Шановні роботодавці, здобувачі вищої освіти, академічна спільното!

Запрошуємо вас до участі в обговоренні Проєкту освітньо-професійної програми «КІБЕРБЕЗПЕКА ТА ЗАХИСТ ІНФОРМАЦІЇ» зі змінами, внесеними відповідно змін, внесених у стандарт вищої освіти за спеціальністю 125 «Кібербезпека» галузі знань 12 «Інформаційні технології» для першого (бакалаврського) рівня вищої освіти (Наказ МОН України №1547 від 29.10.2024)

(Термін реалізації ОПП «КІБЕРБЕЗПЕКА ТА ЗАХИСТ ІНФОРМАЦІЇ»: 2024/2025 – 2027/2028 н.р.)

Пропозиції, відгуки, зауваження стосовно змістового наповнення запропонованої до розгляду освітньо-професійної програми просимо надсилати на електронну адресу голови науково-методичної комісії спеціальності 125 «Кібербезпека та захист інформації» д.т.н., проф. Олексія Смірнова

dr.smirnovoa@gmail.com

Ваших листів також чекаємо за адресою:

Кафедра кібербезпеки та програмного забезпечення, Центральноукраїнський національний технічний університет, проспект Університетський, 8, м.Кропивницький, 25006

ПРОЄКТ

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
Центральноукраїнський національний технічний університет

ЗАТВЕРДЖЕНО
ВЧЕНОЮ РАДОЮ ЦНТУ
Протокол № __ від «__»____2024р.
Освітня програма вводиться в дію
з 1 вересня 2024 р.

Ректор
_____ Володимир КРОПІВНИЙ

ОСВІТНЬО-ПРОФЕСІЙНА ПРОГРАМА «КІБЕРБЕЗПЕКА ТА ЗАХИСТ ІНФОРМАЦІЇ»

РІВЕНЬ ВИЩОЇ ОСВІТИ Перший (бакалаврський) рівень
(назва рівня вищої освіти)

СТУПІНЬ ВИЩОЇ ОСВІТИ Бакалавр
(назва ступеня вищої освіти)

ГАЛУЗЬ ЗНАНЬ 12 Інформаційні технології
(шифр та назва галузі знань)

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

Кропивницький, 2024 р.

ЛИСТ ПОГОДЖЕННЯ
освітньо-професійної програми
«КІБЕРБЕЗПЕКА ТА ЗАХИСТ ІНФОРМАЦІЇ»

Рівень вищої освіти	**Перший (бакалаврський) рівень**
Ступінь вищої освіти	**Бакалавр**
Галузь знань	**12 Інформаційні технології**
Спеціальність	**125 Кібербезпека та захист інформації**

ПЕРЕДМОВА

Освітньо-професійна програма є нормативним документом, який регламентує нормативні, компетентнісні, кваліфікаційні, організаційні, навчальні та методичні вимоги у підготовці здобувачів вищої освіти першого (бакалаврського) рівня з галузі знань 12 «Інформаційні технології», спеціальності 125 «Кібербезпека та захист інформації» (*відповідно постанові Кабінету Міністрів України від 16 грудня 2022 р. № 1392 Про внесення змін до переліку галузей знань і спеціальностей, за якими здійснюється підготовка здобувачів вищої освіти*).

Освітньо-професійна програма заснована на компетентнісному підході підготовки бакалавра у галузі знань 12 «Інформаційні технології», спеціальності 125 «Кібербезпека та захист інформації».

Освітньо-професійна програма розроблена у відповідності до стандарту вищої освіти за спеціальністю 125 «Кібербезпека та захист інформації» галузі знань 12 «Інформаційні технології» для першого (бакалаврського) рівня вищої освіти, затвердженого та введеного в дію наказом Міністерства освіти і науки України від 04.10.2018 р. №1074 (у редакції наказу Міністерства освіти і науки України від 29.10.2024 р. №1547), та у відповідності з Порядком здійснення навчання населення діям у надзвичайних ситуаціях, затвердженим постановою Кабінету Міністрів України № 444 від 26.06.2013 р. зі змінами, внесеними згідно з Постановою Кабінету Міністрів України № 923 від 01.09.2021 робочою групою кафедри кібербезпеки та програмного забезпечення ЦНТУ у складі:

1. Смірнов Олексій Анатолійович, д.т.н., проф., завідувач кафедри кібербезпеки та програмного забезпечення.
2. Дрєєв Олександр Миколайович, к.т.н., доцент, доцент кафедри кібербезпеки та програмного забезпечення.
3. Смірнов Сергій Анатолійович, к.т.н., доцент, доцент кафедри автоматизації виробничих процесів.
4. Улічев Олександр Сергійович, к.т.н., ст.викладач кафедри кібербезпеки та програмного забезпечення.
5. Минайленко Роман Миколайович, к.т.н., доцент, доцент кафедри кібербезпеки та програмного забезпечення.

Гарант освітньо-професійної програми – Смірнов О.А., д.т.н., професор, завідувач кафедри кібербезпеки та програмного забезпечення.

Порядок розробки, експертизи і затвердження програми регулюється пунктом 8 статті 36 Закону України «Про вищу освіту», стандартом вищої освіти за спеціальністю 125 «Кібербезпека та захист інформації» галузі знань 12 «Інформаційні технології» для першого (бакалаврського) рівня вищої освіти, затвердженого та введеного в дію наказом Міністерства освіти і науки України від 04.10.2018 р. №1074 (у редакції наказу Міністерства освіти і науки України від 29.10.2024 р. №1547), а також Положенням про освітні програми та навчальні плани в Центральноукраїнському національному технічному університеті.

Програма схвалена Науково-методичною радою та затверджена Вченою радою Центральноукраїнського національного технічного університету.

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

1. Загальна інформація	
Повна назва вищого навчального закладу та структурного підрозділу	Центральноукраїнський національний технічний університет, механіко-технологічний факультет, кафедра кібербезпеки та програмного забезпечення
Рівень вищої освіти	Перший (бакалаврський)
Ступінь вищої освіти	Бакалавр
Галузь знань	12 Інформаційні технології
Спеціальність	125 Кібербезпека та захист інформації
Освітня кваліфікація	Бакалавр з кібербезпеки та захисту інформації
Кваліфікація в дипломі	Ступінь вищої освіти – Бакалавр Спеціальність – 125 Кібербезпека та захист інформації Освітньо-професійна програма «Кібербезпека та захист інформації»
Офіційна назва освітньої програми	Освітньо-професійна програма «Кібербезпека та захист інформації»
Тип диплому та обсяг освітньої програми	Диплом бакалавра. Обсяг кредитів ЄКТС, необхідний для здобуття ступеня бакалавра зі спеціальності 125 Кібербезпека та захист інформації, становить: – на базі повної загальної середньої освіти – 240 кредитів ЄКТС; – на базі здобутих освітніх ступенів молодшого бакалавра, фахового молодшого бакалавра (освітньо-кваліфікаційного рівня молодшого спеціаліста) ЦНТУ визнає та перезараховує не більше ніж 60 кредитів ЄКТС, отриманих в межах попередньої освітньої програми підготовки фахівців.
Наявність акредитації	Національне агентство із забезпечення якості вищої освіти Сертифікат акредитації освітньої програми № 5234, дійсний до 01.07.2028
Цикл/рівень	Національна рамка кваліфікацій України – 6 рівень, Рамка кваліфікацій Європейського простору вищої освіти QF EHEA – 1-й цикл (1st cycle), Європейська рамка кваліфікацій для навчання впродовж життя EQF LLL – 6 рівень (level 6).
Передумови	Для здобуття ступеня бакалавра зі спеціальності 125

	Кібербезпека та захист інформації можуть вступати особи, які здобули повну загальну середню освіту. Прийом на основі здобутого ступеня молодшого бакалавра, фахового молодшого бакалавра або освітньо-кваліфікаційного рівня молодшого спеціаліста здійснюється в порядку, визначеному законодавством. Умови вступу визначаються Умовами прийому на навчання для здобуття вищої освіти та Правилами прийому на навчання для здобуття вищої освіти до Центральноукраїнського національного технічного університету.
Мова викладання	Українська
Термін дії освітньої програми	До наступного оновлення програми, але не пізніше строку дії сертифіката про акредитацію.
Інтернет-адреса постійного розміщення опису освітньої програми	https://kntu.kr.ua/education/perelik-spetsialnostei-ta-osvitnikh-prohram

2. Мета освітньої програми	
Забезпечення освітньо-професійної підготовки фахівців з кібербезпеки та захисту інформації, які мають ґрунтовний хард- і софтскіловий потенціал ІТ-спеціаліста та здатність професійно самореалізуватися в галузі інформаційних технологій, відповідно до місії Центральноукраїнського національного технічного університету: розвиток кадрового, наукового, освітнього і культурного потенціалу центральноукраїнського регіону, підготовка визнаних на регіональному рівні, в Україні та інших країнах світу висококваліфікованих фахівців, а також надання освітніх і наукових послуг світового рівня якості.	
3. Характеристика освітньої програми	
Предметна область	**Об’єкти вивчення:** – технології кібербезпеки та захисту інформації; – процеси управління кібербезпекою та захистом інформації; – об’єкти інформаційної діяльності, в тому числі інформаційні та інформаційно-комунікаційні системи, інформаційні ресурси і технології. **Цілі навчання:** підготовка фахівців, здатних використовувати і впроваджувати технології кібербезпеки та захисту інформації та розв’язувати складні задачі у галузі кібербезпеки та захисту інформації, зокрема української системи криптографічного захисту інформації «Шифр-Х.509», організація заходів для попередження, локалізації й ліквідації наслідків надзвичайних ситуацій, а також набуття хард- та софтскілів, притаманних професіоналу-практику сфери ІТ і спеціалісту із захисту даних (Data Protection Officer). **Теоретичний зміст предметної області:** Принципи, концепції, теорії захисту життєво важливих інтересів людини, суспільства, держави під час використання кіберпростору, за якого забезпечуються сталий розвиток інформаційного суспільства та цифрового комунікативного середовища, своєчасне виявлення, запобігання і нейтралізація реальних і потенційних загроз національній безпеці України у кіберпросторі. **Методи, методики та технології:** методи, методики, та технології розв’язання теоретичних і практичних задач кібербезпеки та захисту інформації. **Інструменти та обладнання**:

	засоби, пристрої, мережне устаткування, прикладне та спеціалізоване програмне забезпечення, інформаційні системи та комплекси проектування, моделювання, контролю, моніторингу, зберігання, обробки, відображення та захисту даних (інформаційних потоків).
Орієнтація освітньої програми	Освітньо-професійна програма.
Фокус програми	Програма спрямована на здобуття кваліфікації для виконання професійної діяльності у сфері ІТ, розв'язання задач забезпечення кібернетичної безпеки, розвиток софтскілів освіченого громадянина європейської України, набуття професійних навичок ІТ-спеціаліста із захисту даних, умінь застосовувати технології й програмно-технічні засоби проектування, реалізації, впровадження й супроводження програмних засобів різного призначення, комплексних систем захисту інформації, кібербезпеки, комп'ютерних систем і мереж, інтернету речей, веб-технологій, а також забезпечення інформаційного і цивільного захисту, безпеки життєдіяльності. Здобувачі вищої освіти за цією освітньо-професійною програмою мають можливість набути знань і професійних навичок з інших галузей науки, самостійно формуючи індивідуальну освітню траєкторію навчання. *Ключові слова*: кібербезпека, комп'ютерні системи, комп'ютерні мережі, ІТ, програмування, програмне забезпечення, інформаційно-комунікаційні технології, інформаційна безпека, захист інформації.
Особливості програми	Здобувачі вищої освіти за цією освітньо-професійною програмою посилено набувають притаманних професіоналам сфери ІТ софтскілів і навичок міжособистісної взаємодії, віддаленої роботи в команді ІТ-проєкту та критичного оцінювання результатів професійної діяльності, а також вміння створювати інфраструктури відкритих ключів, забезпечувати послугами електронного підпису. Крім цього, підготовка передбачає оволодіння практиками організації безпечної діяльності, зокрема попередження, локалізації й ліквідації наслідків надзвичайних ситуацій природного й техногенного характеру. Ця програма і освітній процес за нею містять всесвітньо визнаний успішний досвід Гарвардського університету з викладання комп'ютерних технологій та програмування, а також використання розробок українських ІТ-компаній в області захисту інформації й банківських технологій.
4. Придатність випускників до працевлаштування та подальшого навчання	

Придатність до працевлаштування	На посади у структурних підрозділах установ/підприємств/організацій, які передбачають наявність вищої освіти зі спеціальності 125 Кібербезпека та захист інформації.
Академічні права випускників	Мають право на здобуття освіти на другому (магістерському) рівні вищої освіти. Здобуття або вдосконалення освіти та професійної підготовки в системі освіти дорослих.
5. Викладання та оцінювання	
Викладання та навчання	В освітньому процесі втілюється: студентоцентрований підхід, нерозривність процесів навчання і наукових досліджень; забезпечення гарантованої якості освіти відповідно до стандартів освіти; врахування світового досвіду, потреб ринку праці, залучення до цього процесу роботодавців, фахівців-практиків, випускників і здобувачів вищої освіти; забезпечення здобувачам вищої освіти сприятливих умов для самостійного навчання та розвитку; інтеграція освітньої та наукової діяльності; забезпечення зворотних зв'язків між учасниками освітнього процесу. Викладання проводиться у вигляді лекцій, лабораторних і практичних занять, консультацій, практик, виконання курсових робіт та курсових проектів, підготовки кваліфікаційної роботи бакалавра, дистанційного навчання в системі MOODLE.
Оцінювання	*Види контролю:* поточний, підсумковий, самоконтроль. *Форми контролю:* усне та письмове опитування, тестовий контроль, захист результатів лабораторних, практичних та індивідуальних робіт, підсумкова атестація – захист кваліфікаційної бакалаврської роботи, Єдиний державний кваліфікаційний іспит.

6. Програмні компетентності	
Інтегральна компетентність	Здатність розв'язувати складні спеціалізовані задачі і практичні завдання у галузі кібербезпеки та захисту інформації.
Загальні компетентності	ЗК 1. Здатність застосовувати знання у практичних ситуаціях. ЗК 2. Знання та розуміння предметної області і розуміння професійної діяльності. ЗК 3. Здатність спілкуватися державною мовою як усно, так і письмово. ЗК 4. Здатність спілкуватися іноземною мовою.

	ЗК 5. Здатність вчитися і оволодівати сучасними знаннями. ЗК 6. Здатність реалізувати свої права і обов'язки як члена суспільства, усвідомлювати цінності громадянського (вільного демократичного) суспільства та необхідність його сталого розвитку, верховенства права, прав і свобод людини і громадянина в Україні. ЗК 7. Здатність ухвалювати рішення й діяти, дотримуючись принципу неприпустимості корупції та будь-яких інших проявів недоброчесності. ЗК 8. Здатність зберігати та примножувати моральні, культурні, наукові цінності і досягнення суспільства на основі розуміння історії та закономірностей розвитку предметної області, її місця у загальній системі знань про природу і суспільство та у розвитку суспільства, техніки і технологій, використовувати різні види та форми рухової активності для активного відпочинку та ведення здорового способу життя.

Спеціальні (фахові, предметні) компетентності	СК 1. Здатність застосовувати законодавчу та нормативно-правову базу, а також державні і міжнародні вимоги, практики і стандарти у професійній діяльності. СК 2. Здатність використовувати інформаційні технології, сучасні методи і моделі кібербезпеки та системи захисту інформації. СК 3. Здатність забезпечувати неперервність бізнес-процесів згідно встановленої політики кібербезпеки та захисту інформації. СК 4. Здатність забезпечувати захист інформації в інформаційних та інформаційно-телекомунікаційних системах згідно встановленої політики кібербезпеки та захисту інформації. СК 5. Здатність відновлювати функціонування інформаційних та інформаційно-телекомунікаційних систем після реалізації загроз , здійснення кібератак, збоїв і відмов різних класів та походження. СК 6. Здатність впроваджувати та забезпечувати функціонування комплексних систем захисту інформації (комплекси нормативно-правових, організаційних та технічних засобів і методів, процедур, практичних прийомів тощо). СК 7. Здатність здійснювати професійну діяльність на основі впровадженої системи управління інформаційною та кібербезпекою. СК 8. Здатність застосовувати методи та засоби криптографічного захисту інформації на об’єктах інформаційної діяльності. СК 9. Здатність застосовувати методи та засоби технічного захисту інформації на об’єктах інформаційної діяльності. СК 10. Здатність виконувати моніторинг інформаційних процесів, аналізувати, виявляти, оцінювати можливі вразливості та загрози інформаційному простору й інформаційним ресурсам згідно з встановленою політикою інформаційної безпеки.
7. Нормативний зміст підготовки здобувачів вищої освіти, сформульований у термінах результатів навчання	
РН 1. Вільно спілкуватися державною мовою усно та письмово при виконанні професійних обов’язків. РН 2. Спілкуватися іноземною мовою з метою забезпечення ефективності професійної комунікації. РН 3. Застосовувати принцип неприпустимості корупції та будь-яких інших проявів недоброчесності у професійній діяльності. РН 4. 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.	

РН 5. 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.
РН 6. Адаптуватися до нових умов і технологій професійної діяльності, прогнозувати кінцевий результат.
РН 7.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.
РН 8. Застосовувати знання й розуміння математики та фізики в професійній діяльності, формалізувати задачі предметної галузі кібербезпеки та захисту інформації, формулювати їх математичну постановку та обирати раціональний метод вирішення.
РН 9. Знати та застосовувати законодавство України та міжнародні вимоги, практики і стандарти з метою здійснення професійної діяльності в галузі кібербезпеки та захисту інформації.
РН 10. Використовувати сучасні інформаційні технології, методи і моделі кібербезпеки та систем захисту інформації для здійснення професійної діяльності.
РН 11. Планувати підготовку та забезпечувати неперервність бізнес-процесів в організаціях згідно зі встановленою політикою кібербезпеки з урахування вимог до захисту інформації.
РН 12. Застосовувати методи та засоби захисту інформації в інформаційних та інформаційно-телекомунікаційних системах відповідно до встановленої політики інформаційної безпеки.
РН 13. 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-телекомунікаційних систем та/або інфраструктури організації в цілому.
РН 14. Вирішувати задачі управління процесами відновлення штатного функціонування інформаційних та інформаційно-телекомунікаційних систем з використанням процедур резервування згідно встановленої політики безпеки і забезпечувати функціонування спеціального програмного забезпечення щодо захисту та відновлення інформації.
РН 15. Збирати, обробляти, зберігати, аналізувати критичні дані для доказу реалізації кіберзагроз, проводити аналіз та дослідження кіберінциденту з метою оперативного відновлення функціонування інформаційної системи.
РН 16. Вирішувати задачі впровадження та супроводу комплексних систем захисту інформації в інформаційних системах.
РН 17. 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 18. Аналізувати, застосовувати методи та засоби криптографічного захисту інформації на об’єктах інформаційної діяльності.

РН 19. Вирішувати задачі щодо організації та контролю стану криптографічного захисту інформації, зокрема відповідно до вимог нормативних документів. 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. РН 21. Виконувати впровадження, підтримку, аналіз ефективності систем виявлення несанкціонованого доступу, дій з інформацією в інформаційній системі, вразливостей, можливих загроз інформаційному простору й інформаційним ресурсам та використовувати комплекси захисту для забезпечення необхідного рівня захищеності інформації в інформаційних системах.

8. Ресурсне забезпечення реалізації програми	
Кадрове забезпечення	Лекції проводяться науково-педагогічними працівниками за основним місцем роботи з науковими ступенями та/або вченими званнями, а також провідними науковцями або спеціалістами-практиками, запрошеними для проведення занять і позааудиторних освітніх заходів. На кафедрі кібербезпеки та програмного забезпечення сформовано групу забезпечення з науково-педагогічних працівників, яка бере участь у забезпеченні якості вищої освіти за освітньо-професійною програмою «Кібербезпека та захист інформації». До проведення занять, керівництва освітньою діяльністю здобувачів вищої освіти залучаються науково-педагогічні працівники, рівень наукової та професійної активності яких засвідчується виконанням Ліцензійних умов провадження освітньої діяльності закладів освіти, затверджених Постановою КМУ від 30 грудня 2015 р. №1187(в редакції від 24 березня 2021 р. № 365). Науково-педагогічні працівники, які виконують всі види навчального навантаження за освітньо-професійною програмою, мають наукові публікації відповідно до профілю дисциплін, які вони викладають, та підвищують свою кваліфікацію відповідно до вимог ст.59 Закону України «Про освіту», ст.60 Закону України «Про вищу освіту» та Порядку підвищення кваліфікації педагогічних і науково-педагогічних працівників, затвердженому постановою Кабінету Міністрів України №800 від 21 серпня 2019 р.
Матеріально-технічне забезпечення	Матеріально-технічне забезпечення освітньої діяльності за освітньо-професійною програмою включає: – забезпеченість приміщеннями для проведення навчальних занять та контрольних заходів, – забезпеченість мультимедійним обладнанням для використання в навчальних аудиторіях, – використання у навчальному процесі спеціалізованих

	комп'ютерних лабораторій кафедри кібербезпеки та програмного забезпечення і інших аудиторій і лабораторій університету зі спеціалізованим устаткуванням та обладнанням. Наявна вся необхідна соціально-побутова інфраструктура, кількість місць у гуртожитках забезпечують 100% потреби.
Інформаційне та навчально-методичне забезпечення	Інформаційне забезпечення освітньої діяльності за освітньо-професійною програмою включає: 1. Наявність офіційного веб-сайту ЦНТУ http://www.kntu.kr.ua , на якому розміщена основна інформація про його діяльність (ліцензії та сертифікати про акредитацію, правила прийому), навчальні та наукові структурні підрозділи та їх склад, нормативні документи, що регламентують освітній процес в університеті, інформація про освітній процес та його організацію. 2. Наявність бібліотеки з трьома читальними залами із загальним фондом близько 500 тис. примірників. 3. Можливість користуватися пошуком у Електронному каталозі бібліотеки у локальній мережі університету. 4. Вільний доступ до інституційного репозитарію ЦНТУ CUNTUR http://dspace.kntu.kr.ua/, у якому містяться наукові праці та навчально-методичні матеріали викладачів і аспірантів університету, повнотекстові публікації наукових збірників видавництва університету, матеріали студентських конференцій та тези доповідей. 5. Доступ до системи дистанційного навчання MOODLE http://moodle.kntu.kr.ua/, яка містить навчально-методичні матеріали з усіх навчальних дисциплін.
9. Академічна мобільність	
Національна кредитна мобільність	На основі двосторонніх договорів між ЦНТУ та закладами вищої освіти України.
Міжнародна кредитна мобільність	На основі двосторонніх договорів між ЦНТУ та вищими навчальними закладами зарубіжних країн-партнерів.
Навчання іноземних здобувачів вищої освіти	Мовою викладання в ЦНТУ є державна мова. Навчання іноземних здобувачів вищої освіти проводиться на загальних умовах, за контрактною формою навчання. В університеті функціонує підготовче відділення, де іноземні громадяни вивчають українську мову.

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

2.1. Перелік компонент освітньо-професійної програми «Кібербезпека та захист інформації»

Код компоненти ОП	Компоненти освітньої програми (навчальні дисципліни, курсові проекти/роботи, практики, державна атестація)	Кількість кредитів	Форма підсумкового контролю
1	2	3	4
1. ОСВІТНІ КОМПОНЕНТИ ЗАГАЛЬНОЇ ПІДГОТОВКИ			
ОКЗ 01	Українська мова (за професійним спрямуванням)	3	залік
ОКЗ 02	Комп'ютерна логіка	3	екзамен
ОКЗ 03	Іноземна мова	5	залік, екзамен
ОКЗ 04	Історія та культура України	6	залік
ОКЗ 05	Вища математика	10	залік, екзамен
ОКЗ 06	Фізика	9	залік, екзамен
ОКЗ 07	Філософія	3	екзамен
ОКЗ 08	Безпека життєдіяльності	2	залік
ОКЗ 09	Основи охорони праці	4	екзамен
ОКЗ 10	Основи здорового способу життя	3	залік
2. ОСВІТНІ КОМПОНЕНТИ СПЕЦІАЛЬНОЇ (ФАХОВОЇ) ПІДГОТОВКИ			
ОКС 01	Soft skills в IT	3	залік
ОКС 02	Основи комп'ютерних технологій	3	екзамен
ОКС 03	Базові методології та технології програмування	7	екзамен, залік
ОКС 04	Комп'ютерні мережі	7	екзамен
ОКС 05	Бази даних	7	залік,екзамен, захист КР
ОКС 06	Вступ до кібербезпеки	7	екзамен, екзамен
ОКС 07	Алгоритми та структури даних	7	залік,екзамен
ОКС 08	Web-програмування	7	залік
ОКС 09	Основи технічного захисту інформації	6	залік
ОКС 10	Інформаційна безпека держави	9	екзамен, екзамен
ОКС 11	Адміністрування інформаційно-телекомунікаційних систем	6	екзамен, екзамен
ОКС 12	Інтернет речей (IoT)	7	залік,екзамен, захист КП
ОКС 13	Криптографічний захист інформації	7	екзамен,залік
ОКС 14	Криптоаналіз	5	залік
ОКС 15	Операційні системи	5	екзамен
ОКС 16	Комплексні системи захисту інформації	6	екзамен

ОКС 17	Організаційне забезпечення захисту інформації	5	екзамен
ОКС 18	Кібербезпека баз даних	6	екзамен
ОКС 19	Захист інформації в інформаційно-телекомунікаційних системах	4	залік
ОКС 20	Проектно-технологічна практика	3	залік
ОКС 21	Переддипломна практика	6	залік
ОКС 22	Підготовка та захист кваліфікаційної роботи	9	захист кваліфікаційної роботи
ОКС 23	Єдиний державний кваліфікаційний іспит	0	ЄДКІ
Загальний обсяг обов'язкових компонент		180	
3. ВИБІРКОВІ ОСВІТНІ КОМПОНЕНТИ			
ВОК 1	Вибіркові освітні компоненти за вибором здобувачів вищої освіти в 2 семестрі	8	заліки
ВОК 2	Вибіркові освітні компоненти за вибором здобувачів вищої освіти в 3 семестрі	10	заліки
ВОК 3	Вибіркові освітні компоненти за вибором здобувачів вищої освіти в 4 семестрі	12	заліки
ВОК 4	Вибіркові освітні компоненти за вибором здобувачів вищої освіти в 5 семестрі	11	заліки
ВОК 5	Вибіркові освітні компоненти за вибором здобувачів вищої освіти в 6 семестрі	4	заліки
ВОК 6	Вибіркові освітні компоненти за вибором здобувачів вищої освіти в 7 семестрі	9	заліки
ВОК 7	Вибіркові освітні компоненти за вибором здобувачів вищої освіти в 8 семестрі	6	заліки
Загальний обсяг вибіркових компонент		60	
Загальний обсяг освітньої програми		**240**	

3. Форми атестації здобувачів вищої освіти

Форми атестації здобувачів вищої освіти	Атестація здійснюється у формі єдиного державного кваліфікаційного іспиту та публічного захисту випускної кваліфікаційної бакалаврської роботи.
Вимоги до єдиного державного кваліфікаційного іспиту	Єдиний державний кваліфікаційний іспит передбачає оцінювання досягнень результатів навчання, визначених Стандартом вищої освіти України першого (бакалаврського) рівня зі спеціальності 125 Кібербезпека та захист інформації.
Вимоги до кваліфікаційної роботи	Випускна кваліфікаційна бакалаврська робота передбачає розв'язок спеціалізованого завдання теоретичного або практичного спрямування в галузі кібербезпеки та захисту інформації. У випускній кваліфікаційній бакалаврській роботі не повинно бути академічного плагіату, фальсифікації та фабрикації. Випускна кваліфікаційна бакалаврська робота розміщується у інституційному репозитарії Центральноукраїнського національного технічного університету http://dspace.kntu.kr.ua/.

4. 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 працівників ЦНТУ та регулярне оприлюднення результатів таких оцінювань на офіційному веб-сайті ЦНТУ;

– забезпечення підвищення кваліфікації педагогічних, наукових і науково-педагогічних працівників;

– забезпечення наявності необхідних ресурсів для організації освітнього процесу, у тому числі самостійної роботи студентів, за 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 ЦНТУ і здобувачів вищої освіти.

В університеті функціонує система забезпечення якості освітньої діяльності та якості вищої освіти (система внутрішнього забезпечення якості) відповідно до Положення про систему забезпечення якості освітньої діяльності та якості вищої освіти у Центральноукраїнському національному технічному університеті.

5. Вимоги професійних стандартів у разі їх наявності

Повна назва та реквізити відповідного Професійного стандарту	1. Адміністратор безпеки мереж і систем, 2139.2 2. Фахівець сфери захисту інформації, 2139.2 3. Фахівець з питань безпеки (інформаційно-комунікаційні технології), 2139.2 4. Конструктор систем кібербезпеки, 2132.2 5. Фахівець з підтримки інфраструктури кіберзахисту, 2139.2 6. Фахівець з реагування на інциденти кібербезпеки, 2139.2 7. Фахівець з криптографічного захисту інформації, 2139.2 8. Фахівець з технічного захисту інформації, 2139.2 9. Фахівець з тестування систем захисту інформації, 2139.2 10. Аудитор інформаційних технологій (з кібербезпеки), 2139.2 11. Фахівець з оцінки заходів захисту інформації (кібербезпеки), 2139.2
Особливості Стандарту вищої освіти, пов'язані з наявністю Професійного стандарту	У стандарті вищої освіти враховані основні цілі професійної діяльності відповідно до наявних професійних стандартів (Додаток 4)

Додаток 1

Зведена таблиця фахових компетентностей та програмних результатів навчання

Фахові компетентності	Результати навчання
СК 1. Здатність застосовувати законодавчу та нормативно-правову базу, а також державні і міжнародні вимоги, практики і стандарти у професійній діяльності.	РН 9. Знати та застосовувати законодавство України та міжнародні вимоги, практики і стандарти з метою здійснення професійної діяльності в галузі кібербезпеки та захисту інформації.
СК 2. Здатність використовувати інформаційні технології, сучасні методи і моделі кібербезпеки та системи захисту інформації.	РН 10. Використовувати сучасні інформаційні технології, методи і моделі кібербезпеки та систем захисту інформації для здійснення професійної діяльності.
СК 3. Здатність забезпечувати неперервність бізнес-процесів згідно встановленої політики кібербезпеки та захисту інформації.	РН 11. Планувати підготовку та забезпечувати неперервність бізнес-процесів в організаціях згідно зі встановленою політикою кібербезпеки з урахування вимог до захисту інформації.
СК 4. Здатність забезпечувати захист інформації в інформаційних та інформаційно-телекомунікаційних системах згідно встановленої політики кібербезпеки та захисту інформації.	РН 12. Застосовувати методи та засоби захисту інформації в інформаційних та інформаційно-телекомунікаційних системах відповідно до встановленої політики інформаційної безпеки. РН 13. 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-телекомунікаційних систем та/або інфраструктури організації в цілому.
СК 5. Здатність відновлювати функціонування інформаційних та інформаційно-телекомунікаційних систем після реалізації загроз , здійснення кібератак, збоїв і відмов різних класів та походження.	РН 14. Вирішувати задачі управління процесами відновлення штатного функціонування інформаційних та інформаційно-телекомунікаційних систем з використанням процедур резервування згідно встановленої політики безпеки і забезпечувати функціонування спеціального програмного забезпечення щодо захисту та відновлення інформації. РН 15. Збирати, обробляти, зберігати, аналізувати критичні дані для доказу реалізації кіберзагроз, проводити аналіз та дослідження кіберінциденту з метою оперативного відновлення функціонування інформаційної системи.
СК 6. Здатність впроваджувати та забезпечувати функціонування комплексних	РН 16. Вирішувати задачі впровадження та супроводу комплексних систем захисту

систем захисту інформації (комплекси нормативно-правових, організаційних та технічних засобів і методів, процедур, практичних прийомів тощо).	інформації в інформаційних системах.
СК 7. Здатність здійснювати професійну діяльність на основі впровадженої системи управління інформаційною та кібербезпекою.	РН 17. 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.
СК 8. Здатність застосовувати методи та засоби криптографічного захисту інформації на об'єктах інформаційної діяльності.	РН 18. Аналізувати, застосовувати методи та засоби криптографічного захисту інформації на об'єктах інформаційної діяльності. РН 19. Вирішувати задачі щодо організації та контролю стану криптографічного захисту інформації, зокрема відповідно до вимог нормативних документів.
СК 9. Здатність застосовувати методи та засоби технічного захисту інформації на об'єктах інформаційної діяльності.	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.
СК 10. Здатність виконувати моніторинг інформаційних процесів, аналізувати, виявляти, оцінювати можливі вразливості та загрози інформаційному простору й інформаційним ресурсам згідно з встановленою політикою інформаційної безпеки.	РН 21. 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.

Додаток 2

Матриця відповідності визначених Стандартом результатів навчання та компетентностей

Результати навчання	Компетентності																				
	Інтегральна компетентність	Загальні компетентності								Спеціальні (фахові) компетентності										
		ЗК1	ЗК2	ЗК3	ЗК4	ЗК5	ЗК6	ЗК7	ЗК8	СК1	СК2	СК3	СК4	СК5	СК6	СК7	СК8	СК9	СК10
РН1	+			+															
РН2	+				+														
РН3	+						+	+											
РН4	+	+	+																
РН5	+	+	+																
РН6	+		+						+										
РН7	+	+							+										
РН8	+					+													
РН9	+						+			+									
РН10	+										+								
РН11	+											+							
РН12	+												+						
РН13	+												+						
РН14	+													+					
РН15	+													+					
РН16	+														+				
РН17	+															+			
РН18	+																+		
РН19	+																+		
РН20	+																	+	
РН21	+																		+

Додаток 3

Матриця відповідності визначених Стандартом компетентностей дескрипторам НРК

Класифікація компетентностей (результатів навчання) за НРК	**Знання** **Зн1** Концептуальні наукові та практичні знання. **Зн2** Критичне осмислення теорій, принципів, методів і понять у сфері професійної діяльності та/або навчання.	**Уміння** **Ум1.** Поглиблені когнітивні та практичні уміння/навички, майстерність та інноваційність на рівні, необхідному для розв'язання складних спеціалізованих задач і практичних проблем у сфері професійної діяльності або навчання.	**Комунікація** **К1.** Донесення до фахівців і нефахівців інформації, ідей, проблем, рішень, власного досвіду та аргументації. **К2.** Збір, інтерпретація та застосування даних. **К3.** Спілкування з професійних питань, у тому числі іноземною мовою, усно та письмово.	**Відповідальність та автономія** **АВ1.** Управління складною технічною або професійною діяльністю чи проектами. **АВ2.** Спроможність нести відповідальність за вироблення та ухвалення рішень у непередбачуваних робочих та/або навчальних контекстах. **АВ3.** Формування суджень, що враховують соціальні, наукові та етичні аспекти. **АВ4.** Організація та керівництво професійним розвитком осіб та груп. **АВ5.** Здатність продовжувати навчання із значним ступенем автономії.
ЗК1	**Зн2**	**Ум1**		
ЗК2	**Зн2**	**Ум1**	**К1**	
ЗК3			**К1, К3**	
ЗК4			**К1, К3**	
ЗК5	**Зн1, Зн2**	**Ум1**	**К2**	**АВ3**
ЗК6	**Зн1**		**К1**	**АВ2, АВ3, АВ4**
ЗК7			**К1**	**АВ2**
ЗК8	**Зн2**		**К2**	**АВ3**
СК1	**Зн2**	**Ум1**	**К2**	
СК2	**Зн1, Зн2**	**Ум1**	**К2**	
СК3		**Ум1**		**АВ1**
СК4		**Ум1**		**АВ1**
СК5		**Ум1**	**К2**	**АВ1, АВ2**
СК6		**Ум1**	**К1**	**АВ1**
СК7		**Ум1**	**К1**	**АВ1**
СК8	**Зн2**	**Ум1**		
СК9	**Зн2**	**Ум1**		
СК10		**Ум1**	**К2**	**АВ2**

Додаток 4

Перелік професійних стандартів

№	Назва професійного стандартута код згідно з Національним класифікатором України ДК 003:2010 «Класифікатор професій»	Мета діяльності за професією
	Адміністратор безпеки мереж і систем, 2139.2	Встановлення та підтримка мереж і систем, їх конкретних компонентів (встановлення, конфігурування і оновлення апаратного та програмного забезпечення, обслуговування баз даних, створення та управління обліковими записами користувачів, нагляд або виконання резервного копіювання та відновлення, впровадження оперативного та технічного контролів безпеки; дотримання політик та процедур безпеки організації тощо). Адміністрування системи управління даними, що дозволяють безпечно зберігати, обробляти, запитувати, захищати та використовувати дані.
	Фахівець сфери захисту інформації, 2139.2	Забезпечення захищеності (конфіденційності, цілісності, доступності) інформації, що обробляється (передається) в інформаційних (автоматизованих), електронних комунікаційних та інформаційно-комунікаційних системах від несанкціонованих дій з інформацією (включаючи комп'ютерні віруси), від витоку технічними каналами та від спеціальних впливів на засоби обробки інформації, а також інформації, що озвучується на об'єктах інформаційної діяльності, – від витоку технічними каналами.
	Фахівець з питань безпеки (інформаційно-комунікаційні технології), 2139.2	Організація та забезпечення кібербезпеки інформаційних систем та інформаційно-комунікаційних технологій; управління наслідками реалізації загроз інформаційної безпеки в межах організації, в тому числі управління спеціальними програмами (проектами) інших сфер відповідальності; формування стратегічного розвитку організації, персоналу, інфраструктури, вимог до безпеки, а також розробка та впровадження політики та стратегії інформаційної безпеки інституції; планування заходів безпеки інформації та кіберзахисту на випадок надзвичайних ситуацій або при реалізації інцидентів; обізнаність про безпеку інформаційних ресурсів організації або анклаву, установ та підприємств різних форм власності.
	Конструктор систем кібербезпеки, 2132.2	Забезпечення ситуації, коли вимоги безпеки зацікавлених сторін, необхідні для захисту місії організації та бізнес-процесів, належним чином ураховуються в усіх аспектах архітектури систем кібербезпеки організації (установи, підприємства), включаючи еталонні моделі, архітектури сегментів та рішень, а також системи для підтримки цих місій та бізнес-процесів.
	Фахівець з підтримки інфраструктури кіберзахисту, 2139.2	Тестування, впровадження, розгортання, підтримка та адміністрування інфраструктурного обладнання та програмного забезпечення кіберзахисту
	Фахівець з реагування на інциденти кібербезпеки, 2139.2	Аналіз, оцінка інцидентів кібербезпеки в рамках мережевого середовища та реагування на них. Усунення інцидентів кібербезпеки та пом'якшення їх наслідків. Відстеження, оцінка стану кібербезпеки систем та своєчасне повідомлення про інциденти кібербезпеки. Відновлення функціональності систем і процесів до робочого стану. Дослідження та аналіз заходів реагування, оцінка ефективності та покращення існуючих практик. Накопичення та проведення аналізу даних про кіберзагрози.
	Фахівець з криптографічного захисту інформації, 2139.2	Забезпечення криптографічного захисту інформації в інформаційних системах\мережах (або автоматизованих системах, інформаційно-комунікаційних системах, системах електронних комунікацій) на основі перетворень інформації з використанням спеціальних даних (ключових даних) для приховування (або відновлення) змісту інформації, підтвердження її справжності, цілісності, авторства тощо.

		Здійснення оцінки рівня безпеки та контролю стану криптографічного захисту інформації в інформаційних системах\мережах (або автоматизованих системах, інформаційно-комунікаційних системах, системах електронних комунікацій). Дослідження рівня захисту програмних засобів і систем що реалізують криптографічні функції. Супроводження робіт зі створення, впровадження та забезпечення функціонування підсистем криптографічного захисту інформації на всіх етапах життєвого циклу інформаційних систем\мереж в організаціях, підприємствах або установах різних форм власності.
	Фахівець з технічного захисту інформації, 2139.2	Забезпечення інженерно-технічними та організаційно-технічними заходами та засобами порядку доступу, конфіденційності, цілісності й доступності (унеможливлення блокування) інформації, яка становить державну та іншу передбачену законом таємницю, а також цілісності та доступності відкритої інформації, важливої для особи, суспільства і держави. Захист інформації та безпосередньо її властивостей, спрямований на забезпечення за допомогою нормативно-правових, організаційних та інженерно-технічних заходів та/або програмно-технічних засобів унеможливлення витоку, знищення та блокування інформації, порушення цілісності та режиму доступу до інформації. Супроводження робіт зі створення, впровадження та забезпечення функціонування систем технічного захисту інформації на етапах життєвого циклу інформаційних, електронних комунікаційних та інформаційно-комунікаційних систем (далі – автоматизовані системи).
	Фахівець з тестування систем захисту інформації, 2139.2	Планування, підготовка та проведення тестування або тестування на проникнення до інформаційних систем/мереж (або автоматизованих систем, інформаційно-комунікаційних систем, систем електронних комунікацій), а також їх інформаційних ресурсів (активів або компонентів) в організаціях, підприємствах або установах різних форм власності. Проведення оцінки стану захищеності інформаційних систем/мереж та стану кібербезпеки на відповідність стандартам, специфікаціям, нормам, вимогам та заявленим технічним характеристикам. Проведення аналізу й звітування щодо результатів тестування, розроблення рекомендацій з виявлення та оцінки відхилень у функціонуванні операційних процесів, а також звітування щодо визначених вразливостей і загроз інформаційній системі та її ресурсам.
	Аудитор інформаційних технологій (з кібербезпеки), 2139.2	Проведення внутрішнього та зовнішнього аудиту об'єктів інформатизації для надання об'єктивних якісних і кількісних оцінок про поточний стан інформаційної безпеки організації у відповідності з визначеними в нормативно-правовій, нормативно-технічний базі критеріями та показниками безпеки. Формування рекомендацій, на основі наданих оцінок, для посилення системи менеджменту інформаційної безпеки, підтримки планів стійкості, відновлення штатного функціонування інфраструктури організації після інцидентів та нештатних ситуацій.
	Фахівець з оцінки заходів захисту інформації (кібербезпеки), 2139.2	Здійснення незалежної комплексної оцінки управлінського, операційного та технічного контролю безпеки, а також покращення контролю, що використовується в системі інформаційних технологій для визначення загальної ефективності заходів контролю. Розроблення, забезпечення та контроль виконання заходів для усунення причин і умов, що можуть призвести до витоку інформації. Здійснення оцінки ступеню захищеності інформаційних систем, а також системного контролю реалізації задекларованих послуг безпеки. Підвищення рівня безпеки інформаційних систем на основі аналізу потенційних недоліків та вразливих точок, а також забезпечення економічної ефективності розгорнутих заходів захисту.
	Кібероператор, 4113	Здійснення збору та оброблення чутливої інформації (даних) та/або встановлення і аналіз геолокації інформаційних систем/мереж для експлуатації, пошуку та/або відстеження цілей (інформаційних потоків або об'єктів), що являють інтерес для інституції, організації, чи установи різних форм власності в рамках чинного законодавства. Виконання мережевої навігації, збирання даних відповідного спрямування з відкритих джерел за допомогою різних онлайн-інструментів, виконання тактичного криміналістичного аналізу, а також у випадку поставленої задачі, в рамках чинного законодавства, прийняття участі у виконанні операцій в інформаційній системі/мережі.