

Материалы лекции можете скачать по ссылке - <https://clck.ru/3LakQi> или по QR коду



Конспект лекции: Информационные технологии в системе мер по профилактике коррупционных и иных правонарушений на государственной гражданской службе

Введение

Коррупция на государственной гражданской службе представляет собой серьёзную угрозу национальной безопасности и эффективному функционированию государственных институтов. Информационные технологии (ИТ) становятся важным инструментом в системе профилактики и противодействия коррупционным и иным правонарушениям, обеспечивая новые возможности для контроля, анализа и предупреждения коррупционных проявлений¹²⁴.

1. Понятие и причины коррупции на государственной службе

- Термин «коррупция» происходит от латинского слова *corruptio* — «порча, подкуп»¹.
- Основные причины коррупции на госслужбе:
 - отсутствие эффективного контроля;
 - наличие больших финансовых ресурсов;
 - лёгкость вывода средств;
 - участие большого числа должностных лиц;
 - возможность сокрытия преступления;
 - недостатки кадровой политики;
 - заинтересованность руководителей¹.

2. Роль информационных технологий в профилактике коррупции

ИТ обеспечивают механизм информационного контроля, который способствует предупреждению коррупционных правонарушений на государственной службе. Внедрение цифровых решений позволяет:

- Автоматизировать сбор и анализ данных о доходах, расходах, имуществе и обязательствах служащих;
- Обеспечить прозрачность и доступность информации;
- Выявлять конфликты интересов и коррупционные схемы;

- Проводить обучение и тестирование госслужащих по антикоррупционным стандартам с помощью информационно-аналитических систем;
- Оперативно мониторить соблюдение антикоррупционных норм и выявлять подозрительные операции¹²³.

3. Информационно-аналитические системы и цифровые технологии

- Пример: информационно-аналитическая система «Методика и тактика противодействия коррупции для государственных и муниципальных служащих», разработанная в Волгоградском институте управления, которая позволяет систематически обучать и контролировать госслужащих, выявлять проблемные зоны и оценивать антикоррупционную среду¹.
- Использование искусственного интеллекта (ИИ), анализа больших данных и машинного обучения для выявления коррупционных сговоров и рисков:
 - ИИ ускоряет обработку больших массивов данных (например, анализ 30 млн документов в Великобритании);
 - выявляет закономерности, указывающие на коррупционные схемы (пример Чехии);
 - мониторит соблюдение стандартов и предупреждает мошенничество (система Dozorro в сфере госзакупок);
 - снижает влияние человеческого фактора, автоматизируя выявление подозрительных операций и конфликтов интересов (программа ARACHNE в ЕС)².
- Применение технологий блокчейн для повышения прозрачности и защиты данных в государственных реестрах и кадастрах, хотя и с учётом рисков утечки информации и злоупотреблений².

4. Профилактика коррупции с использованием ИТ

- Профилактика — совокупность мер предупредительного воздействия, направленных на предотвращение новых форм коррупции и устранение условий, способствующих её развитию⁴.
- Информационные технологии позволяют:
 - выявлять и пресекать коррупционные правонарушения на ранних этапах;
 - обеспечивать систематическое обучение и информирование госслужащих;
 - повышать прозрачность и подотчётность государственных органов;
 - создавать условия для соблюдения законодательства и этических норм¹⁴.
- Важную роль играют кадровые подразделения, которые с помощью ИТ могут контролировать знания и психологическое состояние служащих, а также обеспечивать антикоррупционное просвещение¹.

5. Правовое регулирование и методические материалы

- В России функционирует федеральная государственная информационная система «Единая информационная система управления кадровым

составом государственной гражданской службы Российской Федерации», которая включает методические материалы по противодействию коррупции, рекомендации по урегулированию конфликта интересов и порядок уведомления о иной оплачиваемой работе³.

- Законодательство требует ужесточения санкций за коррупцию и системного контроля с использованием современных технологий¹³.

Примеры Python-кодов для решения задач профилактики коррупции и правонарушений

Детекция подозрительных транзакций (Anti-Money Laundering, AML)

Проблема: Необходимость выявлять цепочки подозрительных транзакций и аномалии²³.

```
import pandas as pd
import matplotlib.pyplot as plt

# Загрузка данных (пример)
df = pd.read_csv('transactions.csv')

# Простое правило: транзакции свыше определённой суммы считаются
# подозрительными
suspicious = df[df['amount'] > 100000]

# Визуализация подозрительных транзакций
plt.figure(figsize=(10, 6))
plt.hist(suspicious['amount'], bins=20, color='red', alpha=0.7)
plt.title('Распределение подозрительных транзакций')
plt.xlabel('Сумма')
plt.ylabel('Количество')
plt.show()
```

Для выполнения кода необходим файл **transactions.csv**

```
import pandas as pd
import matplotlib.pyplot as plt

# Создадим примерные данные транзакций
data = {
    'transaction_id': range(1, 21),
    'amount': [5000, 150000, 30000, 250000, 80000, 120000, 45000, 200000, 70000,
110000,
               9000, 130000, 60000, 170000, 40000, 210000, 10000, 140000, 50000,
190000]
}
```

```
# Создаем DataFrame
df = pd.DataFrame(data)

# Фильтруем подозрительные транзакции (сумма > 100000)
suspicious = df[df['amount'] > 100000]

# Визуализация подозрительных транзакций
plt.figure(figsize=(10, 6))
plt.hist(suspicious['amount'], bins=10, color='red', alpha=0.7)
plt.title('Распределение подозрительных транзакций')
plt.xlabel('Сумма транзакции')
plt.ylabel('Количество транзакций')
plt.grid(axis='y', alpha=0.75)
plt.show()
```



Комментарий: Такой анализ помогает выявлять аномальные операции для последующей проверки.

Объяснение

- Мы создали DataFrame с 20 транзакциями и разными суммами.
- Отфильтровали транзакции с суммой больше 100000 — считаем их подозрительными.

- Построили гистограмму для визуализации распределения подозрительных транзакций.

Построение графа транзакций для выявления коррупционных связей

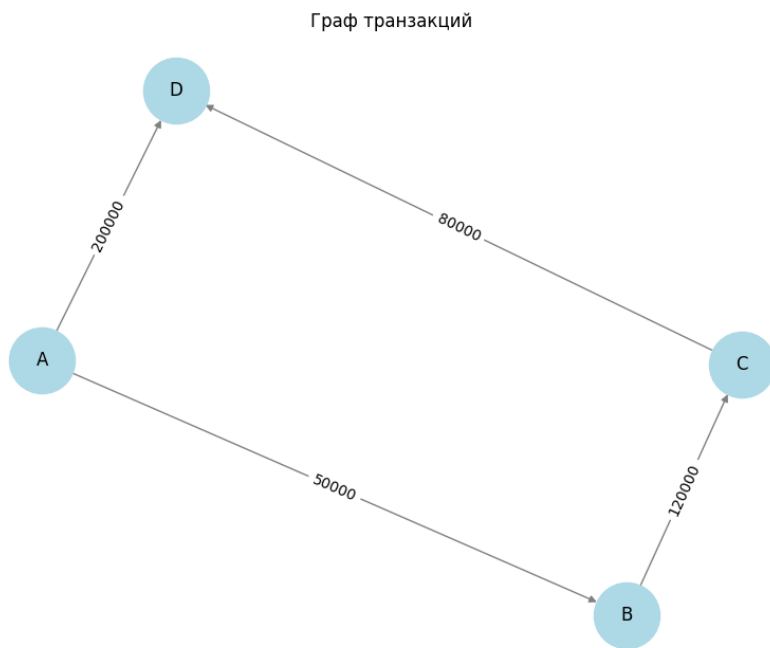
Проблема: Необходимость визуализации и анализа связей между участниками транзакций [3](#).

```
import pandas as pd
import networkx as nx
import matplotlib.pyplot as plt

# Пример данных: отправитель, получатель, сумма
data = [
    {'sender': 'A', 'receiver': 'B', 'amount': 50000},
    {'sender': 'B', 'receiver': 'C', 'amount': 120000},
    {'sender': 'C', 'receiver': 'D', 'amount': 80000},
    {'sender': 'A', 'receiver': 'D', 'amount': 200000},
]

df = pd.DataFrame(data)
G = nx.from_pandas_edgelist(df, 'sender', 'receiver', ['amount'],
create_using=nx.DiGraph())

# Визуализация графа
plt.figure(figsize=(8, 6))
pos = nx.spring_layout(G)
nx.draw(G, pos, with_labels=True, node_color='lightblue', node_size=2000,
edge_color='gray')
edge_labels = nx.get_edge_attributes(G, 'amount')
nx.draw_networkx_edge_labels(G, pos, edge_labels=edge_labels)
plt.title('Граф транзакций')
plt.show()
```



Комментарий: Такой граф позволяет визуально выявлять цепочки переводов и потенциальные коррупционные схемы.

Выводы

- Использование Python и современных библиотек позволяет автоматизировать анализ данных, выявлять подозрительные операции, строить графы связей и визуализировать результаты для последующего расследования.
- Важно применять безопасные практики программирования: валидацию, параметризацию запросов, ограничение привилегий, регулярный аудит кода.
- Для сложных задач рекомендуется использовать библиотеки pandas, scikit-learn, networkx, matplotlib, а также инструменты для автоматизации аудита и мониторинга [123](#).

Ссылки на источники кодов

- Snyk: Code injection in Python: examples and prevention [1](#)
- YouTube: Anti Money Laundering Project in Python2
- EuroPython 2023: Fighting Money Laundering with Python and Open Source Software

Пример кода из открытых проектов для выявления подозрительных транзакций (GitHub/Kaggle):

1. GitHub: проекты по анализу коррупционных схем и финансовых аномалий

- **Поиск и анализ подозрительных транзакций, выявление мошенничества и коррупции с помощью машинного обучения и анализа графов**

Примеры репозиторий:

- [Anti-Corruption ML](#) — коллекция проектов, связанных с анализом коррупционных данных и выявлением аномалий.

- [Financial Fraud Detection](#) — репозитории с моделями машинного обучения для выявления мошенничества в финансовых данных.
- [Network Analysis for Fraud Detection](#) — проекты, использующие графовые модели для выявления подозрительных связей.

2. Kaggle: датасеты и ноутбуки для анализа коррупции и мошенничества

- **Датасеты и проекты с анализом коррупционных данных, финансовых транзакций и выявлением аномалий**

Примеры:

- [Corruption Perceptions Index](#) — данные о восприятии коррупции в разных странах.
- [Financial Fraud Detection](#) — симуляция финансовых транзакций с метками мошенничества.
- [Anti-Money Laundering](#) — проекты с моделями для выявления отмывания денег.

3. Пример кода из открытых проектов для выявления подозрительных транзакций (GitHub/Kaggle)

```
import pandas as pd
from sklearn.ensemble import IsolationForest
import matplotlib.pyplot as plt

# Загрузка примерного датасета с транзакциями
df = pd.read_csv('transactions.csv') # замените на свой файл или датасет Kaggle

# Выбор признаков для анализа
features = ['amount', 'oldbalanceOrg', 'newbalanceOrig', 'oldbalanceDest',
            'newbalanceDest']
X = df[features]

# Обучение модели для выявления аномалий
model = IsolationForest(contamination=0.01, random_state=42)
df['anomaly'] = model.fit_predict(X)

# Фильтрация подозрительных транзакций
suspicious = df[df['anomaly'] == -1]

# Визуализация подозрительных транзакций по сумме
plt.figure(figsize=(10,6))
plt.hist(suspicious['amount'], bins=30, color='red', alpha=0.7)
plt.title('Распределение подозрительных транзакций по сумме')
plt.xlabel('Сумма транзакции')
plt.ylabel('Количество')
plt.show()
```

Для использования реальных данных transactions.csv для решения задачи выявления подозрительных транзакций, как в вашем примере, можно воспользоваться открытыми датасетами с Kaggle:

1. Credit Card Fraud Detection (Kaggle)

Ссылка на датасет:

<https://www.kaggle.com/datasets/mlg-ulb/creditcardfraud>

Файл:

creditcard.csv (можно переименовать в transactions.csv для вашего кода)

Описание:

- Содержит реальные анонимизированные данные о транзакциях по кредитным картам.
- Более 280 000 транзакций, включая как обычные, так и мошеннические операции.
- Используется во многих примерах по анализу и выявлению мошенничества²³.

2. Fraudulent Transactions Data (Kaggle)

Ссылка на датасет:

<https://www.kaggle.com/datasets/miznaarob/fraudulent-transactions-data>

Файл:

Fraud.csv (можно переименовать в transactions.csv)

Описание:

- Более 6 миллионов строк, 10 признаков.
- Содержит метки мошеннических транзакций и может быть использован для задач детекции аномалий⁶.

3. Fraud Detection (Kaggle)

Ссылка на датасет:

<https://www.kaggle.com/kartik2112/fraud-detection>

Файл:

fraudTrain.csv (можно переименовать в transactions.csv)

Описание:

- Содержит синтетические данные по транзакциям с метками мошенничества, подходит для обучения и тестирования моделей⁷.

Вывод:

Для вашего кода с анализом и визуализацией подозрительных транзакций используйте файл creditcard.csv с Kaggle (или любой из указанных выше), переименовав его в transactions.csv и поместив в рабочую директорию скрипта.

Прямая ссылка на скачивание (требуется аккаунт Kaggle):

- <https://www.kaggle.com/datasets/mlg-ulb/creditcardfraud23>
- <https://www.kaggle.com/datasets/miznaarob/fraudulent-transactions-data6>
- <https://www.kaggle.com/kartik2112/fraud-detection7>

Примечание:

Для скачивания потребуется зарегистрироваться и авторизоваться на Kaggle.

Этот конспект отражает основные положения и современные тенденции использования информационных технологий в профилактике коррупции на

государственной гражданской службе с опорой на последние исследования и практические разработки.

Ресурсы и ссылки

- GitHub Topics по теме коррупции и мошенничества:
<https://github.com/topics/anti-corruption>
<https://github.com/topics/fraud-detection>
- Kaggle проекты и датасеты:
<https://www.kaggle.com/datasets/andrewmvd/corruption-perceptions-index>
<https://www.kaggle.com/datasets/ealaxi/paysim1>
- Документация GitHub Code Scanning для поиска уязвимостей в коде:
<https://docs.github.com/ru/code-security/code-scanning/introduction-to-code-scanning/about-code-scanning>

Эти ресурсы и примеры кода помогут начать разработку систем автоматического выявления коррупционных и мошеннических схем с использованием анализа данных и машинного обучения.

Заключение

Информационные технологии являются ключевым элементом современной системы профилактики коррупционных и иных правонарушений на государственной гражданской службе. Их применение позволяет повысить эффективность контроля, обеспечить прозрачность и своевременно выявлять коррупционные риски. Для успешного внедрения необходима системная работа, включающая правовое регулирование, развитие информационно-аналитических систем и обучение государственных служащих.

Библиографические ссылки

1. Голоманчук Э. В., Астафурова О. А. Информационные технологии в противодействии коррупции: теория и практика внедрения. // Безопасность в современном мире. 2019.
2. Цифровые технологии в области противодействия коррупции. Доклад Программы развития ООН. 2021.
3. Методические материалы по вопросам противодействия коррупции на базе федеральной государственной информационной системы. Государственная Дума РФ.
4. Противодействие коррупции в системе государственной службы. SearchInform.

Противодействие коррупции на государственной службе: учебное пособие. УрФУ.