Поетапне впровадження SOC 2 Type 2 для зберігання великих даних на підприємстві

УДК 004.056

Олег Дейнека[1], Олег Гарасимчук[2]

Національний Університет "Львівська Політехніка",
[1]oleh.r.deineka@lpnu.ua , [2] oleh.i.harasymchuk@lpnu.ua

Стрімке зростання обсягів корпоративних даних у поєднанні з підвищенням вимог до їх захисту та підзвітності ставить перед підприємствами принципово нові завдання. Дані перетворились на ключовий стратегічний ресурс, без якого неможливе ефективне функціонування державних і приватних організацій, фінансових установ, охорони здоров'я, промислових та наукових структур [1]. Разом з тим ринок комерційних рішень для управління даними пропонує переважно закриті, вартісні продукти без відкритої документації алгоритмів і процедур, що унеможливлює їх адаптацію під специфіку конкретного підприємства. Це зумовлює потребу у формалізованій, відкритій і відтворюваній методиці, яка б забезпечувала відповідність стандарту SOC 2 Type 2 і могла бути впроваджена незалежно від обраної технологічної платформи.

Стандарт SOC 2 Type 2 (Service Organization Control 2) є одним з найавторитетніших міжнародних стандартів у сфері контролю безпеки сервісних організацій. Він базується на п'яти критеріях довіри (Trust Services Criteria): безпека, доступність, цілісність обробки, конфіденційність та приватність. На відміну від Type 1, що фіксує стан засобів контролю на певний момент часу, Type 2 підтверджує їх операційну ефективність протягом аудиторського періоду – зазвичай від 6 до 12 місяців. Саме тому впровадження SOC 2 Type 2 вимагає не разового технічного налаштування, а системного, безперервного управління процесами зберігання, класифікації та доступу до даних [2,4].

Метою роботи є розроблення формалізованої методики безпечного зберігання та обробки великих обсягів даних, що забезпечує відповідність вимогам SOC 2 Type 2 та може бути застосована незалежно від технологічної платформи.

У рамках наукового дослідження розроблено методику безпечного зберігання великих обсягів даних, що відповідає вимогам SOC 2 Type 2. Методика поєднує організаційні, технічні та процедурні аспекти управління даними і ґрунтується на поетапній архітектурі обробки інформації: від збору та первинного збереження сирих даних – до їх очищення, семантичного збагачення і формування готових аналітичних структур для потреб звітності й аудиту. На кожному рівні реалізуються заходи контролю якості, класифікації та захисту інформації, а результати класифікації безпосередньо визначають застосування політик шифрування і розмежування доступу [3].

Автоматизована ідентифікація чутливих даних – персональної інформації, фінансових відомостей, клієнтських записів – здійснюється із залученням інтелектуальних інструментів аналізу тексту, що суттєво знижує вплив людського фактору на безпеку. Оркестрація інтеграційних потоків, моніторинг

виконання та реагування на порушення забезпечуються засобами автоматизації й сповіщень, тоді як управління секретами та ідентифікація користувачів реалізовані відповідно до вимог SOC 2 щодо контролю доступу та захисту облікових даних [2, 3]

Для успішного впровадження методики на підприємстві запропоновано поетапний системний підхід, що враховує специфіку бізнесу, організаційну структуру та технічні вимоги. Запропонований підхід формалізовано у вигляді послідовного алгоритму впровадження методики, що складається з наступних етапів:

1. Ідентифікація замовника та визначення стратегічних цілей. Налагодження комунікації з технічними і нетехнічними спеціалістами підприємства, збір вимог, узгодження бачення та фіксація критеріїв ефективності (включають показники продуктивності, рівня доступності, точності класифікації даних та відповідності вимогам безпеки) й очікуваних результатів.

2. Формування проєктної команди. Визначення ключових ролей – бізнес-аналітика, керівника проєкту та архітектора рішень – відповідальних за координацію, технічний дизайн і управління проєктом.

3. Планування та декомпозиція завдань. Розподіл проєкту на послідовні цілі та проведення повного аудиту даних підприємства: виявлення локальних і хмарних сховищ, класифікація типів, обсягів і форматів даних, оцінка їх критичності відповідно до вимог SOC 2 Type 2.

4. Розроблення архітектурної візії рішення. Проєктування технічної архітектури з урахуванням бізнес-процесів та наявної IT-інфраструктури: вибір технологічних платформ, принципи організації шарів зберігання і трансформації даних, інтеграційні та захисні механізми, підтримка гібридних сценаріїв і масштабованості.

5. Формалізація проєктного плану та затвердження. Підготовка детального плану з розподілом ролей, заходами контролю якості та безпеки, оцінкою ресурсів і строками; отримання офіційного затвердження від замовника.

6. Розроблення пілотного рішення. Запуск прототипу на обмеженому наборі даних для оцінки працездатності архітектури, виявлення потенційних проблем і збір емпіричних даних щодо функціонування системи.

7. Комплексне тестування. Тестування інтеграційних процесів, трансформації та обробки даних; верифікація коректності метаданих, налаштувань доступу й класифікації чутливих даних; оцінювання ефективності інструментів автоматизованого виявлення конфіденційної інформації.

8. Аналіз результатів та внесення коректив. Оцінювання продуктивності, масштабованості та відповідності системи вимогам безпеки за критеріями часу відповіді, рівня доступності (uptime/SLA), повноти обробки даних, дотримання нормативних вимог щодо класифікації, зберігання і видалення даних, а також експлуатаційної придатності системи.

9. Навчання персоналу та внутрішня документація. Підготовка IT-персоналу і кінцевих користувачів, розроблення документації щодо правил роботи з системою, визначення ролей і стандартів обробки даних.

10. Масштабування та постійна підтримка. Розширення системи на інші підрозділи або додаткові джерела даних; безперервний моніторинг, регулярний

аудит та оновлення відповідно до змін у бізнес-процесах і нормативних вимогах безпеки.

Варто зазначити, шо процес має ітераційний характер і передбачає повернення до попередніх етапів у разі виявлення невідповідностей або змін у вимогах

Галузева специфіка підприємства суттєво визначає пріоритизацію критеріїв Trust Services Criteria. Для фінансового сектору на перший план виходять конфіденційність і цілісність транзакційних журналів; для закладів охорони здоров'я – суворі вимоги до приватності пацієнтських даних; для телекомунікаційних компаній – безперервна доступність сервісів та стійкість до відмов; для виробничих підприємств з Industrial IoT – цілісність потокових даних промислових сенсорів.

Запропонована методика передбачає адаптивний вибір пріоритетних засобів контролю на основі профілю ризиків конкретної галузі, що відрізняє її від універсальних «коробкових» рішень [1, 3].

Впровадження запропонованої методики дозволяє підприємствам різних галузей структуровано підготуватись до сертифікаційного аудиту за стандартом SOC 2 Type 2, сформувати прозору та відтворювану систему управління великими обсягами корпоративних даних, мінімізувати ризики несанкціонованого доступу та витоку інформації.

Кожен етап методики корелює з відповідними критеріями Trust Services Criteria та забезпечує їх поступову імплементацію на організаційному і технічному рівнях.

На відміну від закритих комерційних продуктів, методика є відкритою, адаптованою до різних технологічних середовищ і розрахованою на практичне впровадження силами внутрішньої команди підприємства без залежності від конкретного постачальника хмарних сервісів.

Адаптація реалізується шляхом вибору релевантного набору контролів на основі оцінки ризиків (risk-based approach).

1. Дейнека О. Р., Гарасимчук О. І. Виклики та стратегії зберігання великих обсягів даних у сучасному світі. Захист інформації. 2024. Т. 25, № 4. С. 197–207.
2. Дейнека О. Р., Бортнік Л. Л. Методологія збору, обробки, зберігання та класифікації даних відповідно до вимог SOC 2 Type 2. Комп'ютерні системи та мережі. 2024. Т. 6, № 1. С. 36–43. https://doi.org/10.23939/csn2024.01.036
3. Дейнека О. Р., Гарасимчук О. І. Дослідження проблем класифікації та безпечного зберігання даних. Безпека інформації. 2023. Т. 29, № 2. С. 147–153.
4. AICPA. Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (SOC 2). American Institute of CPAs, 2022. 112 p