ЦЕНТРАЛЬНОУКРАЇНСЬКИЙ НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ
МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

ОСВІТНЬО-ПРОФЕСІЙНА ПРОГРАМА «КІБЕРБЕЗПЕКА»

Першого (бакалаврського) рівня вищої освіти
за спеціальністю 125 Кібербезпека
галузі знань 12 Інформаційні технології
Кваліфікація: бакалавр з кібербезпеки

ЗАТВЕРДЖЕНО
ВЧЕНОЮ РАДОЮ ЦНТУ
протокол №_11_ від «_4_»_06_2019р.

Освітня програма вводиться в дію
з «_1_»_09__2019р.
Ректор _____/Михайло ЧЕРНОВОЛ/

Кропивницький 2019

ЛИСТ ПОГОДЖЕННЯ
ОСВІТНЬО-ПРОФЕСІЙНОЇ ПРОГРАМИ
«КІБЕРБЕЗПЕКА»

Рівень вищої освіти Перший (бакалаврський)
Галузь знань 12 Інформаційні технології
Спеціальність 125 Кібербезпека
Кваліфікація Бакалавр з кібербезпеки

РОЗРОБЛЕНО І СХВАЛЕНО
Науково-методичною комісією
спеціальності 125
«Кібербезпека»

Протокол № 2
від «15» 05 2019р.

Голова НМК спеціальності
_____О.А.Смірнов

ПОГОДЖЕНО
Перший проректор
Центральноукраїнського
національного технічного
університету
_____В.М.Кропівний
«4» 06 2019р.

РЕКОМЕНДОВАНО
Науково-методичною радою
університету
Протокол №5
від «29»05 2019р.
Голова НМР університету
_____В.М.Кропівний

Ректор
Центральноукраїнського
національного технічного
університету
_____Михайло ЧЕРНОВОЛ
«4»06 2019р.

ПЕРЕДМОВА

Розроблено робочою групою (науково-методичною комісією) спеціальності 125 Кібербезпека у складі:

1. Смірнов Сергій Анатолійович, к.т.н., старший викладач кафедри кібербезпеки та програмного забезпечення, ЦНТУ.
2. Лисенко Ірина Анатоліївна, к.т.н., старший викладач кафедри кібербезпеки та програмного забезпечення, ЦНТУ.
3. Мелешко Єлизавета Владиславівна, к.т.н., доц., доцент кафедри кібербезпеки та програмного забезпечення, ЦНТУ.
4. Смірнов Олексій Анатолійович, д.т.н., проф., професор кафедри кібербезпеки та програмного забезпечення, ЦНТУ.
5. Минайленко Роман Миколайович, к.т.н., доц.., доцент кафедри кібербезпеки та програмного забезпечення, ЦНТУ.
6. Коваленко Анна Степанівна, к.т.н., старший викладач кафедри кібербезпеки та програмного забезпечення, ЦНТУ.
7. Доренський Олександр Павлович, к.т.н., доцент кафедри кібербезпеки та програмного забезпечення, ЦНТУ.
8. Якименко Наталія Миколаївна, к.ф.-м.н., доц., доцент кафедри кібербезпеки та програмного забезпечення, ЦНТУ.

1. Профіль освітньої програми «Кібербезпека»
зі спеціальності 125 «Кібербезпека»

1. Загальна інформація	
Повна назва вищого навчального закладу та структурного підрозділу	Центральноукраїнський національний технічний університет, механіко-технологічний факультет, кафедра кібербезпеки та програмного забезпечення
Ступінь, що присвоюється	Бакалавр
Назва галузі знань	12 Інформаційні технології
Назва спеціальності	125 Кібербезпека
Обмеження щодо форм навчання	Денна, заочна, дистанційна
Освітня кваліфікація,	Бакалавр з кібербезпеки
Кваліфікація в дипломі	Ступінь вищої освіти – Бакалавр Спеціальність – 125 Кібербезпека Освітня програма – «Кібербезпека»
Офіційна назва освітньої програми	Кібербезпека
Тип диплому та обсяг освітньої програми	Диплом бакалавра, одиничний. Обсяг освітньої програми бакалавра: - на базі повної загальної середньої освіти– 240 кредитів ЄКТС - на базі ступеня «молодший бакалавр» (освітньо-кваліфікаційного рівня «молодший спеціаліст») 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.
Наявність акредитації	до 01.07.2024 р.
Цикл/рівень	Національна рамка кваліфікацій України (6 рівень) Рамка кваліфікацій Європейського простору вищої освіти QF EHEA (1st cycle) Європейська рамка кваліфікацій для навчання

	впродовж життя EQF LLL (level 6)
Передумови	Повна загальна середня освіта
Мова(и) викладання	Українська
Термін дії освітньої програми	до 01.07.2024 р.
Інтернет-адреса постійного розміщення опису освітньої програми	http://www.kntu.kr.ua/?view=univer&id=25

2. Мета освітньої програми	
Підготовка фахівців, здатних використовувати і впроваджувати технології інформаційної та/або кібербезпеки. Формування особистості фахівця, здатного вирішувати складні спеціалізовані задачі та практичні проблеми інформаційної безпеки, захищеності інформаційного і кіберпросторів держави в цілому або окремих суб'єктів їх інфраструктури від ризику стороннього кібернетичного впливу, здатних розробляти і використовувати технології інформаційної безпеки .	
3. Характеристика освітньої програми	
Предметна область	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. Цілі навчання: підготовка фахівців, здатних використовувати і впроваджувати технології інформаційної та/або кібербезпеки. Теоретичний зміст предметної області 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, управління та ідентифікації ризиків; – методів та засобів оцінювання та забезпечення необхідного рівня захищеності інформації; – методів та засобів технічного та криптографічного захисту інформації; – сучасних інформаційно-комунікаційних технологій; – сучасного програмно-апаратного забезпечення інформаційно-комунікаційних технологій; – автоматизованих систем проектування. Методи, методики та технології:

	Методи, методики, інформаційно-комунікаційні технології та інші 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.
Орієнтація освітньої програми	Освітньо-професійна програма . Ступінь освіти – бакалавр.
Фокус програми	Здобуття вищої освіти в галузі інформаційні технології, спеціальності «Кібербезпека». Акцент на здатності організовувати й підтримувати комплекс заходів щодо забезпечення інформаційної безпеки з урахуванням їхньої правової обґрунтованості, адміністративно-управлінської й технічної реалізації, економічної доцільності, можливих зовнішніх впливів, імовірних загроз і рівня розвитку технологій захисту інформації.
Особливості програми	Інтеграція програмно-апаратних засобів виявлення, моніторингу та забезпечення інформаційної безпеки, сучасних інформаційних технологій захисту інформації в інформаційно-комунікаційних системах, технологій збереження даних в кіберпросторі та інтелектуалізації функцій протидії кіберзлочинності.
4. Придатність випускників до працевлаштування та подальшого навчання	
Придатність до працевлаштування	Фахівець може працювати в підрозділах великих підприємств та установ, забезпечуючи захист комп'ютерних систем та мереж, у відділах спецслужб та правозахисних органів для захисту кіберпростору та інформаційних даних, здійснювати забезпечення захищеної комп'ютеризованої діяльності банків та фінансових установ, виконувати функції розробника систем захисту інформації Фахівець може займати первинні посади (за ДК 003:2010): 3439 (24771). Фахівець із організації інформаційної безпеки. International Standard Classification of Occupations 2008 (ISCO-08): 2529 Security specialist (ICT).
Академічні права	Можливість продовжити навчання за освітньою

випускників	програмою ступеня магістра
5. Викладання та оцінювання	
Викладання та навчання	Втілення в освітньому процесі студентоцентричного підходу; нерозривності процесів навчання і наукових досліджень; забезпечення гарантованої якості освіти відповідно до стандартів освіти; врахування світового досвіду, потреб ринку праці, залучення до цього процесу роботодавців, провідних учених, фахівців-практиків, випускників і здобувачів вищої освіти; впровадження інноваційних навчальних технологій; забезпечення здобувачам вищої освіти сприятливих умов для самостійного навчання та творчого розвитку; інтеграція освітньої та наукової діяльності; забезпечення зворотних зв'язків між учасниками освітнього процесу.
Оцінювання	*Види контролю*: поточний, тематичний, періодичний, підсумковий, самоконтроль. *Форми контролю*: усне та письмове опитування, тестовий контроль, захист лабораторних та індивідуальних робіт, підсумкова атестація – захист бакалаврської роботи

6. Програмні компетентності	
Інтегральна компетентність	Здатність розв’язувати складні спеціалізовані задачі та практичні проблеми у галузі забезпечення інформаційної безпеки і\або кібербезпеки, що характеризується комплексністю та неповною визначеністю умов.
Загальні компетентності	КЗ 1. Здатність застосовувати знання у практичних ситуаціях. КЗ 2. Знання та розуміння предметної області та розуміння професії. КЗ 3. Здатність професійно спілкуватися державною та іноземною мовами як усно, так і письмово. КЗ 4. Вміння виявляти, ставити та вирішувати проблеми за професійним спрямуванням. КЗ 5. Здатність до пошуку, оброблення та аналізу інформації. КЗ 6. Здатність реалізувати свої права і обов’язки як члена суспільства, усвідомлювати цінності громадянського (вільного демократичного) суспільства та необхідність його сталого розвитку, верховенства права, прав і свобод людини і громадянина в Україні; КЗ 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	КФ 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/або кібербезпеки. КФ 2. Здатність до використання інформаційно-комунікаційних технологій, сучасних методів і моделей інформаційної безпеки та/або кібербезпеки. КФ 3. Здатність до використання програмних та програмно-апаратних комплексів засобів захисту інформації в інформаційно-телекомунікаційних (автоматизованих) системах. КФ 4. Здатність забезпечувати неперервність

	бізнесу згідно встановленої політики інформаційної та/або кібербезпеки. КФ 5. Здатність забезпечувати захист інформації, що обробляється в інформаційно-телекомунікаційних (автоматизованих) системах з метою реалізації встановленої політики інформаційної та/або кібербезпеки. К 6. Здатність відновлювати штатне функціонування інформаційних, інформаційно-телекомунікаційних (автоматизованих) систем після реалізації загроз , здійснення кібератак, збоїв та відмов різних класів та походження. КФ 7. Здатність впроваджувати та забезпечувати функціонування комплексних систем захисту інформації (комплекси нормативно-правових, організаційних та технічних засобів і методів, процедур, практичних прийомів та ін.) КФ 8. Здатність здійснювати процедури управління інцидентами, проводити розслідування, надавати їм оцінку. КФ 9. Здатність здійснювати професійну діяльність на основі впровадженої системи управління інформаційною та/або кібербезпекою. КФ 10. Здатність застосовувати методи та засоби криптографічного та технічного захисту інформації на об'єктах інформаційної діяльності. КФ 11. Здатність виконувати моніторинг процесів функціонування інформаційних, інформаційно-телекомунікаційних (автоматизованих) систем згідно встановленої політики інформаційної та/або кібербезпеки. КФ 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.
7. Програмні результати навчання	
1.	- застосовувати знання державної та іноземних мов з метою забезпечення ефективності професійної комунікації;
2.	- організовувати власну професійну діяльність, обирати оптимальні методи та способи розв'язування складних спеціалізованих задач та практичних проблем у професійній діяльності, оцінювати їхню ефективність;
3.	- використовувати результати самостійного пошуку, аналізу та синтезу інформації з різних джерел для ефективного рішення спеціалізованих задач професійної діяльності;

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;
5.	- адаптуватися в умовах частої зміни технологій професійної діяльності, прогнозувати кінцевий результат;
6.	- критично осмислювати основні теорії, принципи, методи і поняття у навчанні та професійній діяльності;
7.	- діяти на основі законодавчої та нормативно-правової бази України та вимог відповідних стандартів, у тому числі міжнародних в галузі інформаційної та /або кібербезпеки;
8.	- готувати пропозиції до нормативних актів щодо забезпечення інформаційної та /або кібербезпеки;
9.	- впроваджувати процеси, що базуються на національних та міжнародних стандартах, виявлення, ідентифікації, аналізу та реагування на інциденти інформаційної та/або кібербезпеки;
10.	- виконувати аналіз та декомпозицію інформаційно-телекомунікаційних систем;
11.	- виконувати аналіз зв’язків між інформаційними процесами на віддалених обчислювальних системах;
12.	- розробляти моделі загроз та порушника;
13.	- аналізувати проекти інформаційно-телекомунікаційних систем базуючись на стандартизованих технологіях та протоколах передачі даних;
14.	- вирішувати завдання захисту програм та інформації, що обробляється в інформаційно-телекомунікаційних системах програмно-апаратними засобами та давати оцінку результативності якості прийнятих рішень;
15.	- використовувати сучасне програмно-апаратне забезпечення інформаційно-комунікаційних технологій;
16.	- реалізовувати комплексні системи захисту інформації в автоматизованих системах (АС) організації (підприємства) відповідно до вимог нормативно-правових документів;
17.	- 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 компонент;
18.	- використовувати програмні та програмно-апаратні комплекси захисту інформаційних ресурсів;
19.	- застосовувати теорії та методи захисту для забезпечення безпеки інформації в інформаційно-телекомунікаційних системах;
20.	- забезпечувати функціонування спеціального програмного

	забезпечення, щодо захисту інформації від руйнуючих програмних впливів, руйнуючих кодів в інформаційно-телекомунікаційних системах;
21.	- вирішувати задачі забезпечення та супроводу (в.т. числі: огляд, тестування, підзвітність) системи управління доступом згідно встановленої політики безпеки в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах;
22.	- вирішувати задачі управління процедурами ідентифікації, автентифікації, авторизації процесів і користувачів в інформаційно-телекомунікаційних системах згідно встановленої політики інформаційної і\або кібербезпеки;
23.	- реалізовувати заходи з протидії отриманню несанкціонованого доступу до інформаційних ресурсів і процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах;
24.	- вирішувати задачі управління доступом до інформаційних ресурсів та процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах на основі моделей управління доступом (мандатних, дискреційних, рольових);
25.	- забезпечувати введення підзвітності 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;
26.	- впроваджувати заходи та забезпечувати реалізацію процесів попередження отриманню несанкціонованого доступу і захисту інформаційних, інформаційно-телекомунікаційних (автоматизованих) систем на основі еталонної моделі взаємодії відкритих систем;
27.	- вирішувати задачі захисту потоків даних в інформаційних, інформаційно-телекомунікаційних (автоматизованих) системах;
28.	- 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;
29.	- здійснювати оцінювання можливості реалізації потенційних загроз інформації, що обробляється в інформаційно-телекомунікаційних системах та ефективності використання комплексів засобів захисту в умовах реалізації загроз різних класів;
30.	- здійснювати оцінювання можливості несанкціонованого доступу до елементів інформаційно-телекомунікаційних систем;
31.	- застосовувати теорії та методи захисту для забезпечення безпеки елементів інформаційно-телекомунікаційних систем;
32.	- вирішувати задачі управління процесами відновлення штатного функціонування інформаційно-телекомунікаційних систем з використанням процедур резервування згідно встановленої політики безпеки;

33.	- вирішувати задачі забезпечення безперервності бізнес процесів організації на основі теорії ризиків;
34.	- приймати участь у розробці та впровадженні стратегії інформаційної безпеки та/або кібербезпеки відповідно до цілей і завдань організації;
35.	- вирішувати задачі забезпечення та супроводу комплексних систем захисту інформації, а також протидії несанкціонованому доступу до інформаційних ресурсів і процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах згідно встановленої політики інформаційної і\або кібербезпеки;
36.	- виявляти небезпечні сигнали технічних засобів;
37.	- вимірювати параметри небезпечних та завадових 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;
38.	- інтерпретувати результати проведення спеціальних вимірювань з використанням технічних засобів, контролю характеристик інформаційно-телекомунікаційних систем відповідно до вимог нормативних документів системи технічного захисту інформації;
39.	- проводити атестацію (спираючись на облік та обстеження) режимних територій (зон), приміщень тощо в умовах додержання режиму секретності із фіксуванням результатів у відповідних документах;
40.	- інтерпретувати результати проведення спеціальних вимірювань з використанням технічних засобів, контролю характеристик ІТС відповідно до вимог нормативних документів системи технічного захисту інформації;
41.	- забезпечувати неперервність процесу ведення журналів реєстрації подій та інцидентів на основі автоматизованих процедур;
42.	- впроваджувати процеси виявлення, ідентифікації, аналізу та реагування на інциденти інформаційної і/або кібербезпеки;
43.	- застосовувати національні та міжнародні регулюючі акти в сфері інформаційної безпеки та/ або кібербезпеки для розслідування інцидентів;
44.	- 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;
45.	- застосовувати ріні класи політик інформаційної безпеки та/ або кібербезпеки, що базуються на ризик-орієнтованому контролі доступу до інформаційних активів;
46.	- здійснювати аналіз та мінімізацію ризиків обробки інформації в інформаційно-телекомунікаційних системах;
47.	- вирішувати задачі захисту інформації, що обробляється в інформаційно-телекомунікаційних системах з використанням сучасних методів та засобів криптографічного захисту інформації;
48.	- виконувати впровадження та підтримку систем виявлення вторгнень

	та використовувати компоненти криптографічного захисту для забезпечення необхідного рівня захищеності інформації в інформаційно-телекомунікаційних системах;
49.	- забезпечувати належне функціонування системи моніторингу інформаційних ресурсів і процесів в інформаційно-телекомунікаційних системах;
50.	- забезпечувати) функціонування програмних та програмно-апаратних комплексів виявлення вторгнень різних рівнів та класів (статистичних, сигнатурних, статистично-сигнатурних);
51.	- підтримувати працездатність та забезпечувати конфігурування систем виявлення вторгнень в інформаційно-телекомунікаційних системах;
52.	- використовувати інструментарій для моніторингу процесів в інформаційно-телекомунікаційних системах;
53.	- вирішувати задачі аналізу програмного коду на наявність можливих загроз.
54.	- усвідомлювати цінності громадянського (вільного демократичного) суспільства та необхідність його сталого розвитку, верховенства права, прав і свобод людини і громадянина в Україні.

8. Ресурсне забезпечення реалізації програми	
Кадрове забезпечення	Лекції проводяться науково-педагогічними працівниками, а також провідними науковцями або спеціалістами практиками (включаючи фахівців іноземних країн), запрошеними для читання лекцій.
Матеріально-технічне забезпечення	Забезпечення комп'ютерною технікою та технологіями сучасного рівня
Інформаційне та навчально-методичне забезпечення	Доступ до найсучасніших інформаційних технологій та ресурсів
9. Академічна мобільність	
Навчання іноземних здобувачів вищої освіти	Мовою викладання в ЦНТУ є державна мова. З метою створення умов для міжнародної академічної мобільності, ЦНТУ має право приймати рішення про викладання однієї чи кількох дисциплін англійською мовою чи іншою офіційною мовою Європейського Союзу, забезпечивши при цьому знання здобувачами вищої освіти з відповідної дисципліни державною мовою. Перелік іноземних мов, якими здійснюється викладання навчальних дисциплін, визначається ЦНТУ. Для викладання навчальних дисциплін іноземною мовою ЦНТУ може утворювати окремі групи для іноземних громадян, осіб без громадянства, які бажають здобувати вищу освіту, за кошти фізичних чи юридичних осіб, або розробляти індивідуальні

	програми. При цьому ЦНТУ забезпечує вивчення такими особами державної мови як окремої навчальної дисципліни.

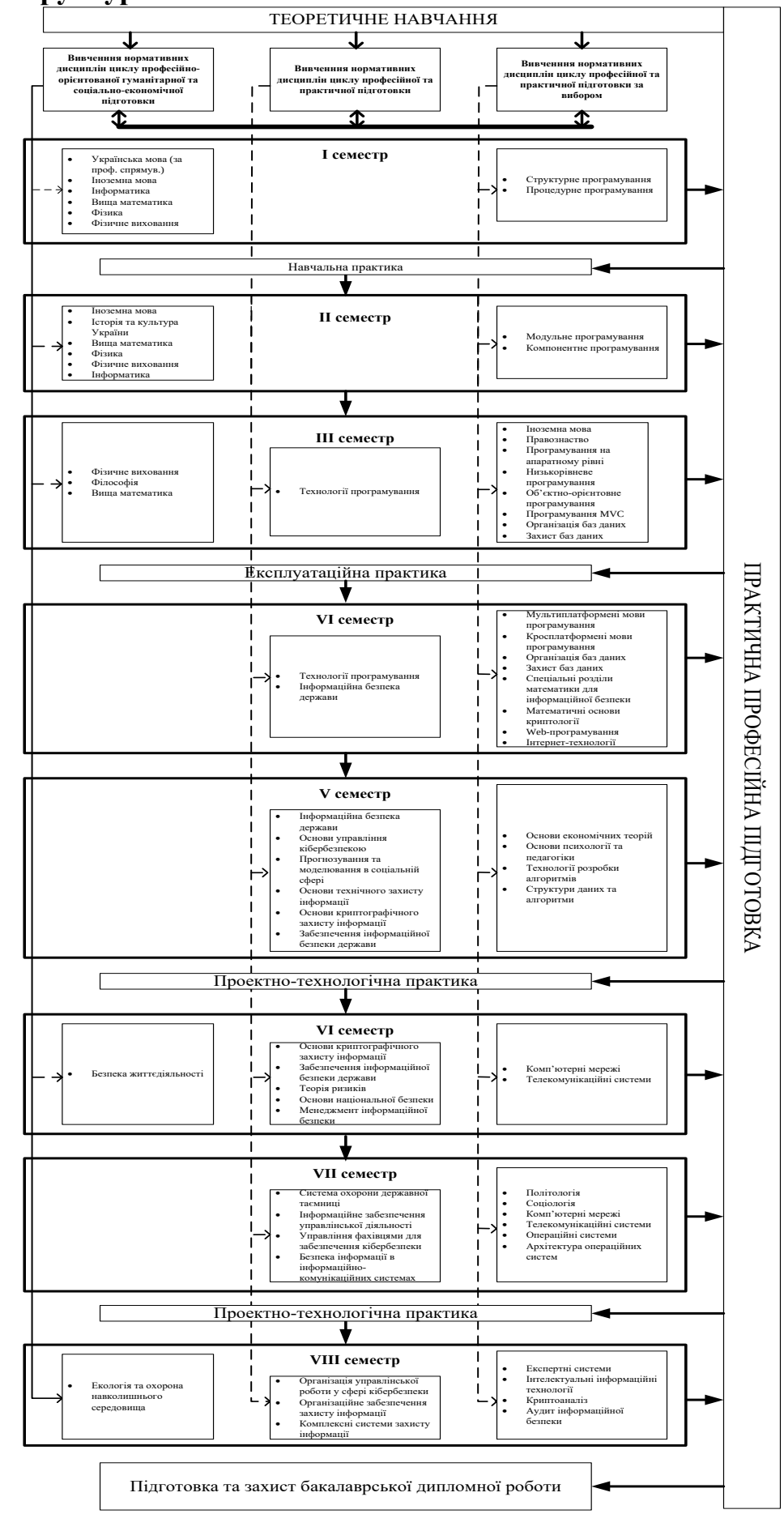
2. Перелік компонент освітньо-професійної програми та їх логічна послідовність

	Компоненти освітньої програми	Кільк. кред.	Форма підсумк. контр.
	Обов'язкові компоненти		
1.	Українська мова (за проф. спрямув.)	3	екзамен
2.	Іноземна мова	5	залік, екзамен
3.	Історія та культура України	5	екзамен
4.	Фізика	9	залік, екзамен
5.	Інформатика	9	екзамен
6.	Фізичне виховання	6	залік
7.	Вища математика	16	екзамен
8.	Філософія	4	екзамен
9.	Безпека життєдіяльності	2	залік
10.	Екологія та охорона навколишнього середовища	3	залік
11.	Технології програмування	8	екзамен
12.	Інформаційна безпека держави	8	залік, екзамен
13.	Основи управління кібербезпекою	4	екзамен
14.	Прогнозування та моделювання в соціальній сфері	5	екзамен
15.	Основи технічного захисту інформації	4	екзамен
16.	Основи криптографічного захисту інформації	7	залік, екзамен
17.	Забезпечення інформаційної безпеки держави	7	залік, екзамен
18.	Теорія ризиків	3	екзамен
19.	Основи національної безпеки	4	екзамен
20.	Система охорони державної таємниці	3	залік
21.	Інформаційне забезпечення управлінської діяльності	4	екзамен

22.	Менеджмент інформаційної безпеки	5	екзамен
23.	Управління фахівцями для забезпечення кібербезпеки	4	екзамен
24.	Безпека інформації в інформаційно-комунікаційних системах	4	екзамен
25.	Організація управлінської роботи у сфері кібербезпеки	3	екзамен
26.	Організаційне забезпечення захисту інформації	3	екзамен
27.	Комплексні системи захисту інформації	4	екзамен
28.	Навчальна практика	6	диф.залік
29.	Експлуатаційна практика	6	диф.залік
30.	Проектно-технологічна практика	6	диф.залік
31.	Переддипломна практика	6	диф.залік
32.	Дипломне проектування	9	
	Загальний обсяг обов'язкових компонент	169	
	Вибіркові компоненти		
1.	Іноземна мова	3	залік
2.	Правознавство	3	залік
3.	Основи економічних теорій	3	залік
4.	Основи психології та педагогіки	3	залік
5.	Політологія	3	залік
6.	Соціологія	3	залік
7.	Структурне програмування	5	екзамен
8.	Процедурне програмування	5	екзамен
9.	Модульне програмування	6	екзамен
10.	Компонентне програмування	6	екзамен
11.	Програмування на апаратному рівні	4	екзамен
12.	Низькорівневе програмування	4	екзамен
13.	Об'єктно-орієнтоване програмування	5	екзамен
14.	Програмування MVC	5	екзамен
15.	Організація баз даних	6	залік, екзамен

16.	Захист баз даних	6	залік, екзамен
17.	Мультиплатформені мови програмування	4	екзамен
18.	Кросплатформені мови програмування	4	екзамен
19.	Спеціальні розділи математики для інформаційної безпеки	7	екзамен
20.	Математичні основи криптології	7	екзамен
21.	Web-програмування	5	екзамен
22.	Інтернет-технології	5	екзамен
23.	Технології розробки алгоритмів	4	екзамен
24.	Структури даних та алгоритми	4	екзамен
25.	Комп'ютерні мережі	7	залік, екзамен
26.	Телекомунікаційні системи	7	залік, екзамен
27.	Операційні системи	3	екзамен
28.	Архітектура операційних систем	3	екзамен
29.	Експертні системи	3	екзамен
30.	Інтелектуальні інформаційні технології	3	екзамен
31.	Криптоаналіз	3	екзамен
32.	Аудит інформаційної безпеки	3	екзамен
	Загальний обсяг вибіркових компонент	**71**	
	Загальний обсяг освітньої програми	**240**	

Структурно-логічна схема ОП



3. Форми атестації здобувачів вищої освіти

Форми атестації здобувачів вищої освіти	Атестація здійснюється у формі публічного захисту кваліфікаційної бакалаврської дипломної роботи. На атестацію виноситься сукупність знань, умінь, навичок, інших компетентностей, набутих особою у процесі навчання за даним стандартом. До атестації допускаються студенти, які виконали всі вимоги програми підготовки.
Вимоги до кваліфікаційної роботи	Кваліфікаційна робота має передбачати розв'язання спеціалізованої задачі в галузі інформаційної та/або кібербезпеки. Кваліфікаційна робота має бути перевірена на плагіат. Оприлюднення на сайті кафедри.

4. Матриця відповідності програмних компетентностей компонентам освітньої програми «Кібербезпека»

		Загальні компетентності							Фахові компетентності											
	Освітні компоненти	**КЗ1**	**КЗ2**	**КЗ3**	**КЗ4**	**КЗ5**	**КЗ6**	**КЗ7**	**КФ1**	**КФ2**	**КФ3**	**КФ4**	**КФ5**	**КФ6**	**КФ7**	**КФ8**	**КФ9**	**КФ10**	**КФ11**	**КФ12**
1-й курс	1. Українська мова			+			+	+												
	2. Вища математика	+				+														
	3. Фізика	+				+														
	4. Іноземна мова	+		+			+													
	5. Фізичне виховання						+	+												
	6. Історія та культура України						+	+												
	7. Структурне програмування	+																		
	8. Інформатика	+	+							+			+							
	9. Модульне програмування	+																		
	10. Навчальна практика	+	+																	
2-й курс	11. Філософія		+					+												
	12. Об’єктно орієнтоване програмування									+	+									
	13. Програмування на апаратному рівні								+											
	14. Технології програмування	+	+			+				+										
	15. КР Технології програмування	+	+			+				+										
	16. Організація баз даних										+		+							
	17. КР Організація баз даних										+	+	+							
	18. Спец. розділи математики для інформаційної безпеки		+							+								+		
	19. Web-програмування -												+							

	20. Кросплатформені мови програмування										+										
	21. Інформаційна безпека держави		+						+	+	+								+		
	22. Експлуатаційна практика					+				+	+										
3-й курс	23. Основи економічних теорій				+																
	24. Безпека життєдіяльності	+						+													
	25. Технології розробки алгоритмів																		+		
	26. Основи управління кібербезпекою	+							+									+		+	+
	27. Прогнозування та моделювання в соціальній сфері									+						+					+
	28. Основи технічного захисту інформації	+	+											+	+				+		+
	29. Забезпечення інформаційної безпеки держави								+												
	30. КР Забезпечення інформаційної безпеки держави								+												
	31. Основи криптографічного захисту інформації	+							+										+		
	32. КП Основи криптографічного захисту інформації	+							+										+		
	33. Теорія ризиків	+																		+	+
	34. Менеджмент інформаційної безпеки	+			+										+	+	+			+	
	35. Основи національної безпеки								+												
	36. Криптоаналіз					+															+
	37. Проектно-технологічна практика					+				+	+							+			
4-й курс	38. Політологія					+	+														
	39. Основи охорони праці	+			+		+														

40. Екологія та охорона навколишнього середовища	+	+				+	+														
41. Безпека інформації в інформаційно-комунікаційних системах									+										+		
42. Інформаційне забезпечення управлінської діяльності	+										+					+					
43. Компютерні мережі									+			+	+								
44. Компютерні мережі									+												
45. Операційні системи										+			+								
46. Управління фахівцями для забезпечення кібербезпеки	+			+							+							+			
47. Система охорони державної таємниці						+		+							+	+					
48. Комплексні системи захисту інформації								+							+						
49. Організаційне забезпечення захисту інформації															+			+			
50. Організація управлінської роботи у сфері кібербезпеки											+							+			
51. Переддипломна практика					+				+	+					+			+			
52. Дипломне проектування	+			+				+													

Зведена таблиця фахових компетентностей та результатів навчання.

Фахові компетентності	Результати навчання
КФ 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/або кібербезпеки.	- готувати пропозиції до нормативних актів і документів з метою забезпечення встановленої політики інформаційної безпеки і \або кібербезпеки; - розробляти проектну документацію, щодо програмних та програмно-апаратних комплексів захисту інформаційних, інформаційно-телекомунікаційних (автоматизованих) систем; - виконувати аналіз реалізації прийнятої політики інформаційної і /або кібербезпеки.
КФ 2. Здатність до використання інформаційно-комунікаційних технологій, сучасних методів і моделей інформаційної та/або кібербезпеки.	- здійснювати професійну діяльність на основі знань сучасних інформаційно-комунікаційних технологій; -розробляти та аналізувати проекти інформаційно-телекомунікаційних систем базуючись на стандартизованих технологіях та протоколах передачі даних; -застосовувати в професійній діяльності знання, навички та практики, щодо структур сучасних обчислювальних систем, методів і засобів обробки інформації, архітектур операційних систем; -здійснювати захист ресурсів і процесів в інформаційно-телекомунікаційних системах на основі моделей безпеки (кінцевих автоматів, управління потоками, *Bell-LaPadula, Biba, Clark-Wilson*, та інші), а також встановлених режимів безпечного функціонування інформаційно-телекомунікаційних системах; - виконувати аналіз програмного забезпечення з метою оцінки на відповідність встановленим вимогам інформаційної і\або кібербезпеки в інформаційно-телекомунікаційних системах.
КФ 3. Здатність до використання програмних та програмно-апаратних комплексів засобів захисту інформації в інформаційно-телекомунікаційних (автоматизованих) системах	-забезпечувати процеси захисту інформаційно-телекомунікаційних (автоматизованих) систем шляхом встановлення та коректної експлуатації програмних та програмно-апаратних комплексів засобів захисту; - забезпечувати функціонування спеціального програмного забезпечення, щодо захисту даних від руйнуючих програмних впливів, руйнуючих кодів в інформаційних, інформаційно-телекомунікаційних (автоматизованих) системах; - виконувати розробку експлуатаційної документації на комплексів засобів захисту.
КФ 4. Здатність забезпечувати неперервність бізнесу згідно встановленої політики інформаційної та/або кібербезпеки.	- вирішувати задачі супроводу (в.т. числі: огляд, тестування, підзвітність) системи управління доступом згідно принципів, критеріїв доступу та встановленої політики безпеки в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах; - реалізовувати заходи з протидії отриманню несанкціонованого доступу до інформаційних ресурсів і процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах; - вирішувати задачі управління доступом до інформаційних

	ресурсів та процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах на основі моделей управління доступом (мандатних, дискреційних, рольових); - вирішувати задачі централізованого і децентралізованого адміністрування доступом до інформаційних ресурсів і процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах; - забезпечувати введення підзвітності системи управління доступом інформаційних ресурсів і процесів в інформаційно-телекомунікаційних системах.
КФ 5 Здатність забезпечувати захист інформації, що обробляється в інформаційно-телекомунікаційних (автоматизованих) системах з метою реалізації встановленої політики інформаційної та/або кібербезпеки.	- обирати основні методи та засоби захисту інформації відповідно до вимог сучасних стандартів інформаційної та/або кібербезпеки, та критеріїв безпеки інформаційних технологій, застосовуючи системний підхід та знання основ теорії захисту інформації; - вирішувати задачі управління процедурами ідентифікації, автентифікації, авторизації, користувачів і процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах - проектувати та реалізувати комплексні системи захисту інформації в автоматизованих системах організації (підприємства) відповідно до вимог нормативних документів системи технічного захисту інформації; -вирішувати задачі захисту потоків даних в інформаційних, інформаційно-телекомунікаційних (автоматизованих) системах; - визначати рівень захищеності інформаційних ресурсів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах; -використовувати інструментальні засоби оцінювання можливості реалізації потенційних загроз інформації, що обробляється в інформаційно-телекомунікаційних (автоматизованих) системах.
КФ 6. Здатність відновлювати штатне функціонування інформаційних, інформаційно-телекомунікаційних (автоматизованих) систем після реалізації загроз, здійснення кібератак, збоїв та відмов різних класів та походження.	-вирішувати задачі управління процесами забезпечення безперервності бізнесу з використанням процедур резервування програмного забезпечення та безпосередньо інформаційних ресурсів; -вирішувати задачі корекції цілей, стратегій, планів забезпечення безперервності бізнес процесів після здійснення кібератак, збоїв та відмов різних класів. -створювати і впроваджувати плани процесу забезпечення безперервності бізнесу; - виконувати аналіз налаштувань елементів інформаційних систем та комунікаційного обладнання;
КФ 7. Здатність впроваджувати та забезпечувати функціонування комплексних систем захисту інформації (комплекси нормативно-правових, організаційних та технічних засобів і методів, процедур, практичних прийомів	- вирішувати задачі супроводу та впровадження комплексних систем захисту інформації, а також протидії несанкціонованому доступу до ресурсів і процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах; -здійснювати оцінку рівня захищеності інформації що обробляється в інформаційно-телекомунікаційних системах використовувати інструментальні засоби оцінювання

та ін.)	наявності потенційних вразливостей; - вирішувати задачі управління комплексною системою захисту інформації в інформаційних та інформаційно-телекомунікаційних (автоматизованих); - вирішувати задачі експертизи, випробування комплексних систем захисту інформації.
КФ 8. Здатність здійснювати процедури управління інцидентами, проводити розслідування, надавати їм оцінку.	- вирішувати задачі попередження та виявлення, ідентифікації, аналізу та реагування на інциденти в інформаційних, інформаційно-телекомунікаційних (автоматизованих) системах; - проводити розслідування інцидентів інформаційної безпеки та/або кібербезпеки базуючись на національних та міжнародних регулюючих актах, процедурах та положеннях в сфері інформаційної безпеки та/або кібербезпеки; - забезпечувати дотримання політики ведення журналів реєстрації подій та інцидентів з встановленим рівнем деталізації;
КФ 9. Здатність здійснювати професійну діяльність на основі впровадженої системи управління інформаційною та/або кібербезпекою.	- забезпечувати безперервність бізнес процесів організації на базі теорії ризиків та системи управління інформаційною безпекою, згідно вітчизняних та міжнародних вимог і стандартів; -забезпечувати функціонування системи управління інформаційною та\або кібербезпекою організації на основі керування інформаційними ризиками, здійснення процедур їх кількісного і якісного оцінки;
КФ 10. Здатність застосовувати методи та засоби криптографічного та технічного захисту інформації на об’єктах інформаційної діяльності.	- аналізувати та визначати можливість застосування технологій, методів та засобів криптографічного захисту інформації; - аналізувати та визначати можливість застосування технологій, методів та засобів технічного захисту інформації; - виявляти небезпечні сигнали технічних засобів; - вимірювати параметри небезпечних та завадових сигналів під час інструментального контролю захищеності інформації від витоку технічними каналами; - визначати ефективність захисту інформації від витоку технічними каналами відповідно до вимог нормативних документів системи технічного захисту інформації; - інтерпретувати результати проведення спеціальних вимірювань з використанням технічних засобів, контролю характеристик інформаційно-телекомунікаційних систем відповідно до вимог нормативних документів системи технічного захисту інформації; – обґрунтовувати можливість створення технічних каналів витоку інформації на об’єктах інформаційної діяльності; – впроваджувати заходи та засоби технічного захисту інформації від витоку технічними каналами;
КФ 11. Здатність виконувати моніторинг ресурсів і процесів функціонування, інформаційно-телекомунікаційних (автоматизованих) систем згідно встановленої політики	- забезпечувати процеси моніторингу доступу до ресурсів і процесів інформаційно-телекомунікаційних систем; -забезпечувати конфігурування та функціонування систем моніторингу ресурсів та процесів в інформаційно-телекомунікаційних системах;

інформаційної та/або кібербезпеки.	
КФ 12. Здатність аналізувати, виявляти та оцінювати можливі загрози, уразливості та дестабілізуючі чинники інформаційному простору та інформаційним ресурсам згідно встановленої політики інформаційної та/або кібербезпеки.	- виконувати впровадження та підтримку систем виявлення вторгнень та використовувати комплекси захисту для забезпечення необхідного рівня захищеності інформації в інформаційних, інформаційно-телекомунікаційних (автоматизованих) системах; - аналізувати ефективність систем виявлення та протидії несанкціонованому доступу до ресурсів і процесів в інформаційно-телекомунікаційних системах; - аналізувати та впроваджувати системи захисту від зловмисних програмних кодів.

5. Вимоги до наявності системи внутрішнього забезпечення якості вищої освіти

Забезпечення якості підготовки здобувачів вищої освіти першого (бакалаврського) рівня освітньої програми «Кібербезпека» передбачає здійснення таких процедур і заходів:

- здійснення моніторингу та періодичного перегляду освітніх програм;
- щорічне оцінювання здобувачів вищої освіти, науково-педагогічних і педагогічних працівників вищого навчального закладу та регулярне оприлюднення результатів таких оцінювань на офіційному веб-сайті вищого навчального закладу, на інформаційних стендах та в будь-який інший спосіб;
- забезпечення підвищення кваліфікації педагогічних, наукових і науково-педагогічних працівників;
- забезпечення наявності необхідних ресурсів для організації освітнього процесу, у тому числі самостійної роботи студентів, за кожною освітньою програмою;
- забезпечення наявності інформаційних систем для ефективного управління освітнім процесом;
- забезпечення публічності інформації про освітні програми, ступені вищої освіти та кваліфікації;
- забезпечення ефективної системи запобігання та виявлення академічного плагіату у наукових працях працівників вищих навчальних закладів і здобувачів вищої освіти;
- інших процедур і заходів.