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

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

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

СИЛАБУС

з освітнього компонента «Системи охорони периметрів»
ступінь вищої освіти – бакалавр
галузь знань – 12 Інформаційні технології
спеціальність – 126 Інформаційні системи і технології
освітня програма – Інформаційні системи та технології охорони і безпеки

Кафедра комп'ютерної інженерії та охоронних систем

Силабус склав(ла) доцент кафедри комп'ютерної інженерії та охоронних систем, к.т.н., доцент Олег КАЙДИК

Силабус затверджений на засіданні кафедри комп'ютерної інженерії та охоронних систем, протокол № 1/1 від «29» серпня 2026 р.

Завідувач кафедри к.т.н., доцент Тарас ТЕРЛЕЦЬКИЙ

Розглянуто та схвалено групою забезпечення освітньої програми «Інформаційні системи та технології охорони і безпеки», протокол № 2 від «29» серпня 2026 р.

Гарант ОП «Інформаційні системи та технології охорони і безпеки» к.т.н., доцент Тарас ТЕРЛЕЦЬКИЙ

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

Затверджений силабус онлайн:
https://e.lntu.edu.ua/syllabus/477

Луцьк – 2026

СИЛАБУС ОСВІТНЬОГО КОМПОНЕНТА «Системи охорони периметрів»

Освітня програма	Інформаційні системи та технології охорони і безпеки
Галузь знань / Спеціальність	12 Інформаційні технології / 126 Інформаційні системи і технології
Рівень вищої освіти	перший (бакалаврський)
Статус дисципліни	нормативна
Мова викладання	українська
Обсяг	5 кредитів ECTS / 150 годин, семестр 7
Форма контролю	екзамен, курсовий проєкт
Викладач(і)	к.т.н., доцент Олег КАЙДИК

1. Мета і завдання дисципліни

Мета: Набуття здобувачами вищої освіти комплексних теоретичних знань та практичних навичок у сфері проектування, встановлення, експлуатування та обслуговування сучасних технічних засобів і систем, які призначені для захисту фізичного периметра об’єктів різного призначення.

Завдання: Ознайомити здобувачів вищої освіти із теоретичним основам функціонування системи охорони периметрів (класифікація технічних засобів, нормативна база та методика аналізу ризиків для розроблення ефективної стратегії захисту). Опанувати технологічні знання щодо принципів роботи, характеристик й впливу зовнішніх чинників на роботу засобів виявлення порушень периметра. Сформувати практичні навички проектування (розроблення технічного завдання, виконання необхідних розрахунків, створення схем розміщення елементів охорони, їх монтаж і первинне налаштування).

Пререквізити: Основи теорії та проектування систем охоронної та пожежної сигналізацій, САПР систем охорони та безпеки

2. Компетентності

ЗК02 — Здатність застосовувати знання у практичних ситуаціях.

ЗК03 — Здатність до розуміння предметної області та професійної діяльності.

ЗК05 — Здатність вчитися і оволодівати сучасними знаннями.

ЗК06 — Здатність до пошуку, оброблення та узагальнення інформації з різних джерел.

СК05 — Здатність оцінювати та враховувати економічні, соціальні, технологічні та екологічні фактори на всіх етапах життєвого циклу інфокомунікаційних систем.

СК06 — Здатність використовувати сучасні інформаційні системи та технології (виробничі, підтримки прийняття рішень, інтелектуального аналізу даних та інші), методики й техніки кібербезпеки під час виконання функціональних завдань та обов’язків.

СК10 — Здатність вибору, проектування, розгортання, інтегрування, управління, адміністрування та супроводжування інформаційних систем, технологій та інфокомунікацій, сервісів та інфраструктури організації.

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

№	Назва теми	Лекції денна/ заочна	Практ./ Семін. денна/ заочна	Лаб. денна/ заочна	Самост. робота денна/ заочна	Разом	Методи навчання	Методи оцінювання	ЗК та СК

№	Назва теми	**Лекції** денна/ заочна	**Практ./ Семін.** денна/ заочна	**Лаб.** денна/ заочна	**Самост. робота** денна/ заочна	**Разом**	**Методи навчання**	**Методи оцінювання**	**ЗК та СК**
Змістовий модуль 1. Теоретичні засади охорони периметрів та класифікація технічних засобів виявлення									
1	Тема 1. Основи фізичного захисту периметрів	4/1	3/0,6	3/1	20/32	30/34,6	МН1, МН2, МН3, МН4, МН6	МО1, МО2, МО4	ЗК02, ЗК03, ЗК05, ЗК06, СК05
2	Тема 2. Класифікація та принципи роботи технічних засобів виявлення	12/1	6/1,6	6/1,5	25/42	49/46,1	МН1, МН2, МН3, МН4, МН6	МО1, МО2, МО4	ЗК02, ЗК03, ЗК05, ЗК06, СК05, СК06
Змістовий модуль 2. Проектування, вибір та експлуатація систем охорони периметрів									
3	Тема 3. Проектування системи охорони периметрів та вибір технічних засобів	6/1	4/1,2	6/1,5	25/32	41/35,7	МН1, МН2, МН3, МН4, МН6	МО1, МО2, МО4, МО7	ЗК02, ЗК03, ЗК05, ЗК06, СК05, СК06, СК10
4	Тема 4. Особливості експлуатації засобів виявлення в системах охорони периметрів	8/1	2/0,6	0/0	20/32	30/33,6	МН1, МН2, МН3, МН4, МН6	МО1, МО2, МО4	ЗК02, ЗК03, ЗК05, ЗК06, СК05, СК06, СК10
	Разом	**30/4**	**15/4**	**15/4**	**90/138**	**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); МН6 — самостійна робота (розв'язання завдань).

Методи оцінювання: МО1 — екзамен; МО2 — усне або письмове опитування; МО4 — тестування; МО7 — презентації результатів виконаних завдань та досліджень.

4. Результати навчання

ПРН05. Аргументувати вибір програмних та технічних засобів для створення інформаційних систем та технологій на основі аналізу їх властивостей, призначення і технічних характеристик з урахуванням вимог до системи і експлуатаційних умов; мати навички налагодження та тестування програмних і технічних засобів інформаційних систем та технологій.

ПРН14. Здійснювати проектування інформаційних систем охорони і безпеки із врахуванням специфіки об'єктів захисту у різних галузях людської діяльності та національної безпеки у

відповідності до чинних нормативних документів і забезпечувати взаємне узгодження технічних параметрів їх складових.

Після успішного завершення цього курсу здобувачі освіти зможуть самостійно здійснювати аудит вразливостей, розробляти проєктно-кошторисну документацію та проєктувати багаторівневі комплексні системи фізичного захисту периметра. Також вони зможуть опанувати навички підбору, монтажу, калібрування та інтеграції сучасних засобів виявлення для ефективного захисту об'єктів будь-якої складності.

5. Неформальна освіта

Підтверджені результати навчання, здобуті у формальній, неформальній чи інформальній освіті, можуть бути визнані відповідно до процедур ЛНТУ.

6. Критерії та форми контролю

Оцінювання — за 100-бальною шкалою (національна шкала / ЄКТС). Підсумковий бал = поточний контроль (20 %) + модульний контроль (20 %) + курсовий проєкт (30 %) + екзамен (30 %).

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

7. Зміст тем

Тема 1. Основи фізичного захисту периметрів

Загальні принципи охорони периметрів.
Типові вимоги, які висуваються до загороджень охоронних периметрів.
Шляхи подолання зловмисниками загороджень охоронних периметрів.

Тема 2. Класифікація та принципи роботи технічних засобів виявлення

Загальна класифікація засобів виявлення.
Радіохвильові засоби виявлення.
Провідниково-хвильові засоби виявлення.
Засоби виявлення, які працюють за принципом «лінії витікаючої хвилі».
Сейсмічні засоби виявлення.
Манометричні засоби виявлення.
Оптично-електронні засоби виявлення.
Вібраційні засоби виявлення.
Волоконно-оптичні засоби виявлення.
Комбіновані й інтегровані засоби виявлення.
Радіолокаційні засоби виявлення.

Тема 3. Проектування системи охорони периметрів та вибір технічних засобів

Проектування системи охорони периметрів.
Вибір та застосування технічних засобів для моніторингу стану периметра.

Тема 4. Особливості експлуатації засобів виявлення в системах охорони периметрів

Типові варіанти побудови системи охорони периметрів, яка експлуатується за простих умов.
Типові варіанти побудови системи охорони периметрів, яка експлуатується за складних умов.

8. Курсовий проєкт

Робочим навчальним планом освітньої програми «Інформаційні системи та технології охорони і безпеки» передбачено виконання здобувачами вищої освіти курсового проекту з курсу «Системи охорони периметрів». Курсовий проект виконується упродовж семестру. Виконання його є обов’язковою умовою успішного вивчення курсу та отримання позитивної оцінки.

Курсовий проект є однією із найважливіших форм навчального процесу, який спрямовано, переважно, на практичну підготовку здобувача освіти та виконується у відповідності до

навчальних планів.

Метою виконання курсового проекту є: закріплення, поглиблення та розширення теоретичних знань; оволодіння навичками самостійної роботи; вироблення вміння формулювати судження і висновки; логічно, послідовно і доказово їх викладати; вироблення уміння публічного захисту; підготовлення до вирішення більш складних інженерно-конструкторських задач.

Курсовий проект захищається в кінці семестру у години, які виділено навчальним планом. Під час виконання та оформлення курсового проекту здобувачу освіти дозволено використовувати наявну базу службової документації та необхідні програмні продукти.

Самостійне виконання курсового проекту дозволяє розвинути у здобувача вищої освіти навички самостійної роботи; систематизувати знання; закріпити теоретичні знання та практично застосувати їх у навчальному курсі. У ході виконання курсового проекту та його оформлення здобувач освіти використовує комп'ютерну техніку.

Курсовий проект оцінюється (максимально) 100-ма балами, які формують поточну успішність, а її виконання обов'язковою складовою модуля залікового кредиту.

Тема курсового проекту: «Проектування гібридної багатоступеневої системи охорони периметра (назва об'єкта)».

Тематика курсового проекту залежить від назви об'єкта, для якого необхідно спроектувати систему охорони периметра. Для проектування цієї системи передбачено наступні об'єкти

– військовий склад паливно-мастильних матеріалів;
– консервний цех та прилеглий склад готової продукції;
– територія автотранспортного підприємства;
– м'ясопереробний завод та комплекс холодильних складів;
– складський комплекс для зберігання зерна та мінеральних добрив;
– адміністративний комплекс льонокомбінату;
– клінічна лікарня;
– заклад вищої освіти;
– авто-/залізничний вокзал;
– підприємство з виготовлення торговельного обладнання.

Варіант курсового проекту з курсу «Системи охорони периметрів» визначається за індивідуальним номером здобувача вищої освіти та являє собою структуровану роботу, яка складається із трьох розділів:

– передпроектне обстеження об'єкта та оцінка ризиків (аналіз об'єкта, який охороняється, та його периметра; модель порушника та можливі шляхи проникнення; огляд наявних систем виявлення порушника на контрольованому периметрі);

– розроблення технічного рішення (обґрунтування вибору типу системи, вибір технічних засобів; структурна схема системи);

– інженерно-технічне та кошторисне обґрунтування системи охорони периметра (розрахунок довжини ділянок контролю та кількості сповіщувачів, розрахунок надійності системи; розрахунок вартості системи).

Інженерно-технічні розрахунки супроводжуються оформленням графічного матеріалу.

Оформлення курсового проекту – машинописний текст, схеми та кресленники. Об'єм роботи: до 25-30 аркушів ф. А4.

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

І. Навчально-методичні матеріали та розробки

Праці автора силабуса:

1. Системи охорони периметрів : конспект лекцій для здобувачів першого (бакалаврського) рівня вищої освіти освітньої програми «Інформаційні системи та технології охорони і безпеки» галузі знань 12 (F) Інформаційні технології спец. 126 (F6) Інформаційні системи та технології денної та заоч. форм навч. / уклад.: О. Л. Кайдик, Т. В. Терлецький. Луцьк : ЛНТУ, 2026. 92 с. URL: https://repository.lntu.edu.ua/handle/123456789/1435

2. Системи охорони периметрів : метод. вказівки до курсового проекту для здобувачів першого (бакалаврського) рівня вищої освіти освітньої програми «Інформаційні системи та технології охорони і безпеки» галузі знань 12 (F) Інформаційні технології спец. 126 (F6) Інформаційні системи та технології денної та заоч. форм навч. / уклад.: О. Л. Кайдик, Т. В. Терлецький. Луцьк : ЛНТУ, 2026. 36 с. URL: https://repository.lntu.edu.ua/handle/123456789/1345

3. Системи охорони периметрів: метод. вказівки до практичних занять для здобувачів першого (бакалаврського) рівня вищої освіти освітньої програми «Інформаційні системи та технології охорони і безпеки» галузі знань 12 (F) Інформаційні технології спец. 126 (F6) Інформаційні системи та технології денної та заоч. форм навч. / уклад.: О. Л. Кайдик, Т. В. Терлецький. Луцьк: ЛНТУ, 2026. 28 с. URL: https://repository.lntu.edu.ua/handle/123456789/2909

4. Системи охорони периметрів: метод. вказівки до лабораторних робіт для здобувачів першого (бакалаврського) рівня вищої освіти освітньої програми «Інформаційні системи та технології охорони і безпеки» галузі знань 12 (F) Інформаційні технології спец. 126 (F6) Інформаційні системи та технології денної та заоч. форм навч. / уклад.: О. Л. Кайдик, Т. В. Терлецький. Луцьк: ЛНТУ, 2026. 16 с. URL: https://repository.lntu.edu.ua/handle/123456789/2915

5. Системи охорони периметрів : метод. вказівки до самостійної роботи для здобувачів першого (бакалаврського) рівня вищої освіти освітньої програми «Інформаційні системи та технології охорони і безпеки» галузі знань 12 (F) Інформаційні технології спеціальності 126 (F6) Інформаційні системи та технології денної та заоч. форм навч. / уклад. О. Л. Кайдик, Т. В. Терлецький. Луцьк : ЛНТУ, 2025. 24 с. URL: https://repository.lntu.edu.ua/handle/123456789/931

Праці інших авторів:

6. Physical Security Systems Assessment Guide. URL: https://surl.li/icyrpg (дата звернення 25.08.2026).

7. Guide Perimeter Intrusion Detection Systems. URL: https://surl.lt/ljaibh (дата звернення 25.08.2026).

8. Fundamentals of Detection Systems in Physical Security. URL: https://rcmp.ca/sites/default/files/doc/gcpsg-gsmgc-021-eng.pdf (дата звернення 25.08.2026).

9. Perimeter Security Sensor TechnoLogies : Handbook. URL: https://surl.li/dshhyy (дата звернення 25.08.2026).

10. Perimeter Intrusion Detection Systems. URL: https://www.midches.com/resources/perimeter-detection-portal (дата звернення 25.08.2026).

11. Design and Evaluation of Physical Protection. URL: https://surl.li/xosdlc (дата звернення 25.08.2026).

ІІ. Наукові праці

Праці автора силабуса:

12. Bahniuk N., Terletskyi T., Kaidyk O., Kostiuchko S., Kondius I. Solving operational tasks in the design of video surveillance systems.

13. Dmytro Uhryn, Artem Karachevtsev, Taras Terletskyi, et al. Modern programming technologies in the tasks of identification and classification of military aircraft using machine learning algorithms. 2024. URL: https://repository.lntu.edu.ua/handle/123456789/5045

14. Taras Terletskyi, Oleh Kaidyk, Anatolii Tkachuk, Oleg Zabolotnyi, Dagmar Cagáňová. Ensuring the reliability of functioning of non-addressed fire alarm. 2022. URL: http://dx.doi.org/10.4108/eai.18-8-2021.170674

15. Taras Terletskyi, Oleh Kaidyk, Larysa Pylypiuk, Inna Kondius, Nina Zdolbitska. Determining the feasibility of applying existing criteria for solving operational problems in the design of CCTV information systems. 2023. URL: https://doi.org/10.31861/sisiot2023.1.01009

16. Пугач С. О., Кайдик О. Л., Терлецький Т. В., Угрин Д. І., Вісин О. О. ГІС-інструменти для аналізу та моделювання надзвичайних ситуацій (на прикладі пожеж у Волинській області). 2025. URL: https://repository.lntu.edu.ua/handle/123456789/5040

17. Puhach S., Slashchuk, A., Poruchynska, I., Kaidyk O. Regional Development and Communication Networks: Case Study of Western Ukraine. 2024. URL: https://repository.lntu.edu.ua/handle/123456789/5042

18. Терлецький Т. В., Кайдик О. Л., Данилюк Ю. М., Бас Р. В., Угрин Д. І. Обґрунтування параметрів відеокамер і тактик їх встановлення на периметрах об’єктів захисту. Комплексне забезпечення якості технологічних процесів та систем : матер. тез доп. XV міжн. наук.-практ. конф. (м. Чернігів, 22-23 травня 2025 р.). Чернігів, 2025. С. 257–258. URL: https://surl.lu/frircr

19. Іщук Д., Нестеровський А., Костючко С., Кайдик О., Терлецький Т. Система безпеки з використанням RFID та мобільних пристроїв. Програмне та апаратне забезпечення в інформаційних технологіях : матер. міжнар. наук.-практ. конф. (м. Луцьк, 6 травня 2025 р.). Луцьк, 2025. С. 72–73. URL: https://surli.cc/vdinpp

20. Кайдик О. Л., Терлецький Т. В., Меус О. С. До питання біометричної автентифіації. Інформаційні технології в освіті, техніці та промисловості : зб. тез доп. всеукр. наук.-техн. конф. молодих вчених і студентів (м. Івано-Франківськ, 13 жовтня 2022 р.). Івано-Франківськ, 2022. С. 56–57. URL: https://surl.li/kqscqf

21. Терлецький Т. В., Кайдик О. Л., Денисюк В. Ю., Пташенчук В. В., Приступа А. Л. Забезпечення необхідного рівня надійності розпізнавання об’єкта спостереження. Комплексне забезпечення якості технологічних процесів та систем : матер. тез доп. XI міжнар. наук.-практ. конф. (м. Чернігів, 26-27 травня 2021 р.). Чернігів, 2021. Т. 2. С. 167–169. URL: https://surl.li/oyladx

22. Терлецький Т., Кайдик О., Марчук М. Теоретико-практичні викладки до проектування відеоспостереження за протяжним периметром. Актуальні проблеми та перспективи розвитку фундаментальних, прикладних, загальнотехнічних та безпекових наук : матер. всеукр. наук.-практ. конф. (м. Київ, 21 червня 2023 р.). Київ, 2023. С. 229–333. URL: https://surl.li/ipjbup

23. Лахно В., Десятко А., Нікітенко Є., Кайдик О. Л. Предиктивний маркер цифрових слідів у системах підтримки прийняття рішень для протидії постквантовим кібератакам. КОМП’ЮТЕРНО-ІНТЕГРОВАНІ ТЕХНОЛОГІЇ: ОСВІТА, НАУКА, ВИРОБНИЦТВО. 2026. № 63. С. 185-193. https://doi.org/10.36910/6775-2524-0560-2026-63-20

24. Artemenko O., Dorenskyi O., Terletskyi T., Kaidyk O., Kramar A. The probabilistic approach to automated visual navigation in closed spaces. CEUR Workshop Proceedings: Applied Information Technologies and Artificial Intelligence Systems (AIT&AIS 2025). 2026. № 4160. 319–331. https://ceur-ws.org/Vol-4160/paper19.pdf

25. Artemenko O., Puhach S., Kaidyk O., Terletskyi T., Zdolbitska N. Analysis of Wildfires Using GIS Technologies (Case Study of Volyn Region, Ukraine). CEUR Workshop Proceedings: Applied Information Technologies and Artificial Intelligence Systems (AIT&AIS 2025). 2026. № 4160. P. 379-390. URL: https://ceur-ws.org/Vol-4160/paper22.pdf

26. Bahniuk N., Terletskyi T., Kaidyk O., Kostiuchko S., Kondius I. Solving operational tasks in the design of video surveillance systems. CEUR Workshop Proceedings: Applied Information Technologies and Artificial Intelligence Systems. 2025. P. 332-342. https://ceur-ws.org/Vol-4160/paper20.pdf

27. Лавренчук С. В., Кайди, О. Л., Мельник К. В., Конкевич Л. М., Лук’янчук Ю. В. Гібридна SQL/NoSQL архітектура для оптимізації продуктивності IoT-моніторингу якості повітря. КОМП’ЮТЕРНО-ІНТЕГРОВАНІ ТЕХНОЛОГІЇ: ОСВІТА, НАУКА, ВИРОБНИЦТВО. 2025. № 61. С. 112-118. https://doi.org/10.36910/6775-2524-0560-2025-61-16

28. Кайдик О. Л., Терлецький Т. В., Пугач С. О., Угрин Д. І., Артеменко О. І. Моделювання та підвищення надійності ідентифікації суб’єктів доступу в СКУД на основі гібридних PCA-алгоритмів. КОМП’ЮТЕРНО-ІНТЕГРОВАНІ ТЕХНОЛОГІЇ: ОСВІТА, НАУКА, ВИРОБНИЦТВО. 2025. № 61. С. 82-90. https://doi.org/10.36910/6775-2524-0560-2025-61-12

29. Пугач С. О., Кайдик О. Л., Терлецький Т. В., Угрин Д. І., Вісин О. О. ГІС-інструменти для аналізу та моделювання надзвичайних ситуацій (на прикладі пожеж у Волинській області). КОМП’ЮТЕРНО-ІНТЕГРОВАНІ ТЕХНОЛОГІЇ: ОСВІТА, НАУКА, ВИРОБНИЦТВО. 2026. № (60). С. 466-475. https://doi.org/10.36910/6775-2524-0560-2025-60-49

30. Krestyanpol L., Cheb D., Kaidyk O. Challenges and Issues in the Use of Certificate Formats in Modern Information Systems: Pathways to Enhancing Cybersecurity. Технологічні комплекси. 2025. Т. 17, № 2. С. 115-122. https://doi.org/10.36910/4293-52779-2025-17-02-09

31. Zdolbitska Nina, Ostapchuk Oleksandr, Lavrenchuk Svitlana, Terletskyi Tarasi, Kaidyk Oleh, Zhyharevych Oksana. Business information system for forecasting raw material stocks for the production of flexible packaging, I4th International Conference on Dependable Systems, Services and Technologies (DESSERT), Greece, October 11-13, 2024. PP. 1-8, doi: 10.1109/DESSERT65323.2024.11122240. URL: https://repository.lntu.edu.ua/handle/123456789/759

32. Угрин Д., Ушенко Ю., Дворжак В., Терлецький Т. В., Кайдик О. Л. Архітектура інтелектуальної системи управління ризиками та розпізнавання видів грибів. Оптико-електронні інформаційно-енергетичні технології. 2024. № 48 (2). С. 114–127. https://doi.org/10.31649/1681-7893-2024-48-2-114-127

33. Puhach S., Slashchuk A., Poruchynska I., Kaidyk O. Regional development and communication networks: Case study of Western Ukraine. Acta Scientiarum Polonorum Administratio Locorum. 2024. № 23 (3). P. 519–534. https://doi.org/10.31648/aspal.9282

34. Uhryn D., Karachevtsev A., Terletskyi T. Modern programming technologies in the tasks of identification and classification of military aircraft using machine learning algorithms. Photonics Applications in Astronomy, Communications, Industry, and High Energy Physics Experiments. 2024. Vol. 13400. P. 1-6. https://doi.org/10.1117/12.3054877

35. Апаратні та програмні засоби захисту інформації : метод. вказівки до лабораторних робіт для здобувачів першого (бакалаврського) рівня вищої освіти освітньої програми «Інформаційні системи та технології охорони і безпеки» галузі знань 12 Інформаційні технології спеціальності 126 Інформаційні системи та технології денної та заоч. форм навч. / уклад. О. Л. Кайдик, Т. В. Терлецький. Луцьк : ЛНТУ, 2025. 68 с. URL: https://repository.lntu.edu.ua/handle/123456789/773

36. Угрин Д., Кайдик О. Л., Циганчук А. Застосування методів штучного інтелекту для діагностики пухлин мозку. Інформаційні технології, економіка та право: стан і перспективи розвитку (ІТЕП-2025): матер. міжнар. наук.-практ. конф. (Чернівці, 09-10 жовт. 2025 р.). Чернівці, 2025. С. 32-33. URL: https://repository.lntu.edu.ua/handle/123456789/5034

37. Денисюк В. Ю., Кайдик О. Л., Марчук Н. А. Аналіз методів дослідження механічних властивостей нанооб'єктів. «Фізика і хімія твердого тіла. Стан, досягнення і перспективи»: матер. VII Всеукр. наук.-практ. конф. (м. Луцьк, 21-22 жовт. 2022 р.). Луцьк: ЛНТУ, 2022. С. 110-111. URL: https://repository.lntu.edu.ua/handle/123456789/3771

38. Kaidyk O., Terletskyi T., Ptashenchuk V., Denysiuk V. About Question of Organising of Physical Access Control System. «Priority directions of development of science and education» : Mater. of the III International research and practical internet conf (December, 24, 2021) : collection of abstracts. Zdar nad Sazavou: «DEL a.s.», 2021. Pp. 56-58. URL: https://repository.lntu.edu.ua/handle/123456789/3777

Праці інших авторів:

39. Bace, R., Mel, P. Intrusion Detection Systems. URL: https://surl.li/effqgz (дата звернення 25.08.2026).

40. Northcutt, S., Zeltser, L., Winters, S., Kent, K., Ritchey, R. W. Inside Network Perimeter Security. URL: https://surl.li/vevttx (дата звернення 25.08.2026).

41. Lohani, D., Crispim-Junior, C. F., Barthélemy, Q., Bertrand, S,. Robinault, L., Tougne. L. Perimeter Intrusion Detection by Video Surveillance: A Survey. URL: https://hal.science/hal-03693500v1/file/main.pdf (дата звернення 25.08.2026).

42. Scarfone, K., Mell, P. Guide to Intrusion Detection and Prevention Systems. URL: https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-94.pdf (дата звернення 25.08.2026).

III. Інформаційні ресурси

43. Fence Security Products : Integrated with PSIM and VMS Under European Standards EN 50131. URL: https://surl.li/cjhezp (дата звернення 25.08.2026).

44. Manufacturer of Perimeter Intrusion Detection Systems for Sensitive Sites URL: https://surl.li/bpgsoc (дата звернення 25.08.2026).

45. Perimeter Intrusion Detection : VibraSector URL: https://surl.li/ysasbv (дата звернення 25.08.2026).

46. Perimeter Intrusion Detection and Security : Protecting critical infrastructure and assets. URL: https://surl.lu/tyocnu (дата звернення 25.08.2026).

47. Perimeter Intrusion Detection System using Sensors, PTZ Cameras & AI. URL: https://surl.li/hwaant (дата звернення 25.08.2026).

48. Perimeter Protection and Intrusion Detection. For commercial and critical infrastructure sites. URL: https://surl.lt/szvkqq (дата звернення 25.08.2026).

49. Qualitative Requirement of Perimeter Intrusion Detection System. URL: https://surl.li/irvdrf (дата звернення 25.08.2026).