

**МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ
«ХАРКІВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ»**

ЗАТВЕРДЖУЮ
Ректор НТУ «ХПІ»



Євген СОКОЛ

«___» _____ 2022 р.

ОСВІТНЬО-ПРОФЕСІЙНА ПРОГРАМА

«Кібербезпека»

Другого (магістерського) рівня вищої освіти

за спеціальністю **125 – Кібербезпека**

галузі знань **12 – Інформаційні технології**

кваліфікація **магістр з кібербезпеки**

ЗАТВЕРДЖЕНО

ВЧЕНОЮ РАДОЮ НТУ «ХПІ»

Голова Вченої ради

/ Леонід ТОВАЖНЯНСЬКИЙ

Протокол № _____

від «___» _____ 2022р.

Харків 2022р.

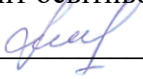
ЛИСТ ПОГОДЖЕННЯ

Освітньо-професійної програми Кібербезпека

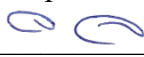
Рівень вищої освіти	Другий (магістерський)
Галузь знань	12 Інформаційні технології
Спеціальність	125 «Кібербезпека»
Кваліфікація	Магістр з кібербезпеки

СХВАЛЕНО

Робочою групою ОПП із спеціальності
«Кібербезпека»

Гарант освітньо-професійної програми
 Олександр МІЛОВ
«___» _____ 2022 р.

ПОГОДЖЕНО

Завідувач кафедри кібербезпеки
Сергій ЄВСЕЄВ 
«___» _____ 2022 р.

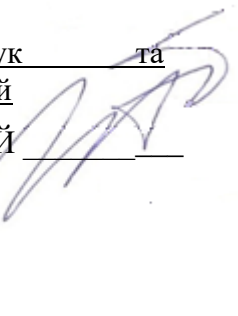
ПОГОДЖЕНО

Студент (член робочої групи ОПП)
група КН-М1122а
Сергій ДУНАЄВ _____
«___» _____ 20__р.

РЕКОМЕНДОВАНО

Методичною радою НТУ «ХП»
Заступник голови методичної ради
 Руслан МИГУЩЕНКО
«___» _____ 2022 р.

ПОГОДЖЕНО

Директор навчально-наукового
інституту
комп'ютерних наук та
інформаційних технологій
Михайло ГОДЛЕВСЬКИЙ 
«___» _____ 2022 р.

РЕЦЕНЗЕНТИ:

Продуктивні зауваження та відгуки на проєкт освітньо-професійної програми (ОПП) одержано від:

1. Ковтун Владислав Юрійович, ТОВ «Сайфер», директор
2. Волощук Олена Борисівна, ТОВ «Distributed Lab», координатор освітньої програми
3. Головашич Сергій Олександрович, ТОВ «Мікрокрипт Текнолоджіс», директор
4. Молодецька Катерина Валеріївна, доктор технічних наук, професор, навчально-наукового центру інформаційних технологій Поліського національного університету, керівник

РЕЦЕНЗІЯ

на освітньо-професійну програму “КІБЕРБЕЗПЕКА”(CYBERSECURITY)
другого (магістерського) рівня вищої освіти
спеціальності 125 “КІБЕРБЕЗПЕКА” (CYBERSECURITY)

Освітньо-професійна програма “КІБЕРБЕЗПЕКА”(CYBERSECURITY) за спеціальністю 125 “КІБЕРБЕЗПЕКА” (CYBERSECURITY), яку втілено до учбового процесу на другому (магістерському) рівні вищої освіти у Національному технічному університеті “Харківський політехнічний інститут”, відповідає сучасним вимогам ІТ-індустрії та відповідному стандарту вищої освіти.

Програма спрямована на підготовку фахівців здатних виконувати професійні роботи та виконувати наукові дослідження у галузі забезпечення безпеки у інформаційно-комунікаційних системах та загальної безпеки інформаційних технологій. Схема навчального процесу є чіткою та зрозумілою й відбиває останні напрямки технологій кібербезпеки та досліджень у цій галузі. Навчальні дисципліни, що забезпечують освітньо-професійну програму, відповідають світовим аналогам та запитам роботодавців. Об’єкт та цілі програми є чіткими та зрозумілими. Засоби та обладнання, що застосовується у навчальному процесі повністю надають студентам можливості отримати не тільки теоретичні знання, але й набути практики у рішенні завдань, які моделюють існуючі виробничі процеси та інциденти кібербезпеки.

Програма обговорювалась зі стейкхолдерами, враховує побажання здобувачів вищої освіти та спрямована на забезпечення загальних та спеціальних (фахових) компетентностей за спеціальністю 125 “КІБЕРБЕЗПЕКА” (CYBERSECURITY). Результати навчання відповідають стандарту освіти та вимогам організацій та компаній, що зараз потребують фахівців відповідного профілю.

В цілому освітньо-професійна програма “КІБЕРБЕЗПЕКА” (CYBERSECURITY) другого (магістерського) рівня вищої освіти спеціальності 125 “КІБЕРБЕЗПЕКА” (CYBERSECURITY) має всі необхідні складові для підготовки сучасних кваліфікованих фахівців, які будуть ефективно вирішувати теоретичні та практичні питання щодо забезпечення кібербезпеки, як на рівні невеликих організацій та підприємств, так й в умовах розгортання та супроводження корпоративних рішень.

Директор ТОВ “Сайфер ІТ”



тн., В.Ю. КОВТУН

РЕЦЕНЗІЯ-ВІДГУК
на освітньо-професійну програму “Кібербезпека” другого (магістерського)
рівня вищої освіти
кафедри кібербезпеки Національного технічного університету
“Харківський політехнічний інститут”

Забезпечення безпеки в кіберпросторі є однією з найактуальніших та найскладніших проблем сьогодення у зв'язку із великими об'ємом даних, які мають бути захищені, та постійною зміною та вдосконаленням відповідних технологій. Кібербезпека на сьогодні є спеціальністю, яка включає в себе декілька великих напрямів: підготовки (побудова архітектури безпеки, управління ризиками, використання професійних стандартів та фреймворки криптології, технічний захист інформації тощо).

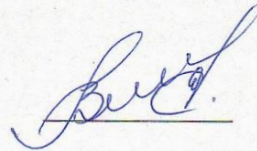
Таким чином підготовка фахівців з кібербезпеки за освітньо-професійною програмою “Кібербезпека” другого (магістерського) рівня вищої освіти є актуальним напрямом освітньої діяльності університету, що дозволяє готувати конкурентоспроможних випускників в галузі безпеки об'єктів критичної інфраструктури.

Схема підготовки фахівців за освітньо-професійною програмою, що акредитується, є правильно побудованою: врахована необхідність отримання студентами знань з дисциплін професійного змісту, які повністю покривають результати навчання, що передбачені стандартом вищої освіти зі спеціальності 125 “Кібербезпека” другого (магістерського) рівня вищої освіти. Створення можливості мобільності з Університетом у Бельсько-Бялій, Польща дозволяє отримати спільні дипломи, підтверджує якість освітніх компонент та їх відповідність вимогам Євросоюзу.

В рамках освітньо-професійної програми “Кібербезпека”, яка складена кафедрою кібербезпеки НТУ ХПІ, автори змогли досить органічно та логічно сформулювати схему підготовки майбутнього фахівця, яка, з одного боку, дозволяє освітній програмі забезпечувати реалізацію результатів навчання передбачених стандартом вищої освіти в повному обсязі, а, з іншого боку, завдяки акценту на технологіях програмування випускники мають можливість працевлаштовуватися не тільки за спеціальністю, але й в ІТ сфері загалом.

Вважаємо, що освітня професійна програма “Кібербезпека” другого (магістерського) рівня вищої освіти, яка складена кафедрою кібербезпеки НТУ ХПІ, має всі необхідні компоненти для підготовки кваліфікованих фахівців, які будуть затребувані на ринку праці як за спеціальністю, так і в цілому на ринку інформаційних технологій.

Керівник освітніх програм
компанії Distributed Lab,
кандидат технічних наук

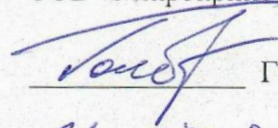


Олена ВОЛОЩУК

ЗАТВЕРДЖУЮ:

Генеральний директор

ТОВ «Мікрокрипт Текнолоджіс»



Головашич С.О.

«21» січня 2022 р.

РЕЦЕНЗІЯ-ВІДГУК

**на освітньо-професійну програму «Кібербезпека»,
підготовлену кафедрою кібербезпеки Національного технічного університету
«Харківський політехнічний інститут»**

Кібербезпека розглядає захист функціонування нової сутності – кіберпростору, середовища, що виникло в результаті взаємодії людей, програмного забезпечення, Інтернет сервісів з використанням технічних пристроїв і мережевих зв'язків.

Якщо раніше проблема безпеки в кіберпросторі стосувалася тільки окремих компаній, то з розвитком Інтернет і мобільного банкінгу, Інтернету речей та багатьох інших сучасних технологій – безпека в кіберпросторі стосується кожного з нас. Фахівці з кібербезпеки забезпечують захист життєво важливих інтересів людини та суспільства, своєчасне виявлення, запобігання і нейтралізацію реальних та потенційних загроз у сфері функціонування інформаційних, комп'ютерних та кіберфізичних систем.

Підготовка досвідчених фахівців у сфері захисту інформації (кібербезпеки) є одним з найбільших викликів сьогодення через необхідність постійного оновлення змісту освіти. Освітня програма «Кібербезпека» сформована кафедрою кібербезпеки НТУ «ХПІ», відповідно до останніх тенденцій розвитку спеціальності та повністю забезпечує досягнення результатів навчання, передбачених стандартом вищої освіти за спеціальністю 125 Кібербезпека. Програма має чітко визначені цілі, які враховують основні її особливості - підготовку фахівця з інформаційної безпеки широкого профілю зі знанням технологій програмування. Складова отримання спільних дипломів з державним Університетом у Бельсько-Бялій (Польща) підтверджує її конкурентоздатність

серед програм Євросоюзу, мобільність програми забезпечує своєчасне корегування в умовах стрімкого розвитку цієї спеціальності.

Однією з основних проблем реалізації освітнього процесу за спеціальністю 125 Кібербезпека є відсутність під час навчання можливості отримати знання та навички від професіоналів-практиків. В рамках викладання за освітньою програмою, що рецензується, залучено викладачів-практиків.

Вважаємо, що Освітньо-професійна програма “Кібербезпека”, що складена та запропонована кафедрою кібербезпеки Національного технічного університету “Харківський політехнічний інститут”, має всі необхідні компоненти для підготовки кваліфікованих фахівців, які будуть високозатребувані на ринку праці.

Генеральний директор
ТОВ «Мікрокрипт Текнолоджис», к.т.н.


Г.Костенашч С.О.


РЕЦЕНЗІЯ

на освітньо-професійну програму “Кібербезпека”
другого (магістерського) рівня спеціальності 125 “Кібербезпека”
Національного технічного університету “Харківський політехнічний інститут”

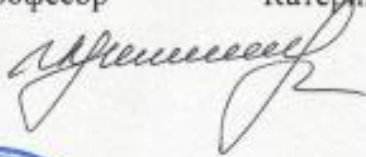
Освітньо-професійна програма (ОПП) “Кібербезпека” підготовки здобувачів вищої освіти другого (магістерського) рівня спеціальності 125 “Кібербезпека” галузі знань 12 “Інформаційні технології” розроблена науково-педагогічними працівниками Національного технічного університету “Харківський політехнічний інститут”. Керівник проєктної групи – гарант освітньої програми д.т.н., проф. Мілов О. В. Подана на рецензування ОПП розроблена на основі стандарту вищої освіти України зі спеціальності 125 “Кібербезпека” другого (магістерського) рівня, затвердженого наказом МОН України від 18 березня 2021 р. № 332. Представлена ОПП містить профіль освітньої програми за відповідною спеціальністю, перелік компонент освітньо-професійної програми та їх логічну послідовність, структурно-логічну схему, інформацію про форму атестації здобувачів вищої освіти.

Метою ОПП є підготовка фахівців, здатних розв’язувати задачі дослідницького та/або інноваційного характеру у сфері інформаційної та/або кібербезпеки, використовувати і впроваджувати технології та застосовувати засоби захисту в системах безпеки контуру бізнес-процесів. Критичний аналіз ОПП показав, що зміст програми повністю враховує інтегральну, загальну й фахові компетентності, які передбачено стандартом. Це забезпечує досягнення здобувачами вищої освіти програмних результатів навчання. Програмні результати ОПП корелюють із складовими професійної компетентності, які формують фундаментальні знання та фахові навички, а загальні компетентності забезпечують розвиток навичок soft skills та сприяють формуванню свідомої громадянської позиції випускника з усталеними цінностями, здатністю до фахового розвитку і самовдосконалення. Фокус ОПП направлено на побудову комплексних систем захисту інформації для забезпечення безпеки контуру бізнес-процесів на основі сучасних технологій та програмних застосунків, в умовах розвитку цифрової економіки, додатково підкреслює сучасну спрямованість програми.

Вважаю, що освітньо-професійна програма підготовки здобувачів вищої освіти другого (магістерського) рівня освіти галузі знань 12 “Інформаційні технології” за спеціальністю 125 “Кібербезпека” у Національному технічному університеті “Харківський політехнічний інститут” характеризується системністю і цільовим підходом до підготовки фахівців з кібербезпеки, відповідає сучасному рівню розвитку науки і практики освітньої діяльності та може бути рекомендована до впровадження в освітньому процесі університету.

Керівник навчально-наукового центру
інформаційних технологій
Поліського національного університету,
доктор технічних наук (21.05.01 –
інформаційна безпека держави), професор

Катерина МОЛОДЕЦЬКА



ПЕРЕДМОВА

Відповідає Стандарту вищої освіти другого (магістерського) рівня галузі знань «Інформаційні технології», спеціальності 125 «Кібербезпека», затвердженого та введеного в дію наказом Міністерства освіти і науки України від 04.10.2018 р. № 1074.

Розроблено робочою групою ОПП «Кібербезпека»

Навчально-наукового інституту комп'ютерних наук та інформаційних технологій Національного технічного університету «Харківський політехнічний інститут»

у складі:

Гарант освітньо-професійної програми

Мілов Олександр Володимирович (доктор технічних наук, професор, професор кафедри кібербезпеки).

Члени робочої групи ОПП :

1. Король Ольга Григорівна, кандидат технічних наук, доцент, доцент кафедри кібербезпеки.

2. Євсєєв Сергій Петрович (доктор технічних наук, професор, завідувач кафедри кібербезпеки).

3. Студент Дунаєв Сергій Владиславович, група КН-М1122а

**ПРОФІЛЬ ОСВІТНЬО-ПРОФЕСІЙНОЇ ПРОГРАМИ ЗА
СПЕЦІАЛЬНІСТЮ 125 – КІБЕРБЕЗПЕКА**

1 – Загальна інформація	
Вищий навчальний заклад та структурний підрозділ	Національний технічний університет «Харківський політехнічний інститут», Навчально-науковий інститут <u>комп'ютерних наук та інформаційних технологій</u> кафедра <u>кібербезпеки</u>
Ступінь вищої освіти та назва кваліфікації мовою оригіналу	Магістр Освітня кваліфікація: магістр з кібербезпеки Кваліфікація в дипломі: магістр з кібербезпеки
Офіційна назва освітньо-професійної програми	Кібербезпека
Тип диплому та обсяг освітньо-професійної програми	Диплом магістра, одиничний, 90 кредитів ЄКТС, термін навчання 1 рік 4 місяці
Наявність акредитації	відсутня
Цикл/рівень	другий (магістерський) рівень вищої освіти; НРК України – 7 рівень, FQ-EHEA– другий цикл, EQF LLL – 7 рівень
Передумови	Набір за спеціальністю освітнього рівня «магістр» здійснюється за результатами зовнішнього незалежного оцінювання (іноземна мова) та вступного фахового випробування. Загальний конкурсний бал для вступу на основі освіти бакалавра не може бути менше 100 балів
Мова викладання	Українська, англійська
Термін дії освітньо-професійної програми	Оновлюється щорічно
Посилання на постійне розміщення опису освітньо-професійної програми	Інтернет-адреса постійного розміщення опису освітньої програми https://cybersecurity.kpi.kharkov.ua
2 – Мета освітньо-професійної програми	
Підготовка фахівців, здатних розв'язувати задачі дослідницького та/або	

інноваційного характеру у сфері інформаційної та/або кібербезпеки, використовувати і впроваджувати технології та застосовувати засоби захисту в системах безпеки контуру бізнес-процесів.	
3 – Характеристика освітньо-професійної програми	
Предметна область (галузь знань, спеціальність)	Галузь знань: 12 Інформаційні технології Спеціальність: 125 – Кібербезпека Об’єкти вивчення: – сучасні процеси дослідження, аналізу, створення та забезпечення функціонування інформаційних систем і технологій, інших бізнес-операційних процесів на об’єктах інформаційної діяльності та критичних інфраструктур сфери інформаційної безпеки та/або кібербезпеки; – інформаційні системи (інформаційно-комунікаційні, інформаційно-телекомунікаційні, автоматизовані) та технології; - інфраструктура об’єктів інформаційної діяльності та критичних інфраструктур; – системи та комплекси створення, обробки, передачі, зберігання, знищення, захисту та відображення даних (інформаційних потоків); – інформаційні ресурси різних класів (в т.ч. державні інформаційні ресурси); – програмне та програмно-апаратне забезпечення (засоби) кіберзахисту; – системи управління інформаційною безпекою та/або кібербезпекою; – технології, методи, моделі та засоби інформаційної безпеки та/або кібербезпеки. Цілі навчання: Підготовка фахівців, здатних розв’язувати задачі дослідницького та/або інноваційного характеру у сфері інформаційної та/або кібербезпеки. Теоретичний зміст предметної області Теоретичні засади наукоємних технологій, фізичні і математичні фундаментальні знання, теорії ідентифікації та прийняття рішень, системного аналізу, складних систем, моделювання та оптимізації процесів, теорія математичної статистики, криптографічного та технічного захисту інформації, теорії ризиків та інших міждисциплінарних теорій і практик у галузі інформаційної безпеки та/або кібербезпеки.

	Методи, методики та технології Методи, моделі, методики та технології створення, обробки, передачі, приймання, знищення, відображення, захисту (кіберзахисту) інформаційних ресурсів у кіберпросторі, а також методи та моделі розробки та використання прикладного і спеціалізованого програмного забезпечення для вирішення професійних задач в галузі інформаційної безпеки та/або кібербезпеки. Технології, методи та моделі дослідження, аналізу, управління та забезпечення бізнес/операційних процесів із застосуванням сукупності нормативно-правових та організаційно-технічних методів і засобів захисту інформаційних ресурсів у кіберпросторі. Інструменти та обладнання. Засоби, пристрої, мережне устаткування та середовище, прикладне та спеціалізоване програмне забезпечення, автоматизовані системи та комплекси проектування, моделювання, експлуатації, контролю, моніторингу, обробки, відображення та захисту даних (інформаційних потоків), а також методи і моделі теорії ризиків та управління інформаційними ресурсами при дослідженні і супроводженні об'єктів інформаційної діяльності у галузі інформаційної безпеки та/або кібербезпеки.
Орієнтація освітньо-професійної програми	Професійна підготовка фахівців у сфері кібербезпеки
Основний фокус освітньо-професійної програми та спеціалізації	Спеціальна освіта у галузі інформаційних технологій зі спеціальності 125 «Кібербезпека». Поглиблене вивчення проведення, як зовнішнього, так й внутрішнього аудиту з метою забезпечення безпеки контуру бізнес-процесів. Отримання сертифікатів курсів академії Cisco, сприяє підвищенню конкурентноспроможності на ринку праці, удосконаленню механізмів аудиту та захисту за мировими методиками. Ключові слова: кібербезпека, цифрова криміналістика, етнічний хакінг.
Особливості програми	Особливостями освітньо-професійної програми спеціальності «Кібербезпека» є формування у здобувачів навичок побудови комплексних систем захисту інформації для забезпечення безпеки контуру бізнес-процесів на

	основі сучасних технологій та програмних застосунків, в умовах розвитку цифрової економіки. Орієнтація на партнерство із вітчизняними та закордонними закладами освіти та науки, приватним сектором, науковцями та практиками, участь в міжнародних програмах спільних дипломів. Можливість навчатися англійською мовою.
4 – Придатність випускників до працевлаштування та подальшого навчання	
Придатність до працевлаштування	Фахівці з кібербезпеки можуть працювати, згідно з чинною редакцією Національного класифікатора України: Класифікатор професій (Зміна № 10 до ДК 003:2010), а саме: 2139.2 Аналітик загроз безпеки; 2139.2 Аналітик систем захисту інформації та оцінки вразливостей; 2139.2 Аналітик з безпеки інформаційно-телекомунікаційних систем; 2139.2 Дізнавач (сфера кібербезпеки та захисту інформації); 2139.2 Експерт-криміналіст (сфера кібербезпеки та захисту інформації); 2139.2 Експерт-криміналіст судової експертизи (сфера кібербезпеки та захисту інформації); 2139.2 Слідчий з кіберзлочинів;
Подальше навчання	Продовження освіти за третім (освітньо-науковим) рівнем вищої освіти. Набуття додаткових кваліфікацій в системі освіти дорослих.
5 – Викладання та оцінювання	
Викладання та навчання	У процесі викладання передбачено застосування таких навчальних технологій, як: лекції, лабораторні роботи, практичні заняття, робота в малих групах, презентації, що розвивають комунікативні та лідерські навички, самостійна робота з літературними джерелами.
Оцінювання	Моніторинг знань та умінь студентів здійснюється у формі поточного та підсумкового контролю. Поточний контроль – усне та письмове опитування, оцінка роботи в малих групах, тестування, захист групових та індивідуальних науково-дослідних завдань та проєктів.

	Підсумковий контроль – усні та письмові екзамени, заліки з урахуванням накопичених балів поточного контролю, захист звітів з практик, захист курсових робіт. Державна атестація – підготовка та публічний захист (представлення) випускної кваліфікаційної роботи. Оцінювання здійснюється за національною шкалою (“відмінно”, “добре”, “задовільно”, “незадовільно”), 100-бальною шкалою та шкалою ECTS (A, B, C, D, E, FX, F).
6 – Програмні компетентності	
Інтегральна компетентність	Здатність особи розв’язувати задачі дослідницького та/або інноваційного характеру у сфері інформаційної безпеки та/або кібербезпеки.
Загальні компетентності (визначені стандартом вищої освіти спеціальності)	КЗ-1. Здатність застосовувати знання у практичних ситуаціях. КЗ-2. Здатність проводити дослідження на відповідному рівні. КЗ-3. Здатність до абстрактного мислення, аналізу та синтезу. КЗ-4. Здатність оцінювати та забезпечувати якість виконуваних робіт. КЗ-5. Здатність спілкуватися з представниками інших професійних груп різного рівня (з експертами з інших галузей знань / видів економічної діяльності).
Спеціальні (фахові) компетентності спеціальності (визначені стандартом вищої освіти спеціальності)	КФ1. Здатність обґрунтовано застосовувати, інтегрувати, розробляти та удосконалювати сучасні інформаційні технології, фізичні та математичні моделі, а також технології створення та використання прикладного і спеціалізованого програмного забезпечення для вирішення професійних задач у сфері інформаційної безпеки та/або кібербезпеки. КФ2. Здатність розробляти, впроваджувати та аналізувати нормативні документи, положення, інструкції й вимоги технічного та організаційного спрямування, а також інтегрувати, аналізувати і використовувати кращі світові практики, стандарти у професійній діяльності в сфері інформаційної безпеки та/або кібербезпеки. КФ3. Здатність досліджувати, розробляти і супроводжувати методи та засоби інформаційної безпеки та/або кібербезпеки на об’єктах інформаційної діяльності та критичної інфраструктури.

	КФ4. Здатність аналізувати, розробляти і супроводжувати систему управління інформаційною безпекою та/або кібербезпекою організації, формувати стратегію і політики інформаційної безпеки з урахуванням вітчизняних і міжнародних стандартів та вимог. КФ5. Здатність до дослідження, системного аналізу та забезпечення безперервності бізнес/операційних процесів з метою визначення вразливостей інформаційних систем та ресурсів, аналізу ризиків та визначення оцінки їх впливу у відповідності до встановленої стратегії і політики інформаційної безпеки та/або кібербезпеки організації. КФ6. Здатність аналізувати, контролювати та забезпечувати систему управління доступом до інформаційних ресурсів згідно встановленої стратегії і політики інформаційної безпеки та/або кібербезпеки організації. КФ7. Здатність досліджувати, розробляти та впроваджувати методи і заходи протидії кіберінцидентам, здійснювати процедури управління, контролю та розслідування, а також надавати рекомендації щодо попередження та аналізу кіберінцидентів в цілому. КФ8. Здатність досліджувати, розробляти, впроваджувати та супроводжувати методи і засоби криптографічного та технічного захисту інформації на об'єктах інформаційної діяльності та критичної інфраструктури, в інформаційних системах, а також здатність оцінювати ефективність їх використання, згідно встановленої стратегії і політики інформаційної безпеки та/або кібербезпеки організації. КФ9. Здатність аналізувати, розробляти і супроводжувати систему аудиту та моніторингу ефективності функціонування інформаційних систем і технологій, бізнес/операційних процесів в галузі інформаційної безпеки та/або кібербезпеки організації в цілому. КФ10. Здатність провадити науково-педагогічну діяльність, планувати навчання, контролювати і супроводжувати роботу з персоналом, а також приймати ефективні рішення з питань інформаційної безпеки та/або кібербезпеки.
	7 – Результати навчання

Результати навчання за спеціальністю (визначені стандартом вищої освіти спеціальності)	РН1. Вільно спілкуватись державною та іноземною мовами, усно і письмово для представлення і обговорення результатів досліджень та інновацій, забезпечення бізнес\операційних процесів та питань професійної діяльності в галузі інформаційної безпеки та/або кібербезпеки. РН2. Інтегрувати фундаментальні та спеціальні знання для розв'язування складних задач інформаційної безпеки та/або кібербезпеки у широких або мультидисциплінарних контекстах. РН3. Проводити дослідницьку та/або інноваційну діяльність в сфері інформаційної безпеки та/або кібербезпеки, а також в сфері технічного та криптографічного захисту інформації у кіберпросторі. РН4. Застосовувати, інтегрувати, розробляти, впроваджувати та удосконалювати сучасні інформаційні технології, фізичні та математичні методи і моделі в сфері інформаційної безпеки та/або кібербезпеки. РН5. Критично осмислювати проблеми інформаційної безпеки та/або кібербезпеки, у тому числі на міжгалузевому та міждисциплінарному рівні, зокрема на основі розуміння нових результатів інженерних і фізико-математичних наук, а також розвитку технологій створення та використання спеціалізованого програмного забезпечення. РН6. Аналізувати та оцінювати захищеність систем, комплексів та засобів кіберзахисту, технології створення та використання спеціалізованого програмного забезпечення. РН7. Обґрунтовувати використання, впроваджувати та аналізувати кращі світові стандарти, практики з метою розв'язання складних задач професійної діяльності в галузі інформаційної безпеки та/або кібербезпеки. РН8. Досліджувати, розробляти і супроводжувати системи та засоби інформаційної безпеки та/або кібербезпеки на об'єктах інформаційної діяльності та критичної інфраструктури. РН9. Аналізувати, розробляти і супроводжувати систему управління інформаційною безпекою та/або кібербезпекою організації на базі стратегії і політики інформаційної безпеки. РН10. Забезпечувати безперервність бізнес/операційних процесів, а також виявляти уразливості інформаційних систем та ресурсів, аналізувати та оцінювати ризики для інформаційної безпеки та/або кібербезпеки організації. РН11. Аналізувати, контролювати та забезпечувати
---	---

	ефективне функціонування системи управління доступом до інформаційних ресурсів відповідно до встановлених стратегії і політики інформаційної безпеки та/або кібербезпеки організації. РН12. Досліджувати, розробляти та впроваджувати методи і заходи протидії кіберінцидентам, здійснювати процедури управління, контролю та розслідування, а також надавати рекомендації щодо попередження та аналізу кіберінцидентів в цілому. РН13. Досліджувати, розробляти, впроваджувати та використовувати методи та засоби криптографічного та технічного захисту інформації бізнес/операційних процесів, а також аналізувати і надавати оцінку ефективності їх використання в інформаційних системах, на об'єктах інформаційної діяльності та критичної інфраструктури. РН14. Аналізувати, розробляти і супроводжувати систему аудиту та моніторингу ефективності функціонування інформаційних систем і технологій, бізнес\операційних процесів у сфері інформаційної та/або кібербезпеки в цілому. РН15. Зрозуміло і недвозначно доносити власні висновки з проблем інформаційної безпеки та/або кібербезпеки, а також знання та пояснення, що їх обґрунтовують до персоналу, партнерів та інших осіб. РН16. Приймати обґрунтовані рішення з організаційно-технічних питань інформаційної безпеки та/або кібербезпеки у складних і непередбачуваних умовах, у тому числі із застосуванням сучасних методів та засобів оптимізації, прогнозування та прийняття рішень. РН17. Мати навички автономного і самостійного навчання у сфері інформаційної безпеки та/або кібербезпеки і дотичних галузей знань, аналізувати власні освітні потреби та об'єктивно оцінювати результати навчання. РН18. Планувати навчання, а також супроводжувати та контролювати роботу з персоналом у напрямку інформаційної безпеки та/або кібербезпеки. РН19. Обирати, аналізувати і розробляти придатні типові аналітичні, розрахункові та експериментальні методи кіберзахисту, розробляти, реалізовувати та супроводжувати проекти з захисту інформації у кіберпросторі, інноваційної діяльності та захисту інтелектуальної власності. РН20. Ставити та вирішувати складні інженерно-прикладні та наукові задачі інформаційної безпеки та/або
--	---

	кібербезпеки з урахуванням вимог вітчизняних та світових стандартів та кращих практик. РН21. Використовувати методи натурального, фізичного і комп'ютерного моделювання для дослідження процесів, які стосуються інформаційної безпеки та/або кібербезпеки. РН22. Планувати та виконувати експериментальні і теоретичні дослідження, висувати і перевіряти гіпотези, обирати для цього придатні методи та інструменти, здійснювати статистичну обробку даних, оцінювати достовірність результатів досліджень, аргументувати висновки. РН23. Обґрунтовувати вибір програмного забезпечення, устаткування та інструментів, інженерних технологій і процесів, а також обмежень щодо них в галузі інформаційної безпеки та/або кібербезпеки на основі сучасних знань у суміжних галузях, наукової, технічної та довідкової літератури та іншої доступної інформації.
8 – Ресурсне забезпечення реалізації програми	
Кадрове забезпечення	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, додаток 12; зі змінами, внесеними згідно з Постановою КМУ № 365 від 24.03.2021). До викладання залучаються викладачі-практики, фахівці та співробітники ІТ-компаній, а також закордонні фахівці.
Матеріально-технічне забезпечення	Відповідає технологічним вимогам щодо матеріально-технічного забезпечення 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, додаток 13)
Інформаційне та навчально-методичне забезпечення	Відповідає технологічним вимогам щодо навчально-методичного та інформаційного забезпечення 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, додатки 14 – 15). Застосування у навчальному процесі LMS (Learning Management System). Доступ до електронного репозитарію НТУ «ХП»

	(eNTUKhPIIR) через мережу Інтернет (у тому числі університетську мережу Wi-Fi).
9 – Академічна мобільність	
Національна кредитна мобільність	На основі двосторонніх договорів про академічну мобільність з університетами України.
Міжнародна кредитна мобільність	На основі двосторонніх договорів. Польсько-українська програма обміну та двох дипломів для підготовки магістрів за спеціальністю «Кібербезпека» з Університетом у Бельсько-Бялій (м. Бельсько-Бяла, Польща).
Навчання іноземних здобувачів освіти	Після отримання Сертифікату про акредитацію освітньої програми передбачається підготовка іноземців та осіб без громадянства.

ПЕРЕЛІК ОСВІТНІХ КОМПОНЕНТ ОСВІТНЬО-ПРОФЕСІЙНОЇ ПРОГРАМИ ТА ЇХ ЛОГІЧНА ПОСЛІДОВНІСТЬ

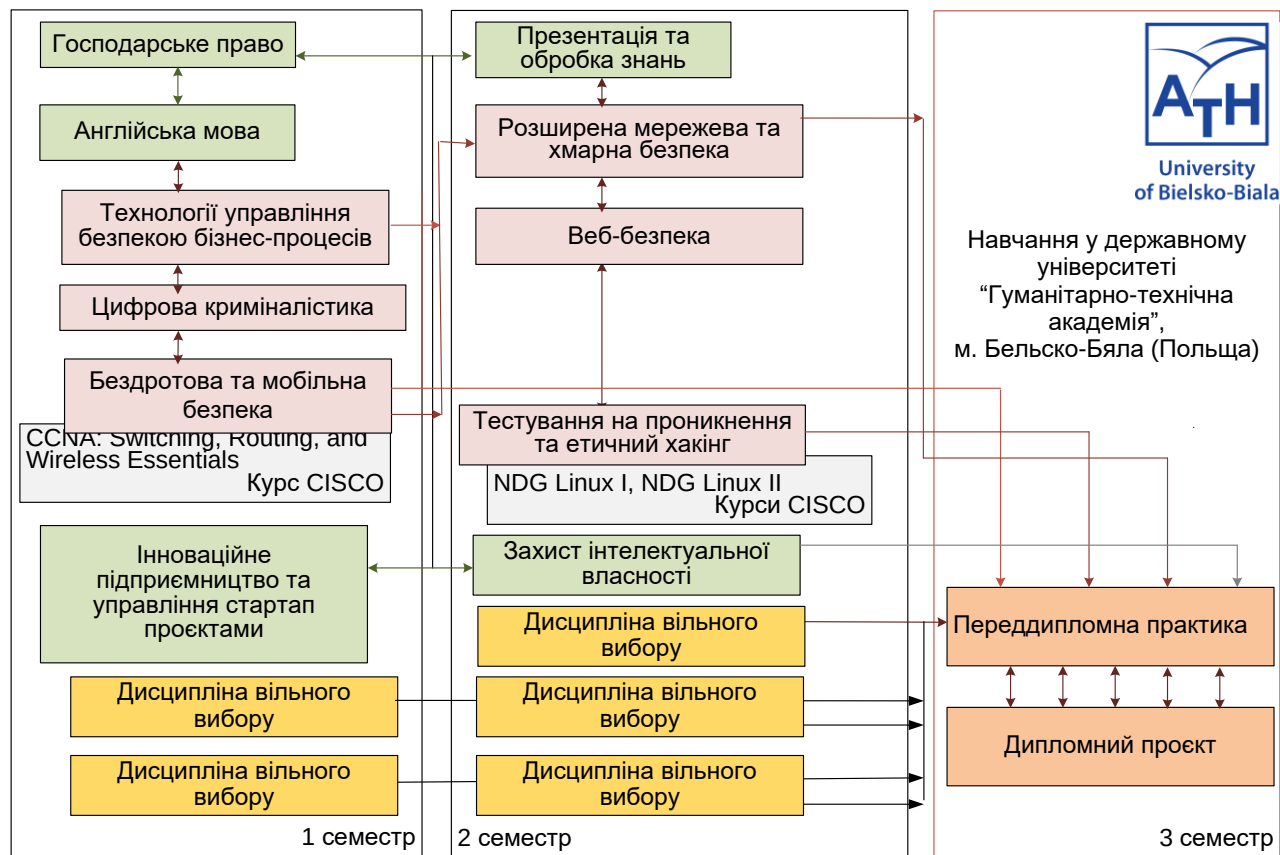
Перелік компонент ОПП

Код н/д	Компоненти освітньо-професійної програми	Кількість кредитів	Форма підсумкового контролю
1	2	3	4
Обов'язкові компоненти ОПП (здобувачі вищої освіти – громадяни України)			
Загальна підготовка			
ЗП 1	Господарське право	3	Залік
ЗП 2	Презентація та обробка знань	3	Залік
ЗП 3	Інноваційне підприємництво та управління стартап проєктами	3	Екзамен
ЗП 4	Англійська мова	3	Екзамен
ЗП 5	Захист інтелектуальної власності	3	Залік
Спеціальна (фахова) підготовка			
ПП1	Технології управління безпекою бізнес-процесів	3	Залік
ПП2	Розширена мережева та хмарна безпека	3	Екзамен
ПП3	Веб-безпека	3	Екзамен
ПП4	Бездротова та мобільна безпека	4	Екзамен
ПП5	Цифрова криміналістика	4	Екзамен
ПП6	Тестування на проникнення та етичний хакінг	3	Екзамен
ПП7	Практика	15	Залік
ПП	Атестація	15	
Загальний обсяг обов'язкових компонент		65	
Вибіркові компоненти ОПП (здобувачі вищої освіти – громадяни України)			
Дисципліни вільного вибору студента профільної підготовки згідно переліку			
ВВП1	Дисципліна 1	5	Залік
ВВП2	Дисципліна 2	5	Залік
ВВП3	Дисципліна 3	5	Залік
ВВП4	Дисципліна 4	5	Залік
ВВП5	Дисципліна 5	5	Залік
Загальний обсяг вибірових компонент:		25	
ЗАГАЛЬНИЙ ОБСЯГ ОСВІТНЬО-ПРОФЕСІЙНОЇ ПРОГРАМИ:		90	

Розподіл змісту освітньо-професійної програми за групами компонентів та циклами підготовки

№ п/п	Цикл підготовки	Обсяг навчального навантаження здобувачавищої освіти (кредитів ECTS / %)		
		Обов'язкові компоненти освітньо-професійної програми	Вибіркові компоненти освітньо-професійної програми	Всього за весь термін навчання
1	Загальна підготовка	15 / 55,56	-	15 / 55,56
2	Спеціальна (фахова) підготовка	50 / 16,66	-	50 / 16,66
3	Дисципліни вільного вибору	-	25 / 27,78	25 / 27,78
Всього за весь термін навчання		65 / 72,22	25 / 27,78	90 / 100

СТРУКТУРНО-ЛОГІЧНА СХЕМА



Семестр	Зміст навчальної діяльності
9	ЗП 1, ЗП 3, ЗП 4, ПП 1, ПП 4, ПП 5
10	ЗП 2, ЗП 5, ПП 2, ПП 3, ПП 6
11	ПП 7, ПП

ФОРМА АТЕСТАЦІЇ ЗДОБУВАЧІВ ВИЩОЇ ОСВІТИ

Форми атестації здобувачів вищої освіти	Атестація здійснюється у формі публічного захисту кваліфікаційної роботи.
Вимоги до кваліфікаційної роботи	Кваліфікаційна робота має розв'язувати складну задачу інформаційної безпеки та/або кібербезпеки і передбачати проведення досліджень та/або здійснення інновацій. Кваліфікаційна робота не повинна містити академічного плагіату, фабрикації, фальсифікації. Кваліфікаційна робота має бути розміщена на офіційному сайті (або у репозитарії) закладу вищої освіти або його підрозділу. Оприлюднення кваліфікаційних робіт з обмеженим доступом здійснюється відповідно до вимог законодавства.

МАТРИЦЯ ВІДПОВІДНОСТІ ВИЗНАЧЕНИХ РЕЗУЛЬТАТІВ НАВЧАННЯ, КОМПЕТЕНТНОСТЕЙ ТА ОСВІТНІХ КОМПОНЕНТІВ

Матриця відповідності визначених Стандартом компетентностей / результатів навчання дескрипторам НРК та матриця відповідності визначених результатів навчання та компетентностей представлені в Таблицях 1 і 2.

Таблиця 1

Матриця відповідності визначених Стандартом компетентностей / результатів навчання дескрипторам НРК

Класифікація компетентностей за НРК	Знання	Уміння	Комунікація	Автономія та відповідальність
ЗАГАЛЬНІ КОМПЕТЕНТНОСТІ				
КЗ1	Зн1,	Ум1, Ум3	К1	АВ1, АВ2
КЗ2	Зн1,	Ум1, Ум2, Ум3		АВ2, АВ3
КЗ3	Зн1	Ум2, Ум3		АВ1
КЗ4	Зн1	Ум3		АВ1, АВ2
КЗ5	Зн1	Ум2	К1	АВ1
СПЕЦІАЛЬНІ (ФАХОВІ) КОМПЕТЕНТНОСТІ				
КФ1	Зн1	Ум2		АВ2
КФ2	Зн1,	Ум2		АВ2
КФ3	Зн1	Ум1, Ум2, Ум3	К1	АВ1, АВ2
КФ4	Зн1,	Ум1, Ум2	К1	АВ1, АВ2
КФ5	Зн1,	Ум1, Ум2	К1	АВ1, АВ2
КФ6	Зн1	Ум1, Ум2	К1	АВ1
КФ7	Зн1	Ум1, Ум2	К1	АВ1
КФ8	Зн1	Ум1, Ум2	К1	АВ1
КФ9	Зн1	Ум1, Ум2	К1	АВ1
КФ10	Зн1	Ум1, Ум2, Ум3	К1	АВ1, АВ2

Таблиця 2

**Матриця відповідності визначених результатів навчання,
компетентностей та освітніх компонентів**

Програмні результат и навчання	Компетентності														
	Інтегральна компетентність														
	Загальні компетентності					Спеціальні (фахові) компетентності									
	КЗ 1	КЗ 2	КЗ 3	КЗ 4	КЗ 5	КФ 1	КФ 2	КФ 3	КФ 4	КФ 5	КФ 6	КФ 7	КФ 8	КФ 9	КФ 10
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	+		+	+		+	+	+			+	+	+	+	

Завідувач випускової кафедри

 Сергій СВСЕБ

Керівник робочої групи

(гарант освітньої програми)

 Олександр МІЛОВ