Міністерство освіти і науки України

Харківський національний університет імені В.Н. Каразіна

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

Кібербезпека у фінансових технологіях
(назва програми)

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

Галузь знань 12 Інформаційні технології
(код, назва галузі)

Спеціальність 125 Кібербезпека та захист інформації
(шифр, назва спеціальності)

ЗАТВЕРДЖЕНО
Вченою радою
Харківського національного університету
імені В.Н. Каразіна
«29» 05 2023 року,
протокол № 9
Введено в дію з 2023 р.
наказом від «01» 06 2023 р.
№ 0114-1/224
Проректор з науково-педагогічної
роботи Олександр ГОЛОВКО

Харків 2023 р.

ЛИСТ ПОГОДЖЕННЯ

освітньо-професійної програми «Кібербезпека у фінансових технологіях»

Освітню програму розглянуто та схвалено:

1. Науково-методичній раді Харківського національного університету імені В.Н. Каразіна
протокол № 8 від « 16» 05 2023 р.

Голова науково-методичної ради ,
проректор з науково-педагогічної роботи _____ Олександр ГОЛОВКО

2. Вченій раді Навчально-наукового інституту «Каразінський банківський інститут»,
протокол № 13 від « 14 » квітня 2023 р.

Голова вченої ради інституту
к.ф.н., доц. _____ Анна ЧХЕАЙЛО

3. Науково-методичній комісії Навчально-наукового інституту «Каразінський банківський інститут»,
протокол № 6 від « 13 » квітня 2023 р.

Голова науково-методичної комісії інституту _____ Валерія КОЧОРБА

4. Кафедрі інформаційних технологій та математичного моделювання:
протокол № 12 від « 12 » квітня 2023 р.

Завідувачка кафедри
к.пед.н. _____ Наталя СТЯГЛИК

5. Кафедри, що забезпечують обов'язкові освітні компоненти освітньої програми

5.1. Кафедрі менеджменту, бізнесу та професійних комунікацій:
протокол № 10 від « 12 » квітня 2023 р.

Завідувачка кафедри
к.е.н., доц. _____ Надія МОРОЗОВА

5.2. . Кафедрі банківського бізнесу та фінансових технологій:
протокол № 11 від « 12 » квітня 2023 р.

Завідувачка кафедри
д.е.н., проф. _____ Галина АЗАРЕНКОВА

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		
Чеканова Наталя Миколаївна	доцент кафедри інформаційних технологій та математичного моделювання	кандидат фізико-математичних наук, доцент кафедри інформаційних технологій
Макарова Ганна Валеріївна	доцент кафедри інформаційних технологій та математичного моделювання	кандидат фізико-математичних наук, доцент кафедри вищої математики

До проекту освітньої програми долучені:

1) НПП кафедри інформаційних технологій та математичного моделювання,

2) здобувачі та випускники даної програми:

Мізюрин Валерій, Development Engineer в EPAM;

Магда Денис, Co-founder, CTO-Tokkea, Winessy;

Курочка Микита, здобувач вищої освіти;

Недзвецький Денис, здобувач вищої освіти;

Григоров Дмитро, здобувач вищої освіти, голова студентської ради інституту;

3) представники роботодавців:

Лебединська Катерина, начальник Управління фінансової безпеки Департаменту Комплаєнс контролю Ukrsibbank BNPParibas Group;

Демченко Марія, Business Control Expert INGBank Ukraine;

Столбов Володимир, начальник Регіонального управління служби безпеки АТ КБ ПриватБанк;

Галушко Володимир, Керівник сектора аналітики ДП «Прозоро. Продажі»

При розробці проекту Програми враховані вимоги:

1) Освітнього стандарту спеціальності 125 «Кібербезпека та захист інформації» 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) наказ МОН України від 28.05.2021 р. №593 «Про внесення змін до деяких стандартів вищої освіти»[Електронний ресурс]. Режим доступу:https://mon.gov.ua/storage/app/media/vishcha-osvita/zatverdzeni%20standarty/2021/06/08/Nak-593.28.05.docx;

5) Національний Класифікатор професій ДК 003:2010 [Електронний ресурс]. Режим доступу: http://dovidnyk.in.ua/directories/profesii. Зі змінами від 29.12.2022[Електронний ресурс]. Режим доступу: https://www.buhoblik.org.ua/rizni/classificator/dodatok-b.html

6) Національна рамка кваліфікацій. [Електронний ресурс]. – Режим доступу: http://zakon3.rada.gov.ua/laws/show/1341-2011-п.

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

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.

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.

Рецензована освітньо-професійна програма відповідає програмі стандарту вищої освіти за спеціальністю 125 «Кібербезпека та захист інформації». Освітні компоненти програми спрямовані на підготовку фахівця з урахуванням загальних тенденцій ІТ-галузі, особливостей спеціальності та специфіки фінансово-кредитної сфери.

Пропонована послідовність вивчення дисциплін і терміни їх вивчення забезпечують відповідність програмних результатів навчання сучасним запитам індустрії.

Освітньо-професійна програма підготовки здобувачів вищої освіти першого (бакалаврського) рівня вищої освіти в галузі знань 12 «Інформаційні технології» за спеціальністю 125 «Кібербезпека та захист інформації», розроблена навчально-науковим інститутом «Каразінський банківський інститут» ХНУ ім. В.Н.Каразіна, відповідає встановленим вимогам та забезпечить фундаментальну підготовку здобувачів освіти, оволодіння ними теоретичними й практичними знаннями, уміннями та навичками зі спеціальності, достатніх для ефективного виконання завдань відповідного рівня професійної діяльності з інформаційних технологій і інформаційної безпеки, а тому може бути рекомендована до впровадження в освітній процес

Рецензент:
Генеральний директор
Sigma Software

Дмитро Вартанян

1. ПРОФІЛЬ ОСВІТНЬОЇ ПРОГРАМИ

1 – Загальна інформація	
Повна назва закладу вищої освіти та структурного підрозділу	Харківський національний університет імені В.Н. Каразіна навчально-науковий інститут «Каразінський банківський інститут»
Офіційна назва програми	Кібербезпека у фінансових технологіях
Ступінь вищої освіти	Бакалавр
Кваліфікація, що присвоюється	Бакалавр з кібербезпеки
Тип диплому та обсяг освітньої програми	Диплом бакалавра, ОДИНИЧНИЙ Обсяг – 240 кредитів ЄКТС Термін навчання 3 роки 10 місяців
Наявність акредитації	Рішення акредитаційної комісії від 17.11.2015 протокол №119 (наказ МОН України від 30.11.2015 №1931л), сертифікат серія НД №2189535. Термін дії до 01.07.2024 р.
Передумови	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	9 років
Інтернет-адреса постійного розміщення опису освітньої програми	http://kbi.karazin.ua/osvitni-programi/
2 - Мета освітньої програми	
Мета програми	Підготовка фахівців, здатних використовувати і впроваджувати технології інформаційної та/або кібербезпеки із використанням сучасних фінансових технологій з урахуванням потреб та вимог бізнесу, зокрема у кредитно-фінансовій та банківській сферах
3 – Характеристика освітньої програми	
Предметна область (галузь знань, спеціальність)	12 Інформаційні технології, 125 Кібербезпека та захист інформації
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 («softskills»), галузевої та фахової підготовки («hardskills»)
Основний фокус освітньої програми та	Підготовка фахівців, які володіють теоретичними та практичними знаннями, сучасними інформаційно-

спеціалізації	комунікаційними технологіями, готових впроваджувати принципи та стандарти інформаційної та/або кібербезпеки в усі сфери діяльності з урахуванням потреб бізнесу, будувати ефективну стратегію цифровізації та автоматизації процесів і технологій фахової діяльності з урахуванням правил забезпечення безпеки інформаційного простору, зокрема у фінансових технологіях
Особливості програми	Програма формує фундаментальні знання та фахові навички застосуванні інформаційних технологій, фінансових технологій, експлуатації інформаційних систем (сервісів), забезпечення їх кібербезпеки. Орієнтована на глибоку спеціальну професійну підготовку сучасних фахівців у сфері кібербезпеки та фінансових технологій, ініціативних та здатних до швидкої адаптації до сучасних змін інформаційного простору. Передбачає можливості короткострокових академічних стажувань за кордоном.
4 – Придатність випускників до працевлаштування та подальшого навчання	
Придатність до працевлаштування	Працевлаштування на підприємствах і організаціях, що використовують комп'ютерну техніку та інформаційні технології (системи, мережі), будь-якої організаційно-правої форми, в яких випускники працюють у якості керівників структурних підрозділів або виконавців окремих напрямків діяльності. Випускники можуть працювати на посадах: 2139.2 Аналітик з безпеки інформаційно-комунікаційних систем 2139.2 Аналітик з оцінки вразливостей 2139.2 Аналітик загроз безпеки 2139.2 Аналітик систем захисту інформації 2139.2 Експерт з управління інформаційними технологіями 2139.2 Експерт-криміналіст (сфера кібербезпеки та захисту інформації) 2149.2 Інженер із впровадження нової техніки й технології 2139.2 Інженер із застосування комп'ютерів 1474 Менеджер (управитель) із комунікаційних технологій 4222 Офісний службовець (інформація) 2132.2 Програміст (база даних) 2132.2 Програміст прикладний 2132.2 Програміст системний 2132.2 Розробник систем захисту інформації 2139.2 Фахівець з кібердосліджень та розробок систем безпеки 2139.2 Фахівець з тестування систем захисту інформації 2139.2 Фахівець з технічного захисту інформації тощо. 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, Casestudy, 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\абокібербезпеки, 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\абокібербезпеки;
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\абокібербезпеки;
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\абокібербезпеки;
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 та захист інформації», 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	Підручники, навчальні посібники, довідкова та інша навчальна література за спеціальністю «Кібербезпека та захист інформації» у бібліотеках інституту та Університету (у тому числі в електронному вигляді). Вітчизняні та закордонні фахові періодичні видання у

забезпечення	бібліотеках за спеціальністю «Кібербезпека та захист інформації». 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. Інституційний репозитарій, який сприяє популяризації наукових здобутків інституту, підвищення його рейтингу через зростання рівня цитованості наукових праць НПП. Діюча система дистанційного навчання забезпечує самостійну та індивідуальну роботу студентів спеціальності 125 «Кібербезпека та захист інформації» освітнього ступеня бакалавр.
9 – Академічна мобільність	
Національна кредитна мобільність	Індивідуальна академічна мобільність реалізується у рамках міжуніверситетських договорів про встановлення науково-освітянських відносин для задоволення потреб розвитку освіти і науки.
Міжнародна кредитна мобільність	На основі двосторонніх договорів між Харківським національним університетом імені В.Н. Каразіна та навчальними закладами країн-партнерів.
Навчання іноземних здобувачів вищої освіти	Не передбачено

2. ПЕРЕЛІК КОМПОНЕНТ ОСВІТНЬО-ПРОФЕСІЙНОЇ 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	Форма підсумкового контролю
1	2	3	4
Обов'язкові компоненти ОП			
ОК 1.	Іноземна мова	6	залік, екзамен
ОК 2.	Іноземна мова за фахом	3	залік

ОК 3.	Історія України	3	екзамен
ОК 4	Філософія	3	екзамен
ОК 5	Банківська студія "Тайм-менеджмент та міжособистісні комунікації в бізнесі"	5	залік
ОК 6	Банківська студія «Банківська система»	3	залік
ОК 7	Вступ до фаху	3	залік
ОК 8	Інформаційні технології	6	екзамен
ОК 9	Вища математика	12	залік, екзамен
ОК 10	Дискретна математика	9	залік, екзамен
ОК 11	Основи алгоритмізації та програмування	6	екзамен
ОК 12	Алгебра і теорія чисел	4	залік
ОК 13	Теорія ймовірностей та математична статистика	7	залік, екзамен
ОК 14	Об’єктно-орієнтоване програмування	5	екзамен
ОК 15	Спеціальні розділи математики	4	залік
ОК 16	Алгоритми та структури даних	3	залік
ОК 17	Комп'ютерна схемотехніка та архітектура комп'ютерів	5	екзамен
ОК 18	Операційні системи	5	екзамен
ОК 19	Комп’ютерні системи та мережі	5	екзамен
ОК 20	Фізика та електротехніка	5	екзамен
ОК 21	Цифрова економіка	5	залік
ОК 22	Технологія створення програмних продуктів	4	залік
ОК 23	Методи та системи штучного інтелекту	5	екзамен
ОК 24	Основи кібербезпеки	3	залік
ОК 25	Теорія інформації та кодування	5	залік
ОК 26	Прикладна криптологія	7	залік, екзамен
ОК 27	Безпека комп'ютерних мереж	4	екзамен
ОК 28	Великі дані в захисті інформації	5	екзамен
ОК 29	Комплексні системи захисту інформації	4	екзамен
ОК 30	Управління інформаційною безпекою	4	залік
ОК 31	Технічний захист інформації	5	екзамен
ОК 32	Стеганографія	5	екзамен
ОК 33	Система стандартів та нормативне забезпечення захисту інформації	5	залік
ОК 34	Навчальна практика – проектно-технологічна (без відриву)	6	залік
ОК 35	Виробнича практика	6	залік
ОК 36	Кваліфікаційна бакалаврська робота	5	
Загальний обсяг обов’язкових компонент		180	
Вибіркові компоненти ОП*			
ВК 1.	Міжфакультетська вибіркова дисципліна 1	3	залік
ВК 2.	Міжфакультетська вибіркова дисципліна 2	3	залік
ВК 3.	Міжфакультетська вибіркова дисципліна 3	3	залік
ВК 4.	Міжфакультетська вибіркова дисципліна 4	3	залік
Обираються 10 (десять) дисциплін за каталогом фахових вибіркових дисциплін інституту для спеціальності 125Кібербезпека та захист інформації першого (бакалаврського) рівня загальним обсягом 48 кредитів ЄКТС			
Загальний обсяг вибіркових компонент		60	
ЗАГАЛЬНИЙ ОБСЯГ ОСВІТНЬОЇ ПРОГРАМИ		240	

Освітня програма передбачає виділення дисциплін двох видів: обов'язкових дисциплін та дисципліни за вільним вибором студента, які визначено відповідно до профілю освітньої програми.

Каталог вибіркових дисциплін доступний за посиланням: http://kbi.karazin.ua/vibirkovi-disciplini-profesijno%d1%97-pidgotovki-opp-kiberbezpeka-u-finansovix-texnologiyax-2023-r/

3. СТРУКТУРНО-ЛОГІЧНА СХЕМА ОСВІТНЬОЇ ПРОГРАМИ

Семестр	Код КОП	Компоненти освітньої програми	Передумови вивчення	Є базою для вивчення
1	2	3	4	5
Загальна підготовка				
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, вибіркові компоненти
1, 2	ОК 9	Вища математика		ОК 12, ОК 13, ОК 14, ОК 15, ОК 16, ОК 17, ОК 20, вибіркові компоненти
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, вибіркові компоненти

1	2	3	4	5
Фахова підготовка				
2	ОК 11	Основи алгоритмізації та програмування	ОК 7, ОК 8, ОК 9, ОК 10	ОК 14, ОК 16, вибіркові компоненти
2	ОК 12	Алгебра і теорія чисел	ОК 9, ОК 10	ОК 13, ОК 15, ОК 16, вибіркові компоненти
3, 4	ОК 13	Теорія ймовірностей та математична статистика	ОК 8, ОК 9, ОК 10, ОК 12	ОК 21, ОК 28, вибіркові компоненти
3	ОК 14	Об’єктно-орієнтоване програмування	ОК 8, ОК 9, ОК 10, ОК 11, ОК 16	ОК 22, вибіркові компоненти
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, вибіркові компоненти
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, вибіркові компоненти
4	ОК 18	Операційні системи	ОК 7, ОК 8, ОК 17	ОК 19, вибіркові компоненти
5	ОК 19	Комп’ютерні системи та мережі	ОК 7, ОК 8, ОК 17, ОК 18	ОК 27, ОК 28, ОК 29, ОК 33, вибіркові компоненти
5	ОК 20	Фізика та електротехніка	ОК 9, ОК 17	ОК 27, ОК 29, ОК 31
5	ОК 21	Цифрова економіка	ОК 5, ОК 6, ОК 8, ОК 13	ОК 28, вибіркові компоненти
6	ОК 22	Технологія створення програмних продуктів	ОК 8, ОК 14, ОК 16	ОК 33, вибіркові компоненти
8	ОК 23	Методи та системи штучного інтелекту	ОК 15, ОК 16, ОК 28, ВК 5, ВК 7	
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, вибіркові компоненти
4	ОК 25	Теорія інформації та кодування	ОК 24	вибіркові компоненти
6,7	ОК 26	Прикладна криптологія	ОК 24	вибіркові компоненти

1	2	3	4	5
6	ОК 27	Безпека комп'ютерних мереж	ОК 17, ОК 19, ОК 24, ОК 29	ОК 30, ОК 31, вибіркові компоненти
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, вибіркові компоненти
7	ОК 30	Управління інформаційною безпекою	ОК 24, ОК 27	вибіркові компоненти
7	ОК 31	Технічний захист інформації	ОК 24, ОК 27	вибіркові компоненти
7	ОК 32	Стеганографія	ОК 24	
8	ОК 33	Система стандартів та нормативне забезпечення захисту інформації	ОК 19, ОК 22, ОК 24	

4.ФОРМИ АТЕСТАЦІЇ ЗДОБУВАЧІВ ВИЩОЇ ОСВІТИ

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

5. Матриця відповідності програмних компетентностей компонентам освітньої програми

Компоненти освітньої програми	Програмні компетентності випускника																							
	ІК	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

	ІК	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	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+

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

	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

	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	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+

	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													+										+					
	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 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				+																+	+		+				
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	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+

Гарант освітньої програми,
к.т.н, доцент

Анатолій КОБИЛІН