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

Затверджено Вченою радою ЦНТУ

Протокол № 10 **від «**26**»** 06 **2024 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**

СХВАЛЕНО
Науково-методичною комісією
спеціальності 125 «Кібербезпека та
захист інформації»
Протокол № 5
від «18» 06 2024 р.

Голова НМК спеціальності

_____ Олексій СМІРНОВ

РЕКОМЕНДОВАНО
Науково-методичною радою
механіко-технологічного факультету
Протокол № 2
від «20» 06 2024 р.

Голова НМР механіко-технологічного
факультету

_____ Віталій МАЖАРА

РЕКОМЕНДОВАНО
Науково-методичною радою
університету
Протокол № 4
від «24» 06 2024 р.

Голова НМР університету

_____ Андрій КИРИЧЕНКО

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» 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 зі змінами, внесеними відповідно до наказу Міністерства освіти і науки України від 13.01.2022 № 26, зі змінами, внесеними відповідно до наказу Міністерства освіти і науки України від 13.06.2024 № 842, 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» галузі знань 12 «Інформаційні технології» для першого (бакалаврського) рівня вищої освіти від 04.10.2018 р. №1074 зі змінами, внесеними відповідно до наказу Міністерства освіти і науки України від 13.01.2022 № 26, зі змінами, внесеними відповідно до наказу Міністерства освіти і науки України від 13.06.2024 № 842, 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 освітньої програми бакалавра: – на базі повної загальної середньої освіти – 240 кредитів ЄКТС; – на базі ступеня «молодший бакалавр» (освітньо-кваліфікаційного рівня «молодший спеціаліст») ЦНТУ визнає та перезараховує не більше ніж 120 кредитів ЄКТС, отриманих в межах попередньої освітньої програми підготовки молодшого бакалавра (молодшого спеціаліста); – на основі ступеня «фаховий молодший бакалавр» ЦНТУ визнає та перезараховує не більше ніж 60 кредитів ЄКТС, отриманих за попередньою освітньою програмою фахової передвищої освіти.
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	Повна загальна середня освіта. Прийом на основі ступенів «молодший бакалавр», «фаховий молодший бакалавр» або освітньо-кваліфікаційного рівня «молодший спеціаліст» здійснюється за результатами зовнішнього незалежного оцінювання 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 IT-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 професійної діяльності випускників: – об'єкти інформатизації, включаючи комп'ютерні, автоматизовані, телекомунікаційні, інформаційні, інформаційно-аналітичні, інформаційно-телекомунікаційні системи, інформаційні ресурси і технології; – технології забезпечення безпеки інформації; – процеси управління інформаційною та/або кібербезпекою об’єктів, що підлягають захисту. Цілі навчання: підготовка фахівців, здатних використовувати і впроваджувати технології інформаційної та/або кібербезпеки, 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 IT і спеціалісту із захисту даних (Data Protection Officer). Теоретичний зміст предметної області Знання: – законодавчої, нормативно-правової бази України та вимог відповідних міжнародних стандартів і практик щодо здійснення професійної діяльності; – принципів супроводу систем та комплексів інформаційної та/або кібербезпеки; – теорії, моделей та принципів управління доступом до інформаційних ресурсів; – теорії систем управління інформаційною та/або кібербезпекою; – методів та засобів виявлення, управління та ідентифікації ризиків; – методів та засобів оцінювання та забезпечення необхідного рівня захищеності інформації;

	– методів та засобів технічного та криптографічного захисту інформації; – сучасних інформаційно-комунікаційних технологій; – сучасного програмно-апаратного забезпечення інформаційно-комунікаційних технологій; – автоматизованих систем проектування. Методи, методики та технології: Методи, методики, інформаційно-комунікаційні технології та інші технології забезпечення інформаційної та/ або кібербезпеки. Інструменти та обладнання: – системи розробки, забезпечення, моніторингу та контролю процесів інформаційної та/ або кібербезпеки; – сучасне програмно-апаратне забезпечення інформаційно-комунікаційних технологій.
Орієнтація освітньої програми	Освітньо-професійна програма.
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	Випускники можуть працювати в підрозділах великих підприємств та установ, забезпечуючи захист комп'ютерних систем та мереж, у відділах спецслужб та правозахисних органів для захисту кіберпростору та інформаційних даних, здійснювати забезпечення захищеної комп'ютеризованої діяльності банків та фінансових установ, виконувати функції розробника систем захисту інформації Випускники можуть займати первинні посади (за ДК 003:2010): − 2131.2 Адміністратор веб-ресурсів − 2131.2 Інженер з контролю якості програмного продукту − 2132.2 Розробник систем захисту інформації − 2139.2 Адміністратор безпеки мереж і систем − 2139.2 Аналітик загроз безпеки − 2139.2 Аналітик систем захисту інформації − 2139.2 Аналітик з оцінки вразливостей − 2139.2 Аналітик з безпеки інформаційно-телекомунікаційних систем − 2139.2 Дізнавач (сфера кібербезпеки та захисту інформації) − 2139.2 Експерт з цифрової криміналістики (сфера кібербезпеки та захисту інформації) − 2139.2 Експерт-криміналіст судової експертизи (сфера кібербезпеки та захисту інформації) − 2139.2 Слідчий з кіберзлочинів − 2139.2 Фахівець з криптографічного захисту інформації − 2139.2 Фахівець з питань безпеки (інформаційно-комунікаційні технології) − 2139.2 Фахівець з підтримки інфраструктури кіберзахисту − 2139.2 Фахівець з реагування на інциденти кібербезпеки − 2139.2 Фахівець з тестування систем безпеки та захисту інформації − 2139.2 Фахівець з технічного захисту інформації

	− 2139.2 Фахівець сфери захисту інформації − 2139.2 Фахівець з кібердосліджень та розробок систем безпеки − 2139.2 Фахівець з оцінки заходів захисту інформації (кібербезпеки) − 2139.2 Фахівець з питань безпеки (інформаційно-комунікаційні технології) − 2139.2 Фахівець з підтримки інфраструктури кіберзахисту − 2139.2 Фахівець з планування політики та стратегії кібербезпеки − 2139.2 Фахівець з реагування на інциденти кібербезпеки − 2139.2 Фахівець з тестування систем безпеки та захисту інформації − 2139.2 Фахівець з технічного захисту інформації − 2139.2 Фахівець з безпеки електронних комунікацій − 2149.2 Професіонал із організації захисту інформації з обмеженим доступом − 2359.2 Інструктор-методист з інформаційної безпеки та кібербезпеки − 3121 Адміністратор веб-сайту − 3439 Фахівець із організації інформаційної безпеки − 3439 Фахівець із організації захисту інформації з обмеженим доступом − 3439 Фахівець із організації інформаційної безпеки. International Standard Classification of Occupations 2008 (ISCO-08): − 2529 Security specialist (ICT).
Академічні права випускників	Можливість продовжити навчання за освітньою програмою ступеня магістра. Набуття додаткових кваліфікацій в системі післядипломної освіти.
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 та практичні проблеми у галузі забезпечення інформаційної безпеки і\або кібербезпеки, що характеризується комплексністю та неповною визначеністю умов.
Загальні компетентності	КЗ 1. Здатність застосовувати знання у практичних ситуаціях. КЗ 2. Знання та розуміння предметної області та розуміння професії. КЗ 3. Здатність професійно спілкуватися державною та іноземною мовами як усно, так і письмово. КЗ 4. Вміння виявляти, ставити та вирішувати проблеми за професійним спрямуванням. КЗ 5. Здатність до пошуку, оброблення та аналізу інформації. КЗ 6. Здатність реалізувати свої права і обов’язки як члена суспільства, усвідомлювати цінності громадянського (вільного демократичного) суспільства та необхідність його сталого розвитку, верховенства права, прав і свобод людини і громадянина в Україні КЗ 7. Здатність зберігати та примножувати моральні, культурні, наукові цінності і досягнення суспільства на основі розуміння історії та закономірностей розвитку предметної області, її місця у загальній системі знань про природу і суспільство та у розвитку суспільства, техніки і технологій, використовувати різні види та форми рухової активності для активного відпочинку та ведення здорового способу життя. КЗ 8. Здатність ухвалювати рішення та діяти, дотримуючись принципу неприпустимості корупції та будь-яких інших проявів недоброчесності.

Фахові компетентності	КФ 1. Здатність застосовувати законодавчу та нормативно-правову базу, а також державні та міжнародні вимоги, практики і стандарти з метою здійснення професійної діяльності в галузі інформаційної та/або кібербезпеки. КФ 2. Здатність до використання інформаційно-комунікаційних технологій, сучасних методів і моделей інформаційної безпеки та/або кібербезпеки. КФ 3. Здатність до використання програмних та програмно-апаратних комплексів засобів захисту інформації в інформаційно-телекомунікаційних (автоматизованих) системах. КФ 4. Здатність забезпечувати неперервність бізнесу згідно встановленої політики інформаційної та/або кібербезпеки. КФ 5. Здатність забезпечувати захист інформації, що обробляється в інформаційно-телекомунікаційних (автоматизованих) системах з метою реалізації встановленої політики інформаційної та/або кібербезпеки. КФ 6. Здатність відновлювати штатне функціонування інформаційних, інформаційно-телекомунікаційних (автоматизованих) систем після реалізації загроз , здійснення кібератак, збоїв та відмов різних класів та походження. КФ 7. Здатність впроваджувати та забезпечувати функціонування комплексних систем захисту інформації (комплекси нормативно-правових, організаційних та технічних засобів і методів, процедур, практичних прийомів та ін.) КФ 8. Здатність здійснювати процедури управління інцидентами, проводити розслідування, надавати їм оцінку. КФ 9. Здатність здійснювати професійну діяльність на основі впровадженої системи управління інформаційною та/або кібербезпекою. КФ 10. Здатність застосовувати методи та засоби криптографічного та технічного захисту інформації на об’єктах інформаційної діяльності. КФ 11. Здатність виконувати моніторинг процесів функціонування інформаційних, інформаційно-телекомунікаційних (автоматизованих) систем згідно встановленої політики інформаційної та/або кібербезпеки. КФ 12. Здатність аналізувати, виявляти та оцінювати можливі загрози, уразливості та дестабілізуючі чинники інформаційному простору та інформаційним ресурсам згідно з встановленою політикою інформаційної та/або кібербезпеки.
7. Програмні результати навчання	
РН 1. Застосовувати знання державної та іноземних мов з метою забезпечення ефективності професійної комунікації.	

РН 2. Організовувати власну професійну діяльність, обирати оптимальні методи та способи розв’язування складних спеціалізованих задач та практичних проблем у професійній діяльності, оцінювати їхню ефективність.
РН 3. Використовувати результати самостійного пошуку, аналізу та синтезу інформації з різних джерел для ефективного рішення спеціалізованих задач професійної діяльності.
РН 4. Аналізувати, аргументувати, приймати рішення при розв’язанні складних спеціалізованих задач та практичних проблем у професійній діяльності, які характеризуються комплексністю та неповною визначеністю умов, відповідати за прийняті рішення.
РН 5. Адаптуватися в умовах частої зміни технологій професійної діяльності, прогнозувати кінцевий результат.
РН 6. Критично осмислювати основні теорії, принципи, методи і поняття у навчанні та професійній діяльності.
РН 7. Діяти на основі законодавчої та нормативно-правової бази України та вимог відповідних стандартів, у тому числі міжнародних в галузі інформаційної та /або кібербезпеки.
РН 8. Готувати пропозиції до нормативних актів щодо забезпечення інформаційної та /або кібербезпеки.
РН 9. Впроваджувати процеси, що базуються на національних та міжнародних стандартах, виявлення, ідентифікації, аналізу та реагування на інциденти інформаційної та/або кібербезпеки.
РН 10. Виконувати аналіз та декомпозицію інформаційно-телекомунікаційних систем.
РН 11. Виконувати аналіз зв’язків між інформаційними процесами на віддалених обчислювальних системах.
РН 12. Розробляти моделі загроз та порушника.
РН 13. Аналізувати проекти інформаційно-телекомунікаційних систем базуючись на стандартизованих технологіях та протоколах передачі даних.
РН 14. Вирішувати завдання захисту програм та інформації, що обробляється в інформаційно-телекомунікаційних системах програмно-апаратними засобами та давати оцінку результативності якості прийнятих рішень.
РН 15. Використовувати сучасне програмно-апаратне забезпечення інформаційно-комунікаційних технологій.
РН 16. Реалізовувати комплексні системи захисту інформації в автоматизованих системах (АС) організації (підприємства) відповідно до вимог нормативно-правових документів.
РН 17. Забезпечувати процеси захисту та функціонування інформаційно-телекомунікаційних (автоматизованих) систем на основі практик, навичок та знань, щодо структурних (структурно-логічних) схем, топології мережі, сучасних архітектур та моделей захисту електронних інформаційних ресурсів з відображенням взаємозв’язків та інформаційних потоків, процесів для внутрішніх і віддалених компонент.
РН 18. Використовувати програмні та програмно-апаратні комплекси захисту інформаційних ресурсів.
РН 19. Застосовувати теорії та методи захисту для забезпечення безпеки інформації в інформаційно-телекомунікаційних системах.

РН 20. Забезпечувати функціонування спеціального програмного забезпечення, щодо захисту інформації від руйнуючих програмних впливів, руйнуючих кодів в інформаційно-телекомунікаційних системах.
РН 21. Вирішувати задачі забезпечення та супроводу (в.т. числі: огляд, тестування, підзвітність) системи управління доступом згідно встановленої політики безпеки в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах.
РН 22. Вирішувати задачі управління процедурами ідентифікації, автентифікації, авторизації процесів і користувачів в інформаційно-телекомунікаційних системах згідно встановленої політики інформаційної і\або кібербезпеки.
РН 23. Реалізовувати заходи з протидії отриманню несанкціонованого доступу до інформаційних ресурсів і процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах.
РН 24. Вирішувати задачі управління доступом до інформаційних ресурсів та процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах на основі моделей управління доступом (мандатних, дискреційних, рольових).
РН 25. Забезпечувати введення підзвітності системи управління доступом до електронних інформаційних ресурсів і процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах з використанням журналів реєстрації подій, їх аналізу та встановлених процедур захисту.
РН 26. Впроваджувати заходи та забезпечувати реалізацію процесів попередження отриманню несанкціонованого доступу і захисту інформаційних, інформаційно-телекомунікаційних (автоматизованих) систем на основі еталонної моделі взаємодії відкритих систем.
РН 27. Вирішувати задачі захисту потоків даних в інформаційних, інформаційно-телекомунікаційних (автоматизованих) системах.
РН 28. Аналізувати та проводити оцінку ефективності та рівня захищеності ресурсів різних класів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах в ході проведення випробувань згідно встановленої політики інформаційної та\або кібербезпеки.
РН 29. Здійснювати оцінювання можливості реалізації потенційних загроз інформації, що обробляється в інформаційно-телекомунікаційних системах та ефективності використання комплексів засобів захисту в умовах реалізації загроз різних класів.
РН 30. Здійснювати оцінювання можливості несанкціонованого доступу до елементів інформаційно-телекомунікаційних систем.
РН 31. Застосовувати теорії та методи захисту для забезпечення безпеки елементів інформаційно-телекомунікаційних систем.
РН 32. Вирішувати задачі управління процесами відновлення штатного функціонування інформаційно-телекомунікаційних систем з використанням процедур резервування згідно встановленої політики безпеки.
РН 33. Вирішувати задачі забезпечення безперервності бізнес процесів організації на основі теорії ризиків.
РН 34. Приймати участь у розробці та впровадженні стратегії інформаційної безпеки та/або кібербезпеки відповідно до цілей і завдань організації.
РН 35. Вирішувати задачі забезпечення та супроводу комплексних систем

захисту інформації, а також протидії несанкціонованому доступу до інформаційних ресурсів і процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах згідно встановленої політики інформаційної і\або кібербезпеки.
РН 36. Виявляти небезпечні сигнали технічних засобів.
РН 37. Вимірювати параметри небезпечних та завадових сигналів під час інструментального контролю процесів захисту інформації та визначати ефективність захисту інформації від витоку технічними каналами відповідно до вимог нормативних документів системи технічного захисту інформації.
РН 38. Інтерпретувати результати проведення спеціальних вимірювань з використанням технічних засобів, контролю характеристик інформаційно-телекомунікаційних систем відповідно до вимог нормативних документів системи технічного захисту інформації.
РН 39. Проводити атестацію (спираючись на облік та обстеження) режимних територій (зон), приміщень тощо в умовах додержання режиму секретності із фіксуванням результатів у відповідних документах.
РН 40. Інтерпретувати результати проведення спеціальних вимірювань з використанням технічних засобів, контролю характеристик ІТС відповідно до вимог нормативних документів системи технічного захисту інформації.
РН 41. Забезпечувати неперервність процесу ведення журналів реєстрації подій та інцидентів на основі автоматизованих процедур.
РН 42. Впроваджувати процеси виявлення, ідентифікації, аналізу та реагування на інциденти інформаційної і/або кібербезпеки.
РН 43. Застосовувати національні та міжнародні регулюючі акти в сфері інформаційної безпеки та/ або кібербезпеки для розслідування інцидентів.
РН 44. Вирішувати задачі забезпечення безперервності бізнес-процесів організації на основі теорії ризиків та встановленої системи управління інформаційною безпекою, згідно з вітчизняними та міжнародними вимогами та стандартами.
РН 45. Застосовувати різні класи політик інформаційної безпеки та/ або кібербезпеки, що базуються на ризик-орієнтованому контролі доступу до інформаційних активів.
РН 46. Здійснювати аналіз та мінімізацію ризиків обробки інформації в інформаційно-телекомунікаційних системах.
РН 47. Вирішувати задачі захисту інформації, що обробляється в інформаційно-телекомунікаційних системах з використанням сучасних методів та засобів криптографічного захисту інформації.
РН 48. Виконувати впровадження та підтримку систем виявлення вторгнень та використовувати компоненти криптографічного захисту для забезпечення необхідного рівня захищеності інформації в інформаційно-телекомунікаційних системах.
РН 49. Забезпечувати належне функціонування системи моніторингу інформаційних ресурсів і процесів в інформаційно-телекомунікаційних системах.
РН 50. Забезпечувати функціонування програмних та програмно-апаратних комплексів виявлення вторгнень різних рівнів та класів (статистичних, сигнатурних, статистично-сигнатурних).

РН 51. Підтримувати працездатність та забезпечувати конфігурування систем виявлення вторгнень в інформаційно-телекомунікаційних системах. РН 52. Використовувати інструментарій для моніторингу процесів в інформаційно-телекомунікаційних системах. РН 53. Вирішувати задачі аналізу програмного коду на наявність можливих загроз. РН 54. Усвідомлювати цінності громадянського (вільного демократичного) суспільства та необхідність його сталого розвитку, верховенства права, прав і свобод людини і громадянина в Україні. РН 55. Знати основи запобігання корупції, суспільної та академічної доброчесності на рівні, необхідному для формування нетерпимості до корупції та проявів не доброчесної поведінки серед здобувачів освіти та вміти застосовувати їх в професійній діяльності.	
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.

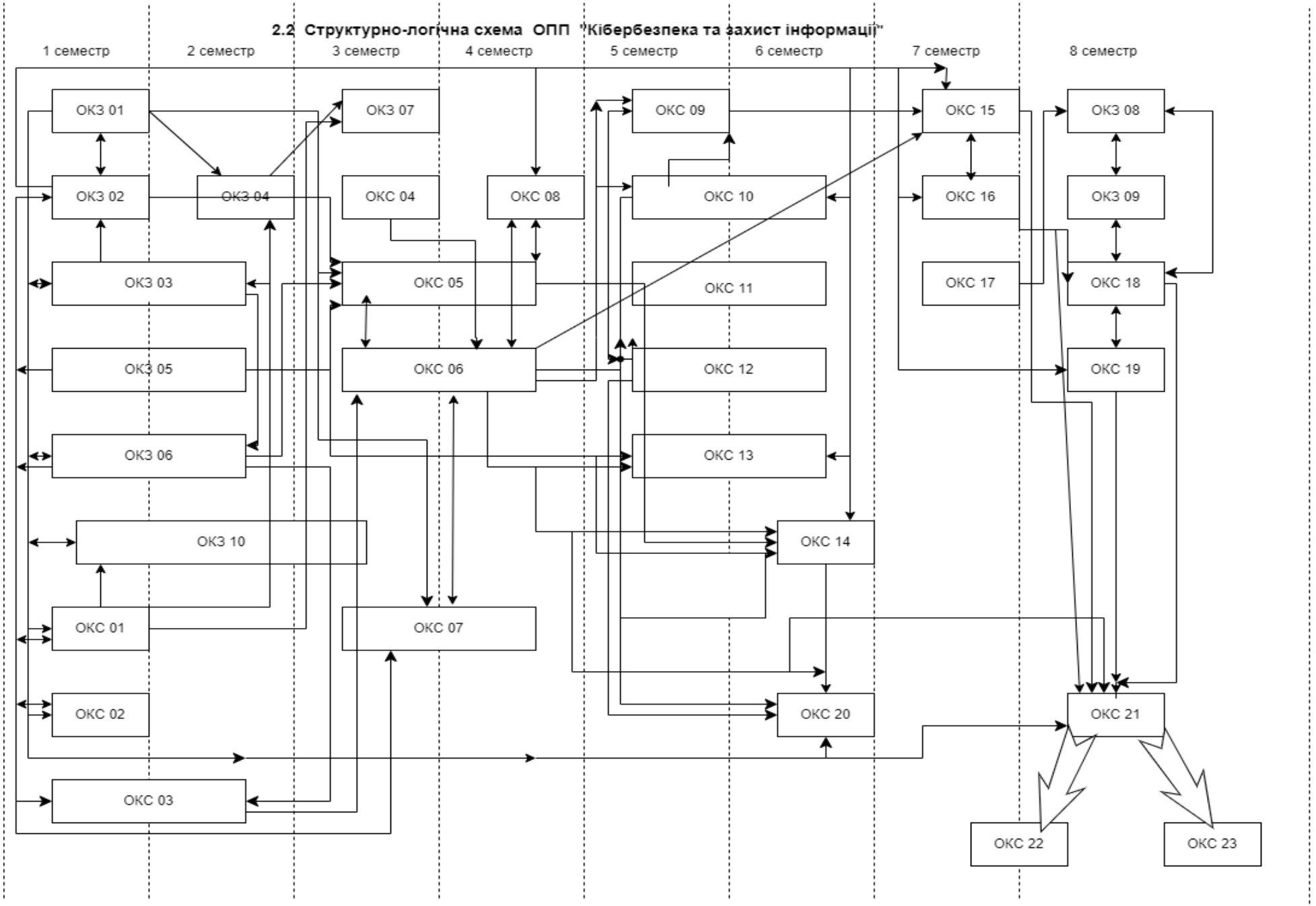
2. Перелік компонент освітньо-професійної програми та їх логічна послідовність

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**	

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. На атестацію виноситься сукупність знань, умінь, навичок, інших компетентностей, набутих особою у процесі навчання за Стандартом вищої освіти України першого (бакалаврського) рівня зі спеціальності 125 «Кібербезпека» та цією освітньою програмою. До атестації допускаються здобувачі освіти, які виконали всі вимоги програми підготовки.
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 цією освітньою програмою.
Вимоги до кваліфікаційної роботи	Випускна кваліфікаційна бакалаврська робота передбачає розв’язання спеціалізованої задачі в галузі кібербезпеки. Випускна кваліфікаційна бакалаврська робота не може містити академічного плагіату, фальсифікації, фабрикації. Випускна кваліфікаційна бакалаврська робота розміщується у інституційному репозитарії Центральноукраїнського національного технічного університету http://dspace.kntu.kr.ua/.

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

ОК	Інт. комп.	Загальні компетентності								Фахові компетентності											
		КЗ1	КЗ2	КЗ3	КЗ4	КЗ5	КЗ6	КЗ7	КЗ8	КФ1	КФ2	КФ3	КФ4	КФ5	КФ6	КФ7	КФ8	КФ9	КФ10	КФ11	КФ12
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	+	+	+		+	+				+	+										

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

	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
РН1.	+		+			+																									
РН2.		+				+			+				+		+		+	+									+		+	+	+
РН3.	+	+	+	+	+	+			+		+	+			+		+			+			+	+	+	+				+	+	+
РН4.		+			+	+	+		+		+	+		+						+				+						+	+	+
РН5.											+			+										+							+	+
РН6.		+		+		+	+				+	+					+						+		+					+	+	+
РН7.	+																												+		+	+
РН8.								+								+				+						+						
РН9.																										+				+	+	+
РН10.														+			+															
РН11.					+											+																
РН12.					+																					+			+			
РН13.														+		+																
РН14.													+			+			+							+		+	+	+	+	+
РН15.												+				+	+								+				+	+	+	+
РН16.																										+						
РН17.														+	+															+	+	+
РН18.																						+			+					+	+	+
РН19.														+		+														+	+	+
РН20.																+																
РН21.								+								+																
РН22.															+	+		+											+			
РН23.								+											+								+					
РН24.								+								+												+				
РН25.								+																								
РН26.																+													+			
РН27.															+			+									+			+		
РН28.					+																	+								+		

PH29.																													+				
PH30.																			+					+								
PH31.																													+				
PH32.																					+												
PH33.																+																	
PH34.																+				+											+		
PH35.								+																			+		+		+		
PH36.																+			+							+							
PH37.																			+			+											
PH38.																			+			+											
PH39.																			+								+						
PH40.																			+			+											
PH41.																+										+							
PH42.																+										+							
PH43.																+										+							
PH44.																+											+						
PH45.																+																	
PH46.																	+									+							
PH47.																+							+	+						+		
PH48.								+								+							+									
PH49.																					+												
PH50.																+													+				
PH51.																					+												
PH52.																					+												
PH53.																+								+									
PH54.				+						+																							
PH55.											+																						

6. 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.