

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ЧЕРКАСЬКИЙ ДЕРЖАВНИЙ ТЕХНОЛОГІЧНИЙ УНІВЕРСИТЕТ

«ЗАТВЕРДЖЕНО»

вченою радою ЧДТУ

протокол № 13 від «26» 06 2025 р.

Освітня програма вводиться в дію

з «01» 09 2025 р.

Ректор ЧДТУ

 Олег ГРИГОР

наказ № 7 від «26» 06 2025 р.

ОСВІТНЬО-ПРОФЕСІЙНА ПРОГРАМА

«Управління кібербезпекою та захист інформації»

Галузь знань	F Інформаційні технології
Спеціальність	F5 Кібербезпека та захист інформації
Рівень програми	Перший (бакалаврський) рівень вищої освіти, 6 рівень НРК, 1 цикл QF-EHEA, 6 рівень EQF
Рік впровадження	2025

РОЗРОБНИКИ ПРОГРАМИ:

Д.Т.Н., професор

науковий ступінь, вчене звання


підпис

Віра БАБЕНКО

ПІБ

К.Т.Н., доцент

науковий ступінь, вчене звання


підпис

Артем ЛАВДАНСЬКИЙ

ПІБ

К.Т.Н., доцент

науковий ступінь, вчене звання


підпис

Ольга НЕЧИПОРЕНКО

ПІБ

К.Т.Н., доцент

науковий ступінь, вчене звання


підпис

Анатолій ЧЕПИНОГА

ПІБ

К.Т.Н., доцент

науковий ступінь, вчене звання

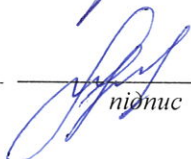

підпис

Інна РОЗЛОМІЙ

ПІБ

К.Т.Н., доцент

науковий ступінь, вчене звання


підпис

Світлана СИСОЄНКО

ПІБ

ПОГОДЖЕНО

Завідувач кафедри інформаційної
безпеки та комп'ютерної інженерії

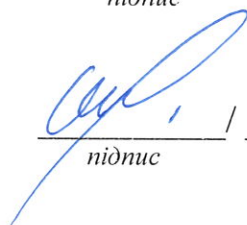
назва кафедри


підпис

/ Віра БАБЕНКО /

ПІБ

Навчально-методичний відділ


підпис

/
ПІБ

ВИЗНАЧЕННЯ І СКОРОЧЕННЯ

У програмі використано терміни та визначення, що наведені у Законі України «Про освіту», Законі України «Про вищу освіту» та Національному освітньому глосарію: вища освіта.

У програмі використані наступні позначення і скорочення:

- ЄКТС (European Credit Transfer and Accumulation System) – Європейська кредитна трансферно-накопичувальна система;
- НРК – Національна рамка кваліфікацій;
- ЗВО – здобувач вищої освіти, заклад вищої освіти;
- ІК – інтегральна компетентність;
- ЗК – загальні компетентності;
- ФК – фахові компетентності;
- ОЗП – обов’язкові компоненти циклу загальної підготовки;
- ОПП – обов’язкові компоненти циклу професійної підготовки;
- ВЗП – вибіркові компоненти циклу загальної підготовки;
- ВПП – вибіркові компоненти циклу професійної підготовки;
- НДВВЗП – навчальні дисципліни вільного вибору циклу загальної підготовки;
- НДВВПП – навчальні дисципліни вільного вибору циклу професійної підготовки;
- А – атестація.

ВСТУП

Освітньо-професійна програма – система освітніх компонентів на відповідному рівні вищої освіти в межах спеціальності, що визначає вимоги до рівня освіти осіб, які можуть розпочати навчання за цією програмою, перелік навчальних дисциплін і логічну послідовність їх вивчення, кількість кредитів ЄКТС, необхідних для виконання цієї програми, а також очікувані результати навчання (компетентності), якими повинен оволодіти здобувач відповідного ступеня вищої освіти.

Освітньо-професійна програма «Управління кібербезпекою та захист інформації» спрямована на підготовку фахівців, здатних ефективно захищати інформаційні ресурси в умовах зростаючих кіберзагроз, дотримуючись принципів сталого управління ризиками, правового регулювання та сучасних технологічних стандартів.

Освітня програма використовується під час проведення ліцензійної експертизи на провадження освітньої діяльності за відповідною спеціальністю та рівнем вищої освіти, інспектування освітньої діяльності за спеціальністю.

Освітня програма призначена для:

- науково-педагогічних та педагогічних працівників закладів вищої освіти (наукових установ);
- здобувачів відповідного рівня вищої освіти;
- роботодавців для отримання інформації щодо академічного та професійного профілю випускників;
- компетентних фахівців з визнання документів про вищу освіту;
- акредитаційних інституцій.

Зміст і структура освітньої програми затверджуються на весь період навчання ЗВО і не може змінюватися протягом терміну навчання.

Зміст освітньої програми крім професійної підготовки забезпечує формування компетентностей, що є необхідними для самореалізації, активної громадянської позиції, соціальної злагоди і здатності до працевлаштування у суспільстві.

Освітня програма оприлюднюється на сайті університету.

Освітньо-професійна програма «Управління кібербезпекою та захист інформації» розроблена на основі стандарту вищої освіти з спеціальності 125 «Кібербезпека та захист інформації» галузі знань 12 «Інформаційні технології» для першого (бакалаврського) рівня вищої освіти, що затверджений наказом Міністерства освіти і науки України 04.10.2018 р. № 1074 з урахуванням змін відповідно до наказу Міністерства освіти і науки України від 29.10.2024 № 1547.

1 ЗАГАЛЬНА ХАРАКТЕРИСТИКА

Рівень програми	Перший (бакалаврський рівень вищої освіти, 6 рівень НРК, 1 цикл QF-EHEA, 6 рівень EQF)
Обсяг програми	- на базі повної загальної середньої освіти становить 240 кредитів ЄКТС, з яких 180 кредитів (75 %) спрямовано на забезпечення загальних та спеціальних (фахових) компетентностей, 60 кредитів (25 %) спрямовано на вибіркову складову. - на базі ступеня «молодший бакалавр» (освітньо-кваліфікаційного рівня «молодший спеціаліст») заклад вищої освіти має право визнати та перезарахувати кредити ЄКТС, отримані в межах попередньої освітньої програми підготовки молодшого бакалавра (молодшого спеціаліста), обсягом не більше ніж 120 кредитів ЄКТС. - на основі ступеня «фаховий молодший бакалавр» заклад вищої освіти має право визнати та перезарахувати не більше ніж 60 кредитів ЄКТС, отриманих за попередньою освітньою програмою фахової передвищої освіти. Прийом на основі ступенів «молодший бакалавр», «фаховий молодший бакалавр» або освітньо-кваліфікаційного рівня «молодший спеціаліст» здійснюється за результатами національного мультипредметного тесту в порядку, визначеному законодавством.
Рік впровадження	2025 рік
Галузь знань	F Інформаційні технології
Спеціальність	F5 Кібербезпека та захист інформації
Вимоги до рівня освіти осіб, які можуть здобувати вищу освіту за програмою	Згідно вимог ст. 5 Закону України «Про вищу освіту» особа має право здобувати ступінь бакалавра за умови наявності в неї повної загальної середньої освіти. Або відповідно до наказу Міністерства освіти і науки України від 28.05.2021 № 593 на основі ступенів «молодший бакалавр», «фаховий молодший бакалавр» або освітньо-кваліфікаційного рівня «молодший спеціаліст».
Термін навчання	Денна форма – 3 роки 10 місяців
Освітня кваліфікація	Бакалавр з кібербезпеки та захисту інформації
Академічні	Мають право на здобуття освіти на другому

права	(магістерському) рівні вищої освіти. Здобуття або вдосконалення освіти та професійної підготовки в системі освіти дорослих.
Ціль програми	Підготувати здобувачів вищої освіти, спроможних розробляти системи управління захистом інформації та комплексні системи захисту інформації, модулі та компоненти криптографічних засобів захисту інформації, використовувати спеціалізовані захищені бази даних для накопичення і обробки інформації з обмеженим доступом, проводити експертизу комплексних систем захисту інформації та здійснювати їх підтримку, впроваджувати програмні системи автоматизованої обробки та захисту інформації, а також організовувати технічний, правовий та соціальний захист інформації.
Особливості програми	Програма забезпечує надання випускникам наступних знань, вмінь та навичок: вміти застосовувати законодавчу та нормативно-правову базу, міжнародні вимоги, практики і стандарти і в галузі кібербезпеки; вміти використовувати інформаційно-комунікаційні технології а також програмні та програмно-апаратні засобів функціонування захищених комп'ютерних систем і мереж та інформаційно-телекомунікаційних систем; забезпечувати неперервність бізнесу згідно встановленої політики кібербезпеки; застосовувати методи та засоби криптографічного та технічного захисту інформації на об'єктах інформаційної діяльності; здійснювати професійну діяльність по забезпеченню ефективного управління інформаційною та/або кібербезпекою.
Підходи до викладання та навчання	Лекції із застосуванням мультимедіа, лабораторні роботи, семінари, практичні заняття в малих групах, дистанційне навчання, самостійна робота на основі підручників, навчальних посібників, конспектів та інших матеріалів, консультації із викладачами.
Система оцінювання	Письмові та усні екзамени, заліки, курсові проекти та роботи, розрахунково-графічні роботи, звіти з лабораторних робіт, звіти з практик, усні та мультимедійні презентації, модульні контрольні роботи.
Форма атестації здобувачів	Атестація здійснюється у формі кваліфікаційного іспиту. До атестації допускаються здобувачі вищої освіти, які виконали всі вимоги програми підготовки. Єдиний державний кваліфікаційний іспит, що передбачає оцінювання досягнень результатів навчання, визначених стандартом та освітньою програмою.

Академічна мобільність	Академічна мобільність реалізується відповідно до Постанови КМУ № 579 “Про затвердження Положення про порядок реалізації права на академічну мобільність” від 12 серпня 2015 року та Положенням про академічну мобільність у Черкаському державному технологічному університеті. (Введеного в дію наказом ректора від 16 листопада 2021 р. № 351/01). Наявність двосторонніх договорів між Черкаським державним технологічним університетом та закладами вищої освіти України забезпечує національну кредитну мобільність. Зміст освітньо-професійної програми дозволяє приймати участь у програмах подвійних дипломів та бути конкурентоспроможним на світовому ринку праці.
Навчання іноземних здобувачів вищої освіти	Не передбачено.

2 ПРОГРАМНІ КОМПЕТЕНТНОСТІ

2.1 Інтегральна компетентність

ІК - здатність розв'язувати складні спеціалізовані задачі і практичні завдання у галузі кібербезпеки та захисту інформації.

2.2 Загальні компетентності

Шифр	Компетентності
ЗК1	Здатність застосовувати знання у практичних ситуаціях.
ЗК2	Знання та розуміння предметної області і розуміння професійної діяльності.
ЗК3	Здатність спілкуватися державною мовою як усно, так і письмово.
ЗК4	Здатність спілкуватися іноземною мовою.
ЗК5	Здатність вчитися і оволодівати сучасними знаннями.
ЗК6	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;
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.

2.3 Спеціальні (фахові) компетентності

Шифр	Компетентності
СК1	Здатність застосовувати законодавчу та нормативно-правову базу, а також державні та міжнародні вимоги, практики і стандарти у професійній діяльності.
СК2	Здатність використовувати інформаційні технології, сучасні методи і моделі кібербезпеки та 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-телекомунікаційних системах згідно встановленої політики кібербезпеки та захисту інформації.

СК5	Здатність відновлювати функціонування інформаційних та інформаційно-телекомунікаційних систем після реалізації загроз, здійснення кібератак, збоїв і відмов різних класів та походження.
СК6	Здатність впроваджувати та забезпечувати функціонування комплексних систем захисту інформації (комплекси нормативно-правових, організаційних та технічних засобів і методів, процедур, практичних прийомів тощо.)
СК7	Здатність здійснювати професійну діяльність на основі впровадженої системи управління інформаційною та кібербезпекою.
СК8	Здатність застосовувати методи та засоби криптографічного захисту інформації на об'єктах інформаційної діяльності.
СК9	Здатність застосовувати методи та засоби технічного захисту інформації на об'єктах інформаційної діяльності.
СК10	Здатність виконувати моніторинг інформаційних процесів, аналізувати, виявляти, оцінювати можливі вразливості та загрози інформаційному простору й інформаційним ресурсам згідно з встановленою політикою інформаційної безпеки.
СК11	Здатність впроваджувати політики, процедури й технічні засоби для забезпечення інформаційної безпеки в корпоративному середовищі.
СК12	Здатність виявляти вразливості в інформаційних системах шляхом проведення тестування на проникнення, сканування, аналізу конфігурацій.

2.4 Нормативний зміст підготовки здобувачів вищої освіти, сформульований у контексті результатів навчання

Кінцеві, підсумкові та інтегративні результати навчання, що визначають нормативний зміст підготовки і корелюються з визначеним вище переліком загальних і фахових компетентностей, подано нижче.

Шифр	Програмні результати навчання
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

Шифр	Програмні результати навчання
	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 області 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-телекомунікаційних 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-телекомунікаційних систем з використання процедур резервування згідно встановленої політики безпеки і забезпечувати функціонування спеціального програмного забезпечення щодо захисту і 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

Шифр	Програмні результати навчання
	наслідками реалізації загроз інформаційній безпеці в кризових ситуаціях, на основі здійснення процедур кількісної і якісної оцінки ризиків.
RH18	Аналізувати, застосовувати методи та засоби криптографічного захисту інформації на об'єктах інформаційної діяльності.
RH19	Вирішувати задачі щодо організації та контролю стану криптографічного захисту інформації, зокрема відповідно до вимог нормативних документів.
RH20	Визначати загрози створення технічних каналів витоку інформації на об'єктах інформаційної діяльності; впроваджувати засоби і заходи технічного захисту інформації від витоку технічними каналами, проводити обслуговування і контроль стану апаратних засобів захисту інформації та комплексів технічного захисту інформації.
RH21	Виконувати впровадження, підтримку, аналіз ефективності систем виявлення несанкціонованого доступу, дій з інформацією в інформаційній системі, вразливостей, можливих загроз інформаційному простору й інформаційним ресурсам та використовувати комплекси захисту для забезпечення необхідного рівня захищеності інформації в інформаційних системах.
RH22	Виконувати впровадження організаційно-розпорядчих та технічних заходів кібербезпеки у корпоративних ІТ-системах.
RH23	Застосовувати принципи управління ризиками для побудови системи захисту інформації з урахуванням бізнес-контексту.
RH24	Здійснювати розвідку, виявлення вразливостей та моделювання атак з використанням сучасних інструментів.
RH25	Виконувати аналіз результатів сканування вразливостей і розробляти рекомендації з усунення загроз.

3 ПЕРЕЛІК КОМПОНЕНТ ОСВІТНЬО-ПРОФЕСІЙНОЇ ПРОГРАМИ

Код компо- ненти	Компоненти освітньо- професійної програми (навчальні дисципліни, практики, кваліфікаційна робота/іспит)	Кількі сть кредитів ЄКТС	Формування компетентностей		Програмні результати навчання
			Загальні	Спеціальні	
1 Обов'язкові компоненти					
1.1 Цикл загальної підготовки					
ОЗП 1	Історія та культура України	3	ЗК6	-	РН6. Адаптуватися до нових умов і технологій професійної діяльності, прогнозувати кінцевий результат.
ОЗП 2	Українська мова за професійним спрямуванням	3	ЗК3, ЗК7	-	РН1. Вільно спілкуватися державною мовою усно та письмово при виконанні професійних обов'язків.
ОЗП 3	Філософія	3	ЗК1, ЗК6, ЗК7	-	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.
ОЗП 4	Іноземна мова за професійним спрямуванням	14	ЗК4	-	РН2. Спілкуватися іноземною мовою з метою забезпечення ефективності професійної комунікації.
ОЗП 5	Фізичне виховання	6	ЗК8	-	РН6. Адаптуватися до нових умов і технологій професійної діяльності, прогнозувати кінцевий результат.
ОЗП 6	Безпека життєдіяльності та цивільний захист	3	ЗК8	-	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.
Загальний обсяг обов'язкових компонент загальної підготовки		32			
1.2 Цикл професійної підготовки					
ОПП 1	Вступ до кібербезпеки	4	ЗК2, ЗК7	СК1, СК2	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. РН9. Знати та застосовувати законодавство України та міжнародні вимоги, практики і стандарти з метою здійснення професійної діяльності в галузі кібербезпеки та захисту інформації.
ОПП 2	Вища математика	8	ЗК1, ЗК5	СК2	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. 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 області кібербезпеки та захисту інформації, формулювати їх математичну постановку та обирати раціональний метод вирішення. РН10. Використовувати сучасні інформаційні технології, методи і моделі кібербезпеки та систем захисту інформації для здійснення професійної діяльності.

ОПП 3	Архітектура комп'ютерів	4	ЗК2	СК5, СК7	РН14. Вирішувати задачі управління процесами відновлення штатного функціонування інформаційних та інформаційно-телекомунікаційних систем з використання процедур резервування згідно встановленої політики безпеки і забезпечувати функціонування спеціального програмного забезпечення щодо захисту і 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. 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 кількісної і якісної оцінки ризиків.
ОПП 4	Алгоритми та структури даних	4	ЗК2	СК8, СК10	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.
ОПП 5	Програмування	9	ЗК1	СК2, СК10	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.

					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. РН10. Використовувати сучасні інформаційні технології, методи і моделі кібербезпеки та систем захисту інформації для здійснення професійної діяльності.
ОПП 6	Фізика	4	ЗК1, ЗК5	СК9	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 області кібербезпеки та захисту інформації, формулювати їх математичну постановку та обирати раціональний метод вирішення. 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.
ОПП 7	Дискретна математика	4	ЗК1, ЗК2, ЗК5	СК2, СК10	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. 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 області кібербезпеки та захисту інформації, формулювати їх математичну постановку та обирати раціональний метод вирішення.
ОПП 8	Основи штучного інтелекту	4	ЗК1, ЗК2	СК2	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. РН10. Використовувати сучасні інформаційні технології, методи і моделі кібербезпеки та систем захисту інформації для здійснення професійної діяльності.
ОПП 9	Інформаційна безпека держави	6	ЗК2	СК1, СК2	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. 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.
ОПП 10	Теорія ймовірності та математична статистика	4	ЗК1, ЗК2	СК2, СК3, СК10	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. 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. 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.
ОПП 11	Бази даних	4	ЗК2	СК2, СК3, СК12	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. 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. РН23. Застосовувати принципи управління ризиками для побудови системи захисту інформації з урахуванням бізнес-контексту.
ОПП 12	Операційні системи	7	ЗК8	СК4, СК5	РН6. Адаптуватися до нових умов і технологій професійної діяльності, прогнозувати кінцевий результат. РН12. Застосовувати методи та засоби захисту інформації в інформаційних та інформаційно-телекомунікаційних 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-телекомунікаційних систем з використання процедур резервування згідно встановленої політики безпеки і забезпечувати функціонування спеціального програмного забезпечення щодо захисту і відновлення інформації.
ОПП 13	Організаційне забезпечення захисту інформації	4	ЗК6	СК7, СК10, СК11	РН9. Знати та застосовувати законодавство України та міжнародні вимоги, практики і стандарти з метою здійснення професійної діяльності в галузі кібербезпеки та захисту інформації. 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 кількісної і якісної оцінки ризиків. 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. РН22. Виконувати впровадження організаційно-розпорядчих та технічних заходів кібербезпеки у корпоративних ІТ-системах.
ОПП 14	Комп'ютерні мережі	8	ЗК2, ЗК5	СК4, СК5	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. РН12. Застосовувати методи та засоби захисту інформації в інформаційних та інформаційно-телекомунікаційних 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-телекомунікаційних систем з використання процедур резервування згідно встановленої політики безпеки і забезпечувати функціонування спеціального програмного забезпечення щодо захисту і відновлення інформації. РН24. Здійснювати розвідку, виявлення вразливостей та моделювання атак з використанням сучасних інструментів.
ОПП 15	Управління ризиками інформаційної безпеки	4	ЗК5	СК3, СК7, СК9, СК10, СК11 РН11. Планувати підготовку та забезпечувати неперервність бізнес-процесів в організаціях згідно зі встановленою політикою кібербезпеки з урахуванням вимог до захисту інформації. 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 кількісної і якісної оцінки ризиків. РН 20. 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.
ОПП 16	Тестування на проникнення	4	ЗК1	СК4, СК6, СК12	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. РН16. Вирішувати задачі впровадження та супроводу комплексних систем захисту інформації в інформаційних системах. 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. РН24. Здійснювати розвідку, виявлення вразливостей та моделювання атак з використанням сучасних інструментів. РН25. Виконувати аналіз результатів сканування вразливостей і розробляти рекомендації з усунення загроз.
ОПП 17	Криптографічний захист інформації	8	ЗК1	СК8, СК11	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. 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. РН22. Виконувати впровадження організаційно-розпорядчих та технічних заходів кібербезпеки у корпоративних ІТ-системах. РН25. Виконувати аналіз результатів сканування вразливостей і розробляти рекомендації з усунення загроз.

ОПП 18	Безпека інформації в комп'ютерних системах	4	ЗК5	СК4, СК8	РН8. Застосовувати знання й розуміння математики та фізики в професійній діяльності, формалізувати задачі предметної області кібербезпеки та захисту інформації, формулювати їх математичну постановку та обирати раціональний метод вирішення. РН12. Застосовувати методи та засоби захисту інформації в інформаційних та інформаційно-телекомунікаційних системах відповідно до встановленої політики інформаційної безпеки. 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.
ОПП 19	Комплексні системи захисту інформації	6	ЗК1	СК6, СК7	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. 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 кількісної і якісної оцінки ризиків.
ОПП 20	Моніторинг та управління інцидентами кібербезпеки	6	ЗК5	СК3, СК5, СК10	РН8. Застосовувати знання й розуміння математики та фізики в професійній діяльності, формалізувати задачі предметної області кібербезпеки та захисту інформації, формулювати їх математичну постановку та обирати раціональний метод вирішення. РН11. Планувати підготовку та забезпечувати неперервність бізнес-процесів в організаціях згідно зі встановленою політикою кібербезпеки з урахуванням вимог до захисту інформації. РН14. Вирішувати задачі управління процесами відновлення

					штатного функціонування інформаційних та інформаційно-телекомунікаційних систем з використання процедур резервування згідно встановленої політики безпеки і забезпечувати функціонування спеціального програмного забезпечення щодо захисту і 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. 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.
ОПП 21	Інженерно-технічний захист інформації	4	ЗК5	СК6, СК9	РН8. Застосовувати знання й розуміння математики та фізики в професійній діяльності, формалізувати задачі предметної області кібербезпеки та захисту інформації, формулювати їх математичну постановку та обирати раціональний метод вирішення. РН16. Вирішувати задачі впровадження та супроводу комплексних систем захисту інформації в інформаційних системах. 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.
ОПП 22	Захист комп'ютерних мереж	6	ЗК1	СК2, СК4	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. РН10. Використовувати сучасні інформаційні технології, методи і

					моделі кібербезпеки та систем захисту інформації для здійснення професійної діяльності. РН12. Застосовувати методи та засоби захисту інформації в інформаційних та інформаційно-телекомунікаційних 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.
ОПП 23	Адміністрування та безпека хмарних технологій	4	ЗК2	СК2, СК3, СК5	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. РН11. Планувати підготовку та забезпечувати неперервність бізнес-процесів в організаціях згідно зі встановленою політикою кібербезпеки з урахуванням вимог до захисту інформації. РН14. Вирішувати задачі управління процесами відновлення штатного функціонування інформаційних та інформаційно-телекомунікаційних систем з використання процедур резервування згідно встановленої політики безпеки і забезпечувати функціонування спеціального програмного забезпечення щодо захисту і 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.
ОПП 24	Безпека програмного забезпечення	4	ЗК6	СК2, СК3, СК8	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.

					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.
ОПП 25	Технології та безпека IoT	4	ЗК1	СК2, СК9	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. РН10. Використовувати сучасні інформаційні технології, методи і моделі кібербезпеки та систем захисту інформації для здійснення професійної діяльності. РН20. Визначати загрози створення технічних каналів витоку інформації на об'єктах інформаційної діяльності; впроваджувати засоби і заходи технічного захисту інформації від витоку технічними каналами, проводити обслуговування і контроль стану апаратних засобів захисту інформації та комплексів технічного захисту інформації.
ОПП 26	Ознайомча практика	4	ЗК1, ЗК3, ЗК7	СК1, СК2, СК3, СК4	РН1. Вільно спілкуватися державною мовою усно та письмово при виконанні професійних обов'язків. РН3. Застосовувати принцип неприпустимості корупції та будь-яких інших проявів недоброчесності у професійній діяльності.
ОПП 27	Перша виробнича практика	4	ЗК1, ЗК3, ЗК7	СК1, СК2, СК3, СК4, СК5, СК6	РН1. Вільно спілкуватися державною мовою усно та письмово при виконанні професійних обов'язків. 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. 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.
ОПП 28	Друга виробнича практика	4	ЗК1, ЗК3, ЗК7	СК1, СК2, СК3, СК4, СК5, СК6, СК7, СК8	РН1. Вільно спілкуватися державною мовою усно та письмово при виконанні професійних обов'язків. 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. 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. 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 кількісної і якісної оцінки ризиків.

					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. РН23. Застосовувати принципи управління ризиками для побудови системи захисту інформації з урахуванням бізнес-контексту.
ОПП 29	Проектна практика	4	ЗК1, ЗК3, ЗК7	СК1, СК2, СК3, СК4, СК5, СК6, СК7, СК8, СК9, СК10, СК11, СК12	РН1. Вільно спілкуватися державною мовою усно та письмово при виконанні професійних обов'язків. 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. 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. 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. 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 кількісної і якісної оцінки ризиків. 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. РН25. Виконувати аналіз результатів сканування вразливостей і розробляти рекомендації з усунення загроз.
Загальний обсяг обов’язкових компонент професійної підготовки		146			
Атестація					
A 1	Кваліфікаційний іспит	2			
	Єдиний державний кваліфікаційний іспит				
Загальний обсяг обов’язкових компонент		180			
2 Вибіркові компоненти					
2.1 Цикл загальної підготовки					
ВЗП 1	Теоретична підготовка БЗВП* / НДВВЗП1	3	-	-	
ВЗП 2	НДВВЗП2	3	-	-	
ВЗП 3	НДВВЗП3	3	-	-	
ВЗП 4	НДВВЗП4	3	-	-	
ВЗП 5	НДВВЗП5	3	-	-	
ВЗП 6	НДВВЗП6	3	-	-	
ВЗП 7	НДВВЗП7	3	-	-	
ВЗП 8	НДВВЗП8	3	-	-	
Загальний обсяг вибірових компонент загальної підготовки		24			
2.2 Цикл професійної підготовки					

ВПП 1	НДВВПП1	4	-	-	
ВПП 2	НДВВПП2	4	-	-	
ВПП 3	НДВВПП3	4	-	-	
ВПП 4	НДВВПП4	4	-	-	
ВПП 5	НДВВПП5	4	-	-	
ВПП 6	НДВВПП6	4	-	-	
ВПП 7	НДВВПП7	4	-	-	
ВПП 8	НДВВПП8	4	-	-	
ВПП 9	НДВВПП9	4	-	-	
Загальний обсяг вибірових компонент професійної підготовки		36			
Загальний обсяг вибірових компонент		60			
Загальний обсяг освітньої програми		240			

* Теоретична підготовка БЗВП - Теоретична підготовка базової загальновійськової підготовки

НДВВЗП містять дисципліни гуманітарного, природничого та соціально-економічного спрямування. НДВВПП містять дисципліни безпосередньо фахової підготовки за певною галуззю знань, які відображають світові та вітчизняні тенденції на ринку праці та індивідуальні спрямування ЗВО.

Вибір навчальних дисциплін вільного вибору обох циклів відбувається з Каталогу, який оновлюється і затверджується рішенням вченої ради Черкаського державного технологічного університету щорічно до початку процедури вибору навчальних дисциплін ЗВО.

Навчальні дисципліни вільного вибору, які включаються до Каталогу, забезпечують поглиблену підготовку ЗВО за освітньої програмою та здобуття додаткових (до тих, що передбачені Стандартом вищої освіти відповідної спеціальності) фундаментальних, природничо-наукових, мовних, загально-економічних, професійно-практичних компетентностей, орієнтованих на задоволення освітніх і культурних потреб ЗВО та сприяння його академічної мобільності.

4 ВИМОГИ ДО НАЯВНОСТІ СИСТЕМИ ВНУТРІШНЬОГО ЗАБЕЗПЕЧЕННЯ ЯКОСТІ ВИЩОЇ ОСВІТИ

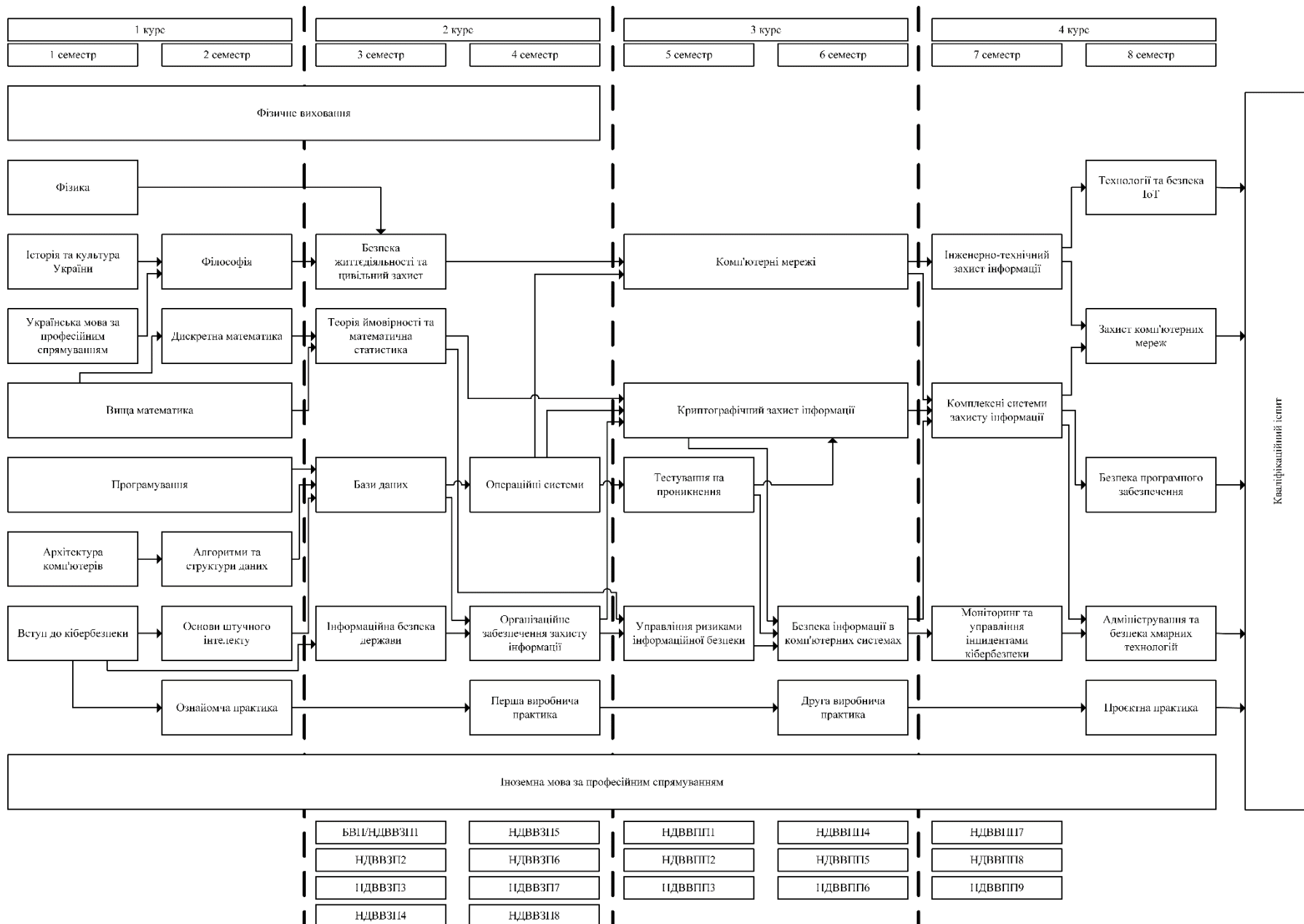
У Черкаському державному технологічному університеті впроваджена система внутрішнього забезпечення якості освітньої діяльності та якості вищої освіти, яка передбачає здійснення таких процедур і заходів:

- удосконалення планування освітньої діяльності через затвердження, моніторинг і періодичний перегляд освітніх програм;
- щорічне оцінювання здобувачів вищої освіти, науково-педагогічних і педагогічних працівників та регулярне оприлюднення результатів таких оцінювань на офіційному веб-сайті університету, на інформаційних стендах та в будь-який інший спосіб;
- посилення кадрового потенціалу шляхом забезпечення підвищення кваліфікації науково-педагогічних працівників; оптимізації процедури конкурсного відбору на заміщення посад науково-педагогічних працівників;
- забезпечення наявності необхідних ресурсів для організації освітнього процесу, в тому числі самостійної роботи здобувачів вищої освіти, за кожною освітньою програмою;
- забезпечення наявності інформаційних систем для ефективного управління освітнім процесом;
- забезпечення публічності та прозорості інформації про освітні програми, ступені вищої освіти та кваліфікації;
- створення ефективної системи запобігання та виявлення академічного плагіату в наукових, навчальних та методичних працях науково-педагогічних працівників і здобувачів вищої освіти;
- інших процедур і заходів, спрямованих на внутрішнє забезпечення якості вищої освіти в Університеті.

Критеріями розроблення освітньої програми є: потреба суспільства та інтелектуальний потенціал (цінність) програми; зацікавленість здобувачів вищої освіти освітньою програмою; конкурентоздатність фахівців, які навчалися за певною програмою, та їх попит на ринку праці; відповідність освітньої програми сучасним і перспективним вимогам до професійної діяльності фахівців, їх особистісним освітнім потребам; зацікавленість факультету (кафедри) та наявність попереднього досвіду підготовки фахівців за суміжними спеціальностями; наявність необхідних навчальних ресурсів тощо.

Функціонування системи внутрішнього забезпечення якості унормовано «Положенням про систему внутрішнього забезпечення якості вищої освіти у Черкаському державному технологічному університеті»

5 СТРУКТУРНО-ЛОГІЧНА СХЕМА ПІДГОТОВКИ



6 ПРИДАТНІСТЬ ДО ПРАЦЕВЛАШТУВАННЯ

Код за КП	Назва професійного стандарту
2139.2	Адміністратор мереж і систем
2139.2	Фахівець сфери захисту інформації
2139.2	Фахівець з питань безпеки (інформаційно-комунікаційні технології)
2132.2	Конструктор систем кібербезпеки
2139.2	Фахівець з підтримки інфраструктури кіберзахисту
2139.2	Фахівець з реагування на інциденти кібербезпеки
2139.2	Фахівець з криптографічного захисту інформації
2139.2	Фахівець з технічного захисту інформації
2139.2	Фахівець з тестування систем захисту інформації
2139.2	Аудитор інформаційних технологій (з кібербезпеки)
2139.2	Фахівець з оцінки заходів захисту інформації (з кібербезпеки)

Додаток 1

Матриця відповідності програмних компетентностей компонентам освітньо-професійної програми

[illegible]

Додаток 2

Матриця відповідності програмних результатів навчання компонентам освітньо-професійної програми

Програмні результати навчання	Компоненти освітньо-професійної програми (навчальні дисципліни)																																		
	ОЗП1	ОЗП2	ОЗП3	ОЗП4	ОЗП5	ОЗП6	ОПП1	ОПП2	ОПП3	ОПП4	ОПП5	ОПП6	ОПП7	ОПП8	ОПП9	ОПП10	ОПП11	ОПП12	ОПП13	ОПП14	ОПП15	ОПП16	ОПП17	ОПП18	ОПП19	ОПП20	ОПП21	ОПП22	ОПП23	ОПП24	ОПП25	ОПП26	ОПП27	ОПП28	ОПП29
РН1		+																													+	+	+	+	
РН2				+																															
РН3							+																									+	+	+	+
РН4							+	+		+	+			+			+			+										+			+	+	+
РН5			+					+		+	+		+	+	+	+				+													+	+	+
РН6	+		+		+	+				+				+	+			+		+															
РН7						+		+			+	+	+			+							+		+			+			+				+
РН8								+				+	+											+		+	+								
РН9							+								+				+											+			+	+	+
РН10								+			+			+	+		+					+						+		+	+		+	+	+
РН11																	+				+					+			+						
РН12																		+		+				+				+							
РН13																		+		+		+						+							
РН14									+									+		+							+			+					
РН15									+																		+			+					
РН16																						+			+		+								
РН17									+										+		+				+									+	+
РН18																							+	+							+				
РН19																							+	+							+				
РН20												+									+						+					+			

PH21																+			+		+	+				+								+	+
PH22																			+				+												
PH23																	+																	+	
PH24																			+		+														
PH25																					+	+													+

Матриця відповідності програмних результатів навчання програмним компетентностям освітньо-професійної програми

Програмні результати навчання	Інтегральна компетентність	Програмні компетентності																			
		Загальні компетентності								Спеціальні компетентності											
		ЗК ₁	ЗК ₂	ЗК ₃	ЗК ₄	ЗК ₅	ЗК ₆	ЗК ₇	ЗК ₈	СК ₁	СК ₂	СК ₃	СК ₄	СК ₅	СК ₆	СК ₇	СК ₈	СК ₉	СК ₁₀	СК ₁₁	СК ₁₂
PH1	+			+																	
PH2	+				+																
PH3	+						+	+													
PH4	+	+	+																		
PH5	+	+	+																		
PH6	+		+						+												
PH7	+	+							+												
PH8	+					+															
PH9	+						+			+											
PH10	+										+										
PH11	+											+									
PH12	+												+								
PH13	+												+								
PH14	+													+							
PH15	+													+							
PH16	+														+						
PH17	+															+					

PH18	+																+				
PH19	+																+				
PH20	+																	+			
PH21	+																		+		
PH22	+																			+	
PH23	+																			+	
PH24	+																				+
PH25	+																				+