Ідея

Що ми знаємо, як це перевірити та чого ми ще не знаємо

Посібник «Konfirmu» для сімей, вчителів, осіб, що приймають рішення, та фахівців.



Документ

10 коробок



Порівняти копії

Матч



Що прийшло?

У двох документах зазначено, що надійшло десять ящиків. Хтось іде на склад, перераховує ящики, що стоять на підлозі, і знаходить дев’ять.

Ми можемо перевірити, чи збігаються документи. Щоб дізнатися, скільки коробок надійшло, нам також потрібна інформація про їхню кількість. Які докази ви попросили б показати людину, яка їх отримала?

Три рівні доказовості

Що ми можемо перевірити?

Копія, підпис і підрахунок дають відповіді на різні питання.

01 Чи є у нас надійне джерело?

Це може бути як сам оригінальний файл, так і його цифровий відбиток, отриманий через надійний канал. Також збережіть інформацію про версію та джерело посилання.

02 Чи містяться в копії ті самі дані?

Хеш — це цифровий відбиток, що обчислюється на основі байтів у файлі. Перевірка цифрового підпису за допомогою надійного ключа також дозволяє підтвердити зв’язок із ключем підписувача.

03 Чи відбулася подія, описана в документі?

Щоб з’ясувати, що сталося, можливо, доведеться перерахувати коробки, перевірити виміри, звернутися до офіційних документів або попросити кваліфіковану особу проаналізувати докази.

> **Три можливі варіанти відповіді**
>
> «Збігається» — коли копії збігаються. «Відрізняється» — коли вони відрізняються. «Поки що не знаю» — коли бракує посилання чи іншого доказу.

Ви можете перевірити в автономному режимі, чи є на вашому пристрої необхідні дані, посилання та інструменти. Відновити втрачений оригінал можна лише за умови наявності його копії.

Помилки, які ми навчилися розпізнавати

Шість висновків із наукової записки від 25 листопада. Кожен результат тесту стосується версії, зазначеної в записці.

F1 Межа у 95 % може охоплювати менший обсяг

Що ми виявили

У цьому прикладі верхня межа, розрахована лінійним методом, охоплює 86,51 % значень, хоча її номінальний рівень становить 95 %.

Як перевірити

На сторінці 7 показано, як обчислити покриття для оберненого значення величини, що підпорядковується нормальному розподілу з середнім значенням 1 і стандартним відхиленням 0,3.

Що це не доводить

Результат стосується саме цієї моделі та цих меж. Для інших вимірювань потрібно провести новий розрахунок.

Для цього випуску було проведено перерахунок показника F1. Команда також повторила цей розрахунок 24 листопада.

F2 Квитанція та розмір партії

Що ми виявили

Для деяких партій накладній, сформованій за допомогою версії, що досліджується, не вдалося підтвердити кількість одиниць товару.

Як перевірити

Під час перевірки слід зафіксувати, скільки одиниць товару надійшло та які докази підтверджують відповідність цієї кількості зазначеному в накладній.

Що це не доводить

Це обмежує інформацію про партію, що міститься у квитанції. У примітці зазначено, що SHA-256 не було зламано.

24 листопада команда знову зіткнулася з проблемою F2. У записці цю проблему було зазначено як невирішену у версії 3.0.0.

F3 Коли зникає відмінність у даних

Що ми виявили

У збереженому вигляді було втрачено розрізнення, яке було присутнє у вихідних даних. На основі квитанції це вже не можна було встановити.

Як перевірити

Під час перевірки команда повинна бути здатна продемонструвати, що в записі збережено всі відповідні відмінності, присутні в оригіналі.

Що це не доводить

Ця відмінність зникла під час візуалізації даних. Цей тест не свідчить про криптографічну колізію.

24 листопада команда повторно виявила проблему F3. У записці ця проблема була зазначена як невирішена у версії 3.0.0.

Коли система повинна зупинитися

Шість висновків із наукової записки від 25 листопада. Кожен результат тесту стосується версії, зазначеної в записці.

F4 Двоє перевіряючих дали різні відповіді

Що ми виявили

У звіті про внутрішню перевірку зазначено, що один перевіряючий виявив 7 із 9 змін, а інший — усі 9.

Як перевірити

Щоб оцінити нову версію, порівняйте її рішення з очікуваними та збережіть результати тестування.

Що це не доводить

Дев'ять прикладів не дозволяють визначити, скільки змін було б виявлено в іншому наборі документів.

Про F4 було повідомлено у внутрішньому звіті від 24 листопада. Команда не проводила повторного тестування для цієї примітки.

F5 «OK», хоча за правилами потрібно було зупинитися

Що ми виявили

Команда виявила чотири ситуації, в яких відповіддю було «OK», хоча за правилами мала бути «VETO».

Як перевірити

Після впровадження запропонованого виправлення 186 із 1 246 тестових випадків перестали повертати результат «OK». Жоден із них не змінився на «OK».

Що це не доводить

У записці описано запропоноване виправлення. Для підтвердження його використання у виробничому середовищі необхідні дані про встановлену версію та результати її тестування.

24 листопада було повідомлено про F5. 25 листопада у записці зазначалося, що виправлення ще не оприлюднено.

F6 Показник, що дуже наближається до граничного значення

Що ми виявили

У прикладі з граничними значеннями 2 та 8 округлення показання до шести знаків після коми дало інший результат, ніж при використанні вищої точності.

Як перевірити

Під час перевірки слід визначити, яка точність використовувалася, та які правила було узгоджено для порівняння результатів вимірювання з граничним значенням.

Що це не доводить

Допустимі відхилення залежать від призначення та відповідних правил. У цьому прикладі не встановлюються допустимі відхилення для інших випадків використання.

Про F6 було повідомлено 24 листопада. На момент написання цієї записки правило щодо посилань ще обговорювалося.

Здоров'я та медицина

Перегляд медичної карти

Три вигадані ситуації, в яких хтось може порівняти запис із надійним еталоном.

01 Картка вакцинації

Порівняння може виявити, що копія була змінена. Для підтвердження того, що вакцина була введена, потрібні докази, отримані під час клінічного прийому. Ефективність вимагає окремих доказів.

02 Результат лабораторного дослідження

Ви можете перевірити, чи збігається отриманий вами звіт із тим, що зберігається в лабораторії. Інтерпретацію фактичного результату повинен здійснювати медичний працівник.

03 Запис про холодовий ланцюг

Ви можете порівняти копію журналу з еталонними даними. Калібрування датчика та фактичні умови зберігання потрібно перевіряти окремо.

> **Датчик може зафіксувати неправильне значення**
> Припустимо, що датчик показує 4 °C. Якщо датчик несправний, фактична температура може відрізнятися, навіть якщо копія журналу повністю збігається з оригіналом.

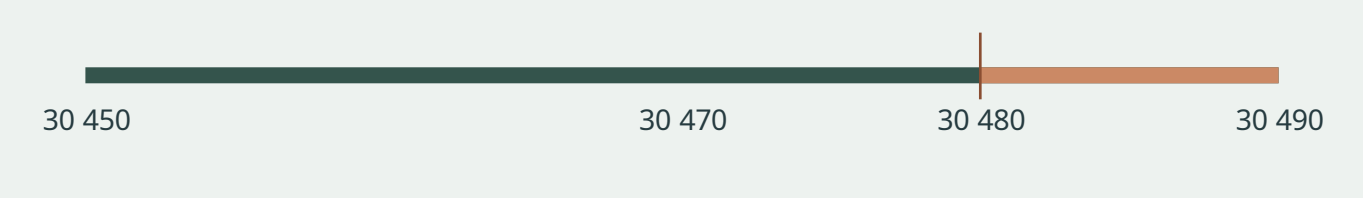
У науковій статті «Konfirmu» описано як дослідний прототип. Це не є медичним пристроєм і не призначене для діагностики, лікування або прийняття рішень щодо окремих осіб.

Експлуатаційна безпека та голосування

У дійсній квитанції може бути вказано «стоп»

Стендові випробування з використанням умовного контейнера та гіпотетичного обмеження в 30 480 кг.

Показник ваги: 30 470 ± 20 кг



Діапазон ваги, у кілограмах · межа 30 480 kg
https://dpsindustrial.nl/konfirmu/guia/pesagem/?lang=uk

Діапазон становить від 30 450 до 30 490 кг. Допуск, що розраховується як різниця між граничним значенням і вагою, коливається від −10 до +30 кг. У верхній межі вага перевищує граничне значення на 10 кг. Квитанція може мати дійсний підпис (VALID), хоча згідно з правилами має бути застосовано зупинку (VETO).

А як щодо голосування?

Перевірка підписаного протоколу може виявити зміни, внесені пізніше. Доступ виборців, точність підрахунку голосів та таємниця голосування — кожна з цих складових вимагає окремих доказів. Квитанція, яка розкриває вибір особи, може порушити таємницю голосування.

Хто може дати дозвіл на проведення операції?

Підпис дає змогу перевірити документ. Відповідальні особи вирішують, чи продовжувати процедуру, спираючись на правила та дані щодо конкретної операції.

Перевірка вашого пристрою

Як перевірити це самостійно

Маючи надійне еталонне значення, ви можете порівняти файл. Ви також можете повторити розрахунок покриття, наведений на сторінці 3.

У примітці вказано версію движка Python 3.0.0, коміт 90b3968, від 24 листопада 2026 року. Код ліцензовано за ліцензією EUPL-1.2.

Офіційний репозиторій коду

SHA-256 двигуна Python, як зазначено в примітці
`529098c652ee8234960d69383e308f60db6a5df8ea6bdae578b538eb806e80cf`

Помістіть маніфест випуску та відповідні файли в одну папку. Виконайте команду, що відповідає вашій операційній системі.

```
sha256sum -c SHA256SUMS.txt        # Linux
shasum -a 256 -c SHA256SUMS.txt    # macOS
```

Команда повідомила про 62 файли, що відповідають критеріям, 247 самоперевірок та 10 наборів правил, перевірених у середовищі Linux із використанням Python 3.13. Ці цифри стосуються саме цього огляду.

F1 · Повторити обчислення в Python

```
from statistics import NormalDist
X, Z = NormalDist(1, 0.3), NormalDist()
u = 1 + Z.inv_cdf(.95) * .3
print(u, X.cdf(0) + 1 - X.cdf(1/u))
print(X.cdf(1/.412) - X.cdf(1/1.588))
```

Для Y = 1/X верхня межа становить 1,493456088, а покриття — 86,51 %. Негативні значення X також відповідають цій межі. Опубліковані, округлені двосторонні межі 0,412 та 1,588 забезпечують покриття 89,14 %.

Покриття — це ймовірність у рамках цієї моделі. У примітці наводяться посилання на JCGM 100 та 101 щодо поширення невизначеності.

Відкрийте додаток-браузер · 143 662 B

https://dpsindustrial.nl/konfirmu/app/

Відкрийте вікно «Порівняти файли». Виберіть вихідний файл і другу копію, а потім натисніть «A4 · Порівняти».

Compare files → Reference file → Second copy → A4 · Compare

SHA-256 HTML-файлу браузерного додатка, перевірено 26 листопада 2026 року
`0a468ec23401f5125ee1e5399ef536b6fba88beab94771e4df6b7910c9723717`

Обмеження та подальші тести

Що ми досі не знаємо

Будь-хто, хто отримує дані, може їх перевірити. Те, що підтверджують ці дані, залежить від джерела та методу, який було використано.

Хто проводив ці випробування?

У записці від 25 листопада зазначено, що тестування проводила ця команда з використанням відповідних систем штучного інтелекту. Незалежна перевірка дозволить визначити версію, повторити тестування та зафіксувати результати, включаючи розбіжності.

Які досягнення зафіксовано?

Перевірка на відповідність 295 вимогам стандарту ECSS-Q-ST-80C Rev.2 проводилася у формі самооцінки. У документах i-DEPOT № 162925 та № 164391 зазначено, що саме та коли було зареєстровано. Якість продукції вимагає окремої оцінки.

Що можна встановити за допомогою часової мітки?

Chronolex дає читачам можливість перевірити цілісність запису. У примітці зазначено, що цей безкоштовний загальнодоступний сервіс маркування часу не гарантує юридичної сили. Докази того, що подія відбулася, все одно необхідні.

Виявили невідповідність?

Запишіть версію, очікуваний результат та те, що ви помітили. Надішліть цю інформацію на адресу

admin@dpsindustrial.nl

Відскануйте або натисніть, щоб відкрити

Офіційний веб-сайт ДПС

Набір із 12 секторів

У архіві ZIP відкрийте папку Exemplos/09-Shipping/. Порівняйте файли 01-original.txt та 02-copia.txt у програмі: у вигаданих записах вказано 24 та 29 коробок. Приклад зважування наведено на сторінці 6.

Першоджерело · Наукова записка від 25 листопада 2026 року
Konfirmu_Scientific_Note.pdf · 88 212 B · SHA-256
884fde70000fa68dccdb4b6527da7a1bce8a7737b3f44c03340f182ae6100f88
DPS Industrial & Maritime Services · Konfirmu · KVK 42005886
Енсхеде, Нідерланди