

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
Центральноукраїнський національний технічний університет

ОСВІТНЬО-ПРОФЕСІЙНА ПРОГРАМА
«Кібербезпека та захист інформації»
першого (бакалаврського) рівня вищої освіти
за спеціальністю 125 «Кібербезпека та захист інформації»
галузі знань 12 «Інформаційні технології»
Кваліфікація: бакалавр з кібербезпеки та захисту інформації

Зміни затверджено Вченою радою ЦНТУ

Протокол № 10 від «26» 06 2025 р.

Голова Вченої ради

 **Володимир КРОПІВНИЙ**

Освітня програма вводиться в дію з 01.09 2024 р.

Наказ № 130-05 від «27» 06 2024 р.

Ректор

 **Володимир КРОПІВНИЙ**

Кропивницький – 2024

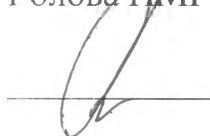
ЛИСТ ПОГОДЖЕННЯ
освітньо-професійної програми
«Кібербезпека та захист інформації»

Рівень вищої освіти **Перший (бакалаврський)**
ГАЛУЗЬ ЗНАНЬ **12 «Інформаційні технології»**
СПЕЦІАЛЬНІСТЬ **125 «Кібербезпека та захист інформації»**
КВАЛІФІКАЦІЯ **бакалавр з кібербезпеки та захисту інформації**

РЕКОМЕНДОВАНО

Науково-методичною радою
університету
Протокол № 4
від «25» 06 2025 р.

Голова НМР університету

 Андрій КИРИЧЕНКО

РЕКОМЕНДОВАНО

Науково-методичною радою
механіко-технологічного факультету
Протокол № 2
від «16» 06 2025 р.

Голова НМР механіко-технологічного
факультету

 Віталій МАЖАРА

СХВАЛЕНО

Науково-методичною комісією
спеціальності F5 «Кібербезпека та
захист інформації»

Протокол № 1
від «27» 05 2025 р.

Голова НМК спеціальності

 Олексій СМІРНОВ

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».

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 №1074 (у редакції наказу Міністерства освіти і науки України від 29.10.2024 №1547), та у відповідності з Порядком здійснення навчання населення діям у надзвичайних ситуаціях, затвердженим постановою Кабінету Міністрів України № 444 від 26.06.2013 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. Дресєв 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., 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 №1074 (у редакції наказу Міністерства освіти і науки України від 29.10.2024 №1547), а також Положенням про освітні програми та навчальні плани в Центральнотехнічному національному технічному університеті.

Програма схвалена Науково-методичною радою та затверджена Вченою радою Центральнотехнічного 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. Термін навчання 3 академічні роки 10 місяців для денної та заочної форми здобуття вищої освіти
Форма здобуття вищої освіти:	денна, заочна
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 ENEA – 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	
Підготовка фахівців з кібербезпеки та захисту інформації, які мають ґрунтовний хард- і софтскіловий потенціал ІТ-спеціаліста, зокрема у сфері штучного інтелекту, QA та QC програмного забезпечення, інтернету речей, та здатність професійно самореалізуватися в галузі інформаційних технологій, відповідно до місії Центральноукраїнського національного технічного університету.	
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, набуття притаманних професіоналу-практику сфери ІТ й фахівцю із захисту даних (Data Protection Officer) хард- та софтскілів, серед яких технології штучного інтелекту, QA та QC, інтернету речей (IoT). 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, методи штучного інтелекту. Інструменти та обладнання: засоби, пристрої, мережеве 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 прикладна орієнтація, спрямована на розвиток ключових soft skills, необхідних для успішної реалізації ІТ-проектів, а також підготовку фахівців, здатних розв'язувати прикладні задачі сучасної кібербезпеки та захисту інформації із використанням технологій штучного інтелекту, інтернету речей (IoT).
Фокус програми	Програма спрямована на здобуття кваліфікації для виконання професійної діяльності у сфері ІТ, розв'язання задач забезпечення кібербезпеки та захисту інформації, 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, із використанням інструментів штучного інтелекту, а також забезпечення 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. <i>Ключові слова:</i> кібербезпека, комп'ютерні системи, комп'ютерні мережі, ІТ, програмування, програмне забезпечення, інформаційно-комунікаційні технології, інформаційна безпека, захист інформації, штучний інтелект, QA та QC, інтернет речей (IoT).
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-проекту та критичного оцінювання результатів професійної діяльності, а також вміння створювати інфраструктури відкритих ключів, забезпечувати послугами електронного підпису, вміння забезпечувати контроль якості програмних засобів, вивчення та практичне застосування методів і алгоритмів штучного інтелекту для розв'язання складних задач. 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: студентоцентризований 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	<i>Види контролю:</i> поточний, підсумковий, самоконтроль. <i>Форми контролю:</i> 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. <i>ЗК 9. Знання законодавчих, нормативно-правових, інженерно-технічних та санітарно-гігієнічних основ забезпечення безпечної діяльності</i> <i>ЗК 10. Здатність застосовувати технології штучного інтелекту в практичних ситуаціях.</i>
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. <i>СК 11. Здатність ініціювати, планувати та реалізовувати процеси забезпечення якості програмних засобів на різних рівнях тестування програмного забезпечення.</i> <i>СК 12. Здатність створювати системи кібербезпеки та захисту інформації з використанням технологій штучного інтелекту.</i> <i>СК 13. Здатність розробляти пристрої інтернету речей для забезпечення задач кібербезпеки та захисту інформації.</i> <i>СК 14. Здатність використовувати сучасні методи і мови програмування для розроблення алгоритмічного та програмного забезпечення систем кібербезпеки та захисту інформації.</i>
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.

- РН 22. Використовувати розподілені системи керування версіями файлів та спільної роботи під час реалізації проєктів у колективі (команді ІТ-проєкту).*
- РН 23. Ідентифікувати, аналізувати та досліджувати небезпечні чинники природнього та техногенного середовищ. Вміти обґрунтовано вибирати пристрої, системи і методи відповідно до майбутнього профілю роботи з попередження виникнення надзвичайних ситуацій, локалізації та ліквідації їхніх наслідків.*
- РН 24. Тестувати програмне забезпечення на різних стадіях реалізації програмних систем.*
- РН 25. Застосовувати програмні засоби штучного інтелекту для вирішення проблем у професійній, особистісній, побутовій, соціальній, громадській, освітній та ін. діяльності.*
- РН 26. Створювати та використовувати моделі штучного інтелекту для вирішення задач кібербезпеки та захисту інформації з використанням базових алгоритмів, програмних інструментів та з урахуванням обмежень обчислювальних ресурсів.*
- РН 27. Проєктувати та реалізовувати повний цикл розробки пристроїв інтернету речей(IoT) для забезпечення задач кібербезпеки та захисту інформації, включаючи вибір апаратних компонентів, написання програмного забезпечення, створення власних протоколів передачі даних та налаштування захищених мережесевих з'єднань.*
- РН 28. Розробляти алгоритмічне та програмне забезпечення систем кібербезпеки та захисту інформації.*

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 №1187(в редакції від 24 березня 2021 № 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
-----------------------------	---

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.

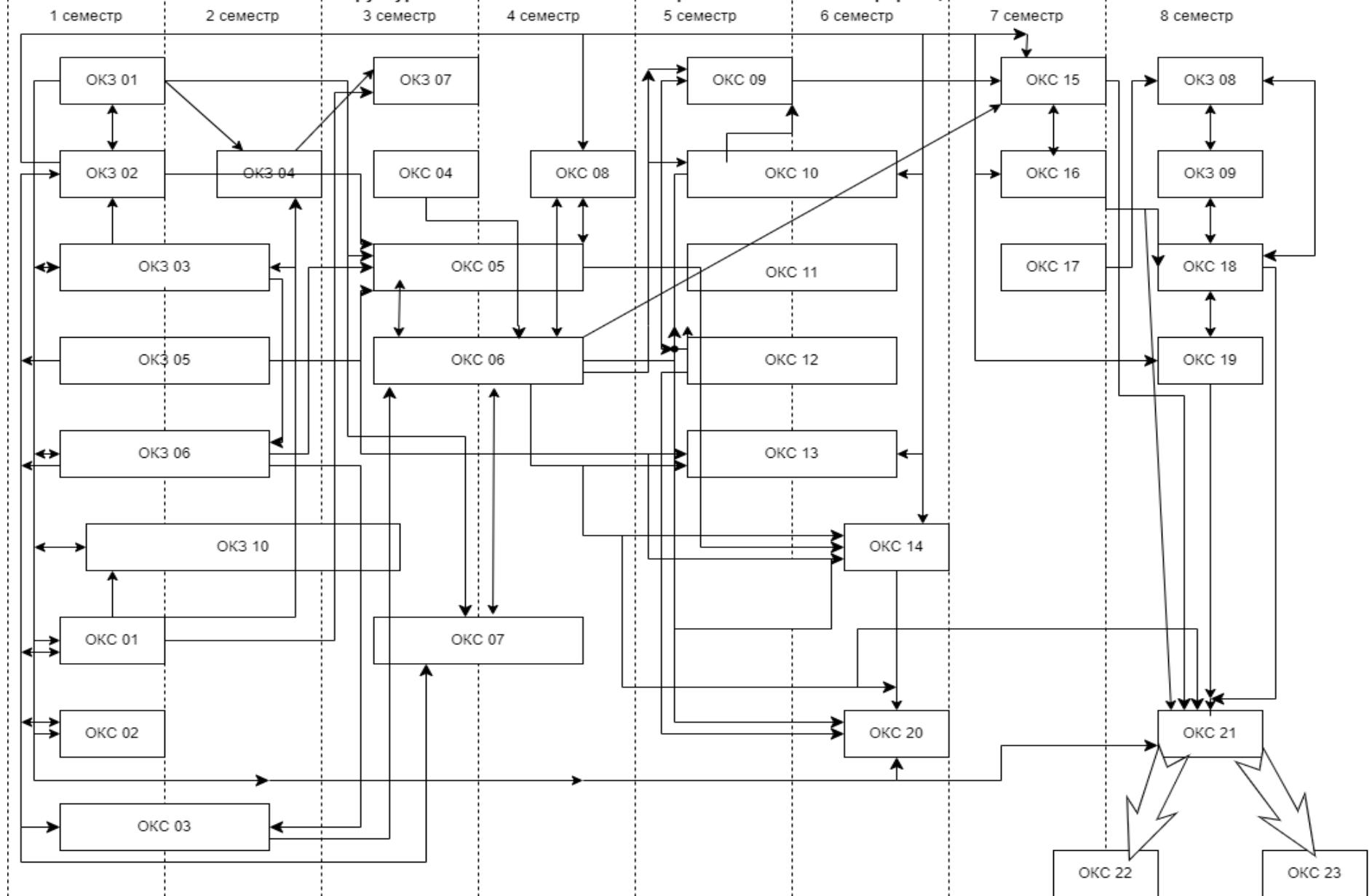
2. Перелік компонент освітньо-професійної програми та їх логічна послідовність

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 ІТ	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 (з обов'язковим включенням компоненти Теоретична підготовка БЗВП*** (3 кредита ЄКТС) в 3-ому семестрі до індивідуального плану здобувачів вищої освіти чоловічої статі (жіночої статі - добровільно)	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 вибірових компонент		60	
Загальний обсяг освітньої програми		240	

2.2 Структурно-логічна схема ОПП "Кібербезпека та захист інформації"



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 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 Центральнотехнічному 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)

**6. Матриця відповідності програмних компетентностей компонентам освітньо-професійної програми
«Кібербезпека та захист інформації»**

ОК	Інт. комп.	Загальні компетентності										Спеціальні (фахові, предметні) компетентності													
		ЗК 1	ЗК 2	ЗК 3	ЗК 4	ЗК 5	ЗК 6	ЗК 7	ЗК 8	ЗК 9	ЗК 10	СК 1	СК 2	СК 3	СК 4	СК 5	СК 6	СК 7	СК 8	СК 9	СК 10	СК 11	СК 12	СК 13	СК 14
ОКЗ 01	+			+																					
ОКЗ 02	+					+																			
ОКЗ 03	+				+																				
ОКЗ 04	+						+		+																
ОКЗ 05	+	+				+																			
ОКЗ 06	+	+				+																			
ОКЗ 07	+						+		+																
ОКЗ 08	+	+								+															
ОКЗ 09	+	+	+							+															
ОКЗ 10	+								+																
ОКС 01	+		+					+					+												
ОКС 02	+	+	+										+										+		+
ОКС 03	+	+									+											+			+
ОКС 04	+	+																		+					
ОКС 05	+											+	+												
ОКС 06	+	+										+	+	+	+	+		+	+	+					
ОКС 07	+																								+
ОКС 08	+												+									+			
ОКС 09	+	+	+															+							
ОКС 10	+	+					+					+													
ОКС 11	+														+	+					+				
ОКС 12	+	+																	+				+	+	
ОКС 13	+	+										+						+							
ОКС 14	+					+														+					
ОКС 15	+												+		+										
ОКС 16	+														+		+			+					
ОКС 17	+											+		+			+	+							
ОКС 18	+	+											+	+											
ОКС 19	+		+										+	+	+	+									
ОКС 20	+	+	+									+	+		+	+		+	+		+	+	+	+	+
ОКС 21	+	+	+									+	+		+	+		+	+		+	+	+	+	+
ОКС 22	+	+	+									+	+		+	+		+	+		+	+	+	+	+

7. Матриця відповідності ПРН компонентам освітньо-професійної програми «Кібербезпека та захист інформації»

ОК	РН 1	РН 2	РН 3	РН 4	РН 5	РН 6	РН 7	РН 8	РН 9	РН10	РН11	РН12	РН13	РН14	РН15	РН16	РН17	РН18	РН19	РН20	РН21	РН22	РН23	РН24	РН25	РН26	РН27	РН28
ОКЗ 01	+																											
ОКЗ 02							+	+																				
ОКЗ 03		+																										
ОКЗ 04						+																						
ОКЗ 05								+																				
ОКЗ 06								+																				
ОКЗ 07						+																						
ОКЗ 08						+																	+					
ОКЗ 09						+																	+					
ОКЗ 10						+																						
ОКС 01			+							+																		
ОКС 02				+	+																					+		+
ОКС 03				+																		+		+	+			+
ОКС 04																					+							
ОКС 05									+	+									+	+	+	+						
ОКС 06									+	+	+	+	+	+	+			+	+	+	+							
ОКС 07																												+
ОКС 08										+						+												
ОКС 09								+	+											+								
ОКС 10								+																				
ОКС 11				+								+		+	+													
ОКС 12				+																+							+	+
ОКС 13				+			+			+								+	+									
ОКС 14						+												+										
ОКС 15				+						+		+																
ОКС 16												+				+					+							
ОКС 17								+		+						+	+											
ОКС 18				+		+				+	+																	
ОКС 19				+						+	+	+	+	+														
ОКС 20				+	+		+	+	+	+		+	+	+	+			+	+					+	+	+	+	+
ОКС 21				+	+		+	+	+	+		+	+	+	+			+	+					+	+	+	+	+
ОКС 22				+	+		+	+	+	+		+	+	+	+			+	+					+	+	+	+	+