочислового, нелінійного, динамічного програмування) та теорії ігор; здобуття практичних навиків ставити реальні прикладні задачі у сфері економіки та управлінні, складати математичні моделі економічних задач та розв'язувати їх методами математичного програмування та теорії ігор, проводити після оптимізаційний аналіз та розробку практичних рекомендацій з прийняття рішень, самостійно опрацьовувати математичну літературу (самостійно розширювати свої знання, розвивати логічне і алгоритмічне мислення, користуватися довідниками і таблицями з різних розділів математики, самостійно освоювати програмні засоби за допомогою літератури та вбудованих довідкових систем або навчаючих програм).

Змістові модулі:

1. Задачі лінійного програмування.
2. Методика розв'язування задач лінійного програмування.
3. Задачі цілочислового програмування. Задачі теорії ігор.
4. Задачі нелінійного програмування. Задачі динамічного програмування.

ВДПП 2.2.2. (1). Організація баз даних та знань

Мета вивчення курсу: формування у студентів навичок практичного застосування існуючих систем управління базами даних; вживання ефективних моделей забезпечення даних на основі вивчення предметної галузі, методів аналізу, пошуку та використання існуючих систем управління базами даних; знайомство з існуючими системами управління базами даних реляційного типу; забезпечення теоретичної та інженерної підготовки фахівців у галузі проектування та використання систем управління базами даних.

Завдання курсу: освоєння студентами навичок використання сучасних інформаційних технологій для проектування баз даних різних предметних областей.

Змістові модулі:

1. Введення в бази даних.
2. Основи проектування баз даних.
3. Методи проектування баз даних.
4. Реляційна алгебра.
5. Нормалізація відносин.
6. Типологія баз даних.
7. Процеси обробки даних.

ВДПП 2.2.2. (2). Інформаційні управляючи системи

Мета вивчення дисципліни: отримання студентами знань з області розробки та створення інформаційно-управляючих систем і технологій. Оволодіння такими знаннями дозволить реалізовувати задачі автоматизації обробки інформації та автоматизації керування об'єктами за допомогою комп'ютерної техніки.

Завдання курсу: придбання системи знань по застосуванню методики аналізу, синтезу, оптимізації роботи інформаційних управляючих систем, розробці та супроводженні програмних комплексів і систем, методології використання інформаційних управляючих систем.

Змістові модулі:

1. Основні концепції інформаційних систем
2. Інформаційне та програмне забезпечення інформаційних управляючих систем

ВДПП 2.2.3. (1). Системи штучного інтелекту

Мета вивчення курсу: вивчення студентами методів та засобів створення комп'ютерних систем штучного інтелекту, отримання відомостей про концептуальні основи штучного інтелекту, методи подання знань і баз знань, системи нечіткої логіки, будову та можливості використання експертних систем, основні поняття про системи розпізнавання образів, штучні нейронні мережі, генетичні алгоритми.

Завдання курсу: отримання студентами знань щодо методів штучного інтелекту, надання основних відомостей щодо структурування та формалізації знань експертів (дуальну стратегію проектування, об'єктно-структурний підхід, алгоритм ОСА або практичні методи структурування), освоєння засобів створення бази знань для експертної системи, ознайомлення з методиками створення моделей знань: продукційні, семантичні мережі, фрейми, формальні логічні моделі для подальшого використання моделі у експертній системі; отримання основних відомостей щодо розробки експертних системи, за допомогою аналізу фахових знань, отриманих від експерта предметної галузі.

Змістові модулі:

1. Представлення знань в інтелектуальних системах.
2. Експертні системи. Еволюційні методи штучного інтелекту.

ВДПП 2.2.3. (2). Захищені банківські технології

Мета вивчення курсу: формування професійної компетентності майбутніх фахівців з кібербезпеки, достатньої для роботи на посаді адміністратора інформаційної безпеки банку та необхідної для розвитку кар'єри.

Завдання курсу: ознайомлення студентів із теоретичними основами функціонування банківської системи України; системою електронних міжбанківських платежів (СЕП), програмно-апаратними засобами НБУ для захисту інформації у СЕП; національною платіжною системою «Український платіжний простір» та захистом транзакцій; адміністративними, технічними і технологічними функціями Засвідчуваного центру ключів НБУ та служби, що їх виконують; призначеннями та організаційними структурами міжнародної міжбанківської телекомунікаційної системи SWIFT, безпекою передачі та опрацювання повідомлень SWIFT; актуальними та перспективними моделями захисту інформації у системах дистанційного банківського обслуговування; протоколом захищених електронних транзакцій SET та його засобів для захисту транзакцій в інтернеті; автоматизованою системою обслуговування фондового ринку та захист інформації у ній.

Змістові модулі:

1. Захист інформації у банківських системах електронних платежів.
2. Безпека дистанційних транзакцій.
3. Структура та функції автоматизованої банківської системи.
4. Система захисту інформації банку.

ВДПП 2.2.4. (1). Захист операційних систем та баз даних

Мета вивчення курсу: формування у студентів базових навичок щодо застосування методів захисту операційних систем і баз даних, знань різних аспектів, пов'язаних із забезпеченням безпеки операційних систем і баз даних, механізмів і сервісів безпеки комп'ютерних систем.

Завдання курсу: розкриття термінологічного апарату з безпеки операційних систем, загальних принципів захисту операційних систем; уявлення про можливі загрози операційним системам; вивчення нормативних вимог і керівних документів по забезпечення безпеки операційних систем; навчання методикам проведення заходів захисту операційних систем; розкриття термінологічного апарату з безпеки систем баз даних, принципів захисту баз даних; уявлення про можливі загрози системам баз даних; вивчення нормативних вимог до забезпечення безпеки систем баз даних; навчання методикам проведення заходів щодо захисту систем баз даних.

Змістові модулі:

1. Безпека клієнтських операційних систем.
2. Безпека серверних операційних систем
3. Апаратні та програмні засоби захисту баз даних
4. Засоби захисту баз даних

ВДПП 2.2.4. (2). Основи системного аналізу та прийняття рішень

Мета вивчення курсу: засвоєння студентами теоретичних знань з системного аналізу інформаційних систем як методологічної основи проектування та моделювання складних систем за допомогою методів системного підходу, широко застосовуваного при вирішенні глобальних і спеціальних проблем, таких як моніторинг, керування технологічними процесами, промисловими і транспортними системами, наукові дослідження, технічне діагностування, і т.п; одержання студентами необхідних теоретичних знань та навичок з використання математичного апарату формалізованих задач системного аналізу та теорії прийняття рішень.

Завдання курсу: вивчення методології системного підходу, набуття навичок використовування методів системного аналізу та теорії прийняття рішень; набуття вміння виконувати усі етапи системного дослідження; отримання знань з побудови відповідних математичних моделей та обрання методу розв'язування задачі системного аналізу відповідно до її типу з подальшим аналізом отриманих результатів.

Змістові модулі:

1. Математичний апарат формалізованих задач системного аналізу.
2. Методологічні принципи і прийоми інформаційного аналізу системних задач.
3. Методи системного аналізу та теорії прийняття рішень.
4. Системний аналіз управління складної багаторівневої ієрархічної системи в умовах багатофакторного ризику.

ВДПП 2.2.5. (1). Моделювання інформаційної безпеки

Мета вивчення курсу: формування у студентів системи знань з методології та інструментарію побудови і використання різних типів моделей інформаційної безпеки організацій.

Завдання курсу: ознайомлення студентів із теоретичними основами інформаційної безпеки систем; формування теоретичного базису щодо розуміння фундаментальних категорій безпеки систем; вивчення та опрацювання концептуальних методологічних підходів щодо моделювання системи безпеки у будь-якій сфері життєдіяльності людини.

Змістові модулі:

1. Термінологія та зміст основних понять моделювання інформаційної безпеки.
2. Методи структурної ідентифікації об'єктів і процесів, поточного стану інформаційної безпеки. Методи визначення ступеню взаємозв'язків між факторами та їх влив на стан інформаційної безпеки підприємства.
3. Оцінка адекватності отриманих моделей. Моделювання можливих сценаріїв зміни інформаційної безпеки організації.

ВДПП 2.2.5. (2). Інформаційна безпека держави

Мета вивчення курсу: набуття студентами розуміння, що інформаційна безпека є однією із суттєвих складових частин національної безпеки країни, її забезпечення завдяки послідовній реалізації грамотно сформульованої національної інформаційної стратегії в значній мірі сприяла б забезпеченню досягнення успіху при вирішенні задач у політичній, військово-політичній, військовій, соціальній, економічній та інших сферах державної діяльності, використовуючи правила відношення інформації до державної таємниці, конфіденційної інформації, що є власністю держави, недержавної конфіденційної і відкритої інформації що потребує захисту, шляхи побудови систем забезпечення інформаційної безпеки. Предметом методології інформаційної безпеки є дослідження способів, методів, засобів і каналів реалізації загроз національним інтересам на інформаційному рівні та їх своєчасного виявлення, запобігання і нейтралізації.

Завдання курсу: ознайомлення з основними напрями державної політики з питань національної безпеки України; розуміння місця і ролі інформаційної безпеки в системі національної безпеки держави; засвоєння методів та чинників, які обумовлюють

неминучість інформаційних воєн розв'язування задач; отримання студентами навичок визначення, класифікація і властивості інформаційної зброї, застосування нейролінгвістичного програмування, знати сучасні технології маніпуляції суспільною свідомістю та сучасні засоби впливу на суспільство, правові основи забезпечення захисту прав і свобод людини в інформаційній сфері; виховувати студента як самоорганізаційну особистість в інформаційному просторі.

Змістові модулі:

1. Основи національної безпеки держави – організаційно-правові аспекти.
2. Сутність і класифікація інформаційних ресурсів.
3. Інформаційна зброя – сутність механізмів дії та можливі наслідки для системи державного управління, суспільства, особистості.
4. Державне і військове управління як об'єкт інформаційної боротьби.
5. Інформаційна безпека суспільства.

ВДПП 2.2.6. (1). Економічна безпека

Мета вивчення курсу: формування теоретичних знань та практичних навичок економіко-правового характеру щодо розвитку відносин між зацікавленими особами зовнішнього та внутрішнього середовищ в системі управління підприємством з метою підвищення рівня його економічної безпеки в ринковій економіці.

Завдання курсу: ознайомлення студентів із теоретичними основами захисту складових підприємства, методики та техніки гарантування безпеки суб'єктів господарювання різних форм власності, видів діяльності, а також вмінь та навичок з виявлення порушень фінансової, кадрової, технічної дисципліни, їх аналізу та встановлення причин виникнення і шляхів подолання.

Змістові модулі:

1. Поняття та основні категорії економічної безпеки.
2. Індикатори та складові економічної безпеки підприємства.
3. Система економічної безпеки підприємства.
4. Особливості діяльності служби безпеки підприємства.
5. Недобросовісна конкуренція та захист комерційної таємниці.
6. Ділова розвідка.

ВДПП 2.2.6. (2). Адміністрування комп'ютерних систем та мереж

Мета вивчення курсу: отримання знань, вмінь та навичок, необхідних фахівцю, який спеціалізується в області адміністрування та експлуатації комп'ютерних мереж для орієнтування в сукупності способів і методів адміністрування найсучаснішої та найновішої комп'ютерної техніки та комп'ютерних мереж.

Завдання курсу: отримання студентами глибоких знань з теорії та практики розгортання, адміністрування та експлуатації комп'ютерних мереж; навичок адміністрування локальних мереж під управлінням найбільш поширених операційних систем з використанням як пропрієтарних, так і відкритих технологій; оволодіння навичками адміністрування мереженого обладнання.

Змістові модулі:

1. Адміністрування робочих станцій і серверів на базі ОС з використанням відкритих технологій.
2. Адміністрування робочих станцій і серверів на базі ОС з використанням пропріє тарних технологій.
3. Адміністрування мереженого обладнання.
4. Моніторинг несправностей комп'ютерних систем, забезпечення захисту даних.

ВДПП 2.2.7. (1). Системи технічного захисту інформації

Мета вивчення курсу: ознайомити з принципами побудови та використання програмних та програмно-апаратних засобів для захисту програмного забезпечення та іншої інформації в комп'ютерних системах.

Завдання курсу: надати основні відомості з принципів побудови систем захисту інформації та методів протидії спробам несанкціонованого доступу до неї з боку сторонніх осіб, привласнення привілей тощо.

Змістові модулі:

1. Захист програмного забезпечення шляхом блокування доступу до комп'ютера.
2. Захист основних операційних систем.

ВДПП 2.2.7. (2). Кібернетична безпека підприємства

Мета вивчення курсу: є надання майбутньому фахівцеві достатнє уявлення про функціонування та розвиток економічної системи в єдності об’єкта та процесу управління.

Завдання курсу: вивчення студентами предмету фундаментальних основ кібернетичної безпеки підприємства, визначення і класифікацію систем, ієрархію економічної системи, як об’єкта кібернетичної безпеки, моделювання об’єктів, принципи, методи і моделі управління.

Змістові модулі:

1.Про співвідношення понять інформаційна та кібернетична безпека.
2.Моделі організації кібернетичної безпеки підприємства. Побудова систем і аудит їх ефективності.
3. Протидія загрозам інформаційної безпеки бізнесу з боку персоналу.
4.Стандарти захисту інформації.
5.Взаємодія служби безпеки з підрозділами ІТ забезпечення підприємства.
6.Електронні інформаційні ресурси, системи і процеси.
7.Типові сценарії несанкціонованого доступу до електронних систем і превентивний захист від них.
8.Захист інформації на АРМ, в мережах компанії і при передачі через Інтернет.
9.Антивірусний захист, захист інформації від програм-шпигунів.

ВДПП 2.2.8. (1). Інформаційно-аналітичне забезпечення інформаційної та кібернетичної безпеки

Мета вивчення курсу: навчання студентів сучасним методам забезпечення інформаційної та кібернетичної безпеки, освоєння міжнародних стандартів життєвого циклу систем і комплексів програм, інформаційно-аналітичне забезпечення інформаційної та кібернетичної безпеки. Освоєння методик аналізу, синтезу, оптимізації та прогнозування забезпечення інформаційної та кібернетичної безпеки.

Завдання курсу: придбання системи знань по застосуванню методик аналізу, синтезу, оптимізації та прогнозування забезпечення інформаційної та кібернетичної безпеки, розробці та супроводженні програмних комплексів і систем, методології використання систем комп'ютерної підтримки процесу розробки систем захисту.

Змістові модулі:

1. Методи інформаційно-аналітичного забезпечення інформаційної та кібернетичної безпеки.
2. Засоби інформаційно-аналітичного забезпечення інформаційної та кібернетичної безпеки.

ВДПП 2.2.8. (2). Фізичні основи захисту інформації

Мета вивчення курсу: надання студентам чітких уявлень про фізичні основи та принципи побудови систем захисту інформації у інформаційних мережах та системах; закласти термінологічний фундамент, навчити студентів правильно проводити аналіз погроз інформаційній безпеці, основним методам, принципам, алгоритмам захисту інформації в комп’ютерних системах з урахуванням сучасного стану та прогнозу розвитку методів, систем та засобів здійснення погроз зі сторони потенційних порушників.

Завдання курсу: ознайомлення студентів з основними методами обробки інформації, існуючими технологіями захисту інформації і практичними навичками з їх створення, впровадження і супроводження, формування певних знань та вмінь з теорії та практики захисту інформації.

Змістові модулі:

1. Комп'ютерні системи обробки інформації як об'єкт захисту.
2. Забезпечення конфіденційності інформації у комп'ютерних мережах та системах.
3. Захист систем зберігання інформації.
4. Системи захисту інформації у комп'ютерних мережах.

ВДПП 2.2.9. (1). Системи та технології кібербезпеки

Мета вивчення курсу: формування у студентів розуміння і визначення функцій та процесів щодо застосування інформаційних технологій для забезпечення кібернетичної безепеки; набуття знань з оцінки кіберризиків, ознайомлення зі стандартами кібернетичної безпеки підприємства.

Завдання курсу: надання студентам знань щодо захищеності активів від загроз конфіденційності, цілісності, доступності у кіберпросторі; надання розуміння застосування кіберзброї – шкідливого програмного забезпечення потенційних і фактичних атак на системи керування; набуття практичних навичок технології забезпечення кібербезпеки; набуття розуміння використання системи управління інформаційною безпекою.

Змістові модулі:

1. Поняття кібернетичної безпеки.
2. Кіберзагрози.
3. Методи захисту кіберзагроз.

ВДПП 2.2.9. (2). Кіберпростір та протидія злочинності

Мета вивчення курсу: формування у студентів розуміння і вивчення систем та технологій кібербезпеки та методики застосування їх для забезпечення протидії злочинності.

Завдання курсу: надання студентам знань щодо застосування систем та технологій кібернетичної безпеки для реалізації функцій по захисту активів від загроз конфіденційності, цілісності, доступності у кіберпросторі; надання розуміння застосування систем та технологій кіберзброї; набуття практичних навичок технологій застосування систем для забезпечення кібербезпеки; набуття розуміння використання системи та технологій управління кібернетичною безпекою задля протидії злочинності.

Змістові модулі:

1. Кіберпростір та методи протидії злочинності.
2. Особливості застосування систем та технологій кібернетичної безпеки.

ВДПП 2.2.10. (1). Національна безпека держави

Мета вивчення курсу: з позицій синергетичного, системного, управлінського підходів дати студентам теоретичні та практичні знання, які дозволять їм професійно орієнтуватися в різноманітних ситуаціях, пов'язаних із підготовкою та реалізацією управлінських рішень у різних сферах національної безпеки (інформаційній, політичній, економічній, соціальній, екологічній тощо).

Завдання курсу: дати студентам базові знання щодо концептуальних засад національної безпеки; ознайомити студентів із загальними проблемами формування системи управління національною безпекою; із основними нормативно-правовими актами, що регламентують суспільні відносини в сфері національної безпеки; стратегіями управління національною безпекою в зарубіжних країнах; дати студентам уявлення про найважливіші складові елементи національної безпеки в контексті глобалізації; навчити студентів практичних навичок щодо теоретичного дослідження складових національної безпеки та ефективності управління національною безпекою в них; дати студентам уявлення про

основні засади організації недержавної системи безпеки; навчити слухачів практичних навичок бенчмаркінгу безпеки.

Змістові модулі:

1. Поняття та зміст загальної теорії національної безпеки.
2. Право і національна безпека України.
3. Інформаційна, геополітична, екологічна та воєнна безпека України.
4. Управління національною безпекою в зарубіжних країнах безпека України
5. Недержавне управління національною безпекою України та бенчмаркінг національної безпеки України.

ВДПП 2.2.10. (2). Захищений документообіг

Мета вивчення курсу: формування у студентів розуміння і вивчення систем та технологій та методик захищеного документообігу та застосування їх для забезпечення захисту.

Завдання курсу: надання студентам розуміння застосування систем та технологій захищеного документообігу; набуття практичних навичок технологій застосування систем документообігу; набуття розуміння використання системи та технологій управління захищеним документообігом.

Змістові модулі:

1. Принципи захищеності документообігу.
2. Особливості застосування систем та технологій захищеного документообігу.