МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ЛУЦЬКИЙ НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ

ПОГОДЖЕНО
Гарант освітньої програми
Кібербезпека
(назва освітньої програми)
зі спеціальності
125 Кібербезпека та захист інформації
(назва спеціальності)
Сергій КОСТЮЧКО
«25» квітня 2023 р.

ЗАТВЕРДЖУЮ
Ректор ЛНТУ
_____ Ірина ВАХОВИЧ
«25» квітня 2023 р.

ОСВІТНЯ ПРОГРАМА

«КІБЕРБЕЗПЕКА»
(назва освітньої програми)

CYBERSECURITY

перший (бакалаврський) рівень вищої освіти
(рівень вищої освіти: перший (бакалаврський) / другий (магістерський) / третій (освітньо-науковий))
спеціальність 125 Кібербезпека та захист інформації
(шифр і назва спеціальності)
галузь знань 12 Інформаційні технології
(шифр і назва галузі знань)

Електронна версія

СХВАЛЕНО
Вченою радою ЛНТУ
протокол №10 від 27.04.2023 р.

Луцьк – 2023

АРКУШ ПОГОДЖЕННЯ

освітньої програми
«КІБЕРБЕЗПЕКА»
першого (бакалаврського) рівня вищої освіти
за спеціальністю 125 Кібербезпека та захист інформації
галузі знань 12 Інформаційні технології

Завідувач кафедри — Сергій КОСТЮЧКО
(протокол № 1 від 26.08.2026 р.)

В.о. начальника відділу забезпечення якості освітнього процесу, ліцензування та акредитації — Олена КУЗЬМАК

Рекомендовано комісією з якості факультету — Інна КОНДІУС
(протокол № 6 від 26.08.2026 р.)

Схвалено вченою радою факультету — Інна КОНДІУС
(протокол № 13 від 26.08.2026 р.)

Схвалено навчально-методичною радою ЛНТУ — Надія КОВАЛЬЧУК
(протокол № 8 від 25.04.2023 р.)

ПЕРЕДМОВА

Переглянуто групою забезпечення та стейкхолдерами, залученими до розроблення та вдосконалення освітньої програми відповідно до Стандарту вищої освіти України підготовки бакалавра за спеціальністю 125 «Кібербезпека та захист інформації».

Гарант освітньої програми:

Костючко Сергій Миколайович – к.т.н., доцент, завідувач кафедри кібербезпеки _____ *(підпис)*

Члени групи забезпечення освітньої програми:

Гордєєв Олександр Олександрович – д.т.н., професор, доцент кафедри інженерії програмного забезпечення _____ *(підпис)*

Гринюк Сергій Васильович – к.т.н., доцент кафедри кібербезпеки _____ *(підпис)*

Поліщук Микола Миколайович – к.т.н., доцент кафедри кібербезпеки _____ *(підпис)*

Стейкхолдери, залучені до розроблення та вдосконалення ОП:

Вознюк Роман Васильович – адміністратор безпеки мереж і систем, комунальне некомерційне підприємство "Нововолинська центральна міська лікарня";

Кулакевич Олег Русланович – директор, ТОВ «РЕДВІНГ СТУДІО».

Рецензії-відгуки зовнішніх стейкхолдерів додаються.

ПРОФІЛЬ ОСВІТНЬОЇ ПРОГРАМИ

1 – ЗАГАЛЬНА ІНФОРМАЦІЯ	
Повна назва закладу вищої освіти	Луцький національний технічний університет, код в ЄДЕБО – 309
Рівень вищої освіти	Перший (бакалаврський)
Офіційна назва освітньої програми	Кібербезпека Cybersecurity
Тип диплому та обсяг освітньої програми	Диплом бакалавра, одиничний. Обсяг ОП - 240 кредитів ЄКТС. Термін навчання - 3 роки 10 місяців.
Форма здобуття освіти	Очна (денна), заочна
Назва кваліфікації	Освітня кваліфікація - Бакалавр з кібербезпеки та захисту інформації, Ступінь вищої освіти – Бакалавр, Спеціальність – F5 Кібербезпека та захист інформації, Галузь знань - F Інформаційні технології, Освітня програма – «Кібербезпека».
Наявність акредитації	Акредитована рішенням НАЗЯВО, протокол № 9 (59) від 16.04.2024, сертифікат №13040 від 29.05.2025.
Цикл/рівень	НРК України – 6 рівень, QF-EHEA – перший цикл (First cycle), EQF-LLL – 6 рівень (Level 6).
Передумови	Для здобуття освітнього ступеня бакалавра зі спеціальності F5 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.
Мова(и) викладання	Українська
Термін дії освітньої програми	3 роки 10 місяців
Інтернет-адреса постійного розміщення освітньої програми	https://lntu.edu.ua/uk/studentu-0/navchannya/osvitniy-programi#5116
2 – МЕТА/ЦІЛІ ОСВІТНЬОЇ ПРОГРАМИ	
Мета - полягає у підготовці кваліфікованих фахівців здатних розробляти, впроваджувати та використовувати технології забезпечення безпеки інформації, адаптувати процеси управління інформаційною та кібербезпекою під конкретні об’єкти інформатизації. Цілі навчання - підготовка фахівців, здатних використовувати і впроваджувати технології кібербезпеки та захисту інформації та розв’язувати складні задачі у галузі кібербезпеки та захисту інформації.	
3 – ХАРАКТЕРИСТИКА ОСВІТНЬОЇ ПРОГРАМИ	

Предметна область (галузь знань, спеціальність, предметна спеціальність або спеціалізація)	Галузь знань F – Інформаційні технології Спеціальність F5 – Кібербезпека та захист інформації 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. 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	Освітня. Програма орієнтована на підготовку кваліфікованих фахівців здатних розробляти, впроваджувати та використовувати технології забезпечення безпеки інформації, адаптувати процеси управління інформаційною та кібербезпекою під конкретні об’єкти інформатизації.
Основний фокус освітньої програми	Акцент ставиться на набутті навичок відповідно до міжнародних та національних нормативно-правових документів, світових практик та стандартів, принципів, теорій, сучасних технологій забезпечення інформаційної та/або кібербезпеки.
Особливості освітньої програми	Особливості здійснення освітнього процесу ґрунтуються на тісній співпраці з регіональними професійними об’єднаннями, вітчизняними та міжнародними ІТ-фірмами; використання здобутків міжнародних професійних та освітніх організацій CISCO, імплементація їх навчальних курсів в освітній процес з видачею міжнародних сертифікатів, залучення здобувачів вищої освіти до практик та стажування в організаціях стейкхолдерів, виконання реальних проєктів. Орієнтація на професійний стандарт «Аналітик загроз безпеки».
4 – ПРИДАТНІСТЬ ВИПУСКНИКІВ ДО ПРАЦЕВЛАШТУВАННЯ ТА ПОДАЛЬШЕ НАВЧАННЯ	
Придатність до працевлаштування	На посади у структурних підрозділах установ/підприємств/організацій, які передбачають наявність вищої освіти зі спеціальності F5 Кібербезпека та захист інформації.

Подальше навчання	Можливість навчання за програмою другого (магістерського) рівня вищої освіти. Набуття додаткових кваліфікацій в системі післядипломної освіти.
5 – ВИКЛАДАННЯ ТА ОЦІНЮВАННЯ	
Викладання та навчання	За домінуючими методами та способами навчання: пасивні (пояснювальні-ілюстративні); активні (проблемні, інтерактивні, проектні, інформаційно-комп’ютерні саморозвиваючі) тощо. За організаційними формами: колективного та інтегративного навчання, електронне навчання в системі Moodle, студентоцентроване тощо. За орієнтацією педагогічної взаємодії: позиційного та контекстного навчання, технології співпраці тощо. Викладання дисципліни здійснюється з дотриманням принципів академічної доброчесності відповідно до Закону України «Про академічну доброчесність» № 4742-IX. Особлива увага приділяється формуванню творчих завдань, що стимулюють критичне мислення, уникненню репродуктивних завдань та навчанню академічного письма.
Оцінювання	Оцінювання навчальних досягнень здобувачів здійснюється за 4-х бальною («відмінно», «добре», «задовільно», «незадовільно»), 100 бальною та шкалою ЄКТС (A, B, C, D, E, F, FX) системах. Види контролю: поточний, тематичний, періодичний, підсумковий, самоконтроль. Форми контролю: усне та письмове опитування, тестові завдання за допомогою комп’ютера, захист лабораторних та індивідуальних робіт, захист курсових тощо. Оцінювання результатів навчання є прозорим і здійснюється з урахуванням дотримання академічної доброчесності.

6 – ПРОГРАМНІ КОМПЕТЕНТНОСТІ

Вид компетентності	Шифр	Опис компетентності
Інтегральна компетентність	ІК	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 (ЗК)	ЗК01	Здатність застосовувати знання у практичних ситуаціях.
	ЗК02	Знання та розуміння предметної області та розуміння професії.
	ЗК03	Здатність професійно спілкуватися державною та іноземною мовами як усно, так і письмово.
	ЗК04	Вміння виявляти, ставити та вирішувати проблеми за професійним спрямуванням.
	ЗК05	Здатність до пошуку, оброблення та аналізу інформації.

	ЗК06	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.
	ЗК07	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.
	ЗК08	Здатність ухвалювати рішення та діяти, дотримуючись принципу неприпустимості корупції та будь-яких інших проявів недоброчесності.
Спеціальні (фахові, предметні) компетентності (СК)	СК01	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.
	СК02	Здатність до використання інформаційно комунікаційних технологій, сучасних методів і моделей інформаційної безпеки та/або кібербезпеки.
	СК03	Здатність до використання програмних та програмно апаратних комплексів засобів захисту інформації в інформаційнотелекомунікаційних (автоматизованих) системах.
	СК04	Здатність забезпечувати неперервність бізнесу згідно встановленої політики інформаційної та/або кібербезпеки.
	СК05	Здатність забезпечувати захист інформації, що обробляється в інформаційно-телекомунікаційних (автоматизованих) системах з метою реалізації встановленої політики інформаційної та/або кібербезпеки.
	СК06	Здатність відновлювати штатне функціонування інформаційних, інформаційно-телекомунікаційних (автоматизованих) систем після реалізації загроз, здійснення кібератак, збоїв та відмов різних класів та походження.

	СК07	Здатність впроваджувати та забезпечувати функціонування комплексних систем захисту інформації (комплекси нормативноправових, організаційних та технічних засобів і методів, процедур, практичних прийомів та ін.)
	СК08	Здатність здійснювати процедури управління інцидентами, проводити розслідування, надавати їм оцінку.
	СК09	Здатність здійснювати професійну діяльність на основі впровадженої системи управління інформаційною та/або кібербезпекою.
	СК10	Здатність застосовувати методи та засоби криптографічного та технічного захисту інформації на об’єктах інформаційної діяльності.
	СК11	Здатність виконувати моніторинг процесів функціонування інформаційних, інформаційно-телекомунікаційних (автоматизованих) систем згідно встановленої політики інформаційної та/або кібербезпеки.
	СК12	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		
Шифр	**Опис програмного результату навчання**	
ПРН01	застосовувати знання державної та іноземних мов з метою забезпечення ефективності професійної комунікації;	
ПРН02	організовувати власну професійну діяльність, обирати оптимальні методи та способи розв’язування складних спеціалізованих задач та практичних проблем у професійній діяльності, оцінювати їхню ефективність;	
ПРН03	використовувати результати самостійного пошуку, аналізу та синтезу інформації з різних джерел для ефективного рішення спеціалізованих задач професійної діяльності;	
ПРН04	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;	
ПРН05	адаптуватися в умовах частої зміни технологій професійної діяльності, прогнозувати кінцевий результат;	
ПРН06	критично осмислювати основні теорії, принципи, методи і поняття у навчанні та професійній діяльності;	

ПРН07	діяти на основі законодавчої та нормативно-правової бази України та вимог відповідних стандартів, у тому числі міжнародних в галузі інформаційної та /або кібербезпеки;
ПРН08	готувати пропозиції до нормативних актів щодо забезпечення інформаційної та /або кібербезпеки;
ПРН09	впроваджувати процеси, що базуються на національних та міжнародних стандартах, виявлення, ідентифікації, аналізу та реагування на інциденти інформаційної та/або кібербезпеки;
ПРН10	виконувати аналіз та декомпозицію інформаційно-телекомунікаційних систем;
ПРН11	виконувати аналіз зв’язків між інформаційними процесами на віддалених обчислювальних системах;
ПРН12	розробляти моделі загроз та порушника;
ПРН13	аналізувати проекти інформаційно-телекомунікаційних систем базуючись на стандартизованих технологіях та протоколах передачі даних;
ПРН14	вирішувати завдання захисту програм та інформації, що обробляється в інформаційно-телекомунікаційних системах програмно-апаратними засобами та давати оцінку результативності якості прийнятих рішень;
ПРН15	використовувати сучасне програмно-апаратне забезпечення інформаційнокомунікаційних технологій;
ПРН16	реалізовувати комплексні системи захисту інформації в автоматизованих системах (АС) організації (підприємства) відповідно до вимог нормативноправових документів;
ПРН17	забезпечувати процеси захисту та функціонування інформаційнотелекомунікаційних (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;
ПРН18	використовувати програмні та програмно-апаратні комплекси захисту інформаційних ресурсів;
ПРН19	застосовувати теорії та методи захисту для забезпечення безпеки інформації в інформаційно-телекомунікаційних системах;
ПРН20	забезпечувати функціонування спеціального програмного забезпечення, щодо захисту інформації від руйнуючих програмних впливів, руйнуючих кодів в інформаційно-телекомунікаційних системах;
ПРН21	вирішувати задачі забезпечення та супроводу (в.т. числі: огляд, тестування, підзвітність) системи управління доступом згідно встановленої політики безпеки в інформаційних та інформаційнотелекомунікаційних (автоматизованих) системах;

ПРН22	вирішувати задачі управління процедурами ідентифікації, автентифікації, авторизації процесів і користувачів в інформаційнотелекомунікаційних системах згідно встановленої політики інформаційної і\або кібербезпеки;
ПРН23	реалізовувати заходи з протидії отриманню несанкціонованого доступу до інформаційних ресурсів і процесів в інформаційних та інформаційнотелекомунікаційних (автоматизованих) системах;
ПРН24	вирішувати задачі управління доступом до інформаційних ресурсів та процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах на основі моделей управління доступом (мандатних, дискреційних, рольових);
ПРН25	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;
ПРН26	впроваджувати заходи та забезпечувати реалізацію процесів попередження отриманню несанкціонованого доступу і захисту інформаційних, інформаційно-телекомунікаційних (автоматизованих) систем на основі еталонної моделі взаємодії відкритих систем;
ПРН27	вирішувати задачі захисту потоків даних в інформаційних, інформаційнотелекомунікаційних (автоматизованих) системах;
ПРН28	аналізувати та проводити оцінку ефективності та рівня захищеності ресурсів різних класів в інформаційних та інформаційнотелекомунікаційних (автоматизованих) системах в ході проведення випробувань згідно встановленої політики інформаційної та\або кібербезпеки;
ПРН29	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;
ПРН30	здійснювати оцінювання можливості несанкціонованого доступу до елементів інформаційно-телекомунікаційних систем;
ПРН31	застосовувати теорії та методи захисту для забезпечення безпеки елементів інформаційно-телекомунікаційних систем;
ПРН32	вирішувати задачі управління процесами відновлення штатного функціонування інформаційно-телекомунікаційних систем з використанням процедур резервування згідно встановленої політики безпеки;
ПРН33	вирішувати задачі забезпечення безперервності бізнес процесів організації на основі теорії ризиків;

ПРН34	приймати участь у розробці та впровадженні стратегії інформаційної безпеки та/або кібербезпеки відповідно до цілей і завдань організації;
ПРН35	вирішувати задачі забезпечення та супроводу комплексних систем захисту інформації, а також протидії несанкціонованому доступу до інформаційних ресурсів і процесів в інформаційних та інформаційнотелекомунікаційних (автоматизованих) системах згідно встановленої політики інформаційної і\або кібербезпеки;
ПРН36	виявляти небезпечні сигнали технічних засобів;
ПРН37	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;
ПРН38	інтерпретувати результати проведення спеціальних вимірювань з використанням технічних засобів, контролю характеристик інформаційнотелекомунікаційних систем відповідно до вимог нормативних документів системи технічного захисту інформації;
ПРН39	проводити атестацію (спираючись на облік та обстеження) режимних територій (зон), приміщень тощо в умовах додержання режиму секретності із фіксуванням результатів у відповідних документах;
ПРН40	інтерпретувати результати проведення спеціальних вимірювань з використанням технічних засобів, контролю характеристик ІТС відповідно до вимог нормативних документів системи технічного захисту інформації;
ПРН41	забезпечувати неперервність процесу ведення журналів реєстрації подій та інцидентів на основі автоматизованих процедур;
ПРН42	впроваджувати процеси виявлення, ідентифікації, аналізу та реагування на інциденти інформаційної і/або кібербезпеки;
ПРН43	застосовувати національні та міжнародні регулюючі акти в сфері інформаційної безпеки та/ або кібербезпеки для розслідування інцидентів;
ПРН44	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;
ПРН45	застосовувати ріні класи політик інформаційної безпеки та/ або кібербезпеки, що базуються на ризик-орієнтованому контролі доступу до інформаційних активів;
ПРН46	здійснювати аналіз та мінімізацію ризиків обробки інформації в інформаційно-телекомунікаційних системах;

ПРН47	вирішувати задачі захисту інформації, що обробляється в інформаційнотелекомунікаційних системах з використанням сучасних методів та засобів криптографічного захисту інформації;
ПРН48	виконувати впровадження та підтримку систем виявлення вторгнень та використовувати компоненти криптографічного захисту для забезпечення необхідного рівня захищеності інформації в інформаційнотелекомунікаційних системах;
ПРН49	забезпечувати належне функціонування системи моніторингу інформаційних ресурсів і процесів в інформаційно-телекомунікаційних системах;
ПРН50	забезпечувати функціонування програмних та програмно-апаратних комплексів виявлення вторгнень різних рівнів та класів (статистичних, сигнатурних, статистично-сигнатурних);
ПРН51	підтримувати працездатність та забезпечувати конфігурування систем виявлення вторгнень в інформаційно-телекомунікаційних системах;
ПРН52	використовувати інструментарій для моніторингу процесів в інформаційнотелекомунікаційних системах;
ПРН53	вирішувати задачі аналізу програмного коду на наявність можливих загроз.
ПРН54	усвідомлювати цінності громадянського (вільного демократичного) суспільства та необхідність його сталого розвитку, верховенства права, прав і свобод людини і громадянина в Україні.
	Визначені ЗВО:
ПРН55	використовувати різні види та форми рухової активності для активного відпочинку та ведення здорового способу життя.
Набуття здобувачами вищої освіти навичок та компетентностей, спрямованих на досягнення глобальних цілей сталого розвитку до 2030 року, проголошених резолюцією Генеральної Асамблеї Організації Об'єднаних Націй від 25 вересня 2015 року №70/1	Освітня програма «КІБЕРБЕЗПЕКА» пропонує здобувачам вищої освіти освітні компоненти, які сприятимуть формуванню навичок та компетентостей, спрямованих на досягнення глобальних цілей сталого розвитку до 2030 року. Відповідність освітніх компонентів Цілям сталого розвитку відображено у матриці формування навичок та компетентностей, спрямованих на досягнення Цілей сталого розвитку.
8 – РЕСУРСНЕ ЗАБЕЗПЕЧЕННЯ РЕАЛІЗАЦІЇ ПРОГРАМИ	

Кадрове забезпечення	Втілення усіх аспектів програми проводиться працівниками з відповідними науковими ступенями та вченими званнями, свідоцтвами про підвищення кваліфікації за спеціальністю.
Матеріально-технічне забезпечення	За кафедрою кібербезпеки закріплені навчальні аудиторії та лабораторії, в яких наявне обладнання та устаткування та організовані робочі місця для проведення занять. Наявне мультимедійне та презентаційне обладнання. Соціальнопобутова інфраструктура. Забезпеченість гуртожитком.
Інформаційне та навчально-методичне забезпечення	• Офіційний сайт ЛНТУ: https://lntu.edu.ua; • точки бездротового доступу Інтернет; • наукова бібліотека, читальні зали ЛНТУ; • електронна бібліотека (репозитарій) http://elibrary.lntu.edu/; • електронний освітній портал ЛНТУ http://mdl.lntu.edu.ua; • навчально-методичні комплекси дисциплін; • дидактичні матеріали для самостійної та індивідуальної роботи студентів; • програми практик.
9 – АКАДЕМІЧНА МОБІЛЬНІСТЬ	
Національна кредитна мобільність	Реалізується положенням університету про національну кредитну мобільність студентів та викладачів у вітчизняних закладах вищої освіти.
Міжнародна кредитна мобільність	Реалізується згідно договорів між Луцьким національним технічним університетом та закладами вищої освіти зарубіжних країн-партнерів.
Навчання іноземних здобувачів вищої освіти	Підготовка іноземців та осіб без громадянства за першим (бакалаврським) освітнім рівнем галузі знань F «Інформаційні технології» спеціальності F5 «Кібербезпека та захист інформації» можлива на загальних умовах.
10 – АКАДЕМІЧНА ДОБРОЧЕСНІСТЬ	
Реалізація освітньої програми здійснюється з дотриманням вимог Закону України «Про академічну доброчесність» № 4742-IX. Академічна доброчесність є складовою внутрішньої системи забезпечення якості освіти. Усі учасники освітнього процесу керуються принципами чесності, довіри, поваги до авторства, справедливості та відповідальності. Порушення академічної доброчесності (плагіат, самоплагіат, фальсифікація, списування, недоброчесне використання штучного інтелекту тощо) тягнуть за собою академічну відповідальність відповідно до Закону України «Про академічну доброчесність» № 4742-IX та внутрішніх нормативних актів.	

ПЕРЕЛІК ОСВІТНІХ КОМПОНЕНТІВ ОСВІТНЬОЇ ПРОГРАМИ

Код освітніх компонентів	Назва освітніх компонентів ОП (ОК, підсумкова атестація)	Кількість кредитів ЄКТС	Форма підсумкового контролю	Семестр
1 Обов'язкова складова				
1.1 Дисципліни загальної підготовки				
ОК.01	Прикладна математика	10	екзамен	1, 2
ОК.02	Фізика	6	залік	2
ОК.03	Іноземна мова	6	залік	1
ОК.04	Ділова українська мова та академічне письмо	4	залік	1
ОК.05	Іноземна мова за професійним спрямуванням	6	залік	3, 4
ОК.06	Дискретна математика	5	екзамен	1
ОК.07	Фізичне виховання	3	залік	1
РАЗОМ дисципліни загальної підготовки		**40**		
1.2 Дисципліни професійної підготовки				
ОК.08	Програмування та реверс-інжиніринг	6	екзамен	1
ОК.09	Нормативно-правове забезпечення кібербезпеки	4	залік	2
ОК.10	Основи кібербезпеки	6	екзамен	2
ОК.11	Комп'ютерна електроніка та схемотехніка	5	залік	3
ОК.12	Теорія інформації та кодування	5	екзамен	2
ОК.13	Сигнали та процеси в системах захисту інформації	5	екзамен	4
ОК.14	Комп'ютерні мережі	6	екзамен	3
ОК.15	Захист операційних систем	6	екзамен	3
ОК.16	Безпека інформаційно-комунікаційних систем	5	екзамен	4
ОК.17	Алгоритми захисту інформації та системне програмування	6	екзамен	2
ОК.18	Безпека баз даних	6	екзамен	4
ОК.19	Аналіз великих даних	5	екзамен	5
ОК.20	Системи моніторингу комп'ютерних систем та мереж	6	екзамен	5
ОК.21	Інформаційна безпека бізнесу	5	екзамен	5
ОК.22	Управління інформаційною безпекою	4	екзамен	5
ОК.23	Системи технічного захисту інформації	6	екзамен, КР	6
ОК.24	Обробка інцидентів та реагування	6	екзамен	6
ОК.25	Аналітик кібербезпеки	5	екзамен	6
ОК.26	Оцінка та управління ризиками	5	екзамен	7

Код освітніх компонентів	Назва освітніх компонентів ОП (ОК, підсумкова атестація)	Кількість кредитів ЄКТС	Форма підсумкового контролю	Семестр
ОК.27	Системи захисту інформації	5	екзамен	7
ОК.28	Прикладна криптологія і стеганографія	5	екзамен	7
ОК.29	Техніки захисту і протидії мережевим атакам	5	екзамен, КР	7
ОК.30	Корпоративна безпека	6	екзамен	8
ОК.31	Аудит інформаційних систем	6	екзамен	8
РАЗОМ дисципліни професійної підготовки		**129**		
2 Вибіркова складова				
2.1 Загальні дисципліни вільного вибору				
ВК.01	Дисципліна 1	5	залік	3
ВК.02	Дисципліна 2	5	залік	3
ВК.03	Дисципліна 4	5	залік	4
ВК.04	Дисципліна 5	5	залік	4
2.2 Професійні дисципліни вільного вибору				
ВК.05	Дисципліна 1	5	залік	5
ВК.06	Дисципліна 2	5	залік	5
ВК.07	Дисципліна 3	5	залік	6
ВК.08	Дисципліна 4	5	залік	6
ВК.09	Дисципліна 5	5	залік	7
ВК.10	Дисципліна 6	5	залік	7
ВК.11	Дисципліна 7	5	залік	8
ВК.12	Дисципліна 8	5	залік	8
3 Практична підготовка				
ОК.32	Фаховий тренінг	3	захист з оцінкою	6
ОК.33	Фахова практика	6	захист з оцінкою	8
4 Атестація				
ОК.34	Підготовка та здача Єдиного державного кваліфікаційного іспиту	2	екзамен	8
Загальний обсяг обов'язкових компонент		**180**		
Загальний обсяг вибіркових компонент		**60**		
Загальний обсяг освітньої програми		***240 (бакалавр)***		

СТРУКТУРНО-ЛОГІЧНА СХЕМА ОП



ФОРМА АТЕСТАЦІЇ ЗДОБУВАЧІВ ВИЩОЇ ОСВІТИ

Форма атестації здобувачів вищої освіти	Атестація здійснюється у формі єдиного державного кваліфікаційного іспиту.
Вимоги до єдиного державного кваліфікаційного іспиту	Єдиний державний кваліфікаційний іспит передбачає оцінювання досягнень результатів навчання, визначених відповідним стандартом.

МАТРИЦЯ ВІДПОВІДНОСТІ РЕЗУЛЬТАТІВ НАВЧАННЯ ТА КОМПЕТЕНТНОСТЕЙ

Програмні результати навчання / Компетентності	ІК	ЗК01	ЗК02	ЗК03	ЗК04	ЗК05	ЗК06	ЗК07	ЗК08	СК01	СК02	СК03	СК04	СК05	СК06	СК07	СК08	СК09	СК10	СК11	СК12
ПРН01				+																	
ПРН02		+	+		+																
ПРН03					+	+															
ПРН04		+			+	+															
ПРН05		+	+		+						+										
ПРН06		+				+															
ПРН07							+		+	+											
ПРН08				+	+					+											
ПРН09										+							+	+			
ПРН10					+						+			+							
ПРН11											+			+							+
ПРН12											+										+
ПРН13										+	+			+							
ПРН14					+							+		+							
ПРН15											+	+									
ПРН16										+				+		+					
ПРН17											+			+		+					
ПРН18												+		+							
ПРН19											+			+							
ПРН20												+		+							+
ПРН21														+		+		+			
ПРН22												+		+		+					
ПРН23												+		+		+					
ПРН24														+		+		+			

Програмні результати навчання / Компетентності	ІК	ЗК01	ЗК02	ЗК03	ЗК04	ЗК05	ЗК06	ЗК07	ЗК08	СК01	СК02	СК03	СК04	СК05	СК06	СК07	СК08	СК09	СК10	СК11	СК12
ПРН25														+				+		+	
ПРН26											+			+		+					
ПРН27											+			+					+		
ПРН28																+		+			+
ПРН29												+				+					+
ПРН30														+							+
ПРН31											+			+							
ПРН32													+		+			+			
ПРН33													+					+			+
ПРН34										+			+					+			
ПРН35												+		+		+					
ПРН36																			+		+
ПРН37										+									+		+
ПРН38										+									+		+
ПРН39										+						+			+		
ПРН40										+									+		+
ПРН41																	+	+		+	
ПРН42																	+			+	+
ПРН43										+							+				
ПРН44										+			+					+			+
ПРН45														+				+			+
ПРН46														+				+			+
ПРН47														+					+		
ПРН48												+							+	+	
ПРН49																		+		+	
ПРН50												+								+	

Програмні результати навчання / Компетентності	ІК	ЗК01	ЗК02	ЗК03	ЗК04	ЗК05	ЗК06	ЗК07	ЗК08	СК01	СК02	СК03	СК04	СК05	СК06	СК07	СК08	СК09	СК10	СК11	СК12
ПРН51												+								+	
ПРН52											+									+	
ПРН53											+	+									+
ПРН54							+		+												
ПРН55								+													

МАТРИЦЯ ВІДПОВІДНОСТІ ПРОГРАМНИХ КОМПЕТЕНТНОСТЕЙ ОСВІТНІМ КОМПОНЕНТАМ ОСВІТНЬОЇ ПРОГРАМИ

Освітні компоненти / Компетентності	ОК.01	ОК.02	ОК.03	ОК.04	ОК.05	ОК.06	ОК.07	ОК.08	ОК.09	ОК.10	ОК.11	ОК.12	ОК.13	ОК.14	ОК.15	ОК.16	ОК.17	ОК.18	ОК.19	ОК.20	ОК.21	ОК.22	ОК.23	ОК.24	ОК.25	ОК.26	ОК.27	ОК.28	ОК.29	ОК.30	ОК.31	ОК.32	ОК.33	ОК.34
ІК	+	+						+			+	+		+	+	+	+			+			+	+			+			+				
ЗК01	+	+		+		+					+			+				+		+	+		+	+			+	+		+		+	+	+
ЗК02										+																	+				+	+	+	+
ЗК03			+	+	+																													
ЗК04	+		+			+		+	+	+				+						+				+			+				+	+	+	+
ЗК05	+	+	+			+		+	+					+	+	+		+	+					+			+				+	+	+	
ЗК06									+																		+							
ЗК07				+			+		+																									
ЗК08									+	+																								+
СК01									+																		+				+			+
СК02								+		+		+	+	+	+	+		+	+	+		+			+		+		+			+	+	
СК03											+									+	+		+			+						+	+	
СК04																+		+						+		+				+				
СК05										+		+					+					+			+			+	+	+				
СК06											+				+								+											
СК07														+													+				+	+	+	
СК08																						+		+	+				+		+	+	+	
СК09														+			+				+							+		+				
СК10																											+	+				+	+	
СК11																			+	+												+	+	
СК12												+	+	+	+	+		+		+		+							+	+	+	+	+	

МАТРИЦЯ ЗАБЕЗПЕЧЕННЯ ПРОГРАМНИХ РЕЗУЛЬТАТІВ НАВЧАННЯ ВІДПОВІДНИМИ ОСВІТНІМИ КОМПОНЕНТАМИ ОСВІТНЬОЇ ПРОГРАМИ

Освітні компоненти / Програмні результати навчання	ОК.01	ОК.02	ОК.03	ОК.04	ОК.05	ОК.06	ОК.07	ОК.08	ОК.09	ОК.10	ОК.11	ОК.12	ОК.13	ОК.14	ОК.15	ОК.16	ОК.17	ОК.18	ОК.19	ОК.20	ОК.21	ОК.22	ОК.23	ОК.24	ОК.25	ОК.26	ОК.27	ОК.28	ОК.29	ОК.30	ОК.31	ОК.32	ОК.33	ОК.34
ПРН01			+	+	+																													
ПРН02	+					+		+					+				+		+								+				+		+
ПРН03	+	+	+						+				+				+		+								+				+		
ПРН04	+	+														+	+						+			+	+			+		+	+	+
ПРН05																				+		+			+				+			+		
ПРН06	+					+				+		+	+						+		+						+					+	+	+
ПРН07									+																					+	+			
ПРН08									+													+									+			
ПРН09									+					+								+								+	+			
ПРН10														+			+		+															+
ПРН11	+													+						+	+						+						+	
ПРН12																										+								
ПРН13														+																				
ПРН14								+							+										+		+		+					+
ПРН15																		+		+														
ПРН16																						+					+							
ПРН17											+																+							
ПРН18																											+		+					
ПРН19								+		+				+	+	+		+			+				+		+	+	+	+				
ПРН20								+				+								+														
ПРН21																						+												
ПРН22															+			+			+	+			+		+		+		+			

Освітні компоненти / Програмні результати навчання	ОК.01	ОК.02	ОК.03	ОК.04	ОК.05	ОК.06	ОК.07	ОК.08	ОК.09	ОК.10	ОК.11	ОК.12	ОК.13	ОК.14	ОК.15	ОК.16	ОК.17	ОК.18	ОК.19	ОК.20	ОК.21	ОК.22	ОК.23	ОК.24	ОК.25	ОК.26	ОК.27	ОК.28	ОК.29	ОК.30	ОК.31	ОК.32	ОК.33	ОК.34
ПРН23										+				+					+															
ПРН24																					+						+							
ПРН25																				+							+							
ПРН26														+	+										+				+					
ПРН27												+							+						+				+					
ПРН28																	+								+	+			+		+	+	+	+
ПРН29												+								+						+							+	+
ПРН30														+	+	+		+				+		+		+	+			+				+
ПРН31											+		+			+		+			+		+					+		+				
ПРН32														+				+				+		+										
ПРН33																+										+				+				
ПРН34										+				+		+						+	+	+						+				
ПРН35											+												+											
ПРН36		+											+																					
ПРН37													+																					
ПРН38													+									+											+	
ПРН39																											+			+	+			
ПРН40																						+										+		
ПРН41																				+					+		+		+		+			
ПРН42																	+	+							+				+					
ПРН43									+			+																		+				+
ПРН44																+										+				+				
ПРН45																						+				+								+
ПРН46																		+							+	+	+		+					
ПРН47																									+		+	+	+					

Освітні компоненти / Програмні результати навчання	ОК.01	ОК.02	ОК.03	ОК.04	ОК.05	ОК.06	ОК.07	ОК.08	ОК.09	ОК.10	ОК.11	ОК.12	ОК.13	ОК.14	ОК.15	ОК.16	ОК.17	ОК.18	ОК.19	ОК.20	ОК.21	ОК.22	ОК.23	ОК.24	ОК.25	ОК.26	ОК.27	ОК.28	ОК.29	ОК.30	ОК.31	ОК.32	ОК.33	ОК.34
ПРН48																				+					+		+	+	+					
ПРН49																				+									+					
ПРН50																								+										
ПРН51																					+	+												
ПРН52													+		+			+		+														
ПРН53								+																										+
ПРН54									+																									
ПРН55							+																											

МАТРИЦЯ ФОРМУВАННЯ НАВИЧОК ТА КОМПЕТЕНТНОСТЕЙ, СПРЯМОВАНИХ НА ДОСЯГНЕННЯ ЦІЛЕЙ СТАЛОГО РОЗВИТКУ ВІДПОВІДНИМИ ОСВІТНІМИ КОМПОНЕНТАМИ ОСВІТНЬОЇ ПРОГРАМИ

Цілі сталого розвитку / Освітні компоненти	ЦІЛЬ 1	ЦІЛЬ 2	ЦІЛЬ 3	ЦІЛЬ 4	ЦІЛЬ 5	ЦІЛЬ 6	ЦІЛЬ 7	ЦІЛЬ 8	ЦІЛЬ 9	ЦІЛЬ 10	ЦІЛЬ 11	ЦІЛЬ 12	ЦІЛЬ 13	ЦІЛЬ 14	ЦІЛЬ 15	ЦІЛЬ 16	ЦІЛЬ 17
ОК.01				+				+	+								
ОК.02				+			+		+								
ОК.03				+				+									+
ОК.04				+				+								+	
ОК.05				+				+									+
ОК.06				+				+	+								
ОК.07			+	+							+						
ОК.08				+				+	+								
ОК.09				+												+	+
ОК.10				+					+							+	
ОК.11				+					+			+					
ОК.12				+					+							+	
ОК.13				+					+							+	
ОК.14				+					+								+
ОК.15				+					+							+	
ОК.16									+							+	+
ОК.17				+					+							+	
ОК.18				+					+							+	
ОК.19				+				+	+								
ОК.20									+		+					+	

Цілі сталого розвитку / Освітні компоненти	ЦІЛЬ 1	ЦІЛЬ 2	ЦІЛЬ 3	ЦІЛЬ 4	ЦІЛЬ 5	ЦІЛЬ 6	ЦІЛЬ 7	ЦІЛЬ 8	ЦІЛЬ 9	ЦІЛЬ 10	ЦІЛЬ 11	ЦІЛЬ 12	ЦІЛЬ 13	ЦІЛЬ 14	ЦІЛЬ 15	ЦІЛЬ 16	ЦІЛЬ 17
ОК.21								+	+							+	
ОК.22								+	+							+	
ОК.23									+		+					+	
ОК.24									+		+					+	
ОК.25								+	+							+	
ОК.26								+	+							+	
ОК.27									+							+	+
ОК.28				+					+							+	
ОК.29									+							+	+
ОК.30								+	+							+	
ОК.31								+	+							+	
ОК.32				+				+	+								
ОК.33				+				+									+
ОК.34				+				+								+	

Перелік нормативних документів, на яких базується освітня програма

1. 1. Про вищу освіту: Закон України. URL: http://zakon4.rada.gov.ua/laws/show/1556-18.
2. 2. Про освіту: Закон України. URL: http://zakon5.rada.gov.ua/laws/show/2145-19.
3. 3. Закон України «Про захист персональних даних». URL: https://zakon.rada.gov.ua/laws/show/2297-17.
4. 4. Закон України «Про доступ до публічної інформації». URL: https://zakon.rada.gov.ua/laws/show/2939-17.
5. 5. Закон України «Про основні засади забезпечення кібербезпеки України». URL: https://zakon.rada.gov.ua/laws/show/2163-19.
6. 6. Закон України «Про захист інформації в інформаційно-комунікаційних системах». URL: https://zakon.rada.gov.ua/laws/show/80/94-%D0%B2%D1%80.
7. 7. Закон України «Про державну таємницю». URL: https://zakon.rada.gov.ua/laws/show/3855-12.
8. 8. Закон України «Про науково-технічну інформацію». URL: https://zakon.rada.gov.ua/laws/show/3322-12.
9. 9. Постанова Кабінету Міністрів України від 19 червня 2019 року № 518 «Про затвердження Загальних вимог до кіберзахисту об’єктів критичної інфраструктури». URL: https://zakon.rada.gov.ua/laws/show/518-2019-п.
10. 10. Національний класифікатор України: Класифікатор професій ДК 003:2010 (із змінами). URL: https://zakon.rada.gov.ua/rada/show/327609-10.
11. 11. Постанова Кабінету Міністрів України від 23 листопада 2011 р. № 1341 (із змінами) «Про затвердження Національної рамки кваліфікацій». URL: http://zakon4.rada.gov.ua/laws/show/1341-2011-п.
12. 12. Постанова Кабінету Міністрів України від 29 квітня 2015 р. № 266 «Про затвердження переліку галузей знань і спеціальностей, за якими здійснюється підготовка здобувачів вищої освіти». URL: http://zakon4.rada.gov.ua/laws/show/266-2015-р.
13. 13. Постанова 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». URL: https://www.kmu.gov.ua/npas/pro-vnesennia-zmin-do-pereliku-haluzei-zna-ii6-1222-1392.
14. 14. Наказ Міністерства освіти і науки України від 01.06.2017 р. № 600 (у редакції наказу Міністерства освіти і науки України від 30.04.2020 р. № 584) «Про затвердження Методичних рекомендацій щодо розроблення освітніх програм». URL: https://mon.gov.ua/storage/app/media/vishcha/naukovometodychna/rada/2020-metod-rekomendacziyi.docx.
15. 15. Закон України «Про академічну доброчесність» від 18.12.2025 № 4742-IX. URL: https://zakon.rada.gov.ua/laws/show/4742-20#Text