

ОЦІНКА РИЗИКІВ ВТРАТ ДАНИХ В ІТ-ПРОЕКТАХ

Шибіка В.І.¹; Петрова Р.В., доцент, к.т.н.²

^{1,2} Харківський національний університет радіоелектроніки

^{1,2} Україна, Харків

¹ valeriia.shybika@nure.ua; ² roksana.petrova@nure.ua

Анотація. Під час дослідження розроблено основні теоретичні та експериментальні результати дослідження ранньої оцінки ризиків втрати даних в ІТ-проектах. Виявлено ключові ризики та запропоновані методи їхнього уникнення, які можуть бути застосовані на практиці для підвищення ефективності ІТ-проектів. Стаття надає практичні рекомендації для оптимізації процесів оцінки ризиків на початкових етапах розробки.

Ключові слова: Оцінка ризиків; ІТ-проекти; втрати даних; ідентифікація загроз; мінімізація ризиків.

Вступна частина. Втрата даних є однією з найсерйозніших загроз для ІТ-проектів, оскільки вона може призвести до втрати цінної інформації, значних фінансових збитків і порушення довіри клієнтів. Актуальність цієї проблеми обумовлена зростанням кількості кібератак, технічних збоїв і людських помилок, що сприяють втраті даних. Сучасні методи оцінки ризиків часто не охоплюють усіх можливих факторів, що ускладнює прийняття ефективних заходів для захисту даних. В останніх дослідженнях головний акцент робиться на застосуванні матричних підходів і автоматизованих систем для аналізу ризиків. Метою цього дослідження є аналіз існуючих методів оцінки ризиків втрати даних в ІТ-проектах і розробка практичних рекомендацій для їх удосконалення.

Метою дослідження є розробка та впровадження методів ранньої оцінки ризиків втрати даних у ІТ-проектах для підвищення їхньої ефективності. Особлива увага зосереджується на ідентифікації загроз, оцінці їхньої ймовірності та наслідків, а також на розробці відповідних заходів для зменшення ризиків.

Відомі методи вирішення цієї проблеми, такі як резервне копіювання, впровадження заходів з кібербезпеки та використання хмарних технологій, не завжди достатньо ефективні через недостатнє врахування всіх можливих загроз. Актуальні дослідження показують, що комплексний підхід до оцінки ризиків, який включає як технічні, так і організаційні аспекти, є необхідним для підвищення рівня захисту даних. Цей комплексний підхід також потребує постійного моніторингу та аналізу нових загроз і технологій для забезпечення актуальності та ефективності заходів з управління ризиками [1].

Основна частина. Першим етапом була ідентифікація основних загроз. На цьому етапі було проведено аналіз типових загроз для ІТ-проектів, що можуть призвести до втрати даних. Основні загрози включають в себе технічні збої (відмова обладнання, помилки програмного забезпечення), кібератаки (віруси, фішинг, злом), природні катастрофи (пожежі) та людський фактор (помилки співробітників, недбале ставлення до безпеки).

Далі слід було визначити оцінку ймовірності та наслідки ризиків. На цьому етапі було застосовано матричний підхід для оцінки ймовірності виникнення кожного ризику та його можливого впливу на ІТ-проект [3]. Створено матрицю ризиків, яка дозволила проаналізувати загрози за двома основними показниками: ймовірність та серйозність наслідків. Матричний підхід дозволив виявити найбільш критичні ризики для ІТ-проектів, зокрема, пов'язані з

технічними збоями та людським фактором, які отримали високу оцінку ймовірності, та кібератаки і природні катастрофи, які мають найсерйозніші наслідки у разі реалізації.

Наступним, третім етапом, стала розробка заходів мінімізації ризиків. На основі оцінки ризиків було створено комплекс заходів, спрямованих на зменшення їхнього впливу на ІТ-проекти. Це включає регулярне резервне копіювання даних на різних носіях та в хмарних сховищах, що забезпечує можливість відновлення у разі втрати [2]. Також передбачено шифрування конфіденційної інформації під час передачі та зберігання, а контроль доступу реалізується шляхом впровадження багаторівневих політик, які обмежують доступ до критичних даних лише для авторизованих користувачів. Крім того, важливим є навчання персоналу для підвищення рівня знань співробітників щодо кібербезпеки та безпечного поводження з даними.

Для оцінки ефективності цих заходів було проведено тестування на вибіркових ІТ-проектах з різних галузей. Результати показали значне зниження ризиків втрати даних завдяки впровадженню систематизованого підходу до їхнього управління. Важливим аспектом тестування була не лише перевірка технічних рішень, але й оцінка готовності персоналу до дотримання нових протоколів безпеки.

Четвертим, завершальним етапом, було впровадження автоматизованих систем моніторингу ризиків. Виявлено потребу в постійному моніторингу можливих загроз, щоб вчасно на них реагувати. Також тестували автоматизовані інструменти для управління ризиками, які допомагають швидко виявляти потенційні загрози, оцінювати їхній вплив і оперативно вживати заходів для їх усунення. Використання таких систем дозволяє зменшити час на виявлення загроз і забезпечити кращий захист даних в реальному часі.

Розширення впровадження автоматизованих систем моніторингу ризиків вимагає інтеграції цих інструментів з існуючими ІТ-системами та процесами компаній. Це потребує не лише технічної реалізації, але й організаційних змін, що включають навчання персоналу та розробку нових політик і процедур [3]. Важливо забезпечити, щоб усі зацікавлені сторони розуміли важливість цих змін і були готові до активної участі у процесі впровадження нових підходів до управління ризиками.

Висновки. На основі проведеного дослідження можна зробити висновок, що сучасні методи оцінки ризиків, зокрема матричні підходи та автоматизовані системи, значно підвищують точність та ефективність процесу управління ризиками втрати даних в ІТ-проектах. Розроблені практичні рекомендації щодо впровадження цих методів у реальні проекти спрямовані на підвищення їхньої безпеки та надійності. Основні результати дослідження включають визначення ключових факторів ризику, розробку стратегії для їхнього уникнення та пом'якшення наслідків, а також впровадження більш жорстких протоколів для захисту даних. Використання новітніх підходів до оцінки ризиків дозволяє зменшити ймовірність втрати даних та забезпечити більш надійний захист інформації в ІТ-проектах, що сприяє підвищенню довіри клієнтів та зменшенню фінансових втрат, пов'язаних з можливими інцидентами.

Додатково, впровадження новітніх підходів до управління ризиками створює основу для безперервного вдосконалення процесів в ІТ-компаніях. Постійний моніторинг і аналіз нових загроз, а також регулярне оновлення заходів безпеки, дозволяють зберігати високий рівень захисту даних у швидко змінюваному технологічному середовищі. Це забезпечує не лише захист від втрат, але й підвищує конкурентоспроможність компаній на ринку за рахунок демонстрації високого рівня кібербезпеки та надійності.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

- [1] Peltier, T. R. (2005). *Information Security Risk Analysis*. Auerbach Publications.
- [2] Smith, J., & Brown, L. (2019). *Risk Management in IT Projects: A Comprehensive Guide*. New York: TechPress.
- [3] Stoneburner, G., Goguen, A., & Feringa, A. (2002). *Risk Management Guide for Information Technology Systems*. NIST Special Publication 800-30.

Shybika V.I, Petrova R.V.

Assessment of data loss risks in it projects

Abstract. During the research, key theoretical and experimental results were developed for the early assessment of data loss risks in IT projects. Key risks were identified and methods for avoiding them were proposed, which can be applied in practice to improve the efficiency of IT projects. The article provides practical recommendations for optimizing risk assessment processes at the initial stages of development.

Keywords: Risk assessment; IT projects; data loss; identification of threats; minimization of risks.