Методологія забезпечення цілісності та доступності версій CRM-системи Salesforce

Златоус Святослав[1], Петро Венгерський[2]

[1,2] *Ivan Franko National University of Lviv, Universytetska 1, 79000 Lviv, Ukraine*

Аннотація

Дане дослідження представляє інноваційний підхід до забезпечення кібербезпеки Salesforce CRM через впровадження спеціалізованого інструменту FlowVersionComparer для систематичного контролю версій Flow-процесів. Застосунок дозволяє детально порівнювати різні версії Flow, візуалізувати зміни та ідентифікувати потенційно небезпечні модифікації, що можуть загрожувати цілісності та доступності корпоративних даних

Keywords

Salesforce, CRM, контроль версій, декларативні інструменти автоматизації, Flow

1. Вступ

Сучасні CRM-системи стали критично важливою складовою інформаційної інфраструктури організацій, обробляючи величезні масиви конфіденційних даних клієнтів та бізнес-процесів. Salesforce, як провідна хмарна CRM-платформа, надає потужні інструменти автоматизації через Flow Builder [1] - декларативний інструмент для створення бізнес-логіки без програмування. Проте динамічна природа Flow-процесів створює унікальні виклики для забезпечення кібербезпеки, зокрема в аспектах контролю змін та аудиту модифікацій критичної бізнес-логіки.

Метою даного дослідження є аналіз ефективності застосування спеціалізованого інструменту FlowVersionComparer для забезпечення кібербезпеки CRM-системи Salesforce через механізми контролю версій Flow-процесів. Основна гіпотеза дослідження полягає в тому, що систематичний контроль версій Flow-процесів через спеціалізовані інструменти порівняння значно підвищує рівень кібербезпеки CRM-системи, забезпечуючи цілісність та доступність критичної бізнес-інформації.

Основною метою дослідження є розробка та валідація методології використання інструменту FlowVersionComparer для підвищення рівня кібербезпеки Salesforce CRM через забезпечення прозорості змін у бізнес-логіці системи.

Ключові завдання дослідження включають: аналіз вразливостей, пов'язаних з неконтрольованими змінами Flow-процесів; оцінку ефективності FlowVersionComparer у виявленні потенційно небезпечних модифікацій; розробку методології інтеграції контролю версій у процеси забезпечення кібербезпеки; валідацію впливу систематичного контролю версій на показники цілісності та доступності даних.[35]

На сьогодні в науковій літературі відсутні дослідження, які б систематично аналізували еволюцію версій Salesforce Flow з позицій забезпечення цілісності та доступності інформації.

[34] Corresponding authors

sviatoslav.zlatous@lnu.edu.ua (С. Златоус); petro.venherskyy@lnu.edu.ua (П. Венгерський)

0009-0007-1834-2796 (С. Златоус); 0000-0001-9808-7404 (П. Венгерський)

[35]

Незважаючи на широке використання платформи Salesforce у корпоративному середовищі та критичну важливість автоматизованих бізнес-процесів для функціонування сучасних організацій, питання впливу версійних змін на збереження даних та їх доступність для різних груп користувачів залишається недостатньо вивченим. Існуючі публікації переважно зосереджуються на технічних аспектах імплементації Flow [2] або загальних практиках розробки [3] [4], тоді як проблематика інформаційної цілісності в контексті міграції між версіями та управління життєвим циклом автоматизованих процесів [5] не отримала належного наукового осмислення. Це створює суттєву прогалину в розумінні ризиків, пов'язаних з оновленням платформи, та відсутність науково обґрунтованих методологій оцінки впливу версійних змін на критичні інформаційні активи підприємства

2. Методологія

Дослідження базувалося на комбінованому підході, що поєднує якісний та кількісний аналіз. Методологія включала чотири основні етапи:

Перший етап передбачав розгортання тестового середовища Salesforce з імплементацією FlowVersionComparer та створенням набору з 50 критичних Flow-процесів, що моделюють типові бізнес-сценарії обробки конфіденційних даних. На другому етапі проводилася симуляція різних сценаріїв модифікації Flow-процесів, включаючи легітимні зміни, помилкові конфігурації та потенційно зловмисні модифікації. Загалом було змодельовано 200 сценаріїв змін протягом 30-денного періоду.

Третій етап включав систематичний аналіз змін через FlowVersionComparer з документуванням часу виявлення, точності ідентифікації критичних змін та повноти відображення модифікацій. Четвертий етап передбачав порівняльний аналіз показників безпеки в контрольній групі (без використання інструменту) та експериментальній групі з активним використанням FlowVersionComparer.

Для оцінки ефективності використовувалися метрики: час виявлення неавторизованих змін (MTTD - Mean Time to Detect), коефіцієнт виявлення критичних змін (CDR - Critical Detection Rate), показник хибнопозитивних спрацювань (FPR - False Positive Rate), індекс цілісності бізнес-логіки (BLI - Business Logic Integrity Index).

2.1. Результати дослідження

Впровадження FlowVersionComparer продемонструвало значне покращення ключових показників кібербезпеки CRM-системи. Аналіз результатів виявив кілька критично важливих тенденцій.

2.1.1. Забезпечення цілісності інформації

FlowVersionComparer ефективно виявляв несанкціоновані зміни в бізнес-логіці, що могли призвести до порушення цілісності даних. Інструмент ідентифікував 96% критичних змін, включаючи модифікації умов доступу до записів, зміни в логіці валідації даних та неавторизовані оновлення правил обробки конфіденційної інформації. Середній час виявлення критичних змін скоротився з 72 годин до 4 годин, що суттєво зменшило вікно вразливості системи.

Особливо ефективним виявилося виявлення "схованих" змін - модифікацій, які не відображаються в стандартних логах аудиту Salesforce. FlowVersionComparer ідентифікував 23 випадки таких змін, включаючи модифікації умов розгалуження, які могли призвести до

несанкціонованого витоку даних. Візуалізація різниці між версіями дозволила адміністраторам безпеки швидко оцінити потенційний вплив змін на цілісність системи.

2.1.2. Підвищення доступності системи

Контроль версій через FlowVersionComparer значно покращив показники доступності системи. Інструмент дозволив виявити та попередити 18 потенційних інцидентів, пов'язаних з некоректними змінами Flow, які могли призвести до збоїв у критичних бізнес-процесах. Середній час відновлення після інцидентів (MTTR) скоротився на 65% завдяки можливості швидкого порівняння та відкату до попередніх робочих версій.

Функція детального порівняння дозволила ідентифікувати конфлікти між різними Flow-процесами, що могли призвести до deadlock-ситуацій. В експериментальній групі кількість інцидентів недоступності, пов'язаних з Flow, зменшилася на 78% порівняно з контрольною групою.

2.1.3. Покращення процесів аудиту та compliance

FlowVersionComparer створив повний аудиторський слід для всіх змін у Flow-процесах, що критично важливо для відповідності регуляторним вимогам. Інструмент автоматично документував не лише факт зміни, але й детальну інформацію про модифіковані елементи, умови та дії. Це дозволило скоротити час проведення аудиторських перевірок на 40% та підвищити їх точність.

Система виявила 12 випадків порушень політик безпеки, включаючи спроби обходу механізмів авторизації через модифікацію Flow-логіки. В усіх випадках порушення були виявлені протягом першої доби після внесення змін, що дозволило запобігти потенційним інцидентам безпеки.

3. Висновки

Проведене дослідження переконливо підтверджує висунуту гіпотезу про критичну роль систематичного контролю версій Flow-процесів у забезпеченні кібербезпеки Salesforce CRM. FlowVersionComparer продемонстрував високу ефективність як інструмент забезпечення цілісності та доступності інформації в CRM-системі.

Ключові висновки дослідження свідчать, що впровадження спеціалізованого інструменту контролю версій Flow знижує ризики кібербезпеки на 73%, скорочує час виявлення критичних змін у 18 разів та підвищує загальний рівень цілісності бізнес-логіки системи на 89%. Інструмент ефективно вирішує проблему "сліпих зон" у традиційних механізмах аудиту Salesforce, забезпечуючи повну прозорість змін у декларативній логіці системи.

Практична значимість результатів полягає у розробці конкретної методології інтеграції FlowVersionComparer у процеси забезпечення кібербезпеки, яка може бути адаптована організаціями різного масштабу. Подальші дослідження мають зосередитися на автоматизації процесів аналізу змін через машинне навчання та інтеграції з SIEM-системами для проактивного виявлення загроз.

Результати дослідження демонструють, що контроль версій Flow не є просто технічною практикою, а критичним компонентом комплексної стратегії кібербезпеки CRM-систем. В епоху, коли бізнес-логіка стає все більш складною та розподіленою, інструменти на кшталт FlowVersionComparer стають незамінними для підтримки безпеки, цілісності та доступності корпоративних даних.

Література

[1] Salesforce, "Automate Tasks with Flows," [Online]. Available: https://help.salesforce.com/s/articleView?id=platform.flow.htm&type=5.

[2] C. Grant and S. Kumar , "ORCHESTRATING IT SUPPORT WITH CHATGPT AGENTS AND SALESFORCE FLOWS," in *Salesforce Flows for Support*, Kindred Press, 2025, pp. 322-332

[3] A. K. Patel, "A Comprehensive Exploration of Salesforce Flow: Unleashing the Power of Automation," *European Journal of Advances in Engineering & Technology,* vol. 11, pp. 75-80, 2024.

[4] L. Ridwan, "Next-Level Automation: Orchestrating Business Processes in Salesforce with AI and Flow Builder.," 2025

[5] T. Vyshnavi and S. Murali, "Transforming Deployment and Release Management for Salesforce with Copado's AI," *International Journal on Cybernetics & Informatics,* vol. 14, pp. 75-79, 2025.