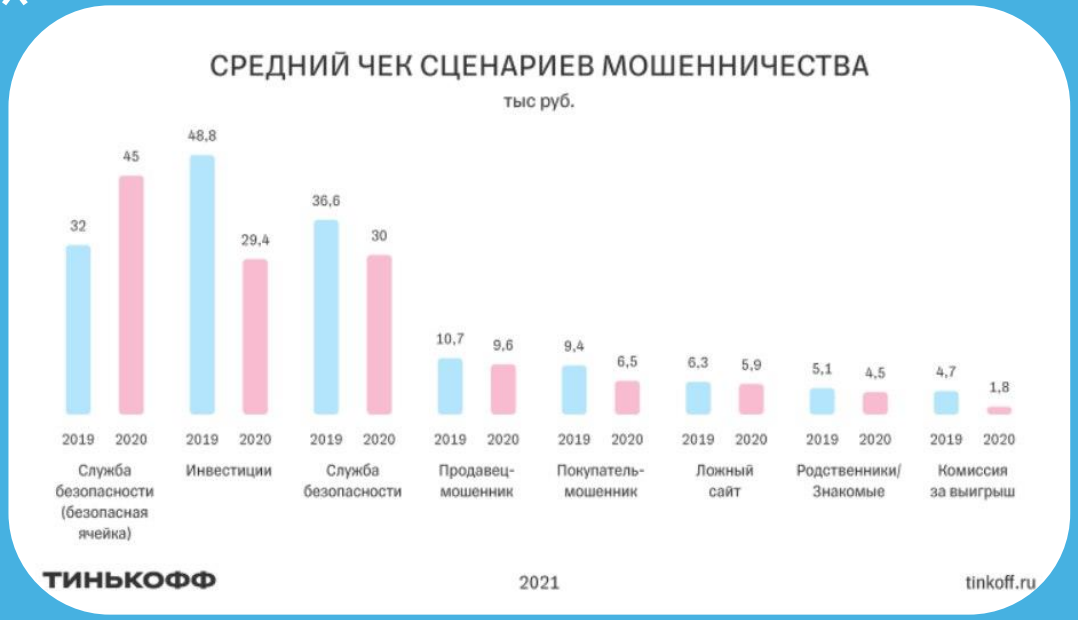
ОПРЕДЕЛЕНИЕ ФРОДОВЫХ ТРАНЗАКЦИЙ

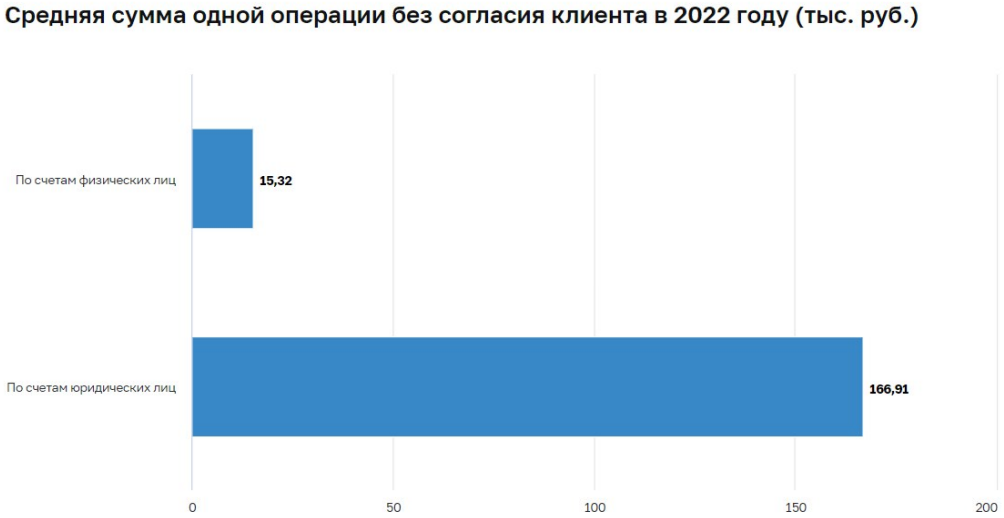
Nuclear IT Hack Spring '24
Q&D

АНАЛИТИКА РЫНКА

*



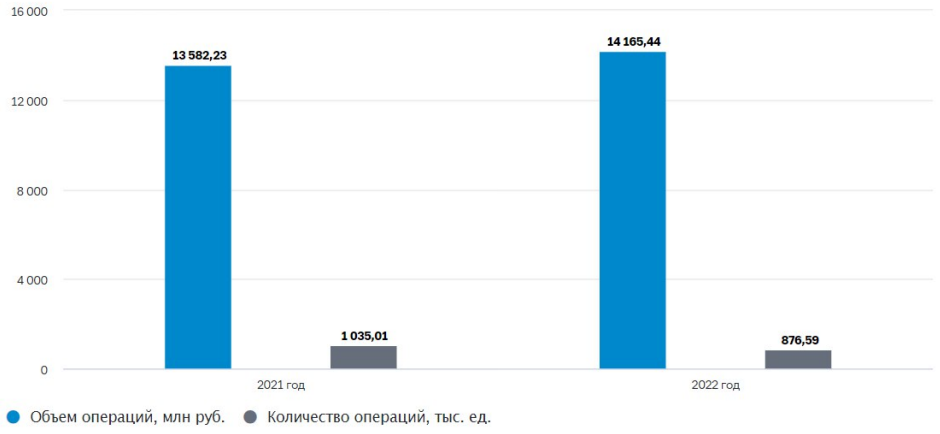
**



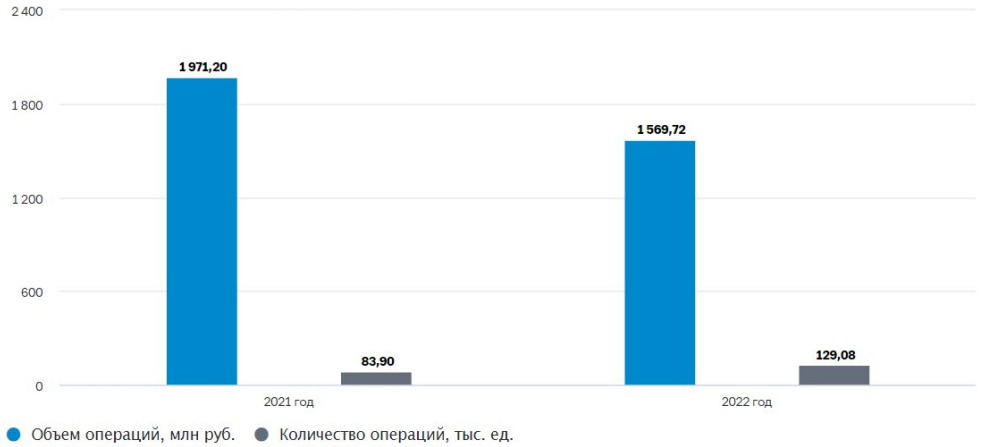
Источники: *Исследование Тинькофф **Отчет ЦБ РФ

АНАЛИТИКА РЫНКА

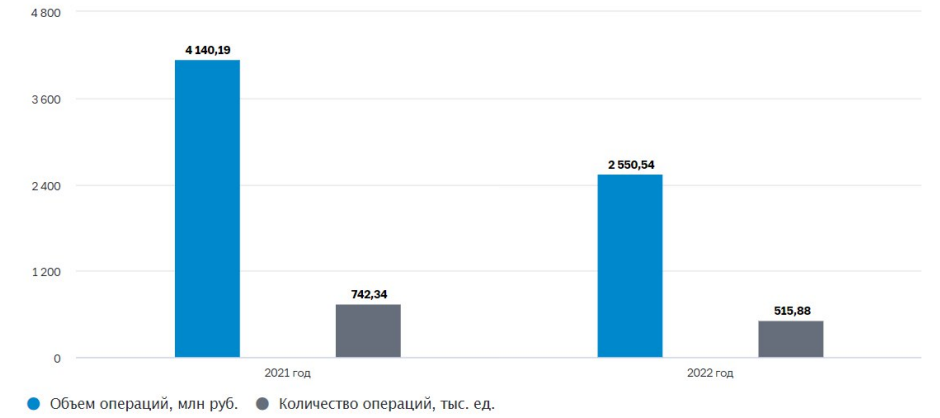
Общий объем и количество операций без согласия клиентов



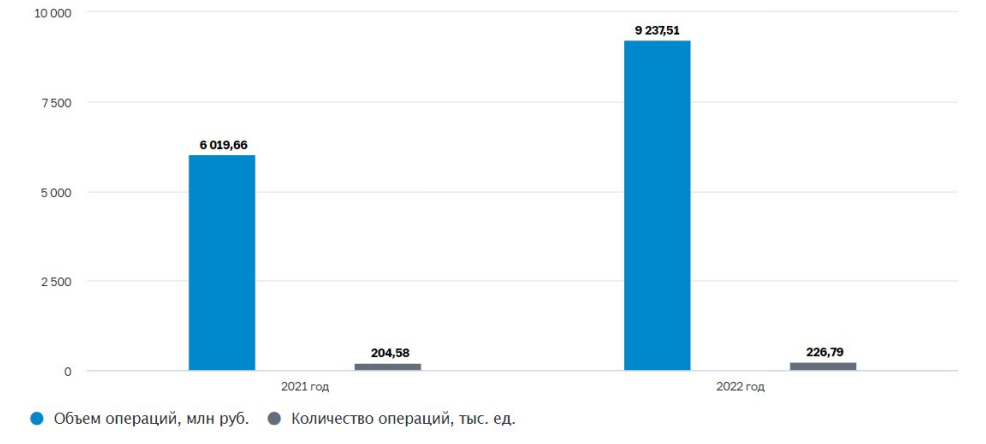
Операции без согласия клиентов в банкоматах, терминалах, импринтерах



Операции без согласия клиентов при оплате товаров и услуг в Интернете (CNP-транзакции)



Операции без согласия клиентов в дистанционном банковском обслуживании



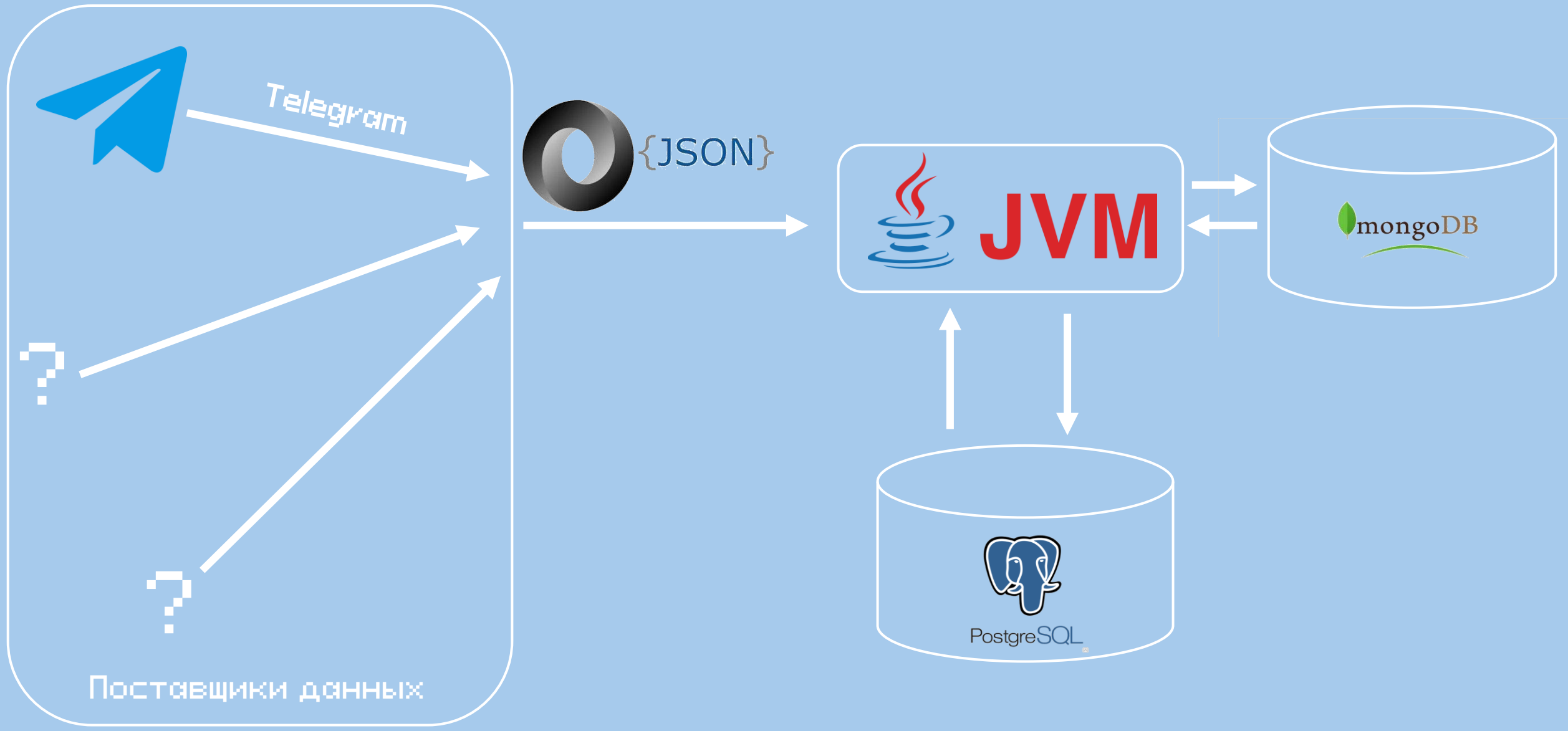
Источник: Отчет ЦБ РФ

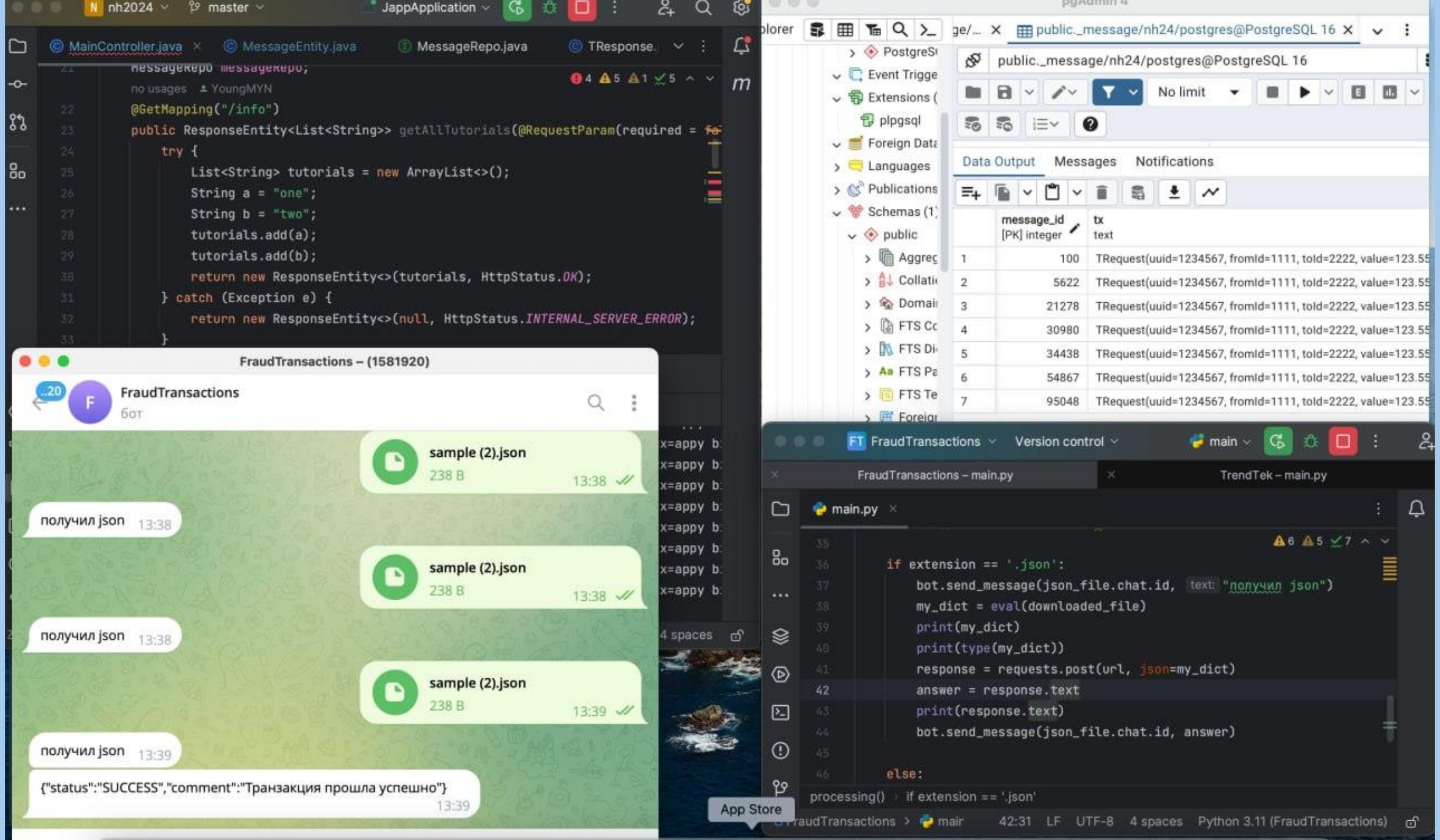
СУЩЕСТВУЮЩИЕ AML/ANTIFRAUD РЕШЕНИЯ

ORACLE®

Comita

Принцип работы системы




nh2024
master
JappApplication
MainController.java
MessageEntity.java
MessageRepo.java
TResponse
no usages YoungMYN
@GetMapping("/info")
public ResponseEntity<List<String>> getAllTutorials(@RequestParam(required = fa
try {
List<String> tutorials = new ArrayList<>();
String a = "one";
String b = "two";
tutorials.add(a);
tutorials.add(b);
return new ResponseEntity<>(tutorials, HttpStatus.OK);
} catch (Exception e) {
return new ResponseEntity<>(null, HttpStatus.INTERNAL_SERVER_ERROR);
}
FraudTransactions – (1581920)
FraudTransactions
бот
sample (2).json
238 B
13:38
получил json
13:38
sample (2).json
238 B
13:38
получил json
13:38
sample (2).json
238 B
13:39
получил json
13:39
{"status":"SUCCESS","comment":"Транзакция прошла успешно"}
13:39
pgAdmin 4
public._message/nh24/postgres@PostgreSQL 16
No limit
Data Output
Messages
Notifications
message_id
[PK] integer
tx
text
1 100 TRequest(uuid=1234567, fromId=1111, toId=2222, value=123.55
2 5622 TRequest(uuid=1234567, fromId=1111, toId=2222, value=123.55
3 21278 TRequest(uuid=1234567, fromId=1111, toId=2222, value=123.55
4 30980 TRequest(uuid=1234567, fromId=1111, toId=2222, value=123.55
5 34438 TRequest(uuid=1234567, fromId=1111, toId=2222, value=123.55
6 54867 TRequest(uuid=1234567, fromId=1111, toId=2222, value=123.55
7 95048 TRequest(uuid=1234567, fromId=1111, toId=2222, value=123.55
FraudTransactions
Version control
main
FraudTransactions – main.py
TrendTek – main.py
main.py
if extension == '.json':
bot.send_message(json_file.chat.id, text: "получил json")
my_dict = eval(downloaded_file)
print(my_dict)
print(type(my_dict))
response = requests.post(url, json=my_dict)
answer = response.text
print(response.text)
bot.send_message(json_file.chat.id, answer)
else:
processing() › if extension == '.json'
App Store
42:31 LF UTF-8 4 spaces Python 3.11 (FraudTransactions)

РЕЙТИНГ НАДЕЖНОСТИ КЛИЕНТА

$$y = \frac{\omega_1 * x_1 + \omega_2 * x_2 + \omega_3 * x_3 + \omega_4 * x_4}{7.4}$$

$$\omega_1 = 5$$

$$\omega_2 = 3$$

$$\omega_3 = 8$$

$$\omega_4 = 1$$

x1 =
- 0, произведено менее 5 операций оплаты или перевода
- 1, произведено менее 10 операций оплаты или перевода
- 2, произведено болне 10 операций оплаты или перевода

x2 =
- 0, аккаунту меньше 2 месяцев
- 1, аккаунту меньше 4 месяцев
- 2, аккаунту больше 4 месяцев

x3 =
- 0, аккаунт не привязан к другим сервисам
- 1, аккаунт привязан к малому кол-ву сервисов
- 2, аккаунт верифицирован с помощью ГосУслуг, аккаунт активен

x4 - оценка по пятибалльной шкале от работника Банка, default=2.5

ВЕРОЯТНОСТЬ ФРОДОВОЙ ТРАНЗАКЦИИ

$$y = \frac{\omega_1 * x_1 + \omega_2 * x_2 + \omega_3 * (6 - x_3) + \omega_4 * x_4}{\omega_1 + \omega_2 + 6 * \omega_3 + \omega_4}$$

$\omega_1 = 5$

$\omega_2 = 7$

$\omega_3 = 3$

$\omega_4 = 5$

x1 = 0, если отправитель и получатель имеют общие транзакции

1, если это первый перевод; отправитель и получатель не имеют друг друга в контактах

x2 = 0, если отправитель не имеет фродовых операций

1, если отправитель уже совершал операции, признанные фродовыми

x3 - рейтинг надёжности отправителя

x4 = 0, если отправление происходит с привычного IP

1, если отправление происходит с нового IP

ПОКУПКИ (E-COMMERCE • POS)

$$y = \frac{\omega_1 * x1 + \omega_2 * x_2 + \omega_3 * x_3 + \omega_4 * x_4}{\omega_1 + \omega_2 + \omega_3 + \omega_4}$$

$\omega_1 = 3$

$\omega_2 = 2$

$\omega_3 = 4$

$\omega_4 = 3$

$$\mathbf{x1} = \begin{cases} 0, \text{ покупка требует верификацию} \\ 1, \text{ покупка не требует авторизацию} \end{cases}$$

$$\mathbf{x2} = \begin{cases} 0, \text{ покупка привычной категории товаров} \\ 1, \text{ покупка новой категории товаров} \end{cases}$$

$$\mathbf{x3} = \begin{cases} 0, \text{ аккаунт до этого не подвергался фроду} \\ 1, \text{ аккаунт до этого подвергался фроду} \end{cases}$$

$$/\mathbf{x4} = \begin{cases} 0, \text{ покупка в привычном месте или с привычного ip} \\ 1, \text{ покупка в новом месте или с нового ip} \end{cases}$$

$$y = \begin{cases} \text{fraud purchase}, & \text{if } y \in [0.8, 1] \\ \text{additional check}, & \text{if } y \in (0.6, 0.8) \\ \text{safe purchase}, & \text{if } y \in [0, 0.6] \end{cases}$$

ОТСЛЕЖИВАНИЕ УРОВНЯ ЦИФРОВОЙ ГРАММОТНОСТИ

1. АКТИВНОСТЬ В СЕТИ
2. АКТИВНОСТЬ В БАНКОВСКИХ ПРИЛОЖЕНИЯХ

ОПРЕДЕЛЕНИЕ СВЯЗЕЙ МЕЖДУ ПОЛЬЗОВАТЕЛЯМИ

1. ОТСЛЕЖИВАНИЕ ЛОКАЦИИ
2. ОТСЛЕЖИВАНИЕ IP
3. ИСПОЛЬЗОВАНИЕ ТЕХНОЛОГИЙ OSINT ДЛЯ ВЫЯВЛЕНИЯ СВЯЗЕЙ МЕЖДУ ПОЛЬЗОВАТЕЛЯМИ

ИДЕИ ДОРАБОТКИ СУЩЕСТВУЮЩИХ ANTIFRAUD СИСТЕМ

1. УЛУЧШЕНИЕ ОТСЛЕЖИВАНИЯ ГЕОЛОКАЦИИ

2. УЧЕТ РИТУАЛОВ

ВЗГЛЯД В БУДУЩЕЕ...

РЕЗЮМЕ КОМАНДЫ

I. Капитан
II. Data scientist
III. Студент 2-го курса направления «Бизнес-информатика» НИЯУ МИФИ

I. Programming engineer
II. Студент 2-го курса направления «Бизнес-информатика» НИЯУ МИФИ

I. Business
II. Студент 2-го курса направления «Бизнес-информатика» НИЯУ МИФИ

I. DevOps engineer
II. Студент 2-го курса направления «Бизнес-информатика» НИЯУ МИФИ