МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ
«ЛЬВІВСЬКА ПОЛІТЕХНІКА»

«ЗАТВЕРДЖУЮ»
В.о.Ректора
Національного університету
«Львівська політехніка»

_____ /Юрій БОБАЛО/
«17» грудня 2024 р.

ОСВІТНЬО – ПРОФЕСІЙНА ПРОГРАМА
“Кібербезпека”

перший (бакалаврський) рівень
(назва рівня вищої освіти)

бакалавр
(назва ступеня, що присвоюється)

галузь знань 12 Інформаційні технології
(шифр та назва галузі знань)

спеціальність 125 Кібербезпека та захист інформації
(код та найменування спеціальності)

Розглянуто та затверджено
на засіданні Вченої ради
Університету
від «17» 12 2024 р.
протокол № 8

Львів 2024 р.

ЛИСТ ПОГОДЖЕННЯ
освітньо-професійної програми

Рівень вищої освіти	Перший (бакалаврський) рівень
Назва галузі знань	12 Інформаційні технології
Назва спеціальності	125 Кібербезпека та захист інформації
Кваліфікація	Бакалавр з кібербезпеки

РОЗРОБЛЕНО І СХВАЛЕНО

Науково-методичною комісією
спеціальності 125 Кібербезпека та
захист інформації
Протокол № 4
від «14» листопада 2024 р.

Голова НМК спеціальності
_____ Валерій ДУДИКЕВИЧ

ПОГОДЖЕНО

Проректор з науково-педагогічної
роботи Національного університету
«Львівська політехніка»

_____Олег ДАВИДЧАК
«_28_»_____11_____2024 р.

Начальник Навчально-методичного
відділу університету

_____Василь ТОМ'ЮК
«_28_»_____11_____2024 р.

РЕКОМЕНДОВАНО

Науково-методичною радою
університету
Протокол № 84
від «19» 12 2024 р.

Голова НМР університету
_____Анатолій ЗАГОРОДНІЙ

Директор ІКТА

_____ Микола МИКИЙЧУК
«_19_» листопада 2024 р.

ПЕРЕДМОВА

Розроблено відповідно до Стандарту вищої освіти України першого (бакалаврського) рівня, галузь знань 12 – Інформаційні технології, спеціальність – 125 Кібербезпека та захист інформації, затвердженого, затвердженого та введеного в дію наказом Міністерства освіти та науки України від 04.10.2018 р. №1074.

Розроблено робочою групою науково-методичної комісії спеціальності 125 «Кібербезпека та захист інформації» у складі:

Дудикевич В.Б.	– д.т.н., професор кафедри ЗІ – гарант освітньо-професійної програми
Опірський І.Р.	– д.т.н., професор, завідувач кафедри ЗІ
Журавель І.М.	– д.т.н., с.н.с., завідувач кафедри БІТ
Гарасимчук О.І.	– к.т.н., доцент кафедри ЗІ
Семенюк С.А.	– к.ф.-м.н., доцент кафедри БІТ
Микитин Г.В.	– д.т.н., професор кафедри ЗІ
Нємкова О. А.	– д.т.н., професор кафедри БІТ
Хома В.В.	– д.т.н., професор кафедри ЗІ
Журавчак Д.Ю.	– Lead Operational Technical Consultant and Lead Splunk Consultant, EPAM
Курій Є.О.	– керівник відділу Інформаційної безпеки Hiveoneer AG
Гордич М.В.	– директор ПП Defence Ukraine
Сусукайло В.А.	– старший аналітик з інформаційної безпеки TS Imagine, член ISACA та OWASP
Ясінський А.А.	– директор Alarm Security
Дзіоба Н.І.	– директор п.п. Iron Sec
Сорока С.О.	– студентка КБ–406

Гарант освітньо-професійної програми _____ (Валерій ДУДИКЕВИЧ)

Проект освітньо-професійної програми обговорений та схвалений на засіданні Вченої ради навчально-наукового інституту комп'ютерних технологій, автоматики та метрології

Протокол № _3_ від «_19_» _листопада_ 2024 р.

Голова Вченої ради ІКТА _____ Микола МИКИЙЧУК

Затверджено та надано чинності

Наказом ректора Національного університету «Львівська політехніка»

від «_19_» _грудня_ 2024 р. № _256-1-10_

1. Профіль освітньо-професійної програми "Кібербезпека" бакалавра зі спеціальності 125 «Кібербезпека та захист інформації»

1 – Загальна інформація	
Повна назва закладу вищої освіти та структурного підрозділу	Національний університет «Львівська політехніка»
Офіційна назва освітньої програми	Кібербезпека Cybersecurity
Ступінь, що присвоюється	Бакалавр
Обмеження щодо форм навчання	Денна, заочна, дистанційна
Кваліфікація в дипломі	Ступінь вищої освіти – бакалавр Спеціальність – 125 Кібербезпека та захист інформації Освітня програма – Кібербезпека
Обсяг освітньої програми	- на базі повної загальної середньої освіти – 240 кредитів ЄКТС; - на базі ступеня «молодший спеціаліст» (освітньо-кваліфікаційного рівня «молодший спеіаліст») заклад вищої освіти має право визнати та перезарахувати не більше, ніж 120 кредитів ЄКТС, отриманих в межах попередньої освітньої програми підготовки молодшого бакалавра (молодшого спеціаліста). Мінімум 75% обсягу освітньої програми має бути спрямовано на забезпечення загальних та спеціальних (фахових) компетентностей за спеціальністю визначеною стандартом вищої освіти.
Мова(и) викладання	Українська мова
2 – Мета освітньої програми	
	Підготовка фахівців, здатних використовувати і впроваджувати технології інформаційної та/або кібербезпеки та захисту інформації.
3 - Характеристика освітньої програми	
Опис предметної області	Об'єкти професійної діяльності випускників: – об'єкти інформатизації, включаючи комп'ютерні, автоматизовані, телекомунікаційні, інформаційні, інформаційно-аналітичні, інформаційно-телекомунікаційні системи, інформаційні ресурси і технології; – технології забезпечення безпеки інформації; – процеси управління інформаційною та/або кібербезпекою об'єктів, що підлягають захисту. Теоретичний зміст предметної діяльності Знання: – законодавчої, нормативно-правової бази України та вимог відповідних міжнародних стандартів і практик щодо здійснення професійної діяльності; – принципів супроводу систем та комплексів інформаційної та/або кібербезпеки; – теорії, моделей та принципів управління доступом до інформаційних ресурсів; – теорії систем управління інформаційною та/або кібербезпекою; – методів та засобів виявлення та ідентифікації ризиків; – методів та засобів оцінювання та забезпечення необхідного рівня захищеності інформації; – методів та засобів технічного та криптографічного захисту

	інформації. Методи, методики та технології: Методи, методики та технології забезпечення інформаційної та/ або кібербезпеки. Інструменти та обладнання: – системи розробки, забезпечення, моніторингу та контролю процесів інформаційної та/або кібербезпеки; – сучасне програмно-апаратне забезпечення інформаційно-комунікаційних технологій.
Академічні права випускників	Можливість продовжити навчання за освітньо-професійною або освітньо-науковою програмою ступеня магістра.
Орієнтація освітньої програми	Освітньо-професійна програма базується на загальновідомих положеннях та результатах сучасних наукових досліджень у галузі інформаційних технологій та орієнтується на актуальні спеціалізації з питань кібербезпеки та захисту інформації, попередження та протидії кіберзлочинів, у межах яких можлива подальша наукова та професійна кар'єра.
Основний фокус освітньої програми та спеціалізації	Спеціальна освіта та професійна підготовка в області кібербезпеки та захисту інформації. ***Ключові слова:*** кібербезпека, системи технічного захисту інформації, управління інформаційною безпекою, безпека інформаційно-комунікаційних систем, адміністрування систем кібербезпеки.
Особливості програми	Інтегрована підготовка фахівців до вирішення завдань у сфері кібербезпеки.
4 – Здатність випускників до працевлаштування та подальшого навчання	
Придатність до працевлаштування	Випускник може займати первинні посади відповідно до професійних стандартів: 1. Адміністратор безпеки мереж і систем, 2139.2; 2. Фахівець сфреи захисту інформації, 2139.2; 3. Фахівець з питань безпеки (інформаційно-комунікаційні технології), 2139.2; 4. Конструктор систем безпеки, 2139.2; 5. Фахівець з підтримки інфраструктури кіберзахисту, 2139.2; 6. Фахівець з реагування на інциденти кібербезпеки, 2139.2; 7. Фахівець з криптографічного захисту інформації, 2139.2; 8. Фахівець з технічного захисту інформації, 2139.2; 9. Фахівець з тестування систем захисту інфорамції, 2139.2; 10. Аудитор інформаційних технологій (з кібербезпеки) 2139.2; 11. Фахівець з оцінки заходів захисту інформації (кібербезпеки), 2139.2; та міжнародної стандартної класифікації професій (International Standard Classification of Occupations 2008 (ISCO - 08): 2529 Security specialist (ICT). Існує можливість отримати міжнародні сертифікати в галузі кібербезпеки.
Подальше навчання	Можливість продовжити навчання на другому (магістерскому) рівні вищої освіти за спеціальністю 125 «Кібербезпека та захист інформації» або іншими спорідненими (суміжними) спеціальностями галузі знань «Інформаційні технології», що узгоджуються з отриманим дипломом бакалавра. Можливість підвищення кваліфікації та отримання додаткової післядипломної освіти.

5 – Викладання та оцінювання	
Викладання та навчання	Ґрунтуються на принципах студентоцентризму та індивідуально-особистісного підходу; реалізуються через навчання на основі досліджень, посилення практичної орієнтованості та творчої спрямованості у формі комбінації лекцій, лабораторних робіт, практичних занять, самостійної навчальної і дослідницької роботи з використанням елементів дистанційного навчання, розв'язування прикладних задач, виконання курсових робіт та проектів, консультації із викладачами, підготовка бакалаврської кваліфікаційної роботи.
Оцінювання	Письмові та усні екзамени, заліки, лабораторні звіти, усні презентації, поточний контроль, захист бакалаврської кваліфікаційної роботи.
6 – Програмні компетентності	
Інтегральна компетентність (ІНТ)	Здатність розв'язувати складні спеціалізовані задачі та практичні завдання у галузі кібербезпеки та захисту інформації.
Загальні компетентності (ЗК)	**ЗК1.** Здатність застосовувати знання у практичних ситуаціях. **ЗК2**. Знання та розуміння предметної області і розуміння професії. **ЗК3.** Здатність спілкуватися державною мовою як усно, так і письмово. **ЗК4.** Здатність спілкуватися іноземною мовою. **ЗК5.** Здатність вчитися і оволодівати сучасними зананнями. **ЗК6.** Здатність реалізовувати 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. **ЗК7.** Здатність ухвалювати рішення й діяти дотримуючись принципу неприпустимості корупції та будь-яких інших проявів недоброчесності. **ЗК8.** 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)	**СК1.** Здатність застосовувати законодавчу та нормативно-правову базу, а також державні і міжнародні вимоги, практики і стандарти у професійній діяльності. **СК2.** Здатність використовувати інформаційні технології, сучасні методи і моделі кібербезпеки та системи 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 способів 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..
Фахові компетентності професійного спрямування (ФКС)	***Вибіркові компоненти блоку 0100 "Кібербезпека комп'ютерних систем та мереж"*** **ФКС1.1.** Знання основних підходів до організації типових комплексів та засобів захисту інформації в інформаційних і комунікаційних системах. **ФКС1.2.** Знання основних моделей ризиків, уразливостей, загроз та атак для обґрунтування варіантів побудови автоматизованої системи моніторингу інформаційної безпеки для інформаційних і комунікаційних систем та її основних складових. **ФКС1.3.** Знання технологій створення систем захисту комп'ютерних систем та мереж для розробки та визначення загальних принципів побудови систем захисту, завдань та вихідних даних, які необхідно враховувати при проектуванні систем захисту. **ФКС1.4.** Знання методик аналізу, синтезу, оптимізації та прогнозування якості процесів функціонування інформаційних процесів та технологій в інформаційно-комунікаційних системах. **ФКС1.5.** Знання та практичні навички використання і захисту хмарних технологій в інформаційно-комунікаційних системах. ***Вибіркові компоненти блоку 0200 "Системи технічного захисту інформації, автоматизація її обробки"*** **ФКС2.1.** Здатність проектувати, розробляти та впроваджувати програмно-апаратні системи захисту інформації, включаючи схемотехнічні рішення, апаратну криптографію та мікропроцесорні системи технічного захисту інформації **ФКС2.2.** Здатність досліджувати, аналізувати та виявляти вразливості апаратних засобів і систем безпеки з метою оцінки їх захищеності та вдосконалення механізмів захисту, включаючи системи бездротового зв'язку та кіберфізичні системи. **ФКС2.3.** Здатність проектувати та впроваджувати комплексні системи фізичної та технічної безпеки об'єктів критичної інфраструктури та об'єктів, що становлять державну таємницю, з урахуванням оцінки ризиків та застосуванням сучасних технічних засобів охорони. **ФКС2.4.** Здатність здійснювати цифрову обробку сигналів та застосовувати методи технічного захисту інформації для протидії витоку інформації технічними каналами в системах передачі та обробки даних. **ФКС2.5.** Здатність розробляти проектну документацію та впроваджувати комплексні рішення з технічного захисту інформації з урахуванням нормативних вимог та сучасних технологій.

	Вибіркові компоненти блоку 0300 "Управління інформаційною безпекою" **ФКС3.1.** Здатність проводити аудит інформаційної безпеки, здійснювати процедури ліцензування та сертифікації систем захисту інформації відповідно до нормативних вимог та міжнародних стандартів, включаючи оцінку відповідності профілям захисту. **ФКС3.2.** Здатність оцінювати ризики інформаційної безпеки, розробляти плани відновлення інформаційних систем та управляти надійністю систем кібербезпеки із застосуванням сучасних методів аналізу та прогнозування. **ФКС3.3.** Здатність проектувати та впроваджувати комплексні системи захисту об'єктів критичної інфраструктури та державної таємниці з урахуванням специфічних вимог до профілів їх кібербезпеки та особливостей інформаційно-телекомунікаційних технологій. **ФКС3.4.**Здатність використовувати методи розвідки на основі відкритих джерел та технології штучного інтелекту для виявлення, аналізу та протидії кіберзагрозам у сучасних інформаційних системах. **ФКС3.5.** Здатність забезпечувати комплексний захист інформації в бездротових мережах та системах передачі даних, включаючи проектування, впровадження та управління системами безпеки з використанням сучасних технологій комп'ютерної обробки інформації. ***Вибіркові компоненти блоку 0400 "Адміністрування систем кібербезпеки"*** **ФКС4.1.** Здатність забезпечувати комплексну безпеку веб-додатків, проводити тестування програмного забезпечення та впроваджувати механізми захисту із застосуванням сучасних методів і засобів аналізу вразливостей. **ФКС4.2.** Здатність організовувати та впроваджувати безпечну інформаційну інфраструктуру підприємства, включаючи системи захисту мережевих операційних систем та механізми моніторингу й журналізації подій безпеки. **ФКС4.3**. Здатність забезпечувати захист великих даних та управляти безпекою систем їх обробки, включаючи застосування технологій штучного інтелекту для виявлення та протидії загрозам інформаційній безпеці. **ФКС4.4.** Здатність проводити аудит інформаційної безпеки, оцінювати ризики та розробляти плани відновлення інформаційних систем з урахуванням специфіки організації та нормативних вимог. **ФКС4.5.** Здатність забезпечувати безпеку бездротових і мобільних технологій, включаючи проектування та впровадження систем захисту для різних типів безпровідних мереж та мобільних пристроїв.
7 –Результати навчання	
Результати навчання (РН)	***Загальні по 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 і передачі сигналів тощо, принципи, методи, 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. **РН10.** Використовувати сучасні інформаційні технології, методи і моделі кібербезпеки та систем захисту інформації для здійснення професійної діяльності. **РН11.** Планувати підготовку та забезпечувати неперервність бізнес процесів в організаціях згідно зі встановленою політикою кібербезпеки з урахуванням вимог до захисту інформації. **РН12.** Застосовувати методи та засоби захисту інформації в інформаційних та інформаційно-комунікаційних системах відповідно до встановленої політики інформаційної безпеки. **РН13.** 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. **РН14.** 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. **РН15.** Збирати, обробляти, зберігати, аналізувати критичні дані для доказу реалізації кіберзагроз, проводити аналіз та дослідження кіберінциденту з метою оперативного відновлення функціонування інформаційної системи. **РН16.** Вирішувати задачі впровадження та супроводу комплексних систем захисту інформації в інформаційних системах. **РН17.** 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

	кількісною та якісної оцінки ризиків. **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. **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 і контроль стану апаратних засобів захисту інформації та комплексів технічного захисту інформації. **РН21.** 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	Понад 80% науково-педагогічних працівників, задіяних до викладання професійно-орієнтованих дисциплін зі спеціальності 125 «Кібербезпека та захист інформації» мають наукові ступені та вчені звання, з практичним досвідом роботи > 15%.
Специфічні характеристики матеріально-технічного забезпечення	Використання сучасного обладнання провідних компаній у галузі інформаційних технологій та інформаційної безпеки, зокрема Xilinx, Altera, а також стандартизованих вітчизняних апаратно-програмних засобів захисту інформації, центр сертифікації ключів, виробництва «Інституту інформаційних технологій» (м.Харків).
Специфічні характеристики інформаційно-методичного забезпечення	Використання віртуального навчального середовища Національного університету «Львівська політехніка» та авторських розробок професорсько-викладацького складу.
9 – Академічна мобільність	
Національна кредитна мобільність	На основі двосторонніх договорів між Національним університетом «Львівська політехніка» та технічними університетами України.
Міжнародна кредитна мобільність	На основі двосторонніх договорів між Національним університетом «Львівська політехніка» та навчальними закладами країн-партнерів
Навчання іноземних здобувачів вищої освіти	Можливе, після вивчення курсу української мови

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

№ п/п	Цикл підготовки	Обсяг навчального навантаження здобувача вищої освіти (кредитів / %)		
		Обов'язкові компоненти освітньо-професійної програми	Вибіркові компоненти освітньо-професійної програми	Всього за весь термін навчання
1	2	3	4	5
1.	Цикл загальної підготовки	70/29,2	12/5	82/34,2
2.	Цикл професійної підготовки	110/45,8	48/20	158/65,8
Всього за весь термін навчання		180/75	60/25	240/100

3. Перелік компонент освітньо-професійної програми

Код н/д	Компоненти освітньої програми (навчальні дисципліни, курсові проекти (роботи), практики, кваліфікаційна робота)	Кількість кредитів	Форма підсумк. контролю
1	2	3	4
Обов'язкові компоненти спеціальності			
1. Цикл загальної підготовки			
СК1.1.	Вища математика ч.1	8	екзамен
СК1.2.	Іноземна мова за професійним спрямуванням ч.1	3	диф. залік
СК1.3.	Основи інформаційної та кібернетичної безпеки	3	диф. залік
СК1.4.	Технології програмування ч.1	7	екзамен
СК1.5.	Українська мова за професійним спрямуванням	3	екзамен
СК1.6.	Фізика	6	екзамен
СК1.7.	Вища математика ч.2	8	екзамен
СК1.8.	Іноземна мова за професійним спрямуванням ч.2	3	диф. залік
СК1.9.	Історія державності та культури України	3	екзамен
СК1.10.	Технології програмування ч.2	7	екзамен
СК1.11.	Нормативно-правове забезпечення та міжнародні стандарти інформаційної та кібернетичної безпеки	6	екзамен
СК1.12.	Дискретна математика	3	диф. залік
СК1.13.	Теорія інформації та кодування	4	екзамен
СК1.14.	Іноземна мова за професійним спрямуванням ч.3	3	диф. залік
СК1.15.	Філософія	3	екзамен
Всього за цикл:		**70**	
2. Цикл професійної підготовки			
СК2.1.	Командна робота	3	диф. залік
СК2.2.	Комп'ютерні мережі та їх захист	5	екзамен
СК2.3.	Програмування скриптовими мовами	4	екзамен
СК2.4.	Бази даних та знань	6	екзамен
СК2.5.	Розроблення безпечних інформаційних систем та основи хмарних технологій	6	екзамен

СК2.6.	Архітектура комп'ютера та операційні системи ч.1	5	екзамен
СК2.7.	Технології вебпрограмування	3	екзамен
СК2.8.	Схемотехніка пристроїв технічного захисту інформації ч.1	5	екзамен
СК2.9.	Методи та засоби технічного захисту інформації ч.1	3	екзамен
СК2.10.	Основи охорони праці та безпека життєдіяльності	3	екзамен
СК2.11.	Безпека програмного забезпечення	4	екзамен
СК2.12.	Криптографічні системи та протоколи	5	екзамен
СК2.13.	Безпека інфраструктури комп'ютерних мереж	6	екзамен
СК2.14.	Технології блокчейну в кібербезпеці	4	екзамен
СК2.15.	Методи стеганографії та стеганоаналізу	3	екзамен
СК2.16.	Технології розслідування інцидентів інформаційної безпеки	3	екзамен
СК2.17.	Етичний хакінг в комп'ютерних системах та мережах	6	екзамен
СК2.18.	Комплексні системи захисту інформації	3	екзамен
СК2.19.	Бази даних та знань (КР)	2	диф. залік
СК2.20.	Комп'ютерні мережі та їх захист (КП)	3	диф. залік
СК2.21.	Архітектура комп'ютера та операційні системи ч.1 (КР)	2	диф. залік
СК2.22.	Криптографічні системи та протоколи (КП)	3	диф. залік
СК2.23.	Безпека інфраструктури комп'ютерних мереж (КП)	3	диф. залік
СК2.24.	Технології розслідування інцидентів інформаційної безпеки (КР)	2	диф. залік
СК2.25.	Комплексні системи захисту інформації (КП)	3	диф. залік
СК2.26.	Практика за темою бакалаврської кваліфікаційної роботи	3	диф. залік
СК2.27.	Виконання бакалаврської кваліфікаційної роботи	9	
СК2.28.	Захист бакалаврської кваліфікаційної роботи	3	
Всього за цикл:		**110**	
Всього за спільні компоненти:		**180**	
Вибіркові компоненти освітньо-професійної програми			
Вибіркові блоки компонентів			
3. Цикл загальної підготовки			
Всього:		**6**	
4. Цикл професійної підготовки			
Вибіркові компоненти блоку 0100: Кібербезпека комп'ютерних систем та мереж			
ВБ1.1.	Основи Інтернету речей та аналітика великих даних	4	екзамен
ВБ1.2.	Архітектура комп'ютера та операційні системи, ч.2	6	екзамен
ВБ1.3.	Системи банківської безпеки	4	екзамен
ВБ1.4.	Прикладна криптографія	3	екзамен
ВБ1.5.	Ризики та інструменти захисту кібербезпеки підприємств	4	екзамен
ВБ1.6.	Інформаційно-комунікаційні системи	4	екзамен
ВБ1.7.	Збирання, аналіз та обробка даних у інформаційно-комунікаційних системах	4	екзамен
ВБ1.8.	Цифрова обробка сигналів та зображень	3	екзамен
ВБ1.9.	Аудит безпеки смарт-контрактів	5	екзамен
ВБ1.10.	Менеджмент інформаційної безпеки	4	екзамен
ВБ1.11.	Основи Інтернету речей та аналітика великих даних (КР)	2	диф. залік
ВБ1.12.	Прикладна криптографія (КР)	2	диф. залік
ВБ1.13.	Цифрова обробка сигналів та зображень (КП)	3	диф. залік
Всього за цикл		**48**	
Всього для блоку		**54**	

Вибіркові компоненти блоку 0200: Системи технічного захисту інформації, автоматизація її обробки			
ВБ2.1.	Схемотехніка пристроїв технічного захисту інформації ч.2.	5	екзамен
ВБ2.2.	Апаратний хакінг	4	екзамен
ВБ2.3.	Технології бездротового зв'язку та їх захист	4	екзамен
ВБ2.4.	Технічні засоби охорони об'єктів та управління технічними засобами інформації	4	диф. залік
ВБ2.5.	Методи та засоби захисту інформації, ч. 2	4	екзамен
ВБ2.6.	Цифрова обробка сигналів	3	диф. залік
ВБ2.7.	Проектування систем безпеки об'єктів критичної інфраструктури та державної таємниці	3	екзамен
ВБ2.8.	Мікропроцесори в системах технічного захисту інформації	4	екзамен
ВБ2.9.	Безпека кіберфізичних систем	3	екзамен
ВБ2.10.	Апаратна криптографія	3	екзамен
ВБ2.11.	Схемотехніка пристроїв технічного захисту інформації ч.2. (КП)	3	диф. залік
ВБ2.12.	Методи та засоби захисту інформації ч.2 (КР)	2	диф. залік
ВБ2.13.	Проектування систем безпеки об'єктів критичної інфраструктури та державної таємниці (КП)	3	диф. залік
ВБ2.14.	Безпека кіберфізичних систем (КП)	3	диф. залік
Всього за цикл		**48**	
Всього для блоку		**54**	
Вибіркові компоненти блоку 0300: Управління інформаційною безпекою			
ВБ3.1.	Аудит, ліцензування та сертифікація інформаційної безпеки	5	екзамен
ВБ3.2.	Основи та безпека інформаційно-телекомунікаційних технологій	5	екзамен
ВБ3.3.	Оцінювання ризиків та планування відновлення інформаційних систем	4	екзамен
ВБ3.4.	Профілі кібербезпеки об'єктів критичної інфраструктури	3	екзамен
ВБ3.5.	Комп'ютерна обробка інформації	3	диф. залік
ВБ3.6.	Технології бездротового зв'язку та їх захист	4	екзамен
ВБ3.7.	Проектування систем безпеки об'єктів критичної інфраструктури та державної таємниці	3	екзамен
ВБ3.8.	Розвідка даних на основі відкритих джерел	4	екзамен
ВБ3.9.	Системи штучного інтелекту в кібербезпеці	3	екзамен
ВБ3.10.	Управління системами кібербезпеки та їх надійність	3	диф. залік
ВБ3.11.	Аудит, ліцензування та сертифікація інформаційної безпеки (КР)	2	диф. залік
ВБ3.12.	Профілі кібербезпеки об'єктів критичної інфраструктури (КП)	3	диф. залік
ВБ3.13.	Проектування систем безпеки об'єктів критичної інфраструктури та державної таємниці (КП)	3	диф. залік
ВБ3.14.	Управління системами кібербезпеки та їх надійність (КП)	3	диф. залік
Всього за цикл		**48**	
Всього для блоку		**54**	

Вибіркові компоненти блоку 0400: Адміністрування систем кібербезпеки			
ВБ4.1.	Безпека веб-додатків	4	екзамен
ВБ4.2.	Організація інформаційних технологій на підприємстві	5	екзамен
ВБ4.3.	Оцінювання ризиків та планування відновлення інформаційних систем	4	екзамен
ВБ4.4.	Аудит інформаційної безпеки	3	екзамен
ВБ4.5.	Безпека мережевих операційних систем	4	екзамен
ВБ4.6.	Великі дані та їх захист	4	екзамен
ВБ4.7.	Тестування програмного забезпечення	3	екзамен
ВБ4.8.	Інструменти мережевої безпеки та системи журналізації подій в комп'ютерних системах	5	екзамен
ВБ4.9.	Безпека бездротових і мобільних технологій	3	екзамен
ВБ4.10.	Системи штучного інтелекту в кібербезпеці	3	екзамен
ВБ4.11.	Організація інформаційних технологій на підприємстві (КП)	3	диф. залік
ВБ4.12.	Великі дані та їх захист (КР)	2	диф. залік
ВБ4.13.	Тестування програмного забезпечення (КР)	2	диф. залік
ВБ4.14.	Безпека бездротових і мобільних технологій (КП)	3	
Всього за цикл		**48**	
Всього для блоку		**54**	
Вибіркові компоненти інших освітньо-професійних програм			
Всього		**6**	
Всього за вибіркові компоненти		**60**	
Всього зо освітньо-професійну програму		**240**	

4. Форми атестації здобувачів вищої освіти

Форми атестації здобувачів вищої освіти	Атестація здійснюється у формі єдиного державного кваліфікаційного іспиту та публічного захисту кваліфікаційної роботи. Єдиний державний кваліфікаційний іспит передбачає оцінювання досягнень результатів навчання, вичзначених стандартом зі спеціальності 125 Кібербезпека та захист інформації для першого (бакалаврського) рівня До атестації допускаються студенти, які виконали всі вимоги програми підготовки.
Вимоги до кваліфікаційної роботи/проекту	Кваліфікаційна робота має передбачати розв'язання спеціалізованої задачі в галузі інформаційної та/або кібербезпеки. Кваліфікаційна робота виконується з грифом ДСК та зберігається у філії РСО кафедри.

5. Матриця відповідності програмних компетентностей навчальним компонентам

	ІНТ	ЗК1	ЗК2	ЗК3	ЗК4	ЗК5	ЗК6	ЗК7	ЗК8	СК1	СК2	СК3	СК4	СК5	СК6	СК7	СК8	СК9	СК10
СК1.1.		•	•														•		
СК1.2.		•			•	•													
СК1.3.		•	•	•						•						•			
СК1.4.		•	•			•					•		•						•
СК1.5.		•	•	•			•		•										
СК1.6.		•							•										
СК1.7.		•	•														•		
СК1.8.		•			•	•													
СК1.9.		•	•				•	•	•										
СК1.10.		•	•			•					•		•						•
СК1.11.		•	•	•			•			•		•				•			
СК1.12.		•				•									•				
СК1.13.		•	•	•							•								
СК1.14.		•			•	•													
СК1.15.		•					•	•	•										
СК2.1.	•	•				•			•		•								•
СК2.2.	•	•	•			•					•		•	•					
СК2.3.		•	•			•					•		•						•
СК2.4.			•			•					•	•	•	•					
СК2.5.		•	•			•					•		•	•					•
СК2.6.		•	•		•	•					•		•					•	•
СК2.7.		•	•			•					•		•					•	
СК2.8.		•				•								•	•			•	
СК2.9.			•	•									•		•			•	
СК2.10.	•	•					•		•										
СК2.11.		•	•			•					•		•	•					•
СК2.12.			•								•		•				•		
СК2.13.		•	•			•							•	•		•			•
СК2.14.			•			•		•				•			•		•		
СК2.15.		•	•	•		•					•		•				•		
СК2.16.		•			•					•	•	•		•		•			•
СК2.17.		•	•			•							•	•					•
СК2.18.		•	•	•						•	•		•		•			•	
СК2.19.			•			•					•	•	•	•					
СК2.20.	•	•	•			•					•		•	•					
СК2.21.		•	•		•	•					•		•					•	
СК2.22.			•								•		•				•		
СК2.23.		•	•			•							•	•					•
СК2.24.		•			•							•	•	•		•			•
СК2.25.		•	•	•							•		•		•			•	
СК2.26.		•	•	•			•		•	•	•		•		•	•	•	•	
СК2.27.	•	•	•	•	•	•				•	•								•
СК2.28.	•			•	•			•	•										

6. Матриця відповідності фахових компетентностей професійного спрямування (ФКС) навчальним компонентам

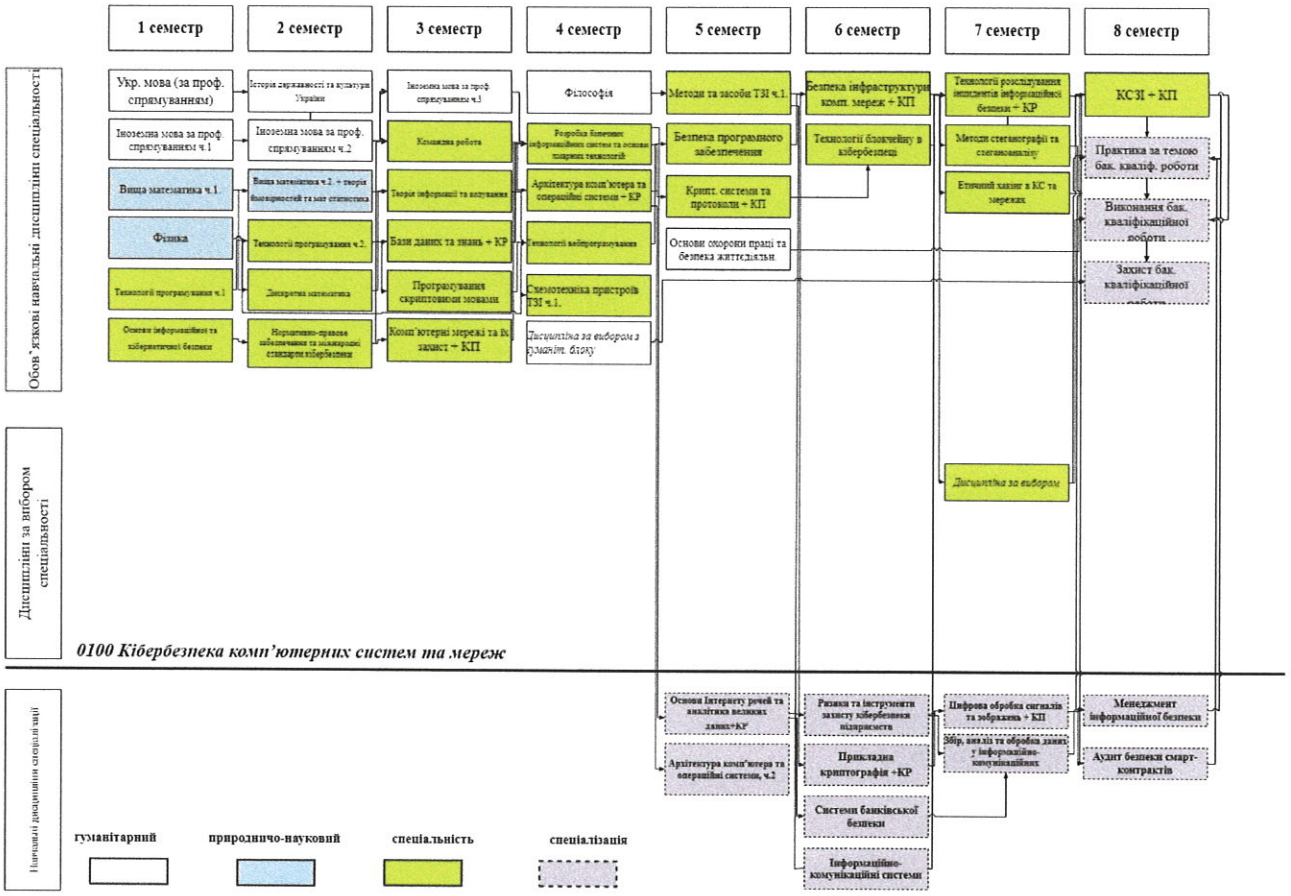
	ФКС1.1	ФКС1.2	ФКС1.3	ФКС1.4	ФКС1.5	ФКС2.1	ФКС2.2	ФКС2.3	ФКС2.4	ФКС2.5	ФКС3.1	ФКС3.2	ФКС3.3	ФКС3.4	ФКС3.5	ФКС4.1	ФКС4.2	ФКС4.3	ФКС4.4	ФКС4.5
ВБ1.1	•	•	•																	
ВБ1.2			•	•																
ВБ1.3	•			•																
ВБ1.4	•	•	•	•	•															
ВБ1.5	•	•	•																	
ВБ1.6	•	•	•		•															
ВБ1.7	•	•		•																
ВБ1.8	•		•																	
ВБ1.9	•	•		•																
ВБ1.10	•	•																		
ВБ1.11	•	•	•																	
ВБ1.12	•	•	•	•	•															
ВБ1.13	•		•																	
ВБ2.1						•	•		•											
ВБ2.2							•	•	•											
ВБ2.3							•	•		•										
ВБ2.4								•	•											
ВБ2.5						•	•	•												
ВБ2.6									•	•										
ВБ2.7								•		•										
ВБ2.8						•		•	•											
ВБ2.9							•			•										
ВБ2.10						•	•	•												
ВБ2.11						•	•		•											
ВБ2.12						•	•	•												
ВБ2.13								•		•										
ВБ2.14							•			•										
ВБ3.1											•	•								
ВБ3.2													•		•					
ВБ3.3												•								
ВБ3.4											•	•		•						
ВБ3.5											•									
ВБ3.6													•	•						
ВБ3.7													•		•					
ВБ3.8														•						
ВБ3.9														•						
ВБ3.10												•	•							
ВБ3.11											•	•								
ВБ3.12											•	•		•						
ВБ3.13													•		•					
ВБ3.14												•	•							
ВБ4.1																			•	•
ВБ4.2																•	•	•		
ВБ4.3																			•	
ВБ4.4																	•		•	
ВБ4.5																•		•		•
ВБ4.6																		•	•	
ВБ4.7																•			•	
ВБ4.8																	*	•	•	
ВБ4.9																		•		•
ВБ4.10																		•		
ВБ4.11																•	•	•		
ВБ4.12																		•	•	
ВБ4.13																•			•	
ВБ4.14																		•		•

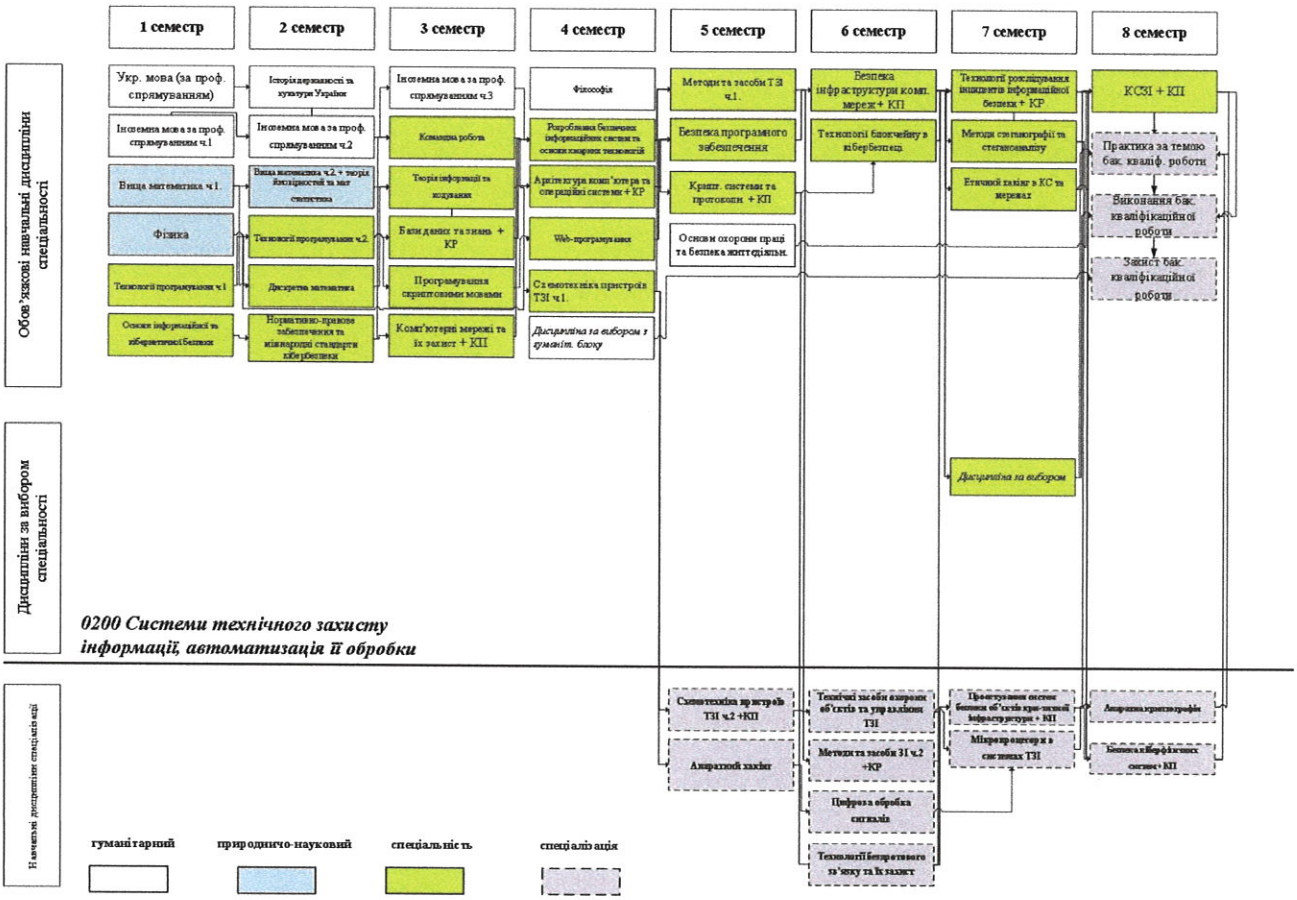
7. Матриця відповідності програмних результатів навчання навчальним компонентам

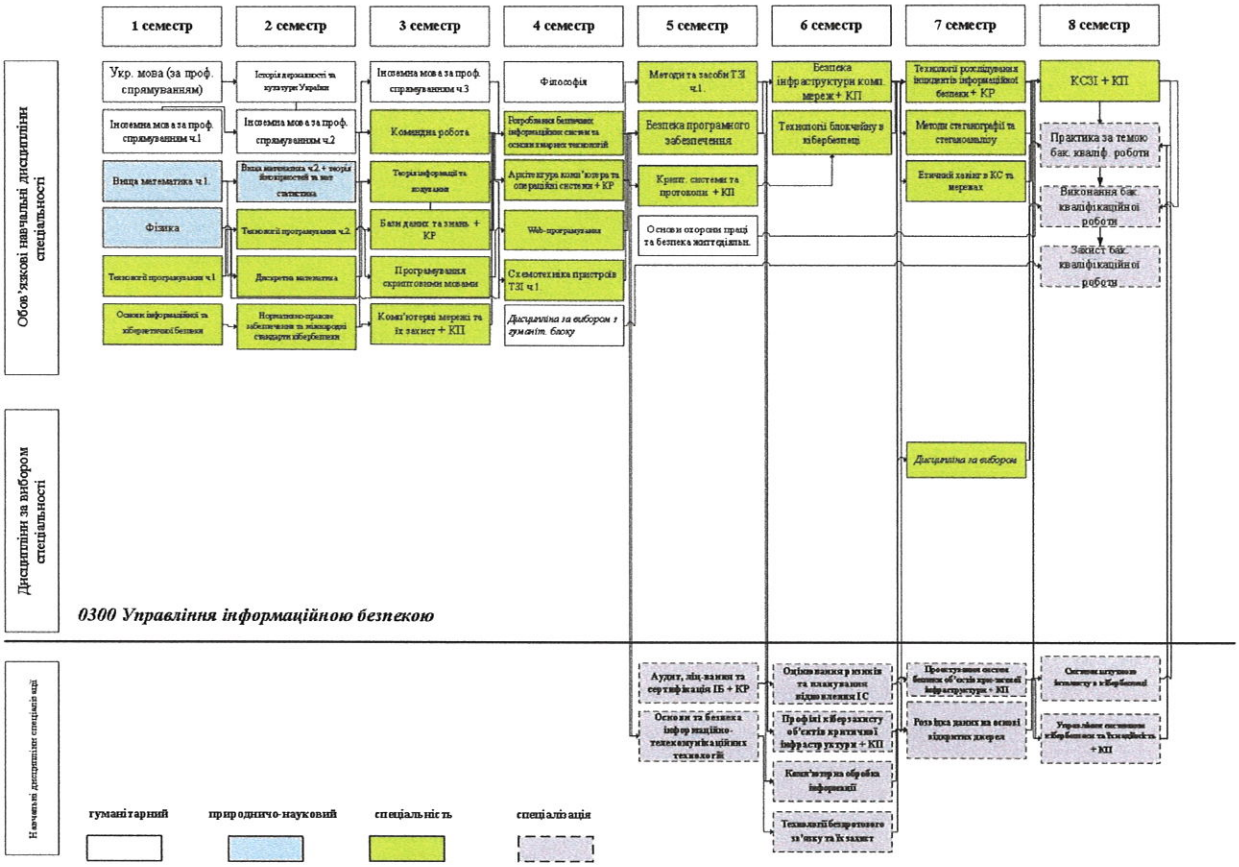
	РН1	РН2	РН3	РН4	РН5	РН6	РН7	РН8	РН9	РН10	РН11	РН12	РН13	РН14	РН15	РН16	РН17	РН18	РН19	РН20	РН21
СК1.1.				•	•		•	•										•			
СК1.2.		•		•		•			•												
СК1.3.					•			•	•	•											
СК1.4.						•				•			•								•
СК1.5.	•				•				•												
СК1.6.				•	•			•													
СК1.7.				•	•		•	•										•			
СК1.8.		•		•		•			•												
СК1.9.			•			•			•												
СК1.10						•				•			•								•
СК1.11				•					•			•					•				
СК1.12				•			•	•										•			
СК1.13	•					•	•	•		•											
СК1.14		•		•		•			•												
СК1.15			•		•	•															
СК2.1.	•			•	•	•				•											
СК2.2.				•		•				•			•								
СК2.3.						•				•			•								•
СК2.4.										•		•			•						•
СК2.5.										•	•	•	•	•	•						•
СК2.6.				•		•				•		•	•								•
СК2.7.					•	•				•		•	•								
СК2.8.						•						•	•		•	•				•	
СК2.9	•											•								•	•
СК2.10			•	•		•			•												
СК2.11				•	•	•	•	•		•		•	•	•	•						•
СК2.12							•	•										•	•		
СК2.13										•		•	•								•
СК2.14			•				•	•			•		•			•		•	•		•
СК2.15						•		•				•						•	•		
СК2.16		•	•							•	•		•	•	•	•	•				•
СК2.17					•					•			•		•						•
СК2.18	•								•	•		•				•				•	
СК2.19										•		•			•						•
СК2.20				•		•				•			•								
СК2.21					•					•		•	•								•
СК2.22							•	•										•	•		
СК2.23										•		•	•								•
СК2.24		•	•							•	•		•	•	•	•	•				•
СК2.25	•								•	•		•				•				•	
СК2.26	•		•		•	•			•	•							•				
СК2.27	•	•	•		•	•			•	•		•	•			•	•	•	•	•	
СК2.28	•	•		•	•		•														

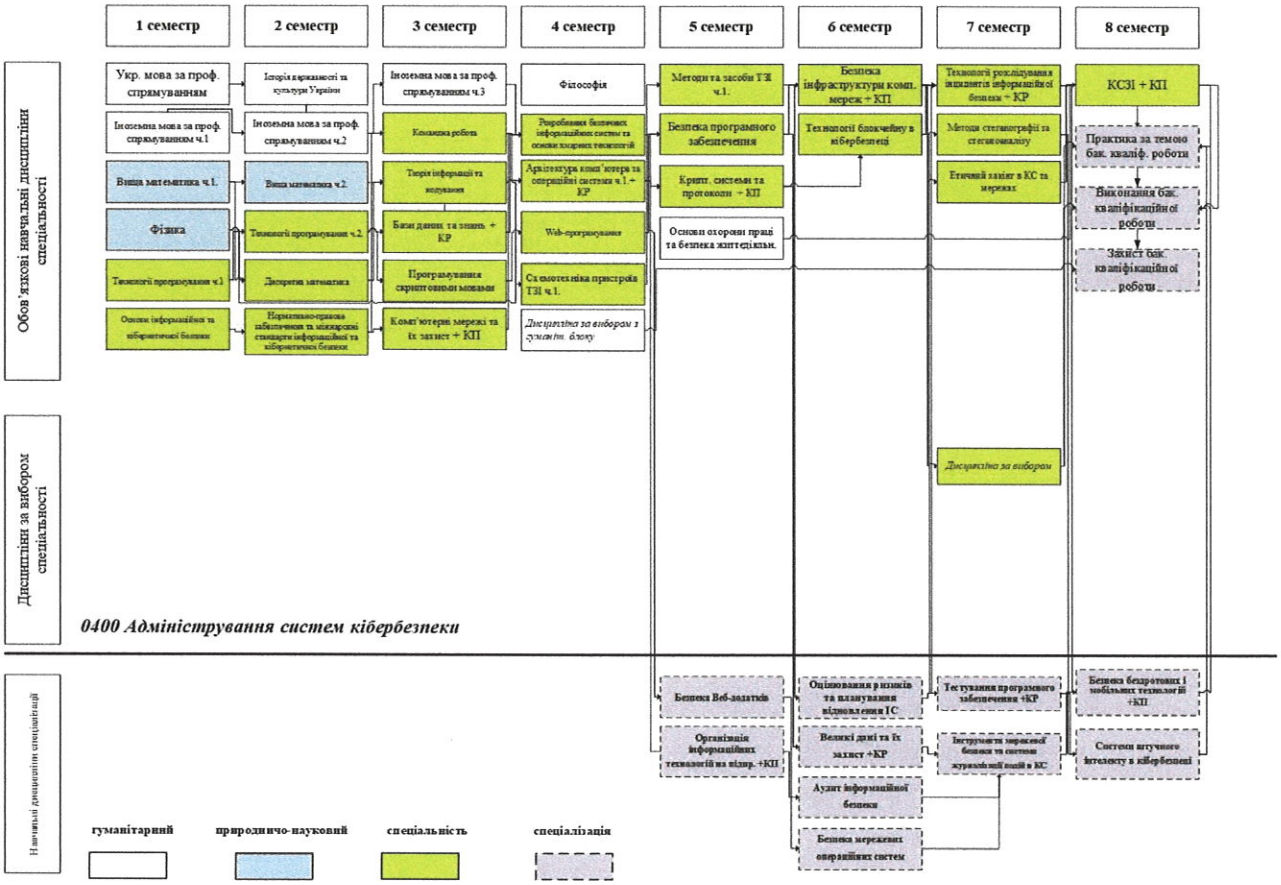
	РН1	РН2	РН3	РН4	РН5	РН6	РН7	РН8	РН9	РН10	РН11	РН12	РН13	РН14	РН15	РН16	РН17	РН18	РН19	РН20	РН21
ВБ1.1	•	•	•	•	•			•	•		•					•				•	
ВБ1.2	•	•		•		•				•		•	•	•							•
ВБ1.3				•	•	•			•	•											•
ВБ1.4	•	•		•	•	•			•	•		•	•	•		•				•	•
ВБ1.5	•			•	•	•	•	•	•	•						•					•
ВБ1.6	•			•			•				•	•	•	•		•		•			
ВБ1.7	•			•	•	•	•	•				•			•						•
ВБ1.8				•	•		•			•											
ВБ1.9	•	•	•	•	•			•	•		•										•
ВБ1.10	•	•		•	•	•			•		•						•				•
ВБ1.11	•		•	•	•				•	•		•	•			•					
ВБ1.12	•	•		•	•	•			•	•		•	•	•		•				•	•
ВБ1.13				•	•		•			•											
ВБ2.1																•				•	•
ВБ2.2				•	•		•					•								•	
ВБ2.3										•		•	•			•					
ВБ2.4										•			•			•					
ВБ2.5	•											•								•	•
ВБ2.6				•			•			•		•									
ВБ2.7				•						•		•	•			•					
ВБ2.8						•				•			•							•	•
ВБ2.9				•						•		•				•					
ВБ2.10													•				•	•	•		•
ВБ2.11																•				•	•
ВБ2.12	•											•								•	•
ВБ2.13				•						•		•	•			•					
ВБ2.14				•						•		•				•					
ВБ3.1				•		•			•		•				•		•				
ВБ3.2				•		•	•			•		•									
ВБ3.3				•				•	•		•			•			•				
ВБ3.4						•			•	•					•						
ВБ3.5				•						•					•				•		
ВБ3.6										•		•	•			•					
ВБ3.7				•						•		•	•			•					
ВБ3.8				•		•				•					•						
ВБ3.9				•	•	•	•	•		•		•	•	•	•						•
ВБ3.10									•	•	•						•				•
ВБ3.11				•		•			•		•				•		•				
ВБ3.12						•			•	•					•						
ВБ3.13				•						•		•	•			•					
ВБ3.14					•				•	•	•						•				•
ВБ4.1				•	•	•				•		•			•						
ВБ4.2					•	•				•				•		•	•				
ВБ4.3				•				•	•		•			•			•				
ВБ4.4				•		•			•		•				•		•				
ВБ4.5		•		•		•				•			•	•	•	•					
ВБ4.6										•	•				•						•
ВБ4.7														•	•					•	•
ВБ4.8				•	•	•	•	•	•	•	•	•	•		•	•	•	•		•	•
ВБ4.9										•		•	•			•					
ВБ4.10				•		•				•		•	•			•					•
ВБ4.11					•	•				•				•		•	•				
ВБ4.12					•					•	•				•						•
ВБ4.13				•											•					•	•
ВБ4.14										•		•	•			•					

Логічно-структурна схема






1 семестр
2 семестр
3 семестр
4 семестр
5 семестр
6 семестр
7 семестр
8 семестр
Обов'язкові навчальні дисципліни спеціальності
Дисципліни за вибором спеціальності
Навчальні дисципліни спеціальності
0300 Управління інформаційною безпекою
Укр. мова (за проф. спрямуванням)
Іноземна мова за проф. спрямуванням ч.1
Вища математика ч.1.
Фізика
Технології програмування ч.1
Основи інформаційної та кібернетичної безпеки
Історія державності та культури України
Іноземна мова за проф. спрямуванням ч.2
Вища математика ч.2. + теорія ймовірностей та мат статистика
Технології програмування ч.2.
Дискретна математика
Нормативно-правове забезпечення та міжнародні стандарти кібербезпеки
Іноземна мова за проф. спрямуванням ч.3
Комп'ютерна робота
Теорія інформації та кодування
Бази даних та знань + КР
Програмування скриптовими мовами
Комп'ютерні мережі та їх захист + КП
Філософія
Розробання безпекових інформаційних систем та основи хмарних технологій
Архітектура комп'ютера та операційні системи + КР
Web-програмування
Схемотехніка пристроїв ТЗІ ч.1.
Дисципліна за вибором з гуманіт. блоку
Методи та засоби ТЗІ ч.1.
Безпека програмного забезпечення
Крипт. системи та протоколи + КП
Основи охорони праці та безпека життєдіяльн.
Безпека інфраструктури комп. мереж + КП
Технології блокчейну в кібербезпеці
Технології розслідування інцидентів інформаційної безпеки + КР
Методи стеганографії та стегоаналізу
Етичний хакінг в КС та мережах
Дисципліна за вибором
КСЗІ + КП
Практика за темою бак. кваліф. роботи
Виконання бак. кваліфікаційної роботи
Захист бак. кваліфікаційної роботи
Аудит, ліцензування та сертифікація ІБ + КР
Основи та безпека інформаційно-телекомунікаційних технологій
Оцінювання ризиків та планування відновлення ІС
Профілі кіберзахисту об'єктів критичної інфраструктури + КП
Комп'ютерна обробка інформації
Технології бездротового зв'язку та їх захист
Проектування систем безпеки об'єктів критичної інфраструктури + КП
Ризик-аналіз даних на основі відкритих джерел
Системи штучного інтелекту в кібербезпеці
Управління системами кібербезпеки та безпекою + КП
гуманітарний
природничо-науковий
спеціальність
спеціалізація


1 семестр
2 семестр
3 семестр
4 семестр
5 семестр
6 семестр
7 семестр
8 семестр
Обов'язкові навчальні дисципліни спеціальності
Дисципліни за вибором спеціальності
Навчальні дисципліни спеціальності
0400 Адміністрування систем кібербезпеки
Укр. мова за проф. спрямуванням
Іноземна мова за проф. спрямуванням ч.1
Вища математика ч.1.
Фізика
Технології програмування ч.1
Основи інформаційної та кібернетичної безпеки
Історія державності та культури України
Іноземна мова за проф. спрямуванням ч.2
Вища математика ч.2.
Технології програмування ч.2.
Дискретна математика
Нормативно-правова забезпечення та міжнародні стандарти інформаційної та кібернетичної безпеки
Іноземна мова за проф. спрямуванням ч.3
Комп'ютерна робота
Теорія інформації та кодування
Бази даних та знань + КР
Програмування скриптовими мовами
Комп'ютерні мережі та їх захист + КП
Філософія
Розробання безпекових інформаційних систем та основи хмарних технологій
Архітектура комп'ютера та операційні системи ч.1. - КР
Web-програмування
Схемотехніка пристроїв ТЗІ ч.1.
Дисципліна за вибором з гуманіт. блоку
Методи та засоби ТЗІ ч.1.
Безпека програмного забезпечення
Крипт. системи та протоколи + КП
Основи охорони праці та безпека життєдіяльн.
Безпека інфраструктури комп. мереж + КП
Технології блокчейну в кібербезпеці
Технології розслідування інцидентів інформаційної безпеки + КР
Методи стеганографії та стегоаналізу
Етичний хакінг в КС та мережах
Дисципліна за вибором
КСЗІ + КП
Практика за темою бак. кваліф. роботи
Виконання бак. кваліфікаційної роботи
Захист бак. кваліфікаційної роботи
Безпека Веб-додатків
Організація інформаційних технологій на підпр. +КП
Оцінювання ризиків та планування відновлення ІС
Великі дані та їх захист +КР
Аудит інформаційної безпеки
Безпека мережевих операційних систем
Тестування програмного забезпечення +КР
Інструменти мережевої безпеки та системи журналювання подій в КС
Безпека бездротових і мобільних технологій +КП
Системи штучного інтелекту в кібербезпеці
гуманітарний
природничо-науковий
спеціальність
спеціалізація