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

Введено в дію наказом від 06.05. 2021 р.
№ 0202-1/204

Проректор з науково-педагогічної роботи
_____ Антон ПАНТЕЛЕЙМОНОВ
«06» травня 2021 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" квітня 2021 року, протокол № 5.

ЛИСТ ПОГОДЖЕННЯ

освітньо-професійної (освітньо-наукової) програми

1.1. Вчена рада Навчально-наукового інституту «Каразінський банківський інститут»:
протокол № 6 від « 25 » лютого 20 21 р.

Голова Вченої ради інституту _____ Б.В. Самородов

1.2. Науково-методична комісія інституту:
протокол № 3 від « 24 » лютого 20 21 р.

Голова науково-методичної комісії інституту _____ І.М.Вядрова

1.3. Кафедра інформаційних технологій та математичного моделювання:
протокол № 6 від « 17 » грудня 20 20 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, професор Харківського державного технічного університету радіоелектроніки по кафедрі застосування ЕОМ (рішення Вченої Ради ХДТУРЕ від 25 грудня 1998 року)
Члени робочої групи		
Соболєв Олександр Вікторович	Доцент кафедри інформаційних технологій та математичного моделювання	кандидат технічних наук
Макарова Ганна Валеріївна	Доцент кафедри інформаційних технологій та математичного моделювання	кандидат фізико-математичних наук, доцент кафедри вищої математики

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.

Зовнішні стейкхолдери, залучені до розробки освітньої програми
Представники бізнесу, роботодавці:

Жукова О. М., президент Харківського банківського союзу
Попов І.О., керівник регіонального центру з підбору персоналу КБ ПАТ«ПРИВАТБАНК»
Зачепа Р.В. , заступник директора по роботі з приватними особами Відділення «Харківська регіональна Дирекція» ПАТ «КРЕДІ АГРІКОЛЬ БАНК»
Столбов В.Ф., начальник управління безпеки Харківського головного регіонального управління ПАТ КБ «ПриватБанк»

РЕЦЕНЗІЯ

на освітньо-професійну програму «Кібербезпека у фінансових технологіях» та навчальний план спеціальності 125 «Кібербезпека» першого (бакалаврського) ступеня вищої освіти навчально-наукового інституту «Каразінський банківський інститут» Харківського національного університету імені В.Н. Каразіна

Сучасний стан розвитку інформаційних технологій та автоматизації всіх сфер діяльності суспільства в Україні та світі обумовлює потребу у підготовці фахівців, здатних не лише забезпечити проектування, розробку й функціонування інформаційно-комунікаційних систем та сервісів, а й спроможних забезпечити належний рівень інформаційної та/або кібербезпеки .

Рецензована освітньо-професійна програма «Кібербезпека у фінансових технологіях» розроблена колективом кафедри інформаційних технологій та математичного моделювання ННІ «Каразінський банківський інститут» (керівник проектної групи – гарант освітньої програми – кандидат технічних наук, доцент Кобилін А.М.) із залученням потенційних роботодавців, що сприяє всебічному урахуванню вимог та потреб ринку праці в галузі інформаційної безпеки фінансово-кредитних установ.

Освітньо-професійна програма містить профіль освітньо-професійної програми, перелік обов'язкових та вибіркових компонент, матрицю відповідності програмних компетентностей компонентам освітньо-професійної програми, матрицю забезпечення програмних результатів навчання відповідним компонентам освітньо-професійної програми, структурно-логічну схему у вигляді міждисциплінарних зв'язків освітніх компонент.

Детальний аналіз рецензованої освітньо-професійної програми показав відповідність програми стандарту вищої освіти за спеціальністю 125 «Кібербезпека». Освітні компоненти програми спрямовані на підготовку фахівця з урахуванням загальних тенденцій галузі інформаційних технологій, особливостей спеціальності та специфіки фінансово-кредитної сфери.

Навчальний план підготовки бакалаврів спеціальності «Кібербезпека» повністю відповідає завданням та змісту освітньо-професійної програми. Пропонована послідовність вивчення дисциплін та графік навчального процесу забезпечують відповідність програмних результатів навчання сучасним запитам потенційних роботодавців.

Вважаю, що освітньо-професійна програма підготовки здобувачів вищої освіти першого (бакалаврського) рівня вищої освіти в галузі знань 12 «Інформаційні технології» за спеціальністю 125 «Кібербезпека», розроблена навчально-науковим інститутом «Каразінський банківський інститут» ХНУ ім. В.Н.Каразіна, відповідає встановленим вимогам та забезпечить здобувачам фундаментальну підготовку теоретичних і практичних знань, умінь та навичок за спеціальністю, достатніх для ефективного виконання завдань відповідного рівня професійної діяльності з інформаційних технологій, інформаційної та/або кібербезпеки, а тому може бути рекомендована до впровадження в освітній процес інституту та університету.

Рецензент: к.т.н., доцент, доцент
кафедри безпеки інформаційних технологій
Харківського національного
університету радіоелектроніки О.Є. Петренко

ПІДПИС ЗАСВІДЧУЮ:
Начальник відділу кадрів
«12» 03 2021

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ ХАРКІВСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ РАДІОЕЛЕКТРОНІКИ
ВІДДІЛ КАДРІВ №1
№02071197

О.І. Січевич

РЕЦЕНЗІЯ

на освітньо-професійну програму «Кібербезпека у фінансових технологіях» та навчальний план спеціальності 125 «Кібербезпека» першого (бакалаврського) ступеня вищої освіти навчально-наукового інституту «Каразінський банківський інститут» Харківського національного університету імені В. Н. Каразіна

Сучасний стан розвитку інформаційних технологій та автоматизації всіх сфер діяльності суспільства в Україні та світі обумовлює потребу у підготовці висококваліфікованих фахівців, здатних не лише забезпечити проектування, розроблення й функціонування інформаційно-комунікаційних систем та сервісів, а й спроможних забезпечити належний рівень їх кібербезпеки.

Рецензована освітньо-професійна програма «Кібербезпека у фінансових технологіях» розроблена колективом кафедри інформаційних технологій та математичного моделювання навчально-наукового інституту «Каразінський банківський інститут» (керівник проектної групи – гарант освітньої програми – кандидат технічних наук, доцент Кобилін А. М.) із залученням потенційних роботодавців, що сприяє всебічному урахуванню вимог та потреб ринку праці в галузі інформаційної безпеки фінансово-кредитних установ.

Освітньо-професійна програма «Кібербезпека у фінансових технологіях» містить профіль освітньо-професійної програми, перелік обов'язкових та вибіркових компонент, матрицю відповідності програмних компетентностей компонентам освітньо-професійної програми, матрицю забезпечення програмних результатів навчання відповідним компонентам освітньо-професійної програми, а також структурно-логічну схему у вигляді міждисциплінарних зв'язків освітніх компонент.

Детальний аналіз рецензованої освітньо-професійної програми «Кібербезпека у фінансових технологіях» показав відповідність програми стандарту вищої освіти за спеціальністю 125 «Кібербезпека». Освітні компоненти програми спрямовані на підготовку висококваліфікованого фахівця з урахуванням загальних тенденцій галузі інформаційних технологій з точки зору кібербезпеки, особливостей спеціальності та специфіки фінансово-кредитної сфери.

Навчальний план підготовки бакалаврів спеціальності 125 «Кібербезпека» повністю відповідає завданням та змісту освітньо-професійної програми. Пропонована послідовність вивчення дисциплін та графік навчального процесу забезпечують відповідність програмних результатів навчання сучасним вимогам потенційних роботодавців.

Вважаю, що освітньо-професійна програма «Кібербезпека у фінансових технологіях» підготовки здобувачів вищої освіти першого (бакалаврського) рівня вищої освіти в галузі знань 12 «Інформаційні технології» за спеціальністю 125 «Кібербезпека», розроблена навчально-науковим інститутом «Каразінський банківський інститут» Харківського національного університету імені В. Н. Каразіна, відповідає встановленим вимогам та забезпечить здобувачам фундаментальну підготовку теоретичних і практичних знань, умінь, навичок та компетентностей за спеціальністю 125 «Кібербезпека», достатніх для ефективного виконання завдань відповідного рівня професійної діяльності з інформаційних технологій та кібербезпеки, а тому може бути рекомендована до впровадження в освітній процес інституту та університету.

Рецензент
професор кафедри комп'ютерних систем,
мереж і кібербезпеки Національного
аерокосмічного університету
ім. М. Є. Жуковського
«Харківський авіаційний інститут»,
доктор технічних наук, доцент О. І. Морозова

Підпис засвідчую:
Начальник ~~Спеціаліст~~ відділу кадрів

1. Профіль освітньої програми

Кібербезпека у фінансових технологіях

зі спеціальності 125 Кібербезпека

1 – Загальна інформація	
Ступінь вищої освіти та назва кваліфікації	Бакалавр, бакалавр з кібербезпеки
Тип диплому та обсяг освітньої програми	Диплом бакалавра державного зразка 240 кредитів, термін навчання 4 роки
Офіційна назва програми	Кібербезпека у фінансових технологіях
Наявність акредитації	Рішення МОН України від 17.11.2015 р., протокол № 119). Сертифікат про акредитацію: Серія НД № 2189535 від 18.09.2017. Термін дії сертифіката до 01.07.2024 р.
Цикл/рівень	НРК України – 6 рівень, FQ-EHEA – перший цикл, EQF-LLL – 6 рівень
Передумови	Особа має право здобувати ступінь бакалавра за умови наявності в неї повної загальної середньої освіти або ступеня «молодший бакалавр» (освітньо-кваліфікаційного рівня «молодший спеціаліст»). Прийом на навчання для здобуття вищої освіти за першим (бакалаврським) рівнем за освітньо-професійною програмою «Кібербезпека у фінансових технологіях» здійснюється на конкурсній основі відповідно до «Правил прийому на навчання до Харківського національного університету імені В.Н. Каразіна»
Мова викладання	українська
Термін дії освітньої програми	10 років
Інтернет-адреса постійного розміщення опису освітньої програми	http://kbi.karazin.ua
2 - Мета освітньої програми	
Мета програми	Підготовка фахівців, здатних використовувати і впроваджувати технології інформаційної та/або кібербезпеки для фінансових технологій

3 – Характеристика освітньої програми	
Предметна область (галузь знань, спеціальність, спеціалізація (за наявності)	12 Інформаційні технології, 125 Кібербезпека
Орієнтація освітньої 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»)
Основний фокус освітньої програми та спеціалізації	технології інформаційної та/або кібербезпеки для фінансових технологій
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.
4 – Придатність випускників до працевлаштування та подальшого навчання	
Придатність до працевлаштування	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
Подальше навчання	Можливість продовжити навчання за освітньою програмою ступеня магістра. Набуття додаткових кваліфікацій в системі післядипломної освіти
5 – Викладання та оцінювання	
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
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
6 – Програмні компетентності	
Інтегральна компетентність	здатність розв’язувати складні спеціалізовані задачі та практичні проблеми у галузі забезпечення інформаційної безпеки і\або кібербезпеки, що характеризується комплексністю та неповною визначеністю умов
Загальні компетентності	
КЗ 1	здатність застосовувати знання у практичних ситуаціях
КЗ 2	знання та розуміння предметної області та розуміння професії
КЗ 3	здатність професійно спілкуватися державною та іноземною мовами як усно, так і письмово
КЗ 4	вміння виявляти, ставити та вирішувати проблеми за професійним спрямуванням
КЗ 5	здатність до пошуку, оброблення та аналізу інформації
КЗ 6	здатність реалізувати свої права і обов’язки як члена суспільства, усвідомлювати цінності громадянського (вільного демократичного) суспільства та необхідність його сталого розвитку, верховенства права, прав і свобод людини і громадянина в Україні
КЗ 7	здатність зберігати та примножувати моральні, культурні, наукові цінності і досягнення суспільства на основі розуміння історії та закономірностей розвитку предметної області, її місця у загальній системі знань про природу і суспільство та у

	розвитку суспільства, техніки і технологій, використовувати різні види та форми рухової активності для активного відпочинку та ведення здорового способу життя
Фахові компетентності	
КФ 1	здатність 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
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
7 – Програмні результати навчання	
Програмні результати навчання	
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.
8 – Ресурсне забезпечення реалізації програми	
Специфічні характеристики кадрового 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).
Специфічні характеристики матеріально-технічного забезпечення	Сучасне інформаційно-комунікаційне обладнання, інформаційні системи та програмні продукти, що застосовують при розробці, впроваджені, експлуатації та забезпеченні кібербезпеки

	інформаційних систем та технологій.
Специфічні характеристики інформаційного та навчально-методичного 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. Навчально-методичного 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
9 – Академічна мобільність	
Національна кредитна мобільність	З вітчизняними ЗВО на основі двосторонніх договорів.
Міжнародна кредитна мобільність	На основі угоди про співробітництво у рамках Програми «Еразмус+»; Університети - партнери, з якими співпрацює Харківський національний університет імені В. Н. Каразіна за програмою подвійного диплому
Навчання іноземних здобувачів вищої освіти	Не передбачено

2. Перелік компонент освітньо-професійної /наукової програми та їх логічна послідовність

2.1 Перелік компонент ОП

Код н/д	Компоненти освітньої програми (навчальні дисципліни, курсові проекти (роботи), практики, кваліфікаційна робота)	Кількість кредитів (семестр)	Форма підсумкового контролю
1	2	3	4
Обов'язкові компоненти ОП			
Блок «Загальна підготовка»			
ОК 1.	Іноземна мова	6 (1,2)	залік, екзамен
ОК 2.	Іноземна мова за фахом	3 (8)	залік
ОК 3.	Історія України	3 (1)	екзамен
ОК 4	Філософія	3 (4)	екзамен
ОК 5	Банківська студія "Тайм-менеджмент та міжособистісні комунікації в бізнесі"	5 (1)	залік
ОК 6	Банківська студія «Банківська система»	3 (2)	залік
ОК 7	Вступ до фаху	3 (1)	залік
ОК 8	Інформаційні технології	6 (1)	екзамен
Блок «Галузева підготовка»			
ОК 9	Вища математика	12 (1, 2)	залік, екзамен
ОК 10	Дискретна математика	9 (1, 2)	залік, екзамен
ОК 11	Основи алгоритмізації та програмування	6 (2)	екзамен
ОК 12	Алгебра і теорія чисел	4 (2)	залік
ОК 13	Теорія ймовірностей та математична статистика	7 (3, 4)	залік, екзамен
ОК 14	Об'єктно-орієнтоване програмування	5 (3)	екзамен, курсова робота
ОК 15	Спеціальні розділи математики	4 (3)	залік
ОК 16	Алгоритми та структури даних	3 (3)	залік
ОК 17	Комп'ютерна схемотехніка та архітектура комп'ютерів	5 (3)	екзамен
ОК 18	Операційні системи	5 (4)	екзамен
ОК 19	Комп'ютерні системи та мережі	5 (5)	екзамен, курсова робота
ОК 20	Фізика та електротехніка	5 (5)	екзамен
ОК 21	Цифрова економіка	5 (5)	залік
ОК 22	Технологія створення програмних продуктів	4 (6)	залік
ОК 23	Методи та системи штучного інтелекту	5 (8)	екзамен
Блок «Фахова підготовка»			
ОК 24	Основи кібербезпеки	3 (2)	залік
ОК 25	Теорія інформації та кодування	5 (4)	залік
ОК 26	Прикладна криптологія	7 (6,7)	залік, екзамен
ОК 27	Безпека комп'ютерних мереж	4 (6)	екзамен
ОК 28	Великі дані в захисті інформації	5 (6)	екзамен
ОК 29	Комплексні системи захисту інформації	4 (5)	екзамен
ОК 30	Управління інформаційною безпекою	4 (7)	залік
ОК 31	Технічний захист інформації	5 (7)	екзамен, курсова робота

ОК 32	Стеганографія	5 (7)	екзамен
ОК 33	Система стандартів та нормативне забезпечення захисту інформації	5 (8)	залік
ОК 34	Навчальна практика – проектно-технологічна (без відриву)	6 (6)	залік
ОК 35	Виробнича практика	6 (8)	залік
ОК 36	Кваліфікаційна бакалаврська робота	5 (8)	
Загальний обсяг обов'язкових компонент		**180**	
Вибіркові компоненти ОП*			
ВК 1.	Міжфакультетська вибіркова дисципліна 1	3 (3)	залік
ВК 2.	Міжфакультетська вибіркова дисципліна 2	3 (4)	залік
ВК 3.	Міжфакультетська вибіркова дисципліна 3	3 (5)	залік
ВК 4.	Міжфакультетська вибіркова дисципліна 4	3 (6)	залік
Блок «Галузева підготовка»			
ВК 5	Чисельні методи / Чисельний аналіз та наукові обчислення	6 (4)	залік
ВК 6	Комп'ютерна графіка та веб-дизайн /Веб-програмування	4 (5)	екзамен
Блок «Фахова підготовка»			
ВК 7	Економіко-математичні методи та моделі / Методи та моделі в економіці	6 (3)	екзамен
ВК 8	Організація баз даних та знань / Структури знань та даних	5 (4)	залік, курсова робота
ВК 9	Безпека банківських систем/ Безпека фінансових технологій	4 (5)	залік
ВК 10	Системний аналіз і теорія прийняття рішень / Системотехнічні методи в інформаційних технологіях / Теорія та практика системного прийняття рішень	4 (6)	залік
ВК 11	Проектування інформаційних систем безпеки/Проектування засобів безпеки ІС	4 (7)	залік
ВК 12	Моделювання бізнес-процесів безпеки/ Бізнес-інжиніринг інформаційних систем	6 (7)	екзамен
ВК 13	Цифрова криміналістика / Основи протидії кіберзлочинності та цифрова криміналістика	4 (7)	залік
ВК 14	Адміністрування та моніторинг комп'ютерних систем / Організація та проведення тестування на проникнення та соціальна інженерія	5 (8)	екзамен
Загальний обсяг вибіркових компонент		**60**	
ЗАГАЛЬНИЙ ОБСЯГ ОСВІТНЬОЇ ПРОГРАМИ		**240**	

***** Кодування навчальних дисциплін відбудеться в наступному порядку:

ОК – компонента (навчальна дисципліна), що є обов'язковою до вивчення;

ВК – компонента (навчальна дисципліна), що обирається за вибором студента з групи навчальних дисциплін для формування власної спеціалізації ;

ПК – компонента блоку «Практична підготовка» , що є обов'язковою до виконання.

2.2 Структурно-логічна схема ОП

Таблиця 2.2.1. Міждисциплінарні зв'язки освітніх компонент освітньо-професійної програми

Семестр	Код КОП	Компоненти освітньої програми	Передумови вивчення	Є базою для вивчення
	1	2	3	4
1,2	ОК 1.	Іноземна мова		ОК 2
8	ОК 2.	Іноземна мова за фахом	ОК 1	
1	ОК 3.	Історія України		
4	ОК 4	Філософія		
1	ОК 5	Банківська студія "Тайм-менеджмент та міжособистісні комунікації в бізнесі"		ОК 21
2	ОК 6	Банківська студія «Банківська система»	ОК 8	ОК 21
1	ОК 7	Вступ до фаху		ОК 11, ОК 17, ОК 18, ОК 19, ОК 24
1	ОК 8	Інформаційні технології		ОК 6, ОК 11, ОК 13, ОК 14, ОК 16, ОК 17, ОК 18, ОК 19, ОК 21, ОК 22, ОК 24, ВК 6, ВК 7, ВК 8
1, 2	ОК 9	Вища математика		ОК 12, ОК 13, ОК 14, ОК 15, ОК 16, ОК 17, ОК 20, ВК 5, ВК 7
1, 2	ОК 10	Дискретна математика	ОК 9,	ОК 11, ОК 12, ОК 13, ОК 14, ОК 16, ОК 17, ОК 23, ОК 24, ОК 28, ВК 8, ВК 10
2	ОК 11	Основи алгоритмізації та програмування	ОК 7, ОК 8, ОК 9, ОК 10	ОК 14, ОК 16, ВК 6
2	ОК 12	Алгебра і теорія чисел	ОК 9, ОК 10	ОК 13, ОК 15, ОК 16, ВК 5
3, 4	ОК 13	Теорія ймовірностей та математична статистика	ОК 8, ОК 9, ОК 10, ОК 12	ОК 21, ОК 28, ВК 7, ВК 10, ВК 12

3	ОК 14	Об’єктно-орієнтоване програмування	ОК 8, ОК 9, ОК 10, ОК 11, ОК 16	ОК 22, ВК 6, ВК 8
3	ОК 15	Спеціальні розділи математики	ОК 9, ОК 10, ОК 12	ОК 23
3	ОК 16	Алгоритми та структури даних	ОК 8, ОК 9, ОК 10, ОК 11, ОК 12	ОК 14, ОК 17, ОК 22, ОК 23, ВК 6, ВК 8, ВК 11,
3	ОК 17	Комп'ютерна схемотехніка та архітектура комп'ютерів	ОК 7, ОК 8, ОК 9, ОК 10, ОК 16	ОК 18, ОК 19, ОК 20, ОК 27, ВК 14
4	ОК 18	Операційні системи	ОК 7, ОК 8, ОК 17	ОК 19, ВК 14
5	ОК 19	Комп’ютерні системи та мережі	ОК 7, ОК 8, ОК 17, ОК 18	ОК 27, ОК 28, ОК 29, ОК 33, ВК 11
5	ОК 20	Фізика та електротехніка	ОК 9, ОК 17, ВК 5	ОК 27, ОК 29, ОК 31
5	ОК 21	Цифрова економіка	ОК 5, ОК 6, ОК 8, ОК 13	ОК 28, ВК 12
6	ОК 22	Технологія створення програмних продуктів	ОК 8, ОК 14, ОК 16	ОК 33, ВК 11, ВК 12
8	ОК 23	Методи та системи штучного інтелекту	ОК 15, ОК 16, ОК 28, ВК 5, ВК 7, ВК 12	
2	ОК 24	Основи кібербезпеки	ОК 7, ОК 8, ОК 10	ОК 25, ОК 26, ОК 27, ОК 29, ОК 30, ОК 31, ОК 32, ОК 33, ВК 11, ВК 14
4	ОК 25	Теорія інформації та кодування	ОК 24	ВК 13
6,7	ОК 26	Прикладна криптологія	ОК 24	ВК 13
6	ОК 27	Безпека комп'ютерних мереж	ОК 17, ОК 19, ОК 24, ОК 29	ОК 30, ОК 31, ВК 13, ВК 14
6	ОК 28	Великі дані в захисті інформації	ОК 13, ОК 19, ОК 21	ОК 23
5	ОК 29	Комплексні системи захисту інформації	ОК 19, ОК 24,	ОК 27, ВК 9, ВК 11, ВК 12, ВК 13, ВК 14
7	ОК 30	Управління інформаційною безпекою	ОК 24, ОК 27	ВК 14

7	ОК 31	Технічний захист інформації	ОК 24, ОК 27	ВК 14
7	ОК 32	Стеганографія	ОК 24	
8	ОК 33	Система стандартів та нормативне забезпечення захисту інформації	ОК 19, ОК 22, ОК 24	
4	ВК 5	Чисельні методи / Чисельний аналіз та наукові обчислення	ОК 9, ОК 10, ОК 12, ОК 12, ОК 13, ОК 15	ОК 20, ОК 23, ВК 10
5	ВК 6	Комп'ютерна графіка та веб-дизайн /Веб-програмування	ОК 8, ОК 11, ОК 14, ОК 16	
3	ВК 7	Економіко-математичні методи та моделі / Методи та моделі в економіці	ОК 8, ОК 9, ОК 13	ВК 10, ОК 23
4	ВК 8	Організація баз даних та знань / Структури знань та даних	ОК 8, ОК 14, ОК 16	ВК 11
5	ВК 9	Безпека банківських систем/ безпека фінансових технологій	ОК 29,	ВК 14
6	ВК 10	Системний аналіз і теорія прийняття рішень / Системотехнічні методи в інформаційних технологіях / Теорія та практика системного прийняття рішень	ОК 10, ОК 13, ВК 5, ВК 7	ВК 11,
7	ВК 11	Проектування інформаційних систем безпеки/Проектування засобів безпеки ІС	ОК 16, ОК 19, ОК 22, ОК 24, ОК 29, ВК 10, ВК 8	ВК 14
7	ВК 12	Моделювання бізнес-процесів безпеки/ Бізнес-інжиніринг інформаційних систем	ОК 13, ОК 21, ОК 22, ОК 29	ОК 23, ВК 14
7	ВК 13	Цифрова криміналістика / Основи протидії кіберзлочинності та цифрова криміналістика	ОК 25, ОК 26, ОК 27, ОК 29	ВК 14
8	ВК 14	Адміністрування та моніторинг комп'ютерних	ОК 17, ОК 24, ОК 27, ОК 29, ОК 30,	

		систем / Організація та проведення тестування на проникнення та соціальна інженерія	ОК 31, ВК 9, ВК 11, ВК 12	

3. Форма атестації здобувачів вищої освіти

Атестація здійснюється у формі:	Атестація здійснюється у формі публічного захисту кваліфікаційної бакалаврський роботи та за рішенням закладу вищої освіти кваліфікаційного іспиту. 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)	Кваліфікаційна бакалаврська 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).

4. Матриця відповідності програмних компетентностей компонентам освітньої програми

Таблиця 4.1.

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
ОК 1			+																				
ОК 2			+																				
ОК 3						+	+																
ОК 4		+		+		+	+																
ОК 5		+		+	+		+																+
ОК 6		+				+	+	+															+
ОК 7																							
ОК 8	+			+	+				+										+				
ОК 9	+	+		+	+		+		+	+		+					+		+				
ОК 10	+	+			+		+										+						
ОК 11	+	+		+	+	+		+	+	+	+	+		+			+		+		+		+
ОК 12	+	+			+				+								+						
ОК 13	+	+			+				+				+		+		+		+				+
ОК 14	+	+	+	+			+		+	+		+					+		+	+			+
ОК 15	+	+			+				+								+						
ОК 16	+	+		+	+	+		+	+	+	+	+		+			+		+		+		+
ОК 17	+	+	+	+	+				+	+	+								+				+
ОК 18	+	+		+					+	+	+	+	+			+	+	+		+	+	+	+
ОК 19	+			+	+			+	+	+	+	+	+		+	+	+		+	+	+	+	+
ОК 20	+			+				+	+								+		+				
ОК 21	+	+							+		+												+
ОК 22	+	+		+		+		+	+	+	+	+		+			+		+	+			+
ОК 23	+			+	+				+	+							+		+		+		
ОК 24	+	+		+		+		+	+			+		+					+	+	+		+
ОК 25										+		+					+						
ОК 26																	+						
ОК 27	+	+		+					+	+	+	+	+				+			+	+		+
ОК 28					+						+	+											
ОК 29	+	+		+					+	+		+	+	+		+	+		+	+	+		+
ОК 30												+			+	+							
ОК 31																	+		+				
ОК 32																		+					
ОК 33	+	+		+	+	+		+		+	+			+			+		+				

Продовження таблиці 4.1

	КЗ1	КЗ2	КЗ3	КЗ4	КЗ5	КЗ6	КЗ7	КФ1	КФ2	КФ3	КФ4	КФ5	КФ6	КФ7	КФ8	КФ9	КФ10	КФ11	КФ12	КФД1	КФД2	КФД3	КФД4
ОК 34	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+
ОК 35	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+
ОК 36	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+
ВК 5	+	+		+	+			+	+	+		+		+			+		+		+		+
ВК 6	+		+	+				+						+		+		+			+		+
ВК 7	+	+		+	+				+	+	+				+				+				+
ВК 8	+	+		+	+				+		+	+	+	+				+	+	+	+		+
ВК 9										+		+											
ВК 10	+	+		+		+		+	+	+		+		+	+	+			+	+	+	+	+
ВК 11	+	+		+	+				+	+	+	+	+	+	+		+	+	+		+		+
ВК 12	+	+	+	+	+	+	+	+	+		+	+		+	+		+	+	+		+		+
ВК 13	+			+					+	+					+	+	+	+	+		+	+	+
ВК 14	+			+	+				+	+	+	+	+					+	+	+	+	+	+

5. Матриця забезпечення програмних результатів навчання (ПРН) відповідними компонентами освітньої програми

Таблиця 5.1.

	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
ОК 1	Іноземна мова	+																										
ОК 2	Іноземна мова за фахом	+																										
ОК 3	Історія України							+																				
ОК 4	Філософія																+											
ОК 5	Банківська студія "Тайм-менеджмент та міжособистісні комунікації в бізнесі"		+	+		+	+																					
ОК 6	Банківська студія «Банківська система»		+				+											+										
ОК 7	Вступ до фаху		+					+											+		+							
ОК 8	Інформаційні технології											+		+														
ОК 9	Вища математика		+	+	+		+																					
ОК 10	Дискретна математика		+	+	+		+				+																	
ОК 11	Основи алгоритмізації та програмування							+	+		+			+			+						+					
ОК 12	Алгебра і теорія чисел		+	+																								
ОК 13	Теорія ймовірностей та математична статистика		+	+	+		+							+														
ОК 14	Об’єктно-орієнтоване програмування	+					+					+								+		+						
ОК 15	Спеціальні розділи математики		+	+	+																							
ОК 16	Алгоритми та структури даних							+	+		+			+			+						+					
ОК 17	Комп'ютерна схемотехніка та архітектура комп'ютерів	+	+								+																	
ОК 18	Операційні системи											+							+			+	+	+	+		+	+
ОК 19	Комп’ютерні системи та мережі										+	+		+		+		+	+	+				+	+		+	+
ОК 20	Фізика та електротехніка								+							+									+			
ОК 21	Цифрова економіка		+															+										
ОК 22	Технологія створення програмних продуктів							+												+		+						
ОК 23	Методи та системи штучного інтелекту			+									+															
ОК 24	Основи кібербезпеки							+	+			+										+	+					+
ОК 25	Теорія інформації та кодування																				+				+			

Продовження таблиці 5.1

	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
ОК 26	Прикладна криптологія				+		+																					+
ОК 27	Безпека комп'ютерних мереж																							+			+	+
ОК 28	Великі дані в захисті інформації			+																								
ОК 29	Комплексні системи захисту інформації														+		+										+	+
ОК 30	Управління інформаційною безпекою			+		+		+																				
ОК 31	Технічний захист інформації														+				+	+	+							
ОК 32	Стеганографія				+						+		+															
ОК 33	Система стандартів та нормативне забезпечення захисту інформації							+	+	+							+											
ОК 34	Навчальна практика – проектно-технологічна	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+
ОК 35	Виробнича практика	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+
ОК 36	Кваліфікаційна бакалаврська робота	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+
ВК 5	Чисельні методи / Чисельний аналіз та наукові обчислення			+					+		+		+				+						+		+			
ВК 6	Комп'ютерна графіка та веб-дизайн /Веб-програмування	+								+															+	+	+	
ВК 7	Економіко-математичні методи та моделі / Методи та моделі в економіці		+	+	+	+							+		+										+			
ВК 8	Організація баз даних та знань / Структури знань та даних				+								+		+					+			+		+	+		+
ВК 9	Безпека банківських систем/ безпека фінансових технологій		+					+	+	+					+		+					+						
ВК 10	Системний аналіз і теорія прийняття рішень / Системотехнічні методи в інформаційних технологіях / Теорія та практика системного прийняття рішень			+					+		+		+				+						+		+			
ВК 11	Проектування інформаційних систем безпеки/Проектування засобів безпеки ІС				+	+					+			+		+			+				+					
ВК 12	Моделювання бізнес-процесів безпеки/ Бізнес-інжиніринг інформаційних систем		+		+ +						+	+										+	+					
ВК 13	Цифрова криміналістика / Основи протидії кіберзлочинності та цифрова криміналістика														+				+									
ВК 14	Адміністрування та моніторинг комп'ютерних систем / Організація та проведення тестування на проникнення та соціальна інженерія													+		+			+		+		+			+		

Продовження таблиці 5.1

	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
ОК 1.	Іноземна мова																											
ОК 2.	Іноземна мова за фахом																											
ОК 3.	Історія України																											+
ОК 4	Філософія																											+
ОК 5	Банківська студія "Тайм-менеджмент та міжособистісні комунікації в бізнесі"																											+
ОК 6	Банківська студія «Банківська система»																											
ОК 7	Вступ до фаху																											+
ОК 8	Інформаційні технології											+		+														
ОК 9	Вища математика																			+								
ОК 10	Дискретна математика																				+							
ОК 11	Основи алгоритмізації та програмування						+																					
ОК 12	Алгебра і теорія чисел				+																+	+						
ОК 13	Теорія ймовірностей та математична статистика																											
ОК 14	Об’єктно-орієнтоване програмування													+										+				
ОК 15	Спеціальні розділи математики																			+								
ОК 16	Алгоритми та структури даних						+																					
ОК 17	Комп'ютерна схемотехніка та архітектура комп'ютерів																											
ОК 18	Операційні системи						+														+							
ОК 19	Комп’ютерні системи та мережі			+	+	+					+	+				+		+		+	+	+		+				
ОК 20	Фізика та електротехніка									+																		

Продовження таблиці 5.1

	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
ОК 21	Цифрова економіка																											
ОК 22	Технологія створення програмних продуктів		+				+		+	+																		
ОК 23	Методи та системи штучного інтелекту													+						+			+			+		
ОК 24	Основи кібербезпеки								+			+																
ОК 25	Теорія інформації та кодування				+																+	+		+				
ОК 26	Прикладна криптологія				+			+		+						+				+	+	+						
ОК 27	Безпека комп'ютерних мереж		+																		+							
ОК 28	Великі дані в захисті інформації																		+									
ОК 29	Комплексні системи захисту інформації					+		+	+			+		+				+		+								
ОК 30	Управління інформаційною безпекою	+		+		+									+			+					+			+		
ОК 31	Технічний захист інформації				+					+		+	+	+										+				
ОК 32	Стеганографія							+													+							
ОК 33	Система стандартів та нормативне забезпечення захисту інформації										+		+	+			+	+										
ОК 34	Навчальна практика – проектно-технологічна	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+
ОК 35	Виробнича практика	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+
ОК 36	Кваліфікаційна бакалаврська робота	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+
ВК 5	Чисельні методи / Чисельний аналіз та наукові обчислення																											
ВК 6	Комп’ютерна графіка та веб-дизайн /Веб-програмування																									+		
ВК 7	Економіко-математичні методи та моделі / Методи та моделі в економіці						+													+								
ВК 8	Організація баз даних та знань / Структури знань та даних																									+		
ВК 9	Безпека банківських систем/ безпека фінансових технологій												+				+		+	+								
ВК 10	Системний аналіз і теорія прийняття рішень / Системотехнічні методи в інформаційних технологіях / Теорія та практика системного прийняття рішень				+		+		+			+							+	+								
ВК 11	Проектування інформаційних систем безпеки/Проектування засобів безпеки ІС							+															+					
ВК 12	Моделювання бізнес-процесів безпеки/ Бізнес-інжиніринг інформаційних систем						+																+					

Продовження таблиці 5.1

	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
ВК 13	Цифрова криміналістика / Основи протидії кіберзлочинності та цифрова криміналістика		+										+			+											
ВК 14	Адміністрування та моніторинг комп'ютерних систем / Організація та проведення тестування на проникнення та соціальна інженерія		+	+	+	+															+		+			+		

6. Матриця відповідності визначених результатів навчання та компетентностей

Таблиця 6.1.

Програмні результати навчання	Інтегральна 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	КФД3	КФД4
РН1				+																				
РН2	+		+																					+
РН3						+																		
РН4		+	+		+	+																		
РН5												+												
РН6	+		+					+																
РН7							+		+															
РН8		+							+															
РН9		+							+															
РН10		+																						
РН11		+																						
РН12		+								+										+				
РН13	+	+			+	+				+										+				
РН14	+	+								+	+													+
РН15										+														
РН16			+		+						+				+									
РН17		+								+														

Продовження таблиці 6.1

	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		+			+											+	+					+		+

Продовження таблиці 6.1

	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	КФД3	КФД4
РН43			+			+			+															
РН44	+	+										+												
РН45													+											
РН46		+			+					+														
РН47	+	+	+							+	+							+			+			
РН48		+															+							
РН49		+																	+					
РН50											+													
РН51											+													
РН52		+			+														+					
РН53		+			+	+															+	+	+	+
РН54							+	+																

Додаток

Зведена таблиця фахових компетентностей та результатів навчання (за Стандартом).

Фахові компетентності	Результати навчання
КФ 1. Здатність застосовувати законодавчу та нормативноправову базу, а також державні та міжнародні вимоги, практики і стандарти з метою здійснення професійної діяльності в галузі інформаційної та/або кібербезпеки.	- готувати пропозиції до нормативних актів і документів з метою забезпечення встановленої політики інформаційної безпеки і \або кібербезпеки; - розробляти проектну документацію, щодо програмних та програмно-апаратних комплексів захисту інформаційних, інформаційно-телекомунікаційних (автоматизованих) систем; - виконувати аналіз реалізації прийнятої політики інформаційної і /або кібербезпеки.
КФ 2. Здатність до використання інформаційнокомунікаційних технологій, сучасних методів і моделей інформаційної та/або кібербезпеки.	- здійснювати професійну діяльність на основі знань сучасних інформаційно-комунікаційних технологій; -розробляти та аналізувати проекти інформаційнотелекомунікаційних систем базуючись на стандартизованих технологіях та протоколах передачі даних; -застосовувати в професійній діяльності знання, навички та практики, щодо структур сучасних обчислювальних систем, методів і засобів обробки інформації, архітектур операційних систем; -здійснювати захист ресурсів і процесів в інформаційнотелекомунікаційних системах на основі моделей безпеки (кінцевих автоматів, управління потоками, *Bell-LaPadula, Biba, Clark-Wilson*, та інші), а також встановлених режимів безпечного функціонування інформаційнотелекомунікаційних системах; - виконувати аналіз програмного забезпечення з метою оцінки на відповідність встановленим вимогам інформаційної і\або кібербезпеки в інформаційнотелекомунікаційних системах.
КФ 3. Здатність до використання програмних та програмно-апаратних комплексів засобів захисту інформації в інформаційнотелекомунікаційних (автоматизованих) системах	-забезпечувати процеси захисту інформаційнотелекомунікаційних (автоматизованих) систем шляхом встановлення та коректної експлуатації програмних та програмно-апаратних комплексів засобів захисту; - забезпечувати функціонування спеціального програмного забезпечення, щодо захисту даних від руйнуючих програмних впливів, руйнуючих кодів в інформаційних, інформаційно-телекомунікаційних (автоматизованих) системах; - виконувати розробку експлуатаційної документації на комплексів засобів захисту.
КФ 4. Здатність забезпечувати неперервність бізнесу згідно встановленої політики інформаційної та/або	- вирішувати задачі супроводу (в.т. числі: огляд, тестування, підзвітність) системи управління доступом згідно принципів, критеріїв доступу та встановленої політики безпеки в інформаційних та

кібербезпеки.	інформаційно-телекомунікаційних (автоматизованих) системах; - реалізовувати заходи з протидії отриманню несанкціонованого доступу до інформаційних ресурсів і процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах; - вирішувати задачі управління доступом до інформаційних ресурсів та процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах на основі моделей управління доступом (мандатних, дискреційних, рольових); - вирішувати задачі централізованого і децентралізованого адміністрування доступом до інформаційних ресурсів і процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) систем; - забезпечувати введення підзвітності системи управління доступом інформаційних ресурсів і процесів в інформаційно-телекомунікаційних системах.
КФ 5 Здатність забезпечувати захист інформації, що обробляється в інформаційнотелекомунікаційних (автоматизованих) системах з метою реалізації встановленої політики інформаційної та/або кібербезпеки.	- обирати основні методи та засоби захисту інформації відповідно до вимог сучасних стандартів інформаційної та/або кібербезпеки, та критеріїв безпеки інформаційних технологій, застосовуючи системний підхід та знання основ теорії захисту інформації; - вирішувати задачі управління процедурами ідентифікації, автентифікації, авторизації, користувачів і процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах; - проектувати та реалізувати комплексні системи захисту інформації в автоматизованих системах організації (підприємства) відповідно до вимог нормативних документів системи технічного захисту інформації; -вирішувати задачі захисту потоків даних в інформаційних, інформаційно-телекомунікаційних (автоматизованих) системах; - визначати рівень захищеності інформаційних ресурсів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах; -використовувати інструментальні засоби оцінювання можливості реалізації потенційних загроз інформації, що обробляється в інформаційно-телекомунікаційних (автоматизованих) системах.
КФ 6. Здатність відновлювати штатне функціонування інформаційних,	-вирішувати задачі управління процесами забезпечення безперервності бізнесу з використанням процедур резервування

інформаційнотелекомунікаційних (автоматизованих) систем після реалізації загроз, здійснення кібератак, збоїв та відмов різних класів та походження.	програмного забезпечення та безпосередньо інформаційних ресурсів; -вирішувати задачі корекції цілей, стратегій, планів забезпечення безперервності бізнес процесів після здійснення кібератак, збоїв та відмов різних класів. -створювати і впроваджувати плани процесу забезпечення безперервності бізнесу; - виконувати аналіз налаштувань елементів інформаційних систем та комунікаційного обладнання
КФ 7. Здатність впроваджувати та забезпечувати функціонування комплексних систем захисту інформації (комплекси нормативноправових, організаційних та технічних засобів і методів, процедур, практичних прийомів та ін.)	- вирішувати задачі супроводу та впровадження комплексних систем захисту інформації, а також протидії несанкціонованому доступу до ресурсів і процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах; -здійснювати оцінку рівня захищеності інформації що обробляється в інформаційно-телекомунікаційних системах використовувати інструментальні засоби оцінювання наявності потенційних вразливостей; - вирішувати задачі управління комплексною системою захисту інформації в інформаційних та інформаційно-телекомунікаційних (автоматизованих); - вирішувати задачі експертизи, випробування комплексних систем захисту інформації.
КФ 8. Здатність здійснювати процедури управління інцидентами, проводити розслідування, надавати їм оцінку.	- вирішувати задачі попередження та виявлення, ідентифікації, аналізу та реагування на інциденти в інформаційних, інформаційно-телекомунікаційних (автоматизованих) системах; - проводити розслідування інцидентів інформаційної безпеки та/або кібербезпеки базуючись на національних та міжнародних регулюючих актах, процедурах та положеннях в сфері інформаційної безпеки та/або кібербезпеки; - забезпечувати дотримання політики ведення журналів реєстрації подій та інцидентів з встановленим рівнем деталізації
КФ 9. Здатність здійснювати професійну діяльність на основі впровадженої системи управління інформаційною та/або кібербезпекою.	- забезпечувати безперервність бізнес процесів організації на базі теорії ризиків та системи управління інформаційною безпекою, згідно вітчизняних та міжнародних вимог і стандартів; -забезпечувати функціонування системи управління інформаційною та\або кібербезпекою організації на основі керування інформаційними ризиками, здійснення процедур їх кількісного і якісного оцінки
КФ 10. Здатність застосовувати методи та засоби криптографічного та технічного захисту інформації на об’єктах	- аналізувати та визначати можливість застосування технологій, методів та засобів криптографічного захисту інформації; - аналізувати та визначати можливість

інформаційної діяльності.	застосування технологій, методів та засобів технічного захисту інформації; - виявляти небезпечні сигнали технічних засобів; - вимірювати параметри небезпечних та завадових сигналів під час інструментального контролю захищеності інформації від витоку технічними каналами; - визначати ефективність захисту інформації від витоку технічними каналами відповідно до вимог нормативних документів системи технічного захисту інформації; - інтерпретувати результати проведення спеціальних вимірювань з використанням технічних засобів, контролю характеристик інформаційно-телекомунікаційних систем відповідно до вимог нормативних документів системи технічного захисту інформації; – обґрунтовувати можливість створення технічних каналів витоку інформації на об'єктах інформаційної діяльності; – впроваджувати заходи та засоби технічного захисту інформації від витоку технічними каналами
КФ 11. Здатність виконувати моніторинг ресурсів і процесів функціонування, інформаційнотелекомунікаційних (автоматизованих) систем згідно встановленої політики інформаційної та/або кібербезпеки.	- забезпечувати процеси моніторингу доступу до ресурсів і процесів інформаційно-телекомунікаційних систем; -забезпечувати конфігурування та функціонування систем моніторингу ресурсів та процесів в інформаційно-телекомунікаційних системах
КФ 12. Здатність аналізувати, виявляти та оцінювати можливі загрози, уразливості та дестабілізуючі чинники інформаційному простору та інформаційним ресурсам згідно встановленої політики інформаційної та/або кібербезпеки.	- виконувати впровадження та підтримку систем виявлення вторгнень та використовувати комплекси захисту для забезпечення необхідного рівня захищеності інформації в інформаційних, інформаційно-телекомунікаційних (автоматизованих) системах; - аналізувати ефективність систем виявлення та протидії несанкціонованому доступу до ресурсів і процесів в інформаційно-телекомунікаційних системах; - аналізувати та впроваджувати системи захисту від зловмисних програмних кодів.

Гарант освітньої програми, к.т.н., доцент **Анатолій КОБИЛІН**