МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
Луцький національний технічний університет

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 заочної форм навчання

Луцьк 2025

УДК 681.52:004.056
С34

Рекомендовано до видання вченою радою факультету комп'ютерних та інформаційних технологій ЛНТУ, протокол № ___ від _____ 2025 року.

Голова Вченої ради факультету КІТ _____ Інна КОНДІУС

Електронна копія друкованого видання передана для внесення в репозитарій ЛНТУ

Директор бібліотеки _____ Наталія ПОЛІЩУК

Розглянуто і схвалено на засіданні кафедри комп'ютерної інженерії та безпеки ЛНТУ, протокол № ___ від _____ 2025 року

Укладачі: _____ Олег КАЙДИК, кандидат технічних наук, доцент кафедри комп'ютерної інженерії та безпеки ЛНТУ

_____ Тарас ТЕРЛЕЦЬКИЙ, кандидат технічних наук, завідувач кафедри комп'ютерної інженерії та безпеки ЛНТУ

Рецензент: _____ Роман ЧУБАЙ, інженер-проектувальник 1 категорії ТОВ «ЄВРОФЕСТ»

Відповідальний за випуск: _____ Тарас ТЕРЛЕЦЬКИЙ, кандидат технічних наук, завідувач кафедри комп'ютерної інженерії та безпеки ЛНТУ

С34 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 заочної форм навчання / уклад. О. Л. Кайдик, Т. В. Терлецький. Луцьк : ЛНТУ, 2025. 20 с.

Методичні вказівки для самостійної роботи спрямовано на ґрунтовну підготовку здобувачів освіти з курсу «Системи контролю та управління доступом». У ньому визначено мету, завдання курсу, а також наведено перелік необхідних інформаційних джерел, які допоможуть ефективно опрацювати, винесених на самостійне вивчення, матеріал.

Для контролю знань передбачено тестові завдання для самооцінювання, а повний перелік екзаменаційних питань допоможе якісно підготуватися до підсумкової атестації.

ВСТУП

Сучасний етап розвитку засобів контролю й управління доступом характеризується їх глибоким проникненням в усі сфери людської діяльності, включаючи галузь охорони та безпеки. Ефективне проектування, розробка, впровадження та експлуатація сучасних рішень безпеки, у цій критично важливій сфері, вимагають не лише високого рівня професійної підготовки фахівців, але й глибокого розуміння принципів захисту захищених зон.

Враховуючи вищесказане бачимо, що дисципліна «Системи контролю та управління доступом» займає важливе місце у підготовці бакалаврів за освітньою програмою «Інформаційні системи та технології охорони і безпеки».

Метою вивчення цієї дисципліни є формування у здобувачів вищої освіти комплексної системи знань відносно теоретичних й практичних аспектів побудови, функціонування та адміністрування сучасних СКУД. Опанування принципів, методів та процедур ідентифікації, автентифікації та авторизації дозволить майбутнім фахівцям забезпечувати санкціонований доступ, захист критичної інфраструктури та безпеку інформаційних і фізичних ресурсів, що є ключовими чинниками їх ефективної експлуатації.

Самостійна робота є невід'ємною складовою освітнього процесу й спрямована на поглиблення, розширення та закріплення теоретичних знань, а також набуття практичних навичок у сфері проектування, встановлення та супроводу СКУД.

Методичні вказівки для самостійної роботи з курсу «Системи контролю та управління доступом» містять перелік тем для самостійного опрацювання, орієнтовні питання для контролю розуміння матеріалу, завдання практичного характеру, а також рекомендації щодо підготовки до контрольних заходів. Успішне виконання завдань, які передбачено цими виданням, дозволить здобувачам вищої освіти не лише якісно підготуватися до поточного та підсумкового контролю, але й сформувати необхідні компетентності для подальшої професійної діяльності у цій сфері їх діяльності.

ЗМІСТ

1 МЕТА ТА ЗАВДАННЯ ДИСЦИПЛІНИ

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

Завдання вивчення дисципліни. 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.

Найменування та опис компетентностей, формування котрих забезпечує вивчення дисципліни:

– загальні компетентності:

КЗ 2. Здатність застосовувати знання у практичних ситуаціях;

КЗ 3. Здатність до розуміння предметної області та професійної діяльності;

КЗ 5. Здатність вчитися і оволодівати сучасними знаннями.

КЗ 6. Здатність до пошуку, оброблення та узагальнення інформації з різних джерел.

– спеціальні компетентності:

КС 1. Здатність аналізувати об'єкт проектування або функціонування та його предметну область;

КС 2. Здатність застосовувати стандарти в області інформаційних систем та технологій при розробці функціональних профілів та систем охорони і безпеки, побудові та інтеграції систем, продуктів, сервісів і елементів інфраструктури об'єкта захисту.

КС 4. Здатність проектувати, розробляти та використовувати засоби реалізації інформаційних систем, технологій та інфокомунікацій (методичні, інформаційні, алгоритмічні, технічні, програмні та інші).

КС 5. Здатність оцінювати та враховувати економічні, соціальні, технологічні та екологічні фактори на всіх етапах життєвого циклу інфокомунікаційних систем.

КС 10. Здатність вибору, проектування, розгортання, інтегрування, управління, адміністрування та супроводжування інформаційних систем, технологій та інфокомунікацій, сервісів та інфраструктури організації.

КС 16. Здатність до програмування контролерів інформаційних систем охорони і безпеки.

Результати навчання. Результати навчання вивчення дисципліни «Системи контролю та управління доступом» базуються на програмних

результатах навчання:

ПРН 5. 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.

ПРН 10. 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.

ПРН 11. Демонструвати вміння розробляти техніко-економічне обґрунтування розроблення інформаційних систем та технологій та вміти оцінювати економічну ефективність їх впровадження.

ПРН 14. 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.

2 САМОСТІЙНА РОБОТА

Самостійна робота №1

Тема. Загальна характеристика СКУД.

Мета: сформувати у слухачів базову систему знань щодо термінології, класифікації та основних вимог, які висуваються до СКУД, як ключового елемента інтегрованої системи безпеки об'єкта.

Завдання: опрацювати матеріал та дати відповіді на запитання.

Рекомендована література: [1; 2; 3; 4; 5; 7; 8; 9].

Запитання для самоконтролю

1. Вимоги безпеки, які необхідно враховувати під час проектуванні СКУД?
2. Вимоги, які висуваються до інтеграції СКУД із іншими системами безпеки.
3. Класифікація СКУД.
4. Ключова термінологія для розуміння роботи СКУД.
5. Компоненти СКУД.
6. Критерії оцінювання ефективності СКУД.
7. Основні поняття та функції СКУД.

8. Технології, які використовуються у СКУД.

Самостійна робота №2

Тема. Організація СКУД.

Мета: сформувати у слухачів системне розуміння принципів побудови, функціонування та моделювання сучасних СКУД, як важливої складової інтегрованої системи безпеки об'єкта.

Завдання: опрацювати матеріал та дати відповіді на запитання.

Рекомендована література: [1; 2; 3; 5; 7; 9].

Запитання для самоконтролю

1. Вплив маршрутів переміщення суб'єктів доступу на безпеку об'єкта.
2. Вплив технологій на забезпечення функціональності точок доступу.
3. Вплив типу точки доступу на загальну безпеку системи.
4. Етапи процесу переміщення суб'єкта доступу в СКУД.
5. Ефективність СКУД на основі моделювання системи.
6. Моніторинг маршрутів переміщення суб'єктів доступу?
7. Оптимізація СКУД за математичною моделлю.
8. Основні компоненти структурної схеми СКУД.
9. Складові математичної моделі СКУД.
10. Технології для з'єднання компонентів СКУД?
11. Типи точок доступу. Зона доступу та її основні елементи.
12. Функції елементів СКУД та їх взаємодія.
13. Які чинники, необхідно враховувати під час проектування зон доступу в СКУД?

Самостійна робота №3

Тема. Методи та засоби ідентифікації в СКУД.

Мета: сформувати у слухачів комплексні знання про ключові методи, технології та засоби, які використовуються для ідентифікації суб'єктів об'єктів доступу у сучасних СКУД.

Завдання: опрацювати матеріал та дати відповіді на запитання.

Рекомендована література: [1; 2; 3; 4; 5; 7; 8; 9].

Запитання для самоконтролю

1. RFID-технологія та як вона працює.
2. Активні та пасивні методи ідентифікації.

3. Карта Віганда та її застосування в СКУД.
4. Компоненти системи RFID.
5. Методи ідентифікації, їх переваги та недоліки.
6. Переваги та недоліки безконтактних смарт-карт?
7. Переваги та недоліки використання штрих-кодів під час ідентифікації суб'єкта.
8. Принцип роботи безконтактних смарт-карт?
9. Сфера застосування пасивних RFID-технологій.
10. Технічні характеристики карт Віганда.
11. Чинники, які впливають на вибір методу ідентифікації.
12. Штрих-коди та їх типи.

Самостійна робота №4

Тема. Біометричні системи ідентифікації.

Мета: сформувати у слухачів комплексне розуміння сутності, принципів роботи та класифікації біометричних методів ідентифікації, а також ознайомити їх з ключовими технологіями, перевагами й перспективними напрямками розвитку сучасних СКУД.

Завдання: опрацювати матеріал та дати відповіді на запитання.

Рекомендована література: [1; 2; 3; 5; 7; 8; 9].

Запитання для самоконтролю

1. Алгоритми та технології для обробки квазістатистичних ознак.
2. Біометричний метод ідентифікації та його основні принципи.
3. Використання біометричних даних у сучасних системах ідентифікації.
4. Вплив сучасних технологій та інновацій на розвиток біометричних систем.
5. Вплив штучного інтелекту на використання біометричних методів для ідентифікації суб'єкта в СКУД.
6. Застосування квазістатистичних ознак для ідентифікації суб'єкта.
7. Квазідинамічні ознаки для покращення точності ідентифікації.
8. Квазістатистичні ознаки та як вони використовуються під час ідентифікації.
9. Переваги та недоліки використання біометричних методів.
10. Сучасні напрямки розвитку біометричних систем доступу.
11. Яка послідовність основних етапів процесу занесення біометричних образів до бази даних системи?

Самостійна робота №5

Тема. Вибір СКУД для облаштування об’єкта доступу.

Мета: сформувати у слухача комплексне розуміння процесу прийняття рішень та критеріїв вибору оптимальної СКУД, яка відповідала б унікальним потребам та характеристикам конкретного об’єкта.

Завдання: опрацювати матеріал та дати відповіді на запитання.

Рекомендована література: [1; 2; 3; 5; 7; 9].

Запитання для самоконтролю

1. Вибір оптимального варіанту СКУД.
2. Вимоги, які висуваються до програмного забезпечення СКУД.
3. Вплив вимог безпеки на вибір обладнання для СКУД.
4. Вплив основних характеристики об’єкта доступу на вибір СКУД.
5. Зони підвищеного ризику в об’єкті доступу та їх вплив на вибір СКУД.
6. Компоненти СКУД та вимоги до них.
7. Методи оцінки безпеки об’єкта доступу.
8. Переваги та недоліки різних типів СКУД.
9. Сучасні тенденції у розвитку СКУД.
10. Типи СКУД та їх відмінності.
11. Чинники, які враховують під час оцінки об’єкта доступу для запровадження СКУД.

Самостійна робота №6

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

Мета: сформувати у слухачів глибоке розуміння архітектурних рішень та специфіки впровадження СКУД на об’єктах великого масштабу з географічно розподіленою інфраструктурою.

Завдання: опрацювати матеріал та дати відповіді на запитання.

Рекомендована література: [1; 2; 5; 6; 7; 9].

Запитання для самоконтролю

1. Вплив змішаної архітектури на гнучкість та масштабованість СКУД.
2. Вплив централізованої архітектури на управління безпекою об’єкта доступу.
3. Вплив централізованої архітектури на швидкість реагування на інциденти безпеки в СКУД.
4. Забезпечення безпеки даних у розподіленій архітектурі СКУД.

5. Ключові особливості розподіленої архітектури СКУД.

6. Основні чинники, які варто враховувати під час вибору централізованої архітектури.

7. Переваги змішаної архітектури СКУД над іншими.

8. Переваги розподіленої архітектури над централізованою.

9. Переваги та недоліки централізованої архітектури СКУД.

10. Реалізація змішаної архітектури СКУД на практиці.

11. Чинники, які варто враховувати під час проектування змішаної архітектури СКУД.

Самостійна робота №7

Тема. Загороджувальні керовані пристрої в СКУД.

Мета: сформувати у слухачів комплексне розуміння ролі, класифікації та технічних вимог до загороджувальних керованих пристроїв, як виконавчих елементів СКУД.

Завдання: опрацювати матеріал та дати відповіді на запитання.

Рекомендована література: [2; 4; 5; 7; 8; 9].

Запитання для самоконтролю

1. Виконавчі пристрої, які застосовують у СКУД. Переваги та недоліки виконавчих елементів ЗКП, які використовуються в СКУД.

2. Виконавчі пристроїв, які використовуються на КПП.

3. Вплив технічних вимог на вибір ЗКП.

4. Забезпечення ефективності роботи виконавчих пристроїв на КПП в умовах великого потоку суб’єктів допуску.

5. Категорії загороджувальних керованих пристроїв.

6. Класифікація ЗКП та її критерії.

7. Технічні вимоги, які висуваються до ЗКП, з огляду на їх безпеку.

8. Типи та характеристики електрозамків для СКУД.

3 ТЕСТОВІ ЗАВДАННЯ ДЛЯ САМОКОНТРОЛЮ

1. Яка із переліченого нижче відповідей найбільш точно відповідає визначенню «Доступ» у контексті СКУД?

A. Порівняння ідентичності двох різних суб’єктів.

B. Набір характеристик, достатніх для ідентифікації.

C. Переміщення суб’єкта або об’єкта доступу в деякій зоні для отримання можливості взаємодії з певним матеріальним або інформаційним ресурсом.

D. Процедура перевірки права власності на володіння ідентифікаційною ознакою.

E. Набір правил та норм, за якими дозволено переміщення поза захищеною зоною.

2. Який ключовий момент слід враховувати для квазідинамічних біометричних характеристик?

A. Вони є абсолютно незмінними протягом життя.

B. Вони не піддаються впливу зовнішніх чинників.

C. Вони вимагають високої роздільної здатності зчитувача.

D. Вони можуть використовувати лише один алгоритм порівняння.

E. Зареєстрований біометричний зразок необхідно піддавати періодичному оновленню.

3. Який із перелічених пунктів не вважається обов'язковим для встановлення під час обстеження архітектурно-планувальних і будівельних рішень об'єкта?

A. Кількість входів/виходів та їх геометричні розміри.

B. Рівень доступу адміністратора системи.

C. Матеріал будівельних конструкцій.

D. Кількість окремих будинків та число їх поверхів.

E. Розташування опалювальних й неопалюваних приміщень.

4. До якої групи, за класифікацією біометричних ознак, належать форма обличчя та відбитки пальців?

A. Квазідинамічні ознаки.

B. Імітаційні ознаки.

C. Квазістатичні ознаки.

D. Динамічні часові ознаки.

E. Радіочастотні ознаки.

5. Яке призначення інтерфейсу RS 485 у мережевій СКУД?

A. Обмін інформацією між контролерами та керуючим комп'ютером.

B. Підключення активних ідентифікаторів.

C. Підключення пристроїв для друку.

D. Зв'язок між контролерами.

E. Передача тривожного сигналу на світловий оповіщувач.

6. До якого виду перекривання проєму, згідно класифікації ЗКП, відносять турнікети та шлагбауми?

A. З повним перекриванням.

B. З блокуванням суб’єкта/об’єкта доступу в проємі.

C. З частковим перекриванням.

D. З автоматичним перекриванням.

E. З механічним перекриванням.

7. Який рівень мережевої взаємодії, під час побудови мережевих СКУД, використовують для зв’язку між контролерами та зчитувальними пристроями?

A. Перший рівень (Ethernet, TCP/IP).

B. Другий рівень (RS 232, USB).

C. Третій рівень (RS 485, RS 422 тощо).

D. Четвертий рівень (сповіщувачі охоронно-пожежної сигналізації).

E. Програмний (системний) рівень інтеграції.

8. Який недолік, з точки зору підключення обладнання, притаманний централізованої архітектури СКУД для великого розподіленого об’єкта?

A. Низька швидкість реакції комплексу.

B. Висока вартість контролера.

C. Необхідність об’єднання контролерів у мережі.

D. Необхідність підключення усього керованого обладнання до одного комп’ютера (сервера).

E. Розділення функцій прийняття рішень та управління.

9. Який коефіцієнт стиснення (за Вейвлет-перетвореннями) для зображення відбитка пальця вважається максимальним для уникнення втрати інформації та є необхідним для успішної ідентифікації?

A. 2.

B. 5.

C. 10.

D. 25.

E. 50.

10. Які методи ідентифікації суб’єктів використовують у СКУД?

A. Має, вміє, знає.

B. Запам’ятовує, має, характеризує.

C. Матеріальний носій, знання, біометричні ознаки.

D. Квазістатичний, квазідинамічний, цифровий.

E. Спостереження, маніпулювання, копіювання.

11. Який показник із перелічених не відноситься до основних показників надійності ЗКП?

A. Показник безвідмовності (середнє напрацювання на відмову).

B. Показник ремонтопридатності (середній час відновлення працездатного стану).

C. Показник довговічності (середній термін служби).

D. Показник електромагнітної сумісності (ступінь жорсткості).

E. Усі зазначені показники відносяться лише надійності.

12. Що виступає джерелом Wiegand-імпульсу в технології Wiegand?

A. Перемикання полярності оболонки феромагнітного дротика.

B. Перемикання полярності магнітного поля серцевини (стержня) дротика Віганда.

C. ЕРС індукції, що наводиться від зовнішнього джерела живлення.

D. Руйнівний вплив постійних магнітів.

E. Зміна опору навантаження в котушці зчитувача.

13. До якої категорії відносять СКУД із місткістю понад 64 контрольованих зони враховуючи класифікацію кількості контрольованих зон?

A. Автономні системи.

B. Мережеві системи.

C. Малої місткості.

D. Середньої місткості.

E. Великої місткості.

14. Який недолік, в контексті великих розподілених об’єктів, є спільним для невеликої ізольованої системи та централізованої системи з віддаленим управлінням?

A. Висока вартість програмного забезпечення.

B. Неможливість інтеграції з охоронною сигналізацією.

C. Необхідність підключення всього керованого обладнання до одного центрального комп’ютера (сервера).

D. Складність інсталяції та обслуговування.

E. Відсутність можливості адміністрування на кількох комп’ютерах.

15. Який із наведених недоліків не притаманний точкам доступу із одностороннім контролем?

A. Не відомо, де знаходиться суб’єкт доступу (в контрольованій зоні чи поза нею).

B. Неконтрольований вхід до зони захисту, оскільки система відслідковує лише вихід.

C. Можливість використання одного ідентифікатора для багаторазового проходу через неконтрольований вихід.

D. Вихід здійснюється через неконтрольоване управління загороджувальним пристроєм.

E. Зниження надійності СКУД.

16. Що конструктивно передбачають в ЗКП для випадків зникнення електроживлення, пожежі або інших стихійних лих?

A. Автоматичне блокування пристрою.

B. Механічне аварійне відкривання.

C. Перехід на резервне живлення на час не менше 1 години.

D. Подача звукової сигналізації без відкривання.

E. Зміна класу стійкості.

17. Що визначає рівень вкладення зон (рівень доступу зон) за умови, коли зони вільного доступу прийнято за нульовий рівень?

A. Категорію доступу суб'єкта.

B. Мінімальна кількість точок доступу, які необхідно пройти, щоб потрапити в цю зону.

C. Кількість приміщень, що входять до складу зони.

D. Рівень контролю, який здійснюється охоронною сигналізацією.

E. Кількість зовнішніх точок доступу.

18. Яке ключове завдання вирішує об'єднання усіх технічних засобів безпеки в інтегровану систему охорони з єдиною базою даних?

A. Створення додаткових ізольованих баз даних для кожного пристрою.

B. Збільшення впливу суб'єктивного людського чинника.

C. Мінімізація капітальних витрат за рахунок виключення дублюючої апаратури.

D. Ускладнення управління та обслуговування систем.

E. Забезпечення роботи виключно через інтерфейс RS 232.

19. Який спосіб кодування в системах радіочастотної ідентифікації не забезпечує синхронізації, але є найпростішим і не потребує додаткових перетворень двійкового коду?

A. Манчестерський код.

B. Диференціальний двохфазний код.

C. Код Ріда-Соломона.

D. Прямий код.

E. Широтно-імпульсна модуляція.

20. Чому електромеханічні замки є неефективними для дверей із високим прохідним навантаженням?

A. Вони не підтримують інтерфейс RS 485.

B. Вони вимагають електроживлення від мережі ~220 В.

C. Через їх високе механічне зношення, яке знижує надійність та термін служби.

D. Вони не мають можливості механічного аварійного відкривання.

E. Вони вимагають постійного живлення електричним струмом обмотки електромагніту.

21. Як називають зону, доступ до якої суб'єкту або об'єкту дозволено лише у встановлені часові та календарні інтервали?

A. Зона вільного (неконтрольованого) доступу.

B. Зона контрольованого доступу.

C. Зона недозволеного доступу.

D. Зона санкціонованого (дозволеного) доступу.

E. Зона обмеженого доступу об'єктів.

22. Як називають функцію СКУД, яка перешкоджає тому, щоб один співробітник, пройшовши через двері, передав свою картку іншій особі для входу?

A. Розблокування виконавчих пристроїв у разі екстреної події.

B. Створення декількох ієрархічних груп користувачів.

C. Функція «ні кроку назад».

D. Програмування часових інтервалів доступу.

E. Контроль у режимі реального часу на плані території.

23. Яка основна перевага біометричного методу контролю доступу?

A. Низька вартість реалізації.

B. Швидке занесення еталонного зразка.

C. Високий ступінь ймовірності одночасного вирішення завдань ідентифікації та автентифікації.

D. Можливість використання у будь-яких умовах НС.

E. Стійкість до психологічних чинників.

24. Який принцип функціонування СКУД порушується, коли «проходження однієї і тієї ж ТД не може бути виконано двічі поспіль в одному і тому ж напрямку без проходження інших точок доступу або цієї ТД в зворотному напрямку»?

A. Санкціоновані дії.

B. Здійсненність.

C. Безперервність.

D. Неповторюваність.

E. Монотонність.

4 ПІДГОТОВКА ДО СЕМЕСТРОВОГО КОНТРОЛЮ

Завдання для підсумкового контролю знань. Підготовка до іспиту відбувається після закінчення теоретичної частини семестру. Час, відведений на підготовку та проведення семестрового контролю з дисциплін поточного семестру, формує сесію.

До іспиту допускаються студенти, які повністю виконали всі інші види навчальної роботи, які передбачено навчальним планом з цієї дисципліни. Іспит проводиться в очній формі. На іспит виносяться питання, кожне з яких оцінюється у 100 балів, а результуюча як середня зважена оцінка.

Питання, які виносяться на іспит, формується на основі теоретичного курсу та самостійної роботи студента.

Критерії оцінювання відповіді. Теоретичні питання оцінюються, виходячи із наступних критеріїв.

За шкалою університету	За шкалою ECTS	За державною шкалою	Критерії оцінювання знань
90-100	A (відмінно)	відмінно	теоретичні питання розкриті повно, студент висвітлив основні поняття, проаналізував та обґрунтував свої відповіді
85-89	B (дуже добре)	добре	ставиться, якщо теоретичні питання розкриті повно, але містять окремі помилки, які не призводять до викривлення сутності питань, які розглядаються
75-84	C (добре)		
65-74	D (задовільно)	задовільно	якщо теоретичні питання висвітлені неповно і лише на репродуктивному рівні, студент продемонстрував знання тільки основної частини програмного матеріалу
60-64	E (достатньо)		
35-59	FX (недостатньо з можливістю повторного складання)	незадовільно	теоретичні питання висвітлені не повно, безсистемно і мають суттєві помилки
0-34	F (незадовільно з обов'язковим повторним курсом)		теоретичні питання не висвітлені зовсім

5 ПЕРЕЛІК ПИТАНЬ, ЯКІ ВИНОСЯТЬСЯ НА ІСПИТ

1. Wiegand-ефект. Переваги Wiegand-карт та зчитувачів.
2. Автентифікація та верифікація.
3. Автономна та мережева СКУД.
4. Автономність у розподіленій архітектурі СКУД.
5. Архітектура та ПЗ контролерів.
6. Біометричні ознаки та їх класифікація.
7. Вибір стратегії налаштування системи біометричної ідентифікації.
8. Вимоги до стійкості загороджувальних керованих пристроїв на несанкціоновані дії руйнівного типу.
9. Вимоги які висуваються до основних компонентів СКУД.
10. Вимоги, які висуваються до ПЗ для ізольованої СКУД.
11. Відкритий, замкнутий та квазізамкнутий маршрути.
12. Вкладена зона доступ. Рівень вкладення зон.
13. Дальність зчитування системи радіочастотної ідентифікації з пасивними ідентифікаторами.
14. Доступ і контролю та управління доступом.
15. Електричні замки у СКУД.
16. Елементи, які беруть участь у роботі СКУД.
17. Етапи занесення еталонного біометричного образу.
18. Етапи процедури ідентифікації.
19. Захищеність ідентифікаторів та основні загрози.
20. Змішана архітектура СКУД та її функціональна надійність.
21. Зона контрольованого доступу та її типи.
22. Ідентифікаційні ознаки та ідентифікатори.
23. Ідентифікація за відбитком пальця: алгоритми та обробка.
24. Ідентифікація за райдужною оболонкою ока.
25. Інтеграція СКУД та її сценарії.
26. Інтегровані системи охорони в СКУД.
27. Інтелектуальний інтерфейсний модуль.
28. Квазідинамічні та перспективні методи ідентифікації.
29. Квазістатичні та квазідинамічні ознаки.
30. Класифікація біометричних методів ідентифікації.
31. Класифікація СКУД за рівнем ідентифікації та кількістю контрольованих зон.
32. Класифікація та функціональне призначення загороджувальних керованих пристроїв.
33. Кодування інформації у радіочастотних системах.

34. Компоненти пристроїв управління доступом у СКУД.
35. Комунікаційні інтерфейси у великих СКУД.
36. Контрольовані зони доступу та їх типи.
37. Критерії оцінювання СКУД.
38. Математичний апарат для теорії КУД.
39. Матриця рішень системи біометричної ідентифікації та ймовірності помилок.
40. Методи та типи ідентифікації в СКУД.
41. Модульний та блочно-агрегатний принцип формування конструкції загороджувальних керованих пристроїв.
42. Надійність загороджувальних керованих пристроїв їх показники та критерії.
43. Носії ідентифікаційних ознак за методами ідентифікації.
44. Обстеження об'єкта доступу та технічне завдання а обладнання об'єкта СКУД.
45. Організація пропускного режиму на пішохідних КПП.
46. Основні правила та рекомендації, які висуваються до розміщення зчитувачів та виконавчих пристроїв в СКУД.
47. Перехід та маршрут суб'єкта доступу.
48. Порівняльна стійкість методів ідентифікації з точки зору різних видів несанкціонованих дій.
49. Права доступу.
50. Принцип роботи пасивного радіочастотного ідентифікатора та зчитувача.
51. Принцип роботи та мета застосування шлюзу (тамбура).
52. Принципи функціонування СКУД за особливостями переміщення суб'єкта доступу.
53. Процедури ідентифікації та автентифікації.
54. Радіочастотна ідентифікація (Proximity-технологія).
55. Реалізація повного циклу СКУД (на довільному прикладі).
56. Рівень доступу та його складові.
57. Система контролю та управління доступом і контроль та управління доступом.
58. Теорія графів в СКУД.
59. Технічні засоби СКУД.
60. Технології зчитування відбитка пальця.
61. Типові варіанти побудови та розміщення СКУД.
62. Точка доступу та її класифікація.

63. Турнікети для СКУД, їх класифікація та види.
64. Функціональні вимоги, які висуваються до ЗКП, та безпека проходу.
65. Функціональні вимоги, які висуваються до СКУД.
66. Функціональні елементи узагальненої структурної схема СКУД.
67. Централізована та розподілена архітектура СКУД для великих об'єктів.
68. Чинники, які впливають на дальність зчитування RFID-систем.
69. Шлюзування та його реалізація в СКУД.
70. Штрихові коди в СКУД.

6 РЕКОМЕНДОВАНІ ДЖЕРЕЛА ІНФОРМАЦІЇ

1. Access Control Systems : Security, Identity Management and Trust Models. URL: https://surl.li/pophrl (дата звернення 28.08.2025).
2. Boddu Raghu. SAP Access Control. Quincy : SAP PRESS, 2023. 695 p.
3. Brian Rhodes. Access Control. URL: https://surl.lu/xvxphm (дата звернення 28.08.2025).
4. Harold F. Tipton, Micki Krause. Information Security Management : Handbook. URL: https://surl.lu/oqhegu (дата звернення 28.08.2025).
5. Kris Hermans. Mastering Access Control : A Comprehensive Guide to Learn Access Control. Traverse City : Independently published, 2023. 393 p.
6. Matej Csányi. Access Control in Operating Systems. URL: https://is.muni.cz/th/uny2u/ xcsanyi_bc.pdf (дата звернення 28.08.2025).
7. Mike Chapple. Access Control and Identity Management. Burlington : World Headquarters Jones & Bartlett Learning, 2021. 376 p.
8. Thomas Norman. Electronic Access Control. URL: https://surl.li/oybgwe (дата звернення 28.08.2025).
9. Кайдик О. Л., Терлецький Т. В., Ткачук А. А. 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 денної та заочної форм навчання. Луцьк : ЛНТУ, 2025. 132 с.

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 заочної форм навчання / уклад. О. Л. Кайдик, Т. В. Терлецький. Луцьк : ЛНТУ, 2025. 20 с.

Комп'ютерний набір та верстка: О. Л. Кайдик.

Редактор: в авторській редакції.

Підп. до друку «___» _____ 2025 р.
Формат 60x84/16. Папір офс. Гарн. Таймс.
Ум. друк. арк. 1,4. Обл. – вид. арк. 1,37.
Тираж _50_ прим. Зам. _______.

Луцький національний технічний університет
43018 м. Луцьк, вул. Львівська, 75