МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ЛУЦЬКИЙ НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ
ФАКУЛЬТЕТ КОМП'ЮТЕРНИХ ТА ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ

ЗАТВЕРДЖУЮ
Декан факультету
_____ Інна КОНДЮС
«29» серпня 2026 р.

ЗАТВЕРДЖУЮ
Перший проректор
_____ Надія КОВАЛЬЧУК
«29» серпня 2026 р.

СИЛАБУС

з освітнього компонента «Фахова практика»
ступінь вищої освіти – бакалавр
галузь знань – 12 Інформаційні технології
спеціальність – 125 Кібербезпека та захист інформації
освітня програма – Кібербезпека

Кафедра кібербезпеки

Силабус склав(ла) асистент (ПП) кафедри кібербезпеки Олег КУЛАКЕВИЧ

Силабус затверджений на засіданні кафедри кібербезпеки, протокол № 2 від «28» серпня 2026 р.

Завідувач кафедри к.т.н., доцент Сергій КОСТЮЧКО

Розглянуто та схвалено групою забезпечення освітньої програми «Кібербезпека», протокол № 2 від «28» серпня 2026 р.

Гарант ОП «Кібербезпека» к.т.н., доцент Сергій КОСТЮЧКО

Схвалено науково-методичною радою університету, протокол № 1/а від «29» серпня 2026 р.

Затверджений силабус онлайн:
https://e.lntu.edu.ua/syllabus/3019

Луцьк – 2026

СИЛАБУС ОСВІТНЬОГО КОМПОНЕНТА «Фахова практика»

Освітня програма	Кібербезпека
Галузь знань / Спеціальність	12 Інформаційні технології / 125 Кібербезпека та захист інформації
Рівень вищої освіти	перший (бакалаврський)
Статус дисципліни	нормативна
Мова викладання	українська
Обсяг	6 кредитів ECTS / 180 годин, семестр 8
Форма контролю	захист (денна); екзамен (заочна)
Викладач(і)	асистент (пп) Олег КУЛАКЕВИЧ

1. Мета і завдання дисципліни

Мета: Метою фахової практики є закріплення та поглиблення теоретичних знань, отриманих здобувачами вищої освіти під час навчання, формування й удосконалення практичних навичок у сфері інформаційної та кібербезпеки, набуття досвіду професійної діяльності в реальних виробничих умовах. Особлива увага приділяється ознайомленню з організаційною структурою та інформаційною інфраструктурою підприємств, застосуванню сучасних технологій і засобів захисту інформації, аналізу кіберзагроз, оцінюванню ризиків, виявленню вразливостей інформаційних систем та розробленню заходів щодо забезпечення їх безпеки. Практика спрямована на розвиток професійних компетентностей, самостійності у вирішенні практичних завдань і готовності до майбутньої професійної діяльності за спеціальністю.

Завдання: Розширення та закріплення теоретичних знань і практичних навичок, що необхідні для успішного працевлаштування; отримання навичок самостійної роботи; освоєння раціональної роботи над завданнями, грамотного їх оформлення, складання звітів про виконану роботу.

2. Компетентності

ЗК01 — Здатність застосовувати знання у практичних ситуаціях.

ЗК02 — Знання та розуміння предметної області та розуміння професії.

ЗК04 — Вміння виявляти, ставити та вирішувати проблеми за професійним спрямуванням.

ЗК05 — Здатність до пошуку, оброблення та аналізу інформації.

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.

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.

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.

3. Структура дисципліни, розподіл годин, зв'язок тем з компетентностями

№	Назва розділу (етапу)	Години денна/ заочна	Методи навчання	Методи оцінювання	ЗК та СК
1	Розділ 1. Проходження інструктажу з техніки безпеки	5/5	МН1, МН2, МН6	МО2	ЗК01, ЗК02, ЗК04, ЗК05, СК02, СК03, СК07, СК08, СК10, СК11, СК12
2	Розділ 2. Ознайомлення з метою та програмою практики, отримання завдання	5/5	МН1, МН2, МН6	МО2	ЗК01, ЗК02, ЗК05, ЗК04, СК02, СК03, СК07, СК08, СК12, СК11, СК10
3	Розділ 3. Поняття стандартизації. Оформлення документів згідно стандартів ДСТУ	20/20	МН1, МН2, МН6	МО2	ЗК01, ЗК02, ЗК04, ЗК05, СК02, СК03, СК07, СК08, СК10, СК11, СК12
4	Розділ 4. Збір матеріалів про підприємство	20/20	МН1, МН2, МН6	МО2	ЗК01, ЗК02, ЗК04, ЗК05, СК02, СК03, СК07, СК08, СК10, СК11, СК12
5	Розділ 5. Виконання завдань, поставлених керівниками практики від навчального закладу та підприємства	120/120	МН1, МН2, МН6	МО2	ЗК01, ЗК02, ЗК04, ЗК05, СК02, СК03, СК07, СК08, СК10, СК11, СК12
6	Розділ 6. Захист звіту про практику	10/10	МН1, МН2, МН6	МО1, МО2	ЗК01, ЗК02, ЗК04, ЗК05, СК02, СК03, СК07, СК08, СК10, СК11, СК12
	Разом	**180/180**			

Легенда: ЗК — загальна компетентність (номер за п. 2); СК — спеціальна (фахова) компетентність (номер за п. 2). Повне формулювання кожного коду наводиться в ОП / стандарті спеціальності.

Методи навчання: МН1 — словесний метод (лекція, дискусія, співбесіда тощо); МН2 — практичний метод (лабораторні та практичні заняття); МН6 — самостійна робота (розв'язання завдань).

Методи оцінювання: МО1 — екзамен; МО2 — усне або письмове опитування.

4. Результати навчання

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;

ПРН06. критично осмислювати основні теорії, принципи, методи і поняття у навчанні та професійній діяльності;

ПРН11. виконувати аналіз зв’язків між інформаційними процесами на віддалених обчислювальних 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;

ПРН38. інтерпретувати результати проведення спеціальних вимірювань з використанням технічних засобів, контролю характеристик інформаційнотелекомунікаційних систем відповідно до вимог нормативних документів системи технічного захисту інформації;

5. Цілі сталого розвитку

ЦСР 4 – Якісна освіта

ЦСР 8 – Гідна праця та економічне зростання

ЦСР 17 – Партнерство заради сталого розвитку

6. Неформальна освіта

Рекомендовані курси, тренінги, стажування та інші: результати навчання, здобуті у формальній, неформальній чи інформальній освіті, можуть бути визнані відповідно до процедур ЛНТУ. Підтвердженнями можуть бути сертифікати тематичних тренінгів, вебінарів чи онлайн-курсів разом з описом досягнутих результатів навчання та, за потреби, коротке верифікаційне завдання або портфоліо.

7. Критерії та форми контролю

Оцінювання — за 100-бальною шкалою (національна шкала / ЄКТС).

Складова	Ваговий коефіцієнт	Форми контролю
Оцінка керівника практики	40 %	Перевірка звіту та щоденника практики, виконання індивідуального завдання й програми практики, дотримання графіка; відгук (висновок) керівника
Оцінка комісії на захисті	60 %	Публічний захист: доповідь за результатами практики з презентацією, відповіді на запитання членів комісії
Разом	**100 %**	

Академічна доброчесність: самостійне виконання завдань; коректне посилання на джерела; позначення частин тексту, згенерованих засобами ШІ. Порушення академічної доброчесності не толеруються.

8. Зміст тем

Розділ 1. Проходження інструктажу з техніки безпеки

Проходження вступного інструктажу з охорони праці, техніки безпеки та ознайомлення з правилами внутрішнього трудового розпорядку підприємства.

Розділ 2. Ознайомлення з метою та програмою практики, отримання завдання

Ознайомлення з метою, завданнями та програмою фахової практики. Отримання індивідуального завдання та узгодження плану його виконання.

Розділ 3. Поняття стандартизації. Оформлення документів згідно стандартів ДСТУ

Ознайомлення з основами стандартизації, нормативно-правовою базою у сфері інформаційної та

кібербезпеки. Вивчення вимог до оформлення технічної документації відповідно до стандартів ДСТУ.

Розділ 4. Збір матеріалів про підприємство

Збір та аналіз інформації про підприємство, його організаційну структуру, напрями діяльності, інформаційну інфраструктуру та застосовувані засоби захисту інформації.

Розділ 5. Виконання завдань, поставлених керівниками практики від навчального закладу та підприємства

Виконання практичних та індивідуальних завдань, визначених керівниками практики від університету та підприємства. Застосування сучасних технологій, методів та інструментів забезпечення інформаційної та кібербезпеки.

Розділ 6. Захист звіту про практику

Узагальнення результатів виконаної роботи, оформлення звітної документації відповідно до встановлених вимог. Підготовка та захист звіту про проходження фахової практики.

9. Загальні вимоги

Освітній процес регулюється академічними правилами ЛНТУ. Здобувачі освіти зобов’язані ознайомитися з вимогами, визначеними Кодексом академічної доброчесності ЛНТУ та Політикою етичного використання штучного інтелекту в ЛНТУ, і дотримуватися принципів академічної доброчесності та етичного використання штучного інтелекту в освітній діяльності.

Академічна доброчесність. Учасники освітнього процесу зобов’язані дотримуватися Закону України «Про академічну доброчесність» від 18.12.2025 № 4742-IX та внутрішніх нормативних документів ЛНТУ. Не допускаються академічний плагіат, фабрикація, фальсифікація, привласнення авторства, несамостійне виконання завдань, а також недоброчесне використання результатів, згенерованих штучним інтелектом.

Використання штучного інтелекту. Інструменти штучного інтелекту можуть використовуватися для пошуку ідей, пояснення методів, попереднього структурування, мовного редагування та допоміжного аналізу неконфіденційних даних, якщо конкретне завдання не передбачає повністю самостійного виконання. Здобувач освіти має зазначати використаний інструмент, мету та етап його застосування, перевіряти факти й розрахунки та самостійно обґрунтовувати висновки.

10. Література

II. Наукові праці

Праці інших авторів:

1. Про затвердження стандарту вищої освіти за спеціальністю 125 «Кібербезпека» для першого (бакалаврського) рівня вищої освіти : наказ Міністерства освіти і науки України від 04.10.2018 № 1074 (зі змінами, внесеними наказом МОН від 29.10.2024 № 1547). URL: https://mon.gov.ua/npa/pro-zatverdzhennya-standartu-vishoyi-osviti-za-specialnistyu-125-kiberbezpeka-dlya-pershogo-bakalavrskogo-rivnya-vishoyi-osviti.

2. Про освітню програму у Луцькому національному технічному університеті : положення ЛНТУ від 25.06.2026 № 38-26. Луцьк : ЛНТУ, 2026. URL: https://drive.google.com/uc?export=download&id=1-0KWrf0oo-3yETdT8A6K4ObiHL_JAfsq.

3. Про організацію освітнього процесу в Луцькому національному технічному університеті : положення ЛНТУ від 31.07.2026 № 60-26 (зі змінами від 27.08.2026 № 98-26). Луцьк : ЛНТУ, 2026. URL: https://lntu.edu.ua/uk/orders-and-instructions?field_data_value=&field_nazva_value=&field_nomer_nakaz_target_id=&field_posada_nakaz_target_id=All&field_viddil_target_id=All&page=1

4. Про практичну підготовку здобувачів вищої освіти у Луцькому національному технічному університеті : положення ЛНТУ, редакція 02, від 03.10.2025 № 840. Луцьк : ЛНТУ, 2025. URL: https://drive.google.com/file/d/1PWOrscivgxQtdxsOqZBvbrIKfaX6RfIf/edit

5. ДСТУ 3008:2015. Інформація та документація. Звіти у сфері науки і техніки. Структура та правила оформлювання. На заміну ДСТУ 3008-95. Київ: ДП «УкрНДНЦ», 2016.

6. ДСТУ ISO 80000-1:2016. Величини та одиниці. Частина 1. Загальні положення (ISO 80000-1:2009, IDT). Київ: ДП «УкрНДНЦ».

7. ДСТУ 3582:2013. Інформація та документація. Бібліографічний опис. Скорочення слів і словосполучень українською мовою. Загальні вимоги та правила. Київ : Мінекономрозвитку України, 2014.

8. ДСТУ 1.5:2015. Національна стандартизація. Правила розроблення, викладання та оформлення національних нормативних документів. Київ : ДП «УкрНДНЦ».

9. ДСТУ 8302:2015. Інформація та документація. Бібліографічне посилання. Загальні положення та правила складання. Київ : ДП «УкрНДНЦ», 2016.

10. Про затвердження переліку галузей знань і спеціальностей, за якими здійснюється підготовка здобувачів вищої та фахової передвищої освіти : постанова Кабінету Міністрів України від 29.04.2015 № 266 (у редакції постанови від 30.08.2024 № 1021, зі змінами). URL: https://zakon.rada.gov.ua/laws/show/266-2015-%D0%BF (дата звернення: 28.10.2026).

11. Про рішення Ради національної безпеки і оборони України від 14 травня 2021 року «Про Стратегію кібербезпеки України» : Указ Президента України від 26.08.2021 № 447/2021. URL: https://zakon.rada.gov.ua/laws/show/447/2021.

12. Про затвердження Ліцензійних умов провадження освітньої діяльності : постанова Кабінету Міністрів України від 30.12.2015 № 1187 (зі змінами). URL: https://zakon.rada.gov.ua/laws/show/1187-2015-%D0%BF.

13. Деякі питання оприлюднення інформації про діяльність вищих навчальних закладів: наказ Міністерства освіти і науки України від 19.02.2015 № 166 (зі змінами). URL: https://zakon.rada.gov.ua/rada/show/v0166729-15.

14. Про особливості запровадження переліку галузей знань і спеціальностей, за якими здійснюється підготовка здобувачів вищої освіти, затвердженого постановою Кабінету Міністрів України від 29 квітня 2015 року № 266: наказ Міністерства освіти і науки України від 06.11.2015 № 1151 (зі змінами). URL: https://zakon.rada.gov.ua/laws/show/z1460-15.

15. Про навчально-методичне забезпечення освітнього процесу Луцького національного технічного університету : положення ЛНТУ від 31.07.2026 № 61-26. Луцьк : ЛНТУ, 2026. URL: https://drive.google.com/uc?export=download&id=1QzuKjtRMFz3HEm20HT0Xns9a1fMqmsYl