

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» серпня 2024 року,

протокол № 16

Введено в дію з 2024 р.

наказом від «29» серпня 2024 р.

№ 0114-1/240

Проректор з науково-педагогічної
роботи

Олександр ГОЛОВКО

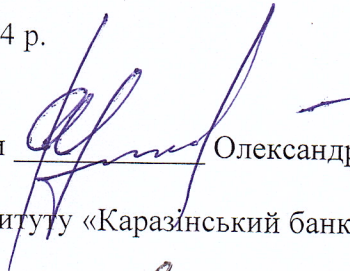


Харків 2024 р.

ЛИСТ ПОГОДЖЕННЯ
освітньо-професійної програми «Кібербезпека у фінансових технологіях»

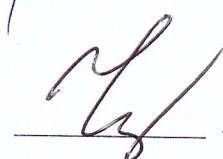
Освітню програму розглянуто та схвалено:

1. Науково-методичній раді Харківського національного університету імені В.Н. Каразіна
протокол № 10 від «18» серпня 2024 р.

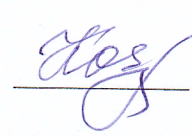
Голова науково-методичної ради,
проректор з науково-педагогічної роботи  Олександр ГОЛОВКО

2. Вченій раді Навчально-наукового інституту «Каразінський банківський інститут»,
протокол № 13 від «28» червня 2024 р.

Голова вченої ради інституту
к.ф.н., доц.

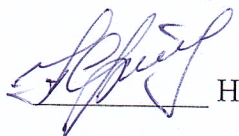
 Анна ЧХЕАЙЛО

3. Науково-методичній комісії Навчально-наукового інституту «Каразінський банківський інститут»,
протокол № 14 від «27» червня 2024 р.

Голова науково-методичної комісії інституту  Валерія КОЧОРБА

4. Кафедрі інформаційних технологій та математичного моделювання:
протокол № 14 від « 20 » червня 2024 р.

Завідувачка кафедри
к.пед.н.

 Наталя СТЯГЛИК

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

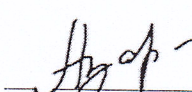
5.1. Кафедрі менеджменту, бізнесу та професійних комунікацій:
протокол № 22 від « 26 » червня 2024 р.

Завідувачка кафедри
к.е.н., доц.

 Надія МОРОЗОВА

5.2. Кафедрі банківського бізнесу та фінансових технологій:
протокол № 19 від « 26 » червня 2024 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, випускник ОПП, IOS Developer в TechBlitz;

Недзвецький Денис, випускник ОПП, DevOps в Smartn Soft Team;

Андренко Катерина, здобувач вищої освіти, голова студентської ради інституту;

Ягло Валерія, здобувач вищої освіти, голова студентської ради інституту;

Дракон Дар'я, здобувач вищої освіти, голова студентської ради інституту;

- 3) представники роботодавців:

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

Демченко Марія, Business Control Expert ING Bank 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 № 1547 від 29.10.2024 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>.
- 7) Наказ МОН України від 13.06.2024 р. №842 “Про внесення змін до деяких стандартів вищої освіти”. [Електронний ресурс]. Режим доступу: <https://mon.gov.ua/storage/app/sites/1/vishcha-osvita/zatverdzeni%20standarty/2024/Nakaz-842.vid.13.06.2024.pdf>

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 та захисту інформації
Тип диплому та обсяг освітньої програми	Диплом бакалавра, ОДИНИЧНИЙ Обсяг – 240 кредитів ЄКТС Термін навчання 3 роки 10 місяців
Наявність акредитації	Сертифікат про акредитацію спеціальності УД 21016936, дійсний до 01.07.2025
Передумови	Вступ на базі повної загальної середньої освіти; на основі ступенів «молодший бакалавр», «фаховий молодший бакалавр» або 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	3 роки 10 місяців
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 спеціалізації	Підготовка фахівців, які володіють теоретичними та практичними знаннями, сучасними інформаційно-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. Ключові слова: кібербезпека, захист інформації, стандарти безпеки, фінансові технології, автоматизація бізнес-процесів.
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-правової форми, в яких випускники працюють у якості керівників структурних підрозділів або виконавців окремих напрямків діяльності. Випускники можуть працювати на посадах: 2131.2 Аналітик комп'ютерних систем 2139.2 Адміністратор безпеки мереж і систем, 2139.2 Фахівець сфери захисту інформації, 2139.2 Фахівець з питань безпеки (інформаційно-комунікаційні технології), 2132.2 Конструктор систем кібербезпеки, 2139.2 Фахівець з підтримки інфраструктури кіберзахисту, 2139.2 Фахівець з реагування на інциденти кібербезпеки, 2139.2 Фахівець з криптографічного захисту інформації, 2139.2 Фахівець з технічного захисту інформації, 2139.2 Фахівець з тестування систем захисту інформації, 2139.2 Аудитор інформаційних технологій (з кібербезпеки), 2139.2 Фахівець з оцінки заходів захисту інформації (кібербезпеки), 2149.2 Професіонал із організації інформаційної безпеки 2149.2 Професіонал із організації захисту інформації з обмеженим доступом
	2149.2 Фахівець (сфера захисту інформації)

	247 Професіонали з безпеки та якості 2433 Професіонали в галузі інформації та інформаційного аналізу 2433.2 Професіонали в галузі інформації та інформаційні аналітики 3119 Технік (сфера захисту інформації) 3121 Фахівець з інформаційних технологій 315 Інспектори з безпеки та якості 3439 Фахівець із організації інформаційної безпеки 3439 Інспектор з організації захисту секретної інформації 3439 Фахівець із організації захисту інформації з обмеженим доступом 4133 Оператор технічних засобів контролю на безпеку 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, колоквиум тощо
6 – Програмні компетентності	
Інтегральна компетентність	Здатність розв'язувати складні спеціалізовані задачі і практичні завдання у галузі кібербезпеки та захисту інформації.
Загальні компетентності	
ЗК 1	Здатність застосовувати знання у практичних ситуаціях.
ЗК 2	Знання та розуміння предметної області і розуміння професійної діяльності.
ЗК 3	Здатність спілкуватися державною мовою як усно, так і письмово.
ЗК 4	Здатність спілкуватися іноземною мовою.
ЗК 5	Здатність вчитися і оволодівати сучасними знаннями.
ЗК 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 та свобод людини і громадянина в Україні.

ЗК 7	Здатність ухвалювати рішення й діяти, дотримуючись принципу неприйнятності корупції та будь-яких інших проявів недоброчесності.
ЗК 8	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.
Спеціальні (фахові, предметні) компетентності	
СК 1	Здатність застосовувати законодавчу та нормативно-правову базу, а також державні і міжнародні вимоги, практики і стандарти у професійній діяльності.
СК 2	Здатність використовувати інформаційні технології, сучасні методи і моделі кібербезпеки та системи захисту інформації.
СК 3	Здатність забезпечувати неперервність бізнес-процесів згідно встановленої політики кібербезпеки та захисту інформації.
СК 4	Здатність забезпечувати захист інформації в інформаційних та інформаційно-комунікаційних системах згідно встановленої політики кібербезпеки й захисту інформації.
СК 5	Здатність відновлювати функціонування інформаційних та інформаційно-комунікаційних систем після реалізації загроз, здійснення кібератак, збоїв і відмов різних класів та походження.
СК 6	Здатність впроваджувати та забезпечувати функціонування комплексних систем захисту інформації (комплекси нормативно-правових, організаційних та технічних засобів і методів, процедур, практичних прийомів тощо).
СК 7	Здатність здійснювати професійну діяльність на основі впровадженої системи управління інформаційною та кібербезпекою.
СК 8	Здатність застосовувати методи та засоби криптографічного захисту інформації на об'єктах інформаційної діяльності.
СК 9	Здатність застосовувати методи та засоби технічного захисту інформації на об'єктах інформаційної діяльності.
СК 10	Здатність виконувати моніторинг інформаційних процесів, аналізувати, виявляти, оцінювати можливі вразливості та загрози інформаційному простору й інформаційним ресурсам згідно з встановленою політикою інформаційної безпеки.
СКД 1	здатність до проектування, розробки та використання програмних додатків у фінансових технологіях з необхідним рівнем кібербезпеки
СКД 2	здатність до оцінювання рівня кібербезпеки у фінансових технологіях, системах та сервісах
СКД 3	вміння знаходити вразливості в фінансових технологіях, системах та сервісах
СКД 4	здатність організовувати процес оцінки та забезпечення належного рівня кібербезпеки фінансових технологіях, системах та сервісах з урахуванням цілей сталого розвитку
7 – Програмні результати навчання	

PH1	Вільно спілкуватися державною мовою усно та письмово при виконанні професійних обов'язків.
PH2	Спілкуватися іноземною мовою з метою забезпечення ефективності професійної комунікації.
PH3	Застосовувати принцип неприйнятності корупції та будь-яких інших проявів недоброчесності у професійній діяльності.
PH4	Організовувати власну професійну діяльність, обирати і використовувати оптимальні методи та способи розв'язання складних спеціалізованих задач і практичних проблем у професійній діяльності, оцінювати їхню ефективність.
PH5	Аналізувати, аргументувати, приймати рішення при розв'язанні складних спеціалізованих задач і практичних завдань у професійній діяльності, які характеризуються комплексністю та неповною визначеністю умов, відповідати за прийняті рішення.
PH6	Адаптуватися до нових умов і технологій професійної діяльності, прогнозувати кінцевий результат.
PH7	Застосовувати й адаптувати теорії інформації та кодування, математичної статистики, чисел, криптографії та стеганографії, оброблення і передачі сигналів тощо, принципи, методи, поняття кібербезпеки та захисту інформації у навчанні та професійній діяльності.
PH8	Застосовувати знання і розуміння математики та фізики в професійній діяльності, формалізувати задачі у предметній галузі кібербезпеки та захисту інформації, формулювати їх математичну постановку та обирати раціональні методи вирішення.
PH9	Знати та застосовувати законодавство України та міжнародні вимоги, практики і стандарти з метою здійснення професійної діяльності в галузі кібербезпеки та захисту інформації.
PH10	Використовувати сучасні інформаційні технології, методи і моделі кібербезпеки та систем захисту інформації для здійснення професійної діяльності.
PH11	Планувати підготовку та забезпечувати неперервність бізнес-процесів в організаціях згідно зі встановленою політикою кібербезпеки з урахуванням вимог до захисту інформації.
PH12	Застосовувати методи та засоби захисту інформації в інформаційних та інформаційно-комунікаційних системах відповідно до встановленої політики інформаційної безпеки.
PH13	Впроваджувати, налаштовувати, супроводжувати та підтримувати функціонування програмних і програмно-апаратних комплексів і систем кібербезпеки та захисту інформації як необхідні процедури для функціонування інформаційних й інформаційно-комунікаційних систем та/або інфраструктури організації в цілому.
PH14	Вирішувати задачі управління процесами відновлення штатного функціонування інформаційних та інформаційно-комунікаційних систем з використанням процедур резервування згідно встановленої політики безпеки і забезпечувати функціонування спеціального програмного забезпечення щодо захисту та відновлення інформації.

PH15	Збирати, обробляти, зберігати, аналізувати критичні дані для доказу реалізації кіберзагроз, проводити аналіз та дослідження кіберінциденту з метою оперативного відновлення функціонування інформаційної системи.
PH16	Вирішувати задачі впровадження та супроводу комплексних систем захисту інформації в інформаційних системах.
PH17	Забезпечувати функціонування системи управління кібербезпекою і захистом інформації організації, включаючи персонал та управління наслідками реалізації загроз інформаційній безпеці в кризових ситуаціях, на основі здійснення процедур кількісної і якісної оцінки ризиків.
PH18	Аналізувати, застосовувати методи та засоби криптографічного захисту інформації на об'єктах інформаційної діяльності.
PH19	Вирішувати задачі щодо організації та контролю стану криптографічного захисту інформації, зокрема відповідно до вимог нормативних документів.
PH20	Визначати загрози створення технічних каналів витоку інформації на об'єктах інформаційної діяльності; впроваджувати засоби і заходи технічного захисту інформації від витоку технічними каналами, проводити обслуговування і контроль стану апаратних засобів захисту інформації та комплексів технічного захисту інформації.
PH21	Виконувати впровадження, підтримку, аналіз ефективності систем виявлення несанкціонованого доступу, дій з інформацією в інформаційній системі, вразливостей, можливих загроз інформаційному простору й інформаційним ресурсам та використовувати комплекси захисту для забезпечення необхідного рівня захищеності інформації в інформаційних системах.
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, впровадженні, 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 та захист інформації» у бібліотеках інституту та Університету (у тому числі в електронному вигляді). Вітчизняні та закордонні фахові періодичні видання у 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-освітніх 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 за фахом	12	екзамен

ОК 2.	Історія України: цивілізаційний вимір	3	екзамен
ОК 3.	Філософія	3	екзамен
ОК 4	Банківська студія "Тайм-менеджмент та міжособистісні комунікації в бізнесі"	5	залік
ОК 5	Банківська студія «Банківська система»	3	залік
ОК 6	Вступ до фаху	3	залік
ОК 7	Інформаційні технології	6	екзамен
ОК 8	Вища математика	12	залік, екзамен
ОК 9	Дискретна математика	10	залік, екзамен
ОК 10	Основи алгоритмізації та програмування	6	екзамен
ОК 11	Алгебра і теорія чисел	4	залік
ОК 12	Теорія ймовірностей та математична статистика	7	залік, екзамен
ОК 13	Об'єктно-орієнтоване програмування	4	екзамен
ОК 14	Спеціальні розділи математики	4	залік
ОК 15	Алгоритми та структури даних	3	залік
ОК 16	Комп'ютерна схемотехніка та архітектура комп'ютерів	4	екзамен
ОК 17	Операційні системи	5	екзамен
ОК 18	Комп'ютерні системи та мережі	5	екзамен
ОК 19	Фізика та електротехніка	5	екзамен
ОК 20	Цифрова економіка	4	залік
ОК 21	Технологія створення програмних продуктів	4	залік
ОК 22	Методи та системи штучного інтелекту	4	екзамен
ОК 23	Основи кібербезпеки	3	залік
ОК 24	Теорія інформації та кодування	4	залік
ОК 25	Прикладна криптологія	7	залік, екзамен
ОК 26	Безпека комп'ютерних мереж	4	екзамен
ОК 27	Великі дані в захисті інформації	3	екзамен
ОК 28	Комплексні системи захисту інформації	4	екзамен
ОК 29	Управління інформаційною безпекою	4	залік
ОК 30	Технічний захист інформації	5	екзамен
ОК 31	Стеганографія	5	екзамен
ОК 32	Система стандартів та нормативне забезпечення захисту інформації	5	залік
ОК 33	Навчальна практика – проектно-технологічна (без відриву)	6	залік
ОК 34	Виробнича практика	6	залік
ОК 35	Кваліфікаційна бакалаврська робота	5	
Загальний обсяг обов'язкових компонент		177	
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 11 (одинадцять) дисциплін за каталогом фахових вибірових дисциплін інституту для спеціальності 125 Кібербезпека та захист інформації першого (бакалаврського) рівня загальним обсягом 51 кредитів ЄКТС			
ВК 5	Чисельні методи / Чисельний аналіз та наукові обчислення	5	залік

БК 6	Комп'ютерна графіка та веб-дизайн /Вебпрограмування	4	екзамен
БК 7	Економіко-математичні методи та моделі / Методи та моделі в економіці	6	екзамен
БК 8	Організація баз даних та знань / Структури знань та даних	5	залік
БК 9	Безпека банківських систем/ Безпека фінансових технологій	4	залік
БК 10	Системний аналіз і теорія прийняття рішень / Системотехнічні методи в інформаційних технологіях / Теорія та практика системного прийняття рішень	4	залік
БК 11	Проектування інформаційних систем безпеки/Проектування засобів безпеки ІС	4	залік
БК 12	Моделювання бізнес-процесів безпеки/ Бізнес-інжиніринг інформаційних систем	5	екзамен
БК 13	Цифрова криміналістика / Основи протидії кіберзлочинності та цифрова криміналістика	4	залік
БК 14	Адміністрування та моніторинг комп'ютерних систем / Організація та проведення тестування на проникнення та соціальна інженерія	6	екзамен
БК 15	Вибіркова дисципліна за фахом 11 Паттерни проектування / Хмарні обчислення	4	залік
Загальний обсяг вибірових компонент		63	
Факультативні компоненти ОП			
ФК 1	Фізичне виховання		
ФК 2	Іноземна мова за фахом		к/р
ФК 3	Класифікація та кластеризація даних		
ЗАГАЛЬНИЙ ОБСЯГ ОСВІТНЬОЇ ПРОГРАМИ		240	

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

3. СТРУКТУРНО-ЛОГІЧНА СХЕМА ОСВІТНЬОЇ ПРОГРАМИ

		Передумови (дисципліни, які забезпечують)																																
		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
Загальна підготовка	Дисципліни, що забезпечуються																																	
	ОК 1. Іноземна мова за фахом	✗																																
	ОК 2. Історія України: цивілізаційний вибір		✗																															
	ОК 3. Філософія		☑	✗	☑																													
	ОК 4. БС "Тайм-менеджмент та міжособистісні комунікації в бізнесі"				✗																													
	ОК 5. БС «Банківська система»				☑	✗																												
	ОК 6. Вступ до фаху						✗																											
	ОК 7. Інформаційні технології							✗																										
	ОК 8. Вища математика								✗																									
ОК 9. Дискретна математика							☑		✗																									
Навчана підготовка	ОК 10. Алгебра і теорія чисел							☑		☑	✗																							
	ОК 11. Спеціальні розділи математики							☑		☑		✗																						
	ОК 12. Теорія ймовірностей та математична статистика							☑		☑			✗										☑											
	ОК 13. Основи алгоритмізації та програмування					☑		☑		☑				✗																				
	ОК 14. Алгоритми та структури даних						☑		☑		☑			☑	✗																			
	ОК 15. Об'єктно-орієнтоване програмування							☑						☑	☑	✗																		
	ОК 16. Технологія створення програмних продуктів			☑	☑										☑	☑	✗																	
	ОК 17. Фізика та електротехніка								☑		☑							✗																
	ОК 18. Операційні системи							☑		☑	☑				☑				✗															
Фахова підготовка	ОК 19. Комп'ютерні системи та мережі							☑		☑								☑	☑	✗		☑	☑											
	ОК 20. Цифрова економіка				☑		☑														✗													
	ОК 21. Комп'ютерна схемотехніка та архітектура комп'ютерів							☑				☑						☑				✗												
	ОК 22. Теорія інформації та кодування						☑		☑					☑									✗											
	ОК 23. Основи кібербезпеки						☑		☑	☑	☑											☑		✗										
	ОК 24. Прикладна криптологія								☑	☑	☑			☑									☑	☑	✗									
	ОК 25. Великі дані в захисті інформації							☑					☑		☑							☑		☑		✗								
	ОК 26. Методи та системи штучного інтелекту					☑	☑			☑				☑			☑										☑	✗						
	ОК 27. Безпека комп'ютерних мереж																	☑	☑			☑	☑						✗					
	ОК 28. Технічний захист інформації																	☑	☑			☑	☑						☑	✗				
	ОК 29. Стеганографія												☑		☑								☑			☑				☑		✗		
	ОК 30. Система стандартів та нормативне забезпечення захисту інформації																☑															✗		
	ОК 31. Управління інформаційною безпекою			☑							☑															☑							☑	✗
ОК 32. Комплексні системи захисту інформації								☑	☑									☑				☑		☑					☑	☑		☑	☑	✗

4.ФОРМИ АТЕСТАЦІЇ ЗДОБУВАЧІВ ВИЩОЇ ОСВІТИ

Атестація здійснюється у формі:	Атестація здійснюється у формі публічного захисту кваліфікаційної бакалаврської роботи та складанням атестаційного екзамену (єдиний державний кваліфікаційний іспит). 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 єдиного державного кваліфікаційного іспиту	Єдиний державний кваліфікаційний іспит передбачає оцінювання досягнень результатів навчання, визначених Стандартом.
Вимоги до кваліфікаційної роботи (за наявності)	Кваліфікаційна робота має передбачати розв'язок спеціалізованого завдання теоретичного або практичного спрямування в галузі кібербезпеки та захисту інформації. У кваліфікаційній роботі не повинно бути академічного плагіату, фальсифікації та фабрикації. Кваліфікаційна робота має бути оприлюднена (за виключенням робіт, що містять інформацію з обмеженим доступом) на офіційному сайті закладу вищої освіти або його структурного підрозділу, або у репозитарії закладу вищої освіти. 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		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	ОК 34	ОК 35			
Програмні компетентності випусника	ІК	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+			
	ЗК1	+			+			+	+	+	+	+	+	+	+	+	+	+	+	+	+	+					+	+	+				+		+	+	+		
	ЗК2					+	+				+			+			+	+	+	+	+	+	+				+	+	+					+		+	+		
	ЗК3				+										+								+												+	+	+		
	ЗК4	+																																	+	+	+		
	ЗК5	+			+			+	+	+	+	+	+	+	+	+	+	+	+			+	+	+			+	+	+					+	+	+	+		
	ЗК6		+																																	+	+	+	
	ЗК7		+	+	+		+											+					+													+	+	+	
	ЗК8			+	+																			+												+	+	+	
	СК1						+											+					+									+			+	+	+	+	
	СК2							+	+	+	+	+	+		+	+				+		+		+			+	+						+	+	+	+	+	
	СК3																					+					+									+	+	+	
	СК4													+													+		+	+	+			+		+	+	+	
	СК5																			+	+										+			+		+	+	+	
	СК6																																		+		+	+	
	СК7																							+				+	+				+	+		+	+	+	
	СК8													+																	+					+	+	+	
	СК9									+		+			+															+	+						+	+	+
	СК10									+		+		+	+								+	+				+							+		+	+	+
	СКД 1														+	+	+	+				+			+	+		+			+					+	+	+	
	СКД 2																											+	+					+		+	+	+	
	СКД 3																	+							+		+							+		+	+	+	
	СКД 4															+													+			+		+		+	+	+	

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

PH	OK 1	OK 2	OK 3	OK 4	OK 5	OK 6	OK 7	OK 8	OK 9	OK 10	OK 11	OK 12	OK 13	OK 14	OK 15	OK 16	OK 17	OK 18	OK 19	OK 20	OK 21	OK 22	OK 23	OK 24	OK 25	OK 26	OK 27	OK 28	OK 29	OK 30	OK 31	OK 32	OK 33	OK 34	OK 35		
PH 1				+												+					+													+	+		
PH 2	+			+																	+	+												+	+		
PH 3			+	+	+	+															+														+	+	
PH 4										+			+		+		+	+	+	+	+	+						+			+			+	+		
PH 5							+	+	+	+	+	+	+	+	+	+					+						+	+			+		+	+	+		
PH 6		+			+					+		+	+			+		+	+	+	+							+							+	+	
PH7								+	+		+	+		+							+	+				+	+								+	+	
PH8								+	+	+	+	+	+	+	+	+	+				+					+		+							+	+	
PH9																					+										+				+	+	
PH10							+																			+	+						+			+	+
PH11																												+			+				+	+	
PH12													+																			+		+		+	
PH13													+								+	+					+		+						+	+	
PH14																															+				+	+	
PH15								+				+		+												+	+	+		+					+	+	
PH16																						+						+					+			+	+
PH17																															+				+	+	
PH18																								+					+						+	+	
PH19																							+	+	+						+				+	+	
PH20																							+	+	+			+							+	+	
PH21																																+			+	+	

Гарант освітньої програми,
к.т.н, доцент



Анатолій КОБИЛІН