Міністерство освіти і науки України
ДВНЗ «Університет банківської справи»
Інститут банківських технологій та бізнесу

ОСВІТНЯ ПРОГРАМА
125 Кібербезпека

Шифр галузі	*Галузь знань*	*Код і найменування спеціальності*	*Спеціалізація (за наявності)*	*Ступінь вищої освіти (освітній ступінь)*
12	Інформаційні технології	125 Кібербезпека	–	Бакалавр

Розроблено:	**Погоджено:**	**Затверджено:**
Гарант освітньої програми Завідувач кафедри інформаційних технологій та кібербезпеки, к.т.н, доцент Гордєєв О.О.	Проректор з навчально-методичної роботи д.е.н., професор Кузнецова С.А.	Ректор, д.е.н, професор Смовженко Т.С.
Проектна група: Доцент кафедри інформаційних технологій та кібербезпеки, к.е.н. Краліч В. Р. Доцент кафедри інформаційних технологій та кібербезпеки, к.е.н, доцент Чмерук Г.Г. Доцент кафедри інформаційних технологій та кібербезпеки, к.п.н, доцент Бурлакова І.А.	Директор ІБТБ д.е.н., професор Швець Н.Р.	Вчена рада Протокол №11 від 30.06.2017р.
	Завідувач кафедри інформаційних технологій та кібербезпеки, к.т.н, доцент Гордєєв О.О.	
	Представник керівництва з якості к.філол.н., доц. Семів А.Р.	Навчально-методична рада Протокол № 7 від 22.06.2017р.
	Голова робочої групи : д.е.н., професор Кавун С.В.	
Видання:1	Чинний з 01.07.2017р.	Примірник контрольний

І. Загальна характеристика

Повна назва вищого навчального закладу та структурного підрозділу	Державний вищий навчальний заклад «Університет банківської справи» Інститут банківських технологій та бізнесу
Рівень вищої освіти	Перший (бакалаврський)
Галузь знань	12 «Інформаційні технології»
Офіційна назва освітньої програми	Освітньо-професійна програма освітнього рівня бакалавр за спеціальністю 125 Кібербезпека
Ступінь, що присвоюється	Бакалавр
Спеціальність	125 Кібербезпека
Спеціалізація (за наявності)	-
Варіативна компонента	Кібербезпека
Освітня кваліфікація	Бакалавр з кібербезпеки
Професійна(і) кваліфікація(ї)	-
Кваліфікація в дипломі	Освітня кваліфікація «Бакалавр з кібербезпеки»
Тип диплому та обсяг освітньої програми	Диплом бакалавра одиничний, 240 кредитів ЄКТС, 3 роки 10 місяців
Рівень/цикл	FQ-EHEA – перший цикл, EQF LLL – 6 рівень, НРК – 6 рівень / Бакалавр
Акредитація освітньої програми	-
Сертифікація освітньої програми	-
Мова(и)викладання	Українська
Термін дії освітньої програми	з 6.07.2017 р. до 1.07.2027 р.
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 молодшого спеціаліста
Обмеження щодо форм навчання	Не має
Академічні права випускників	FQ-EHEA – другий цикл, EQF LLL – 7 рівень, НРК – 7 рівень / Магістр
Інтернет-адреса постійного розміщення опису освітньої програми	http://www.ubs.edu.ua/ua/ibtb/

ІІ. Профіль освітньої програми

Тип диплома та обсяг програми	Диплом бакалавра одиничний, - на базі повної загальної середньої освіти з терміном навчання 11 років становить 240 кредитів ЄКТС; - на базі повної загальної середньої освіти з терміном навчання 12 років становить 180-240 кредитів ЄКТС; - на базі молодшого бакалавра становить 120 кредитів ЄКТС
Вищий навчальний заклад	Державний вищий навчальний заклад «Університет банківської справи» Інститут банківських технологій та бізнесу
Акредитуюча інституція	Акредитаційна комісія України (Національне агентство з забезпечення якості вищої освіти)
Період акредитації	2019-2020 рр.
Рівень програми	FQ-EHEA – перший цикл, EQF LLL – 6 рівень, НРК – 6 рівень / Бакалавр

А	**Ціль програми**
Формування особистості фахівця здатного розв'язувати складні спеціалізовані задачі та практичні проблеми з кібербезпеки та інформаційної безпеки взагалі, що характеризується комплексністю та невизначеністю умов.	

В	**Характеристика програми**	
1	*Предметна область, напрям*	Інформаційні технології в части кібербезпеки
2	*Фокус програми: загальна/спеціальна*	Спеціалізована вища освіта в кібербезпеці, спеціалізація – не передбачено
3	*Орієнтація програми*	Профіль освітньої програми орієнтований на освітньо-професійний та прикладний напрямок підготовки
4	*Особливості програми*	- вивчення банківських систем та технологій (дистанційне банківське обслуговування, платіжні системи), та забезпечення кібербезпеки для них; - вивчення технологій проектування та оцінювання людино-машинних інтерфейсів. Вивчення причин та наслідків впливу людино-машинних інтерфейсів на кібербезпеку інформаційних систем; - вивчення методів (технік) соціальної інженерії та організація та проведення тестування на проникнення.

С	**Працевлаштування та продовження освіти**

1	*Працевлаштування*	менеджер (управитель) систем з інформаційної безпеки (1495), помічник керівника виробничого підрозділу, помічник керівника іншого основного підрозділу, помічник керівника малого підприємства без апарату управління, помічник керівника підприємства (установи, організації), фахівець (сфера захисту інформації), фахівець із організації захисту інформації з обмеженим доступом, фахівець із організації інформаційної безпеки (3439), фахівець з режиму секретності, інспектор з організації захисту секретної інформації, аналітик систем забезпечення кібербезпеки, фахівець з організації та проведення тестування на проникнення.
2	*Продовження освіти*	Можливість навчання за програмою другого циклу FQ-EHEA, 7 рівня EQF-LLL та 7 рівня НРК
D	**Стиль та методика навчання**	
1	*Підходи до викладання та навчання*	Лекції з виростанням мультимедійного обладнання, лабораторні роботи, семінари, практичні заняття в малих групах, самостійна робота на основі підручників та конспектів, консультації із викладачами, вебінари, підготовка бакалаврської роботи.
2	*Система оцінювання*	Оцінювання навчальних досягнень студентів здійснюється за 100 бальною, 4-х бальною шкалами («відмінно», «добре», «задовільно», «незадовільно») і вербальною («зараховано», «не зараховано») системами. Види контролю: поточний, тематичний, періодичний, підсумковий, самоконтроль. Форми контролю: усне та письмове опитування, тестові завдання, лабораторні звіти, презентації, захист курсових робіт та проектів, звіти з практик та науково-дослідних робіт *Атестація* – кваліфікаційний іспит і підготовка та захист кваліфікаційної бакалаврської роботи.
E	**Загальні компетентності**	

	шифр	Зміст
	КЗ 01	Здатність застосовувати знання у практичних ситуаціях
	КЗ 02	Знання та розуміння предметної області та розуміння професії
	КЗ 03	Здатність спілкуватися рідною та другою іноземною мовою як усно, так і письмово
	КЗ 04	Здатність здійснювати професійну діяльність згідно з вимогами санітарно-

		гігієнічного режиму, охорони праці, техніки безпеки та протипожежної безпеки
	КЗ 05	Вміння виявляти, ставити та вирішувати проблеми
	КЗ 06	Здатність до пошуку, оброблення та аналізу інформації з різних джерел
	КЗ 07	Навички міжособистісної взаємодії
	КЗ 08	Прагнення до збереження навколишнього середовища
	КЗ 09	Здатність діяти соціально відповідально та громадянсько свідомо
	КЗ 10	Здатність вчитися і бути сучасно навченим
	КЗ 11	Здатність приймати обґрунтовані рішення
	КЗ 12	Здатність до адаптації та дії в новій ситуації
	КЗ 13	Дотримання та пропагування здорового способу життя
	КЗ 14	Здатність бути критичним та самокритичним
2	**Спеціальні професійні компетенції**	
	СПК 01	Здатність використовувати законодавчу та нормативно-правову бази, а також вимоги відповідних, в тому числі і міжнародних, стандартів та практик щодо здійснення професійної діяльності
	СПК 02	Здатність до використання інформаційних і комунікаційних технологій з метою пошуку нової інформації, створення баз даних, аналізу розподілених АС, каналів зв'язку, систем управління процесами, баз даних, оперативного планування роботи систем на основі аналізу інформаційних потоків та їх оптимізації
	СПК 03	Здатність здійснювати проектування (розробку) систем, технологій і засобів інформаційної безпеки
	СПК 04	Здатність здійснювати протидію несанкціонованому проникненню в ІТ системи і мережі
	СПК 05	Здатність прогнозувати, виявляти та оцінювати стан інформаційної безпеки об'єктів і систем
	СПК 06	Здатність відновлювати нормальне функціонування ІТ систем і мереж після здійснення кібернападів, збоїв та відмов
	СПК 07	Здатність виконувати спеціальні дослідження технічних і програмно-апаратних засобів захисту обробки інформації в ІТС
	СПК 08	Здатність проводити техніко-економічного аналіз й обґрунтовувати проектні рішення з забезпечення кібербезпеки
	СПК 09	Здатність формувати комплекс заходів (правил, процедур, практичних прийомів та ін.) для управління інформаційною безпекою
	СПК 10	Здатність здійснювати управління інцидентами інформаційної та кібербезпеки
	СПК 11	Здатність здійснювати управління ризиками інформаційної та кібербезпеки
	СПК 12	Здатність виконувати моніторинг даних, комп'ютерних зловживань та аномалій
	СПК 13	Здатність прогнозувати, виявляти та оцінювати можливі загрози інформаційному простору держави та дестабілізуючі чинники
	СПК 14	Здатність проводити дослідження у практичній професійній діяльності

F	Програмні результати навчання
	Загальні результати навчання
РН 1	застосувати концептуальні знання з навчальних дисциплін загальної підготовки для засвоєння навчальних дисциплін професійної підготовки
РН 2	проектувати майбутню професійну діяльність з урахуванням її значущості для громадянина та держави,а також напрямків розвитку інформаційної та кібербезпеки
РН 3	застосувати знання державної та однієї з іноземних мов з метою забезпечення ефективності професійної комунікації
РН 4	дотримуватись вимог санітарно-гігієнічного режиму, охорони праці, техніки безпеки та протипожежної безпеки при здійсненні професійної діяльності
РН 5	організувати власну професійну діяльність, обирати оптимальні методи та способи розв'язування складних спеціалізованих задач та практичних проблему професійній діяльності, оцінювати їхню ефективність
РН 6	використати результати самостійного пошуку, аналізу та синтезу інформації з різних джерел для ефективного рішення спеціалізованих задач професійної діяльності
РН 7	дотримуватись норм міжособистісного спілкування у професійній взаємодії
РН 8	прогнозувати наслідки результатів діяльності людини з метою збереження навколишнього середовища
РН 9	використовувати історичну спадщину та культурні традиції свого народу для професійного зростання, саморозвитку, самовдосконалення
РН 10	вдосконалювати професійний та особистісний розвиток протягом усього життя
РН 11	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
РН 12	адаптуватися в умовах частої зміни технологій професійної діяльності, прогнозувати кінцевий результат
РН 13	демонструвати та пропагувати здоровий спосіб життя
РН 14	критично осмислювати основні теорії, принципи, методи і поняття у навчанні та професійній діяльності
	Фахові результати навчання
РН 15	діяти на основі законодавчої, нормативно-правової баз України та вимог відповідних стандартів, тому числі міжнародних
РН 16	готувати пропозиції до нормативних актів щодо забезпечення інформаційної безпеки
РН 17	здійснювати професійну діяльність на основі знань сучасних інформаційно-комунікаційних технологій
РН 18	застосувати програмні засоби, навички роботи в телекомунікаційних та комп'ютерних мережах
РН 19	використати спеціалізовані комп'ютерні програми в професійній діяльності
РН 20	обирати відповідну технологію програмування, виконати аналіз специфікації задач
РН 21	виконувати аналіз програмного забезпечення з метою пошуку, ідентифікації, виявлення та усунення помилок програмування
РН 22	виконувати декомпозицію ІТС
РН 23	розробляти структурні схеми з відображенням зв'язків між інформаційними процесами на віддалених системах
РН 24	розробляти модель загроз, розробляти модель порушника
РН 25	розробляти проекти ІТС базуючись на стандартизованих технологіях та протоколах передачі даних
РН 26	вирішувати завдання захисту програм та даних ІТС програмно-апаратними засобами та давати оцінку якості прийнятих рішень
РН 27	вибирати основні методи та способи захисту інформації відповідно до вимог сучасних

	стандартів інформаційної безпеки щодо критеріїв безпеки інформаційних технологій, застосовуючи системний підхід та знання основ теорії інформаційної безпеки
РН 28	проектувати та реалізувати комплексні систему захисту інформації АС організації (підприємства) відповідно до вимог нормативних документів системи технічного захисту інформації
РН 29	застосовувати теорії та методи захисту для забезпечення безпеки інформації в інформаційних і комунікаційних системах та мережах
РН 30	здійснювати оцінку можливості проникнення в ІТ системи та мережі шляхом експлуатації наявних вразливостей
РН 31	здійснювати оцінку захищеності ІТ систем та мереж
РН 32	використовувати інструментальні засоби оцінки наявних вразливостей
РН 33	оцінювати можливості та ефективність застосування, в тих чи інших умовах, інструментальних засобів оцінки вразливостей ІТ систем та мереж
РН 34	виконувати налаштування інформаційних систем та комунікаційного обладнання
РН 35	виконувати захист інформаційних систем від комп'ютерних вірусів
РН 36	забезпечувати впровадження та дотримання політики кіберзахисту в ІТС, процедур, і правил
РН 37	організовувати процес створення планів неперервності бізнесу
РН 38	приймати участь у розробці планів відновлення, неперервності процесів організації для забезпечення здатності організації продовжувати виконувати необхідну діяльність в період порушення ІТ
РН 39	виявляти небезпечні сигнали технічних засобів
РН 40	вимірювати параметри небезпечних сигналів для технічних каналів витоку інформації та визначати ефективність захисту від витоку інформації відповідно до вимог нормативних документів системи технічного захисту інформації
РН 41	інтерпретувати результати проведення спеціальних вимірювань з використанням технічних засобів, контролю характеристик ІТСМ відповідно до вимог нормативних документів системи технічного захисту інформації
РН 42	проводити атестацію (спираючись на облік та обстеження) режимних територій (зон), приміщень тощо в умовах додержання режиму секретності із фіксуванням результатів у відповідних документах
РН 43	виконувати дослідження, перевірку, аналіз та оцінювання об'єктів щодо їх відповідності вимогам нормативних документів та можливості їх використання для забезпечення інформації
РН 44	обґрунтування інвестицій в інформаційну безпеку
РН 45	аналізувати економічну ефективність заходів інформаційної безпеки
РН 46	визначати особливості організаційної структури та організації робіт
РН 47	використовувати міжнародні та національні специфічні для сектора економіки вимоги та кращі практики
РН 48	приймати участь у розробці та впровадженні стратегії інформаційної безпеки та/або кібербезпеки відповідно до цілей і завдань організації
РН 49	приймати участь у розробці та впровадженні політики, стандартів та процедур інформаційної безпеки та/ або кібербезпеки
РН 50	на основі політики захисту організації розробляти нормативні документи для її реалізації
РН 51	впроваджувати процеси виявлення, ідентифікації, аналізу та реагування на інциденти інформаційної/кібербезпеки
РН 52	застосовувати національні та міжнародні регулюючі актів в сфері інформаційної безпеки для розслідування внутрішніх та зовнішніх інцидентів інформаційної безпеки
РН 53	розробляти та оцінювати моделі і політику безпеки на основі використання сучасних принципів, способів та методів теорії захищених систем

РН 54	застосовувати політики, що базуються риск адаптивному контролі доступу
РН 55	здійснювати аналіз ризиків функціонування ІКС: визначати послідовність аналізу, формувати моделі порушника та загроз, використовувати сучасні методи та методики аналізу ризиків, оцінювання та управління ризиками
РН 56	виконувати конфігурування систем виявлення вторгнень та використовувати компоненти захисту для забезпечення необхідного рівня захищеності ІТС
РН 57	використовувати інструментарій для моніторингу даних в ІТС
РН 58	виконувати аналіз зловмисного програмного коду
РН 59	характеризувати стан інформаційної безпеки особистості, суспільства та держави
РН 60	характеризувати основні форми інформаційного протиборства в умовах входження держави в інформаційне суспільство
РН 61	використовувати теоретичні і практичні методи та методики досліджень у галузі інформаційної безпеки
РН 62	застосовувати системний підхід та знання основ теорії інформаційної безпеки

G	Ресурсне забезпечення реалізації програми	
1	*Кадрове забезпечення*	Якісний склад науково-педагогічних працівників, що забезпечує навчальний процес освітнього ступеня бакалавр зі спеціальності 125 «Кібербезпека» галузі знань 12 «Інформаційні технології» складає 20 % докторів наук та професорів, 60% кандидатів наук та доцентів та без звань та степенів 20%.
2	*Матеріальне-технічне забезпечення*	Обслуговування навчального процесу з підготовки фахівців зі спеціальності 125 «Кібербезпека» галузі знань 12 «Інформаційні технології» освітнього ступеня бакалавр забезпечує власна матеріально-технічна база інституту, яка включає навчальні та комп`ютерні аудиторії (загальною площею 6770,4 кв.м.) обладнані інтерактивними дошками, необхідним технічним спеціалізованим забезпеченням та сучасною комп`ютерною технікою. Встановлені сервери ліцензійних центру сертифікації ключів та системи електронного документообігу (встановлені за офіційними договорами із компаніями-розробниками) надають можливість проведення навчальних практичних та лабораторних занять на базі віртуальних середовищ. Побудовано навчально-тренувальну банківську систему – програмно-технічний комплекс, який дає можливість відтворити роботу дворівневої банківської системи у двох напрямах: модель взаємодії НБУ з іншими банками і модель взаємодії головного банку з філіями. В інститутах функціонують навчально-тренувальні банки, які можуть виконувати функції філії головного банку, або самостійної банківської установи. В інституті функціонує бібліотека з двома читальними

		залами, що забезпечує виконання навчального плану освітнього ступеня бакалавр зі спеціальності 125 «Кібербезпека» галузі знань 12 «Інформаційні технології». Розвинена соціальна інфраструктура, до якої належить медпункт, їдальня та персональний Wi-Fi осередок «IT-Space» сприяє підготовці фахівців, гуртожиток, в якому забезпечено проживання студентів у повному обсязі.
3	*Інформаційне та навчально-методичне забезпечення*	Фонд бібліотеки налічує 17556 примірників підручників, навчальних посібників, довідкової та іншої навчальної літератури, фахових періодичних видань тощо, що на 100% забезпечує всі дисципліни навчального плану спеціальності 125 «Кібербезпека» галузі знань 12 «Інформаційні технології» освітнього ступеня бакалавр навчально-методичною літературою в паперовому та електронному вигляді. Внутрішня електронна мережа (бібліотека) містить у електронному вигляді методичні матеріали за всіма дисциплінами навчального плану. Створено інституційний репозитарій, який сприяє популяризації наукових здобутків інституту, підвищення його рейтингу через зростання рівня цитування наукових праць НПП. Діюча система дистанційного навчання забезпечує самостійну та індивідуальну роботу студентів спеціальності 125 «Кібербезпека» галузі знань 12 «Інформаційні технології» освітнього ступеня бакалавр.
Н	**Академічна мобільність**	
1	*Національна кредитна мобільність*	Організація кредитної мобільності (окрім 1-го курсу) бакалаврів. Проект «Національний Еразмус+ Офіс в Україні» (НЕО); в межах об'єднання Економосвіта; серед інститутів Університету.
2	*Міжнародна кредитна мобільність*	Організація кредитної мобільності (окрім 1-го курсу) бакалаврів. Проект «Еразмус+ КА1 (Е+ ІСМ)»; програми подвійних дипломів: Університет ім. Миколоса Ромеріса, м. Вільнюс (Литва); Балтійська міжнародна академія м. Рига (Латвія); Краківський економічний університет м. Краків (Польща); Вища школа менеджменту м. Барселона (Іспанія); Швейцарська школа бізнесу м. Монте (Швеція).
3	*Навчання іноземних здобувачів вищої освіти*	Передбачено

ІІІ. Структура та компоненти освітньої програми

В основу розроблення освітньо-професійної програми покладено компетентнісний підхід з використанням ЄКТС, де для досягнення запланованих результатів навчання за освітньо-професійною 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.

Освітньо-професійна 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 освітньо-професійної 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)	***36***	***6***	***42***
	- галузева підготовка (2)	***60***	***6***	***66***
	- фахова предметна підготовка (3)	***60***	***48***	***108***
практична підготовка				***24***
Загальний обсяг		***156***	***60***	***240***

Розподіл кредитів за навчальними дисциплінами, структурно-логічна

послідовність їх вивчення, форми підсумкового контролю наведено в таблиці 4.

Таблиця 4

Розподіл змісту та обсягу кредитів ЄКТС за компонентами освітньої програми

Компоненти освітньої програми (навчальні дисципліни, практики, кваліфікаційна робота тощо)		**кредити ЄКТС**	**форма підсумкового контролю**	**семестр**
№ з/п	**Назва**			
1.Блок «Загальна підготовка» (1)				
1.1.Обов'язкові дисципліни				
ЗОД1	УБС студія "Тайм-менеджмент та міжособистісні комунікації в бізнесі"	6	ЗАЛІК	1
ЗОД2	Інформаційні технології (рівень А)	6	ЕКЗ	1
ЗОД3	Професійна іноземна мова та міжнародні бізнес-комунікації	12	ЗАЛІК, ЕКЗ	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 дисциплін за блоком 1		**36**		
1.2.Вибіркові дисципліни				
ЗВД1	Вибіркова дисципліна блоку "Загальна підготовка"	6	ЗАЛІК	1
Загальний обсяг вибіркових дисциплін за блоком 1		**6**		
Загальний обсяг дисциплін за блоком 1		**42**		
2. Блок «Галузева підготовка»				
2.1. Обов'язкові дисципліни				
ГОД1	Математика (Рівень А - Вища математика)	6	ЕКЗ	1
ГОД2	Математика (Рівень С - Статистика (у т.ч. теорія ймовірності))	6	ЕКЗ	2
ГОД3	Математика (Рівень В - Дискретна математика)	6	ЕКЗ	1
ГОД4	Програмування (Рівень А - Алгоритми та структури даних)	6	ЕКЗ	2
ГОД5	Комп. сист. та мережі (Рівень А - Фізика та електротехніка)	6	ЗАЛІК	3
ГОД6	Комп. сист. та мережі (Рівень В - Комп'ютерна схемотехніка та архітектура комп'ютерів)	6	ЕКЗ	3

ГОД7	Комп. сист. та мережі (Рівень С - Комп'ютерні системи та мережі)	6	ЕКЗ	4
ГОД8	Інформаційні технології (Рівень А - Операційні системи)	6	ЕКЗ	4
ГОД9	Кібербезпека (Рівень А - Основи кібербезпеки)	6	ЗАЛІК	2
ГОД10	Банківські технології (Рівень В - Цифрова економіка)	6	ЗАЛІК	5
Загальний обсяг обов'язкових дисциплін за блоком 2		**60**		
2.2.Вибіркові дисципліни				
ГВД1	Вибіркова дисципліна блоку "Галузева підготовка" - Чисельні методи та системний аналіз	6	ЗАЛІК	4
Загальний обсяг вибіркових дисциплін за блоком 2		**6**		
Усього за блоком 2		**66**		
3. Блок «Фахова підготовка»				
3.1.Обов'язкові дисципліни				
ФОД1	Кібербезпека (Рівень D - Комплексні системи захисту інформації)	6	ЕКЗ	7
ФОД2	Інформаційні технології (Рівень F - Технологія створення програмних продуктів)	6	ЕКЗ	6
ФОД3	Кібербезпека (Рівень С - Система стандартів інформаційної безпеки)	6	ЗАЛІК	6
ФОД4	Кібербезпека (Рівень Е - Проектування інформаційних систем безпеки)	6	ЕКЗ	7
ФОД5	Моделювання (Рівень D - Моделювання бізнес-процесів безпеки)	6	ЕКЗ	7
ФОД6	Математика (Рівень D - Методи та системи штучного інтелекту)	6	ЕКЗ	7
ФОД7	Комп. сист. та мережі (Рівень D - Безпека комп'ютерних мереж)	6	ЕКЗ	5
ФОД8	Інформаційні технології (Рівень Е - Організація баз даних та знань)	6	ЕКЗ	6
ФОД9	Кібербезпека (Рівень В - Функціональна безпека комп'ютерних систем)	6	ЕКЗ	6
ФОД10	Програмування (Рівень В - Обєктно-орієнтовне програмування)	6	ЕКЗ	3

Загальний обсяг обов'язкових дисциплін за блоком 3		**60**		
3.2. Вибіркові дисципліни				
ФВД1	Моделювання (Рівень А - Економіко-математичні методи та моделі)	6	ЗАЛІК	3
	Моделювання (Рівень В - Терія ризиків)	6	ЗАЛІК	3
ФВД2	Кібербезпека (Рівень F - Основи протидії кіберзлочинності та цифрова криміналістика)	6	ЗАЛІК	7
	Банківські технології (Рівень D - Платіжні системи)	6	ЗАЛІК	7
ФВД3	Інформаційні технології (Рівень В - Комп'ютерна графіка та веб-дизайн)	6	ЕКЗ	4
	Банківські технології (Рівень А - Технології дистанційного банківського обслуговування)	6	ЕКЗ	4
ФВД4	Кібербезпека (Рівень G - Організація та проведення тестування на проникнення та соціальна інженерія)	6	ЕКЗ	8
	Комп. сист. та мережі (Равень Е - Адміністрування та моніторинг комп'ютерних систем)	6	ЕКЗ	8
ФВД5	Кібербезпека (Рівень Н - Правові основи інформаційної безпеки)	6	ЗАЛІК	8
	Кібербезпека (Рівень І - Інформаційна безпека держави)	6	ЗАЛІК	8
ФВД6	Інформаційні технології (Рівень D - Технології проектування та оцінювання людино - машинних інтерфейсів)	6	ЗАЛІК	5
	Моделювання (Рівень С -Теорія прийняття рішень)	6	ЗАЛІК	5
ФВД7	Програмування (Рівень D - Високорівневе программування (веб-программування))	6	ЕКЗ	5
	Банківські технології (Рівень С - Безпека фінансових ринків)	6	ЕКЗ	5
ФВД8	Інформаційні технології (Рівень С - Великі данні)	6	ЗАЛІК	4

	Програмування (Рівень С - Кросплатформіне програмування)	6	ЗАЛІК	4
Загальний обсяг вибіркових дисциплін за блоком 3		**48**		
Усього за блоком 3		**108**		
ПП1	Навчальна практика (Проектно-технологічна практика)	6		7
ПП2	Виробнича практика	6		8
ПП3	Бакалаврський тренінг (семінар)	6		8
ПП4	Кваліфікаційна бакалаврська робота	6		8
Всього практична підготовка		**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 співвідношення результатів навчання та компетентностей наведено в табл. 5.

Матрицю співвідношення навчальних дисциплін та результатів навчання наведено в табл. 6.

VI - Форми атестації здобувачів вищої освіти

Атестація здобувачів кваліфікації бакалавр з кібербезпеки здійснюється у формі:	кваліфікаційного іспиту публічного захисту кваліфікаційної бакалаврської роботи за спеціальністю 125 кібербезпека. Атестація здійснюється екзаменаційною комісією відповідно до вимог стандарту вищої освіти після виконання студентом навчального плану та завершується видачою диплома встановленого зразка. На атестацію виноситься увесь нормативний зміст підготовки фахівця.

	Термін проведення атестації визначається навчальним планом та графіком освітнього процесу. До атестації допускаються студенти, які виконали всі вимоги освітньої програми та навчального плану. Результати атестації визначаються оцінками за національною шкалою «відмінно», «добре», «задовільно», «незадовільно»
Вимоги до кваліфікаційної роботи	Кваліфікаційна бакалаврська робота передбачає розв'язання складного спеціалізованого завдання або практичної проблеми в галузі кібербезпеки, що характеризується комплексністю та невизначеністю умов. Кваліфікаційна бакалаврська робота має бути перевірений на плагіат. Кваліфікаційна бакалаврська робота має бути розміщений на сайті вищого навчального закладу.
Вимоги до кваліфікаційного іспиту	Кваліфікаційний іспит передбачає оцінювання обов'язкових результатів навчання, визначених стандартом вищої освіти за спеціальністю 125 Кібербезпека та цією освітньою програмою.

Таблиця 5

Матриця співвідношення результатів навчання та компетентностей

	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
КЗ 01	+																										
КЗ 02		+																									
КЗ 03			+																								
КЗ 04				+																							
КЗ 05					+																						
КЗ 06						+																					
КЗ 07							+																				
КЗ 08								+																			
КЗ 09									+																		
КЗ 10										+																	
КЗ 11											+																
КЗ 12												+															
КЗ 13													+														
КЗ 14														+													
СПК 01															+	+											
СПК 02																	+	+	+	+	+						
СПК 03																						+	+	+	+	+	+

	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
СПК 03	+																										
СПК 04		+																									
СПК 05			+	+	+	+																					
СПК 06							+	+	+	+	+																
СПК 07												+	+	+	+	+											
СПК 08																	+	+	+	+							
СПК 09																					+	+	+				
СПК 10																								+	+		
СПК 11																										+	+

	РН 55	РН 56	РН 57	РН 58	РН 59	РН 60	РН 61	РН 62
СПК 11	+							
СПК 12		+	+	+				
СПК 13					+	+		
СПК 14							+	+

Таблиця 6

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
1. Блок "Загальна підготовка "																											
1.1. Обов'язкові дисципліни																											
УБС студія "Тайм-менеджмент та міжособистісні комунікації в бізнесі"	+		+					+																+			
Інформаційні техно-логії (рівень А)			+																+	+	+	+					
Професійна іноземна мова та міжнародні бізнес-комунікації	+		+		+																						
УБС студія «Банківська система (рівень А)»		+	+										+	+	+	+		+					+		+	+	
УБС студія "Лідерство та командна робота"	+		+			+	+	+	+	+		+															
1.2. Вибіркові дисципліни																											
Вибіркова						+				+				+													

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
дисципліна блоку "Загальна підготовка"																											

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	РН 55	РН 56	РН 57	РН 58	РН 59	РН 60	РН 61	РН 62
2. Блок « Галузева підготовка»																																			
2.1. Обов'язкові дисципліни																																			
Математика (Рівень А - Вища математика)				+															+	+	+	+													
Математика (Рівень С - Статистика (у т.ч. теорія ймовірності))			+	+										+												+					+			+	+
Математика (Рівень В - Дискретна математика)		+	+									+	+		+	+	+	+								+									
Програмування (Рівень А - Алгоритми та структури даних)		+	+	+		+			+				+	+	+	+	+	+		+					+	+									
Програмування (Рівень В - Об'єктно-орієнтоване програмування)	+																							+		+					+				
Комп. сист. та мережі (Рівень А - Фізика та електротехніка)	+							+	+																+										
Комп. сист. та мережі (Рівень В - Комп'ютерна		+	+	+		+	+	+	+	+			+	+			+						+		+	+									

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	РН 55	РН 56	РН 57	РН 58	РН 59	РН 60	РН 61	РН 62
схемотехніка та архітектура комп'ютерів)																																			
Комп. сист. та мережі (Рівень С - Комп'ютерні системи та мережі)	+	+	+	+			+	+	+				+			+	+		+	+		+			+										
Комп. сист. та мережі (Рівень D - Безпека комп'ютерних мереж)			+		+									+								+				+						+		+	
Інформаційні технології (Рівень А - Операційні системи)		+	+	+		+			+	+		+		+	+	+						+	+	+											
Інформаційні технології (Рівень Е - Організація баз даних та знань)		+	+	+		+	+	+	+				+	+	+	+	+	+			+		+	+	+										
Кібербезпека (Рівень А - Основи кібербезпеки)																		+	+	+	+	+	+	+	+	+										
Банківські технології (Рівень В - Цифрова економіка)		+	+										+	+	+	+	+	+	+																
2.2. Вибіркові дисципліни																																			
Вибіркова дисципліна блоку "Галузева підготовка" - Чисельні методи та системний аналіз		+	+	+			+		+	+		+	+	+	+	+	+	+		+	+		+	+											
3.Блок "Фахова підготовка "																																			
3.1. Обов'язкові дисципліни																																			
Кібербезпека (Рівень D - Комплексні системи захисту інформації)		+	+	+				+	+	+				+	+	+		+			+			+	+	+									

Навчальна дисципліна	РН28	РН29	РН30	РН31	РН32	РН33	РН34	РН35	РН36	РН37	РН38	РН39	РН40	РН41	РН42	РН43	РН44	РН45	РН46	РН47	РН48	РН49	РН50	РН51	РН52	РН53	РН54	РН55	РН56	РН57	РН58	РН59	РН60	РН61	РН62
Інформаційні технології (Рівень F - Технологія створення програмних продуктів)	+			+																				+							+				
Кібербезпека (Рівень C - Система стандартів інформаційної безпеки)		+	+	+		+	+	+	+				+	+		+	+	+		+	+	+				+									
Кібербезпека (Рівень E - Проектування інформаційних систем безпеки)		+		+		+	+	+		+	+	+		+	+	+			+	+	+		+	+	+										
Моделювання (Рівень D - Моделювання бізнес-процесів безпеки)		+	+	+			+	+	+		+	+	+	+	+	+			+	+	+		+												
Математика (Рівень D - Методи та системи штучного інтелекту)		+	+	+			+	+	+		+	+	+	+	+	+		+			+		+	+	+										
3.2. Вибіркові дисципліни																																			
Моделювання (Рівень A - Економіко-математичні методи та моделі)				+															+	+	+	+													
Моделювання (Рівень B - Теорія ризиків)																	+									+		+							+
Кібербезпека (Рівень F - Основи протидії кіберзлочинності та цифрова криміналістика)						+		+																	+										+
Банківські технології (Рівень D - Платіжні	+									+														+											

Навчальна дисципліна	РН28	РН29	РН30	РН31	РН32	РН33	РН34	РН35	РН36	РН37	РН38	РН39	РН40	РН41	РН42	РН43	РН44	РН45	РН46	РН47	РН48	РН49	РН50	РН51	РН52	РН53	РН54	РН55	РН56	РН57	РН58	РН59	РН60	РН61	РН62
системи)																																			
Інформаційні технології (Рівень В - Комп'ютерна графіка та веб-дизайн)		+					+							+	+	+	+			+		+	+	+											
Банківські технології (Рівень А - Технології дистанційного банківського обслуговування)										+														+											
Кібербезпека (Рівень G - Організація та проведення тестування на проникнення та соціальна інженерія)						+									+					+										+	+				
Комп. сист. та мережі (Равень Е - Адміністрування та моніторинг комп'ютерних систем)		+	+				+		+				+	+			+	+	+					+		+									
Кібербезпека (Рівень Н - Правові основи інформаційної безпеки)																								+	+										
Кібербезпека (Рівень І - Інформаційна безпека держави)																						+	+		+							+	+		
Інформаційні технології (Рівень D - Технології проектування та оцінювання людино - машинних інтерфейсів)																+																+			

Навчальна дисципліна	РН28	РН29	РН30	РН31	РН32	РН33	РН34	РН35	РН36	РН37	РН38	РН39	РН40	РН41	РН42	РН43	РН44	РН45	РН46	РН47	РН48	РН49	РН50	РН51	РН52	РН53	РН54	РН55	РН56	РН57	РН58	РН59	РН60	РН61	РН62
Моделювання (Рівень С -Теорія прийняття рішень)																												+							+
Програмування (Рівень D - Високорівневе программування (веб-программування))	+																							+		+					+				
Банківські технології (Рівень С - Безпека фінансових ринків)		+								+																									
Інформаційні технології (Рівень С - Великі данні)																										+						+			
Програмування (Рівень С - Кросплатформіне програмування)	+							+																											
Кібербезпека (Рівень В - Функціональна безпека комп'ютерних систем)																							+		+	+				+					
Навчальна практика - Проектно-технологічна практика																													+	+	+		+	+	+
Виробнича практика - Переддипломна практика																													+	+	+		+	+	+
Бакалаврський семінар																												+	+	+	+	+	+	+	+
Кваліфікаційна бакалаврська робота																												+	+	+	+	+	+	+	+

VII Вимоги до наявності системи внутрішнього забезпечення якості вищої освіти

У ДВНЗ «Університет банківської справи» повинна функціонувати 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.

Система забезпечення вищим навчальним закладом 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.

VIII Вимоги професійних стандартів (у разі їх наявності)

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

Гарант освітньої програми:
Завідувач кафедри інформаційних систем
та кібербезпеки ІБТБ
ДВНЗ «Університет банківської справи»

к.т.н., доцент Гордєєв О.О.