

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

ЗАТВЕРДЖУЮ
Ректор НТУ «ХПІ»

_____ Євген СОКОЛ

«___» _____ 2025 р.

**ОСВІТНЬО-ПРОФЕСІЙНА ПРОГРАМА
«КІБЕРБЕЗПЕКА»**

Першого (бакалаврського) рівня вищої освіти

за спеціальністю **F5 – Кібербезпека та захист інформації**

галузі знань **F – Інформаційні технології**

кваліфікація **бакалавр з кібербезпеки та захисту інформації**

ЗАТВЕРДЖЕНО
ВЧЕНОЮ РАДОЮ НТУ «ХПІ»
Голова вченої ради

_____ / Євген СОКОЛ

Протокол № _____

від «___» _____ 2025 р.

Харків 2025 р.

ЛИСТ ПОГОДЖЕННЯ

Освітньо-професійної програми «Кібербезпека»

Рівень вищої освіти	Перший (бакалаврський)
Галузь знань	F – Інформаційні технології
Спеціальність	F5 – Кібербезпека та захист інформації
Кваліфікація	Бакалавр з кібербезпеки та захисту інформації

СХВАЛЕНО

Робочою групою ОПП із спеціальності
«Кібербезпека та захист інформації»
Гарант ОПП

_____ Сергій ЄВСЕЄВ
« ____ » _____ 2025 р.

РЕКОМЕНДОВАНО

Методичною радою НТУ «ХПІ»
Заступник голови методичної ради

_____ Руслан МИГУЩЕНКО
« ____ » _____ 2025 р.

ПОГОДЖЕНО

Завідувач кафедри
кібербезпека

_____ Сергій ЄВСЕЄВ
« ____ » _____ 2025 р.

ПОГОДЖЕНО

Директор навчально-наукового інституту
комп'ютерних наук та інформаційних
технологій

_____ Михайло ГОДЛЕВСЬКИЙ
« ____ » _____ 2025 р.

ПОГОДЖЕНО

Здобувач вищої освіти
(член робочої групи ОПП)
№ групи КН-11226

_____ Діана СПІКО
« ____ » _____ 2025 р.

РЕЦЕНЗЕНТИ:

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

1. МОЛОДЕЦЬКА Катерина Валеріївна, доктор технічних наук, професор, професор кафедри менеджменту організацій Києво-Могилянської бізнес-школи Національний університет «Києво-Могилянська академія»
2. КОВТУН Владислав Юрійович, кандидат технічних наук, доцент, директор ТОВ “Сайфер”
3. ГОЛОВАШИЧ Сергій Олександрович, кандидат технічних наук, доцент директор ТОВ “Мікрокрипт Текнолоджіс”
4. ВОЛОЩУК Олена Борисівна, кандидат технічних наук, керівник освітніх програм ТОВ “Distributed Lab”.
5. ШАПОВАЛ Ольга Сергіївна, виконавчий директор Громадської спілки «Харківський кластер інформаційних технологій»

Рецензії

ПЕРЕДМОВА

Відповідає Стандарту вищої освіти першого (бакалаврського) рівня галузі знань F “Інформаційні технології”, спеціальності F5 “Кібербезпека та захист інформації”, затвердженого та введеного в дію наказом Міністерства освіти і науки України від 29.10.2024 р. № 1547.

Розроблено робочою групою освітньо-професійної програми “Кібербезпека” Навчально-наукового інституту комп’ютерних наук та інформаційних технологій Національного технічного університету “Харківський політехнічний інститут” у складі:

Гарант освітньо-професійної програми

ЄВСЕЄВ Сергій Петрович, доктор технічних наук, професор, завідувач кафедри кібербезпеки.

Члени робочої групи ОПП:

1. КОРОЛЬ Ольга Григорівна, кандидат технічних наук, доцент, доцент кафедри кібербезпеки.
2. ПОГАСІЙ Сергій Сергійович, доктор технічних наук, доцент, професор кафедри кібербезпеки.
3. МІЛЕВСЬКИЙ Станіслав Валерійович, доктор технічних наук, доцент, професор кафедри кібербезпеки.
4. СПІКО Діана Сергіївна, студентка групи КН-1122б.

1. ПРОФІЛЬ ОСВІТНЬО-ПРОФЕСІЙНОЇ ПРОГРАМИ ЗА СПЕЦІАЛЬНІСТЮ F5 – КІБЕРБЕЗПЕКА ТА ЗАХИСТ ІНФОРМАЦІЇ

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	Бакалавр Освітня кваліфікація: бакалавр з кібербезпеки та захисту інформації. Кваліфікація в дипломі: бакалавр з кібербезпеки та захисту інформації
Офіційна назва освітньо-професійної програми	Кібербезпека
Тип диплому та обсяг освітньо-професійної програми	Диплом бакалавра, одиничний, 240 кредитів ЄКТС, термін навчання 3 роки 10 місяців
Наявність акредитації	Національне агентство забезпечення якості вищої освіти. Україна. Сертифікат № 9111 термін дії до 01.07.2029р.
Цикл/рівень	перший (бакалаврський) рівень вищої освіти; НРК України – 6 рівень, FQ-EHEA– перший цикл, EQF LLL – 6 рівень
Передумови	Для здобуття освітнього ступеня бакалавра зі спеціальності F5 Кібербезпека та захист інформації можуть вступати особи, які здобули повну загальну середню освіту. Прийом на основі здобутого ступеня молодшого бакалавра, фахового молодшого бакалавра або освітньо-кваліфікаційного рівня молодшого спеціаліста здійснюється в порядку, визначеному законодавством.
Мова викладання	Українська мова, англійська мова
Термін дії освітньо-професійної програми	Переглядається щорічно
Посилання на постійне розміщення опису освітньо-професійної програми	https://blogs.kpi.kharkov.ua/v2/quality/dokumenty/diyuchy-osvitni-programy/osvitnij-riven-bakalavr/
2 – Мета освітньої програми	
Підготовка фахівців, здатних використовувати і впроваджувати технології інформаційної та/або кібербезпеки, а також технологій цифрової економіки.	
3 – Характеристика освітньої програми	
Предметна область (галузь знань, спеціальність)	Галузь знань: F “Інформаційні технології” Спеціальність: F5 “Кібербезпека та захист інформації” Об’єкти вивчення:

	– технології кібербезпеки та захисту інформації; – процеси управління кібербезпекою та захистом інформації; об'єкти інформаційної діяльності, в тому числі інформаційні та інформаційно-комунікаційні системи, інформаційні ресурси і технології. Цілі навчання: підготовка фахівців, здатних використовувати і впроваджувати технології кібербезпеки та захисту інформації та розв'язувати складні задачі у галузі кібербезпеки та захисту інформації. Теоретичний зміст предметної області: принципи, концепції, теорії захисту життєво важливих інтересів людини, суспільства, держави під час використання кіберпростору, за якого забезпечуються сталий розвиток інформаційного суспільства та цифрового комунікативного середовища, своєчасне виявлення, запобігання і нейтралізація реальних і потенційних загроз національній безпеці України у кіберпросторі. Методи, методики та технології: методи, методики та технології розв'язання теоретичних і практичних задач кібербезпеки та захисту інформації. Інструменти та обладнання: засоби, пристрої, мережне устаткування, прикладне та спеціалізоване програмне забезпечення, інформаційні системи та комплекси проектування, моделювання, контролю, моніторингу, зберігання, обробки, відображення та захисту даних (інформаційних потоків).
Орієнтація освітньо-професійної програми	Професійна підготовка фахівців у сфері кібербезпеки та захисту інформації
Основний фокус освітньо-професійної програми та спеціалізації	Спеціальна освіта у галузі інформаційних технологій зі спеціальності F5 “Кібербезпека та захист інформації”. Поглиблене вивчення інформаційних технологій захисту інформації, інформаційної безпеки, кібербезпеки, та безпеки інформації, розробки та використання програмного забезпечення захисту інформації, кібербезпеки та інформаційної безпеки. Ключові слова: кібербезпека, інформаційна безпека, захист інформації, інформаційні технології.
Особливості програми	Особливістю програми спеціальності “Кібербезпека та захист інформації” є орієнтація на сучасні вимоги до фахівців в галузі інформаційної та/або кібербезпеки, набуття здобувачами вищої освіти конкурентоспроможних компетентностей на основі синергізму отримання результатів навчання з інформаційної та/або кібербезпеки та програмування, використання курсів мережевої академії Cisco з Networking, Cybersecurity, IoT & Data Analytics, OS and IT, Programming Courses. Можливість навчатися англійською мовою.
4 – Придатність випускників до працевлаштування та подальшого навчання	

Придатність до працевлаштування	Працевлаштування на посади у структурних установ/підприємств/організацій, які передбачають наявність вищої освіти зі спеціальності F5 Кібербезпека та захист інформації. Фахівці з кібербезпеки та захисту інформації можуть працювати на посадах, згідно з чинною редакцією Національного класифікатора України: Класифікатор професій ДК 003:2010, а саме: 2139.2 Фахівець сфери захисту інформації; 2139.2 Фахівець з питань безпеки (інформаційно-комунікаційні технології); 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 безпеки та захисту інформації; 2139.2 Аудитор інформаційних технологій (з кібербезпеки); 2139.2 Фахівець з оцінки заходів захисту інформації (кібербезпеки).
Подальше навчання	Студени, які пройшли підготовку за даною навчальною програмою та отримали диплом бакалавра, мають право на здобуття освіти на другому (магістерському) рівні вищої освіти у ЗВО України та за кордоном в галузі знань “Інформаційні технології” або суміжних. Здобуття або вдосконалення освіти та професійної підготовки в системі дорослих.
5 – Викладання та оцінювання	
Викладання та навчання	Студентоцентроване навчання, проблемно-орієнтоване навчання, дистанційне навчання в системі Microsoft 365, самонавчання, навчання через проєктну практику, навчання через лабораторну практику. У процесі викладання передбачено застосування таких навчальних технологій, як: лекції, лабораторні роботи, практичні заняття, робота в малих групах, семінари-дискусії, brainstorming, презентації, що розвивають комунікативні та лідерські навички, самостійна робота з літературними джерелами; змішані форми навчання з використанням дистанційних платформ.
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. Підсумковий контроль – усні та письмові екзамени, заліки з урахуванням накопичених балів поточного контролю, захист звітів з лабораторних занять, захист курсових робіт. Державна атестація – єдиний державний кваліфікаційний іспит. 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 розв'язувати складні спеціалізовані задачі і практичні завдання у галузі кібербезпеки та захисту інформації.
Загальні компетентності (визначені стандартом вищої освіти спеціальності)	ЗК1. Здатність застосовувати знання у практичних ситуаціях. ЗК2. 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 і свобод людини і громадянина в Україні. ЗК 7. Здатність ухвалювати рішення й діяти дотримуючись принципу неприпустимості 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 (визначені стандартом вищої освіти спеціальності)	СК1. Здатність застосовувати законодавчу та нормативно-правову базу, а також державні та міжнародні вимоги, практики і стандарти у професійній діяльності. СК2. Здатність використовувати інформаційні технології, сучасні методи і моделі кібербезпеки та систем захисту інформації. СК3. Здатність забезпечувати неперервність бізнес-процесів згідно встановленої політики кібербезпеки та захисту інформації. СК4. Здатність забезпечувати захист інформації в інформаційних та інформаційно-комунікаційних системах згідно встановленої політики кібербезпеки й захисту інформації. СК5. Здатність відновлювати функціонування інформаційних та інформаційно-комунікаційних систем після реалізації загроз, здійснення кібератак, збоїв і відмов різних класів та походження. СК6. Здатність впроваджувати та забезпечувати функціонування комплексних систем захисту інформації

	(комплекси нормативно-правових, організаційних та технічних засобів і методів, процедур, практичних прийомів тощо.) СК7. Здатність здійснювати професійну діяльність на основі впровадженої системи управління інформаційною та кібербезпекою. СК8. Здатність застосовувати методи та засоби криптографічного захисту інформації на об'єктах інформаційної діяльності. СК9. Здатність застосовувати методи та засоби технічного захисту інформації на об'єктах інформаційної діяльності. СК10. Здатність виконувати моніторинг інформаційних процесів, аналізувати, виявляти, оцінювати можливі вразливості та загрози інформаційному простору й інформаційним ресурсам згідно з встановленою політикою інформаційної безпеки.
7 – Результати навчання	
Результати навчання за спеціальністю (визначені стандартом вищої освіти спеціальності)	РН1. Вільно спілкуватися державною мовою усно та письмово при виконанні професійних обов'язків. РН2. Спілкуватися іноземною мовою з метою забезпечення ефективності професійної комунікації. РН3. Застосовувати принцип неприпустимості корупції та будь-яких інших проявів недоброчесності у професійній діяльності. РН4. 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. РН5. 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. РН6. Адаптуватися до нових умов і технологій професійної діяльності, прогнозувати кінцевий результат. РН7. Застосовувати й адаптувати теорії інформації та кодування, математичної статистики, чисел, криптографії та стеганографії, оброблення та передачі сигналів тощо, принципи, методи і поняття кібербезпеки та захисту інформації у навчанні та професійній діяльності. РН8. Застосовувати знання й розуміння математики та фізики в професійній діяльності, формалізувати задачі предметної галузі кібербезпеки та захисту інформації, формулювати їх математичну постановку та обирати раціональний метод вирішення. РН9. Знати та застосовувати законодавство України та міжнародні вимоги, практики і стандарти з метою здійснення професійної діяльності в галузі кібербезпеки та захисту інформації.

	RH10. Використовувати сучасні інформаційні технології, методи і моделі кібербезпеки та систем захисту інформації для здійснення професійної діяльності. RH11. Планувати підготовку та забезпечувати неперервність бізнес-процесів в організаціях згідно зі встановленою політикою кібербезпеки з урахуванням вимог до захисту інформації. RH12. Застосовувати методи та засоби захисту інформації в інформаційних та інформаційно-комунікаційних системах відповідно до встановленої політики інформаційної безпеки. RH13. 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. RH14. 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. RH15. Збирати, обробляти, зберігати, аналізувати критичні дані для доказу реалізації кіберзагроз, проводити аналіз та дослідження кіберінциденту з метою оперативного відновлення функціонування інформаційної системи. RH16. Вирішувати задачі впровадження та супроводу комплексних систем захисту інформації в інформаційних системах. RH17. 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. RH18. Аналізувати, застосовувати методи та засоби криптографічного захисту інформації на об'єктах інформаційної діяльності. RH19. Вирішувати задачі щодо організації та контролю стану криптографічного захисту інформації, зокрема відповідно до вимог нормативних документів. RH20. 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. RH21. 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	
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, зі змінами, внесеними згідно з Постановою КМУ № 365 від 24.03.2021. Додаток 15-16). 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, зі змінами, внесеними згідно з Постановою КМУ № 365 від 24.03.2021. Додаток 17). Навчально-науково-виробнича база у вигляді: –навчальні корпуси, комп’ютерні класи, об’єднані локальною обчислювальною мережею з виходом до Інтернету, мультимедійне обладнання;–спеціалізоване програмне забезпечення.
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, (зі змінами, внесеними згідно з Постановою КМУ № 365 від 24.03.2021. Додаток 18). Застосування у навчальному процесі LMS (Learning Management System). Доступ до електронного репозитарію НТУ “ХПІ” (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. Угоди про співпрацю щодо реалізації програм внутрішньої академічної мобільності здобувачів вищої освіти за освітньою програмою “Кібербезпека” спеціальності F5 “Кібербезпека та захист інформації” з Одеським національним технологічним університетом, Чернігівським національним технологічним університетом.
Міжнародна	На основі двостороннього договору з університетом ім. Яна

кредитна мобільність	Длугоша в м. Ченстохові (Польща).
Навчання іноземних здобувачів вищої освіти	Підготовка іноземних громадян та осіб без громадянства здійснюється українською або англійською мовою відповідно до вимог Закону України «Про вищу освіту»..

2. ПЕРЕЛІК ОСВІТНІХ КОМПОНЕНТ ОСВІТНЬО-ПРОФЕСІЙНОЇ ПРОГРАМИ «КІБЕРБЕЗПЕКА» ТА ЇХ ЛОГІЧНА ПОСЛІДОВНІСТЬ

2.1 Перелік компонент ОПП

Код н/д	Компоненти освітньо-професійної програми	Кількість кредитів	Форма підсумкового контролю
1	2	3	4
1. Обов'язкові компоненти ОПП (здобувачі вищої освіти, як громадяни України, так і іноземці)			
1.1 Загальна підготовка (здобувачі вищої освіти – громадяни України)			
ЗП 1	Історія та культура України	4	Екзамен
ЗП 2	Українська мова (професійного спрямування)	3	Залік
ЗП 3	Іноземна мова	16	Залік, Екзамен
ЗП 4	Фізика	6	Екзамен
ЗП 5	Основи гуманітарно-філософських знань у професійній діяльності	4	Екзамен
ЗП 6	Вища математика	12	Залік, Екзамен
ЗП	Фізичне виховання	8	Залік
1.1 Загальна підготовка (здобувачі вищої освіти – іноземці)			
ЗП 1	Історія та культура України	4	Екзамен
ЗП 2	Іноземна мова	4	Залік, Екзамен
ЗП 3	Українська мова як іноземна	12	Залік, Екзамен
ЗП 4	Фізика	6	Екзамен
ЗП 5	Основи гуманітарно-філософських знань у професійній діяльності	4	Екзамен
ЗП 6	Вища математика	12	Залік, Екзамен
ЗП 7	Мова професійного навчання	9	Залік, Екзамен
ЗП	Фізичне виховання	6	Залік
1.2 Спеціальна (фахова) підготовка			
СП 1	Вступ до спеціальності. Ознайомча практика	3	Залік
СП 2	Основи програмування	4	Екзамен
СП 3	Теорія інформації і кодування	3	Екзамен
СП 4	Правове регулювання кібербезпеки	4	Залік
СП 5	Алгоритми та структури даних	5	Екзамен
СП 6	Фізичні основи технічних засобів розвідки	5	Екзамен
СП 7	Інформаційна безпека держави	3	Залік
СП 8	Основи соціальної інженерії	4	Залік
СП 9	Математичні основи криптології	4	Екзамен
СП 10	Технології програмування	5	Екзамен
СП 11	Комп'ютерні мережі	5	Екзамен
СП 12	Архітектура та захист операційних систем	5	Залік
СП 13	Інструментальні засоби програмування	6	Екзамен

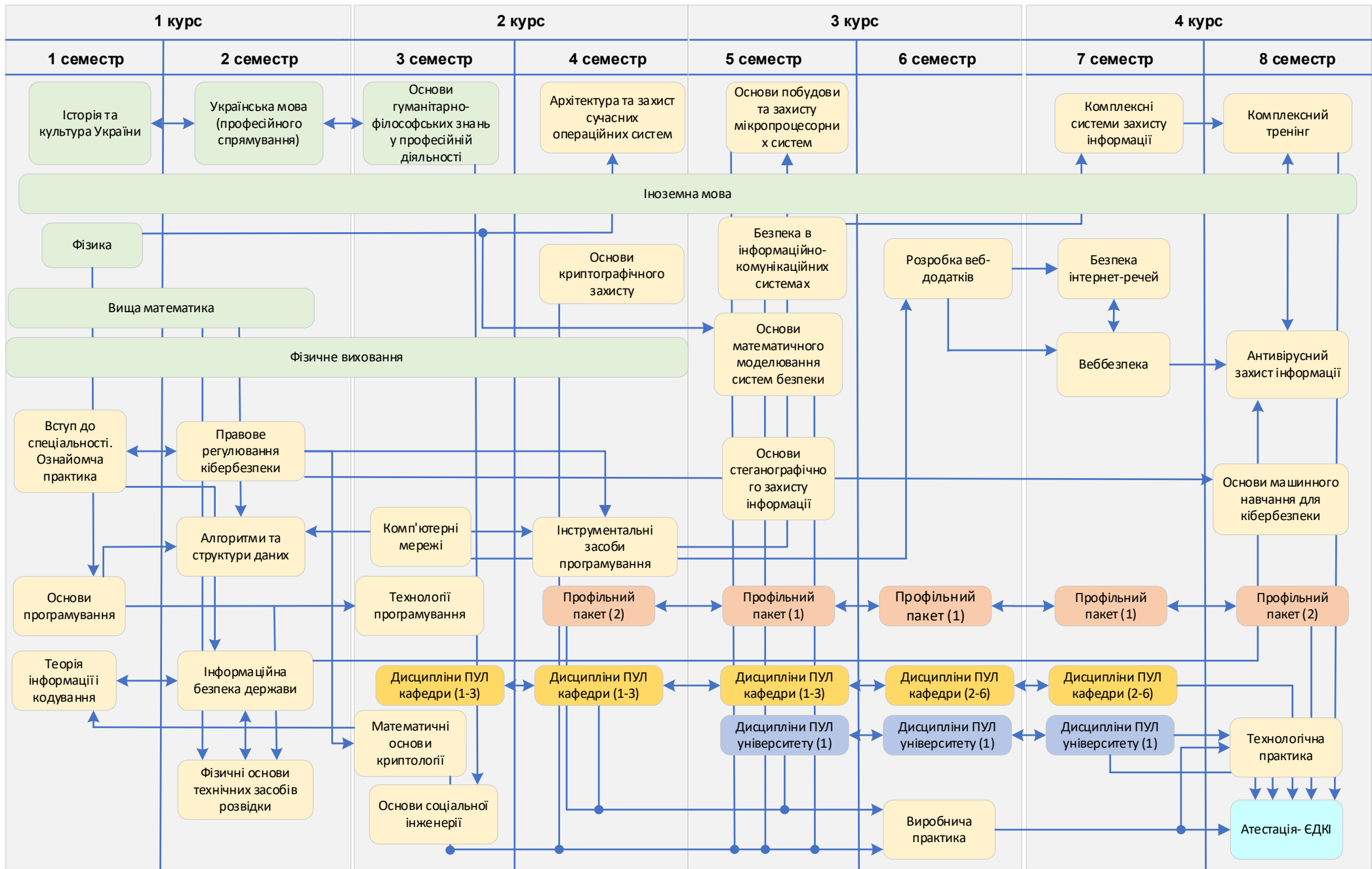
1	2	3	4
СП 14	Основи криптографічного захисту	5	Залік
СП 15	Основи побудови та захисту мікропроцесорних систем	4	Екзамен
СП 16	Основи математичного моделювання систем безпеки	4	Екзамен
СП 17	Основи стеганографічного захисту інформації	5	Залік
СП 18	Безпека в інформаційно-комунікаційних системах	4	Залік
СП 19	Розробка веб-додатків	6	Екзамен
СП 20	Комплексні системи захисту інформації	4	Екзамен
СП 21	Безпека інтернет-речей	4	Залік
СП 22	Веббезпека	5	Залік
СП 23	Комплексний тренінг	4	Залік
СП 24	Антивірусний захист інформації	5	Залік
СП 25	Основи машинного навчання для кібербезпеки	4	Екзамен
2. Практична підготовка			
ПП 1	Виробнича практика	6	Залік
ПП 2	Технологічна практика	6	Залік
3. Атестація			
СП	Атестація	3	
Загальний обсяг обов'язкових компонент		178	
4. Вибіркові компоненти ОПП (здобувачі вищої освіти, як громадяни України, так і іноземці)			
Профільований пакет дисциплін 01 <u>“Штучний інтелект в системах захисту”</u>			
ВП1.1	Етичний хакінг	3	Екзамен
ВП1.2	Дата майнінг	3	Екзамен
ВП1.3	Математичні основи штучного інтелекту	3	Екзамен
ВП1.4	Python для штучного інтелекту та машинного навчання	4	Екзамен
ВП1.5	Генетичні алгоритми	3	Екзамен
ВП1.6	Python для інтернет-речей	3	Екзамен
ВП1.7	Системний інжиніринг	3	Екзамен
Профільований пакет дисциплін 02 <u>“Блокчейн-технологія та безпека банківських систем”</u>			
ВП2.1	Децентралізовані системи	3	Екзамен
ВП2.2	Ризик-менеджмент	3	Екзамен
ВП2.3	Blockchain: основи та приклади застосування	3	Екзамен
ВП2.4	Безпека банківських систем	4	Екзамен
ВП2.5	Захист об'єктів критичної інфраструктури	3	Екзамен
ВП2.6	Організація документообігу з обмеженим доступом	3	Екзамен
ВП2.7	Безпека в соціальних мережах	3	Екзамен
Профільований пакет дисциплін 03 <u>“Innovation Campus”</u>			
ВП3.1	Основи кібербезпеки	3	Екзамен
ВП3.2	Розробка корпоративних інформаційних	3	Екзамен

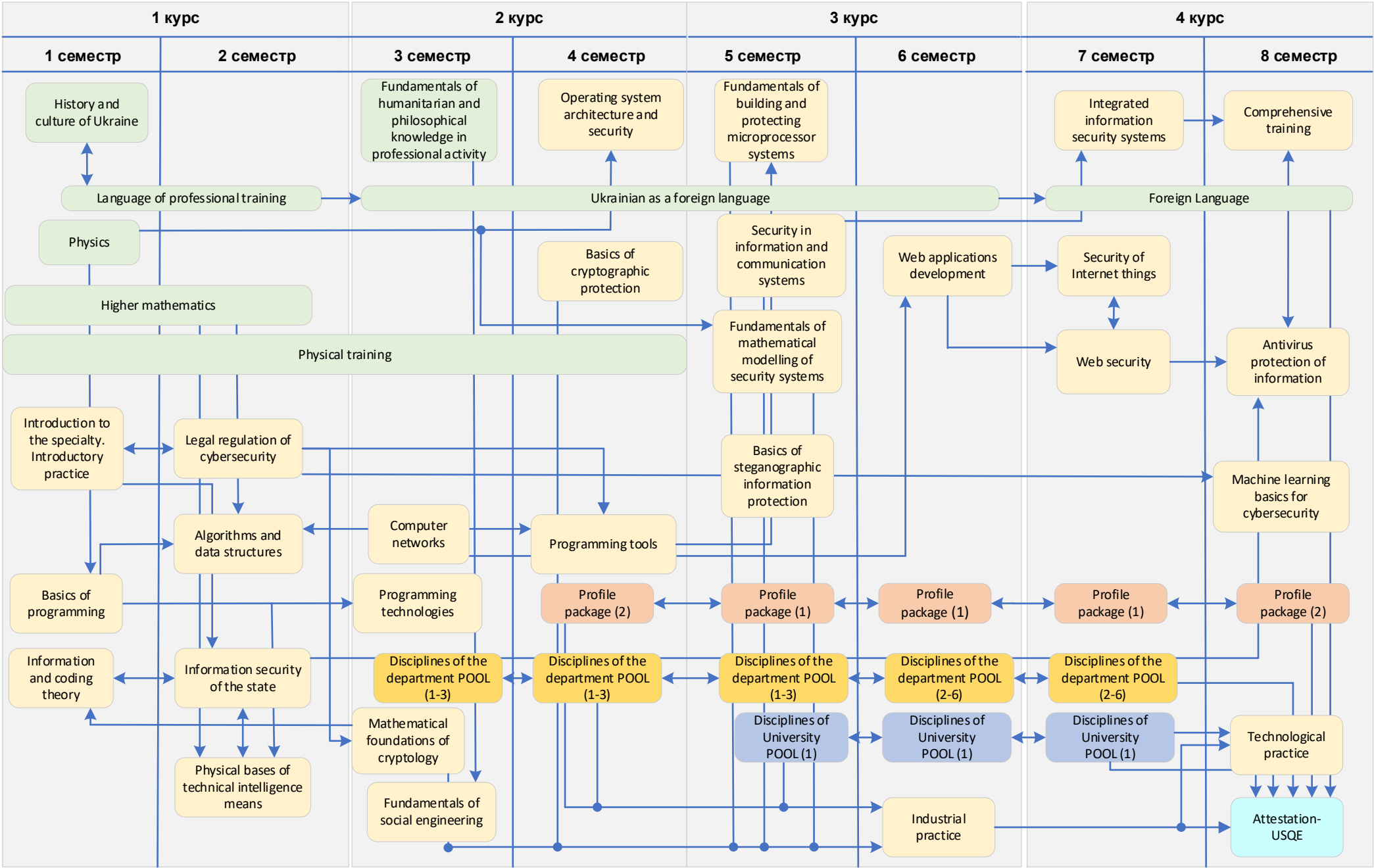
	систем (частина 1)		
ВПЗ.3	Розробка корпоративних інформаційних систем (частина 2)	3	Екзамен
ВПЗ.4	Бази даних для корпоративних інформаційних систем	4	Екзамен
ВПЗ.5	Архітектура корпоративних інформаційних систем	3	Екзамен
ВПЗ.6	Безпека та аудит бездротових та рухомих мереж	3	Екзамен
ВПЗ.7	Захист об'єктів критичної інфраструктури	3	Екзамен
Дисципліни вільного вибору студента профільної підготовки згідно переліку			
ОКВП1	ОК ВВ ПП 1	4	Залік
ОКВП2	ОК ВВ ПП 2	4	Залік
ОКВП3	ОК ВВ ПП 3	4	Залік
ОКВП4	ОК ВВ ПП 4	4	Залік
ОКВП5	ОК ВВ ПП 5	4	Залік
ОКВП6	ОК ВВ ПП 6	4	Залік
ОКВП7	ОК ВВ ПП 7	4	Залік
Дисципліни вільного вибору студента із загальноуніверситетського каталогу дисциплін			
ОКВ1	ОК ВВ ЗП 1	4	Залік
ОКВ2	ОК ВВ ЗП 2	4	Залік
ОКВ3	ОК ВВ ЗП 3	4	Залік
Загальний обсяг вибірових компонент:		62	
ЗАГАЛЬНИЙ ОБСЯГ ОСВІТНЬО-ПРОФЕСІЙНОЇ ПРОГРАМИ:		240	

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

№п/п	Цикл підготовки	Обсяг навчального навантаження здобувача вищої освіти (кредитів ECTS / %)		
		Обов'язкові компоненти освітньо-професійної програми	Вибіркові компоненти освітньо-професійної програми	Всього за весь термін навчання
1	Загальна підготовка	53 / 22,1	-	53 / 22,1
2	Спеціальна (фахова) підготовка	125 / 52,1	-	125 / 52,1
3	Дисципліни вільного вибору	-	62 / 25,8	60 / 25,8
Всього за весь термін навчання		178 / 74,2	62 / 25,8	240 / 100

3. СТРУКТУРНО-ЛОГІЧНА СХЕМА





4. ФОРМА АТЕСТАЦІЇ ЗДОБУВАЧІВ ВИЩОЇ ОСВІТИ

Форми атестації здобувачів вищої освіти	Атестація здійснюється у формі єдиного державного кваліфікаційного іспиту.
Вимоги до єдиного державного кваліфікаційного іспиту	Єдиний державний кваліфікаційний іспит передбачає оцінювання досягнень результатів навчання, визначених стандартом вищої освіти спеціальності «Кібербезпека та захист інформації» та освітньою програмою.

5. ЗВЕДЕНА ТАБЛИЦЯ ФАХОВИХ КОМПЕТЕНТНОСТЕЙ ТА ПРОГРАМНИХ РЕЗУЛЬТАТІВ НАВЧАННЯ

Фахові компетентності	Результати навчання
СК1. Здатність застосовувати законодавчу та нормативно-правову базу, а також державні та міжнародні вимоги, практики і стандарти з метою здійснення професійної діяльності в галузі кібербезпеки та захисту інформації.	РН9. Вміти застосовувати законодавчу та нормативно-правову базу, а також державні та міжнародні вимоги, практики і стандарти з метою здійснення професійної діяльності в галузі кібербезпеки та захисту інформації.
СК2. Здатність використовувати інформаційні технології, сучасні методи і моделі кібербезпеки та систем захисту інформації.	РН10. Вміти використовувати сучасні інформаційні технології, методи і моделі кібербезпеки та систем захисту інформації для здійснення професійної діяльності.
СК3. Здатність забезпечувати неперервність бізнес-процесів згідно встановленої політики кібербезпеки та захисту інформації.	РН11. Планувати підготовку та забезпечувати неперервність процесів в організаціях згідно встановленої політики кібербезпеки та з урахування вимог до захисту інформації.
СК4. Здатність забезпечувати захист інформації в інформаційних системах згідно встановленої політики кібербезпеки та захисту інформації.	РН12. Застосовувати методи захисту інформації в інформаційних системах згідно встановленої політики інформаційної безпеки. РН13. Впроваджувати, налаштовувати, супроводжувати та підтримувати функціонування програмних та програмно-апаратних комплексів і систем кібербезпеки та захисту інформації як необхідні процедури для функціонування інформаційних систем та\або інфраструктури організації в цілому.
СК5. Здатність відновлювати функціонування інформаційних систем після реалізації загроз, здійснення кібератак, збоїв та відмов різних класів та походження.	РН14. Вирішувати задачі управління процесами відновлення штатного функціонування інформаційних систем з використанням процедур резервування згідно встановленої політики безпеки та забезпечувати функціонування спеціального програмного забезпечення, щодо захисту та відновлення інформації; РН15. Збирати, обробляти, зберігати, аналізувати критичні дані для доказу реалізації кіберзагроз, проводити аналіз та дослідження кіберінциденту з метою оперативного відновлення функціонування інформаційної системи.
СК6. Здатність впроваджувати та забезпечувати функціонування	РН16. Вирішувати задачі впровадження та супроводу комплексних систем захисту

комплексних систем захисту інформації (комплекси нормативно-правових, організаційних та технічних засобів і методів, процедур, практичних прийомів тощо).	інформації в інформаційних системах.
СК7. Здатність здійснювати професійну діяльність на основі впровадженої системи управління інформаційною та кібербезпекою.	РН17. Забезпечувати функціонування системи управління кібербезпекою та захистом інформації організації, включаючи персонал та управління наслідками реалізації загроз інформаційній безпеці в кризових ситуаціях, на основі здійснення процедур кількісної і якісної оцінки ризиків.
СК8. Здатність застосовувати методи та засоби криптографічного захисту інформації на об'єктах інформаційної діяльності.	РН18. Аналізувати, застосовувати методи та засоби криптографічного захисту інформації на об'єктах інформаційної діяльності. РН19. Вирішувати задачі щодо організації та контролю стану криптографічного захисту інформації, зокрема відповідно до вимог нормативних документів.
СК9. Здатність застосовувати методи та засоби технічного захисту інформації на об'єктах інформаційної діяльності.	РН20. 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 та контроль стану апаратних засобів захисту інформації та комплексів технічного захисту інформації.
СК10. Здатність виконувати моніторинг інформаційних процесів, аналізувати, виявляти та оцінювати можливі вразливості та загрози інформаційному простору й інформаційним ресурсам згідно з встановленою політикою інформаційної безпеки.	РН21. Виконувати впровадження, підтримку, аналіз ефективності систем виявлення несанкціонованого доступу, дій з інформацією в інформаційній системі, вразливостей, можливих загроз інформаційному простору та інформаційним ресурсам та використовувати комплекси захисту для забезпечення необхідного рівня захищеності інформації в інформаційних системах.

6. МАТРИЦЯ ВІДПОВІДНОСТІ ВИЗНАЧЕНИХ СТАНДАРТОМ КОМПЕТЕНТНОСТЕЙ / РЕЗУЛЬТАТІВ НАВЧАННЯ ДЕСКРИПТОРАМ НРК

Класифікація компетентностей за НРК	Знання	Уміння	Комунікація	Відповідальність і автономія
ЗАГАЛЬНІ КОМПЕТЕНТНОСТІ				
ЗК1. Здатність застосовувати знання у практичних ситуаціях.	+	+		
ЗК2. 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 і свобод людини і громадянина в Україні.	+		+	+
ЗК 7. Здатність ухвалювати рішення й діяти дотримуючись принципу неприпустимості 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) КОМПЕТЕНТНОСТІ				
СК1. Здатність застосовувати законодавчу та нормативно-правову базу, а також державні та міжнародні вимоги, практики і стандарти у професійній діяльності.	+	+	+	
СК2. Здатність використовувати інформаційні технології, сучасні методи і моделі кібербезпеки та систем захисту інформації.	+	+	+	
СК3. Здатність забезпечувати неперервність бізнес-процесів згідно встановленої політики кібербезпеки та захисту інформації.		+		+

СК4. Здатність забезпечувати захист інформації в інформаційних та інформаційно-комунікаційних системах згідно встановленої політики кібербезпеки й захисту інформації.		+		+
СК5. Здатність відновлювати функціонування інформаційних та інформаційно-комунікаційних систем після реалізації загроз, здійснення кібератак, збоїв і відмов різних класів та походження.		+	+	+
СК6. Здатність впроваджувати та забезпечувати функціонування комплексних систем захисту інформації (комплекси нормативно-правових, організаційних та технічних засобів і методів, процедур, практичних прийомів тощо).		+	+	+
СК7. Здатність здійснювати професійну діяльність на основі впровадженої системи управління інформаційною та кібербезпекою.		+	+	+
СК8. Здатність застосовувати методи та засоби криптографічного захисту інформації на об'єктах інформаційної діяльності.	+	+		
СК9. Здатність застосовувати методи та засоби технічного захисту інформації на об'єктах інформаційної діяльності.	+	+		
СК10. Здатність виконувати моніторинг інформаційних процесів, аналізувати, виявляти, оцінювати можливі вразливості та загрози інформаційному простору й інформаційним ресурсам згідно з встановленою політикою інформаційної безпеки.		+	+	+

[illegible]

Результати навчання	Компетентності																		
	Інтегральна компетентніс	Загальні компетентності								Спеціальні (фахові) компетентності									
		ЗК1	ЗК2	ЗК3	ЗК4	ЗК5	ЗК6	ЗК7	ЗК8	СК1	СК2	СК3	СК4	СК5	СК6	СК7	СК8	СК9	СК10
		СП4, СП5, СП7, СП8, СП9, СП10, СП11, СП12, СП14, СП15, СП16, СП16, СП17, СП19, СП21, СП22, СП23, СП24, СП25, ПП1, ПП2	СП2, СП5, СП4, СП6, СП7, СП10, СП13, СП14, СП15, СП16, СП17, СП18, СП19, СП20, СП21, СП22, СП23, СП25, ПП1, ПП2																
PH5	СП	ЗП4, ЗП, СП2, СП3, СП4, СП5, СП7, СП8, СП9, СП10, СП11, СП12, СП14, СП15, СП16,	ЗП4, ЗП5, ЗП6, СП1, СП2, СП4, СП5, СП6, СП7, СП10, СП13, СП14, СП15, СП16, СП17,																

Результати навчання	Компетентності																		
	Інтегральна компетентніс	Загальні компетентності								Спеціальні (фахові) компетентності									
		ЗК1	ЗК2	ЗК3	ЗК4	ЗК5	ЗК6	ЗК7	ЗК8	СК1	СК2	СК3	СК4	СК5	СК6	СК7	СК8	СК9	СК10
		СП19, СП21, СП22, СП23, СП24, СП25, ПП1, ПП2	СП18, СП19, СП20, СП21, СП22, СП23, СП25, ПП1, ПП2																
PH6	СП		ЗП4, ЗП5, ЗП6, СП1, СП2, СП4, СП5, СП6, СП7, СП10, СП13, СП14, СП15, СП16, СП17, СП18, СП19, СП20, СП21, СП22, СП23, СП25, ПП1, ПП2						ЗП1, ЗП4, ЗП5, ЗП, СП1, СП3, СП17, СП20, СП23, СП25										
PH7	СП	ЗП4, ЗП,							ЗП1, ЗП4,										

Результати навчання	Компетентності																		
	Інтегральна компетентність	Загальні компетентності								Спеціальні (фахові) компетентності									
		ЗК1	ЗК2	ЗК3	ЗК4	ЗК5	ЗК6	ЗК7	ЗК8	СК1	СК2	СК3	СК4	СК5	СК6	СК7	СК8	СК9	СК10
		СП2, СП3, СП4, СП5, СП7, СП8, СП9, СП10, СП11, СП12, СП14, СП15, СП16, СП19, СП21, СП22, СП23, СП24, СП25, ПП1, ПП2							ЗП5, ЗП, СП1, СП3, СП17, СП20, СП23										
PH8	СП					ЗП4, ЗП6, СП1, СП2, СП3, СП4, СП5, СП6, СП7, СП9, СП10, СП11, СП12, СП14,													

Результати навчання	Компетентності																			
	Інтегральна компетентніс	Загальні компетентності								Спеціальні (фахові) компетентності										
		ЗК1	ЗК2	ЗК3	ЗК4	ЗК5	ЗК6	ЗК7	ЗК8	СК1	СК2	СК3	СК4	СК5	СК6	СК7	СК8	СК9	СК10	
					СП15, СП16, СП23, СП25															
PH9	СП					ЗП1, СП1, СП4, СП7				СП1, СП7, СП8, СП10, СП11, СП14, СП20, СП23, СП24										
PH10	СП										СП2, СП3, СП5, СП8, СП9, СП10, СП11, СП12, СП14, СП16, СП18, СП19, СП20, СП21, СП22, СП23, СП24, СП25, ПП1, ПП2									
PH11	СП											СП11, СП14,								

Результати навчання	Компетентності																		
	Інтегральна компетентніс	Загальні компетентності								Спеціальні (фахові) компетентності									
		ЗК1	ЗК2	ЗК3	ЗК4	ЗК5	ЗК6	ЗК7	ЗК8	СК1	СК2	СК3	СК4	СК5	СК6	СК7	СК8	СК9	СК10
												СП20, СП21, СП24							
PH12	СП												СП9, СП11, СП12, СП14, СП19, СП20, СП21, СП22, СП23, СП24, СП25						
PH13	СП												СП9, СП11, СП12, СП14, СП19, СП20, СП21, СП22, СП23, СП24, СП25						
PH14	СП													СП8, СП11, СП14, СП15, СП21, СП24, СП25					
PH15	СП													СП8, СП11, СП14,					

Результати навчання	Компетентності																		
	Інтегральна компетентність	Загальні компетентності								Спеціальні (фахові) компетентності									
		ЗК1	ЗК2	ЗК3	ЗК4	ЗК5	ЗК6	ЗК7	ЗК8	СК1	СК2	СК3	СК4	СК5	СК6	СК7	СК8	СК9	СК10
														СП15, СП21, СП24, СП25					
PH16	СП														СП11, СП12, СП14, СП20, СП23, СП25, ПП2				
PH17	СП															СП7, СП16, СП23, СП25, ПП1, ПП2			
PH18	СП																СП3, СП9, СП11, СП12, СП14, СП15, СП18, СП21, СП23, СП24, ПП2		
PH19	СП																СП3, СП9, СП11, СП12, СП14, СП15,		

Результати навчання	Компетентності																		
	Інтегральна компетентність	Загальні компетентності								Спеціальні (фахові) компетентності									
		ЗК1	ЗК2	ЗК3	ЗК4	ЗК5	ЗК6	ЗК7	ЗК8	СК1	СК2	СК3	СК4	СК5	СК6	СК7	СК8	СК9	СК10
																	СП18, СП21, СП23, СП24, ПП2		
PH20	СП																	СП6, СП12, СП14, СП15, СП19, СП20, СП22, СП23, ПП2	
PH21	СП																		СП8, СП11, СП14, СП16, СП18, СП23, СП24, СП25, ПП1

8. РЕЗУЛЬТАТИ ОБГОВОРЕННЯ ОСВІТНЬОЇ ПРОГРАМИ

Стейкхолдери (вказати ПІБ та посаду, місце роботи)	Рекомендація	враховано / частково враховано / не враховано	Примітка
Шаповал О. С., виконавчий директор Громадської спілки «Харківський кластер інформаційних технологій»	Приділити більше уваги опануванню принципів безпеки в базах даних. Акцентувати увагу на вивченні хмарних технологій і DevOps.	Враховано. За рахунок вибірових освітніх компонентів: Безпека в DEVOPS, Бази даних з SQL і Python	
Гарант ОПП, завідувач кафедри, д.т.н., професор Євсєєв С.П. Члени робочої групи ОПП	Освітньо-професійну програму привести у відповідність до вимог Стандарту вищої освіти за спеціальністю 125 Кібербезпека та захист інформації першого (бакалаврського) рівня вищої освіти, затвердженого та введеного в дію наказом Міністерства освіти і науки України від 24.10.2024р. № 1547.	Враховано. Зміни внесено.	
Гарант ОПП, завідувач кафедри, д.т.н., професор Євсєєв С.П. Члени робочої групи ОПП	Зміна шифру спеціальності та галузі знань (згідно з постановою Кабінету Міністрів України від 30 серпня 2024 р. No 1021).	Враховано. Зміни внесено.	
Волощук О. Б., к. т. н., керівник освітніх програм ТОВ “Distributed Lab”	Позитивний відгук. Без зауважень.	-	
Молодецька К. В., доктор технічних наук, професор, професор кафедри менеджменту організацій Києво-Могилянської бізнес- школи Національний університет «Києво-	Позитивний відгук. Без зауважень.	-	

Могилянська академія»			
Ковтун В. Ю., кандидат технічних наук, доцент, директор ТОВ “Сайфер”	Позитивний відгук. Без зауважень.	-	
Головашич С. О., кандидат технічних наук, доцент директор ТОВ “Мікрокрипт Технолоджіс”	Позитивний відгук. Без зауважень.	-	

9. ПЛАН ВРАХУВАННЯ ЗАУВАЖЕНЬ ТА ВИПРАВЛЕННЯ НЕДОЛІКІВ ЗА ОСВІТНЬОЮ ПРОГРАМОЮ

Рекомендації, надані під час останньої акредитації	Період врахування (короткостроковий/довгостроковий/не доцільно враховувати)	Заходи, направлені на врахування рекомендацій	Терміни впровадження заходів
Рекомендації експертної групи та Галузевої експертної ради			
Рекомендація 1 Переглянути в наступній редакції ОПП перелік затверджених професійних стандартів в сфері кібербезпеки відповідно до Національного класифікатора професій України ДК 003:2010.	Довгостроковий	Оновлення у ОПП переліку затверджених професійних стандартів в сфері кібербезпеки відповідно до Національного класифікатора професій України ДК 003:2010.	Березень 2026 н.р.
Рекомендація 2 Посилити поінформованість студентів щодо внутрішніх процедур організації освітнього процесу. Рекомендовано переглянути та оновити літературу в силабусах освітніх компонентів.	Довгостроковий	Посилити поінформованість студентів щодо внутрішніх процедур організації освітнього процесу. Оновити літературу в силабусах освітніх компонентів.	Травень 2026 н.р.
Рекомендація 3 Використання кіберполігону для ознайомлення здобувачів з його можливостями	Довгостроковий	Використання кіберполігону для ознайомлення здобувачів з його можливостями	Початок кожного навчального року
Рекомендація 4 Забезпечувати постійне оновлення інформації щодо всіх аспектів	Довгостроковий	Оновлення інформації щодо всіх аспектів провадження ОПП на сайті кафедри.	Початок кожного навчального року

провадження ОПП на сайті кафедри.			
-----------------------------------	--	--	--

Директор навчально-наукового інституту
комп'ютерних наук та інформаційних технологій _____ Михайло ГОДЛЕВСЬКИЙ

Гарант освітньої програми _____ Сергій ЄВСЕЄВ