МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ЛУЦЬКИЙ НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ
ФАКУЛЬТЕТ ЦИФРОВИХ, ОСВІТНІХ ТА СОЦІАЛЬНИХ ТЕХНОЛОГІЙ

ЗАТВЕРДЖУЮ
Декан факультету
_____ Галина ГЕРАСИМЧУК
«26» серпня 2026 р.

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

СИЛАБУС

з освітнього компонента «Інформаційні та комунікаційні технології у цивільній безпеці»
ступінь вищої освіти – магістр
галузь знань – К Безпека та оборона
спеціальність – К10 Цивільна безпека
освітня програма – Цивільна безпека

Кафедра цивільної безпеки

Силабус склав(ла) доцент кафедри цивільної безпеки, к.т.н., доцент Микола РУДИНЕЦЬ

Силабус затверджений на засіданні кафедри цивільної безпеки, протокол № 1 від «26» серпня 2026 р.

Завідувач кафедри к.т.н., доцент Валентина ФЕДОРЧУК-МОРОЗ

Розглянуто та схвалено групою забезпечення освітньої програми «Цивільна безпека», протокол № 1 від «26» серпня 2026 р.

Гарант ОП «Цивільна безпека» к.т.н., доцент Микола РУДИНЕЦЬ

Схвалено науково-методичною радою університету, протокол № 1 від «26» серпня 2026 р.

Затверджений силабус онлайн:
https://e.lntu.edu.ua/syllabus/2826

Луцьк – 2026

СИЛАБУС ОСВІТНЬОГО КОМПОНЕНТА «Інформаційні та комунікаційні технології у цивільній безпеці»

Освітня програма	Цивільна безпека
Галузь знань / Спеціальність	К Безпека та оборона / К10 Цивільна безпека
Рівень вищої освіти	другий (магістерський)
Статус дисципліни	нормативна
Мова викладання	українська
Обсяг	5 кредитів ECTS / 150 годин, семестр 2
Форма контролю	залік
Викладач(і)	к.т.н., доцент Микола РУДИНЕЦЬ

1. Мета і завдання дисципліни

Мета: Мета вивчення дисципліни
Надбання і закріплення знань про функціонування інформаційних систем і комп'ютерних технологій, організацію діалогу користувача з інформаційною системою, методів збору, обробки, пересилки і використання інформації та можливостей її застосування у професійній діяльності.

Завдання: Завдання вивчення дисципліни
- одержати систематичні, теоретичні знання про сучасні прикладних інформаційні технології;
- сформувати здатність до системного творчого мислення, наполегливість у досягненні мети;
- вивчити методи аналізу, опрацювання та узагальнення професійної і науково-технічної інформації;
- надати можливість майбутньому фахівцю практичні основи використання інформаційних систем у процесі дослідження продуктів, сервісів інформаційних технологій, інших об'єктів професійної діяльності;
- засвоїти методи створення та експлуатації автоматизованих систем електронного документообігу;
- надати можливість майбутньому фахівцю набути навички використання прикладних систем обробки даних для персональних комп'ютерів і локальних комп'ютерних мереж під час розв'язання завдань фахового спрямування.

Пререквізити: Іноземна мова за професійним спрямуванням, Методологія наукової та інноваційної діяльності

2. Компетентності

ІК — інтегральна компетентність: Здатність розв'язувати задачі дослідницького та/або інноваційного характеру у сфері цивільної безпеки

ЗК01 — Здатність до пошуку, оброблення та аналізу інформації з різних джерел.

СК06 — Здатність застосовувати сучасні інформаційні та комунікаційні технології, спеціалізоване програмне забезпечення у сфері професійної діяльності

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

№	Назва теми	**Лекції** денна/ заочна	**Практ./ Семін./ лаб** денна/ заочна	**Самост. робота** денна/ заочна	**Разом**	**Методи навчання**	**Методи оцінювання**	**ЗК та СК**
Змістовий модуль 1. Інформаційні та комунікаційні технології у цивільній безпеці								

№	Назва теми	Лекції денна/ заочна	Практ./ Семін./ лаб денна/ заочна	Самост. робота денна/ заочна	Разом	Методи навчання	Методи оцінювання	ЗК та СК
1	Тема 1. Інформаційні системи та технології у професійній діяльності	1/1	3/–	9/14	13/15	МН1, МН2, МН3, МН4, МН5, МН6, МН7	МО2, МО4, МО7, МО9	ЗК01
2	Тема 2. Комп’ютерні мережі та їх роль у системі цивільного захисту	1/1	4/2	10/15	15/18	МН1, МН2, МН3, МН4, МН5, МН6, МН7	МО2, МО4, МО7, МО9	ЗК01, СК06
3	Тема 3. Інформаційна безпека та захист даних	1/1	4/1	12/16	17/18	МН1, МН2, МН3, МН4, МН5, МН6, МН7	МО2, МО4, МО9	ЗК01, СК06
4	Тема 4. Інтернет-сервіси у професійній діяльності	4/–	4/–	12/16	20/16	МН1, МН2, МН3, МН4, МН5, МН6, МН7	МО2, МО4, МО9	ЗК01, СК06
Змістовий модуль 2. Прикладні ІКТ у сфері цивільної безпеки								
5	Тема 5. Автоматизовані системи оповіщення та реагування на надзвичайні ситуації	2/1	4/1	10/15	16/17	МН1, МН2, МН3, МН4, МН5, МН6, МН7	МО2, МО4, МО7, МО9	ЗК01, СК06
6	Тема 6. Системи моделювання і прогнозування надзвичайних ситуацій	2/1	3/1	12/15	17/17	МН1, МН2, МН3, МН4, МН5, МН6, МН7	МО2, МО4, МО7, МО9	ЗК01, СК06

№	Назва теми	**Лекції** денна/ заочна	**Практ./ Семін./ лаб** денна/ заочна	**Самост. робота** денна/ заочна	**Разом**	**Методи навчання**	**Методи оцінювання**	**ЗК та СК**
7	Тема 7. Штучний інтелект у системі цивільної безпеки	2/1	4/1	12/15	18/17	МН1, МН2, МН3, МН4, МН5, МН6, МН7	МО2, МО4, МО7, МО9	ЗК01, СК06
8	Тема 8. Використання ІКТ в освітньому процесі фахівців цивільної безпеки	2/–	4/–	12/16	18/16	МН1, МН2, МН3, МН4, МН5, МН6, МН7	МО2, МО4, МО7, МО9	ЗК01, СК06
	ІЗ/КПІЗ			16/16	16/16			
	Разом	**15/6**	**30/6**	**105/138**	**150/150**			

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); МН3 — наочний метод (метод ілюстрацій і метод демонстрацій); МН4 — робота з навчально-методичною літературою (конспектування, тезування, анотування, рецензування, складання реферату); МН5 — відеометод у сполученні з новітніми інформаційними технологіями та комп'ютерними засобами навчання (дистанційні, мультимедійні, веб-орієнтовані тощо); МН6 — самостійна робота (розв'язання завдань); МН7 — індивідуальна науково-дослідна робота здобувачів вищої освіти.

Методи оцінювання: МО2 — усне або письмове опитування; МО4 — тестування; МО7 — презентації результатів виконаних завдань та досліджень; МО9 — залік.

4. Результати навчання

ПРН03. Інтегрувати знання з різних галузей для розв'язання теоретичних та/або практичних задач і проблем у сфері цивільної безпеки.

ПРН07. Використовувати сучасні інформаційні та комунікаційні технології, спеціалізоване програмне забезпечення під час розв'язання практичних та/або наукових задач.

ПРН17. Відшуковувати необхідну інформацію в спеціальній літературі, базах даних, інших джерелах інформації, аналізувати та об'єктивно оцінювати інформацію розробляти науково-обґрунтовані рекомендації на основі отриманих даних.

5. Цілі сталого розвитку

ЦСР 4 – Якісна освіта

ЦСР 7 – Доступна та чиста енергія

ЦСР 8 – Гідна праця та економічне зростання

ЦСР 9 – Промисловість, інновації та інфраструктура

ЦСР 11 – Сталий розвиток міст і громад

ЦСР 13 – Пом'якшення наслідків зміни клімату

ЦСР 16 – Мир, справедливість та сильні інститути

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). Підсумковий бал = поточний контроль (40 %) + ІЗ/КПІЗ (10 %) + модульний контроль (50 %).

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

8. Зміст тем

Тема 1. Інформаційні системи та технології у професійній діяльності

Поняття інформаційної системи. Класифікація інформаційних систем. Основні компоненти: технічне забезпечення, програмне забезпечення, бази даних, персонал. Функції інформаційних систем у цивільному захисті. Принципи автоматизації управління.

Тема 2. Комп’ютерні мережі та їх роль у системі цивільного захисту

Типи комп’ютерних мереж, архітектура, протоколи зв’язку, кіберстійкість інфраструктури. Застосування комп’ютерних мереж у системах моніторингу, оповіщення, зв’язку з аварійними підрозділами.

Тема 3. Інформаційна безпека та захист даних

Загрози інформаційній безпеці. Методи та засоби захисту інформації. Криптографічний захист, управління доступом, резервування. Нормативно-правове забезпечення безпеки інформації в Україні.

Тема 4. Інтернет-сервіси у професійній діяльності

Інтернет як середовище комунікацій. Електронна пошта, хмарні сервіси, відеоконференції, соціальні мережі. Застосування онлайн-платформ для оперативного управління та інформування населення.

Тема 5. Автоматизовані системи оповіщення та реагування на надзвичайні ситуації

Класифікація систем оповіщення: загальнодержавні, територіальні, об’єктові. Автоматизація процесів передачі інформації. Вимоги до надійності та сумісності. Досвід ДСНС України.

Тема 6. Системи моделювання і прогнозування надзвичайних ситуацій

Принципи роботи ГІС. Картографування небезпек, аналіз територіальних ризиків, прогнозування зон ураження. Застосування ArcGIS, QGIS, FloodMap, Forecast, NUKEMAP у практиці цивільної безпеки.

Тема 7. Штучний інтелект у системі цивільної безпеки

Огляд сучасних тенденцій у сфері цифровізації, впровадження штучного інтелекту, блокчейну, Інтернету речей (IoT) та роботизованих систем у сфері цивільного захисту. Поняття та принципи роботи систем ШІ. Машинне навчання, нейронні мережі, інтелектуальний аналіз даних. Застосування ШІ у прогнозуванні НС, управлінні евакуацією, аналізі відеопотоків, оптимізації рішень. Етичні та правові аспекти.

Тема 8. Використання ІКТ в освітньому процесі фахівців цивільної безпеки

Електронні освітні системи (Moodle, Google Classroom), дистанційні технології, VR-тренажери, гейміфіковані моделі навчання. Практичний досвід застосування 3D та віртуальної реальності у підготовці рятувальників.

9. Опис ІЗ/КПІЗ

Виконання ІЗ є одним із обов'язкових складових модулів залікового кредиту з дисципліни «Інформаційні та комунікаційні технології у цивільній безпеці». ІЗ виконується самостійно кожним студентом.

Зміст ІЗ: реферати за обраними і узгодженими з викладачем темами.

Теми рефератів:

1. Інформаційна система підтримки управління цивільною безпекою
2. Геоінформаційні технології в оцінюванні ризиків надзвичайних ситуацій
3. Цифровий моніторинг небезпечних природних явищ
4. Застосування штучного інтелекту для прогнозування ризиків
5. Інформаційні технології в системах оповіщення населення
6. Кібербезпека інформаційних систем цивільного захисту
7. Хмарні технології в організації роботи служб цивільної безпеки
8. Інтернет речей у системах раннього виявлення небезпек
9. Безпілотні літальні апарати та дистанційне зондування Землі в цивільній безпеці
10. Інформаційні технології для оцінювання ризиків на потенційно небезпечних об'єктах
11. Системи підтримки прийняття рішень під час надзвичайних ситуацій
12. Цифрові комунікації та управління інформаційними потоками під час криз
13. Використання великих даних для аналізу надзвичайних ситуацій
14. Цифрове моделювання поширення небезпечних факторів
15. Розроблення цифрової інформаційної панелі для моніторингу стану безпеки
16. Захист персональних даних та інформаційна етика в цивільній безпеці
17. Електронний документообіг у системі управління цивільним захистом
18. Цифрова трансформація системи цивільної безпеки територіальної громади
19. Інформаційне забезпечення евакуаційних заходів
20. Технологія автоматизованих робочих місць.
21. Мережні технології.
22. Мобільні технології.
23. Системи моніторингу надзвичайних ситуацій.
24. CRM-системи.
25. Автоматизація документообігу.

10. 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.

11. Література

І. Навчально-методичні матеріали та розробки

Праці автора силабуса:

1. Інформаційні та комунікаційні технології у сфері професійної діяльності [Текст] : Конспект лекцій для здобувачів другого (магістерського) рівня вищої освіти освітньої програми «Цивільна безпека» галузі знань 26 – Цивільна безпека спеціальності 263 – Цивільна безпека денної та заочної форм навчання / уклад. М. В. Рудинець. – Луцьк: Відділ іміджу та промоції ЛНТУ, 2024. – 100с.

2. Інформаційні та комунікаційні технології у цивільній безпеці [Текст]: Методичні вказівки до практичних занять та виконання самостійної роботи для здобувачів другого (магістерського) рівня галузі знань 26 «Цивільна безпека» спеціальності 263 «Цивільна безпека» денної та заочної форм навчання / уклад. М.В. Рудинець – Луцьк: ЛНТУ, 2024. – 72 с.

3. Лобойченко В, М., Вісин В. В. Шубалий О. М. та ін. Цивільна безпека: навч. посібн. магістерський курс / за заг. ред. В. І. Федорчук-Мороз. Луцьк: ЛНТУ, 2024. 441 с. URL: https://repository.lntu.edu.ua/handle/123456789/4191

Праці інших авторів:

4. Бутенко Т. А., Сирий В. М. Інформаційні системи та технології: навчальний посібник. – Харків: ХНАУ ім. В. В. Докучаєва, 2020. 207 с. URL: https://repo.btu.kharkov.ua/bitstream/123456789/4849/1/INFO_SYSTEMS_20.pdf.

5. Виганяйло С. М. Інформаційне забезпечення професійної діяльності: навч. посіб. – Харків: ХНУВС, 2021. 108 с. URL: https://cutt.ly/SVuI8n1.

6. Кавун С. В. Інформаційна безпека. – ХНЕУ, 2020. – 116 с.

7. Азаров, О. Д., Захарченко, С. М., Кадук, О. В. та ін. Комп’ютерні мережі : підручник / О. Д. Азаров, С. М. Захарченко, О. В. Кадук та ін. – Вінниця : ВНТУ, 2020. – 378 с.

8. Когут Ю. І. Штучний інтелект і безпека: практичний посібник / Ю. І. Когут. – Київ : Юрінком Інтер, 2024. – 294 с. – Режим доступу: https://jurkniga.ua/contents/shtuchniy-intelekt-i-bezpeka.pdf

9. Звенігородський О. С., Зінченко О. В., Чичкарьов Є. А., Кисіль Т. М. Штучний інтелект. Вступний курс: навчальний посібник / О. С. Звенігородський, О. В. Зінченко, Є. А. Чичкарьов, Т. М. Кисіль. – Київ : ДУІКТ, 2022. – Режим доступу: https://duikt.edu.ua/uploads/l_492_92652604.pdf

ІІ. Наукові праці

Праці автора силабуса:

10. Tryhuba A., Koval N., Tryhuba I., Firman I., Famuliak V., Tatomyr A., Hulko B., Rozhko I., Rudynets M., & Fedorchuk-Moroz V. A Data-Driven Risk-Informed Decision Support Framework for Sustainable Municipal Organic Waste Management in Smart Cities. Sustainability. 2026. № 18 (12). С. 5862. URL: https://repository.lntu.edu.ua/handle/123456789/4359

11. Рудинець М. В., Федорчук-Мороз В. І. Вплив інформаційних технологій на ментальне здоров’я населення в умовах війни. Актуальні питання охорони праці, цивільної та техногенної безпеки. 2025. № 2 (2). С. 83-92. URL: https://repository.lntu.edu.ua/handle/123456789/4179

12. Федорчук-Мороз, В. І. Рудинець М. В. Підвищення рівня культури безпеки та зниження психосоціальних ризиків на підприємствах в умовах воєнного стану. Вісті Донецького гірничого інституту. 2024. №2. С. 128-137. URL: https://repository.lntu.edu.ua/handle/123456789/4183

13. Tryhuba A., Ratushnyi A., The Model of the Formation of Values and the Information System of Their Determination in the Projects of the Creation of Territorial Emergency and Rescue Structures. IT Project Management. 2023. P. 59–70. Режим доступу: https://ceur-ws.org/Vol-3453/paper6.pdf

14. Рудинець М. В. Федорчук-Мороз В. І. Обґрунтування застосування віртуальної реальності як інноваційного елементу проектів системи захисту населення від надзвичайних ситуацій. Український журнал будівництва та архітектури. 2022. № 3 (009). С. 75-83. URL: https://repository.lntu.edu.ua/handle/123456789/4237

15. Рудинець М. В. Федорчук-Мороз В. І. Інноваційний проектний підхід до зацікавленості населення у захисті від надзвичайних ситуацій. Вісті Донецького гірничого інституту. 2022. № 1 (50). С. 124-131. URL: https://repository.lntu.edu.ua/handle/123456789/4238

16. Koval N., Tryhuba A., Kondysiuk I., Tryhuba I., Boiarchuk O., Rudynets M., Grabovets V., Onyshchuk V. Forecasting the Fund of Time for Performance of Works in Hybrid Projects Using Machine Training Technologies. CEUR Workshop Proceedings. 2021. Vol. 2917. P. 196–206. URL: https://repository.lntu.edu.ua/handle/123456789/5300

17. Федорчук-Мороз В І., Рудинець М. В. Інноваційні проєкти підвищення безпеки праці в сучасних умовах розвитку виробничих технологій. Український журнал будівництва та архітектури. 2021. № 6. С. 69-74. URL: https://repository.lntu.edu.ua/handle/123456789/4240

18. Sivakovska O., Rudynets M., Yashchuk A., Redko R., Zabolotnyi O. Project Safety Management Systems of Students with 3D Game Development. 5th EAI International Conference on Management of Manufacturing Systems (Cham, 03 August 2021). P. 459-468. URL: https://repository.lntu.edu.ua/handle/123456789/4277

Праці інших авторів:

19. Готович В. А., Карташов В. В., Максим’як Ю. Б., Матійчук Л. П. Задача розробки програмної платформи для місцевої автоматизованої системи централізованого оповіщення. 2025 · Комп’ютерно-інтегровані технології: освіта, наука, виробництво, № 59, с. 88–96. DOI: 10.36910/6775-2524-0560-2025-59-12

20. Тютюник В. В., Тютюник О. О., Усачов Д. В. Особливості застосування нечітких когнітивних карт для сценарного моделювання функціонування критичної інфраструктури в умовах надзвичайних ситуацій воєнного характеру. 2025 · Сучасні інформаційні технології у сфері безпеки та оборони, т. 54, № 3, с. 93–102. DOI: 10.33099/2311-7249/2025-54-3-93-102

21. Рубан І., Тютюник В., Тютюник О. Особливості створення системи підтримки прийняття антикризових рішень в умовах невизначеності вхідної інформації при надзвичайних ситуаціях. 2021 · Сучасні інформаційні технології у сфері безпеки та оборони, т. 40, № 1, с. 75–84. DOI: 10.33099/2311-7249/2021-40-1-75-84

22. Сніцаренко П., Кацалап В. Методичний підхід щодо синтезу систем моніторингу інформаційного простору за критерієм оптимальності в інтересах сил оборони України. 2022 · Сучасні інформаційні технології у сфері безпеки та оборони, т. 44, № 2, с. 82–88. DOI: 10.33099/2311-7249/2022-44-2-82-88

III. Інформаційні ресурси

23. FloodMap – онлайн-сервіс для моделювання затоплень. URL: https://floodmap.net/

24. Google Maps – карта для аналізу інфраструктури та орієнтування на місцевості. URL: https://maps.google.com/

25. ArcGIS Online – інструмент для картографічного аналізу та побудови карт ризиків. URL: https://www.arcgis.com/

26. Державна служба України з надзвичайних ситуацій (ДСНС) – інформація про управління надзвичайними ситуаціями. URL: https://dsns.gov.ua/.

27. Кодекс цивільного захисту України. – Режим доступу: URL: https://zakon.rada.gov.ua/laws/show/5403-17#Text

28. Forecast: онлайн-інструмент для швидкого розрахуноку зон хімічного ураження та візуалізація наслідків аварій на інтерактивній карті. URL: http://forecast.inf.ua/.

29. NUKEMAP – онлайн-інструмент для моделювання ядерних вибухів. URL: https://nukemap.org/

30. ДСТУ 2226-93 Автоматизовані системи. Терміни та визначення. URL: https://online.budstandart.com/ua/catalog/doc-page.html?id_doc=61937.

31. ДБН В.2.5-76:2014 Автоматизовані системи раннього виявлення загрози виникнення надзвичайних ситуацій та оповіщення населенняю URL: https://online.budstandart.com/ua/catalog/doc-page.html?id_doc=57710.

32. ComputerWorld Украина. [Електронний ресурс] / Режим доступу до ресурсу:

https://www.computerworld.com.ua

33. Державна служба України з надзвичайних ситуацій [Електронний ресурс] / Режим доступу до ресурсу: https://dsns.gov.ua/.

34. Верховна Рада України: офіційний веб-сайт. URL: www.rada.gov.ua

35. Кабінет Міністрів України: офіційний веб-сайт. URL: www.kmu.gov.ua

36. Служба підтримки Microsoft. URL: https://support.microsoft.com/uk-ua

37. Офіційний сайт Mathcad (PTC). URL: https://www.ptc.com/en/products/mathcad.