Міністерство освіти і науки України
Луцький національний технічний університет
Факультет комп'ютерних та інформаційних технологій
Кафедра кібербезпеки

ЄДИНИЙ ДЕРЖАВНИЙ КВАЛІФІКАЦІЙНИЙ ІСПИТ (ЄДКІ)

Методичні вказівки з підготовки до єдиного державного кваліфікаційного іспиту (ЄДКІ)
для здобувачів першого (бакалаврського) рівня вищої освіти
освітньої програми «Кібербезпека»
галузь знань 12 Інформаційні технології
спеціальності 125 Кібербезпека та захист інформації
денної та заочної форм навчання

Луцьк 2026

УДК 004.056

Рекомендовано до видання вченою радою факультету КІТ ЛНТУ,
протокол № _____ від «___» _____ 20 26 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 кібербезпеки
ЛНТУ, протокол № _____ від « _____» _____ 20 26 року.

Завідувач кафедри КБ _____ Сергій КОСТЮЧКО

Укладачі: _____ Сергій КОСТЮЧКО, кандидат технічних наук,
завідувач кафедри кібербезпеки ЛНТУ

Рецензент: _____ Олександр БУРБАН, кандидат технічних наук,
викладач фахових дисциплін

Відповідальний за випуск: _____ Сергій КОСТЮЧКО, кандидат
технічних наук, доцент кафедри кібербезпеки ЛНТУ

Єдиний державний кваліфікаційний іспит. Методичні вказівки з підготовки до єдиного державного кваліфікаційного іспиту (ЄДКІ) для здобувачів першого (бакалаврського) рівня вищої освіти освітньої програми «Кібербезпека» галузь знань 12 Інформаційні технології спеціальності 125 Кібербезпека та захист інформації денної та заочної форм навчання / уклад. С.М. Костючко. Луцьк: ЛНТУ, 2026. 39 с.

ЗМІСТ

ВСТУП 4
1. ЗАГАЛЬНІ ПОЛОЖЕННЯ 5
2. ОРГАНІЗАЦІЯ САМОСТІЙНОЇ ПІДГОТОВКИ 7
3. ЗАКОНОДАВЧА ТА НОРМАТИВНО-ПРАВОВА БАЗА 8
4. ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ В КІБЕРБЕЗПЕЦІ 11
5. БЕЗПЕКА ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ СИСТЕМ 15
6. КОМПЛЕКСНІ СИСТЕМИ ЗАХИСТУ ІНФОРМАЦІЇ 19
7. УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ ТА КІБЕРБЕЗПЕКОЮ 22
8. КРИПТОГРАФІЧНИЙ ЗАХИСТ ІНФОРМАЦІЇ 25
9. ТЕХНІЧНИЙ ЗАХИСТ ІНФОРМАЦІЇ 29
10. КОМПЛЕКСНЕ ПОВТОРЕННЯ ПЕРЕД ЄДКІ 32
СПИСОК ВИКОРИСТАНИХ І РЕКОМЕНДОВАНИХ ДЖЕРЕЛ 36
ДОДАТОК А. ЛИСТ САМОКОНТРОЛЮ 37

ВСТУП

Єдиний державний кваліфікаційний іспит (ЄДКІ) для здобувачів першого (бакалаврського) рівня є формою зовнішнього оцінювання результатів навчання у сфері кібербезпеки та захисту інформації. Підготовка до нього має інтегрувати теоретичні знання, технічні навички, розуміння нормативних вимог і здатність аналізувати професійні ситуації.

Ці методичні вказівки призначені для здобувачів спеціальності F5 «Кібербезпека та захист інформації» і побудовані за зразком методичних вказівок ЛНТУ для підготовки до ЄДКІ за спеціальністю D4. Предметне наповнення адаптоване за наданою програмою ЄДКІ зі спеціальності 125 «Кібербезпека» (наказ МОН від 04.11.2022 № 980).

Навчальний матеріал зосереджено на законодавчому регулюванні, інформаційних технологіях, безпеці інформаційно-комунікаційних систем, комплексному захисті, управлінні ризиками та інцидентами, криптографії, технічних каналах витоку і протидії їм. Кожний розділ містить тематичні пояснення, ситуаційні приклади, питання для самоперевірки та орієнтовні тренувальні тестові завдання.

1. ЗАГАЛЬНІ ПОЛОЖЕННЯ

1.1. Мета і завдання

Мета методичних вказівок – надати послідовну структуру повторення знань і навичок за тематикою ЄДКІ, допомогти здобувачам виявити прогалини, сформувати обґрунтовані стратегії вибору відповідей та підвищити якість самопідготовки.

– систематизувати ключові терміни та зв’язки між поняттями інформаційної і кібербезпеки;

– повторити процедури забезпечення конфіденційності, цілісності, доступності та автентичності;

– закріпити знання технологій захисту мереж, операційних систем і даних;

– відпрацювати аналіз практичних ситуацій та вибір технічних і організаційних рішень;

– сформувати навички роботи з тестовими завданнями та самоаналізу результатів.

1.2. Структура програми і питома вага розділів

Розділ програми ЄДКІ	**Питома вага**
Законодавча та нормативно-правова база, державні та міжнародні вимоги, практики і стандарти	8–12 %
Інформаційні технології в інформаційній та/або кібербезпеці	14–18 %
Безпека інформаційно-комунікаційних систем	15–25 %
Комплексні системи захисту інформації	8–10 %
Управління інформаційною та/або кібербезпекою	16–20 %
Криптографічний захист інформації	11–15 %
Технічний захист інформації	12–16 %

Діапазони наведено за програмою 2022 року. Вони не є гарантованою кількістю завдань у конкретному екзаменаційному варіанті.

1.3. Когнітивні рівні

Рівень	**Зміст за програмою**
A	Знання: відтворення фактів, термінів, характеристик.
B	Знання і розуміння: пояснення призначення, функцій, відмінностей.
C	Знання, розуміння, застосування: виконання обчислень і вибір дій.
D	Знання, розуміння, застосування, аналіз / синтез / оцінка.

2. ОРГАНІЗАЦІЯ САМОСТІЙНОЇ ПІДГОТОВКИ

2.1. Рекомендована послідовність

– Ознайомитися з офіційною програмою та зіставити її теми з вивченими дисциплінами.

– Провести вхідну діагностику знань за сімома розділами та позначити слабкі теми.

– Повторити теоретичні положення, відтворити схеми і виконати типові розрахунки.

– Виконати тематичні тести, проаналізувати кожну помилку і повторити відповідний матеріал.

– Провести змішане тестування з обмеженням часу; скласти індивідуальний план завершального повторення.

2.2. Орієнтовний чотиритижневий план

Тиждень	**Опрацювання**	**Очікуваний результат**
1	Розділи 1–2; діагностика	Розуміння вимог та ІТ-основ
2	Розділи 3–4	Захист мереж, систем і моделі загроз
3	Розділи 5–6	Ризики, інциденти і криптографія
4	Розділ 7; змішані тести	Повторення, аналіз помилок і готовність до іспиту

2.3. Методика роботи з тестами

Спочатку визначте ключове запитання та обмеження в умові; далі виключіть варіанти, що суперечать визначенням, принципам роботи технологій або заданим умовам. Для обчислювальних задач записуйте формулу і проміжні результати. Для ситуаційних – відділяйте ознаки інциденту від припущень і перевіряйте пріоритетність дій. Після перевірки пояснюйте не лише правильний вибір, а й помилки в альтернативних відповідях.

Нормативно-правові акти, стандарти та процедури можуть змінюватися. Їх чинність потрібно перевіряти за офіційними джерелами безпосередньо перед іспитом.

3. ЗАКОНОДАВЧА ТА НОРМАТИВНО-ПРАВОВА БАЗА

Тематичний матеріал цього розділу структуровано відповідно до розділів і підрозділів наданої програми ЄДКІ; приклади, питання і тестові завдання створені для навчальної підготовки та не є відтворенням офіційних екзаменаційних завдань.

3.1. Законодавство України в галузі інформаційної та кібербезпеки

Закон України «Про інформацію» встановлює загальні засади інформаційних відносин, а законодавство про захист інформації в інформаційно-комунікаційних системах визначає правові підходи до захисту інформації в таких системах. Закон «Про основні засади забезпечення кібербезпеки України» визначає базову термінологію, засади кіберзахисту та учасників національної системи кібербезпеки. Під час повторення важливо розрізняти інформацію з обмеженим доступом, персональні дані, державну таємницю та права й обов’язки суб’єктів обробки інформації. Положення законів потрібно читати у чинній редакції.

Практична ситуація. Організація обробляє персональні дані працівників: необхідно визначити законну підставу, мету і мінімально необхідний обсяг обробки, а також забезпечити належні заходи захисту.

Рекомендація до опрацювання. Складіть коротку схему ключових понять теми «Законодавство України в галузі інформаційної та кібербезпеки», зіставте визначення, призначення та типові обмеження і поясніть, якими ознаками можна підтвердити правильність технічного або організаційного рішення.

3.2. Національні стандарти та нормативні документи ТЗІ

Державні стандарти та нормативні документи технічного захисту інформації забезпечують спільну термінологію, підходи до оцінювання захищеності та визначення вимог до систем. У програмі згадані ДСТУ 3396.0–2, ДСТУ ISO/IEC 15408-1, НД ТЗІ 1.1-003-99 і НД ТЗІ 2.5-004-99. У підготовці слід розрізняти загальні принципи захисту, функціональні послуги

безпеки, оцінювання відповідності та порядок застосування конкретного документа.

Практична ситуація. Для інформаційної системи з обмеженим доступом готують перелік загроз і вимог до послуг захисту; вибір заходів має спиратися на категорії інформації та умови експлуатації.

Рекомендація до опрацювання. Складіть коротку схему ключових понять теми «Національні стандарти та нормативні документи ТЗІ», зіставте визначення, призначення та типові обмеження і поясніть, якими ознаками можна підтвердити правильність технічного або організаційного рішення.

3.3. Міжнародні стандарти й вимоги

ISO/IEC 27001 регламентує вимоги до системи управління інформаційною безпекою, а ISO/IEC 27002 надає настанови щодо заходів контролю. Сімейство ISO/IEC 15408 (Common Criteria) використовується для оцінювання безпеки IT-продуктів. Регламент ЄС 2019/881 пов’язаний із європейською рамкою сертифікації кібербезпеки та ENISA. Слід розрізняти сертифікацію продукту, управлінську систему організації і настанови з контролів.

Практична ситуація. Якщо організації потрібно системно управляти ризиками, доцільно визначити контекст, ризики, контрольні заходи та процедури перевірки результативності, а не обмежуватися встановленням окремих захисних засобів.

Рекомендація до опрацювання. Складіть коротку схему ключових понять теми «Міжнародні стандарти й вимоги», зіставте визначення, призначення та типові обмеження і поясніть, якими ознаками можна підтвердити правильність технічного або організаційного рішення.

3.4. Питання для самоперевірки

1. Які основні поняття та принципи охоплює тема «законодавство україни в галузі інформаційної та кібербезпеки»?

2. Які типові загрози, помилки або обмеження слід враховувати в цій темі?

3. Як застосувати вивчені положення до наведеної практичної ситуації?

4. Які основні поняття та принципи охоплює тема «національні стандарти та нормативні документи тзі»?

5. Які типові загрози, помилки або обмеження слід враховувати в цій темі?

6. Як застосувати вивчені положення до наведеної практичної ситуації?

7. Які основні поняття та принципи охоплює тема «міжнародні стандарти й вимоги»?

8. Які типові загрози, помилки або обмеження слід враховувати в цій темі?

9. Як застосувати вивчені положення до наведеної практичної ситуації?

3.5. Тренувальні тестові завдання

У кожному завданні виберіть одну правильну відповідь.

1. Який закон визначає базові засади забезпечення кібербезпеки України?

А. Про основні засади забезпечення кібербезпеки України

Б. Про бухгалтерський облік

В. Про місцеві вибори

Г. Про державні закупівлі

2. Який стандарт установлює вимоги до системи управління інформаційною безпекою?

А. ISO/IEC 15408-3

Б. ISO/IEC 27001

В. IEEE 802.3

Г. RFC 791

3. Який документ найближче пов’язаний з Common Criteria?

А. ISO/IEC 15408

Б. ISO 9004

В. IEEE 802.11

Г. TLS 1.3

4. ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ В КІБЕРБЕЗПЕЦІ

Тематичний матеріал цього розділу структуровано відповідно до розділів і підрозділів наданої програми ЄДКІ; приклади, питання і тестові завдання створені для навчальної підготовки та не є відтворенням офіційних екзаменаційних завдань.

4.1. Модель OSI та стек TCP/IP

Модель OSI поділяє мережеву взаємодію на сім логічних рівнів; стек TCP/IP реалізує практичні механізми передавання даних. Ethernet працює переважно на канальному рівні, IP – на мережевому, TCP і UDP – на транспортному, DNS, HTTP і SMTP – на прикладному. Інкапсуляція додає службові заголовки під час передавання даних. TCP забезпечує керування встановленням з’єднання та надійність доставлення, тоді як UDP є безз’єднальним і не гарантує доставлення.

Практична ситуація. Під час аналізу недоступного вебресурсу окремо перевіряють DNS-резолюцію, IP-маршрут, TCP-з’єднання та відповідь прикладного протоколу.

Рекомендація до опрацювання. Складіть коротку схему ключових понять теми «Модель OSI та стек TCP/IP», зіставте визначення, призначення та типові обмеження і поясніть, якими ознаками можна підтвердити правильність технічного або організаційного рішення.

4.2. Архітектура комп’ютерів і віртуалізація

Центральний процесор виконує інструкції, оперативна пам’ять зберігає активні дані, а накопичувачі забезпечують довготривале зберігання. Віртуальна пам’ять ізолює адресні простори процесів і дає ОС керувати сторінками пам’яті. Гіпервізор типу 1 працює безпосередньо на апаратній платформі, типу 2 – поверх основної ОС. Сегментація, ізоляція віртуальних машин і належне адміністрування гіпервізора знижують ризик міжсистемного впливу.

Практична ситуація. Для лабораторного дослідження шкідливих файлів використовують ізольовану ВМ із контрольованими мережевими інтерфейсами та знімками стану.

Рекомендація до опрацювання. Складіть коротку схему ключових понять теми «Архітектура комп'ютерів і віртуалізація», зіставте визначення, призначення та типові обмеження і поясніть, якими ознаками можна підтвердити правильність технічного або організаційного рішення.

4.3. Алгоритми, структури даних і програмування

Алгоритм характеризують коректність, скінченність і обчислювальна складність. Лінійний пошук має O(n), двійковий пошук у відсортованому масиві – O(log n); типовий ефективний алгоритм сортування має O(n log n). Об'єктно-орієнтоване програмування використовує інкапсуляцію, наслідування та поліморфізм; клас описує атрибути й методи об'єктів. Під час розробки безпечного ПЗ варто перевіряти введення, межі масивів, типи даних і помилки доступу.

Практична ситуація. У журналі з мільйона записів двійковий пошук можливий лише після визначення порядку сортування за відповідним ключем.

Рекомендація до опрацювання. Складіть коротку схему ключових понять теми «Алгоритми, структури даних і програмування», зіставте визначення, призначення та типові обмеження і поясніть, якими ознаками можна підтвердити правильність технічного або організаційного рішення.

4.4. Операційні системи, процеси, пам'ять і файлові системи

ОС керує процесами, потоками, пам'яттю, файлами, пристроями та доступом. Процес має власні ресурси й адресний простір; потоки одного процесу зазвичай поділяють його адресний простір. Права доступу, облікові записи, ACL, механізми ізоляції процесів і журнали аудиту є основою захисної конфігурації. Під час аналізу NTFS або файлових систем Linux розрізняють дозволи, метадані та журналювання.

Практична ситуація. Зловмисник не може прочитати файл, якщо права DAC/ACL не надають йому доступ; водночас адміністративні привілеї потребують окремого контролю.

Рекомендація до опрацювання. Складіть коротку схему ключових понять теми «Операційні системи, процеси, пам’ять і файлові системи», зіставте визначення, призначення та типові обмеження і поясніть, якими ознаками можна підтвердити правильність технічного або організаційного рішення.

4.5. Питання для самоперевірки

1. Які основні поняття та принципи охоплює тема «модель osi та стек tcp/ip»?

2. Які типові загрози, помилки або обмеження слід враховувати в цій темі?

3. Як застосувати вивчені положення до наведеної практичної ситуації?

4. Які основні поняття та принципи охоплює тема «архітектура комп’ютерів і віртуалізація»?

5. Які типові загрози, помилки або обмеження слід враховувати в цій темі?

6. Як застосувати вивчені положення до наведеної практичної ситуації?

7. Які основні поняття та принципи охоплює тема «алгоритми, структури даних і програмування»?

8. Які типові загрози, помилки або обмеження слід враховувати в цій темі?

9. Як застосувати вивчені положення до наведеної практичної ситуації?

10. Які основні поняття та принципи охоплює тема «операційні системи, процеси, пам’ять і файлові системи»?

11. Які типові загрози, помилки або обмеження слід враховувати в цій темі?

12. Як застосувати вивчені положення до наведеної практичної ситуації?

4.6. Тренувальні тестові завдання

У кожному завданні виберіть одну правильну відповідь.

1. Який протокол належить до транспортного рівня?

А. IP

Б. TCP

В. DNS

Г. Ethernet

2. Яка асимптотична складність двійкового пошуку у відсортованому масиві?

А. $O(n^2)$

Б. $O(n)$

В. $O(\log n)$

Г. $O(2^n)$

3. Що зазвичай спільне для потоків одного процесу?

А. Окремі файлові системи

Б. Адресний простір процесу

В. Різні ядра ОС

Г. Незалежні облікові записи

5. БЕЗПЕКА ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ СИСТЕМ

Тематичний матеріал цього розділу структуровано відповідно до розділів і підрозділів наданої програми ЄДКІ; приклади, питання і тестові завдання створені для навчальної підготовки та не є відтворенням офіційних екзаменаційних завдань.

5.1. Ідентифікація, автентифікація та авторизація

Ідентифікація визначає заявлену сутність користувача; автентифікація перевіряє підтвердження цієї сутності; авторизація встановлює дозволені операції. Багатофакторна автентифікація поєднує незалежні фактори (знання, володіння, властивість). Принцип найменших привілеїв зменшує наслідки компрометації. Облікові записи мають бути індивідуальними, а права – переглядатися відповідно до ролей.

Практична ситуація. Працівнику потрібен доступ лише для перегляду звітів – надання права змінювати записи порушує принцип мінімально необхідних повноважень.

Рекомендація до опрацювання. Складіть коротку схему ключових понять теми «Ідентифікація, автентифікація та авторизація», зіставте визначення, призначення та типові обмеження і поясніть, якими ознаками можна підтвердити правильність технічного або організаційного рішення.

5.2. Захисні програмно-апаратні засоби

Міжмережевий екран контролює трафік за правилами, антивірус або EDR аналізує активність кінцевого пристрою, IDS виявляє ознаки атак, а IPS може блокувати підозрілі потоки. Сигнатурний підхід зіставляє події з відомими шаблонами; аномальний – виявляє відхилення від базового профілю. Система керування каталогом і ACL забезпечують централізоване адміністрування і контроль доступу. Жодний засіб не замінює багаторівневий захист.

Практична ситуація. IDS генерує сповіщення про відоме сканування портів; IPS за коректно налаштованою політикою може припинити з’єднання.

Рекомендація до опрацювання. Складіть коротку схему ключових понять теми «Захисні програмно-апаратні засоби», зіставте визначення, призначення

та типові обмеження і поясніть, якими ознаками можна підтвердити правильність технічного або організаційного рішення.

5.3. Відновлення, резервування та журнали аудиту

Резервування компонентів підвищує доступність, а резервне копіювання створює незалежні копії даних для відновлення. RPO позначає припустимий обсяг втрати даних у часі, RTO – цільовий час відновлення сервісу. Потрібно визначати періодичність копій, місце зберігання, захист копій і регулярні тести відновлення. Журнали подій мають містити достатній контекст, синхронізований час та бути захищеними від підроблення.

Практична ситуація. За RPO 1 година і копіями раз на добу політика резервування не забезпечує встановленої цілі; потрібно змінити інтервал або механізм реплікації.

Рекомендація до опрацювання. Складіть коротку схему ключових понять теми «Відновлення, резервування та журнали аудиту», зіставте визначення, призначення та типові обмеження і поясніть, якими ознаками можна підтвердити правильність технічного або організаційного рішення.

5.4. Моніторинг і SIEM

Моніторинг збирає події з ОС, мережевих пристроїв, засобів захисту і застосунків. SIEM здійснює централізований збір, нормалізацію, кореляцію та представлення подій. Важливо розрізняти подію, сповіщення та підтверджений інцидент; визначати контекст, достовірність і пріоритет. Кореляційне правило може пов’язувати серію невдалих входів із наступним успішним входом з нетипового джерела.

Практична ситуація. SOC-аналітик перевіряє часову послідовність входів, IP-адресу, роль користувача та додаткові журнали, перш ніж класифікувати подію як інцидент.

Рекомендація до опрацювання. Складіть коротку схему ключових понять теми «Моніторинг і SIEM», зіставте визначення, призначення та типові обмеження і поясніть, якими ознаками можна підтвердити правильність технічного або організаційного рішення.

5.5. Мережеві протоколи захисту й VPN

TLS забезпечує криптографічний захист сеансів прикладного обміну; HTTPS – це HTTP поверх TLS. IPsec захищає IP-трафік, зокрема у тунельному режимі. VPN формує захищений логічний канал поверх іншої мережі. RADIUS застосовують для мережевої автентифікації, авторизації та обліку. Потрібно розуміти, що шифрування каналу не гарантує безпечності кінцевої системи або достовірності введених користувачем даних.

Практична ситуація. Для захищеного доступу працівника до внутрішньої мережі налаштовують VPN із перевіркою ідентичності та обмеженням доступу до потрібних ресурсів.

Рекомендація до опрацювання. Складіть коротку схему ключових понять теми «Мережеві протоколи захисту й VPN», зіставте визначення, призначення та типові обмеження і поясніть, якими ознаками можна підтвердити правильність технічного або організаційного рішення.

5.6. Питання для самоперевірки

1. Які основні поняття та принципи охоплює тема «ідентифікація, автентифікація та авторизація»?

2. Які типові загрози, помилки або обмеження слід враховувати в цій темі?

3. Як застосувати вивчені положення до наведеної практичної ситуації?

4. Які основні поняття та принципи охоплює тема «захисні програмно-апаратні засоби»?

5. Які типові загрози, помилки або обмеження слід враховувати в цій темі?

6. Як застосувати вивчені положення до наведеної практичної ситуації?

7. Які основні поняття та принципи охоплює тема «відновлення, резервування та журнали аудиту»?

8. Які типові загрози, помилки або обмеження слід враховувати в цій темі?

9. Як застосувати вивчені положення до наведеної практичної ситуації?

10. Які основні поняття та принципи охоплює тема «моніторинг і siem»?

11. Які типові загрози, помилки або обмеження слід враховувати в цій темі?

12. Як застосувати вивчені положення до наведеної практичної ситуації?

13. Які основні поняття та принципи охоплює тема «мережеві протоколи захисту й vpn»?

14. Які типові загрози, помилки або обмеження слід враховувати в цій темі?

15. Як застосувати вивчені положення до наведеної практичної ситуації?

5.7. Тренувальні тестові завдання

У кожному завданні виберіть одну правильну відповідь.

1. Яку функцію виконує авторизація?

А. Визначає права на дії

Б. Встановлює IP-адресу

В. Перевіряє фізичну особу лише за паролем

Г. Стискає дані

2. Який показник визначає цільовий час відновлення?

А. RPO

Б. RTO

В. MTU

Г. TTL

3. Який засіб призначений для кореляції журналів безпеки?

А. SIEM

Б. DHCP

В. NAT

Г. RAID

6. КОМПЛЕКСНІ СИСТЕМИ ЗАХИСТУ ІНФОРМАЦІЇ

Тематичний матеріал цього розділу структуровано відповідно до розділів і підрозділів наданої програми ЄДКІ; приклади, питання і тестові завдання створені для навчальної підготовки та не є відтворенням офіційних екзаменаційних завдань.

6.1. Дослідження середовища та проєктування захисту

Перед проєктуванням захисту визначають інформаційні активи, категорії інформації, межі системи, функції користувачів, технічне і фізичне середовища. Модель загроз описує можливі події, джерела загроз, уразливості й наслідки; модель порушника – потенційні можливості, мотивацію та доступ. Обрані заходи мають відповідати сформульованим вимогам і бути перевірюваними.

Практична ситуація. Для навчальної лабораторії моделюють загрозу несанкціонованого доступу до серверів з боку користувача з обмеженими правами і визначають відповідні межі доступу.

Рекомендація до опрацювання. Складіть коротку схему ключових понять теми «Дослідження середовища та проєктування захисту», зіставте визначення, призначення та типові обмеження і поясніть, якими ознаками можна підтвердити правильність технічного або організаційного рішення.

6.2. Моделі загроз і модель порушника

Конфіденційність порушується внаслідок несанкціонованого розкриття; цілісність – несанкціонованої зміни; доступність – блокування або відмови; автентичність – підміни джерела чи об’єкта. Технічні канали витоку становлять окрему групу ризиків. Модель порушника враховує внутрішній чи зовнішній доступ, рівень знань, ресурси, можливі дії та межі впливу.

Практична ситуація. Фальсифікація електронного документа насамперед створює загрозу цілісності та автентичності, а шифрування даних зловмисником – доступності.

Рекомендація до опрацювання. Складіть коротку схему ключових понять теми «Моделі загроз і модель порушника», зіставте визначення, призначення

та типові обмеження і поясніть, якими ознаками можна підтвердити правильність технічного або організаційного рішення.

6.3. Оцінка захищеності

Оцінювання захищеності передбачає зіставлення реалізованих заходів із визначеними вимогами, перевірку конфігурацій, журналів, управління доступом, стійкості процедур резервування та реагування. Важливо відрізняти формальну наявність політики від технічної та організаційної результативності її виконання. Результати слід оформлювати як докази з переліком відхилень, їх впливом і рекомендованими коригувальними діями.

Практична ситуація. Наявність правила заборони доступу не доводить його дієвість; доцільно перевірити застосовані права та спробу доступу в контрольованому тесті.

Рекомендація до опрацювання. Складіть коротку схему ключових понять теми «Оцінка захищеності», зіставте визначення, призначення та типові обмеження і поясніть, якими ознаками можна підтвердити правильність технічного або організаційного рішення.

6.4. Питання для самоперевірки

1. Які основні поняття та принципи охоплює тема «дослідження середовища та проєктування захисту»?

2. Які типові загрози, помилки або обмеження слід враховувати в цій темі?

3. Як застосувати вивчені положення до наведеної практичної ситуації?

4. Які основні поняття та принципи охоплює тема «моделі загроз і модель порушника»?

5. Які типові загрози, помилки або обмеження слід враховувати в цій темі?

6. Як застосувати вивчені положення до наведеної практичної ситуації?

7. Які основні поняття та принципи охоплює тема «оцінка захищеності»?

8. Які типові загрози, помилки або обмеження слід враховувати в цій темі?

9. Як застосувати вивчені положення до наведеної практичної ситуації?

6.5. Тренувальні тестові завдання

У кожному завданні виберіть одну правильну відповідь.

1. Яка властивість порушується в разі несанкціонованої зміни файлу?

   А. Доступність

   Б. Цілісність

   В. Масштабованість

   Г. Продуктивність

2. Що описує модель порушника?

   А. Лише перелік кабелів

   Б. Можливості, доступ і дії потенційного суб’єкта загроз

   В. Лише таблицю маршрутизації

   Г. Лише програмне забезпечення

3. Що є коректною основою перевірки захищеності?

   А. Особисте враження

   Б. Визначені вимоги і докази виконання

   В. Реклама продукту

   Г. Кількість серверів

7. УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ ТА КІБЕРБЕЗПЕКОЮ

Тематичний матеріал цього розділу структуровано відповідно до розділів і підрозділів наданої програми ЄДКІ; приклади, питання і тестові завдання створені для навчальної підготовки та не є відтворенням офіційних екзаменаційних завдань.

7.1. Кіберінциденти, реагування та розслідування

Кіберінцидент – подія або сукупність подій, що негативно впливає чи може вплинути на кібербезпеку. Типовий цикл реагування охоплює підготовку, виявлення та аналіз, стримування, усунення причини, відновлення і аналіз отриманих уроків. Під час розслідування зберігають часову послідовність, цілісність цифрових доказів і документують дії. Не кожне сповіщення IDS є підтвердженою атакою.

Практична ситуація. За ознак компрометації облікового запису спочатку перевіряють докази та масштаби доступу, здійснюють стримування відповідно до процедур і зберігають журнали.

Рекомендація до опрацювання. Складіть коротку схему ключових понять теми «Кіберінциденти, реагування та розслідування», зіставте визначення, призначення та типові обмеження і поясніть, якими ознаками можна підтвердити правильність технічного або організаційного рішення.

7.2. Ризики та методи їх оброблення

Ризик пов’язує ймовірність або можливість реалізації загрози з наслідками для активу. Ідентифікація охоплює актив, загрозу, уразливість та наслідок; аналіз визначає рівень ризику; оцінювання порівнює його з критеріями прийнятності. Варіанти оброблення: уникнення, зниження, передавання (розподіл) і усвідомлене прийняття ризику. Приклад навчальної моделі: $R = P \times I$, де P – оцінка ймовірності, I – оцінка впливу; шкали мають бути визначені заздалегідь.

Практична ситуація. Якщо ризик оцінено як P=4 та I=5 за п’ятибальною шкалою, умовний показник дорівнює 20; рішення залежить від порогів ризику організації.

Рекомендація до опрацювання. Складіть коротку схему ключових понять теми «Ризики та методи їх оброблення», зіставте визначення, призначення та типові обмеження і поясніть, якими ознаками можна підтвердити правильність технічного або організаційного рішення.

7.3. Політики інформаційної безпеки

Політика ІБ установлює принципи, відповідальність і загальні правила; стандарти, процедури та інструкції конкретизують її виконання. Політики доступу, використання інформаційних ресурсів, резервного копіювання, реагування та управління змінами повинні бути зрозумілими, доведеними до персоналу, актуальними й контрольованими. Показники результативності дають змогу перевіряти виконання вимог.

Практична ситуація. Політика вимагає своєчасного блокування доступу після звільнення; фактичне виконання перевіряють за заявками, часом деактивації і результатами аудиту.

Рекомендація до опрацювання. Складіть коротку схему ключових понять теми «Політики інформаційної безпеки», зіставте визначення, призначення та типові обмеження і поясніть, якими ознаками можна підтвердити правильність технічного або організаційного рішення.

7.4. Питання для самоперевірки

1. Які основні поняття та принципи охоплює тема «кіберінциденти, реагування та розслідування»?

2. Які типові загрози, помилки або обмеження слід враховувати в цій темі?

3. Як застосувати вивчені положення до наведеної практичної ситуації?

4. Які основні поняття та принципи охоплює тема «ризики та методи їх оброблення»?

5. Які типові загрози, помилки або обмеження слід враховувати в цій темі?

6. Як застосувати вивчені положення до наведеної практичної ситуації?

7. Які основні поняття та принципи охоплює тема «політики інформаційної безпеки»?

8. Які типові загрози, помилки або обмеження слід враховувати в цій темі?

9. Як застосувати вивчені положення до наведеної практичної ситуації?

7.5. Тренувальні тестові завдання

У кожному завданні виберіть одну правильну відповідь.

1. Який етап іде після стримування інциденту в типовому циклі реагування?

А. Усунення причини

Б. Відмова від документування

В. Видалення всіх журналів

Г. Публікація паролів

2. Що означає прийняття ризику?

А. Гарантію відсутності загроз

Б. Усвідомлене рішення залишити ризик на визначеному рівні

В. Неможливість його оцінки

Г. Автоматичне передавання ризику третій особі

3. Яке значення умовного ризику $R=P\times I$ за $P=3$ та $I=4$?

А. 7

Б. 12

В. 1

Г. 24

8. КРИПТОГРАФІЧНИЙ ЗАХИСТ ІНФОРМАЦІЇ

Тематичний матеріал цього розділу структуровано відповідно до розділів і підрозділів наданої програми ЄДКІ; приклади, питання і тестові завдання створені для навчальної підготовки та не є відтворенням офіційних екзаменаційних завдань.

8.1. Математичні основи криптографії

Арифметика за модулем визначає еквівалентність чисел за остачею. Найбільший спільний дільник обчислюють алгоритмом Евкліда; обернений елемент $a^{-1} \bmod n$ існує, якщо $\gcd(a,n)=1$. Теореми Ферма та Ейлера застосовують під час доведення властивостей операцій у скінченних множинах. Криптографічна геш-функція створює фіксований відбиток даних і має забезпечувати стійкість до знаходження прообразу, другого прообразу та колізій. Генерація випадкових і псевдовипадкових даних є критичною для ключів.

Практична ситуація. Для $17 \bmod 5$ отримуємо 2; обернений до 3 за модулем 7 дорівнює 5, оскільки $3\times5 \bmod 7 = 1$.

Рекомендація до опрацювання. Складіть коротку схему ключових понять теми «Математичні основи криптографії», зіставте визначення, призначення та типові обмеження і поясніть, якими ознаками можна підтвердити правильність технічного або організаційного рішення.

8.2. Симетричне шифрування

У симетричній криптосистемі той самий секретний ключ (або тісно пов’язані ключі) застосовується для шифрування й розшифрування. AES є блоковим шифром із розміром блоку 128 біт та ключами 128/192/256 біт; режими роботи визначають спосіб оброблення повідомлень довільної довжини. Потрібно відрізняти конфіденційність від автентичності та цілісності: режими автентифікованого шифрування забезпечують комплексні властивості за належного використання. Класичні шифри Цезаря, Вернама та гамування корисні для засвоєння принципів, але не є універсально придатними для сучасного захисту.

Практична ситуація. Повторне використання nonce у деяких режимах може призвести до суттєвого порушення безпеки, навіть якщо алгоритм AES реалізовано правильно.

Рекомендація до опрацювання. Складіть коротку схему ключових понять теми «Симетричне шифрування», зіставте визначення, призначення та типові обмеження і поясніть, якими ознаками можна підтвердити правильність технічного або організаційного рішення.

8.3. Асиметрична криптографія та цифровий підпис

Асиметрична криптографія використовує пару відкритого та особистого ключів. RSA спирається на математичні властивості модульних обчислень, а обмін Діффі–Геллмана дає змогу узгоджувати спільний секрет у відповідній групі. Цифровий підпис забезпечує перевірку автентичності джерела та цілісності підписаних даних, якщо належно реалізовано управління ключами. Сам по собі цифровий підпис не шифрує повідомлення.

Практична ситуація. Підписувач створює підпис особистим ключем, а перевіряльник використовує відповідний відкритий ключ; для довіри важлива перевірка належності ключа.

Рекомендація до опрацювання. Складіть коротку схему ключових понять теми «Асиметрична криптографія та цифровий підпис», зіставте визначення, призначення та типові обмеження і поясніть, якими ознаками можна підтвердити правильність технічного або організаційного рішення.

8.4. Цифрова стеганографія та водяні знаки

Стеганографія приховує факт існування повідомлення у контейнері (зображенні, аудіо чи іншому об’єкті); криптографія передусім приховує зміст. Метод LSB змінює найменш значущі біти окремих компонентів цифрового зображення. Основні характеристики стеганосистем: місткість, непомітність, стійкість до модифікацій, надійність відновлення повідомлення. Цифрові водяні знаки використовують для маркування, контролю походження та інших спеціалізованих завдань.

Практична ситуація. У 8-бітному значенні пікселя заміна останнього біта змінює числове значення не більше ніж на 1, але не гарантує невиявлюваності вбудовування.

Рекомендація до опрацювання. Складіть коротку схему ключових понять теми «Цифрова стеганографія та водяні знаки», зіставте визначення, призначення та типові обмеження і поясніть, якими ознаками можна підтвердити правильність технічного або організаційного рішення.

8.5. Питання для самоперевірки

1. Які основні поняття та принципи охоплює тема «математичні основи криптографії»?

2. Які типові загрози, помилки або обмеження слід враховувати в цій темі?

3. Як застосувати вивчені положення до наведеної практичної ситуації?

4. Які основні поняття та принципи охоплює тема «симетричне шифрування»?

5. Які типові загрози, помилки або обмеження слід враховувати в цій темі?

6. Як застосувати вивчені положення до наведеної практичної ситуації?

7. Які основні поняття та принципи охоплює тема «асиметрична криптографія та цифровий підпис»?

8. Які типові загрози, помилки або обмеження слід враховувати в цій темі?

9. Як застосувати вивчені положення до наведеної практичної ситуації?

10. Які основні поняття та принципи охоплює тема «цифрова стеганографія та водяні знаки»?

11. Які типові загрози, помилки або обмеження слід враховувати в цій темі?

12. Як застосувати вивчені положення до наведеної практичної ситуації?

8.6. Тренувальні тестові завдання

У кожному завданні виберіть одну правильну відповідь.

1. Який розмір блоку AES?

А. 64 біти

Б. 128 біт

В. 192 біти

Г. 256 біт

2. За якої умови існує обернений елемент a modulo n?

А. a=n

Б. gcd(a,n)=1

В. a парне

Г. n від’ємне

3. Чим перевіряють цифровий підпис в асиметричній схемі?

А. Відкритим ключем підписувача

Б. Паролем мережі Wi-Fi

В. Лише гешем без ключа

Г. Приватним ключем перевіряльника

9. ТЕХНІЧНИЙ ЗАХИСТ ІНФОРМАЦІЇ

Тематичний матеріал цього розділу структуровано відповідно до розділів і підрозділів наданої програми ЄДКІ; приклади, питання і тестові завдання створені для навчальної підготовки та не є відтворенням офіційних екзаменаційних завдань.

9.1. Технічні канали витоку

Технічний канал витоку виникає, коли інформативний сигнал поширюється фізичним середовищем і може бути сприйнятий поза санкціонованими межами. У програмі розглянуто віброакустичні, електричні, електромагнітні, оптичні, оптоелектронні та параметричні канали. Потрібно розрізняти джерело інформативного сигналу, шлях поширення, перетворення та засіб перехоплення. Оцінка ризику залежить від фізичних умов, характеристик обладнання і режимів роботи.

Практична ситуація. Мовлення в приміщенні може спричиняти механічні коливання огороджувальних конструкцій; захист передбачає аналіз фізичного шляху поширення.

Рекомендація до опрацювання. Складіть коротку схему ключових понять теми «Технічні канали витоку», зіставте визначення, призначення та типові обмеження і поясніть, якими ознаками можна підтвердити правильність технічного або організаційного рішення.

9.2. Пасивні й активні методи захисту

Пасивні методи зменшують небажане поширення інформативного сигналу: екранування, фільтрація, звукопоглинання, конструктивне розмежування. Активні методи вводять маскувальні сигнали або здійснюють інші контрольовані впливи відповідно до технічних умов. Вибір засобів повинен спиратися на оцінювання конкретного каналу та виконуватися з дотриманням вимог безпеки експлуатації.

Практична ситуація. Для електромагнітного каналу спочатку оцінюють можливі шляхи випромінювання і провідні лінії, а потім обирають екранування чи фільтрацію.

Рекомендація до опрацювання. Складіть коротку схему ключових понять теми «Пасивні й активні методи захисту», зіставте визначення, призначення та типові обмеження і поясніть, якими ознаками можна підтвердити правильність технічного або організаційного рішення.

9.3. Виявлення технічних засобів перехоплення і фізична безпека

Пошук несанкціонованих засобів отримання інформації здійснюють за встановленою процедурою з урахуванням типів потенційних каналів і характеристик контрольованого приміщення. Технічні засоби охорони, відеоспостереження та системи контролю фізичного доступу доповнюють захист інформації, але не підмінюють його. Доступ до приміщень, конфігурацій захисного обладнання та результатів обстежень має контролюватися.

Практична ситуація. Порушення контролю доступу до серверної може створити передумови для фізичного втручання, незалежно від налаштувань мережевого екрана.

Рекомендація до опрацювання. Складіть коротку схему ключових понять теми «Виявлення технічних засобів перехоплення і фізична безпека», зіставте визначення, призначення та типові обмеження і поясніть, якими ознаками можна підтвердити правильність технічного або організаційного рішення.

9.4. Питання для самоперевірки

1. Які основні поняття та принципи охоплює тема «технічні канали витоку»?

2. Які типові загрози, помилки або обмеження слід враховувати в цій темі?

3. Як застосувати вивчені положення до наведеної практичної ситуації?

4. Які основні поняття та принципи охоплює тема «пасивні й активні методи захисту»?

5. Які типові загрози, помилки або обмеження слід враховувати в цій темі?

6. Як застосувати вивчені положення до наведеної практичної ситуації?

7. Які основні поняття та принципи охоплює тема «виявлення технічних засобів перехоплення і фізична безпека»?

8. Які типові загрози, помилки або обмеження слід враховувати в цій темі?

9. Як застосувати вивчені положення до наведеної практичної ситуації?

9.5. Тренувальні тестові завдання

У кожному завданні виберіть одну правильну відповідь.

1. Який метод належить до пасивного технічного захисту?

А. Екранування

Б. Активне шумове маскування

В. Генерація перешкод

Г. Передача даних

2. До якого класу належать небажані випромінювання електронного обладнання?

А. Оптичного завжди

Б. Електромагнітного

В. Лише соціального

Г. Організаційного

3. Який захід знижує ризики фізичного втручання в серверну?

А. Контроль доступу

Б. Вимкнення журналів

В. Спільний пароль для всіх

Г. Відсутність інвентаризації

10. КОМПЛЕКСНЕ ПОВТОРЕННЯ ПЕРЕД ЄДКІ

10.1. Алгоритм завершального повторення

Після тематичної підготовки потрібно провести принаймні одне змішане тренування, що охоплює всі сім розділів. Завдання варто перемішувати, обмежувати тривалість виконання та фіксувати не лише результат, а й причини кожної помилки. Якщо здобувач правильно відповідає випадково, питання потрібно вважати таким, що потребує повторення.

10.2. Змішаний тренувальний тест

Нижче наведено 21 авторське навчальне запитання (по три з кожного розділу). Рекомендований тренувальний час – 25–30 хвилин; це методична рекомендація, а не офіційний регламент ЄДКІ.

1. Який закон визначає базові засади забезпечення кібербезпеки України?

А. Про основні засади забезпечення кібербезпеки України

Б. Про бухгалтерський облік

В. Про місцеві вибори

Г. Про державні закупівлі

2. Який стандарт установлює вимоги до системи управління інформаційною безпекою?

А. ISO/IEC 15408-3

Б. ISO/IEC 27001

В. IEEE 802.3

Г. RFC 791

3. Який документ найближче пов’язаний з Common Criteria?

А. ISO/IEC 15408

Б. ISO 9004

В. IEEE 802.11

Г. TLS 1.3

4. Який протокол належить до транспортного рівня?

А. IP

Б. TCP

В. DNS

Г. Ethernet

5. Яка асимптотична складність двійкового пошуку у відсортованому масиві?

А. $O(n^2)$

Б. $O(n)$

В. $O(\log n)$

Г. $O(2^n)$

6. Що зазвичай спільне для потоків одного процесу?

А. Окремі файлові системи

Б. Адресний простір процесу

В. Різні ядра ОС

Г. Незалежні облікові записи

7. Яку функцію виконує авторизація?

А. Визначає права на дії

Б. Встановлює IP-адресу

В. Перевіряє фізичну особу лише за паролем

Г. Стискає дані

8. Який показник визначає цільовий час відновлення?

А. RPO

Б. RTO

В. MTU

Г. TTL

9. Який засіб призначений для кореляції журналів безпеки?

А. SIEM

Б. DHCP

В. NAT

Г. RAID

10. Яка властивість порушується в разі несанкціонованої зміни файлу?

А. Доступність

Б. Цілісність

В. Масштабованість

Г. Продуктивність

11. Що описує модель порушника?

А. Лише перелік кабелів

Б. Можливості, доступ і дії потенційного суб’єкта загроз

В. Лише таблицю маршрутизації

Г. Лише програмне забезпечення

12. Що є коректною основою перевірки захищеності?

А. Особисте враження

Б. Визначені вимоги і докази виконання

В. Реклама продукту

Г. Кількість серверів

13. Який етап іде після стримування інциденту в типовому циклі реагування?

А. Усунення причини

Б. Відмова від документування

В. Видалення всіх журналів

Г. Публікація паролів

14. Що означає прийняття ризику?

А. Гарантію відсутності загроз

Б. Усвідомлене рішення залишити ризик на визначеному рівні

В. Неможливість його оцінки

Г. Автоматичне передавання ризику третій особі

15. Яке значення умовного ризику $R=P\times I$ за $P=3$ та $I=4$?

А. 7

Б. 12

В. 1

Г. 24

16. Який розмір блоку AES?

А. 64 біти

Б. 128 біт

В. 192 біти

Г. 256 біт

17. За якої умови існує обернений елемент a modulo n?

А. a=n

Б. gcd(a,n)=1

В. a парне

Г. n від’ємне

18. Чим перевіряють цифровий підпис в асиметричній схемі?

А. Відкритим ключем підписувача

Б. Паролем мережі Wi-Fi

В. Лише гешем без ключа

Г. Приватним ключем перевіряльника

19. Який метод належить до пасивного технічного захисту?

А. Екранування

Б. Активне шумове маскування

В. Генерація перешкод

Г. Передача даних

20. До якого класу належать небажані випромінювання електронного обладнання?

А. Оптичного завжди

Б. Електромагнітного

В. Лише соціального

Г. Організаційного

21. Який захід знижує ризики фізичного втручання в серверну?

А. Контроль доступу

Б. Вимкнення журналів

В. Спільний пароль для всіх

Г. Відсутність інвентаризації

10.3. Ключі до тренувальних тестів

Тематичні тести:

Розділ	Завдання 1	Завдання 2	Завдання 3
3	А	Б	А
4	Б	В	Б
5	А	Б	А
6	Б	Б	Б
7	А	Б	Б
8	Б	Б	А
9	А	Б	А

Змішаний тест:

1 – А 2 – Б 3 – А 4 – Б 5 – В 6 – Б 7 – А

8 – Б 9 – А 10 – Б 11 – Б 12 – Б 13 – А 14 – Б

15 – Б 16 – Б 17 – Б 18 – А 19 – А 20 – Б 21 – А

10.4. Аналіз результатів

Для кожного неправильного завдання запишіть тему, первинну відповідь, правильний варіант, правило або визначення, на якому ґрунтується рішення, і конкретну дію для усунення прогалини. Не варто оцінювати готовність лише за відсотком правильних відповідей, отриманим на одному наборі питань.

СПИСОК ВИКОРИСТАНИХ І РЕКОМЕНДОВАНИХ ДЖЕРЕЛ

1. Програма єдиного державного кваліфікаційного іспиту зі спеціальності «Кібербезпека» на першому (бакалаврському) рівні вищої освіти: наказ МОН України від 04.11.2022 № 980.

2. Закон України «Про інформацію». Офіційний портал Верховної Ради України: https://zakon.rada.gov.ua/.

3. Закон України «Про основні засади забезпечення кібербезпеки України». Офіційний портал Верховної Ради України: https://zakon.rada.gov.ua/.

4. Закон України «Про захист інформації в інформаційно-комунікаційних системах». Офіційний портал Верховної Ради України: https://zakon.rada.gov.ua/.

5. Закон України «Про захист персональних даних». Офіційний портал Верховної Ради України: https://zakon.rada.gov.ua/.

6. ISO/IEC 27001. Information security management systems – Requirements.

7. ISO/IEC 27002. Information security controls.

8. ISO/IEC 15408. Information technology – Security techniques – Evaluation criteria for IT security.

9. NIST SP 800-61. Computer Security Incident Handling Guide.

10. NIST SP 800-30. Guide for Conducting Risk Assessments.

11. RFC 8446. The Transport Layer Security (TLS) Protocol Version 1.3.

12. RFC 4301. Security Architecture for the Internet Protocol.

13. Постанова Кабінету Міністрів України від 15.07.2026 № 915 (перелік спеціальностей, для яких передбачено ЄДКІ): https://zakon.rada.gov.ua/laws/show/915-2026-%D0%BF.

ДОДАТОК А. ЛИСТ САМОКОНТРОЛЮ

Тематичний розділ	**Самооцінка (0–5)**	**Помилки / теми для повторення**
Законодавча та нормативно-правова база, державні та міжнародні вимоги, прак		
Інформаційні технології в інформаційній та/або кібербезпеці		
Безпека інформаційно-комунікаційних систем		
Комплексні системи захисту інформації		
Управління інформаційною та/або кібербезпекою		
Криптографічний захист інформації		
Технічний захист інформації		

Індивідуальний висновок: сильні теми _____.

Теми, які потребують доопрацювання _____.

Дата повторного тренувального тестування _____.

Єдиний державний кваліфікаційний іспит. Методичні вказівки з підготовки до єдиного державного кваліфікаційного іспиту (ЄДКІ) для здобувачів першого (бакалаврського) рівня вищої освіти освітньої програми «Кібербезпека» галузь знань 12 Інформаційні технології спеціальності 125 Кібербезпека та захист інформації денної та заочної форм навчання / уклад. С.М. Костючко. Луцьк: ЛНТУ, 2026. 39 с.

Комп’ютерний набір С.М. Костючко

Редактор С.М. Костючко

Підп. до друку «___» _____ 2025р.
Формат 60х84/16. Папір офс. Гарнітура Таймс.
Ум. друк. арк. ____. Тираж 10 прим. Зам. ____

Відділ іміджу та промоцій
Луцького національного технічного університету
43018, м. Луцьк, вул. Львівська, 75
ВІП ЛНТУ