МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ
«ЛЬВІВСЬКА ПОЛІТЕХНІКА»

«ЗАТВЕРДЖУЮ»
Ректор
Національного університету
«Львівська політехніка»
_____ /Бобало Ю.Я./
«___» 05 2018 р.

ОСВІТНЬО – ПРОФЕСІЙНА ПРОГРАМА

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
(код та найменування спеціальності)

Розглянуто та затверджено
на засіданні Вченої ради
Університету
від «30» 05 2018 р.
протокол № 44

Львів 2018 р.

ЛИСТ ПОГОДЖЕННЯ
освітньо-професійної програми

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

РОЗРОБЛЕНО І СХВАЛЕНО

Науково-методичною комісією
спеціальності 125 Кібербезпека
Протокол № 7
від «18» квітня 2018 р.

Голова НМК спеціальності
_____ В.Б. Дудикевич

ПОГОДЖЕНО

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

_____ О.Р. Давидчак
«03» 05 2018 р.

Начальник Навчально-методичного
відділу університету

_____ В.М Свірідов
«03» 05 2018 р.

РЕКОМЕНДОВАНО

Науково-методичною радою
університету
Протокол № 35
від «03» 05 2018 р.

Голова НМР університету
_____ А.Г. Загородній

Директор ІКТА

_____ М.М.Микийчук
«18» 04 2018 р.

ПЕРЕДМОВА

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

Дудикевич В.Б.	– д.т.н., проф., завідувач кафедри ЗІ
Максимович В.М.	– д.т.н., проф., завідувач кафедри БІТ
Хома В.В.	– д.т.н., професор кафедри ЗІ
Опірський І.Р.	– к.т.н., доцент кафедри ЗІ
Гарасимчук О.І.	– к.т.н., доцент кафедри ЗІ
Журавель І.М.	– к.т.н., доцент кафедри БІТ
Тимошик Н.П.	– к.т.н, директор ПП "Under Defence"
Гембаровська Я.Б.	– студентка групи УІ-41

Гарант освітньо-професійної програми _____ (Дудикевич В.Б.)

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

Протокол № 7 від « 10 » квітня 2018 р.

Голова Вченої ради ІКТА _____ М.М. Микийчук
(підпис) (прізвище, ініціали)

Затверджено та надано чинності

Наказом ректора Національного університету «Львівська політехніка»

від « 22 » 06 2018 р. № 313-1-10

1. Профіль освітньо-професійної програми “Кібербезпека” бакалавра зі спеціальності 125 «Кібербезпека»

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 Освітня програма - Кібербезпека
Обсяг освітньої програми	-на на базі повної загальної середньої освіти – 240 кредитів ЄКТС; -набазі 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.
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, 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. ***Ключові слова:*** кібербезпека, системи технічного захисту інформації, управління інформаційною безпекою, безпека інформаційно-комунікаційних систем.
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 Держаного класифікатора професій ДК 003:2010 : - фахівець з технічного захисту інформації, - фахівець із організації інформаційної безпеки, - фахівець із організації захисту інформації з обмеженим доступом, - фахівець з інформаційних технологій, - фахівець з режиму секретності, - фахівець з організації та проведення тестування на проникнення, - менеджер систем з інформаційної безпеки, - аналітик систем забезпечення кібербезпеки, - адміністратор баз даних, - адміністратор комп'ютерних систем та мереж, - аудитор з кібербезпеки, - розробник засобів захисту інформації, - проектувальник систем захисту інформації, - прикладний програміст, - провідний спеціаліст/керівник служби ТЗІ, тощо, 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» 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 роботи.
6 – Програмні компетентності	
Інтегральна компетентність (ІНТ)	Здатність розв'язувати складні спеціалізовані задачі та практичні проблеми під час професійної діяльності у галузі забезпечення інформаційної безпеки і/або кібербезпеки, що характеризується комплексністю та неповною визначеністю умов.
Загальні компетентності (ЗК)	ЗК 1. Здатність застосовувати знання у практичних ситуаціях. ЗК 2. Знання та розуміння предметної області та розуміння професії. ЗК 3. Здатність професійно спілкуватися державною та іноземною мовами як усно, так і письмово. ЗК 4. Вміння виявляти, ставити та вирішувати проблеми за професійним спрямуванням. ЗК 5. Здатність до пошуку, оброблення та аналізу інформації. ЗК 6. Здатність реалізовувати 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 зберігати та примножувати моральні, культурні, наукові цінності і досягнення суспільства на основі розуміння історії та закономірностей розвитку предметної області, її місця у загальній системі знань про природу і суспільство та у розвитку суспільства, техніки і технологій, використовувати різні види та форми рухової активності для активного відпочинку та ведення здорового способу життя.
Фахові компетентності спеціальності (ФК)	ФК 1. Здатність застосовувати законодавчу та нормативно-правову базу, а також державні та міжнародні вимоги, практики і стандарти з метою здійснення професійної діяльності в галузі інформаційної та кібербезпеки. ФК 2. Здатність до використання інформаційно-комунікаційних технологій, сучасних методів і моделей інформаційної безпеки та/або кібербезпеки. ФК 3. Здатність до використання програмних та програмно-апаратних комплексів засобів захисту інформації в інформаційно-телекомунікаційних (автоматизованих) системах. ФК 4. Здатність забезпечувати неперервність бізнесу згідно встановленої політики інформаційної та/або кібербезпеки. ФК 5. Здатність забезпечувати захист інформації, що обробляється в інформаційно-телекомунікаційних (автоматизованих) системах з метою реалізації встановленої політики інформаційної та/або кібербезпеки.

	ФК 6. Здатність відновлювати штатне функціонування інформаційних, інформаційно-телекомунікаційних (автоматизованих) систем після реалізації загроз, здійснення кібератак, збоїв та відмов різних класів та походження. ФК 7. Здатність впроваджувати та забезпечувати функціонування комплексних систем захисту інформації (комплекси нормативно-правових, організаційних та технічних засобів і методів, процедур, практичних прийомів та ін.) ФК 8. Здатність здійснювати процедури управління інцидентами, проводити розслідування, надавати їм оцінку. ФК 9. Здатність здійснювати професійну діяльність на основі впровадженої системи управління інформаційною та/або кібербезпекою. ФК 10. Здатність застосовувати методи та засоби криптографічного та технічного захисту інформації на об'єктах інформаційної діяльності. ФК 11. Здатність виконувати моніторинг процесів функціонування інформаційних. інформаційно-телекомунікаційних (автоматизованих) систем згідно встановленої політики інформаційної та/або кібербезпеки. ФК 12. Здатність аналізувати, виявляти та оцінювати можливі загрози, уразливості та дестабілізуючі чинники інформаційному простору та інформаційним ресурсам згідно з встановленою політикою інформаційної та/або кібербезпеки.
Фахові компетентності професійного спрямування (ФКС)	***Вибіркові компоненти блоку 0100 "Кібербезпека комп'ютерних систем та мереж"*** ФКС 1.1. Знання основних підходів до організації типових комплексів та засобів захисту інформації в інформаційних і комунікаційних системах. ФКС 1.2. Знання нових вітчизняних та міжнародних стандартів інформаційної безпеки. ФКС 1.3. Знання основних моделей уразливостей, загроз та атак для обґрунтування варіантів побудови автоматизованої системи моніторингу інформаційної безпеки для інформаційних і комунікаційних систем та її основних складових. ФКС 1.4. 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. ФКС 1.5. Знання методик аналізу, синтезу, оптимізації та прогнозування якості процесів функціонування інформаційних процесів та технологій в розподілених інформаційно-комунікаційних системах. ФКС 1.6. Знання та вміння ефективно оцінювати ризики проникнення в інформаційно-комунікаційні системи з врахуванням усіх потенційних загроз. ФКС 1.7. Знання сучасних підходів до ідентифікації, автентифікації, авторизації процесів та користувачів у інформаційно-комунікаційних системах. ФКС 1.8. Знання сучасних методів захисту від руйнуючих кодів в інформаційно-комунікаційних системах. ФКС 1.9. Знання та практичні навички використання і захисту хмарних технологій в інформаційно-комунікаційних системах.

	ФКС 1.10. Знання з розробки, адміністрування та захисту розподіленої бази даних, як сукупності взаємопов'язаних баз даних, розподілених у комп'ютерній мережі. ФКС 1.11. Знання основ комп'ютерних експертиз та виявлення шкідливого програмного забезпечення. ***Вибіркові компоненти блоку 0200 "Системи технічного захисту інформації, автоматизація її обробки"*** ФКС 2.1. Здатність обґрунтовувати та реалізовувати систему захисту інформаційних ресурсів з обмеженим доступом на об'єктах інформаційної діяльності. ФКС 2.2. Уміння проводити атестацію (спираючись на облік та обстеження) режимних територій (зон), приміщень тощо в умовах додержання режиму секретності із фіксуванням результатів у відповідних документах. ФКС 2.3. Уміння здійснювати оцінку відповідності системи захисту інформації автоматизованої системи своєму призначенню відповідно до вимог діючих стандартів. ФКС 2.4. Здатність до використання засобів захисту програмного забезпечення від несанкціонованого копіювання, впливу комп'ютерних вірусів тощо. ФКС 2.5. Здатність до здійснення технічного обслуговування, контролю і діагностики комплексної системи захисту інформації в організації. ФКС 2.6. Уміння будувати та використовувати комплексну систему захисту інформації в організації. ФКС 2.7. Уміння організувати моніторинг стану інформаційної системи та аналізувати порушення інформаційної безпеки. ФКС 2.8. Здатність виконувати спеціальні дослідження технічних і програмно-апаратних засобів захисту обробки інформації в інформаційно-телекомунікаційних системах. ФКС 2.9. Уміння аналізувати види і форми інформації, що попадають під дію загроз; види, методи і шляхи реалізації загроз на основі аналізу структури та змісту інформаційних процесів підприємств, установ, організацій, цілей та завдань їх діяльності. ФКС 2.10. Уміння прогнозувати стан інформаційної безпеки підприємства, установи, організації і визначати вплив ефективності задіяних заходів і засобів технічного та програмного захисту інформації. ФКС 2.11. Володіння досвідом участі у проведенні атестації об'єктів, приміщень, технічних засобів, систем, програм і алгоритмів на предмет відповідності вимогам державних або корпоративних нормативних документів щодо захисту інформації. ***Вибіркові компоненти блоку 0300 "Управління інформаційною безпекою"*** ФКС 3.1. Здатність використовувати професійно-профільовані знання й практичні навички для вирішення практичних завдань в галузі управління інформаційною безпекою. ФКС 3.2. Здатність обґрунтовувати та реалізовувати систему захисту інформаційних ресурсів з обмеженим доступом на об'єктах інформаційної діяльності. ФКС 3.3. Уміння проводити атестацію (спираючись на облік та обстеження) режимних територій (зон), приміщень тощо в умовах додержання режиму секретності із фіксуванням результатів у відповідних документах.

	ФКС 3.4. Уміння аналізувати ризики для оцінки реальних загроз порушення захисту та охорони. ФКС 3.5. Здатність здійснювати правове забезпечення інформаційної безпеки, прогнозування та моделювання в соціальній сфері. ФКС 3.6. Здатність створювати, впроваджувати, моніторити та вдосконалювати систему менеджменту інформаційної безпеки підприємства (установи). ФКС 3.7. Уміння реагувати на інциденти інформаційної безпеки; ФКС 3.8. Здатність проводити аудит підприємств (установ) за інформаційною безпекою. ФКС 3.9. Уміння збирати та аналізувати вихідні дані для проектування систем захисту інформації, визначати вимоги, здійснювати порівняльний аналіз підсистем за показниками інформаційної безпеки. ФКС 3.10. Уміння організовувати і підтримувати виконання комплексу заходів з інформаційної безпеки, управляти процесом їх реалізації з урахуванням вирішуваних завдань і організаційної структури об'єкта захисту, зовнішніх впливів, ймовірних загроз і рівня розвитку технологій захисту інформації. ФКС 3.11. Уміння формувати комплекс заходів з інформаційної безпеки з урахуванням його правової обґрунтованості, адміністративно-управлінської, технічної реалізованості та економічної доцільності. ***Вибіркові компоненти блоку 0400 "Адміністрування систем кібербезпеки"*** ФКС 4.1. Володіння медотодологіями проведення оцінки ризиків та проактивного виявленння загроз, вміння ідентифікувати вразливості інформаційної безпеки та застосовувати ефективні інструменти для їх помягшення. ФКС 4.2. Уміння написати політику кібербезпеки на об'єкті інформаційної діяльності, спираючись на міжнародні та вітчизняні стандарти, а також застосовувати кращі існуючі практики. ФКС 4.3. Уміння працювати із інцидентами інформаційної безпеки, виконувати їх оцінку, визначати пріоритети та аналізувати інциденти. ФКС 4.4. Здатність опрацьовувати та аналізувати журнали реєстрації подій, уміння розробляти синтаксичні аналізатори. ФКС 4.5. Уміння виявляти шкідливе програмне забезпечення та здатність застосовувати принципи і методи ефективної протидії. ФКС 4.6. Уміння проводити криміналістичну експертизу слідів кібератак в кібернетичному просторі. ФКС 4.7. Уміння розробляти програмне забезпечення із виявлення шкідливих програм і кібератак. ФКС 4.8. Здатність забезпечувати захист інформації, що обробляється в системах кібербезпеки, здійснювати адміністрування таких систем та їх експлуатацію. ФКС 4.9. Здатність виконувати моніторинг даних, комп'ютерних зловживань та аномалій. ФКС 4.10. Уміння аналізувати інформацію, надану інформаційними системами, з метою виявлення типових ознак можливого несанкціонованого доступу. ФКС 4.11. Уміння здійснювати адміністрування підсистем інформаційної безпеки об'єкта, а також підсистем передачі даних.

7 –Результати навчання	
Знання (ЗН)	***Загальні по спеціальності:*** ЗН 1. Застосовувати знання державної та іноземної мов з метою забезпечення ефективності професійної комунікації. ЗН 2. Організовувати власну професійну діяльність, обирати оптимальні методи та способи розв'язування складних спеціалізованих задач та практичних проблем у професійній діяльності, оцінювати їхню ефективність. ЗН 3. Використовувати результати самостійного пошуку, аналізу та синтезу інформації з різних джерел для ефективного рішення спеціалізованих задач професійної діяльності. ЗН 4. Аналізувати, аргументувати, приймати рішення при розв'язанні складних спеціалізованих задач та практичних проблем у професійній діяльності, які характеризуються комплексністю та неповною визначеністю умов, відповідати за прийняті рішення. ЗН 5. Адаптуватися в умовах частої зміни технологій професійної діяльності, прогнозувати кінцевий результат. ЗН 6. Критично осмислювати основні теорії, принципи, методи і поняття у навчанні та професійній діяльності. ЗН 7. Діяти на основі законодавчої та нормативно-правової бази України та вимог відповідних стандартів, у тому числі міжнародних в галузі інформаційної та/або кібербезпеки. ЗН 8. Готувати пропозиції до нормативних актів щодо забезпечення інформаційної та/або кібербезпеки. ЗН 9. Впроваджувати процеси, що базуються на національних та міжнародних стандартах, ідентифікації, аналізу та реагування на інциденти інформаційної та/або кібербезпеки. ЗН 10. Використовувати сучасне програмно-апаратне забезпечення для забезпечення захисту інформації та давати оцінку результативності якості прийнятих рішень. ЗН 11. Реалізовувати комплексні системи захисту інформації в автоматизованих системах (АС) організації (підприємства) відповідно до вимог нормативно-правових документів. ЗН 12. Усвідомлювати цінності громадянського (вільного демократичного) суспільства та необхідність його сталого розвитку, верховенства права, прав і свобод людини і громадянина в Україні. ЗН 13. Знання сучасних досягнень інноваційних технологій в галузі інформаційних технологій, кібербезпеки та управління; ЗН 14. Знання і розуміння наукових принципів, що лежать в основі кібербезпеки та інформаційних технологій. ЗН 15. Володіння методами загальнонаукового аналізу у сфері інформаційних технологій та інформаційної безпеки. ЗН 16. Знання правових основ дослідницьких робіт і законодавства України в галузі інформаційної безпеки. ЗН 17. Здатність використовувати уміння за експериментальними розрахунками характеристик і вибором елементів конкретної автоматизованої системи забезпечувати необхідний рівень захисту інформації в організації (на підприємстві). ЗН 18. Здатність продемонструвати знання сучасного стану справ та новітніх технологій в галузі інформаційних технологій та інформаційної безпеки. ЗН 19. Знання математичних моделей завдань забезпечення інформаційної безпеки та захисту інформації.

	ЗН 20. Знання основних підходів до організації типових комплексів та засобів захисту інформації в інформаційних і комунікаційних системах. ЗН 21. Знання нових вітчизняних та міжнародних стандартів інформаційної безпеки. ЗН 22. Знання основних моделей уразливостей, загроз та атак для обґрунтування варіантів побудови автоматизованої системи моніторингу інформаційної безпеки для інформаційних і комунікаційних систем та її основних складових. ЗН 23. 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. ЗН 24. Знання методик аналізу, синтезу, оптимізації та прогнозування якості процесів функціонування інформаційних процесів та технологій в розподілених інформаційно-комунікаційних системах. ЗН 25. Знання математичних методів оптимізації з метою одержання найкращих характеристик функціонування засобів та систем. ***Для блоку 0100 "Кібербезпека комп'ютерних систем та мереж"*** ЗН 1.1. Виконувати аналіз та декомпозицію інформаційно-телекомунікаційних систем. ЗН 1.2. Виконувати аналіз зв'язків між інформаційними процесами на віддалених обчислювальних системах. ЗН 1.3. Забезпечувати процеси захисту та функціонування інформаційно-телекомунікаційних (автоматизованих) систем на основі практик, навичок та знань, щодо структурних (структурно-логічних) схем, топології мережі, сучасних архітектур та моделей захисту електронних інформаційних ресурсів з відображенням взаємозв'язків та інформаційних потоків, процесів для внутрішніх і віддалених компонет. ЗН 1.4. Застосовувати теорії та методи захисту для забезпечення безпеки інформації в інформаційно-телекомунікаційних системах. ЗН 1.5. Забезпечувати функціонування спеціального програмного забезпечення, щодо захисту інформації від руйнуючих програмних впливів, руйнуючих кодів в інформаційно-телекомунікаційних системах. ЗН 1.6. Вирішувати задачі захисту інформації, що обробляється в інформаційно-телекомунікаційних системах з використанням сучасних методів та засобів криптографічного захисту інформації. ЗН 1.7. Використовувати впровадження та підтримку систем виявлення вторгнень та використовувати компоненти криптографічного захисту для забезпечення необхідного рівня захищеності інформації в інформаційно-телекомунікаційних системах. ЗН 1.8. Забезпечувати належне функціонування систем моніторингу інформаційних ресурсів і процесів в інформаційно-телекомунікаційних системах. ЗН 1.9. Забезпечувати функціонування програмних та програмно-апаратних комплексів виявлення вторгнень різних рівнів та класів (статистичних, сигнатурних, статистично-сигнатурних). ЗН 1.10. Підтримувати працездатність та забезпечувати

	конфігурування систем виявлення вторгнень в інформаційно-телекомунікаційних системах. ЗН 1.11. Використовувати інструментарій для моніторингу процесів в інформаційно-телекомунікаційних системах. ***Для 0200 "Системи технічного захисту інформації, автоматизація її обробки"*** ЗН 2.1. Розробляти моделі загроз та порушника. ЗН 2.2. Використовувати програмні та програмно-апаратні комплекси захисту інформаційних ресурсів. ЗН 2.3. Вирішувати задачі забезпечення та супроводу (в т.ч.: огляд, тестування, підзвітність) системи управління доступом згідно встановленої політики безпеки в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах. ЗН 2.4. Вирішувати задачі управління процедурами ідентифікації, автентифікації, авторизації процесів і користувачів в інформаційно-телекомунікаційних системах згідно встановленої політики інформаційної і/або кібербезпеки. ЗН 2.5. Реалізовувати заходи з протидії отриманню несанкціонованого доступу до інформаційних ресурсів і процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах. ЗН 2.6. Вирішувати задачі забезпечення та супроводу комплексних систем захисту інформації, а також протидіяти несанкціонованому доступу до інформаційних ресурсів і процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах згідно встановленої політики інформаційної і/або кібербезпеки. ЗН 2.7. Виявляти небезпечні сигнали технічних засобів. ЗН 2.8. Вимірювати параметри небезпечних та завадостійких сигналів під час інструментального контролю процесів захисту інформації та визначати ефективність захисту інформації від витоку технічними каналами відповідно до вимог нормативних документів системи технічного захисту інформації. ЗН 2.9. Інтерпретувати результати проведення спеціальних вимірювань з використанням технічних засобів, контролю характеристик інформаційно-телекомунікаційних систем відповідно до вимог нормативних документів системи технічного захисту інформації. ЗН 2.10. Уміння застосовувати знання технічних характеристик, конструкційних особливостей, призначення і правил експлуатації устаткування та обладнання для вирішення технічних задач спеціальності. ЗН 2.11. Володіння правовими та науково-організаційними основами проведення ліцензування, атестації та сертифікації об'єктів захисту інформації. ***Для блоку 0300 "Управління інформаційною безпекою"*** ЗН 3.1. Аналізувати проекти інформаційно-телекомунікаційних систем базуючись на стандартизованих технологіях та протоколах передачі даних. ЗН 3.2. Вирішувати задачі управління доступом до інформаційних ресурсів та процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах на основі моделей управління доступом (мандатних, дискреційних, рольових).

	ЗН 3.3. Забезпечувати ведення підзвітності і системи управління доступом до електронних інформаційних ресурсів і процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах з використанням журналів реєстрації подій, їх аналізу та встановлених процедур захисту. ЗН 3.4. Проводити атестації (спираючись на облік та обстеження) режимних територій (зон), приміщень, тощо в умовах додержання режиму секретності із фіксуванням результатів у відповідних документах. ЗН 3.5. Забезпечувати неперервність процесу ведення журналів реєстрації подій та інцидентів на основі автоматизованих процедур. ЗН 3.6. Впроваджувати процеси виявлення, ідентифікації, аналізу та реагування на інциденти інформаційної і/або кібербезпеки. ЗН 3.7. Застосовувати національні та міжнародні регулюючі акти у сфері інформаційної безпеки та/або кібербезпеки для розслідування інцидентів. ЗН 3.8. Вирішувати задачі забезпечення безперервності бізнес-процесів організації на основі теорії ризиків та встановленої системи управління інформаційною безпекою, згідно з вітчизняними та міжнародними вимогами та стандартами. ЗН 3.9. Застосовувати різні класи політик інформаційної безпеки та/або кібербезпеки, що базуються на ризик-орієнтованому контролі доступу до інформаційних активів. ЗН 3.10. Здійснювати аналіз та мінімізацію ризиків обробки інформації в інформаційно-телекомунікаційних системах. ЗН 3.11. Здатність продемонструвати знання та розуміння методологій проектування, відповідних нормативних документів, чинних стандартів і технічних умов. ***Для блоку 0400 "Адміністрування систем кібербезпеки"*** ЗН 4.1. Вирішувати завдання захисту програм та інформації, що обробляється в інформаційно-телекомунікаційних системах програмно-апаратними засобами та давати оцінку результативності якості прийнятих рішень. ЗН 4.2. Впроваджувати заходи та забезпечувати реалізацію процесів попередження отриманню несанкціонованого доступу і захисту в інформаційних та інформаційно-телекомунікаційних (автоматизованих) систем на основі еталонної моделі взаємодії відкритих систем. ЗН 4.3. Вирішувати задачі захисту потоків даних в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах ЗН 4.4. Аналізувати та проводити оцінку ефективності та рівня захищеності ресурсів різних класів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах в ході проведення випробувань згідно встановленої політики інформаційної та/або кібербезпеки. ЗН 4.5. Здійснювати оцінювання можливості реалізації потенційних загроз інформації, що обробляється в інформаційно-телекомунікаційних системах та ефективності використання комплексних засобів захисту в умовах реалізації загроз різних класів. ЗН 4.6. Здійснювати оцінювання можливості несанкціонованого доступу до елементів інформаційно-телекомунікаційних систем.

	ЗН 4.7. Застосовувати теорії та методи захисту для забезпечення безпеки елементів інформаційно-телекомунікаційних систем. ЗН 4.8. Вирішувати задачі управління процесами відновлення штатного функціонування інформаційно-телекомунікаційних систем з використанням процедур резервуванням згідно встановленої політики безпеки. ЗН 4.9. Вирішувати задачі забезпечення безперервності бізнес процесів організації на основі теорії ризиків. ЗН 4.10. Приймати участь у розробці та впровадженні стратегії інформаційної безпеки та/або кібербезпеки відповідно до цілей і завдань організації. ЗН 4.11. Вирішувати задачі аналізу програмного коду на наявність можливих загроз.
Комунікація (КОМ)	1. Уміння спілкуватись, включаючи усну та письмову комунікацію українською мовою та однією з іноземних мов (англійською, німецькою, французькою, іспанською); 2. Здатність використання різноманітних методів, зокрема інформаційних технологій, для ефективно спілкування на професійному та соціальному рівнях.
Автономія і відповідальність (АіВ)	1. Здатність адаптуватись до нових ситуацій та приймати рішення; 2. Здатність усвідомлювати необхідність навчання впродовж усього життя з метою поглиблення набутих та здобуття нових фахових знань; 3. Здатність відповідально ставитись до виконуваної роботи та досягати поставленої мети з дотриманням вимог професійної етики; 4. Здатність демонструвати розуміння основних засад охорони праці та безпеки життєдіяльності та їх застосування.
8 – Ресурсне забезпечення реалізації програми	
Специфічні характеристики кадрового забезпечення	Понад 80% науково-педагогічних працівників, задіяних до викладання професійно-орієнтованих дисциплін зі спеціальності 125 «Кібербезпека» 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	83/34,6	12/5	95/39,6
2.	Цикл професійної підготовки	97/40,4	48/20	145/60,4
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.	Історія державності та культури України	4	екзамен
СК1.4.	Робота в Інтернет	3	диф. залік
СК1.5.	Технології програмування ч.1	6	екзамен
СК1.6.	Українська мова (за професійним спрямуванням)	3	екзамен
СК1.7.	Фізика ч.1	3	екзамен
СК1.8.	Вища математика ч.2	5	екзамен
СК1.9.	Іноземна мова за професійним спрямуванням ч.2	3	екзамен
СК1.10.	Основи інформаційної безпеки	4	диф. залік
СК1.11.	Технології програмування ч.2	7	екзамен
СК1.12.	Фізика ч.2	4	екзамен
СК1.13.	Філософія	3	екзамен
СК1.14.	Вища математика ч.3 (Теорія ймовірностей та математична статистика)	3	екзамен
СК1.15.	Дискретна математика	4	екзамен
СК1.16.	Інформаційні технології	4	екзамен
СК1.17.	Метрологія та вимірювання	3	диф. залік
СК1.18.	Основи теорії кіл, сигналів та процесів	3	екзамен
СК1.19.	Схемотехніка	4	екзамен
СК1.20.	Фізика ч.3	3	диф. залік
СК1.21.	Політологія	3	екзамен
Всього за цикл:		**83**	

*2. **Цикл професійної підготовки***			
СК2.1.	Правове забезпечення інформаційної безпеки	4	диф. залік
СК2.2.	Бази даних та знань	5	екзамен
СК2.3.	Комп'ютерні мережі	5	екзамен
СК2.4.	Операційні системи	5	екзамен
СК2.5.	Криптографічні системи та протоколи, частина 1	5	екзамен
СК2.6.	Методи та засоби технічного захисту інформації, частина 1	5	екзамен
СК2.7.	Теорія інформації та кодування	5	екзамен
СК2.8.	Теорія ризиків	3	диф. залік
СК2.9.	Архітектура комп'ютерних систем	4	екзамен
СК2.10.	Безпека інфраструктури комп'ютерних мереж	5	екзамен
СК2.11.	Криптографічні системи та протоколи, частина 2	5	екзамен
СК2.12.	Безпека програмного забезпечення	5	екзамен
СК2.13.	Основи охорони праці та безпека життєдіяльності	3	диф. залік
СК2.14.	Технології розслідування інцидентів інформаційної безпеки	4	екзамен
СК2.15.	Комплексні системи захисту інформації	4	екзамен
СК2.16.	Менеджмент інформаційної безпеки	3,5	екзамен
СК2.17.	Безпека інфраструктури комп'ютерних мереж (КР)	2	диф. залік
СК2.18.	Архітектура комп'ютерних систем (КР)	2	диф. залік
СК2.19.	Комп'ютерні мережі (КП)	3	диф. залік
СК2.20.	Комплексні системи захисту інформації (КП)	3	диф. залік
СК2.21.	Практика за темою бакалаврської кваліфікаційної роботи	4,5	диф. залік
СК2.22.	Виконання бакалаврської кваліфікаційної роботи	9	
СК2.23.	Захист бакалаврської кваліфікаційної роботи	3	
Всього за цикл:		**97**	
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.	WEB-програмування	3	диф. залік
ВБ1.2.	Основи телекомунікаційних технологій	3	диф. залік
ВБ1.3.	Чисельні методи	3	екзамен
ВБ1.4.	Алгоритмічні основи криптології	3	екзамен
ВБ1.5.	Безпека інтернету речей	3	диф. залік
ВБ1.6.	Спеціалізовані методи обчислень для інформаційно-комунікаційних систем	3	диф. залік
ВБ1.7.	Інформаційно-комунікаційні системи	3	екзамен
ВБ1.8.	Системи банківської безпеки	3	диф. залік
ВБ1.9.	Технологія блокчейну	3	диф. залік
ВБ1.10.	Аналіз шкідливого програмного забезпечення	3	диф. залік
ВБ1.11.	Безпека хмарних технологій	4	екзамен
ВБ1.12.	Прикладна криптографія	4	екзамен

ВБ1.13.	Методи та засоби криптоаналізу	3	екзамен
ВБ1.14.	Чисельні методи (КП)	3	диф. залік
ВБ1.15.	Інформаційно-комунікаційні системи (КР)	2	диф. залік
ВБ1.16.	Прикладна криптографія (КР)	2	диф. залік
Всього за цикл		**48**	
Всього для блоку		**48**	
Вибіркові компоненти блоку 0200: Системи технічного захисту інформації, автоматизація її обробки			
ВБ2.1.	Поля і хвилі в системах технічного захисту інформації	3	диф. залік
ВБ2.2.	Схемотехніка пристроїв технічного захисту інформації	3	диф. залік
ВБ2.3.	Технічні засоби охорони об’єктів	3	диф. залік
ВБ2.4.	Елементи дискретних пристроїв інформаційних систем	3	екзамен
ВБ2.5.	Обчислювальні методи криптографії	3	диф. залік
ВБ2.6.	Програмування скриптовими мовами	3	диф. залік
ВБ2.7.	Цифрова обробка сигналів	3	екзамен
ВБ2.8.	Засоби приймання, передавання та обробки інформації в системах технічного захисту інформації	3	екзамен
ВБ2.9.	Методи та засоби захисту інформації, ч. 2	3	екзамен
ВБ2.10.	Системи запису та відтворення інформації	3	диф. залік
ВБ2.11.	Контрольно-вимірювальна апаратура інформаційної безпеки	3	диф. залік
ВБ2.12.	Мікропроцесори в системах технічного захисту інформації	4	екзамен
ВБ2.13.	Організаційне забезпечення технічного захисту інформації	3	диф. залік
ВБ2.14.	Системи охорони державної таємниці	3	екзамен
ВБ2.15.	Апаратна криптографія	3	екзамен
ВБ2.16.	Методи та засоби захисту інформації (КР)	2	диф. залік
Всього за цикл		**48**	
Всього для блоку		**48**	
Вибіркові компоненти блоку 0300: Управління інформаційною безпекою			
ВБ3.1.	Командна робота	3	диф. залік
ВБ3.2.	Забезпечення інформаційної та кібербезпеки держави, ч. 1	3	диф. залік
ВБ3.3.	Основи телекомунікаційних технологій	3	екзамен
ВБ3.4.	Забезпечення інформаційної та кібербезпеки держави, ч. 2	3	екзамен
ВБ3.5.	Інформаційно-аналітичне забезпечення кібербезпеки	3	диф. залік
ВБ3.6.	Міжнародні стандарти і практики у галузі інформаційної безпеки	3	диф. залік
ВБ3.7.	Соціотехнічна безпека	3	диф. залік
ВБ3.8.	Забезпечення неперервності та інформаційної безпеки бізнесу	3	диф. залік
ВБ3.9.	Комп’ютерна обробка інформації	4	диф. залік

ВБ3.10.	Прогнозування та моделювання в соціальній сфері	4	екзамен
ВБ3.11.	Аварійне планування та відновлення інформаційних систем	3	екзамен
ВБ3.12.	Аудит інформаційної безпеки	4	екзамен
ВБ3.13.	Системи охорони державної таємниці	3	диф. залік
ВБ3.14.	Стандартизація, сертифікація, ліцензування та акредитація	3	диф. залік
ВБ3.15.	Системний аналіз інформаційної безпеки	3	екзамен
Всього за цикл		**48**	
Всього для блоку		**48**	
Вибіркові компоненти блоку 0400: Адміністрування систем кібербезпеки			
ВБ4.1.	Командна робота	3	диф. залік
ВБ4.2.	Веб-програмування	3	диф. залік
ВБ4.3.	Програмування скриптовими мовами, ч.1	3	диф. залік
ВБ4.4.	Безпека веб-додатків ч.1	4	диф. залік
ВБ4.5.	Безпека мережевих операційних систем	4	диф. залік
ВБ4.6.	Програмування скриптовими мовами, ч.2	4	екзамен
ВБ4.7.	Безпека веб-додатків ч.2	4	екзамен
ВБ4.8.	Інструменти мережевої безпеки	4	екзамен
ВБ4.9.	Системи журналізації подій в комп'ютерних системах і мережах	3	диф. залік
ВБ4.10.	Аудит інформаційної безпеки	4	екзамен
ВБ4.11.	Тестування на проникнення у комп'ютеризованих системах і мережах	5	екзамен
ВБ4.12.	Тестування програмного забезпечення	4	екзамен
ВБ4.13.	Безпека мобільних технологій	3	екзамен
Всього за цикл		**48**	
Всього для блоку		**48**	
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 публічного захисту кваліфікаційної роботи. На атестацію виноситься сукупність знань, умінь, навичок, інших компетентностей, набутих особою в процесі навчання за даним стандартом. 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	ЗК 1	ЗК 2	ЗК 3.	ЗК 4	ЗК 5	ЗК 6	ЗК 7.	ФК 1	ФК 2	ФК 3.	ФК 4	ФК 5	ФК 6	ФК 7.	ФК 8.	ФК 9	ФК 10	ФК 11	ФК 12.
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.	•	•				•									•					
СК1.16.		•	•	•	•					•							•		•	•
СК1.17.		•			•	•				•									•	
СК1.18.		•				•			•	•									•	
СК1.19.		•			•					•									•	
СК1.20.		•	•		•	•														
СК1.21.		•				•	•													
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.	•			•			•	•												
	ІНТ	ЗК 1	ЗК 2	ЗК 3.	ЗК 4	ЗК 5	ЗК 6	ЗК 7.	ФК 1	ФК 2	ФК 3.	ФК 4	ФК 5	ФК 6	ФК 7.	ФК 8.	ФК 9	ФК 10	ФК 11	ФК 12.

6. Матриця відповідності фахові компетентності професійного спрямування (ФКС) навчальним компонентам

блоку 0100
«Кібербезпека комп'ютерних систем та мереж»

	ФКС 1.1	ФКС 1.2	ФКС 1.3	ФКС 1.4	ФКС 1.5	ФКС 1.6	ФКС 1.7	ФКС 1.8	ФКС 1.9	ФКС 1.10	ФКС 1.11
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.	•	•									
ВБ1.14.					•			•			
ВБ1.15.	•				•		•		•		
ВБ1.16.		•		•		•					

блоку 0200
«Системи технічного захисту інформації, автоматизація її обробки»

	ФКС 2.1	ФКС 2.2	ФКС 2.3	ФКС 2.4	ФКС 2.5	ФКС 2.6	ФКС 2.7	ФКС 2.8	ФКС 2.9	ФКС 2.10	ФКС 2.11
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	•								•	•	
ВБ2.15	•			•				•			
ВБ2.16	•	•	•			•			•	•	•

блоку 0300
«Управління інформаційною безпекою»

	ФКС 3.1	**ФКС 3.2**	**ФКС 3.3**	**ФКС 3.4**	**ФКС 3.5**	**ФКС 3.6**	**ФКС 3.7**	**ФКС 3.8**	**ФКС 3.9**	**ФКС 3.10**	**ФКС 3.11**
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					•	•	•				
ВБ3.15		•		•		•			•		

блоку 0400
«Адміністрування систем кібербезпеки»

	ФКС 4.1	**ФКС 4.2**	**ФКС 4.3**	**ФКС 4.4**	**ФКС 4.5**	**ФКС 4.6**	**ФКС 4.7**	**ФКС 4.8**	**ФКС 4.9**	**ФКС 4.10**	**ФКС 4.11**
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	•			•				•		•	

7. Матриця відповідності програмних результатів навчання /навчальним компонентам

	ЗН1	ЗН2	ЗН3	ЗН4	ЗН5	ЗН6	ЗН7	ЗН8	ЗН9	ЗН10	ЗН11	ЗН12	ЗН13	ЗН14	ЗН15	ЗН16	ЗН17	ЗН18	ЗН19	ЗН20	ЗН21	ЗН22	ЗН23	ЗН24	ЗН25	КОМ1	КОМ2	АіВ1	АіВ2	АіВ3	АіВ4
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.														•	•		•		•						•						
СК1.16.	•			•	•	•								•	•													•			
СК1.17.		•	•	•		•																		•							
СК1.18.				•		•									•																
СК1.19.						•				•			•		•										•						
СК1.20.				•		•								•														•	•	•	
СК1.21.						•						•															•				
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.	•											•						•								•	•			•	
	ЗН1	**ЗН2**	**ЗН3**	**ЗН4**	**ЗН5**	**ЗН6**	**ЗН7**	**ЗН8**	**ЗН9**	**ЗН10**	**ЗН11**	**ЗН12**	**ЗН13**	**ЗН14**	**ЗН15**	**ЗН16**	**ЗН17**	**ЗН18**	**ЗН19**	**ЗН20**	**ЗН21**	**ЗН22**	**ЗН23**	**ЗН24**	**ЗН25**	**КОМ1**	**КОМ2**	**АіВ1**	**АіВ2**	**АіВ3**	**АіВ4**

блоку 0100
«Кібербезпека комп'ютерних систем та мереж»

	ЗН1.1	**ЗН1.2**	**ЗН1.3**	**ЗН1.4**	**ЗН1.5**	**ЗН1.6**	**ЗН1.7**	**ЗН1.8**	**ЗН1.9**	**ЗН1.10**	**ЗН1.11**
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.				•			•				
ВБ1.14.	•	•		•							
ВБ1.15.	•	•	•	•							
ВБ1.16.				•		•			•		

блоку 0200
«Системи технічного захисту інформації, автоматизація її обробки»

	ЗН2.1	**ЗН2.2**	**ЗН2.3**	**ЗН2.4**	**ЗН2.5**	**ЗН2.6**	**ЗН2.7**	**ЗН2.8**	**ЗН2.9**	**ЗН2.10**	**ЗН2.11**
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					•	•					•
ВБ2.15		•			•	•					
ВБ2.16	•	•		•	•	•				•	•

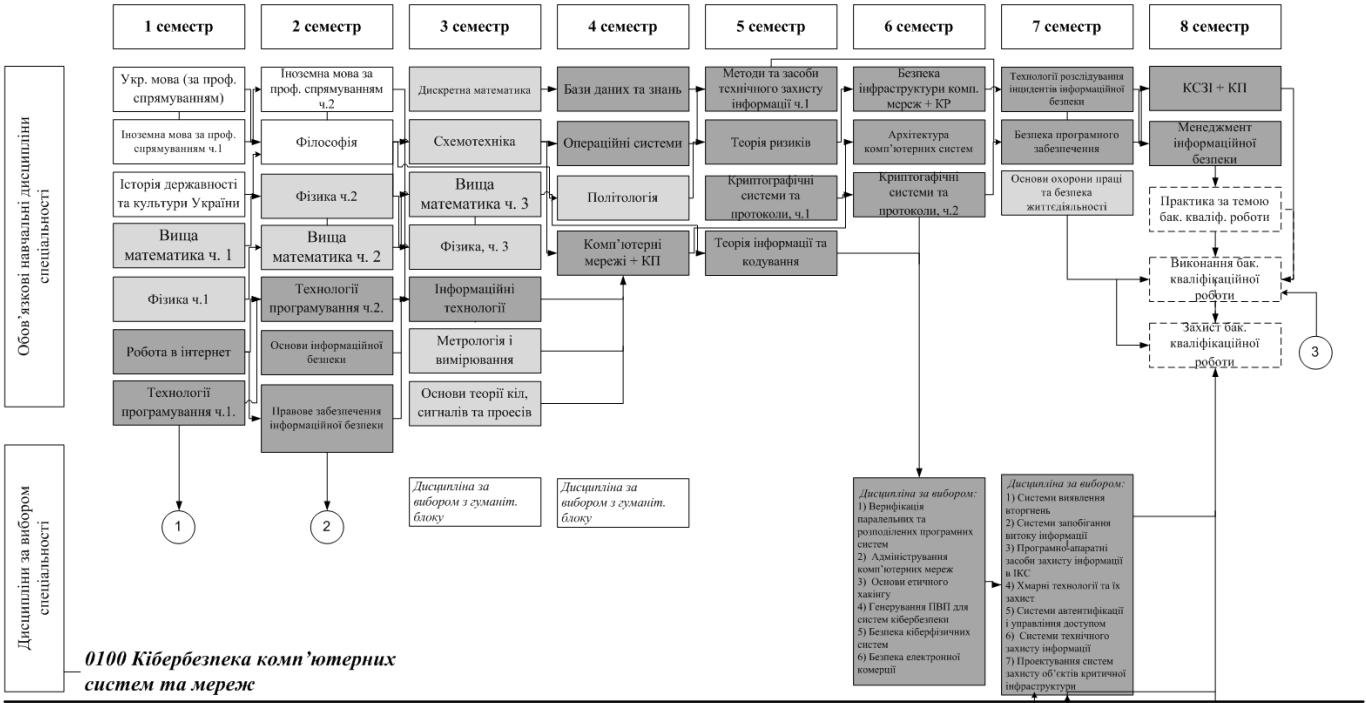
блоку 0300
«Управління інформаційною безпекою»

	ЗН3.1	**ЗН3.2**	**ЗН3.3**	**ЗН3.4**	**ЗН3.5**	**ЗН3.6**	**ЗН3.7**	**ЗН3.8**	**ЗН3.9**	**ЗН3.10**	**ЗН3.11**
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											•
ВБ3.15	•		•		•					•	

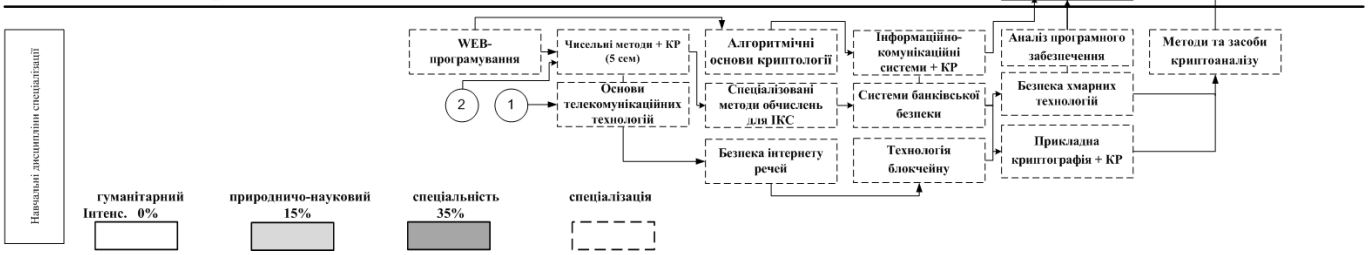
блоку 0400
«Адміністрування систем кібербезпеки»

	ЗН4.1	**ЗН4.2**	**ЗН4.3**	**ЗН4.4**	**ЗН4.5**	**ЗН4.6**	**ЗН4.7**	**ЗН4.8**	**ЗН4.9**	**ЗН4.10**	**ЗН4.11**
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				•	•	•					

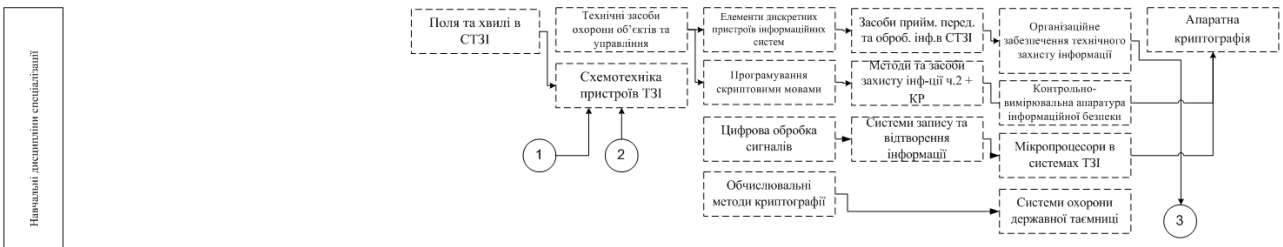
Логічно-структурна схема



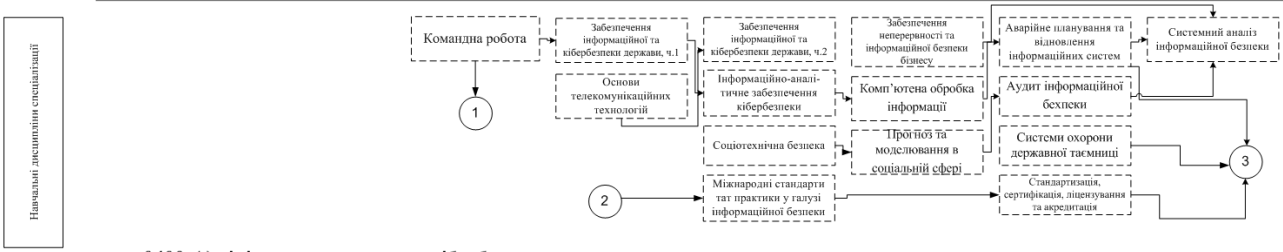
0100 Кібербезпека комп'ютерних систем та мереж



0200 Системи технічного захисту інформації, автоматизація її обробки



0300 Управління інформаційною безпекою



0400 Адміністрування систем кібербезпеки