

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ДЕРЖАВНИЙ УНІВЕРСИТЕТ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ
ТЕХНОЛОГІЙ
КАФЕДРА ІНЖЕНЕРІЇ ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ



**Методичні рекомендації до самостійної роботи
студентів з вивчення дисципліни
«СЕРТИФІКАЦІЯ ТА ЛІЦЕНЗУВАННЯ
ПРОГРАМНОГО ПРОДУКТУ»**

для здобувачів вищої освіти
спеціальності
121 «Інженерія програмного забезпечення»

Київ — 2024

Замрій І.В., Бажан Ю.П., Глушкова О.І.

Методичні рекомендації до самостійної роботи студентів з вивчення дисципліни «Сертифікація та ліцензування програмного продукту» для здобувачів вищої освіти спеціальності 121 «Інженерія програмного забезпечення». — К.: ДУІКТ, 2024. —16 с.

Укладачі: Замрій І.В., д-р техн. наук, доц.

Бажан Ю.П.

Глушкова О.І.

Рецензент: Вишнівський В.В., д-р техн. наук, проф.

Методичні рекомендації обговорено і затверджено на засіданні кафедри інженерії програмного забезпечення. Протокол №2 від 26.09.2024 р.

Рекомендовано Вченою радою Навчально-наукового інституту інформаційних технологій Державного університету інформаційно-комунікаційних технологій. Протокол №3 від 23.10. 2024 року.

Методичні вказівки з дисципліни «Сертифікація та ліцензування програмного продукту» містять перелік теоретичних питань, спрямованих на формування прикладних навичок у сфері забезпечення якості та правомірного використання програмного забезпечення.

Головна мета вказівок полягає в набутті студентами умінь і відпрацюванні навичок, необхідних сучасному фахівцю з інженерії програмного забезпечення для розуміння правових, організаційних і технічних аспектів сертифікації програмних продуктів, ліцензування програмного забезпечення, управління інтелектуальною власністю та забезпечення відповідності програмних систем вимогам національних і міжнародних стандартів і регуляторних норм.

Методичні вказівки призначені для здобувачів вищої освіти, які навчаються за спеціальністю 121 «Інженерія програмного забезпечення», а також для студентів інших спеціальностей, пов'язаних із програмуванням, бізнес-аналізом і проєктуванням інформаційних систем.

Вступ

Діяльність фахівця в галузі програмної інженерії у сучасних умовах нерозривно пов'язана із забезпеченням відповідності програмних продуктів нормативним, правовим і технічним вимогам, що висуваються замовниками, користувачами, регуляторами та іншими зацікавленими сторонами. Розробка й супровід програмних систем дедалі частіше потребують урахування питань сертифікації, ліцензування та захисту інтелектуальної власності на всіх етапах життєвого циклу програмного забезпечення.

Спеціаліст у галузі програмної інженерії повинен мати навички ефективної комунікації з колегами, партнерами, замовниками, клієнтами, користувачами та представниками регуляторних органів щодо вимог до сертифікації програмних продуктів, умов ліцензування та дотримання стандартів і правових норм.

Фахівець із розробки, тестування та супроводу програмного забезпечення має володіти знаннями про процедури сертифікації ПЗ, підготовку технічної й супровідної документації, формування доказів відповідності, вибір моделей ліцензування та управління ризиками порушення авторських і ліцензійних прав. Він повинен розуміти місце програмного продукту в нормативному та інформаційному середовищі, оцінювати вимоги стандартів і регуляторів, аналізувати правові обмеження й забезпечувати відповідність програмної системи встановленим критеріям якості та безпеки.

Зміст

Тема 1	
Документація процесу розробки програмного продукту.....	5
Навчальні цілі	
Теоретичний зміст	
Завдання для самостійної роботи	
Питання для самоконтролю	
Тема 2	
Сертифікація програмного продукту.....	8
Навчальні цілі	
Теоретичний зміст	
Завдання для самостійної роботи	
Питання для самоконтролю	
Тема 3	
Ліцензування програмного продукту.....	11
Навчальні цілі	
Теоретичний зміст	
Завдання для самостійної роботи	
Питання для самоконтролю	
Тема 4	
Авторське право на програмний продукт.....	13
Навчальні цілі	
Теоретичний зміст	
Завдання для самостійної роботи	
Питання для самоконтролю	
Список джерел.....	15

Тема 1 : Документація процесу розробки програмного продукту

Навчальні цілі

Навчитись визначати та описувати процес сертифікаційного тестування програмного забезпечення. Сформувані розуміння етапів і вимог до проведення сертифікаційних випробувань відповідно до національних і міжнародних стандартів.

Теоретичний зміст

Процес розробки програмного забезпечення є впорядкованою сукупністю етапів життєвого циклу ПЗ (SDLC), що включає аналіз вимог, проєктування, реалізацію, тестування, впровадження та супровід. Кожен із цих етапів супроводжується створенням відповідної документації, яка забезпечує формалізацію вимог, фіксацію архітектурних рішень, відстеження змін і контроль якості продукту. У сучасній ІТ-індустрії документація є не лише технічним артефактом, а інструментом управління ризиками, забезпечення прозорості розробки та основою для подальшої сертифікації й правового захисту програмного продукту.

Документація в інженерії програмного забезпечення виконує ключові функції: забезпечує узгодженість між замовником, бізнес-аналітиками, розробниками і тестувальниками; формалізує функціональні та нефункціональні вимоги; створює основу для планування і проведення тестування; слугує доказовою базою під час сертифікації; забезпечує відтворюваність і аудит процесу розробки. Відповідно до міжнародних стандартів ISO/IEC 12207 та ISO/IEC 15289 документація є невід'ємною складовою процесів життєвого циклу ПЗ та необхідною умовою підтвердження відповідності програмного продукту встановленим вимогам якості й безпеки.

Особливого значення документація набуває у контексті сертифікації програмного продукту. Органи сертифікації оцінюють не лише функціональність ПЗ, але й повноту, актуальність і структурованість документації. Саме вона підтверджує, що продукт створено в керованому процесі, тестування проводилося за визначеними методиками, а результати є достовірними та відтворюваними. У критичних інформаційних системах документація також використовується для аудиту інформаційної безпеки, перевірки відповідності регуляторним вимогам і аналізу готовності системи до промислової експлуатації.

В українській ІТ-практиці питання документації та сертифікації набули особливої актуальності у фінансовому, державному та оборонному секторах.

Фінтех-компанії, банки та платіжні сервіси, такі як NovaPay, monobank, ПриватБанк або державні розрахункові платформи, зобов'язані підтверджувати відповідність своїх програмних продуктів вимогам інформаційної безпеки, захисту персональних даних та стабільності функціонування. Для цього застосовуються внутрішні стандарти розробки, обов'язкове тестування, аудит коду й формалізована документація, яка є основою для регуляторних перевірок Національного банку України.

Державні цифрові сервіси також демонструють сучасний підхід до документування та сертифікації. Платформа Дія і пов'язані з нею інформаційні системи створюються з використанням стандартизованих підходів до опису вимог, архітектури, API та безпекових механізмів. Це дозволяє не лише забезпечувати масштабованість і надійність сервісів, але й проходити перевірки щодо відповідності вимогам захисту державних інформаційних ресурсів. Документація таких проєктів використовується як для внутрішнього контролю якості, так і для зовнішніх аудитів і сертифікаційних процедур.

В українських IT-компаніях, що працюють на міжнародний ринок, таких як EPAM Ukraine, SoftServe, GlobalLogic або Luxoft, документування процесів розробки є частиною корпоративних систем управління якістю. Компанії впроваджують стандарти ISO 9001, ISO/IEC 27001 та моделі зрілості процесів, що вимагають наявності формалізованої технічної та процесної документації. Це дозволяє підтверджувати відповідність розробки міжнародним вимогам і забезпечувати готовність проєктів до сертифікації у сфері безпеки, медицини або автомобільної індустрії.

Таким чином, якісно сформована документація створює підґрунтя для подальших етапів дисципліни — планування сертифікаційного тестування, розробки тестових сценаріїв, підготовки звітів про відповідність і прийняття рішень щодо допуску програмного продукту до експлуатації. В умовах розвитку цифрової держави, фінтех-сектору та критичних інформаційних систем в Україні документація стає не лише інструментом розробки, а стратегічним елементом забезпечення якості, безпеки та довіри до програмного забезпечення.

Завдання для самостійної роботи

1. Описати призначення програмного продукту, сферу його застосування та цільову аудиторію.
2. Визначити нормативні документи, стандарти або технічні регламенти, вимогам яких має відповідати програмний продукт.

3. Сформувати перелік функціональних вимог до ПЗ відповідно до обраного стандарту або специфікації.
4. Визначити нефункціональні вимоги, зокрема вимоги до якості, безпеки, надійності, продуктивності та захисту даних.

Питання для самоконтролю

1. Яке призначення програмної документації у життєвому циклі ПЗ?
2. Які документи належать до документації продукту?
3. Які документи належать до документації процесу?
4. Яке значення має документ вимог для подальшого тестування?
5. Чому документація є ключовим елементом сертифікації ПЗ?
6. Яке основне призначення документації процесу розробки в межах ІТ-проєкту?
7. У чому полягає принципова різниця між продуктовою та процесною документацією?
8. Які існують основні типи процесної документації (плани, звіти, графіки, протоколи)?
9. Як документація впливає на "технічний борг" та підтримку програмного продукту в майбутньому?
10. Які міжнародні стандарти регулюють процеси документування в програмній інженерії?
11. Що має містити Документація архітектури ПЗ?
12. Як документуються зміни в коді за допомогою систем контролю версій?
13. Що таке WBS (Work Breakdown Structure) і як вона відображається в проєктній документації?
14. Як документуються ризики проєкту (Реєстр ризиків)?
15. Яке значення мають Протоколи нарад (Meeting Minutes) для процесу розробки?
16. Як здійснюється документування процесу управління конфігураціями?
17. Яка роль інструментів CI/CD у документуванні результатів збирання та розгортання продукту?
18. Які критерії якості застосовуються до самої документації?
19. Як проводиться аудит (рев'ю) документації процесу?
20. Як документується процес передачі продукту на підтримку?

Тема 2. Сертифікація програмного продукту

Навчальні цілі

Навчитись розуміти призначення та роль сертифікації програмного продукту в життєвому циклі розробки. Сформувати здатність визначати підходи, процедури та результати сертифікації програмного забезпечення відповідно до встановлених стандартів і нормативних вимог.

Теоретичний зміст

Сертифікація програмного продукту є важливим інструментом забезпечення якості, безпеки та надійності програмного забезпечення в умовах сучасної цифрової економіки. Вона полягає в офіційному підтвердженні відповідності програмного продукту встановленим вимогам стандартів, нормативно-правових актів або технічних регламентів. Сертифікація дозволяє знизити ризики використання програмного забезпечення в критичних інформаційних системах, фінансових сервісах, державних інформаційних ресурсах та інших сферах, де помилки або вразливості можуть призвести до значних збитків і втрати довіри користувачів. У сучасних умовах цифровізації державних і комерційних послуг сертифікація програмних продуктів стає інструментом формування прозорих і безпечних відносин між розробником, користувачем і регулятором.

Процес сертифікації програмного продукту охоплює комплекс організаційних, технічних і процедурних заходів. Він починається з підготовки пакета документації, що містить опис функціональних характеристик програмного забезпечення, архітектури системи, вимог до інформаційної безпеки, експлуатаційної документації та результатів внутрішнього тестування. Далі проводяться сертифікаційні випробування, під час яких незалежна уповноважена організація оцінює відповідність продукту встановленим критеріям. Випробування можуть включати функціональне, навантажувальне, безпекове тестування, аналіз програмного коду, перевірку журналів подій та механізмів контролю доступу. У критичних системах додатково перевіряються криптографічні засоби захисту та дотримання вимог щодо обробки персональних даних.

Сертифікацію програмних продуктів класифікують за різними ознаками. За обов'язковістю вона поділяється на обов'язкову і добровільну. Обов'язкова сертифікація встановлюється для програмного забезпечення, що використовується у сферах державного управління, фінансів, оборони, медицини та інших критичних галузях. Добровільна сертифікація ініціюється

розробником для підтвердження якості продукту та підвищення його конкурентоспроможності. За об'єктом оцінювання розрізняють сертифікацію програмного коду, готового програмного продукту та процесів розробки. За глибиною перевірки застосовують декларативну сертифікацію або сертифікацію з повним незалежним аудитом і зовнішніми випробуваннями.

Важливу роль у сертифікації відіграють міжнародні та національні стандарти. ISO/IEC 25010 визначає модель якості програмного забезпечення, ISO/IEC 12207 регламентує процеси життєвого циклу розробки, а ISO/IEC 27001 встановлює вимоги до систем управління інформаційною безпекою. Галузеві регламенти застосовуються для фінансових, медичних і державних інформаційних систем. Відповідність стандартам підвищує довіру користувачів, партнерів і регуляторів до програмного продукту.

Окремим напрямом є сертифікація хмарних сервісів і програмного забезпечення як сервісу. У таких моделях оцінюється не лише сам продукт, а й інфраструктура його розміщення, механізми резервного копіювання, безперервність надання послуг та захист персональних даних. Це особливо актуально для електронних державних сервісів і фінансових платформ.

Результатом сертифікації є прийняття рішення про відповідність програмного продукту встановленим вимогам і видача сертифіката. Наявність сертифіката може бути обов'язковою умовою виходу продукту на ринок або участі в державних закупівлях. Таким чином, сертифікація програмного продукту виступає механізмом контролю якості, управління ризиками, забезпечення інформаційної безпеки та формування довіри до сучасних цифрових систем.

Завдання для самостійної роботи

1. Опрацювати нормативні документи, що регламентують сертифікацію програмного забезпечення в Україні та міжнародній практиці.
2. Побудувати схему процесу сертифікації програмного продукту із зазначенням основних етапів і результатів кожного з них.
3. Навести приклади програмних продуктів, що підлягають обов'язковій сертифікації, та обґрунтувати причини такої вимоги.

Питання для самоконтролю

1. У чому полягає мета сертифікації програмного продукту?
2. Які основні етапи процесу сертифікації програмного забезпечення?
3. Які документи є необхідними для проходження сертифікаційних випробувань?

4. Чим відрізняється обов'язкова сертифікація від добровільної?
5. Хто є учасниками процесу сертифікації (замовник, орган із сертифікації, випробувальна лабораторія)?
6. Що таке акредитація органу з сертифікації та чому вона важлива для визнання сертифіката на міжнародному рівні?
7. Які елементи програмного продукту можуть підлягати сертифікації (код, документація, інтерфейси)?
8. Як класифікуються програмні продукти залежно від ступеня ризику (наприклад, рівні критичності в авіоніці чи медицині)?
9. Чим відрізняються методи «білої скриньки» та «чорної скриньки» під час сертифікаційних випробувань?
10. Як проводиться оцінка надійності ПЗ (reliability) під час сертифікації?
11. Які специфічні вимоги висуваються до сертифікації засобів криптографічного захисту інформації?
12. Який термін дії сертифіката відповідності на програмний продукт?
13. Чи потрібно проходити сертифікацію заново після випуску критичного оновлення (patch) або нової версії ПЗ?
14. Що таке інспекційний контроль за сертифікованим продуктом?
15. Яку юридичну відповідальність несе орган із сертифікації за помилкові висновки?
16. Як співвідносяться сертифікація програмного продукту та його державна реєстрація (наприклад, у реєстрі ПЗ)?
17. Що таке взаємне визнання сертифікатів (наприклад, угода CCRA) і як воно допомагає в експорті ПЗ?
18. Які особливості сертифікації хмарних сервісів (SaaS) порівняно з локальним ПЗ?

Тема 3. Ліцензування програмного продукту

Навчальні цілі

Навчитись розуміти призначення та правову природу ліцензування програмного продукту. Сформувати здатність визначати види ліцензій, умови їх застосування та вимоги до правомірного використання програмного забезпечення.

Теоретичний зміст

Ліцензування програмного продукту є правовим механізмом надання дозволу на використання програмного забезпечення відповідно до визначених умов власника авторських прав. На відміну від сертифікації, яка підтверджує якість і відповідність продукту стандартам, ліцензування регулює питання інтелектуальної власності, розподілу прав та відповідальності сторін. Ліцензія визначає обсяг дозволених дій користувача, зокрема встановлення, копіювання, модифікацію, поширення або комерційне використання програмного забезпечення. Вибір моделі ліцензування впливає на бізнес-стратегію компанії-розробника, спосіб монетизації продукту та рівень контролю над його використанням.

Сучасна практика передбачає різні підходи до ліцензування, серед яких пропрієтарні, відкриті, умовно-безкоштовні, підписні та корпоративні моделі. Пропрієтарні ліцензії передбачають повне збереження виключних майнових прав за правовласником і надають користувачу обмежене право використання програмного продукту без доступу до вихідного коду, що характерно для комерційного програмного забезпечення. Відкриті ліцензії дозволяють доступ до вихідного коду та його модифікацію за умови дотримання визначених ліцензійних правил, що сприяє розвитку спільнот розробників і технологічній прозорості. Умовно-безкоштовні моделі надають користувачу можливість безоплатного використання обмеженої версії продукту з подальшою оплатою за розширений функціонал. Підписка як сервіс передбачає надання доступу до програмного забезпечення протягом визначеного часу із регулярною оплатою, що є типовим для хмарних і SaaS-рішень. Корпоративні ліцензії дозволяють використання програмного продукту великою кількістю користувачів у межах однієї організації з централізованим управлінням правами доступу. Кожен із цих підходів має власні правові та технічні особливості, переваги й обмеження. Важливу роль у ліцензуванні відіграють міжнародні норми авторського права, Бернська конвенція, угоди WIPO, а також національне законодавство про авторське право і суміжні права.

Порушення умов ліцензії може призвести до юридичної відповідальності, фінансових санкцій або заборони використання програмного продукту. У сфері корпоративних і державних інформаційних систем ліцензування також є інструментом забезпечення інформаційної безпеки, контролю оновлень та легальності програмного забезпечення. Окрему увагу приділяють ліцензуванню програмного забезпечення як сервісу (SaaS), де користувач отримує доступ до функціоналу без встановлення продукту, а правові відносини регулюються умовами онлайн-договорів.

Такі моделі вимагають визначення відповідальності за збереження даних, доступність сервісу та захист персональної інформації. Таким чином, ліцензування програмного продукту є необхідною умовою правомірного використання програмного забезпечення, захисту інтересів розробника та формування прозорих відносин між виробником і користувачем.

Завдання для самостійної роботи

1. Опрацювати основні види ліцензій програмного забезпечення та підготувати коротку порівняльну таблицю їх характеристик.
2. Навести приклади відкритих та пропрієтарних ліцензій і визначити сфери їх застосування.
3. Проаналізувати типову користувацьку ліцензійну угоду (EULA) будь-якого програмного продукту.

Питання для самоконтролю

1. У чому полягає правова сутність ліцензування програмного продукту?
2. Які основні види ліцензій програмного забезпечення?
3. Чим відрізняється відкрита ліцензія від пропрієтарної?
4. Які наслідки має порушення умов ліцензійної угоди?
5. Які обов'язкові істотні умови мають бути прописані в ліцензійному договорі згідно з законодавством?
6. Що означає термін «обсяг прав», що надаються за ліцензією?
7. У чому полягає різниця між виключною, невиключною та одиничною ліцензіями?
8. Які територіальні та часові обмеження можуть встановлюватися в ліцензійній угоді?
9. Опишіть особливості ліцензій типу «Perpetual» (безстрокова) та «Subscription» (підписка).
10. Чим відрізняються ліцензії «на користувача» (Per User) від ліцензій «на пристрій» (Per Device)?

11. Що таке OEM-ліцензії та які обмеження щодо розповсюдження вони накладають?
12. Які особливості мають корпоративні ліцензії (Volume Licensing)?
13. Що таке ліцензування за моделлю SaaS (Software as a Service) і чи надається в цьому випадку копія ПЗ користувачеві?
14. Що таке «ліцензійний аудит» і які права має правовласник щодо його проведення у клієнта?
15. Які ризики виникають при змішуванні (mixing) кодів під різними ліцензіями (проблема сумісності ліцензій)?
16. Що таке положення про обмеження відповідальності (Disclaimer of Warranty) у ліцензіях?
17. Які наслідки для бізнесу може мати використання ПЗ без належної ліцензії?
18. Як відбувається розірвання ліцензійної угоди та які обов'язки виникають у користувача після цього?

Тема 4. Авторське право на програмний продукт

Навчальні цілі

Навчитись розуміти правову природу авторського права на програмні продукти. Сформулювати здатність визначати об'єкти авторського права у сфері програмного забезпечення, права автора та механізми їх правового захисту.

Теоретичний зміст

Авторське право на програмний продукт є основним правовим інструментом захисту результатів інтелектуальної діяльності у сфері розробки програмного забезпечення. В Україні програмні продукти визнаються об'єктом авторського права і охороняються як літературні твори; право виникає автоматично з моменту створення коду без необхідності державної реєстрації, хоча реєстрація може використовуватися як доказ авторства у разі виникнення спорів. Законодавство гарантує автору виключні майнові та немайнові права, що включають контроль над використанням, копіюванням, поширенням та модифікацією програмного забезпечення. Майнові права дозволяють отримувати винагороду за використання програмного продукту через продаж ліцензій або передачу прав, а немайнові забезпечують визнання авторства та захист репутації автора. Авторське право захищає форму вираження

програмного продукту, тобто конкретний програмний код, але не захищає ідеї, алгоритми чи математичні методи, що лежать в основі функціонування системи. У трудових або договірних відносинах важливим є правильне визначення переходу майнових прав від розробника до роботодавця чи замовника, оскільки відсутність таких положень може призвести до юридичних конфліктів щодо прав на створений продукт.

Сучасна практика ІТ-індустрії України демонструє різні підходи до реалізації авторського права. Наприклад, державний цифровий сервіс Дія є програмним продуктом, що охороняється авторським правом, але частина його програмного коду оприлюднена як відкритий вихідний код. Це дозволяє іншим розробникам використовувати і вдосконалювати окремі компоненти за умов дотримання ліцензії, зберігаючи при цьому правовий захист держави як правовласника. Такий підхід поєднує принципи відкритості цифрової держави та захисту інтелектуальної власності. В українських ІТ-компаніях типовою є практика укладання договорів, які закріплюють перехід майнових прав на програмний продукт до компанії-замовника або роботодавця, що забезпечує правову визначеність при комерціалізації продукту та виході на міжнародні ринки.

Додаткову увагу в сучасних умовах приділяють захисту авторських прав у цифровому середовищі. До таких механізмів належать використання ліцензійних ключів, цифрових підписів, систем контролю доступу та договірних обмежень у користувацьких угодах. Окремим актуальним напрямом є визначення правового режиму програмних продуктів, створених із застосуванням штучного інтелекту або з використанням відкритих бібліотек, що потребує дотримання умов відповідних ліцензій. Порухення авторських прав у сфері програмного забезпечення може призвести до цивільної, адміністративної або кримінальної відповідальності. Таким чином, авторське право забезпечує правову основу функціонування ІТ-ринку, захищає інтереси розробників і компаній та стимулює розвиток цифрової економіки України.

Завдання для самостійної роботи

1. Опрацювати положення законодавства України щодо авторського права на програмні продукти.
2. Визначити, які елементи програмного забезпечення охороняються авторським правом, а які — ні.
3. Навести приклади типових порушень авторських прав у сфері програмного забезпечення.

Питання для самоконтролю

1. Коли виникає авторське право на програмний продукт?
2. Які права надає авторське право розробнику програмного забезпечення?
3. Які елементи програмного продукту не підлягають авторсько-правовій охороні?
4. Які складові програми підлягають захисту (вихідний код, об'єктний код, інтерфейс, документація)?
5. Чи поширюється авторське право на ідеї, алгоритми, методи роботи та мови програмування? Обґрунтуйте відповідь.
6. У чому полягає різниця між захистом програми як «літературного твору» та патентуванням функціоналу?
7. Що таке «похідний твір» у контексті програмного забезпечення?
8. Чим відрізняються дозвільні ліцензії (MIT, BSD) від суворих вільних ліцензій?
9. Які ризики виникають при використанні Open Source компонентів у комерційному продукті?
10. Які існують технічні засоби захисту авторського права (DRM)?
11. Яка відповідальність (цивільна, адміністративна, кримінальна) передбачена за порушення авторських прав на ПЗ?
12. Що таке «вільне використання» програмного продукту в наукових та освітніх цілях?

Рекомендована література:

1. Wiegers K., Beatty J. Software Requirements: 3rd Edition. Microsoft Press, Redmond, 2021. 640 p.
2. Sommerville I. Software Engineering: 11th Edition. Pearson Education, London, 2021. 816 p.
3. ISTQB. ISTQB Certified Tester Foundation Level Syllabus v4.0. International Software Testing Qualifications Board, Brussels, 2023. 123 p.
4. ISO/IEC/IEEE 12207:2022. Systems and Software Engineering — Software Life Cycle Processes. International Organization for Standardization, Geneva, 2022. 142 p.
5. ISO/IEC/IEEE 15289:2023. Systems and Software Engineering — Content of Life-Cycle Information Items. International Organization for Standardization, Geneva, 2023. 118 p.

6. ISO/IEC 25010:2023. Systems and Software Engineering — Systems and Software Quality Requirements and Evaluation (SQuaRE) — System and Software Quality Models. International Organization for Standardization, Geneva, 2023. 34 p.
7. ISO/IEC/IEEE 29148:2018. Systems and software engineering — Life cycle processes — Requirements engineering.
8. ISO/IEC 27001:2022. Information Security, Cybersecurity and Privacy Protection — Information Security Management Systems — Requirements. International Organization for Standardization, Geneva, 2022. 22 p.
9. European Union Agency for Cybersecurity (ENISA). Cybersecurity Certification Framework for ICT Products and Services. ENISA Report, Athens, 2023. 96 p.
10. WIPO. Intellectual Property and Software: Copyright and Licensing in the Digital Economy. World Intellectual Property Organization, Geneva, 2022. 110 p.
11. OECD. Digital Product Assurance and Certification in the Global Software Market. OECD Publishing, Paris, 2024. 88 p.
12. Стандартизація та сертифікація товарів і послуг / Надія Салухіна, Олена Язвінська – Центр навчальної літератури, 2023 рік, 426 стор.
13. Цивільний кодекс України. Книга четверта «Право інтелектуальної власності».
14. Закон України «Про інформацію».
15. Закон України «Про авторське право і суміжні права».
16. Beck K., Beedle M., van Bennekum A. et al. Manifesto for Agile Software Development. 2001.
17. Sommerville I. Software Engineering. 10th ed. Pearson Education, 2016.