


**МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ЛУЦЬКИЙ НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ
ВІДОКРЕМЛЕНИЙ СТРУКТУРНИЙ ПІДРОЗДІЛ
«ТЕХНІЧНИЙ ФАХОВИЙ КОЛЕДЖ ЛУЦЬКОГО НАЦІОНАЛЬНОГО
ТЕХНІЧНОГО УНІВЕРСИТЕТУ»**


ПОГОДЖУЮ

Директор
Відокремленого структурного підрозділу
«Технічний фаховий коледж Луцького
національного технічного університету»
кандидат технічних наук, доцент

 Олег ГЕРАСИМЧУК
«23» квітня 2024 р.

ЗАТВЕРДЖУЮ

Ректор
Луцького національного технічного
університету
доктор економічних наук, професор

 Ірина ВАХОВИЧ
«26» квітня 2024 р.



ОСВІТНЬО-ПРОФЕСІЙНА ПРОГРАМА

«ЗАХИСТ ТА БЕЗПЕКА ІНФОРМАЦІЙНИХ СИСТЕМ»

підготовки здобувачів фахової передвищої освіти
освітньо-професійного ступеня фаховий молодший бакалавр

ГАЛУЗЬ ЗНАНЬ 12 ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ

СПЕЦІАЛЬНІСТЬ 125 КІБЕРБЕЗПЕКА ТА ЗАХИСТ ІНФОРМАЦІЇ

КВАЛІФІКАЦІЯ ФАХОВИЙ МОЛОДШИЙ БАКАЛАВР

З КІБЕРБЕЗПЕКИ

СХВАЛЕНО

Педагогічною радою Відокремленого
структурного підрозділу «Технічний
фаховий коледж Луцького
національного технічного
університету»

протокол № 6 від 23 квітня 2024 р.

ЗАТВЕРДЖЕНО

Вченою радою Луцького національного
технічного університету

протокол № 10 від 26 квітня 2024 р.

Луцьк 2024 р.

ЛИСТ ПОГОДЖЕННЯ

освітньо-професійної програми

«ЗАХИСТ ТА БЕЗПЕКА ІНФОРМАЦІЙНИХ СИСТЕМ»

Освітньо-професійний ступінь – фаховий молодший бакалавр

Галузь знань – 12 Інформаційні технології

Спеціальність – 125 Кібербезпека та захист інформації

Кваліфікація – фаховий молодший бакалавр з кібербезпеки


Освітньо-професійна програма розглянута на засіданні циклової комісії комп'ютерних систем та інформаційних технологій ТФК ЛНТУ

Протокол №10 від «17» квітня 2024 р.

Голова циклової комісії

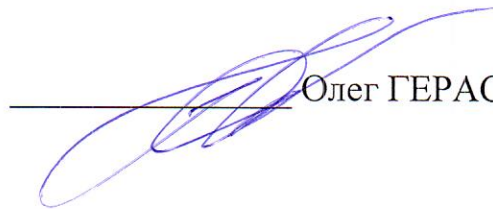

Петро ВОВК

Голова групи забезпечення
освітньо-професійної програми,
керівник проектної групи


Олександр КЛЕХА

Схвалено педагогічної радою ТФК ЛНТУ
Протокол № 6 від «23» квітня 2024 р.

Голова педагогічної ради
ТФК ЛНТУ


Олег ГЕРАСИМЧУК

ЗМІСТ

1. Передмова.
2. Профіль освітньо-професійної програми із спеціальності 125 Кібербезпека та захист інформації.
3. Перелік компонент освітньо-професійної програми та їх логічна послідовність.
 - 3.1. Перелік компонент освітньо-професійної програми.
 - 3.2. Структурно-логічна схема освітньо-професійної програми.
4. Матриця відповідності компетентностей освітньо-професійної програми дескрипторам НРК.
5. Матриця відповідності програмних результатів навчання та компетентностей освітньо-професійної програми.
6. Матриця відповідності компетентностей освітньо-професійної програми освітнім компонентам.
7. Матриця забезпечення програмних результатів навчання відповідним компонентам освітньо-професійної програми.
8. Форма атестації здобувачів фахової передвищої освіти.
9. Вимоги до наявності системи внутрішнього забезпечення якості фахової передвищої освіти.
10. Перелік нормативних документів, на яких базується освітньо-професійна програма фахової передвищої освіти.

1. Передмова

Освітньо-професійна програма (ОПП) «Захист та безпека інформаційних систем» для підготовки здобувачів фахової передвищої освіти за спеціальністю 125 Кібербезпека та захист інформації містить обсяг кредитів ЄКТС, необхідний для здобуття відповідного ступеня фахової передвищої освіти; перелік компетентностей випускника; нормативний зміст підготовки здобувачів фахової передвищої освіти, сформульований у термінах результатів навчання; форми атестації здобувачів фахової передвищої освіти; вимоги до наявності системи внутрішнього забезпечення якості фахової передвищої освіти.

Вперше затверджено і введено в дію 23 квітня 2024 року на підставі засідання педагогічної ради Відокремленого структурного підрозділу «Технічний фаховий коледж Луцького технічного університету», протокол №6.

Освітньо-професійну програму розроблено членами проектної групи у складі:

Клеха Олександр Васильович – спеціаліст вищої категорії, викладач спецдисциплін Відокремленого структурного підрозділу «Технічний фаховий коледж Луцького національного технічного університету» – голова проектної групи.

Костючко Сергій Миколайович – кандидат технічних наук, доцент, спеціаліст вищої категорії, викладач спецдисциплін Відокремленого структурного підрозділу «Технічний фаховий коледж Луцького національного технічного університету» – член проектної групи.

Багнюк Наталія Володимирівна – кандидат технічних наук, доцент, спеціаліст, викладач спецдисциплін Відокремленого структурного підрозділу «Технічний фаховий коледж Луцького національного технічного університету» – член проектної групи.

Освітньо-професійна програма (ОПП) «Захист та безпека інформаційних систем» є нормативним документом ТФК ЛНТУ, у якому визначається нормативний зміст навчання, встановлюються вимоги до змісту, обсягу й рівня освіти та професійної підготовки фахового молодшого бакалавра галузі знань 12 Інформаційні технології спеціальності 125 Кібербезпека та захист інформації.

Освітньо-професійна програма «Захист та безпека інформаційних систем» використовується під час:

- ліцензування та акредитації освітньо-професійної програми, інспектуванні освітньої діяльності за спеціальністю;
- розробки навчального плану, робочих навчальних планів, програм навчальних дисциплін й практик;
- розробки засобів діагностики якості фахової передвищої освіти;
- професійної орієнтації здобувачів освіти;
- формування індивідуальних планів здобувачів освіти;
- атестації фахових молодших бакалаврів спеціальності 125 Кібербезпека та захист інформації.

Освітньо-професійна програма «Захист та безпека інформаційних систем» враховує вимоги Законів України «Про освіту», «Про фахову передвищу освіту», Національної рамки кваліфікацій і встановлює:

- обсяг та термін навчання фахового молодшого бакалавра;
- загальні компетенції фахового молодшого бакалавра;
- професійні компетенції за зазначеною спеціальністю;
- перелік та обсяг навчальних дисциплін для опанування компетентностей освітньої програми;
- вимоги до структури навчальних дисциплін.

Користувачі освітньо-професійної програми:

- здобувачі фахової передвищої освіти;
- викладачі, які здійснюють підготовку фахових молодших бакалаврів за освітньо-професійною програмою «Захист та безпека інформаційних систем» із спеціальності 125 Кібербезпека та захист інформації;
- екзаменаційна комісія спеціальності 125 Кібербезпека та захист інформації;
- приймальна комісія ТФК ЛНТУ.

Освітньо-професійна програма спеціальності 125 Кібербезпека та захист інформації поширюється на циклові комісії коледжу, що здійснюють підготовку здобувачів фахової передвищої освіти ступеня фаховий молодший бакалавр за освітньо-професійною програмою «Захист та безпека інформаційних систем» із спеціальності 125 Кібербезпека та захист інформації.

2. Профіль освітньо-професійної програми «Захист та безпека інформаційних систем» зі спеціальності 125 Кібербезпека та захист інформації галузі знань 12 Інформаційні технології

I. Загальна характеристика	
Повна назва закладу фахової передвищої освіти та випускової циклової комісії	Відокремлений структурний підрозділ «Технічний фаховий коледж Луцького національного технічного університету», код в ЄДЕБО – 778 циклова комісія комп'ютерних систем та інформаційних технологій
Рівень освіти	фахова передвища
Освітньо-професійний ступінь	фаховий молодший бакалавр
Галузь знань	12 Інформаційні технології
Спеціальність	125 Кібербезпека та захист інформації
Форма здобуття освіти	Денна
Освітня кваліфікація	фаховий молодший бакалавр з кібербезпеки
Професійна кваліфікація	не надається
Наявність акредитації	ОПП не акредитована
Термін дії освітньо-професійної програми	До чергового перегляду
Цикл/рівень	НРК України – 5 рівень, FQ-ЕНЕА – початковий (короткий цикл), EQF LLL – 5 рівень
Вимоги до осіб, які можуть розпочати навчання за програмою	Повна загальна середня освіта. Решта вимог визначаються правилами прийому на освітньо-професійну програму фахового молодшого бакалавра
Обсяг освітньо-професійної програми	180 кредитів ЄКТС Термін навчання 2 роки 10 місяців (на базі ПЗСО)
Мова викладання	Українська
Інтернет - адреса постійного розміщення опису освітньо-професійної програми	https://tk.lntu.edu.ua
II. Мета освітньо-професійної програми	
Полягає у підготовці фахівців здатних розв'язувати типові та спеціалізовані професійні завдання з інформаційної безпеки та/або кібербезпеки, підвищувати ефективність захисту існуючих інформаційних систем виробництва,	

обслуговувати системи захисту та безпеки в процесі професійної діяльності або навчання.

III. Характеристика освітньо-професійної програми

Предметна область	<p>Об'єкт:</p> <ul style="list-style-type: none">- 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. <p>Цілі навчання: формування та розвиток загальних і професійних компетентностей у фахівців, здатних формулювати та розв'язувати завдання, пов'язані з захистом та безпекою інформаційних систем.</p> <p>Теоретичний зміст предметної області:</p> <ul style="list-style-type: none">- законодавча, нормативно-правова база України та вимоги відповідних міжнародних стандартів і практик щодо здійснення професійної діяльності;- принципи супроводу систем та комплексів інформаційної та/або кібербезпеки;- теорії, моделі та принципи управління доступом до інформаційних ресурсів;- теорії систем управління інформаційною та/або кібербезпекою;- методи та засоби виявлення, управління та ідентифікація ризиків;- методи та засоби оцінювання та забезпечення необхідного рівня захищеності інформації;- методи та засоби технічного та криптографічного захисту інформації;- сучасні інформаційно-комунікаційні технології;- сучасне програмно-апаратне забезпечення захисту і безпеки інформаційних систем. <p>Методи, методики та технології:</p> <ul style="list-style-type: none">- методи, методики та технології захисту та безпеки інформаційних систем;- методи збору, обробки, аналізу, моделювання та інтерпретації результатів досліджень у галузі інформаційних технологій. <p>Інструменти та обладнання:</p> <ul style="list-style-type: none">- системи розробки, забезпечення, моніторингу та контролю процесів інформаційної та/або кібербезпеки;- сучасне програмно-апаратне забезпечення інформаційно-комунікаційних технологій.
Особливості	Освітньо-професійна програма спрямована на підготовку

освітньо-професійної програми	<p>висококваліфікованих здобувачів освіти освітньо-професійного ступеня фаховий молодший бакалавр з захисту та безпеки інформаційних систем шляхом здобуття фундаментальних, теоретико-методичних, фахових знань, практичних умінь, навичок та інших компетентностей, достатніх для розв'язування типових спеціалізованих задач у професійній діяльності.</p> <p>Унікальність освітньо-професійної програми полягає у використанні хмарних технологій захисту та безпеки інформаційних систем з акцентом на системах Internet of things, Cloud сервісах, Big Data (сховищ), супроводі систем і компонентів захисту та безпеки загального та спеціального призначення, створення та супроводу інтелектуальних програмних рішень захисту.</p>
IV. Придатність випускників до працевлаштування та подальшого навчання	
Академічні права випускників	<p>Можливість продовження навчання за початковим (короткий цикл) та першим (бакалаврським) рівнем вищої освіти. Набуття додаткових кваліфікацій у системі освіти дорослих.</p>
Працевлаштування випускників	<p>Після підготовки фахівцю присвоюється освітня кваліфікація – фаховий молодший бакалавр з кібербезпеки, він здатний виконувати зазначену в класифікаторі професій ДК 003:2010 професійну роботу і може займати відповідну первинну посаду:</p> <ul style="list-style-type: none"> - 3119 - технік (сфера захисту інформації); - 3439 - фахівець із організації інформаційної безпеки; - 3439 - фахівець із організації захисту інформації з обмеженим доступом; - 3439 - фахівець з режиму секретності; - 3121 - фахівець з інформаційних технологій.
V. Викладання та оцінювання	
Викладання та навчання	<p>Комбінація лекцій, практичних та семінарських занять, лабораторних робіт із використанням студентоорієнтованого, проблемно-орієнтованого, професійно-орієнтованого навчання, міждисциплінарних тренінгів та майстер-класів (за потреби: з елементами дистанційного навчання); участь у наукових студентських конференціях, конкурсах, що дають змогу розвивати практичні компетенції та адаптують до інтерактивних, інформаційно-комунікаційних освітніх технологій.</p> <p>Невід'ємною складовою є самостійна робота, консультації із викладачами, навчальна, виробнича та технологічна практики.</p>
Оцінювання	<p>Оцінювання результатів навчання здобувачів освіти здійснюється за 4-х бальною шкалою («відмінно», «добре», «задовільно», «незадовільно»), вербальною («зараховано», «незараховано») шкалою.</p> <p>Види контролю: поточний та підсумковий.</p> <p>Форми контролю: усне та письмове опитування, тестові завдання, вирішення та презентації індивідуальних завдань,</p>

	захист лабораторних та індивідуальних робіт, захист звітів з практики, курсових робіт та/або проектів. Підсумковий контроль: заліки, диференційовані заліки та екзамени.
VI. Програмні компетентності	
Інтегральна компетентність (ІК)	Здатність вирішувати типові спеціалізовані задачі в галузі кібербезпеки або у процесі навчання, що вимагає застосування положень і методів відповідних наук та може характеризуватися певною невизначеністю умов; нести відповідальність за результати своєї діяльності; здійснювати контроль інших осіб у визначених ситуаціях.
Загальні компетентності (ЗК)	<p>ЗК1. Здатність застосовувати знання у різних практичних ситуаціях.</p> <p>ЗК2. Знання та розуміння предметної області та розуміння професії.</p> <p>ЗК3. Здатність професійно спілкуватися державною та іноземною мовами як усно, так і письмово.</p> <p>ЗК4. Вміння виявляти, ставити та вирішувати проблеми за професійним спрямуванням.</p> <p>ЗК5. Здатність до пошуку, оброблення та аналізу інформації.</p> <p>ЗК6. Здатність реалізувати свої права і обов'язки як члена суспільства, усвідомлювати цінності громадянського суспільства та необхідність його сталого розвитку, верховенства права, прав і свобод людини і громадянина в Україні.</p> <p>ЗК7. 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.</p> <p>ЗК8. Здатність використовувати різні види та форми рухової активності для активного відпочинку та ведення здорового способу життя.</p> <p>ЗК9. Здатність до роботи в команді.</p>
Спеціальні компетентності (СК)	<p>СК1. Здатність застосовувати законодавчу та нормативно-правову базу, а також державні та міжнародні вимоги, рекомендовані практики і стандарти з метою здійснення професійної діяльності в галузі кібербезпеки.</p> <p>СК2. Здатність до використання інформаційно-комунікаційних технологій, сучасних методів і моделей кібербезпеки.</p> <p>СК3. Здатність до розробки та використання програмних та програмно-апаратних засобів захисту інформації для забезпечення кібербезпеки.</p> <p>СК4. Здатність забезпечувати працездатність інформаційно-комунікаційних систем згідно встановленої політики кібербезпеки.</p> <p>СК5. Здатність забезпечувати захист інформації для реалізації</p>

	<p>встановленої політики кібербезпеки установи чи підприємства.</p> <p>СК6. Здатність відновлювати штатне функціонування інформаційно-комунікаційних систем після реалізації кіберзагроз, збоїв і відмов різних класів та походження.</p> <p>СК7. Здатність забезпечувати функціонування комплексних систем захисту інформації.</p> <p>СК8. Здатність здійснювати протидію несанкціонованому проникненню в інформаційно-комунікаційні системи і мережі.</p> <p>СК9. Здатність здійснювати процедури управління інцидентами, проводити розслідування, надавати їм оцінку.</p> <p>СК10. Здатність застосовувати методи та засоби криптографічного, стенографічного і технічного захисту інформації.</p> <p>СК11. Здатність виконувати моніторинг процесів функціонування та тестування інформаційно-комунікаційних систем згідно встановленої політики кібербезпеки.</p> <p>СК12. Здатність застосовувати теоретичні знання та практичні навички з організації та функціонування сучасних операційних систем, уміння зі створення та використання безпечного програмного забезпечення для керування обчислювальними ресурсами в багатокористувацьких операційних системах.</p> <p>СК13. Здатність виявляти та оцінювати можливі загрози, уразливості та дестабілізуючі чинники інформаційному простору та інформаційним ресурсам згідно з встановленою політикою інформаційної та/або кібербезпеки.</p> <p>СК14. Здатність вибору захищених хмарних платформ та сервісів, безпечного розгортання на них, інтегрування, адміністрування і супроводу інформаційних систем.</p>
VII. Програмні результати навчання	
<p>Результати навчання</p>	<p>РН1. Знати законодавчу та нормативно-правову базу України та вимоги відповідних стандартів, у тому числі міжнародних в галузі інформаційної безпеки та/або кібербезпеки.</p> <p>РН2. Знати національні та міжнародні стандарти, регулюючі акти виявлення, ідентифікації, аналізу та реагування на інциденти в сфері інформаційної безпеки та/або кібербезпеки.</p> <p>РН3. Знати державну та іноземні мови з метою забезпечення ефективності професійної комунікації.</p> <p>РН4. Вміти адаптуватися до умов частотої зміни технологій професійної діяльності, прогнозувати кінцевий результат.</p> <p>РН5. Вміти використовувати сучасні програмні та програмно-апаратні комплекси захисту інформаційних ресурсів.</p> <p>РН6. Вміти використовувати результати самостійного пошуку, аналізу та синтезу інформації з різних джерел для ефективного рішення спеціалізованих задач професійної діяльності.</p> <p>РН7. Знати основні методи розробки моделі загроз та порушника.</p> <p>РН8. Вміти використовувати комплексні системи захисту</p>

інформації в автоматизованих системах (АС) організації (підприємства) відповідно до вимог нормативно-правових документів.

РН9. Знати теорію та методи захисту для забезпечення безпеки інформації в інформаційно-телекомунікаційних системах.

РН10. Вміти забезпечувати функціонування спеціального програмного забезпечення, щодо захисту інформації від руйнуючих програмних впливів, руйнуючих кодів в інформаційно-телекомунікаційних системах.

РН11. Вміти впроваджувати заходи щодо попередження отримання несанкціонованого доступу і захисту інформаційних, інформаційно-телекомунікаційних (автоматизованих) систем на основі еталонної моделі взаємодії відкритих систем згідно зі встановленою політикою інформаційної безпеки та/або кібербезпеки.

РН12. Вміти вирішувати задачі щодо управління доступом до інформаційних ресурсів та процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах на основі моделей управління доступом (мандатних, дискреційних, рольових).

РН13. Вміти вирішувати задачі захисту потоків даних в інформаційних, інформаційно-телекомунікаційних (автоматизованих) системах, в тому числі з використанням сучасних методів та засобів криптографічного захисту інформації.

РН14. Вміти вирішувати задачі управління процесами відновлення штатного функціонування інформаційно-телекомунікаційних систем з використанням процедур резервування згідно встановленої політики безпеки.

РН15. Вміти 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.

РН16. Знати системи виявлення вторгнень та використовувати компоненти криптографічного захисту для забезпечення необхідного рівня захищеності інформації в інформаційно-телекомунікаційних системах.

РН17. Вміти підтримувати працездатність з використанням інструментарію для моніторингу процесів в інформаційно-телекомунікаційних системах.

РН18. Вміти вирішувати задачі аналізу програмного коду на наявність можливих загроз.

РН19. Вміти вирішувати задачі безпеки функціонування інформаційних систем, розгорнутих на хмарних платформах.

VIII. Ресурсне забезпечення реалізації освітньо-професійної програми

Кадрове забезпечення	<p>Група забезпечення – це педагогічні працівники, які мають кваліфікацію відповідно до спеціальності, працюють в коледжі за основним місцем роботи, мають стаж педагогічної роботи, пройшли чергову атестацію, підвищили або підтвердили свою кваліфікаційну категорію.</p> <p>В процесі організації освітнього процесу залучаються фахівці з кібербезпеки з досвідом дослідницької, управлінської та практичної роботи.</p> <p>Циклова комісія нараховує 16 педагогічних працівників, з них 5 з вищою кваліфікаційною категорією (3 викладачі методисти), 3 кандидати наук. Інші циклові комісії, задіяні в підготовці за освітньо-професійною програмою «Захист та безпека інформаційних систем», також мають висококваліфікованих педагогічних працівників.</p>
Матеріально-технічне забезпечення	<p>Забезпеченість навчальними приміщеннями, комп'ютерними робочими місцями, мультимедійним обладнанням відповідає потребі та повністю забезпечує освітній процес протягом усього циклу підготовки за освітньо-професійною програмою.</p> <p>В ТФК ЛНТУ використовуються комп'ютерні та спеціалізовані лабораторії, френд-зона, встановлено локальні комп'ютерні мережі, бездротовий доступ до мережі Інтернет.</p> <p>Наявна вся необхідна соціально-побутова інфраструктура: бібліотека, у тому числі читальна зала, медичний пункт, їдальня, актові та конференц зали, спортивний зал та спортивний майданчик.</p>
Інформаційне та навчально-методичне забезпечення	<p>Офіційний веб-сайт коледжу (https://tk.lntu.edu.ua) містить інформацію про освітньо-професійні програми, навчальну, наукову і виховну діяльність, діяльність студентського самоврядування, структурні підрозділи коледжу, правила прийому, контакти тощо.</p> <p>Електронний варіант навчально методичних комплексів навчальних дисциплін (методичні вказівки до виконання практичних, лабораторних та самостійних робіт, конспекти лекцій) розміщено на Інформаційному порталі коледжу (https://e-tk.lntu.edu.ua/), доступ до якого мають всі учасники освітнього процесу.</p> <p>Бібліотека, у т.ч. читальний зал – 71,4 м²; читальна зала коледжу передбачає 30 посадкових місць; загальний бібліотечний фонд складає 18795 примірників наукової, технічної, навчальної, художньої літератури, періодичних видань, словників, довідкової літератури, серед них і наукові фахові журнали в кількості 11 найменувань.</p>

3. Перелік компонентів освітньо-професійної програми та їх логічна послідовність

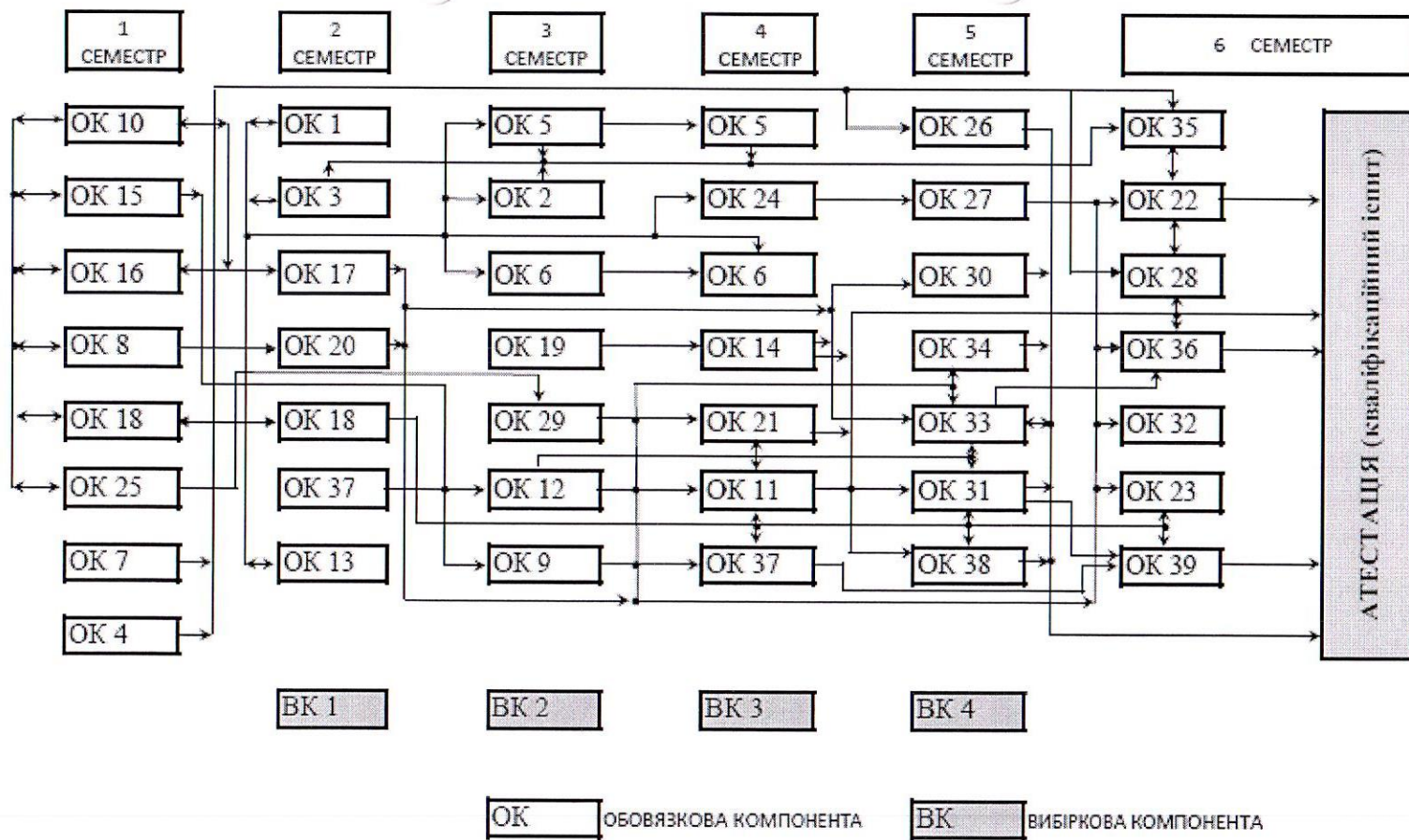
3.1. Перелік компонентів освітньо-професійної програми

Код н/д	Компоненти освітньо-професійної програми	Кількість кредитів	Форма підсумкового контролю
1. Обов'язкові компоненти ОПП			
1.1. Цикл загальної підготовки			
ОК 1	Історія України (від найдавніших часів до сьогодення)	3	Екзамен
ОК 2	Українська мова (за професійним спрямуванням)	3	Екзамен
ОК 3	Соціологія	3	Диф. залік
ОК 4	Основи комунікації	3	Диф. залік
ОК 5	Іноземна мова (за професійним спрямуванням)	6	Диф. залік, екзамен
ОК 6	Фізичне виховання	4	Диф. залік, диф. залік
ОК 7	Правознавство	3	Залік
ОК 8	Web-технології	4	Диф. залік
ОК 9	Вища математика та теорія ймовірності	4	Екзамен
ОК 10	Вступ до спеціальності	4	Диф. залік
ОК 11	Дискретна математика	3	Екзамен
ОК 12	Алгоритми і структури даних	4	Диф. залік
ОК 13	Економічна теорія	3	Диф. залік
ОК 14	Психологічні аспекти кібербезпеки	3	Диф. залік
ОК 15	Стандартизація та сертифікація в галузі ІТ	3	Диф. залік
Всього за циклом загальної підготовки		53	-
1.2. Цикл професійної підготовки			
ОК 16	Основи інформаційної безпеки	4	Диф. залік
ОК 17	Нормативно-правове забезпечення інформаційної безпеки	4	Екзамен
ОК 18	Основи програмування	8	Диф. залік, екзамен
ОК 19	Комп'ютерна вірусологія та антивірусний захист	4	Диф. залік
ОК 20	Кодування інформації та архітектура комп'ютерів	4,5	Екзамен
ОК 21	Комп'ютерні мережі	4	Екзамен
ОК 22	Організація та безпека баз даних (КР)	5	Екзамен, КР
ОК 23	Охорона праці та безпека життєдіяльності	3	Екзамен
ОК 24	Комп'ютерна схемотехніка та електроніка	4	Екзамен
ОК 25	Операційні системи та системне програмне забезпечення	5	Екзамен
ОК 26	Комплексні системи захисту інформації	3,5	Диф. залік
ОК 27	Сигнали і процеси в системах захисту інформації	3	Диф. залік
ОК 28	Якість та тестування інформаційних систем	4	Екзамен
ОК 29	Захист інформації (КР)	6	Екзамен
ОК 30	Адміністрування комп'ютерних систем та мереж	3	Екзамен
ОК 31	Системи технічного захисту інформації (КР)	5	Екзамен, КР
ОК 32	Безпека інтернету речей (IoT)	3	Диф. залік
ОК 33	Безпека безпроводових мереж	3	Диф. залік
ОК 34	Аналіз вразливостей інформаційних систем	3	Диф. залік
ОК 35	Безпека Web ресурсів	3	Диф. залік
ОК 36	Безпека хмарних платформ та сервісів	3	Диф. залік
Всього за циклом професійної підготовки		85	-

1.3 Цикл практичної підготовки			
ОК 37	Навчальна практика	10,5	Диф. залік, диф. залік
ОК 38	Виробнича практика	4,5	Диф. залік
ОК 39	Технологічна практика	6	Диф. залік
ОК40	Атестація	3	кваліфікаційний іспит
Всього за циклом практичної підготовки		24	
Всього за циклом нормативних дисциплін		162	
Вибіркові навчальні компоненти			
2.1.Цикл загальної підготовки за вибором студента			
ВК 1	Загальна вибіркова дисципліна №1 (підприємництво та бізнес-культура, правове регулювання підприємницької діяльності, фінансова грамотність)	4	Диф. залік
ВК 2	Загальна вибіркова дисципліна №2 (маркетинг в соціальних мережах, основи креативного менеджменту, лідерство та командотворення)	4	Диф. залік
Всього за циклом загальної підготовки		8	
2.2.Цикл професійної підготовки за вибором студента			
ВК 3	Фахова вибіркова дисципліна №3 (криптовалюти та технологія BLOCKCHAIN, основи інформаційної гігієни, взаємодія зі штучним інтелектом)	5	Диф. залік
ВК 4	Фахова вибіркова дисципліна №4 (основи шифрування та криптографії, клієнт-серверна взаємодія, моніторинг та логування)	5	Диф. залік
Всього за циклом професійної підготовки		10	
Всього вибіркові освітні компоненти за вибором студента		18	
Разом		180	

3.2. Структурно-логічна схема освітньо-професійної програми

Курс	Семестр	Обов'язкові компоненти освітньої програми	Кількість обов'язкових компонентів за семестр	Кількість вибірових компонентів за семестр	Кількість компонентів за навчальний рік (з них обов'язкових)
1	1	ОК4, ОК7, ОК8, ОК10, ОК15, ОК16, ОК18, ОК25	8	0	8 (8)
	2	ОК1, ОК3, ОК13, ОК17, ОК18, ОК20, ОК37, ВК1	7	1	8 (7)
2	3	ОК2, ОК5, ОК6, ОК9, ОК12, ОК19, ОК29, ВК2	7	1	8 (7)
	4	ОК5, ОК6, ОК11, ОК14, ОК21, ОК24, ОК37, ВК3	7	1	8 (7)
3	5	ОК26, ОК27, ОК30, ОК31, ОК33, ОК34, ОК38, ВК4	7	1	8 (7)
	6	ОК22, ОК23, ОК28, ОК32, ОК35, ОК36, ОК39, ОК40	8	0	8 (8)



4. Матриця відповідності компетентностей освітньо-професійної програми дескрипторам НРК

Класифікація компетентностей за НРК	Знання	Уміння /навички	Комунікація	Відповідальність та автономія
	ЗН1 Всебічні спеціалізовані емпіричні та теоретичні знання у сфері навчання та/або професійної діяльності, усвідомлення меж цих знань	УМ1 Широкий спектр когнітивних та практичних умінь/навичок, необхідних для розв'язання складних задач у спеціалізованих сферах професійної діяльності та/або навчання УМ2 Знаходження творчих рішень або відповідей на чітко визначені конкретні та абстрактні проблеми на основі ідентифікації та застосування даних УМ3 Планування, аналіз, контроль та оцінювання власної роботи та роботи інших осіб у спеціалізованому контексті	К1 Взаємодія з колегами, керівниками та клієнтами у питаннях, що стосуються розуміння, навичок та діяльності у професійній сфері та/або у сфері навчання К2 Донесення до широкого кола осіб (колеги, керівники, клієнти) власного розуміння, знань, суджень, досвіду, зокрема у сфері професійної діяльності	ВА1 Організація та нагляд (управління) в контекстах професійної діяльності або навчання в умовах непередбачуваних змін ВА2 Здатність продовжувати навчання з деяким ступенем автономії ВА3 Покращення результатів власної діяльності і роботи інших
Загальні компетентності (ЗК)				
ЗК1	ЗН1	УМ1	К1, К2	ВА2
ЗК2	ЗН1		К1, К2	ВА2
ЗК3	ЗН1		К1, К2	ВА2
ЗК4	ЗН1		К1, К2	ВА2
ЗК5	ЗН1	УМ1		ВА2
ЗК6	ЗН1	УМ2		ВА2
ЗК7	ЗН1	УМ1		ВА3
ЗК8	ЗН1			ВА2
ЗК9	ЗН1	УМ1	К1, К2	ВА3
Спеціальні компетентності (СК)				
СК1	ЗН1	УМ1		
СК2	ЗН1	УМ1	К1, К2	ВА2, ВА3
СК3	ЗН1	УМ1		ВА1, ВА2, ВА3
СК4	ЗН1	УМ 1, УМ 3	К1, К2	ВА1, ВА3
СК5	ЗН1	УМ1, УМ2	К1, К2	ВА2, ВА3
СК6	ЗН1	УМ1, УМ2	К1, К2	ВА1, ВА2, ВА3
СК7	ЗН1	УМ1, УМ2	К1, К2	ВА1, ВА2, ВА3
СК8	ЗН1	УМ1, УМ3	К1, К2	ВА1, ВА2, ВА3
СК9	ЗН1	УМ1, УМ3	К1, К2	ВА1, ВА2, ВА3
СК10	ЗН1	УМ1, УМ2, УМ3	К2	ВА1, ВА2, ВА3
СК11	ЗН1	УМ2, УМ3	К2	ВА2, ВА3
СК12	ЗН1	УМ1, УМ2, УМ3	К2	ВА2, ВА3
СК13	ЗН1	УМ1, УМ3	К1	ВА3
СК14	ЗН1	УМ1, УМ3	К1	ВА1, ВА2, ВА3

5. Матриця відповідності програмних результатів навчання та компетентностей освітньо-професійної програми

Результати навчання	Компетентності																						
	Загальні									Спеціальні													
	ЗК1	ЗК2	ЗК3	ЗК4	ЗК5	ЗК6	ЗК7	ЗК8	ЗК9	СК1	СК2	СК3	СК4	СК5	СК6	СК7	СК8	СК9	СК10	СК11	СК12	СК13	СК14
PH1			+		+	+	+			+													
PH2			+		+		+			+													+
PH3			+																				
PH4		+			+		+	+			+											+	
PH5	+			+				+			+	+	+		+			+		+			
PH6		+		+	+		+													+			+
PH7		+															+	+		+		+	
PH8	+			+				+			+	+		+		+							
PH9		+			+													+				+	
PH10	+			+							+	+	+	+					+	+	+		+
PH11	+			+				+			+		+	+	+		+						+
PH12	+			+				+			+		+	+			+				+		
PH13	+			+							+	+	+	+									
PH14	+			+							+	+	+		+					+			
PH15	+							+										+					
PH16	+	+						+				+					+	+	+		+	+	
PH17	+			+							+		+		+					+			
PH18	+			+	+						+	+								+	+		
PH19	+			+				+			+		+	+	+		+						+

Умовні позначення

+ - компетентність, яка набувається

ОК – обов’язковий загальний чи професійний компонент

ВК – вибіркового загальний чи професійний компонент

ЗК – загальна компетентність
ФК – фахова компетентність

6. Матриця відповідності компетентностей освітньо-професійної програми освітнім компонентам

	OK1	OK2	OK3	OK4	OK5	OK6	OK7	OK8	OK9	OK10	OK11	OK12	OK13	OK14	OK15	OK16	OK17	OK18	OK19	OK20	OK21	OK22	OK23	OK24	OK25	OK26	OK27	OK28	OK29	OK30	OK31	OK32	OK33	OK34	OK35	OK36	OK37	OK38	OK39	OK40	
ЗК1		+			+							+	+	+					+			+			+	+			+								+	+	+	+	
ЗК2										+				+		+				+	+	+			+	+	+		+	+	+	+	+	+	+	+	+	+	+	+	
ЗК3		+		+	+																																				+
ЗК4												+			+	+	+												+												+
ЗК5									+		+	+				+				+		+																			+
ЗК6	+		+	+			+						+				+																								+
ЗК7	+		+	+			+						+																												+
ЗК8						+																		+																	+
ЗК9				+									+								+			+			+		+									+			+
СК1							+								+		+																								+
СК2																			+		+											+	+	+		+	+		+	+	+
СК3							+											+	+	+				+	+		+					+	+		+	+		+	+	+	+
СК4																					+	+			+	+					+	+	+	+		+	+	+	+	+	+
СК5																+			+			+				+	+		+		+	+	+		+	+		+	+	+	+
СК6																					+	+				+	+				+	+						+	+	+	+
СК7																+									+			+		+	+						+			+	+
СК8													+		+				+		+	+				+		+		+		+								+	+
СК9				+											+	+									+																+
СК10							+	+		+	+							+		+				+	+		+	+		+							+			+	+
СК11												+	+			+						+		+	+		+	+		+				+				+	+	+	+
СК12																			+					+			+		+								+	+		+	+
СК13													+		+				+							+		+												+	+
СК14														+																+		+	+		+	+		+	+	+	+

Умовні позначення+

+ - компетентність, яка набувається

OK – обов'язковий загальний чи професійний компонент

ЗК – загальна компетентність

СК – спеціальна (фахова) компетентність

7. Матриця забезпечення програмних результатів навчання відповідним компонентам освітньо-професійної програми

	ОК1	ОК2	ОК3	ОК4	ОК5	ОК6	ОК7	ОК8	ОК9	ОК10	ОК11	ОК12	ОК13	ОК14	ОК15	ОК16	ОК17	ОК18	ОК19	ОК20	ОК21	ОК22	ОК23	ОК24	ОК25	ОК26	ОК27	ОК28	ОК29	ОК30	ОК31	ОК32	ОК33	ОК34	ОК35	ОК36	ОК37	ОК38	ОК39	ОК40					
PH1	+						+								+		+																								+				
PH2							+								+	+																										+			
PH3		+		+	+																																						+		
PH4			+					+		+				+		+				+		+	+			+			+								+						+		
PH5																				+			+			+			+											+			+		
PH6	+									+				+				+																					+			+		+	
PH7										+				+		+							+					+		+									+				+		
PH8																					+					+	+			+	+						+			+		+			
PH9								+		+	+	+				+		+		+								+		+									+				+		
PH10																+			+		+		+			+			+									+		+		+	+		
PH11						+															+		+	+	+	+				+					+				+		+	+			
PH12													+								+	+							+	+							+	+			+		+		
PH13									+		+	+				+		+	+	+				+				+											+				+		
PH14								+				+				+							+					+										+	+				+		
PH15									+				+		+		+												+	+											+		+		
PH16											+	+				+				+	+	+	+				+		+	+							+			+			+		
PH17																					+				+			+	+									+		+		+	+		
PH18								+											+	+	+									+								+			+		+		
PH19																																								+		+		+	+

Умовні позначення

+ - програмний результат, який забезпечується

ОК – обов'язків загальний чи професійний компонент

PH – програмні результати навчання

8. Форма атестації здобувачів фахової передвищої освіти

Форма атестації здобувачів фахової передвищої освіти	<p>Атестація випускників освітньо-професійної програми спеціальності 125 Кібербезпека та захист інформації здійснюється у формі кваліфікаційного іспиту.</p> <p>Після виконання навчального плану за освітньо-професійною програмою, здобувач освіти отримує документ про фахову передвищу освіту встановленого зразка про присудження освітньо-професійного ступеня фаховий молодший бакалавр з захисту та безпеки інформаційних систем</p>
Вимоги до кваліфікаційного іспиту	<p>Кваліфікаційний іспит спрямований на перевірку досягнення результатів навчання, визначених освітньо-професійною програмою спеціальності 125 Кібербезпека та захист інформації. Програма кваліфікаційного іспиту включає 7 дисциплін професійного циклу:</p> <ol style="list-style-type: none">1. Організація та безпека баз даних;2. Захист інформації;3. Системи технічного захисту інформації;4. Комп'ютерні мережі;5. Комплексні системи захисту інформації;6. Аналіз вразливостей інформаційних систем;7. Безпека хмарних платформ та сервісів <p>Кваліфікаційний іспит складається з трьох частин: із тестової перевірки знань, теоретичних питань і практичного ситуаційного завдання.</p>

9. Вимоги до наявності системи внутрішнього забезпечення якості фахової передвищої освіти

<p>Принципи та процедури забезпечення якості освіти</p>	<p>Визначені та легітимізовані у Законі України «Про фахову передвищу освіту» від 06.06.2019 р. № 2745-VIII і рекомендаціях щодо забезпечення якості освіти в Європейському просторі Європейської асоціації із забезпечення якості вищої освіти, Національного стандарту України «Системи управління якістю» ДСТУ ISO 9001:2015.</p> <p>Принципи забезпечення якості освіти:</p> <ul style="list-style-type: none"> - відповідність європейським та національним стандартам якості фахової передвищої освіти; - автономія навчального закладу, який несе відповідальність за забезпечення якості освітньої діяльності та якості фахової передвищої освіти; - здійснення моніторингу якості; - системний підхід, який передбачає управління якістю на всіх стадіях освітнього процесу; - постійне підвищення якості освітнього процесу; - залучення студентів, роботодавців та інших зацікавлених сторін до процесу забезпечення якості фахової передвищої освіти; - відкритість інформації на всіх етапах забезпечення якості. <p>Процедури забезпечення якості освіти:</p> <ul style="list-style-type: none"> - удосконалення планування освітньої діяльності: моніторинг та періодичне оновлення освітньо-професійних програм; - якісний відбір контингенту здобувачів фахової передвищої освіти освітнього-професійного ступеня фаховий молодший бакалавр; - збільшення частки викладачів з науковими ступенями та вченими (почесними) званнями в складі циклових комісій ТФК ЛНТУ; - удосконалення матеріально-технічної та навчально-методичної баз для реалізації освітнього процесу; - забезпечення необхідних ресурсів для підтримки здобувачів фахової передвищої освіти за освітньо-професійним ступенем фаховий молодший бакалавр; - розвиток інформаційних систем з метою підвищення ефективності управління освітнім процесом; - забезпечення публічності інформації про діяльність ТФК ЛНТУ; - створення ефективної системи запобігання та виявлення академічного плагіату у наукових працях працівників ТФК ЛНТУ і здобувачів фахової передвищої освіти; - створення ефективної системи запобігання корупції та хабарництва в освітньому процесі ТФК ЛНТУ
<p>Моніторинг та періодичний перегляд освітньо-професійних програм</p>	<p>Моніторинг та періодичний перегляд освітньо-професійних програм проводиться за вимогами відповідного положення, розробленого ТФК ЛНТУ. Критерії, за якими відбувається перегляд освітньо-професійної програми, формулюються як результат зворотного зв'язку із науково-педагогічними, педагогічними працівниками, студентами, випускниками,</p>

	<p>роботодавцями, так і внаслідок прогнозування розвитку галузі, потреб суспільства та ринку праці.</p> <p>Показниками сучасності освітньо-професійної програми є:</p> <ul style="list-style-type: none"> - оновлюваність; - участь роботодавців у розробці та внесенні змін в освітньо-професійну програму; - рівень задоволеності випускників змістом освітньо-професійної програми; - відгуки роботодавців про рівень підготовки випускників
<p>Щорічне оцінювання здобувачів фахової передвищої освіти</p>	<p>Оцінювання знань та практичних умінь студентів здійснюється у ТФК ЛНТУ на підставі власного положення про організацію освітнього процесу.</p> <p>Система оцінювання якості підготовки студентів включає: вхідний, поточний, семестровий, підсумковий контроль та атестацію здобувачів фахової передвищої освіти, які здобувають освітньо-професійний ступінь фахового молодшого бакалавра</p>
<p>Підвищення кваліфікації педагогічних працівників</p>	<p>Викладацький склад ТФК ЛНТУ підвищує кваліфікацію в Україні і за кордоном. ТФК ЛНТУ забезпечує різні форми підвищення кваліфікації педагогічних працівників щорічно. Загальна кількість академічних годин для підвищення кваліфікації педагогічного працівника закладу фахової передвищої освіти впродовж п'яти років не може бути меншою за 120 годин.</p> <p>У ТФК ЛНТУ реалізуються власні програми та форми підвищення кваліфікації (семінари, майстер-класи, тренінги, конференції, вебінари, круглі столи, школи молодого викладача тощо)</p>
<p>Наявність необхідних ресурсів для організації освітнього процесу</p>	<p>Ресурсами для організації освітнього процесу у ТФК ЛНТУ є:</p> <ul style="list-style-type: none"> - навчальний план; - робочий навчальний план; - робочі програми навчальних дисциплін та практик. <p>Відповідно до діючих ліцензійних умов:</p> <ul style="list-style-type: none"> - належне навчально-методичне забезпечення (комплекси) навчальних дисциплін; - сучасні інформаційні джерела та комп'ютерна техніка; - власна веб-сторінка; - інтернет-зв'язок; - бібліотека із сучасною навчальною літературою, науковими, довідковими та фаховими періодичними виданнями; - інформаційно-комунікаційні засоби зв'язку; - наявність баз для проведення всіх видів практики; - кадрове забезпечення викладання навчальних дисциплін
<p>Наявність інформаційних систем для ефективного управління освітнім процесом</p>	<p>Електронна система збору і аналізу інформації (ЄДЕБО). Система електронного документообігу. Електронна скринька. Електронна платформа Moodle. Microsoft Office 365. Microsoft Teams</p>
<p>Публічність інформації про</p>	<p>Наявність офіційного сайту ТФК ЛНТУ, на якому оприлюднюються: статут, власне положення про організацію</p>

освітньо-професійні програми, ступені вищої освіти та кваліфікації	освітнього процесу, правила прийому, ступені освіти, за якими проводиться підготовка фахівців, у тому числі за рівнем фаховий молодший бакалавр, основні дані про освітньо-професійні програми тощо.
Запобігання та виявлення академічного плагіату	Розроблені та діють Положення про запобігання та виявлення академічного плагіату у Відокремленому структурному підрозділі «Технічний фаховий коледж Луцького національного технічного університету», Положення про академічну доброчесність учасників освітнього процесу Відокремленого структурного підрозділу «Технічний фаховий коледж Луцького національного технічного університету» Процедури та заходи: - формування колективу в ТФК ЛНТУ, який не сприймає і не допускає академічну нечесність; - створення умов нетерпимості до випадків академічного плагіату; - перевірка робіт на плагіат; - виявлення та притягнення до відповідальності винних у академічному плагіаті

10. Перелік нормативних документів, на яких базується освітньо-професійна програма фахової передвищої освіти

1. Конституція України № 254к/96-ВР від 28.06.1996.
2. Про фахову передвищу освіту: Закон України від 06 червня 2020 р. № 2745-VIII / Законодавство України. – Офіційний сайт Верховної Ради України. URL : <https://zakon.rada.gov.ua/laws/show/2745-19#Text>
3. Про освіту: Закон України від 5 вересня 2017 р. № 2145-VIII. / Законодавство України. – Офіційний сайт Верховної Ради України. URL : <https://zakon.rada.gov.ua/laws/show/2145-19>
4. Постанова Кабінету Міністрів України від 25 червня 2020 р. № 519 « Про затвердження Національної рамки кваліфікацій».
5. Постанова Кабінету Міністрів №1187 від 30.12.2015 «Про затвердження Ліцензійних умов провадження освітньої діяльності закладів освіти» зі змінами. – URL: <https://zakon.rada.gov.ua/laws/show/1187-2015-%D0%BF#Text>