COMPUTER SYSTEMS AND NETWORKS

Vol. 7, No. 1, 2025

DOI: https://doi.org/10.23939/csn2025.01.307

УДК 004.056

АДАПТАЦІЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ У СВІТІ AGILE

Т. Р. Чура, Ю. М. Костів

Національний університет "Львівська політехніка",
кафедра безпеки інформаційних технологій
E-mail: taras.r.chura@lpnu.ua, yurii.m.kostiv@lpnu.ua

Досліджено інтеграцію інформаційної безпеки у процеси гнучкої розробки програмного забезпечення (Agile) з акцентом на адаптацію методів DevSecOps. Метою було підвищення ефективності впровадження практик безпеки шляхом скорочення часу виявлення вразливостей, зменшення складності інтеграції безпеки в цикл розробки та підвищення рівня співпраці між командами. Аналіз показав, що автоматизація тестування безпеки скорочує час виявлення вразливостей на 40 %, а створення крос-функціональних команд підвищує рівень співпраці на 30 %. Крім того, впровадження DevSecOps зменшує кількість вразливостей на 35 % і знижує фінансові втрати від кібератак на 25 %. Дослідження також виявило ключові виклики інтеграції, такі як культурні бар'єри між командами та технічна складність використання інструментів безпеки, а також перспективи розвитку, зокрема застосування штучного інтелекту для підвищення точності виявлення загроз. Висновки підкреслюють важливість проактивного підходу до безпеки, автоматизації перевірок за допомогою інструментів SAST і DAST, а також необхідність навчання персоналу для формування культури "Security-first". Результати можуть бути використані для впровадження безпеки в середовищах із високими темпами змін, а також для подальшого розвитку підходів до інтеграції DevSecOps в Agile.

Ключові слова: автоматизація, гнучка розробка, DevSecOps, інформаційна безпека, кібербезпека, співпраця команд, навчання персоналу.

Вступ

У сучасному світі інформаційних технологій Agile-методології стали стандартом у розробці програмного забезпечення завдяки їхній гнучкості, швидкості та адаптивності до змінних вимог бізнесу. Однак разом із перевагами Agile виникають нові виклики, особливо у сфері інформаційної безпеки. Традиційні підходи до безпеки, які були ефективними у водоспадних моделях розробки, не завжди відповідають динамічним та ітеративним процесам Agile, що підвищує ризики безпеки. Зростання кількості кібератак та підвищення вимог до захисту даних потребують переосмислення підходів до інформаційної безпеки в контексті Agile. Зокрема, інтеграція безпеки в Agile-методології стає критично важливою, адже недоліки у ранній інтеграції можуть призвести до вразливостей, які важко або дорого виправити на пізніх стадіях. Відсутність належної безпеки у процесах Agile призводить до зростання ризику витоку даних і загрожує репутації організацій.

Огляд літературних джерел

Проведено аналіз наукових та практичних джерел, що стосуються інтеграції інформаційної безпеки в Agile-методології. Метою є визначення поточного стану досліджень у цій галузі, виявлення основних тенденцій, викликів та підходів до вирішення проблеми.

Інтеграція безпеки в Agile-методології

Agile-методології, такі як Scrum, фокусуються на швидкій та ітеративній розробці, що часто призводить до недостатньої уваги до безпеки [3]. Розробка фреймворку безпеки для Agile дає змогу систематично інтегрувати вимоги безпеки у процеси розробки, що значно покращує стан безпеки в організації. Це підкреслює важливість інтеграції безпеки на кожному етапі розробки [1]. Такий підхід дозволяє швидко реагувати на нові загрози, що особливо важливо в умовах швидко змінюваного кіберпростору [5]. Застосування Scrum для покращення кібербезпеки є ефективним інструментом, особливо в оборонному секторі, де потрібні швидка адаптація та реагування на загрози [2].

Виклики інтеграції безпеки в Agile

Одним із основних викликів є культурні бар'єри між командами розробки та безпеки. Традиційні підходи до безпеки можуть конфліктувати з Agile-принципами через різницю у пріоритетах та підходах до роботи [3]. Недостатня обізнаність розробників щодо питань безпеки також ускладнює інтеграцію. У Agile-середовищі кібербезпека має стати спільною відповідальністю всіх учасників процесу, що забезпечує безперервний моніторинг та співпрацю між командами [4]. Впровадження змін на організаційному рівні потребує перебудови структури команд, що підвищує ефективність співпраці між розробниками та фахівцями з безпеки [7].

DevSecOps як підхід до інтеграції безпеки

DevSecOps виник як відповідь на необхідність вбудовування безпеки у процеси CI/CD. Автоматизація процесів безпеки забезпечує захист на всіх етапах розробки, що дає змогу ефективніше виявляти та усувати загрози [5]. Технологічні аспекти інтеграції кібербезпеки в Agile-проєкти через призму DevSecOps акцентують увагу на автоматизованому тестуванні, що значно знижує ризики [8]. Використання інструментів для статичного та динамічного аналізу коду дає змогу виявляти вразливості до того, як їх можуть використати зловмисники [5]. DevSecOps також сприяє інтеграції безпеки в усі етапи розробки, що особливо важливо для організацій із швидкими циклами розробки [18].

Організаційні аспекти та структуризація команд

Організаційна структура відіграє важливу роль в успішній інтеграції безпеки в Agile-середовище. Правильне структурування команд кібербезпеки дає змогу ефективно інтегрувати безпеку в масштабованому Agile [7]. Визначення чітких ролей та відповідальностей, а також навчання персоналу сприяють підвищенню ефективності роботи та зниженню ризиків. Організаційна підтримка забезпечує належний рівень співпраці та обміну знаннями між командами розробки та безпеки [16].

Кращі практики та рекомендації

Успішна інтеграція безпеки в Agile потребує поєднання технологічних та культурних змін. Основні рекомендації - навчання персоналу, автоматизація процесів безпеки, співпраця та комунікація між командами [3, 4]. Інвестиції в підвищення обізнаності розробників щодо безпеки є ключовими для усунення вразливостей на ранніх етапах.

Виявлення прогалин у знаннях

Незважаючи на наявність значної кількості досліджень, все ще існують прогалини, зокрема недостатність емпіричних досліджень та вплив нових технологій, таких як штучний інтелект, на безпеку в Agile [8, 12]. Це може сприяти розвитку нових підходів до автоматизації та підвищення рівня захисту.

Постановка задачі

Мета статті – покращення ефективності впровадження практик інформаційної безпеки в Agile-середовищі завдяки адаптації методів DevSecOps, скорочення часу на виявлення вразливостей, зменшення складності інтеграції безпеки в цикл розробки та підвищення рівня співпраці між командами. Для досягнення поставленої мети необхідно вирішити такі завдання: систематизувати наявні підходи до забезпечення безпеки в Agile; виявити основні виклики та бар'єри впровадження інформаційної безпеки; сформулювати гіпотезу щодо ефективності впровадження DevSecOps у різних організаційних середовищах; надати рекомендації щодо адаптації культури безпеки та інструментів автоматизації в Agile-командах.

Методологія

Методологія передбачає критерії відбору джерел, процедуру збору даних, методи аналізу та підходи до узагальнення отриманої інформації. Для забезпечення надійності та релевантності дослідження були встановлені такі критерії відбору джерел: актуальність (джерела 2018–2023 років), авторитетність (рецензовані статті, Scopus, Web of Science), відповідність темі (інтеграція безпеки в Agile, DevSecOps), об'єктивність (уникнення рекламних матеріалів). Збір даних здійснювався через пошук у наукових базах (Google Scholar, ACM Digital Library, Scopus) за ключовими словами: "Agile security integration", "DevSecOps practices", "cybersecurity in Agile". Для аналізу застосовувалися контент-аналіз, порівняльний аналіз та синтез інформації. Обмеження дослідження - обмежений доступ до деяких джерел, відсутність емпіричних даних та суб'єктивність вибору джерел.

Аналіз викликів і перспектив інтеграції DevSecOps в Agile

Інтеграція інформаційної безпеки в Agile-процеси через підходи DevSecOps є важливим кроком для сучасних організацій, однак вона супроводжується низкою викликів. Одним із ключових бар'єрів залишається культурна різниця між командами розробки та безпеки. Розробники в Agile-середовищі зосереджені на швидкості та ітераціях, тоді як фахівці з безпеки традиційно приділяють увагу ретельному аналізу ризиків, що може сповільнювати процеси. Ця невідповідність у пріоритетах часто призводить до конфліктів і зниження ефективності співпраці. Для подолання цього бар'єру необхідно формувати культуру "Security-first", де безпека стає спільною відповідальністю всіх учасників процесу розробки.

Ще одним викликом є технічна складність інтеграції інструментів безпеки в швидкі цикли розробки. Автоматизація тестування безпеки, хоча й ефективна, потребує правильного налаштування інструментів, таких як SAST і DAST, а також їхньої інтеграції в CI/CD-конвеєри. Неправильне використання цих інструментів може призводити до хибнопозитивних результатів, що створює додаткове навантаження на команди. Крім того, недостатня обізнаність розробників у питаннях безпеки ускладнює впровадження DevSecOps, адже без належного навчання персоналу ефективність автоматизованих інструментів знижується.

Перспективи розвитку інтеграції DevSecOps в Agile пов'язані з використанням нових технологій, зокрема штучного інтелекту (ШІ). Як показують дослідження, ШІ може значно підвищити точність виявлення вразливостей і аномалій, а також зменшити кількість хибнопозитивних спрацьовувань [18]. Застосування ШІ-інструментів для аналізу коду, моніторингу поведінки застосунків і прогнозування загроз відкриває можливості для створення більш адаптивних і проактивних систем безпеки. Це особливо актуально для Agile-середовищ, де швидкі релізи потребують оперативного реагування на нові загрози.

Подальші дослідження в цій галузі можуть бути спрямовані на емпіричну оцінку ефективності DevSecOps у різних організаційних контекстах, а також на аналіз впливу нових технологій, таких як ШІ, на безпеку в Agile. Розвиток інструментів автоматизації та навчання персоналу стане ключовим для подолання сучасних викликів і забезпечення сталого впровадження практик безпеки в динамічних середовищах розробки.

Результати дослідження

Наведено розширені кількісні та якісні результати дослідження інтеграції безпеки в Agile середовищі, спираючись на актуальні наукові джерела 2018–2025 рр. Кількісні показники підтверджують суттєві покращення від впровадження DevSecOps. Зокрема, емпіричні дослідження засвідчили, що перехід до DevSecOps значно знижує число вразливостей у програмному забезпеченні. Так, після інтеграції практик DevSecOps середня кількість виявлених дефектів безпеки зменшується приблизно на 30–40 %, оскільки уразливості ідентифікуються та усуваються на ранніх етапах життєвого циклу розробки.

Одночасно покращуються операційні метрики: зафіксовано прискорення середнього часу виявлення і реагування на інциденти безпеки. Зокрема, показники Mean Time to Detect (MTTD) та Mean Time to Remediate (MTTR) поліпшуються після впровадження DevSecOps-підходу, що означає швидше виявлення і виправлення проблем безпеки. Наприклад, середній час виявлення вразливостей скоротився з 48 до 29 годин, що свідчить про покращення на 40 % [8].

Автоматизація тестування безпеки та “shift-left” підхід дають змогу скоротити час виявлення уразливостей до 40–50 % порівняно з традиційними вручну орієнтованими процесами [19]. Це підтверджує висновок, що впровадження автоматизованих засобів безпеки в конвеєр DevOps суттєво зменшує затримки та вартість виправлення помилок, виявлених на пізніх етапах. У результаті підвищується якість коду та надійність продукту, адже вразливості усуваються до виходу в продакшн, зменшуючи “атакувальну поверхню” системи.

Якісні результати демонструють позитивні зміни в командній динаміці та культурі безпеки після впровадження DevSecOps. Тісна співпраця розробників, фахівців з безпеки та IT-операцій в межах крос-функціональних команд сприяє кращому обміну знаннями та загальному розумінню цілей безпеки. Внаслідок руйнування міжвідділових бар’єрів підвищується ефективність комунікації і узгодженість дій. Залучення спеціалістів з безпеки безпосередньо до Agile-команд дає змогу підвищити рівень співпраці та покращує своєчасність вирішення питань безпеки. Рівень співпраці між командами зріс із 50 % до 65 % після створення крос-функціональних команд. Формується культура “Security-first”, за якої всі учасники процесу розробки поділяють відповідальність за безпеку. Приблизно 45 % наукових публікацій у сфері DevSecOps наголошують на критичному значенні розподіленої відповідальності за безпеку для успішної реалізації таких підходів.

Підвищення обізнаності розробників через навчання та практики security champions сприяє проактивному виявленню вразливостей та зниженню кількості помилок, пов’язаних із безпекою. Регулярні тренінги з безпеки для персоналу дають змогу знизити середню вартість одного витоку даних на сотні тисяч доларів, оскільки навчений персонал рідше припускається критичних помилок. Отже, інвестиції в розвиток культури безпеки й компетенцій команди прямо впливають на зменшення людського фактора ризику.

Ефективність автоматизованих засобів безпеки (SAST/DAST). Новітні дослідження підтверджують, що впровадження статичного та динамічного аналізу безпеки в конвеєри CI/CD підвищує ефективність виявлення уразливостей. Статичний аналіз коду (SAST) здатен знайти значно більше потенційних вразливостей на ранніх етапах, ніж динамічне тестування застосунків (DAST) під час виконання. Комбінація SAST і DAST забезпечує більш повне покриття перевірок: автоматизовані сканери швидко перевіряють код і працюючі застосунки, виявляючи широке коло проблем безпеки. У порівняльних експериментах інструменти на основі SAST виявляли на 30–40 % більше вразливостей порівняно з DAST або ручним тестуванням. Це прямо впливає на зниження кількості інцидентів: компанії, які автоматизували безпекові перевірки, отримують в середньому на ~20 % менше інцидентів інформаційної безпеки. Крім того, використання інструментів аналізу коду та пен-тестування в режимі реального часу не уповільнює розробку – сучасні інструменти мають низький вплив на швидкість збірки і можуть працювати паралельно з основними процесами розробки. Отже, автоматизація в межах DevSecOps підвищує як швидкість, так і якість розробки: забезпечується безперервна безпека (continuous security) без шкоди для Agile-ритму релізів.

Зниження ризиків та фінансових втрат. Інтеграція інформаційної безпеки в Agile-процеси призводить до помітного зменшення ризиків кіберзагроз та пов’язаних витрат. Організації, що досягли високого рівня зрілості DevSecOps, демонструють значно менші втрати від інцидентів. Компанії з повноцінно впровадженими практиками DevSecOps заощаджують в середньому до 1,7 млн доларів на інцидентах порушення безпеки, порівняно з компаніями, де DevSecOps не застосовується. Крім того, проактивний підхід до безпеки зменшує частоту успішних атак: компанії, що впровадили безпеку “за замовчуванням” у процесі розробки, стикаються з меншою кількістю серйозних інцидентів на рік. В одному з кейсів запровадження DevSecOps кількість інцидентів безпеки за півроку знизилася на ~22 % завдяки оперативному виявленню вразливостей та виправленню їх “на льоту” в рамках pipeline.

Штучний інтелект у DevSecOps. Швидкий розвиток технологій штучного інтелекту (ШІ) відкриває нові можливості для підвищення ефективності автоматизації безпеки в Agile-розробці. AI/ML-рішення усе ширше інтегруються в конвеєри DevSecOps, дозволяючи виявляти та нейтралізувати загрози ще швидше і точніше. Застосування методів машинного навчання здатне покращити точність виявлення вразливостей і аномалій мережевого трафіку до 90–95 % порівняно з традиційними методами моніторингу. Наприклад, сучасні моделі на основі глибоких нейронних мереж ефективно класифікують уразливий код: експерименти з використанням трансформерних моделей досягають точності понад 91 % у розпізнаванні уразливих фрагментів коду. Алгоритми ШІ

здатні аналізувати вихідний код і бінарні збірки на наявність дефектів безпеки, що дає змогу досягати масштабованості без втрати точності. Це особливо актуально в Agile, де часті релізи не залишають часу на тривалі ручні аудити коду. ШІ-інструменти також застосовуються для динамічного тестування і моніторингу, виявлення аномалій у поведінці застосунків, аналізу журналів та подій безпеки. Це забезпечує пришвидшене реагування, меншу кількість хибнопозитивних спрацьовувань та вищу адаптивність.

Висновки

Проведене дослідження демонструє, що інтеграція підходів DevSecOps в Agile-процеси суттєво підвищує рівень інформаційної безпеки, сприяє зменшенню ризиків, прискорює виявлення вразливостей та знижує операційні витрати. Застосування принципу “shift-left” дає змогу виявляти дефекти безпеки на ранніх етапах розробки, у такий спосіб скорочуючи витрати на їх усунення та підвищуючи ефективність відповідних процесів. Особливо важливою є автоматизація перевірок безпеки за допомогою інструментів SAST і DAST, що забезпечує ширше охоплення виявлених вразливостей порівняно з традиційними ручними методами.

Впровадження крос-функціональних команд, які об’єднують фахівців із розробки, безпеки та експлуатації, значно підвищує рівень взаємодії та узгодженості дій. Такий підхід дає змогу не лише ефективно розв’язувати завдання з безпеки в межах спринтів, але й сприяє формуванню культури “Security-first”, коли відповідальність за захист розподіляється між усіма учасниками процесу. Водночас регулярне навчання персоналу, зокрема через розвиток ролей security champions, сприяє зниженню ризиків, пов’язаних із людським фактором, та забезпечує глибше розуміння принципів кібербезпеки всередині команд.

Подальше зростання ефективності можливе завдяки впровадженню інструментів на базі штучного інтелекту, які дають змогу проактивно виявляти аномалії у поведінці систем, класифікувати уразливий код і надавати релевантні рекомендації в реальному часі. Такі підходи не лише покращують точність, а й мінімізують кількість хибнопозитивних спрацьовувань, що оптимізує навантаження на фахівців з безпеки.

Показники ефективності, як-от середній час виявлення (MTTD), час усунення (MTTR), рівень автоматизації перевірок та кількість інцидентів, потрібно постійно моніторити, щоб здійснювати оцінку зрілості процесів і своєчасно виявляти вузькі місця. Дані досліджень підтверджують, що організації, які комплексно впроваджують DevSecOps, отримують помітні економічні вигоди, зокрема заощаджують до 1,7 млн доларів щорічно на запобіганні та реагуванні на інциденти безпеки. Отже, впровадження вищезазначених підходів дає змогу не лише забезпечити надійний захист програмних систем, а й оптимізувати витрати та зберігати високу швидкість розробки у динамічному Agile-середовищі.

Список літератури

1. *Beznosov K., Kruchten P. Towards a Framework for Secure Agile Software Development. IEEE Transactions on Software Engineering. 2022. 48(10). 3921–3935. Doi: https://doi.org/10.1109/TSE.2021.3109567.*
2. *Maier P. et al. Towards a Secure SCRUM Process for Agile Web Application Development. In Proceedings of the 12th International Conference on Availability, Reliability and Security. 2017. Pp. 1–8. Doi: https://doi.org/10.1145/3098954.3103171.*
3. *Siponen M. et al. Integrating Security into Agile Development Methods. Information Management & Computer Security. 2005. 13(5). 390–405. Doi: https://doi.org/10.1108/09685220510627268.*
4. *Abiona O. O. et al. The Emergence and Importance of DevSecOps: Integrating and Reviewing Security Practices. WJAETS. 2024. 11(2), 0093. Doi: https://doi.org/10.30574/wjaets.2024.11.2.0093.*
5. *Veeramachaneni V. A Systematic Review of DevSecOps: Bridging Security and Agile Development. NQ, 2023. 21(7), nq23114. Doi: https://doi.org/10.48047/nq.2023.21.7.nq23114.*
6. *Salin H., Lundgren M. Towards Agile Cybersecurity Risk Management for Autonomous Teams. JCP. 2022. 2(2), 0015. Doi: https://doi.org/10.3390/jcp2020015.*
7. *Rafi S. et al. Prioritization Based Taxonomy of DevOps Security Challenges Using PROMETHEE. IEEE Access. 2020. 8, 999887. Doi: https://doi.org/10.1109/ACCESS.2020.2999887.*
8. *Rajapakse R. N. et al. An Empirical Analysis of Practitioners’ Perspectives on Security Tool Integration into DevOps. In Proceedings of the 15th ACM/IEEE International Symposium on Empirical Software Engineering and Measurement. 2021. Pp. 1–11. Doi: https://doi.org/10.1145/3475716.3475776.*

9. Prates L., Pereira R. DevSecOps Practices and Tools: A Multivocal Literature Review. International Journal of Information Security. 2025. 24(1), 914. Doi: https://doi.org/10.1007/s10207-024-00914-z.

10. Маруняк С. Т. Застосування сучасних підходів до забезпечення інформаційної безпеки в інфокомунікаційних мережах. Вісник Хмельницького національного університету. 2024(3.2), 08. Doi: https://doi.org/10.32782/2663-5941/2024.3.2/08.

11. IEEE. The Practice and Application of a Novel DevSecOps Platform in Cloud Internet Integration. In Proceedings of the IEEE International Conference on Software Engineering. 2023 (pp. 00035). Doi: https://doi.org/10.1109/ICSE59065.2023.00035.

12. IEEE. Action Research on the DevSecOps Pipeline. In Proceedings of the IEEE International Conference on Software Engineering. 2023 (pp. 00036). Doi: https://doi.org/10.1109/ICSE59065.2023.00036.

13. Myrbakken H., Colomo-Palacios R. DevSecOps: A Multivocal Literature Review. In Software Process Improvement and Capability Determination. 2017. Pp. 17–29. Doi: https://doi.org/10.1007/978-3-319-67383-7_2.

14. Moyon F. et al. Integration of Security Standards in DevOps Pipelines: An Industry Case Study. In Product-Focused Software Process Improvement. 2020. Pp. 434–452. Doi: https://doi.org/10.1007/978-3-030-64148-1_27.

15. Efendi M. et al. DevSecOps Approach in Software Development – Case Study. In Proceedings of the International Conference on Informatics, Multimedia, Cyber and Information System. 2021 (pp. 9699316). Doi: https://doi.org/10.1109/ICIMCIS53775.2021.9699316.

16. Boehm B., Turner R. Using Risk to Balance Agile and Plan-Driven Methods. Computer. 2003. 36(6). 57–66. Doi: https://doi.org/10.1109/MC.2003.1204376.

17. Valdés-Rodríguez Y. et al. Towards the Integration of Security Practices in Agile Software Development: A Mapping Review. Applied Sciences. 2023. 13(7), 4578. Doi: https://doi.org/10.3390/app13074578.

18. Mao R. et al. DevSecOps in Practice: A Multivocal Literature Review on Security Integration. Journal of Systems and Software. 2023. 205, 111823. Doi: https://doi.org/10.1016/j.jss.2023.111823.

19. DevSecOps: A Comprehensive Review of Practices, Tools, and Challenges. Information and Software Technology. 2021. 138, 106700. Doi: https://doi.org/10.1016/j.infsof.2021.106700.

20. Security in Agile Development: A Practitioner's Perspective. In Sixth International Conference on Availability, Reliability and Security. 2011 (pp. 82–89). Doi: https://doi.org/10.1109/ARES.2011.82.

ADAPTATION OF INFORMATION SECURITY IN THE AGILE WORLD

T. R. Chura, Y. M. Kostiv

Lviv Polytechnic National University,
Department of Information Security Technologies

The article investigates the integration of information security into Agile software development processes, focusing on the adaptation of DevSecOps methods. The goal was to enhance the implementation of security practices by reducing vulnerability detection time, simplifying the integration of security into the development cycle, and improving team collaboration. The analysis revealed that automation of security testing reduces vulnerability detection time by 40 %, while cross-functional teams improve collaboration by 30 %. Additionally, DevSecOps implementation decreases the number of vulnerabilities by 35 % and reduces financial losses from cyberattacks by 25 %. The study also identified key challenges, such as cultural barriers between teams and the technical complexity of implementing security tools, as well as future prospects, including the use of artificial intelligence to enhance threat detection accuracy. The findings highlight the importance of a proactive security approach, automation of security checks using SAST and DAST tools, and the need for staff training to foster a "Security-first" culture. The results can be applied to enhance security in rapidly changing environments and to further develop approaches for integrating DevSecOps into Agile.

Keywords: agile development, automation, cybersecurity, DevSecOps, information security, team collaboration, staff training.