УДК 004.4:658.5

С. Г. Московко; Р. Н. Квєтний, д-р техн. наук, проф.

ІНТЕГРАЦІЯ МЕХАНІЗМІВ БЕЗПЕКИ ТА КОНФІДЕНЦІЙНОСТІ У ПРЕДМЕТНУ МОДЕЛЬ ПРЕДМЕТНО-ОРІЄНТОВАНИХ СИСТЕМ ЕЛЕКТРОННОЇ КОМЕРЦІЇ

Стаття присвячена інтеграції механізмів інформаційної безпеки безпосередньо у предметну модель предметно-орієнтованих систем електронної комерції з фокусом на цілях захисту (конфіденційність, цілісність, доступність) і політиках, що їх реалізують. Показано, що запізніле впровадження захисту на етапах тестування чи розгортання не дає змоги повноцінно врахувати вимоги безпеки в архітектурі та підвищує ризики інцидентів. Запропоновано формалізований підхід, у межах якого цілі захисту (конфіденційність, цілісність, доступність) позначаються на рівні доменної моделі, а атрибути безпеки (властивості суб'єктів/об'єктів/сесій) маркуються для реалізації політик доступу з використанням мета-моделювання та моделей загроз. Сформульовано математичну постановку із множинами об'єктів, загроз і атрибутів, вагами ризику та критерієм мінімізації інтегрального ризику. Ключовим внеском є формальна функція атрибуції, що дозволяє ідентифікувати критичні об'єкти, визначати зони підвищеної небезпеки й узгоджено застосовувати політики доступу (RBAC/ABAC) і відповідні технічні механізми (авторизація, шифрування) з урахуванням контексту інформаційних потоків і зовнішніх інтеграцій.

Ефективність підходу продемонстровано на прикладі типової e-commerce системи, спроєктованої за принципами domain-drivendesign із доменами «Користувачі», «Каталог», «Замовлення», «Платежі» та «Доступ». Раннє вбудовування безпекових атрибутів забезпечує прозоре узгодження вимог безпеки з бізнес-логікою, полегшує взаємодію аналітиків і фахівців з кібербезпеки та створює основу для автоматизованої валідації. Експериментально показано зменшення кількості критичних об'єктів і високоризикових елементів та зниження інтегральної оцінки ризику порівняно з традиційними підходами, що підтверджує дієвість принципу «security by design»; підхід також узгоджується з «privacy by design» щодо персональних даних як складової конфіденційності. Результати можуть бути використані для побудови безпечних систем електронної комерції з відповідністю сучасним стандартам і регуляторним вимогам, включно з ISO/IEC 27001, PCI DSS та GDPR, а також для подальшої автоматизації перевірок через шаблони, правила та інструменти моделювання.

Ключові слова: *електронна комерція, предметна модель, інформаційна безпека, конфіденційність, моделювання загроз, мета-моделювання.*

Вступ

Інформаційні системи електронної комерції відіграють визначальну роль у цифровій економіці, забезпечуючи автоматизовану взаємодію між постачальниками, споживачами та платіжними сервісами. З огляду на їхню масштабованість, динамічність і високий ступінь інтеграції з зовнішніми платформами (CRM-системи, аналітичні модулі, платіжні шлюзи), критично важливим постає питання гарантування інформаційної безпеки та захисту конфіденційних даних. Обробка персональних і фінансових відомостей вимагає відповідності сучасним міжнародним стандартам (ISO/IEC 27001, PCI DSS) і нормативно-правовому регулюванню, зокрема GDPR та Закону України «Про захист персональних даних».

Попри наявність розвинених технічних засобів захисту, більшість з них впроваджуються лише на завершальних етапах життєвого циклу системи – під час тестування, розгортання чи експлуатації. Такий підхід призводить до втрати можливостей своєчасного врахування вимог безпеки в архітектурі системи, підвищує ризики інформаційних інцидентів та ускладнює адаптацію систем до змін середовища або регуляторних вимог. Особливо критичним є той факт, що на етапі побудови предметної моделі – як основи логіко-структурного проєктування – питання безпеки зазвичай розглядаються поверхнево або зовсім ігноруються. У межах цієї роботи конфіденційність розглядається як одна з цілей інформаційної безпеки (разом із

цілісністю та доступністю), що враховується вже на рівні предметної моделі.

У зв'язку з цим актуальним є створення методологічного підходу до інтеграції механізмів забезпечення безпеки та конфіденційності безпосередньо у предметну модель. Такий підхід має забезпечувати цілісну реалізацію принципів «вбудованої безпеки» (security by design) шляхом включення у модель структурованих вимог до захисту даних, атрибутів безпеки та політик доступу.

Актуальність дослідження зумовлена необхідністю врахування вимог інформаційної безпеки саме на етапі моделювання логіки системи, що дає змогу запобігти типовим загрозам, таким як несанкціонований доступ, витік конфіденційної інформації та порушення цілісності бізнес-процесів.

Наукова новизна полягає у формалізації функції атрибуції атрибутів безпеки до об'єктів предметної області та в інтеграції моделей загрозу структуру предметної моделі, що дозволяє проводити валідацію безпеки системи вже на архітектурному рівні.

Метою роботи є розроблення формалізованого підходу до інтеграції механізмів інформаційної безпеки у предметну модель інформаційних систем електронної комерції з урахуванням ризик-орієнтованого аналізу та сучасних моделей загроз з формальним позначенням цілей захисту (C/I/A) та атрибутів безпеки, які використовують політики доступу.

Постановка задачі

Для підвищення рівня інформаційної безпеки в системах електронної комерції доцільно здійснювати інтеграцію механізмів інформаційної безпеки не як додаткового шару після проєктування функціоналу, а безпосередньо на етапі моделювання предметної області. Такий підхід дозволяє врахувати специфіку даних, логіку бізнес-процесів, а також потенційні загрози ще до впровадження системи. У зв'язку з цим постає необхідність формалізованого опису предметної моделі із вбудованими політиками доступу, обмеженнями, шифруванням та іншими механізмами, що реалізують цілі конфіденційності, цілісності та доступності даних.

Для вирішення цієї науково-прикладної проблеми необхідно виконати такі основні завдання:

1. Провести аналіз наявних підходів до моделювання систем електронної комерції з урахуванням вимог безпеки.
2. Визначити базові компоненти предметної моделі предметно-орієнтованої системи електронної комерції.
3. Розробити концептуальну модель інтеграції механізмів безпеки та конфіденційності на рівні логічного представлення предметної області.
4. Реалізувати прикладну модель для демонстрації ефективності запропонованого підходу в умовах онлайн-магазину.
5. Провести кількісну оцінку ефективності запропонованої моделі шляхом вимірювання зниження критичних об'єктів, високоризикових елементів та інтегрального ризику у порівнянні з традиційними підходами.

Розв'язання зазначених завдань дозволить сформувати цілісний підхід до побудови безпечних інформаційних систем електронної комерції на основі предметно-орієнтованого моделювання.

Огляд літератури

Сучасні дослідники дедалі частіше застосовують предметно-орієнтований підхід (Domain-Driven Design, DDD) у розробці електронної комерції, акцентуючи увагу на важливості побудови архітектури навколо бізнес-доменів. Зокрема, у дослідженні Naresh Pala [1] на прикладі великомасштабної e-commerce платформи було доведено, що використання DDD дозволяє суттєво покращити гнучкість та управління складністю

системи, підвищуючи її узгодженість із бізнес-цілями та ефективність взаємодії з користувачами.

Водночас, актуальним залишається питання інтеграції механізмів безпеки безпосередньо на етапі проєктування, що відоме як принцип «Security by Design». Faisal Nabi та ін. [2] наголошують на необхідності вбудовування перевірок безпеки в логіку компонентів e-commerce застосунків, оскільки лише традиційних методів захисту (шифрування, автентифікації тощо) недостатньо для запобігання логічним вразливостям. Ibrahim Alfadli [3] також підтверджує необхідність комплексної моделі безпеки, яка охоплює автентифікацію, авторизацію, шифрування та моніторинг транзакцій, і показує, що саме інтеграція цих механізмів у архітектуру веб-сайтів електронної комерції дозволяє значно зменшити ризики витоку даних та інших інформаційних інцидентів.

Окрім безпеки, інтеграція механізмів конфіденційності за принципом «Privacy by Design» набуває ключового значення для відповідності регуляторним вимогам (GDPR). Gedeon та ін. [4] підкреслюють, що комплексне впровадження принципів безпеки та конфіденційності за проєктом сприяє формуванню довіри споживачів, що особливо важливо у сфері електронної комерції. Утім, систематичний огляд Andrade та ін. [5] виявив нестачу чітких моделей і методологій, які могли б забезпечити належну інтеграцію приватності у життєвий цикл розробки програмного забезпечення.

Водночас, дослідження Saqib Saeed [6] емпірично підтверджує прямий вплив сприйняття рівня безпеки та приватності на довіру користувачів та їх поведінку під час онлайн-покупок. Автор наголошує, що органічна інтеграція захисту даних та прозорість обробки інформації формують позитивний користувацький досвід та сприяють зростанню бізнес-результатів e-commerce платформ.

Отже, сучасні наукові дослідження підкреслюють необхідність комплексного застосування предметно-орієнтованого підходу в поєднанні з принципами «безпеки за проєктом» та «конфіденційності за проєктом». Це забезпечує як відповідність сучасним регуляторним стандартам, так і підвищує довіру користувачів, створюючи умови для сталого розвитку платформ електронної комерції.

Методологія

Методологічна основа дослідження ґрунтується на концепції включення вимог безпеки та конфіденційності безпосередньо у логічну структуру предметної моделі інформаційної системи електронної комерції. На першому етапі було здійснено формалізацію предметної області з визначенням базових об'єктів, що виступають носіями критичних даних та операцій. До ключових компонентів такої моделі належать сутності користувачів, транзакції, продукти, інформаційні потоки, а також допоміжні служби, зокрема логістичні модулі, шлюзи оплати та комунікаційні підсистеми. Для кожного з компонентів визначаються структурні атрибути, які впливають на подальшу інтеграцію політик доступу та захисту даних. У таблиці 1 наведено узагальнене представлення компонентів предметної області, їх функціональної ролі та потенційних ризиків безпеки.

Таблиця 1

Компоненти предметної моделі та їх атрибути безпеки

Компонент	Роль	Атрибути безпеки	CIA	Механізми	Потенційні загрози
Користувач	Взаємодіяз системою	Роль користувача; унікальний ідентифікатор користувача; рівень довіри; вимога багатофакторної автентифікації;	C/I/A	Пароль + багатофакторна автентифікація; керування сесіями; політики доступу на основі ролей/атрибутів;	Несанкціонований доступ, крадіжка облікових даних
Продукт	Опис товару/послуги	Ідентифікатор власника запису; класифікація даних (публічні або внутрішні); дозволені операції редагування;	I/A	Контроль цілісності цін та описів; погодження змін; розмежування прав редагування; моніторинг змін	Несанкціонована зміна інформації про товар, фальсифікація
Замовлення	Транзакційна сутність	Ідентифікатор замовлення; посилання на власника (ідентифікатор покупця);	C/I	Авторизація транзакцій; контроль переходів між статусами; перевірка цілісності сум і валют;	Підробка замовлень, зміна деталей замовлення
Платіжна інформація	Обробка платежів	Рівень конфіденційності (високий); вимога токенізації платіжного номера; ідентифікатор мерчанта;	C/I/A	Шифрування каналу зв'язку; токенізація; шифрування даних у сховищі з керуванням ключами; сегментація відповідно до PCI DSS;	Перехоплення платіжних даних, шахрайство
Інформаційні потоки	Обмін між компонентами	Класифікація потоку (чутливий або нечутливий); наявність та перетин межі довіри;	C/I	Шифрування каналу ; підпис повідомлень; перевірки цілісності; лімітування запитів; контроль витоків на шлюзах	Перехоплення або модифікація даних під час передачі
Політики доступу	Визначення прав доступу	Тип політики (на основі ролей або атрибутів); перелік атрибутів, що використовуються в правилах; порогові значення ризику;	C/I	Централізовані точки прийняття та застосування рішень доступу; принцип найменших привілеїв; періодичний перегляд прав	Ескалація привілеїв, несанкціонований доступ
Служби обробки	Обробка запитів і транзакцій	Клас критичності сервісу; цільові показники відновлення часу та даних; унікальний ідентифікатор сервісу;	A/I	Масштабування; резервування; перевірки працездатності; переривання ланцюга збоїв; моніторинг показників якості	Відмова в обслуговуванні (DoS), збої в обробці

Звернімо увагу, що атрибути безпеки самі по собі нічого не "забезпечують"; вони є даними для прийняття рішень у політиках доступу. Досягнення цілей C/I/A відбувається через поєднання атрибутів, політик та відповідних механізмів/контролів.

Наступним кроком було формування концептуальної моделі, яка дозволяє здійснювати інтеграцію механізмів безпеки та конфіденційності безпосередньо в логічне представлення предметної області. Така інтеграція реалізується через мета-моделювання, що дає змогу описувати додаткові властивості без зміни структури основної моделі [7 – 11]. У запропонованому підході на кожному об'єкті предметної моделі явним чином позначаються цілі захисту (конфіденційність, цілісність, доступність), що визначають очікуваний рівень захищеності даних і операцій [16, 17]. Окремо для суб'єктів, об'єктів та сесій маркуються атрибути безпеки (права доступу, рівні класифікації даних, ідентифікатори, часові обмеження дії дозволів, вимоги до автентифікації), які використовуються політиками доступу для реалізації цих цілей − у підходах RBAC/ABAC у контексті модель-орієнтованої інженерії [13, 20]. Паралельно з цим для кожного об'єкта формується просторово-контекстне уявлення можливих загроз на основі активів системи [14], що дозволяє враховувати не лише саму сутність, але й її функцію в загальній бізнес-логіці системи. Такий підхід відповідає принципу «security by design», оскільки вимоги до захисту включаються безпосередньо на етапі моделювання доменної логіки [9, 16]. Аспекти «privacy by design» застосовуються як складова забезпечення конфіденційності, насамперед у частині обробки персональних даних та відповідності регуляторним вимогам [4, 5, 17].

Запропонована модель детально проілюстрована на рис. 1. На ньому відображено взаємодію доменних об'єктів із компонентами платформи та інтеграцію цілей захисту (C/I/A), атрибутів безпеки, що використовуються політиками доступу (RBAC/ABAC), і релевантних загроз у кожному сегменті моделі [15, 16].

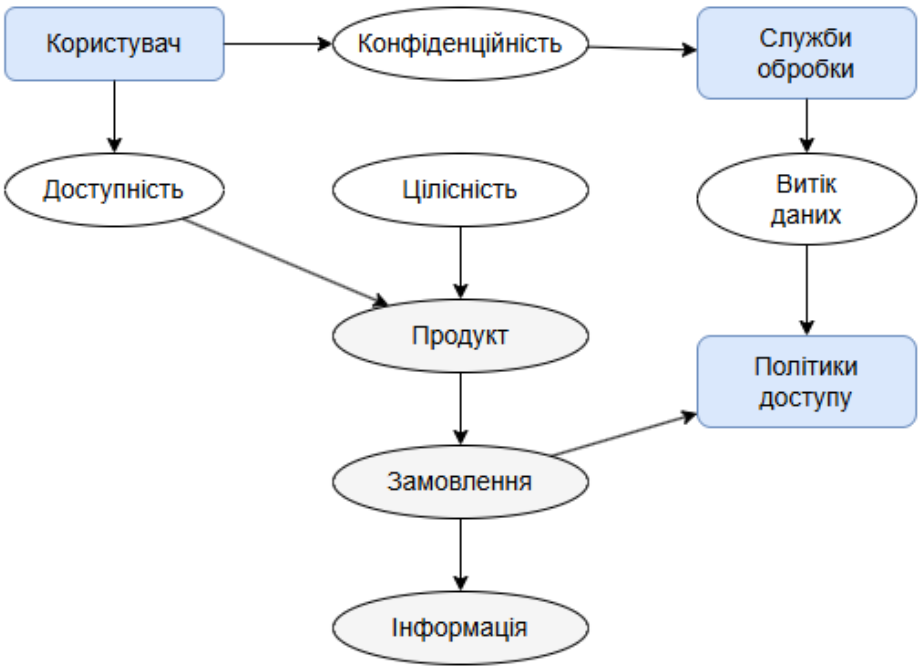

Рис. 1. Схема інтеграції атрибутів безпеки у предметну модель e-commerce системи

Зокрема, на рівні моделі для персональних даних користувача позначається ціль «конфіденційність», після чого встановлюються відповідні атрибути безпеки (клас даних, рівень доступу, вимоги до багатофакторної автентифікації, термін дії токенів). На основі цих атрибутів політики доступу та механізми шифрування застосовуються узгоджено, що зменшує ризик витоків і забезпечує мінімізацію обробки чутливої інформації [2, 3, 4, 16, 17].

Водночас забезпечується постійна доступність критичних функцій системи (перегляд товарів, оформлення замовлень), а атрибут цілісності прикріплюється безпосередньо до об'єктів продукту, контролюючи критично важливі дані, як SKU або ціни товарів [10, 12].

Крім того, визначені загрози, наприклад витік даних під час обробки інформації, тісно пов'язані з належним налаштуванням політик доступу та авторизації, які дозволяють контролювати дії користувачів та мінімізувати ризики [18 – 20]. Політики доступу, інтегровані в логіку моделі, забезпечують відповідний контроль і авторизацію транзакцій, що відповідає сучасним підходам до автоматизованого моделювання загроз і аналізу ризиків [15].

Таким чином, модель чітко відокремлює цілі захисту (C/I/A) від атрибутів безпеки, що керують політиками доступу, і пов'язує їх із конкретними загрозами та механізмами контролю. Це підвищує прозорість архітектурних рішень і забезпечує відтворюваність перевірок відповідності, включаючи автоматизовану валідацію політик та атрибутів; підхід відповідає принципу «security by design» і узгоджується з «privacy by design» у частині обробки персональних даних [16, 17]. Запропонований підхід відповідає сучасним тенденціям програмної інженерії, де вимоги безпеки враховуються ще на етапах моделювання, забезпечуючи вищу стійкість до загроз і кращу відповідність регуляторним стандартам захисту даних [15 – 17].

Приклад застосування

У рамках демонстрації запропонованого підходу до інтеграції безпеки в предметну модель було побудовано логічну структуру типової системи електронної комерції – онлайн-магазину, який охоплює ключові бізнес-процеси, включно з управлінням продуктами, формуванням замовлень, обробкою платежів, контролем доступу та взаємодією з зовнішніми службами. Архітектура системи сформована на основі принципів domain-drivendesign, де кожна функціональна зона представлена окремим доменом, із власною моделлю предметної області, атрибутами й відповідальністю. Це забезпечує логічну ізоляцію компонентів і чітке відображення структури бізнесу в архітектурі програмного забезпечення.

У моделі виділено окремий домен «Користувачі», в межах якого описано загальну сутність користувача з базовими властивостями та ролями, такими як покупець, продавець і адміністратор. Кожна з ролей має розширення функціональності, що реалізується через спадкування. У домені «Каталог» зосереджено опис продуктів, їхніх властивостей, цін, категорій та наявності. Цей контекст пов'язується з модулями кошика та замовлень, які формують транзакційну логіку системи. У домені «Замовлення» відображено створення замовлень, фіксацію деталей покупки, облік статусів і взаємозв'язок з користувачем. Модуль «Платежі» включає платіжну інформацію та інтеграцію з зовнішнім платіжним шлюзом, що відповідає за обробку фінансових даних. Домен «Доступ» містить механізми авторизації, збереження токенів, контроль прав доступу і реалізацію політик для обмеження дій користувачів залежно від їхніх ролей. Окремим сегментом представлено «Зовнішні сервіси», що забезпечують інтеграцію з логістичними компаніями, CRM-системами й ERP-рішеннями.

Архітектурна побудова моделі підпорядковується принципам чистої архітектури. Доменні модулі ізольовані від інфраструктурних залежностей, усі взаємодії між компонентами організовані через явно визначені інтерфейси. Таке проєктування дозволяє масштабувати окремі частини системи без порушення цілісності загальної логіки та спрощує впровадження механізмів безпеки на кожному рівні моделі.

На основі описаної структури створено контекстну діаграму системи, яка ілюструє взаємозв'язки між доменами та ролями користувачів (рис. 2).

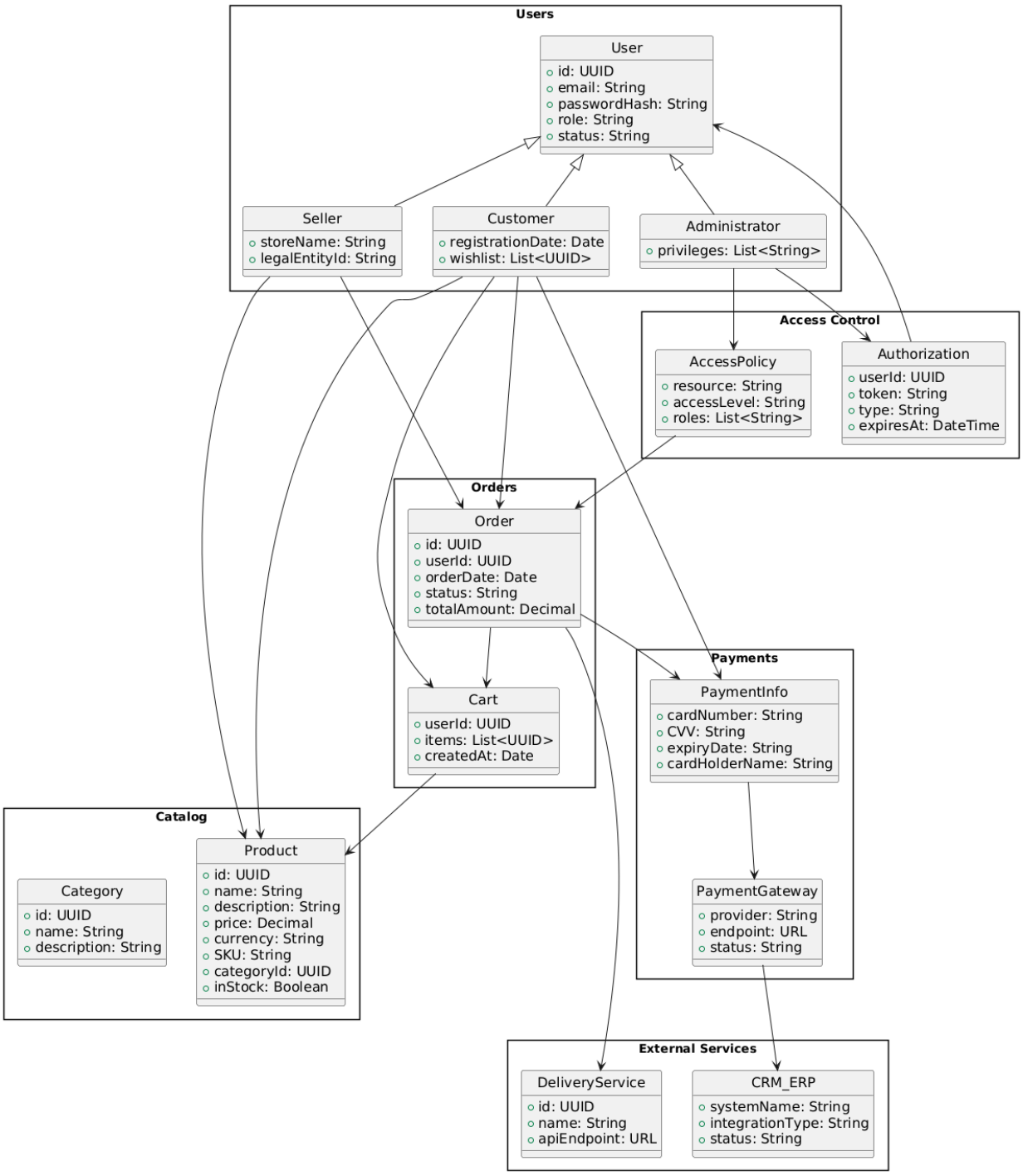

Рис. 2. Контекстна модель онлайн-магазину

У діаграмі представлено, як покупець взаємодіє з кошиком, замовленням, каталогом і платіжною інформацією, продавець має доступ до управління товарами та замовленнями, а адміністратор здійснює контроль доступу через механізми авторизації та політики. Також показано потоки даних між замовленням і службами доставки, а також між платіжним шлюзом і зовнішніми обліковими системами.

Контекстна модель виконує функцію опорної логічної схеми для подальшого вбудовування механізмів безпеки. Вона дозволяє ще на етапі логічного проєктування визначити критичні об'єкти, вузли обміну чутливими даними та ті компоненти, які потребують посиленого захисту. Такий підхід забезпечує реалізацію принципу безпеки за задумом, коли захисні властивості системи формуються не як додатковий етап, а як складова самої архітектури.

У межах цієї моделі кожен домен має чітко визначені межі відповідальності, потоки даних є

контрольованими, а взаємодії між ролями користувачів і системними компонентами можна деталізувати з урахуванням політик доступу, атрибутів безпеки та ризиків, притаманних предметній області електронної комерції. Така побудова є основою для подальшого формального маркування елементів моделі з позиції конфіденційності, цілісності та доступності, а також для моделювання загроз і ризик-орієнтованої оцінки ще до етапу впровадження системи.

Експериментальна оцінка

Мета цього підрозділу − кількісно оцінити ефективність запропонованого підходу інтеграції механізмів інформаційної безпеки у предметну модель шляхом порівняння базового проєкту та проєкту з атрибутивними політиками і позначеними цілями захисту (конфіденційність, цілісність, доступність). Розглядалися дві моделі. Базова модель M0 відтворює предметну модель онлайн-магазину без явного маркування атрибутів безпеки та без формалізованих політик доступу, з мінімальним застосуванням ролей і базовим шифруванням на зовнішніх межах. Модель M1 є тотожною за бізнес-логікою, але містить позначення цілей захисту на об'єктах, маркування атрибутів безпеки для суб'єктів, об'єктів і сесій, політики доступу на основі атрибутів у поєднанні з ролями, а також визначені механізми та контроль (шифрування каналів і сховищ, токенізація платіжних реквізитів, аудит-трейли, контроль станів транзакцій).

Для оцінювання використано три метрики. Перша − кількість критичних об'єктів, тобто об'єктів, для яких принаймні одна з цілей захисту має високий рівень і які перетинають межу довіри або обробляють персональні чи платіжні дані. Друга − кількість високоризикових елементів, визначених за залишковим ризиком R у шкалі [0; 1] як добуток ймовірності та впливу з порогом 0.6; вихідні оцінки отримано за п'ятибальною шкалою з подальшим нормуванням. Третя – інтегральний ризик як зважена сума ризиків елементів із вагами, що відображають критичність активів.

Формалізація розрахунків здійснювалась так. Для кожного елемента (i) оцінювались нормовані значення ймовірності реалізації загрози $\Pr_i \in [0,1]$ та впливу $\text{Impact}_i \in [0,1]$. Залишковий ризик елемента визначався як:

$$R_i = \Pr_i \times \text{Impact}_i. \#(1)$$

Елемент відносився до класу високоризикових, якщо $(R_i \geq T)$, де поріг $(T = 0{,}6)$. Інтегральний ризик системи обчислювався за формулою:

$$R_{\text{total}} = \sum_{i=1}^{N} w_i \cdot R_i \#(2)$$

де w_i − вага критичності активу (вищі значення для персональних і платіжних даних, нижчі − для довідкових сутностей), а N − кількість оцінених елементів.

Процедура передбачала ідентифікацію активів, загроз і меж довіри на контекстній діаграмі та діаграмах потоків даних, формування трійок «актив – загроза – контроль» для кожного елемента, початкову оцінку для M0 та переоцінку для M1 після застосування атрибутивних політик доступу, шифрування на міжсервісних каналах і у сховищі, токенізації чутливих реквізитів, розширеного аудиту та контролю станів транзакцій. Далі обчислено значення метрик для обох моделей та виконано порівняння.

Результати показали зменшення кількості критичних об'єктів з 25 до 15 (−40 %), скорочення високоризикових елементів з 15 до 5 (−67 %) та зниження інтегрального ризику приблизно на 30 % у моделі M1 порівняно з M0. Зниження зумовлене явною класифікацією активів і сегментацією потоків, застосуванням атрибутивних політик і технічних контролів,

що зменшують поверхню атаки та вплив потенційних інцидентів. Оцінювання базується на експертних шкалах і стосується розглянутого сценарію; поширення висновків на інші домени потребує додаткових кейс-досліджень і статистичної перевірки.

Висновки

Запропонований підхід доводить, що інтеграція механізмів інформаційної безпеки з позначенням цілей захисту (конфіденційність, цілісність, доступність) та маркуванням атрибутів безпеки безпосередньо у предметну модель системи електронної комерції забезпечує вимірюване підвищення стійкості. Практичне застосування на прототипі онлайн-магазину дало змогу зменшити кількість критичних об'єктів з 25 до 15 (40 %), скоротити елементи із високим рівнем ризику з 15 до 5 (67 %) та знизити інтегральну оцінку ризику на 30 %. Здобуті результати підтверджують доцільність переходу від «постфактум» впровадження механізмів безпеки до моделювання за принципом «security by design».

Додатковою перевагою методики є її прозорість для бізнес аналітиків: атрибути безпеки маркуються у тій самій моделі, в якій описується домен, що спрощує комунікацію між розробниками й фахівцями з кібербезпеки. Обмеженням роботи є апробація лише на одному сценарії предметної області, тому узагальнені висновки потребують перевірки в інших контекстах, зокрема у фінансах і медицині, де регуляторні вимоги жорсткіші.

Перспективи подальших досліджень охоплюють: автоматизацію маркування на основі правил і шаблонів, розробку інструментів візуальної перевірки коректності атрибутів, а також поєднання статичної оцінки ризику з прогнозними механізмами машинного навчання для динамічного реагування на появу нових загроз

СПИСОК ЛІТЕРАТУРИ

1. Pala N. Domain-Driven Design in E-Commerce: Aligning Business Goals with Technical Solutions. *International Journal of Scientific Research in Computer Science, Engineering and Information Technology*. 2025. Vol. 11, №2. P. 2767–2787. DOI: 10.32628/CSEIT23112579.

2. Nabi F., Tao X., Yong J. Security aspects in modern service component-oriented application logic for social e-commerce systems. *Social Network Analysis and Mining*. 2021. Vol. 11, № 22. DOI: 10.1007/s13278-020-00717-9.

3. Alfadli I. Integrated e-commerce security model for websites. *International Journal of Advanced and Applied Sciences*. 2022. Vol. 9, №4. P. 106–113. DOI: 10.21833/ijaas.2022.04.013.

4. Privacy and Security by Design / I. J. Gedeon et al. *IEEE Consumer Electronics Magazine*. 2020. Vol. 9, №2. P. 76–77. DOI: 10.1109/MCE.2019.2954762.

5. Privacy by Design and Software Engineering: A Systematic Literature Review / V. C. Andrade et al. In: *Proceedings of the 21st Brazilian Symposium on Software Quality (SBQS 2022)*. 2022. DOI: 10.1145/3571473.3571480.

6. Saeed S. A Customer-Centric View of E-Commerce Security and Privacy. *Applied Sciences*. 2023. Vol. 13, №2. P. 1020. DOI: 10.3390/app13021020.

7. Brambilla G., Cabot J., Wimmer M. Model-Driven Software Engineering in Practice. 2nd ed. Place of publication not identified : Morgan & Claypool, 2017. DOI: 10.2200/S00441ED1V01Y201208SWE001.

8. Hafiz M. A collection of privacy design patterns. *In: Proceedings of the 2006 Conference on Pattern Languages of Programs*. 2006. DOI: 10.1145/1415472.1415485.

9. Sabillon E., Cano J., Cavaller V. Security by Design in the Software Development Life Cycle. *Information*. 2019. Vol. 10, №10. P. 318. DOI: 10.3390/info10100318.

10. Idani A., Ledru Y., Vega G. Formal model-driven security combining B-method and process algebra. *Innovations in Systems and Software Engineering*. 2025. V. 21. P. 475–499. DOI: 10.1007/s11334-025-00611-7.

11. Abdmeziem F., Boukhedouma S., Oussalah M. C. On the Data Security of Information Systems: Comparison of Approaches and Challenges. *In: Computational Science and Its Applications – ICCSA 2021. Lecture Notes in Computer Science.* 2021.Vol. 12953. Springer. P. 162–177. DOI: 10.1007/978-3-030-86970-0_18.

12. Shaked A. A Model-Based Methodology to Support Systems Security Design and Assessment. *Journal of Industrial Information Integration.* 2023. Vol. 33. P. 100465. DOI: 10.1016/j.jii.2023.100465.

13. Development of Metamodel for Information Security Risk Management / M. Salem et al. *In: Kids Cybersecurity Using Computational Intelligence Techniques. Studies in Computational Intelligence*. 2023. Vol. 1080. Springer. P. 243–253. DOI: 10.1007/978-3-031-21199-7_17.

14. Asset-Oriented Threat Modeling / N. Messe et al. *In: Proceedings of the IEEE International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom)*. 2020. P. 491–501. DOI: 10.1109/TrustCom50675.2020.00073.

15. Automated Threat Modelling and Risk Analysis in E-Government Using BPMN / D. Granata et al. *Connection Science*. 2023. Vol. 35, №1. DOI: 10.1080/09540091.2023.2284645.
16. de Kinderen S., Kaczmarek-Heß M., Hacks S. A Multi-level Reference Model and a Dedicated Method for Cyber-Security by Design. *Business & Information Systems Engineering*. 2024. V. 67. P. 511–530. DOI: 10.1007/s12599-024-00899-y.
17. Drev M., Delak B. Conceptual Model of Privacy by Design. *Journal of Computer Information Systems*. 2022. Vol. 62, №5. P. 888–895. DOI: 10.1080/08874417.2021.1939197.
18. Al-Hawari F. Software design patterns for data management features in web-based information systems. *Journal of King Saud University – Computer and Information Sciences*. 2022. Vol. 34. P. 10028–10043. DOI: 10.1016/j.jksuci.2022.10.003.
19. Ehikioya S. A., Guillemot E. A critical assessment of the design issues in e-commerce systems development. *Engineering Reports*. 2020. Vol. 2, №4. P. e12155. DOI: 10.1002/eng2.12155.
20. Proper H. A., Guizzardi G. Understanding the variety of domain models: views, programs, animations, and other models. *SN Computer Science*. 2024. Vol. 5. Art. №861. DOI: 10.1007/s42979-024-03163-y.

Стаття надійшла до редакції 11.12.2025.
Стаття пройшла рецензування 18.12.2025.

Московко Сергій Геннадійович – аспірант, факультет інтелектуальних інформаційних технологій та автоматизації, e-mail: cakedispensers@gmail.com.

Квєтний Роман Наумович – д-р техн. наук, професор кафедри автоматизації та інтелектуальних інформаційних технологій, факультет інтелектуальних інформаційних технологій та автоматизації, e-mail: rkvetny@vntu.edu.ua.
Вінницький національний технічний університет.