Міністерство освіти і науки України
Харківський національний університет імені В.Н. Каразіна

Введено в дію наказом від 31.08 2020 р.
№ 2202-7/80

Ректор _____ В.С.Бакіров

"___" _____ 20___ р.

Освітньо-професійна програма
(освітньо-професійна / освітньо-наукова)

Кібербезпека у фінансових технологіях
(назва програми)

Спеціальність 125 Кібербезпека
(шифр, назва спеціальності)

Спеціалізація _____
(назва спеціалізації)

перший (бакалаврський) рівень вищої освіти
(перший (бакалаврський), другий (магістерський), третій (освітньо-науковий)

Затверджено вченою радою університету "26" серпня 2020 року,
протокол №13

ЛИСТ ПОГОДЖЕННЯ

освітньо-професійної програми

Гарант освітньої програми _____ А.М.Кобилін

Кафедра інформаційних технологій та математичного моделювання:
протокол № 1 від « 26 » серпня 2020 р.

Завідувач кафедри інформаційних технологій
та математичного моделювання _____ Н.І.Стяглик

ПЕРЕДМОВА

Розроблено робочою групою у складі:

Прізвище, ім'я, по батькові	Найменування посади (для сумісників – місце основної роботи, посада)	Науковий ступінь, вчене звання, за якою кафедрою (спеціальністю) присвоєно
Керівник робочої групи		
Кобилін Анатолій Михайлович	Доцент кафедри інформаційних технологій та математичного моделювання	кандидат технічних наук, доцент кафедри застосування ЕОМ
Члени робочої групи		
Горбач Тетяна Вікторівна	Доцент кафедри інформаційних технологій та математичного моделювання	кандидат технічних наук
Соболєв Олександр Вікторович	Доцент кафедри інформаційних технологій та математичного моделювання	кандидат технічних наук

При розробці проекту Програми враховані вимоги:

1) Освітнього стандарту спеціальності 125 «Кібербезпека» галузі знань 12 «Інформаційні технології» за першим (бакалаврським) рівнем вищої освіти, затверджений і введений в дію наказом Міністерства освіти і науки України № 1074 від 04.10.2018 року;
2) Закон України № 1556-VII «Про вищу освіту» // Відомості Верховної Ради (ВВР), 2014, № 37-38;
3) Закон України від 05.09.2017 р. «Про освіту». [Електронний ресурс]. — [Режим доступу: http://zakon3.rada.gov.ua/laws/show/2145-19];
4) Національний Класифікатор професій ДК 003:2010 [Електронний ресурс]. Режим доступу: http://dovidnyk.in.ua/directories/profesii.
5) Національна рамка кваліфікацій. [Електронний ресурс]. – Режим доступу: http://zakon3.rada.gov.ua/laws/show/1341-2011-п.
6) Постанова Кабінету Міністрів України від 29.04.15 року № 266 «Про затвердження переліку галузей знань і спеціальностей, за якими здійснюється підготовка здобувачів вищої освіти». [Електронний ресурс]. – Режим доступу: http://zakon4.rada.gov.ua/laws/show/266-2015-%D0%BF

7) Методичні рекомендації щодо розроблення стандартів вищої освіти, затверджені Наказом Міністерства освіти і науки України від 01 червня 2016 р. № 600 (зі змінами) [Електронний ресурс]. – Режим доступу: https://mon.gov.ua/ua/osvita/visha-osvita/naukovo-metodichna-rada-ministerstva osviti-i-nauki-ukrayini/metodichni-rekomendaciyi-vo.

І. Загальна характеристика

Рівень вищої освіти	Перший (бакалаврський) рівень
Ступінь вищої освіти	Бакалавр
Галузь знань	12 Інформаційні технології
Спеціальність	125 Кібербезпека
Освітня кваліфікація	Бакалавр з кібербезпеки
Професійна кваліфікація (за наявності)	
Кваліфікація в дипломі	Ступінь вищої освіти – Бакалавр Спеціальність – 125 Кібербезпека Освітня програма – «Кібербезпека в фінансових технологіях»
Тип диплома	Диплом бакалавра державного зразка
Варіативна компонента	
Обсяг освітньої програми у ЄКТС	- на базі повної загальної середньої освіти – 240 кредитів ЄКТС, - на базі ступеня «молодший бакалавр» (освітньо-кваліфікаційного рівня «молодший спеціаліст»): 120 кредитів ЄКТС (вступ на 1 курс зі скороченим терміном навчання); 240 кредитів (за умови перезарахування не більше ніж 120 кредитів ЄКТС, отриманих в межах попередньої освітньої програми підготовки молодшого бакалавра (молодшого спеціаліста)).
Акредитація освітньої програми	-
Сертифікація освітньої програми (за наявності)	-
Мова(и) викладання	Українська, англійська
Термін дії освітньої програми	10 років
Вимоги до рівня освіти осіб, які можуть розпочати навчання за цією програмою	Особа має право здобувати ступінь бакалавра за умови наявності в неї повної загальної середньої освіти або ступеня «молодший бакалавр» (освітньо-кваліфікаційного рівня «молодший спеціаліст»)
Обмеження щодо форм навчання	Денна, заочна, дистанційна
Академічні права випускників	Мають право продовжити навчання на другому (магістерському) рівні вищої освіти. Набуття додаткових кваліфікацій в системі післядипломної освіти.
Інтернет-адреса постійного розміщення освітньої програми	http://kbi.karazin.ua

Зовнішні стейкхолдери, залучені до розробки освітньої програми:

представники бізнесу, роботодавці		
Посада	*ПІБ*	*Підпис*
Заступник директора з роздрібного бізнесу «Східний макро-регіон» ПАТ «Credit Agricole Bank»	Зачепа Р.В.	
Директор з економіки та фінансів ТОВ «Інра-Софт»	Чхеайло А.А.	
Начальник управління безпеки Харківського Головного регіонального управління ПАТ КБ «ПриватБанк»	Столбов В.Ф.	
директор малого приватного підприємства «Прінт»	Наугольний О.В.	
Професійні громадські організації		
Посада	*ПІБ*	*Підпис*
президент Харківського банківського союзу	Жукова О. М.	
Інші стейкхолдери		
Посада	*ПІБ*	*Підпис*
К.т.н, доцент кафедри інформаційних технологій та математики Українська інженерно-педагогічна академія	Трохимчук С.М.	
д.ф.-м.н., професор, професор кафедри інформаційних технологій проектування Національний аерокосмічний університет ім. М. Є. Жуковського "Харківський авіаційний інститут"	Яковлев С. В.	

ІІ. Профіль освітньої програми

Заклад вищої освіти та код ЄДЕБО	Харківський національний університет імені В.Н.Каразіна навчально-науковий інститут «Каразінський банківський інститут», код ЄДЕБО 62
Тип диплома	Диплом бакалавра державного зразка
Обсяг освітньої програми у ЄКТС	- на базі повної загальної середньої освіти - 240 кредитів ЄКТС; - на базі ступеня «молодший бакалавр» (освітньо-кваліфікаційного рівня «молодший спеціаліст»): 120 кредитів ЄКТС (вступ на 1 курс зі скороченим терміном навчання); 240 кредитів (за умови перезарахування не більше ніж 120 кредитів ЄКТС, отриманих в межах попередньої освітньої програми підготовки молодшого бакалавра (молодшого спеціаліста)).
Рівень вищої освіти	Перший (бакалаврський) рівень
Рівень кваліфікації (за НРК)	6 рівень Національної рамки кваліфікацій та перший цикл вищої освіти Рамки кваліфікацій Європейсъкого простору вищої освіти
Акредитуюча інституція	
Період акредитації	2020-2025 рр.

А	**Цілі освітньої програми**	
	Підготовка фахівців, здатних використовувати і впроваджувати технології інформаційної та/або кібербезпеки для фінансових технологій	
В	**Опис предметної області**	
1.	*Об’єкт вивчення*	– об'єкти інформатизації, включаючи комп'ютерні, автоматизовані, телекомунікаційні, інформаційні, інформаційно-аналітичні, інформаційно-телекомунікаційні системи, інформаційні ресурси і технології; – технології забезпечення безпеки інформації; – процеси управління інформаційною та/або кібербезпекою об’єктів, що підлягають захисту
2.	*Цілі навчання*	підготовка фахівців, здатних використовувати і впроваджувати технології інформаційної та/або кібербезпеки
3.	*Теоретичний зміст предметної*	Знання – законодавчої, нормативно-правової бази

	області	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.
4.	*Методи, методики та технології*	Методи, методики, інформаційно-комунікаційні технології та інші технології забезпечення інформаційної та/ або кібербезпеки
5.	*Орієнтація програми*	Програма ґрунтується на знаннях та навичках в галузях інформаційно-комунікаційних технологій, інформаційній безпеки, кібербезпеки та фінансових технологіях, але не обмежується ними. Знання забезпечуються за рахунок дисциплін загальної підготовки («soft skills»), галузевої та фахової підготовки («hard skills»)
6.	*Особливості програми*	Програма формує фундаментальні знання та фахові навички застосуванні інформаційних технологій, фінансових технологій, експлуатації інформаційних систем (сервісів), забезпечення їх кібербезпеки. Передбачає можливості короткострокових академічних стажувань за кордоном.
С	**Працевлаштування та продовження освіти**	
1	*Працевлаштування випускників*	Фахівець з організації захисту інформації, технік із конфігурування та налагодження комп’ютерної системи, технік з обслуговування інженерно-технічних засобів охорони, технік (сфера захисту

		інформації), технік із системного адміністрування (системний адміністратор, мережевій адміністратор, адміністратор інформаційних систем), фахівець з інформаційних технологій, фахівець із організації інформаційної безпеки, прикладний програміст, системний програміст, веб-програміст, інженер з експлуатації засобів захисту інформації, адміністратор баз даних; спеціаліст з проектування та впровадження систем захисту інформації, спеціаліст з проектування та інформаційного захисту комп'ютерних мереж. Можуть працювати на національному та міжнародному рівнях	
2	*Академічні права випускників*	Можливість продовжити навчання за освітньою програмою ступеня магістра. Набуття додаткових кваліфікацій в системі післядипломної освіти	
D	**Стиль та методика навчання**		
1	*Підходи до викладання та навчання*	Технології навчання: інтерактивні, дискусійні лекції з використанням мультимедійного обладнання, семінари, практичні заняття, лабораторні роботи, командна робота, самостійна робота, бізнес кейси, тренінги, дискусії, індивідуальні заняття, дебати, практична підготовка, хакатони, консультації із викладачами, вебінари, E-Learning, підготовки курсових робіт, бакалаврський семінар	
2	*Порядок оцінювання*	Оцінювання здійснюється за ECTS-рейтингом, 100 бальною та національною шкалами. Форми контролю визначаються за кожною компонентою освітньої програми. Підсумковий контроль – екзамен або залік. Поточний контроль: тестування, бліц-опитування, контрольна робота, Case study, захист результатів виконання групових або індивідуальних аналітично-розрахункових робіт, презентація, дискурс, тренінг-PBL (Problem-Based Learning), есе, колоквіум тощо	
E	**Програмні компетентності випускника**		
	Група	*шифр*	*Зміст*
1	*Інтегральна компетентність*	ІК	здатність розв'язувати складні спеціалізовані задачі та практичні проблеми у галузі забезпечення інформаційної безпеки і\або

			кібербезпеки, що характеризується комплексністю та неповною визначеністю умов
2	*Загальні компетентності*		
2.1 2.2	*Загальні нормативні 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
	Загальні додаткові (фахові) компетентності		
3	*Спеціальні (фахові, предметні) компетентності*		
3.1	*Спеціальні нормативні компетентності*	КФ 1	здатність застосовувати законодавчу та нормативно-правову базу, а також державні та міжнародні вимоги, практики і стандарти з метою здійснення професійної діяльності в галузі інформаційної 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
3.2	*Спеціальні додаткові (фахові) компетентності*	КФД 1	здатність до проектування, розробки та використання програмних додатків у фінансових технологіях з необхідним рівнем кібербезпеки
		КФД 2	здатність до оцінювання рівня кібербезпеки у фінансових технологіях, системах та сервісах
		КФД 3	вміння знаходити вразливості в фінансових технологіях, системах та сервісах
		КФД 4	здатність організовувати процес оцінки та забезпечення належного рівня кібербезпеки фінансових технологіях, системах та сервісах
F	**Програмні результати навчання**		
	шифр	*Зміст*	
	РН1	- застосовувати знання державної та іноземних мов з метою забезпечення ефективності професійної комунікації;	
	РН2	- організовувати 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;
	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-комунікаційних технологій;
	РН16	- реалізовувати комплексні системи захисту інформації в автоматизованих системах (АС) 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 інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах;
	РН22	- вирішувати задачі управління процедурами ідентифікації, автентифікації, авторизації процесів і користувачів в інформаційно-телекомунікаційних системах згідно встановленої політики інформаційної і\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 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 неперервність процесу ведення журналів реєстрації подій та 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 людини і громадянина в Україні.
G	**Ресурсне забезпечення реалізації програми**	
1	*Кадрове забезпечення*	Група забезпечення спеціальності складається з науково-педагогічних працівників, які мають кваліфікацію відповідно до спеціальності «Кібербезпека», працюють в Університеті за основним місцем роботи, мають стаж науково-педагогічної діяльності понад два роки, рівень наукової та професійної активності, який засвідчується виконанням не менше чотирьох видів та результатів (самоаналіз), міжнародне визнання. Частка тих, хто має науковий ступінь та/або вчене

		звання становить не менше 60 відсотків. Відповідає кадровим вимогам щодо забезпечення провадження освітньої діяльності у сфері вищої освіти згідно з діючим законодавством України (Постанова кабінету міністрів України «Про затвердження Ліцензійних умов провадження освітньої діяльності закладів освіти» від 30 грудня 2015 р. № 1187).
2	*Інструменти та обладнання*	Сучасне інформаційно-комунікаційне обладнання, інформаційні системи та програмні продукти, що застосовують при розробці, впроваджені, експлуатації та забезпеченні кібербезпеки інформаційних систем та технологій.
3	*Інформаційне забезпечення*	Підручники, навчальні посібники, довідкова та інша навчальна література за спеціальністю «Кібербезпека» у бібліотеках інституту та Університету (у тому числі в електронному вигляді). Вітчизняні та закордонні фахові періодичні видання у бібліотеках за спеціальністю «Кібербезпека». Доступ до баз даних періодичних наукових видань англійською мовою. Навчально-методичне забезпечення в системі Moodle. Інформаційні ресурси в Інтернет, на офіційному веб-сайті Університету та доступ студентів до навчальних ресурсів через внутрішню мережу Інституту. Сертифіковані курси Академії «Cisco» та Microsoft.
4	*Навчально-методичне забезпечення*	Включає наступні обов’язкові складові: навчальний план, за яким здійснюється підготовка здобувачів вищої освіти; навчально-методичне забезпечення навчальних дисциплін (включає обов’язково – робочі програми навчальних дисциплін та екзаменаційні білети (у разі, якщо екзамен передбачено навчальним планом); програми з усіх видів практичної підготовки; методичні матеріали для проведення підсумкової атестації здобувачів вищої освіти; контрольні завдання для оцінювання рівня знань студентів при проведенні акредитації освітньої програми
Н	**Академічна мобільність**	

1	*Національна кредитна мобільність*	Між інститутами Університету (Київ, Львів, Харків, Черкаси). З вітчизняними закладами вищої освіти на основі двосторонніх договорів.
2	*Міжнародна кредитна мобільність*	Організація кредитної мобільності (окрім 1-го курсу) бакалаврів. Проект **«Еразмус+»**
3	*Навчання іноземних здобувачів вищої освіти*	Можливе, на основі договорів між ДВНЗ «Університет банківської справи» та зарубіжними університетами, а також на основі розробки програм подвійних дипломів ДВНЗ «Університет банківської справи» та зарубіжних університетів-партнерів.

ІІІ. Структура та компоненти освітньої програми

В основу розроблення освітньої програми покладено компетентнісний підхід з використанням ЄКТС, де для досягнення запланованих результатів навчання за освітньою програмою (навчальною дисципліною, модулем) передбачаються певні витрати часу студентом, тобто необхідний і достатній обсяг навчального навантаження студента, виражений у кількості кредитів ЄКТС (1 кредит ЄКТС дорівнює 30 годинам). 1 семестр - 30 кредитів ЄКТС, навчальний (академічний) рік – 60 кредитів ЄКТС.

Освітня програма передбачає виділення дисциплін двох видів: обов'язкових дисциплін та дисципліни за вільним вибором студента, які розподілені за блоками підготовки (загальна, галузева, фахова/предметна) відповідно до профілю освітньої програми.

До блоку *загальної підготовки* відносяться навчальні дисципліни, що спрямовані на формування загальних компетентностей у здобувача вищої освіти, зокрема, емоційного інтелекту, світогляду, організаційних та комунікаційних навичок.

До блоку *галузевої підготовки* відносяться навчальні дисципліни, що спрямовані на формування спеціальних фахових компетентностей за галуззю знань у здобувача вищої освіти, зокрема, ключові для всіх спеціальностей конкретної галузі знань та підтримуючого характеру.

До блоку *фахової/предметної підготовки* відносяться навчальні дисципліни, що спрямовані на формування спеціальних фахових компетентностей за спеціальністю у здобувача вищої освіти, зокрема, предметної області та професійного спрямування.

Навчальне навантаження студента включає всі види його роботи (самостійну, аудиторну, лабораторну, дослідницьку тощо) відповідно до навчального плану. В таблиці 3 представлений розподіл змісту освітньої програми та обсягу кредитів ЄКТС.

Таблиця 3

Загальний розподіл змісту освітньої програми та обсягу кредитів ЄКТС за компонентами

Блоки підготовки		Академічні години/кредити ЄКТС		
		Обов'язкові дисципліни	Вибіркові дисципліни	Всього
	- загальна підготовка (1)	1080/36	180/6	1260/42
	- галузева підготовка (2)	1800/60	180/6	1980/66
	- фахова предметна підготовка (3)	1800/60	1440/48	3240/108
	- практична підготовка (4)			720/24
Загальний обсяг		4680/156	1800/60	7200/240

Розподіл кредитів за навчальними дисциплінами, структурно-логічна послідовність їх вивчення, форми підсумкового контролю наведено в таблиці 4.

Таблиця 4

Розподіл змісту освітньої програми та обсягу кредитів ЄКТС за компонентами освітньої програми

Компоненти освітньої програми (навчальні дисципліни, практики, кваліфікаційна робота тощо)		***кредити ЄКТС***	***форма підсумкового контролю***	***семестр***
Код*	***Назва***			
Блок «Загальна підготовка» (1)				
Обов'язкові компоненти				
ЗОД1	УБС студія «Тайм-менеджмент та міжособистісні комунікації в бізнесі»	6	залік	1
ЗОД2	Інформаційні технології (рівень А)	6	екзамен	1
ЗОД3	Професійна іноземна мова та міжнародні бізнес-комунікації	12	залік, екзамен	1, 2
ЗОД4	УБС студія «Банківська система» (рівень А)	6	залік	3
ЗОД5	УБС студія «Лідерство та командна робота»	6	залік	5
Загальний обсяг обов'язкових компонент за блоком 1		**36**		
Вибіркові компоненти				
ЗВД1	Вибіркова дисципліна блоку «Загальна	6	залік	2

	підготовка»			
Загальний обсяг вибіркових компонент за блоком 1		**6**		
Блок «Галузева підготовка» (2)				
Обов'язкові компоненти				
ГОД1	Математика (Рівень А - Вища математика)	6	екзамен	1
ГОД2	Програмування (Рівень А - Алгоритми та структури даних)	6	екзамен	2
ГОД3	Математика (Рівень С - Статистика (у т.ч. й Теорія ймовірностей)	6	екзамен	2
ГОД4	Інформаційні технології (Рівень F - Технологія створення програмних продуктів)	6	екзамен	6
ГОД5	Математика (Рівень В - Дискретна математика)	6	екзамен	1
ГОД6	Комп'ютерні системи та мережі (Рівень В - Комп'ютерна схемотехніка та архітектура комп'ютерів)	6	екзамен	3
ГОД7	Комп'ютерні системи та мережі (Рівень А - Фізика та електротехніка)	6	залік	3
ГОД8	Комп'ютерні системи та мережі (Рівень С - Комп'ютерні системи та мережі)	6	екзамен	4
ГОД9	Інформаційні технології (Рівень А - Операційні системи)	6	екзамен	4
ГОД10	Фінансові технології (Рівень В - Цифрова економіка)	6	залік	5
Загальний обсяг обов'язкових компонент за блоком 2		**60**		
Вибіркові компоненти				
ГВД1	Вибіркова дисципліна блоку «Галузева підготовка»	6	залік	4
Загальний обсяг вибіркових компонент за блоком 2		**6**		
Блок «Фахова/предметна підготовка» (3)				
Обов'язкові компоненти				
ФОД1	Кібербезпека (Рівень D - Комплексні системи захисту інформації)	6	екзамен	8
ФОД2	Кібербезпека (Рівень А - Основи кібербезпеки)	6	залік	2
ФОД3	Кібербезпека (Рівень С - Система стандартів інформаційної безпеки)	6	залік	6
ФОД4	Кібербезпека (Рівень Е - Проектування інформаційних систем безпеки)	6	екзамен	7
ФОД5	Моделювання (Рівень D - Моделювання бізнес-процесів безпеки)	6	екзамен	7
ФОД6	Математика (Рівень D - Методи та системи штучного інтелекту)	6	екзамен	7

ФОД7	Комп’ютерні системи та мережі (Рівень D - Безпека комп'ютерних мереж)	6	екзамен	5
ФОД8	Інформаційні технології (Рівень E - Великі дані)	6	екзамен	6
ФОД9	Кібербезпека (Рівень B - Функціональна безпека комп'ютерних систем)	6	екзамен	6
ФОД10	Програмування (Рівень B - Об′єктно-орієнтовне програмування)	6	екзамен	3
Загальний обсяг обов’язкових компонент за блоком 3		**60**		
Вибіркові компоненти				
ФВД1.1	Моделювання (Рівень A - Економіко-математичні методи та моделі)	6	залік	3
ФВД1.2	Моделювання (Рівень B - Теорія ризиків)	6	залік	3
ФВД2.1	Кібербезпека (Рівень F - Основи протидії кіберзлочинності та цифрова криміналістика)	6	залік	7
ФВД2.2	Фінансові технології (Рівень D - Платіжні системи, технології та сервіси)	6	залік	7
ФВД3.1	Інформаційні технології (Рівень B - Комп'ютерна графіка та веб-дизайн)	6	екзамен	4
ФВД3.2	Фінансові технології (Рівень A - Технології дистанційного банківського обслуговування)	6	екзамен	4
ФВД4.1	Кібербезпека (Рівень G - Організація та проведення тестування на проникнення та соціальна інженерія)	6	екзамен	8
ФВД4.2	Комп’ютерні системи та мережі (Рівень E - Адміністрування та моніторинг комп’ютерних систем)	6	екзамен	8
ФВД5.1	Кібербезпека (Рівень H - Правові основи інформаційної безпеки)	6	залік	8
ФВД5.2	Кібербезпека (Рівень I - Інформаційна безпека держави)	6	залік	8
ФВД6.1	Інформаційні технології (Рівень D - Технології проектування та оцінювання людино-машинних інтерфейсів)	6	залік	5
ФВД6.2	Моделювання (Рівень C - Теорія прийняття рішень)	6	залік	5
ФВД7.1	Програмування (Рівень D - Високорівневе програмування (веб-програмування))	6	екзамен	5
ФВД7.2	Фінансові технології (Рівень C - Безпека фінансових ринків)	6	екзамен	5
ФВД8.1	Інформаційні технології (Рівень C - Організація баз даних та знань)	6	залік	4

ФВД8.2	Програмування (Рівень С – Крос-платформне програмування)	6	залік	4
Загальний обсяг вибіркових компонент за блоком 3		**48**		
Блок «Практична підготовка» (4)				
ПП1	Навчальна практика - Проектно-технологічна практика	6	залік	6
ПП2	Виробнича практика	6	залік	8
ПП3	Бакалаврський тренінг (семінар)	6	залік	7
ПП4	Кваліфікаційна бакалаврська робота	6		8
Загальний обсяг вибіркових компонент за блоком 4		**24**		
ЗАГАЛЬНИЙ ОБСЯГ ОСВІТНЬОЇ ПРОГРАМИ		**240**		

* Кодування навчальних дисциплін відбудеться в наступному порядку:

ЗОД – навчальна дисципліна блоку «Загальна підготовка», що є обов'язковою для вивчення;

ЗВД – навчальна дисципліна блоку «Загальна підготовка», що обирається за вибором студента з групи навчальних дисциплін для формування власної спеціалізації ;

ГОД – навчальна дисципліна блоку «Галузева підготовка», що є обов'язковою для вивчення;

ГВД – навчальна дисципліна блоку «Галузева підготовка», що обирається за вибором студента з групи навчальних дисциплін для формування власної спеціалізації ;

ФОД – навчальна дисципліна блоку «Фахова/предметна підготовка», що є обов'язковою для вивчення;

ФВД – навчальна дисципліна блоку «Фахова/предметна підготовка», що обирається за вибором студента з групи навчальних дисциплін для формування власної спеціалізації .

Матрицю відповідності визначених Стандартом вищої освіти України: першій (бакалаврський) рівень, галузь знань 12 – Інформаційні технології, спеціальність 125 – Кібербезпека, затвердженим Наказом Міністерства освіти і науки України 04.10.2018 р. (далі – Стандарт) компетентностей дескрипторам НРК наведено в таблиці 5.

Матрицю співвідношення результатів навчання та компетентностей наведено в таблиці 6.

Матрицю співвідношення навчальних дисциплін та результатів навчання наведено в таблиці 7.

VI - Форми атестації здобувачів вищої освіти

Атестація здійснюється у формі:	Атестація здійснюється у формі публічного захисту кваліфікаційної бакалаврський роботи та за рішенням закладу вищої освіти кваліфікаційного екзамену. На атестацію виноситься сукупність знань, умінь,

	навичок, інших компетентностей, набутих особою у процесі навчання за Стандартом. До атестації допускаються студенти, які виконали всі вимоги програми підготовки.
Вимоги до кваліфікаційної роботи (за наявності)	Кваліфікаційний проект/робота має передбачати розв'язання спеціалізованої задачі в галузі інформаційної та/або кібербезпеки. У кваліфікаційній бакалаврській роботі не може бути академічного плагіату, фальсифікації та списування. Кваліфікаційна бакалаврська робота оприлюднюється на офіційному сайті Інституту або Університету. Загальні вимоги до кваліфікаційної бакалаврської роботи визначені розділом 5 Положення про навчально-методичне забезпечення освітньої програми. Додаткові вимоги можуть визначати Інститут, випускова кафедра (група забезпечення спеціальності).

Таблиця 5

Матриця відповідності визначених Стандартом компетентностей дескрипторам НРК (за ___ рівнем, _____)

Класифікація компетентностей за НРК	**Знання**	**Уміння**	**Комунікація**	**Автономія та відповідальність**
Загальні компетентності				
Спеціальні (фахові) компетентності				

Таблиця не передбачена Стандартом

Таблиця 6

Матриця відповідності визначених результатів навчання та компетентностей

Програмні результати навчання	компетентність	Загальні компетентності							Спеціальні (фахові) компетентності															
		Загальні нормативні компетентності (КЗ)							Спеціальні (фахові) нормативні компетентності (КФ)												Спеціальні (фахові) додаткові компетентності (КФД)			
	ІК	КЗ 1	КЗ 2	КЗ 3	КЗ 4	КЗ 5	КЗ 6	КЗ 7	КФ 1	КФ 2	КФ 3	КФ 4	КФ 5	КФ 6	КФ 7	КФ 8	КФ 9	КФ 10	КФ 11	КФ 12	КФД 1	КФД 2	КФДЗ	КФД4
РН1				+																				
РН2	+		+																					+
РН3						+																		
РН4		+	+		+	+																		
РН5												+												
РН6	+		+					+																
РН7							+		+															
РН8		+							+															
РН9		+							+															
РН10		+																						
РН11		+																						
РН12		+								+										+				
РН13	+	+			+	+				+										+				
РН14	+	+								+	+													+
РН15										+														
РН16			+		+						+				+									
РН17		+								+														

	ІК	КЗ 1	КЗ 2	КЗ 3	КЗ 4	КЗ 5	КЗ 6	КЗ 7	КФ 1	КФ 2	КФ 3	КФ 4	КФ 5	КФ 6	КФ 7	КФ 8	КФ 9	КФ 10	КФ 11	КФ 12	КФД 1	КФД 2	КФДЗ	КФД4
РН18		+									+												+	+
РН19										+											+			
РН20											+													
РН21	+	+			+								+											+
РН22	+	+			+					+			+									+		+
РН23		+																						
РН24	+	+																						
РН25															+									
РН26		+															+					+		+
РН27	+	+			+					+											+	+		+
РН28					+	+							+											+
РН29		+			+															+				+
РН30					+																			
РН31										+														
РН32	+	+			+								+	+										
РН33		+										+												
РН34		+																						
РН35	+	+	+												+									
РН36		+			+																			
РН37		+																		+				
РН38		+																		+				
РН39		+																						
РН40		+			+													+		+				
РН41																+								
РН42		+			+											+	+					+		+

	ІК	КЗ 1	КЗ 2	КЗ 3	КЗ 4	КЗ 5	КЗ 6	КЗ 7	КФ 1	КФ 2	КФ 3	КФ 4	КФ 5	КФ 6	КФ 7	КФ 8	КФ 9	КФ 10	КФ 11	КФ 12	КФД 1	КФД 2	КФДЗ	КФД4
РН43			+			+			+															
РН44	+	+										+												
РН45													+											
РН46		+			+					+														
РН47	+	+	+							+	+							+			+			
РН48		+															+							
РН49		+																	+					
РН50											+													
РН51											+													
РН52		+			+														+					
РН53		+			+	+															+	+	+	+
РН54							+	+																

Таблиця 7

Матриця відповідності програмних компетентностей компонентам освітньо-професійної програми

Компоненти освітньої програми	Програмні компетентності випускника																						
	КЗ1	КЗ2	КЗ3	КЗ4	КЗ5	КЗ6	КЗ7	КФ1	КФ2	КФ3	КФ4	КФ5	КФ6	КФ7	КФ8	КФ9	КФ10	КФ11	КФ12	КФД1	КФД2	КФД3	КФД4
ЗОД1		+		+	+		+																+
ЗОД2	+			+	+				+										+				
ЗОД3			+																				
ЗОД4		+				+		+															+
ЗОД5		+					+				+												+
ЗВД1						+	+																
ГОД1	+	+		+	+		+		+														
ГОД2	+	+		+	+	+		+	+	+	+	+		+					+		+		+
ГОД3	+	+		+	+				+			+			+				+				+
ГОД4	+	+		+		+		+	+		+	+		+					+	+			+
ГОД5	+	+		+	+		+																
ГОД6	+	+	+	+	+				+		+								+				+
ГОД7	+			+				+	+														
ГОД8	+			+	+			+	+	+	+	+	+		+	+	+		+	+	+	+	+
ГОД9	+	+		+					+	+	+	+				+	+			+	+	+	+
ГОД10	+	+							+														+
ГВД1	+	+		+	+			+	+	+		+		+					+		+		+
ФОД1	+	+		+					+	+		+	+	+		+	+		+	+	+		+
ФОД2	+	+		+		+		+	+			+		+					+	+	+		+
ФОД3	+	+		+	+	+		+		+	+			+			+		+				
ФОД4	+	+		+	+				+	+	+	+	+	+	+		+	+	+		+		+
ФОД5	+	+	+	+	+	+	+	+	+		+	+		+	+		+	+	+		+		+
ФОД6	+			+	+				+								+		+				
ФОД7	+	+		+					+	+	+	+	+				+			+	+		+
ФОД8					+							+											
ФОД9	+									+	+												
ФОД10	+	+	+	+			+		+	+		+					+		+	+			+
ФВД1.1	+	+		+	+				+	+	+								+				+
ФВД1.2	+			+					+		+	+											
ФВД2.1	+			+					+	+					+	+			+		+	+	+
ФВД2.2		+			+			+															+
ФВД3.1	+		+	+				+						+		+		+			+		+
ФВД3.2	+								+														

	КЗ1	КЗ2	КЗ3	КЗ4	КЗ5	КЗ6	КЗ7	КФ1	КФ2	КФ3	КФ4	КФ5	КФ6	КФ7	КФ8	КФ9	КФ10	КФ11	КФ12	КФД1	КФД2	КФД3	КФД4
ФВД4.1	+		+	+					+	+									+				+
ФВД4.2	+			+	+				+	+	+	+	+					+	+	+	+	+	+
ФВД5.1	+	+		+	+			+		+				+					+				
ФВД5.2	+					+		+															
ФВД6.1	+	+	+	+	+	+	+	+	+		+								+				+
ФВД6.2	+	+		+		+		+	+	+		+		+		+			+	+	+	+	+
ФВД7.1	+	+	+	+			+		+	+		+					+		+	+			+
ФВД7.2	+	+							+												+		
ФВД8.1	+	+		+	+				+			+	+	+				+	+	+	+		+
ФВД8.2	+	+		+	+	+		+	+	+		+	+	+					+	+	+		+

Таблиця 8

Матриця співвідношення навчальних дисциплін та результатів навчання

	Навчальна дисципліна	РН 1	РН 2	РН 3	РН 4	РН 5	РН 6	РН 7	РН 8	РН 9	РН 10	РН 11	РН 12	РН 13	РН 14	РН 15	РН 16	РН 17	РН 18	РН 19	РН 20	РН 21	РН 22	РН 23	РН 24	РН 25	РН 26	РН 27
ЗОД1	УБС студія «Тайм-менеджмент та міжособистісні комунікації в бізнесі»		+	+		+	+																					
ЗОД2	Інформаційні технології (рівень А)											+		+														
ЗОД3	Професійна іноземна мова та міжнародні бізнес-комунікації	+																										
ЗОД4	УБС студія «Банківська система» (рівень А)		+															+										
ЗОД5	УБС студія «Лідерство та командна робота»		+			+	+																					
ЗВД1	Вибіркова дисципліна блоку «Загальна підготовка»																											
ГОД1	Математика (Рівень А - Вища математика)			+	+		+																					
ГОД2	Програмування (Рівень А - Алгоритми та структури даних)							+	+		+			+			+						+					
ГОД3	Математика (Рівень С - Статистика (у т.ч. теорія ймовірності))		+	+									+															
ГОД4	Інформаційні технології (Рівень F - Технологія створення програмних продуктів)							+												+		+						
ГОД5	Математика (Рівень В - Дискретна математика)			+	+		+				+																	
ГОД6	Комп'ютерні системи та мережі (Рівень В - Комп'ютерна схемотехніка та архітектура комп'ютерів)	+	+								+																	
ГОД7	Комп'ютерні системи та мережі (Рівень А - Фізика та електротехніка)								+							+									+			
ГОД8	Комп'ютерні системи та мережі (Рівень С - Комп'ютерні системи та мережі)										+	+		+		+		+	+	+				+	+		+	+
ГОД9	Інформаційні технології (Рівень А - Операційні системи)											+							+			+	+	+	+		+	+
ГОД10	Фінансові технології (Рівень В - Цифрова економіка)		+															+										
ГВД1	Вибіркова дисципліна блоку «Галузева підготовка» - Чисельні методи та системний аналіз			+					+		+		+				+						+		+		
ФОД1	Кібербезпека (Рівень D - Комплексні системи захисту інформації)														+		+										+	+
ФОД2	Кібербезпека (Рівень А - Основи кібербезпеки)							+	+			+										+	+					+
ФОД3	Кібербезпека (Рівень С - Система стандартів інформаційної безпеки)							+	+	+							+											
ФОД4	Кібербезпека (Рівень Е - Проектування інформаційних систем безпеки)				+	+					+			+		+			+				+				

		РН 1	РН 2	РН 3	РН 4	РН 5	РН 6	РН 7	РН 8	РН 9	РН 10	РН 11	РН 12	РН 13	РН 14	РН 15	РН 16	РН 17	РН 18	РН 19	РН 20	РН 21	РН 22	РН 23	РН 24	РН 25	РН 26	РН 27
ФОД5	Моделювання (Рівень D - Моделювання бізнес-процесів безпеки)		+		+ +						+	+										+	+					
ФОД6	Математика (Рівень D - Методи та системи штучного інтелекту)			+									+															
ФОД7	Комп’ютерні системи та мережі (Рівень D - Безпека комп'ютерних мереж)																							+			+	+
ФОД8	Інформаційні технології (Рівень E - Великі дані)			+																								
ФОД9	Кібербезпека (Рівень B - Функціональна безпека комп'ютерних систем)																				+							
ФОД10	Програмування (Рівень B - Об′єктно-орієнтовне програмування)	+					+					+								+		+						
ФВД1.1	Моделювання (Рівень A - Економіко-математичні методи і моделі)		+	+	+	+							+		+										+			
ФВД1.2	Моделювання (Рівень B - Теорія ризиків)																											
ФВД2.1	Кібербезпека (Рівень F - Основи протидії кіберзлочинності та цифрова криміналістика)														+				+									
ФВД2.2	Фінансові технології (Рівень D - Платіжні системи, технології та сервіси)		+															+										
ФВД3.1	Інформаційні технології (Рівень B - Комп'ютерна графіка та веб-дизайн)	+								+															+	+	+	
ФВД3.2	Фінансові технології (Рівень A - Технології дистанційного банківського обслуговування)																	+						+				
ФВД4.1	Кібербезпека (Рівень G - Організація та проведення тестування на проникнення та соціальна інженерія)														+						+							
ФВД4.2	Комп’ютерні системи та мережі (Рівень E - Адміністрування та моніторинг комп’ютерних систем)															+			+				+			+		
ФВД5.1	Кібербезпека (Рівень H - Правові основи інформаційної безпеки)								+	+							+											
ФВД5.2	Кібербезпека (Рівень I - Інформаційна безпека держави)							+		+																		
ФВД6.1	Інформаційні технології (Рівень D - Технології проектування та оцінювання людино - машинних інтерфейсів)	+	+	+	+	+	+	+				+		+		+												
ФВД6.2	Моделювання (Рівень C - Теорія прийняття рішень)							+	+	+		+							+	+		+	+			+	+	+
ФВД7.1	Програмування (Рівень D - Високорівневе програмування (веб-програмування))	+					+					+								+		+						
ФВД7.2	Банківські технології (Рівень C - Безпека фінансових ринків)		+															+										
ФВД8.1	Інформаційні технології (Рівень C - Організація баз даних та знань)				+								+		+					+			+		+	+		+
ФВД8.2	Програмування (Рівень C – Крос-платформне програмування)							+	+					+			+						+					+

Продовження таблиці 8

Матриця співвідношення навчальних дисциплін та результатів навчання

Навчальна дисципліна		РН 28	РН 29	РН 30	РН 31	РН 32	РН 33	РН 34	РН 35	РН 36	РН 37	РН 38	РН 39	РН 40	РН 41	РН 42	РН 43	РН 44	РН 45	РН 46	РН 47	РН 48	РН 49	РН 50	РН 51	РН 52	РН 53	РН 54
ЗОД1	УБС студія «Тайм-менеджмент та міжособистісні комунікації в бізнесі»																											
ЗОД2	Інформаційні технології (рівень А)																											
ЗОД3	Професійна іноземна мова та міжнародні бізнес-комунікації																											
ЗОД4	УБС студія «Банківська система» (рівень А)																											
ЗОД5	УБС студія «Лідерство та командна робота»																											
ЗВД1	Вибіркова дисципліна блоку «Загальна підготовка»																											+
ГОД1	Математика (Рівень А - Вища математика)																			+								
ГОД2	Програмування (Рівень А - Алгоритми та структури даних)						+																					
ГОД3	Математика (Рівень С - Статистика (у т.ч. й Теорія ймовірностей)	+													+													
ГОД4	Інформаційні технології (Рівень F - Технологія створення програмних продуктів)		+				+		+	+																		
ГОД5	Математика (Рівень В - Дискретна математика)																											
ГОД6	Комп'ютерні системи та мережі (Рівень В - Комп'ютерна схемотехніка та архітектура комп'ютерів)																											
ГОД7	Комп'ютерні системи та мережі (Рівень А - Фізика та електротехніка)									+																		
ГОД8	Комп'ютерні системи та мережі (Рівень С - Комп'ютерні системи та мережі)			+	+	+					+	+				+		+		+	+	+		+				
ГОД9	Інформаційні технології (Рівень А - Операційні системи)						+														+							
ГОД10	Фінансові технології (Рівень В - Цифрова економіка)																											
ГВД1	Вибіркова дисципліна блоку «Галузева підготовка» Чисельні методи та системний аналіз																											
ФОД1	Кібербезпека (Рівень D - Комплексні системи захисту інформації)					+		+	+			+		+				+		+								
ФОД2	Кібербезпека (Рівень А - Основи кібербезпеки)								+			+																
ФОД3	Кібербезпека (Рівень С - Система стандартів інформаційної безпеки)										+		+	+			+	+										
ФОД4	Кібербезпека (Рівень Е - Проектування інформаційних систем безпеки)							+															+					

		РН 28	РН 29	РН 30	РН 31	РН 32	РН 33	РН 34	РН 35	РН 36	РН 37	РН 38	РН 39	РН 40	РН 41	РН 42	РН 43	РН 44	РН 45	РН 46	РН 47	РН 48	РН 49	РН 50	РН 51	РН 52	РН 53	РН 54
ФОД5	Моделювання (Рівень D - Моделювання бізнес-процесів безпеки)						+																+					
ФОД6	Математика (Рівень D - Методи та системи штучного інтелекту)													+						+								
ФОД7	Комп’ютерні системи та мережі (Рівень D - Безпека комп'ютерних мереж)		+																		+							
ФОД8	Інформаційні технології (Рівень E - Великі дані)																		+									
ФОД9	Кібербезпека (Рівень B - Функціональна безпека комп'ютерних систем)																	+										
ФОД10	Програмування (Рівень B - Об′єктно-орієнтовне програмування)													+										+				
ФВД1.1	Моделювання (Рівень A - Економіко-математичні методи та моделі)						+													+								
ФВД1.2	Моделювання (Рівень B - Теорія ризиків)				+		+												+	+								
ФВД2.1	Кібербезпека (Рівень F - Основи протидії кіберзлочинності та цифрова криміналістика)		+										+			+												
ФВД2.2	Фінансові технології (Рівень D - Платіжні системи, технології та сервіси)																											
ФВД3.1	Інформаційні технології (Рівень B - Комп'ютерна графіка та веб-дизайн)																									+		
ФВД3.2	Фінансові технології (Рівень A - Технології дистанційного банківського обслуговування)																											
ФВД4.1	Кібербезпека (Рівень G - Організація та проведення тестування на проникнення та соціальна інженерія)		+	+	+																							
ФВД4.2	Комп’ютерні системи та мережі (Рівень E - Адміністрування та моніторинг комп’ютерних систем)					+															+		+			+		
ФВД5.1	Кібербезпека (Рівень H - Правові основи інформаційної безпеки)										+		+				+											
ФВД5.2	Кібербезпека (Рівень I - Інформаційна безпека держави)																											
ФВД6.1	Інформаційні технології (Рівень D - Технології проектування та оцінювання людино - машинних інтерфейсів)		+																									
ФВД6.2	Моделювання (Рівень C - Теорія прийняття рішень)								+			+																
ФВД7.1	Програмування (Рівень D - Високорівневе програмування (веб-програмування))													+										+				
ФВД7.2	Банківські технології (Рівень C - Безпека фінансових ринків)																											
ФВД8.1	Інформаційні технології (Рівень C - Організація баз даних та знань)																									+		
ФВД8.2	Програмування (Рівень C - Кросплатформне програмування)					+				+																		

Таблиця 9

Таблиця міждисциплінарних зав'язків освітніх компонент освітньо-професійної програми

Семестр	Код КОП	Компоненти освітньої програми	Передумови вивчення	Є базою для вивчення
	1	2	3	4
1	ЗОД1	УБС студія «Тайм-менеджмент та міжособистісні комунікації в бізнесі»		ГОД10
1	ЗОД2	Інформаційні технології (рівень А)		ЗОД4, ГОД2, ГОД3, ГОД4, ГОД6, ГОД8, ГОД9, ГОД10, ФОД2, ФВД1.1, ФВД3.1, ФВД7.1, ФВД8.1
1, 2	ЗОД3	Професійна іноземна мова та міжнародні бізнес-комунікації		
3	ЗОД4	УБС студія «Банківська система» (рівень А)	ЗОД2, ГОД3	ФВД2.2, ФВД3.2
5	ЗОД5	УБС студія «Лідерство та командна робота»		
2	ЗВД1	Вибіркова дисципліна блоку «Загальна підготовка»		

1	ГОД1	Математика (Рівень А - Вища математика)		ГОД2, ГОД3, ГОД5, ГОД7, ГВД1, ФОД10, ФВД1.1, ФВД1.2, ФВД7.2
2	ГОД2	Програмування (Рівень А - Алгоритми та структури даних)	ГОД1, ГОД5, ЗОД2	ГОД4, ГОД6, ФОД4, ФОД6, ФОД10, ФВД3.1, ФВД7.1, ФВД8.1, ФВД8.2
2	ГОД3	Математика (Рівень С - Статистика (у т.ч. й Теорія ймовірностей)	ГОД1, ГОД5, ЗОД2	ЗОД4, ГОД10, ГВД1, ФОД5, ФОД8, ФВД1.1, ФВД1.2, ФВД6.2, ФВД7.2
6	ГОД4	Інформаційні технології (Рівень F - Технологія створення програмних продуктів)	ЗОД2, ГОД2, ФОД10	ФОД3, ФОД4, ФВД7.1,
1	ГОД5	Математика (Рівень В - Дискретна математика)	ГОД1	ГОД2, ГОД3, ГОД6, ГВД1, ФОД2, ФОД6, ФОД8, ФОД10, ФВД1.2, ФВД6.2, ФВД8.1
3	ГОД6	Комп’ютерні системи та мережі (Рівень В - Комп'ютерна схемотехніка та архітектура комп'ютерів)	ЗОД2, ГОД2, ГОД5, ГОД7	ГОД8, ГОД9, ФОД7, ФВД4.1, ФВД4.2
3	ГОД7	Комп’ютерні системи та мережі (Рівень А - Фізика	ГОД1	ГОД6, ГОД8, ФВД4.2

		та електротехніка)		
4	ГОД8	Комп’ютерні системи та мережі (Рівень С - Комп'ютерні системи та мережі)	ЗОД2, ГОД6, ГОД7	ГОД9, ФОД1, ФОД3, ФОД4, ФОД8, ФОД7, ФОД9, ФВД4.1, ФВД4.2
4	ГОД9	Інформаційні технології (Рівень А - Операційні системи)	ЗОД2, ГОД6, ГОД8	ФОД7, ФВД4.1, ФВД4.2
5	ГОД10	Фінансові технології (Рівень В - Цифрова економіка)	ЗОД1, ЗОД2, ГОД3	ФОД5, ФВД2.2
4	ГВД1	Вибіркова дисципліна блоку «Галузева підготовка» «Чисельні методи»	ГОД1, ГОД3, ГОД5	ФОД6, ФВД6.2
8	ФОД1	Кібербезпека (Рівень D - Комплексні системи захисту інформації)	ГОД8,ФОД3,ФОД4, ФВД7.2	
2	ФОД2	Кібербезпека (Рівень А - Основи кібербезпеки)	ЗОД2, ГОД5	ФОД3, ФОД4, ФОД5, ФОД9, ФВД2.1, ФВД3.2
6	ФОД3	Кібербезпека (Рівень С - Система стандартів інформаційної безпеки)	ГОД4, ГОД8, ФОД2	ФОД1, ФОД4, ФОД5, ФОД9, ФВД5.1, ФВД5.2

7	ФОД4	Кібербезпека (Рівень Е - Проектування інформаційних систем безпеки)	ГОД2, ГОД4, ГОД8, ФОД2, ФОД3, ФОД9, ФВД6.1, ФВД6.2, ФВД8.1, ФВД8.2	ФОД1, ФВД2.1, ФВД4.1
7	ФОД5	Моделювання (Рівень D - Моделювання бізнес-процесів безпеки)	ГОД3, ФОД2, ФОД3, ГОД10	ФВД4.2
7	ФОД6	Математика (Рівень D - Методи та системи штучного інтелекту)	ГОД2, ГОД5, ГВД1	
5	ФОД7	Комп’ютерні системи та мережі (Рівень D - Безпека комп'ютерних мереж)	ГОД6, ГОД8, ГОД9	ФОД9, ФВД2.2, ФВД5.1, ФВД5.2
6	ФОД8	Інформаційні технології (Рівень Е - Великі дані)	ГОД3, ГОД5, ГОД 8	
6	ФОД9	Кібербезпека (Рівень В - Функціональна безпека комп'ютерних систем)	ГОД8, ФОД2, ФОД3, ФОД7,	ФОД4, ФВД2.1, ФВД2.2
3	ФОД10	Програмування (Рівень В - Об¢єктно-орієнтовне програмування)	ГОД1, ГОД2, ГОД5	ГОД4, ФВД3.1, ФВД7.1, ФВД8.1,
3	ФВД1.1	Моделювання (Рівень А - Економіко-математичні	ЗОД2, ГОД1, ГОД3	ФВД6.2, ФВД7.2

		методи та моделі)		
3	ФВД1.2	Моделювання (Рівень B - Теорія ризиків)	ГОД1, ГОД3, ГОД5	ФВД6.2, ФВД7.2
7	ФВД2.1	Кібербезпека (Рівень F - Основи протидії кіберзлочинності та цифрова криміналістика)	ФОД2, ФОД4, ФОД9	ФВД5.1, ФВД5.2
7	ФВД2.2	Фінансові технології (Рівень D - Платіжні системи, технології та сервіси)	ЗОД4, ГОД10, ФОД7, ФОД9, ФВД3.2, ФВД7.2	
4	ФВД3.1	Інформаційні технології (Рівень B - Комп'ютерна графіка та веб-дизайн)	ЗОД2, ГОД2, ФОД10	ФВД6.1, ФВД7.1
4	ФВД3.2	Фінансові технології (Рівень A - Технології дистанційного банківського обслуговування)	ЗОД4, ФОД2	ФВД2.2,
8	ФВД4.1	Кібербезпека (Рівень G - Організація та проведення тестування на проникнення та соціальна інженерія)	ГОД6, ГОД8, ГОД9, ФОД4	

8	ФВД4.2	Комп’ютерні системи та мережі (Рівень Е - Адміністрування та моніторинг комп’ютерних систем)	ГОД6, ГОД7, ГОД8, ГОД9, ФОД5	
8	ФВД5.1	Кібербезпека (Рівень Н - Правові основи інформаційної безпеки)	ФОД3, ФОД7, ФВД2.1	
8	ФВД5.2	Кібербезпека (Рівень І - Інформаційна безпека держави)	ФОД3, ФОД7, ФВД2.1	
5	ФВД6.1	Інформаційні технології (Рівень D - Технології проектування та оцінювання людино-машинних інтерфейсів)	ФВД8.2, ФВД3.1	ФОД4
5	ФВД6.2	Моделювання (Рівень С - Теорія прийняття рішень)	ГОД3, ГОД5, ФВД1.1, ФВД1.2, ГВД1	ФОД4
5	ФВД7.1	Програмування (Рівень D - Високорівневе програмування (веб-програмування))	ЗОД2, ГОД2, ГОД4, ФОД10, ФВД8.2	
5	ФВД7.2	Фінансові технології (Рівень С - Безпека фінансових ринків)	ГОД1, ГОД3, ФВД1.1, ФВД1.2	ФОД1, ФВД2.2

4	ФВД8.1	Інформаційні технології (Рівень С - Організація баз даних та знань)	ЗОД2, ГОД2, ГОД5, ФОД10	ФОД4
4	ФВД8.2	Програмування (Рівень С – Крос-платформне програмування)	ГОД2	ФОД4, ФВД6.1, ФВД7.1

VII Вимоги до наявності системи внутрішнього забезпечення якості вищої освіти

У ДВНЗ «Університет банківської справи» функціонує система забезпечення вищим навчальним закладом 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 вищого навчального закладу, 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;

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 вищих навчальних закладів і здобувачів вищої освіти;

9) інших процедур і заходів.

У ДВНЗ «Університет банківської справи» система забезпечення якості освітньої діяльності та якості вищої освіти (система внутрішнього забезпечення якості) за поданням закладу вищої освіти 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.

VIII Вимоги професійних стандартів (за наявності)

Професійний стандарт	
Особливості стандарту вищої освіти, пов'язані з наявністю даного Професійного стандарту	