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 контрою та управління доступом»
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/482

Луцьк – 2026

СИЛАБУС ОСВІТНЬОГО КОМПОНЕНТА «Системи контрою та управління доступом»

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 5
Форма контролю	екзамен
Викладач(і)	к.т.н., доцент Олег КАЙДИК

1. Мета і завдання дисципліни

Мета: Набуття здобувачами вищої освіти необхідних знань та практичних навичок у сфері проектування, впровадження та управління системами контролю доступу.

Завдання: Ознайомити здобувачів вищої освіти із принципами роботи систем контролю доступу, їх типами та функціональними можливостями. Сформувати навички для оцінювання ризиків і загроз, які пов’язаних із доступом до об’єкту та розроблення систем контролю доступу враховуючи специфіку політики безпеки.

Пререквізити: Мікропроцесорна техніка та промислові контролери, Технології захисту інформації

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.

СК01 — Здатність аналізувати об’єкт проектування або функціонування та його предметну область.

СК02 — Здатність застосовувати стандарти в області інформаційних систем та технологій при розробці функціональних профілів та систем, побудові та інтеграції систем, продуктів, сервісів і елементів інфраструктури організацій.

СК04 — Здатність проектувати, розробляти та використовувати засоби реалізації інформаційних систем, технологій та інфокомунікацій (методичні, інформаційні, алгоритмічні, технічні, програмні та інші).

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

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

СК16 — Здатність до програмування контролерів інформаційних систем охорони і безпеки.

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
Змістовий модуль 1. Вступ до систем контролю та управління доступом									

№	Назва теми	Лекції денна/ заочна	Практ./ Семін. денна/ заочна	Лаб. денна/ заочна	Самост. робота денна/ заочна	Разом	Методи навчання	Методи оцінювання	ЗК та СК
1	Тема 1. Загальна характеристика СКУД	4/0,5	0/0	2/0,5	10/18	16/19	МН1, МН2, МН3, МН4, МН6	МО1, МО2, МО4	ЗК02, ЗК03, ЗК05, ЗК06, СК01, СК02, СК05
2	Тема 2. Організація СКУД	4/0,5	0/0	4/1,5	10/18	18/20	МН1, МН2, МН3, МН4, МН6	МО1, МО2, МО4	ЗК02, ЗК03, ЗК05, ЗК06, СК01, СК02, СК04, СК05, СК10
3	Тема 3. Методи та засоби ідентифікації в СКУД	4/1	8/0,6	4/1,5	10/18	26/21,1	МН1, МН2, МН3, МН4, МН6	МО1, МО2, МО4	ЗК02, ЗК03, ЗК05, ЗК06, СК01, СК02, СК04, СК05, СК10
4	Тема 4. Біометричні системи ідентифікації	4/1	10/0,4	2/1	10/18	26/20,4	МН1, МН2, МН3, МН4, МН6	МО1, МО2, МО4	ЗК02, ЗК03, ЗК05, ЗК06, СК01, СК02, СК04, СК05, СК10, СК16
Змістовий модуль 2. Вибір та реалізація систем контролю доступом									
5	Тема 5. Вибір СКУД для облаштування об’єкта доступу	4/1	12/1	0/0	13/22	29/24	МН1, МН2, МН3, МН4, МН6	МО1, МО2, МО4	ЗК02, ЗК03, ЗК05, ЗК06, СК01, СК02, СК04, СК05, СК10, СК16
6	Тема 6. Особливості СКУД для великих розподілених об’єктів доступу	4/1	0/0	0/0	10/20	14/21	МН1, МН2, МН3, МН4, МН6	МО1, МО2, МО4	ЗК02, ЗК03, ЗК05, ЗК06, СК01, СК02, СК04, СК05, СК10, СК16
7	Тема 7. Загороджувальні керовані пристрої в СКУД	6/1	0/0	3/1,5	12/22	21/24,5	МН1, МН2, МН3, МН4, МН6	МО1, МО2, МО4	ЗК02, ЗК03, ЗК05, ЗК06, СК01, СК02, СК04, СК05, СК16, СК10
	Разом	**30/6**	**30/2**	**15/6**	**75/136**	**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.

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.

ПРН10. Розуміти і враховувати соціальні, екологічні, етичні, економічні аспекти, вимоги охорони праці, виробничої санітарії, пожежної безпеки та існуючих державних і закордонних стандартів під час формування технічних завдань та рішень.

ПРН11. Демонструвати вміння розробляти техніко-економічне обґрунтування розроблення інформаційних систем та технологій та вміти оцінювати економічну ефективність їх впровадження.

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 вищої освіти зможуть проектувати, налаштовувати та адмініструвати сучасні фізичні й мережеві системи контролю доступу для будь-яких об'єктів. Зокрема, вони набудуть достатньо знань для роботи фахівцями з інсталяції Smart Home та IoT-рішень, системними інтеграторами або інженерами з технічних засобів охорони й безпеки.

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 (30 %) + екзамен (50 %).

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. Загальна характеристика СКУД

Основні поняття, термінологія та визначення системи контролю та управління доступом.
Критерії оцінювання СКУД та їх класифікація.
Вимоги, які висуваються до СКУД.

Тема 2. Організація СКУД

Узагальнена структурна схема СКУД.
Структура зон доступу.
Маршрути переміщення суб’єкта доступу.
Особливості точок доступу.
Математична модель СКУД.

Тема 3. Методи та засоби ідентифікації в СКУД

Основні методи та типи ідентифікації.
Пасивна радіочастотна технологія ідентифікації.
Штрихові коди.
Карти Віганда.
Безконтактні смарт-карти.

Тема 4. Біометричні системи ідентифікації

Біометричний метод ідентифікації.
Ідентифікація на основі квазістатистичних ознак.
Ідентифікація на основі квазідинамічних ознак.
Перспективні напрямки біометричних систем ідентифікації.

Тема 5. Вибір СКУД для облаштування об’єкта доступу

Огляд об’єкта доступу на можливість застосування СКУД.
Вимоги, які висуваються до основних компонентів СКУД.
Типові варіанти СКУД.

Тема 6. Особливості СКУД для великих розподілених об’єктів доступу

Централізована архітектура СКУД.
Розподілена архітектура СКУД.
Змішана архітектура СКУД.
Програмне забезпечення для великих СКУД.

Тема 7. Загороджувальні керовані пристрої в СКУД

Класифікація ЗКП.
Загальні технічні вимоги, які висуваються до ЗКП.
Виконавчі пристрої для контролю суб’єкта доступу у приміщенні.
Виконавчі пристрої для контролю суб’єкта доступу на КПП.

8. Опис ІЗ/КПІЗ

Не передбачено навчальним планом.

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 контролю та управління доступом : конспект лекцій 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 деннної та заоч. форм навч. / уклад. О. Л. Кайдик, Т. В. Терлецький, А. А. Ткачук. Луцьк : ЛНТУ, 2025. 132 с. URL: https://repository.lntu.edu.ua/handle/123456789/619

2. Системи контролю та управління доступом : методичні 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. 20 с. URL: https://repository.lntu.edu.ua/handle/123456789/620

3. Кайдик О. Л., Терлецький Т. В., Угрин Д. І., Кондіус І. С. Системи контрою та управління

доступом: навч. посіб. для студ. техн. спец. Луцьк: ЛНТУ, 2026. 240 с. URL: https://repository.lntu.edu.ua/handle/123456789/4952

Праці інших авторів:

4. Boddu, Raghu. SAP Access Control. Quincy : SAP PRESS, 2023. 695 p.

5. Kris, Hermans. Mastering Access Control : A Comprehensive Guide to Learn Access Control. Traverse City : Independently published, 2023. 393 p.

6. Mike, Chapple. Access Control and Identity Management. URL: https://surl.li/hrotpw (дата звернення 26.08.2026).

II. Наукові праці

Праці автора силабуса:

7. 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

8. 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. Photonics Applications in Astronomy, Communications, Industry, and High Energy Physics Experiments. 2024. Vol. 13400. P. 1-6. https://doi.org/10.1117/12.3054877

9. 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

10. 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

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

12. Кайдик О. Л., Терлецький Т. В., Назарчук А. О., Угрин Д. І., Шкідіна К. С. Про одноразові паролі, як механізм підвищення безпеки системи контролю та управління доступом. 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. 267-268. URL: https://surl.lu/frircr

13. Мотрунчик Д., Садовий М., Кайдик О., Терлецький Т., Приступа А. Про віддалену реєстрацію суб’єктів доступу в СКУД. Програмне та апаратне забезпечення в інформаційних технологіях : матер. міжнар. наук.-практ. конф. (м. Луцьк, 6 травня 2025 р.). Луцьк, 2025. С. 128-129. URL: https://surli.cc/vdinpp

14. Кайдик О. Л., Терлецький Т. В., Кондіус І. С., Меус О. С., Остапюк В. В. До питання організації процедури ідентифікування суб’єктів доступу в СКУД. Прогресивні напрямки розвитку автоматичних технологічних комплексів : зб. наук. праць VII міжнар. наук.-техн. конф. (м. Луцьк, 28-30 травня 2024 р.). Луцьк, 2024. С. 82-84. URL: http://surl.li/vwsjfy

15. Меус О., Кайдик О., Кошелюк В., Терлецький Т., Мотрунчик Д. Про структурні підходи до ідентифікування об’єктів доступу та їх недоліки. 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. 246-247. URL: https://surl.li/ipjbup

16. Кайдик О. Л., Терлецький Т. В., Меус О. С., Садовий М. О., Бас Р. В. Методи розпізнавання за геометрією кисті руки. Приладобудування та метрологія : сучасні проблеми, тенденції розвитку : матер. тез доп. V всеукр. наук.-практ. конф. (м. Луцьк, 20-22 жовтня 2022 р.). Луцьк, 2022. С. 37-38. URL: https://surl.li/wyejwc

Праці інших авторів:

17. Rahaman, M. S., Tisha, S. N., Song, E., & Cerny, T. (2023). Access Control Design Practice and Solutions in Cloud-Native Architecture: A Systematic Mapping Study. Sensors, 23(7), 3413. https://doi.org/10.3390/s23073413

18. Farhadighalati, N., Estrada-Jimenez, L. A., Nikghadam-Hojjati S., & Barata J. (2025) A Systematic Review of Access Control Models: Background, Existing Research, and Challenges. IEEE Access, 13, 17777-17806. https://doi: 10.1109/ACCESS.2025.3533145

19. Ahsan, M. S., & Pathan, A.-S. K. (2025). A Comprehensive Survey on the Requirements, Applications, and Future Challenges for Access Control Models in IoT: The State of the Art. IoT, 6(1), 9. https://doi.org/10.3390/iot6010009

20. Shafei, H. A. & Tan, C. C. (2024). A Closer Look at Access Control in Multi-User Voice Systems. IEEE Access, 12, 40933-40946. https://doi.org/10.1109/ACCESS.2024.3379141.

21. Mangla, M. (2025). Behavioral Analytics and AI in Zero Trust Security: A Framework for Adaptive Identity and Access Management. International Journal Science and Technology. https://doi.org/10.56127/IJST.V4I1.2275

III. Інформаційні ресурси

22. Access Control Systems : Security, Identity Management and Trust Models. URL: https://surl.li/soqebk (дата звернення 26.08.2026).

23. Access Control Technologies : Handbook. URL: https://www.dhs.gov/sites/default/files/publications/ACT-HB_0915-508.pdf (дата звернення 26.08.2026).

24. Access Control: Training Book. URL: https://surl.li/ebwgps (дата звернення 26.08.2026).

25. Brian, Rhodes. Access Control. URL: https://ipvm-uploads.s3.amazonaws.com/uploads/5b71/626a/Access-Control-101-Book.pdf (дата звернення 26.08.2026).

26. Harold F., Tipton, Micki, Krause. Information Security Management : Handbook. URL: https://books.google.com.ua/books?id=B0Lwc6ZEQhcC&printsec=frontcover&redir_esc=y#v=onepage&q&f=false (дата звернення 26.08.2026).

27. Thomas, Norman. Electronic Access Control. URL: https://books.google.com.ua/books?id=hFZHYDy4Oe8C&printsec=frontcover&redir_esc=y#v=onepage&q&f=false (дата звернення 26.08.2026).

28. Access Control Systems : Contents. URL: https://en.dictator.de/wp-content/uploads/K8E-Access-Control-Systems.pdf (дата звернення 26.08.2026).

29. Designing and Installing Access Control Solutions : A Practical Guide for Professionals. URL: https://cctvdvrsystem.co.uk/wp-content/uploads/2021/08/Access-Control-Installation-E-book.pdf (дата звернення 26.08.2026).

30. Getting Started With Physical Access Control. URL: https://go.getgenea.com/hubfs/Genea%20Assets/eBook-%20Physical%20Access%20Control.pdf (дата звернення 26.08.2026).

31. Introduction to Access Control Systems : A guide to getting started with access control. URL: https://www.scribd.com/document/527498501/Kisi-Introduction-to-Access-Control-Systems (дата звернення 26.08.2026).

32. Matej Csányi. Access Control in Operating Systems. URL: https://is.muni.cz/th/uny2u/xcsanyi_bc.pdf (дата звернення 26.08.2026).

33. Our Service is Your Security : Products Catalog. URL: https://www.full-protection.com/downloads/3-Catalog-Full-Protection-ACCESS%20CONTROL.pdf (дата звернення 26.08.2026).

34. Security and Privacy Controls for Information Systems and Organizations. URL: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5.pdf (дата звернення 26.08.2026).

35. Standard: Access Control. URL: https://www.sjsu.edu/it/docs/security/policies-standards/Standard_Access_Control.pdf (дата звернення 26.08.2026).

36. Understanding Different Types of Access Control in Cybersecurity. URL: https://searchinform.com/articles/cybersecurity/access-control/types-of-access-control/ (дата звернення 26.08.2026).