МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ

МОСКОВСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ГЕОДЕЗИИ И КАРТОГРАФИИ

Отчёт

Коммерческая организация «Салон красоты»

Выполнил: Студент группы ИБ3-1б Лысенко Анна Сергеевна

Проверил преподаватель: Сверлов Егор Дмитриевич

Москва 2024

СОДЕРЖАНИЕ

[ЦЕЛЬ РАБОТЫ 3](#_Toc181632455)

[СОЗДАНИЕ РЕПОЗИТОРИЯ 4](#_Toc181632456)

[РАЗРАБОТКА СЦЕНАРИЕВ MITRE ATT&CK 5](#_Toc181632457)

[РАБОТА С БДУ ФСТЭК 6](#_Toc181632458)

[ПОДНЯТИЕ СИСТЕМЫ 19](#_Toc181632459)

[ВЫВОД 20](#_Toc181632460)

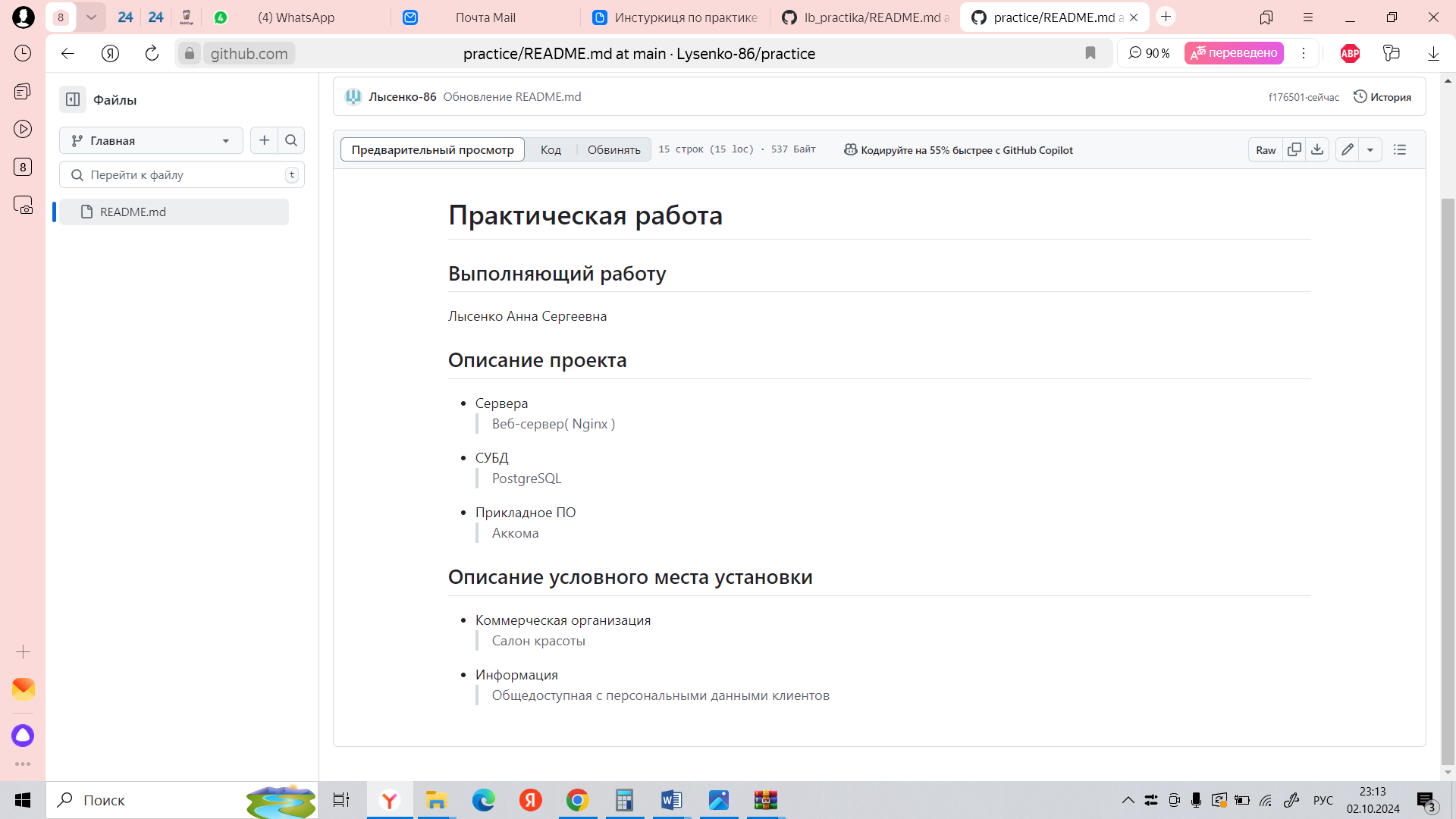
# ЦЕЛЬ РАБОТЫ

Целью работы является практической деятельности по анализу и оценке информационных систем. Студент должен создать собственные репозитории Git для выполнения различных заданий, включая создание схемы системы, разработку сценариев атак с использованием матрицы Mitre ATT&CK и работу с моделью угроз, основанной на методике ФСТЭК. Работа направлена на практическое применение знаний в области информационной безопасности и управление проектом, включающим анализ систем и угроз, разработку документации и защиту информационных систем в учебной среде.

# СОЗДАНИЕ РЕПОЗИТОРИЯ

Для выполнения практической работы я выбрала коммерческую организацию «Салон красоты». Мной был организован собственный репозиторий Git, в который выгружались отчеты при выполнении работы.

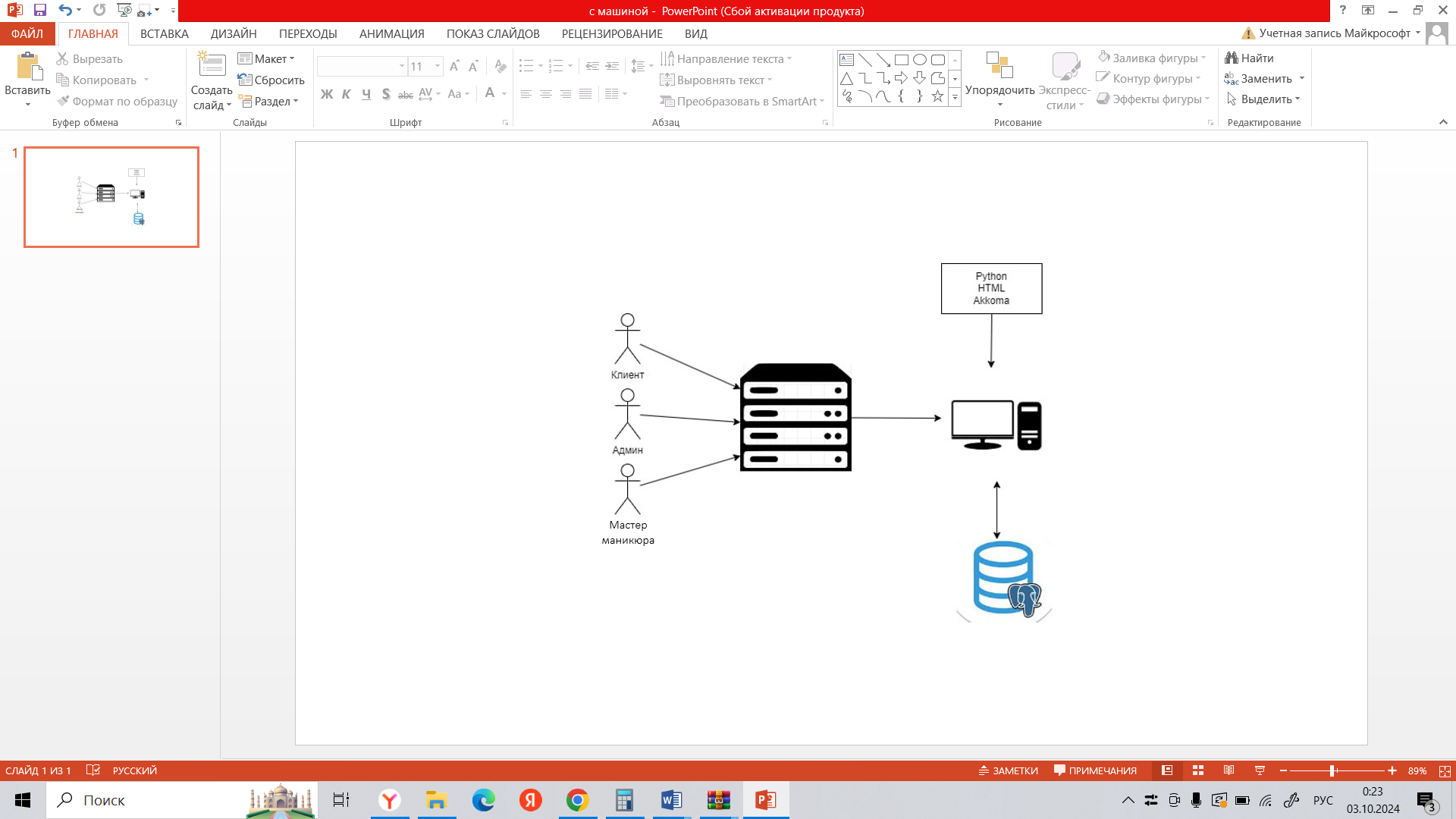
**Ссылка на репозиторий:** <https://github.com/Lysenko-86/practice/blob/main/README.md>

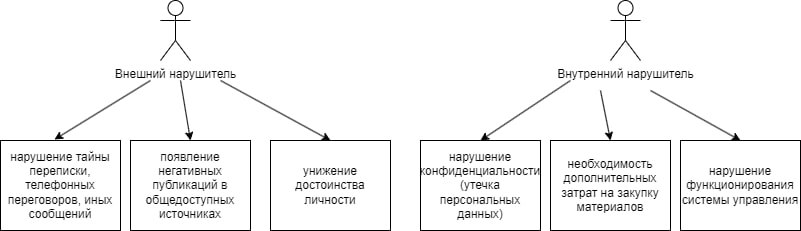


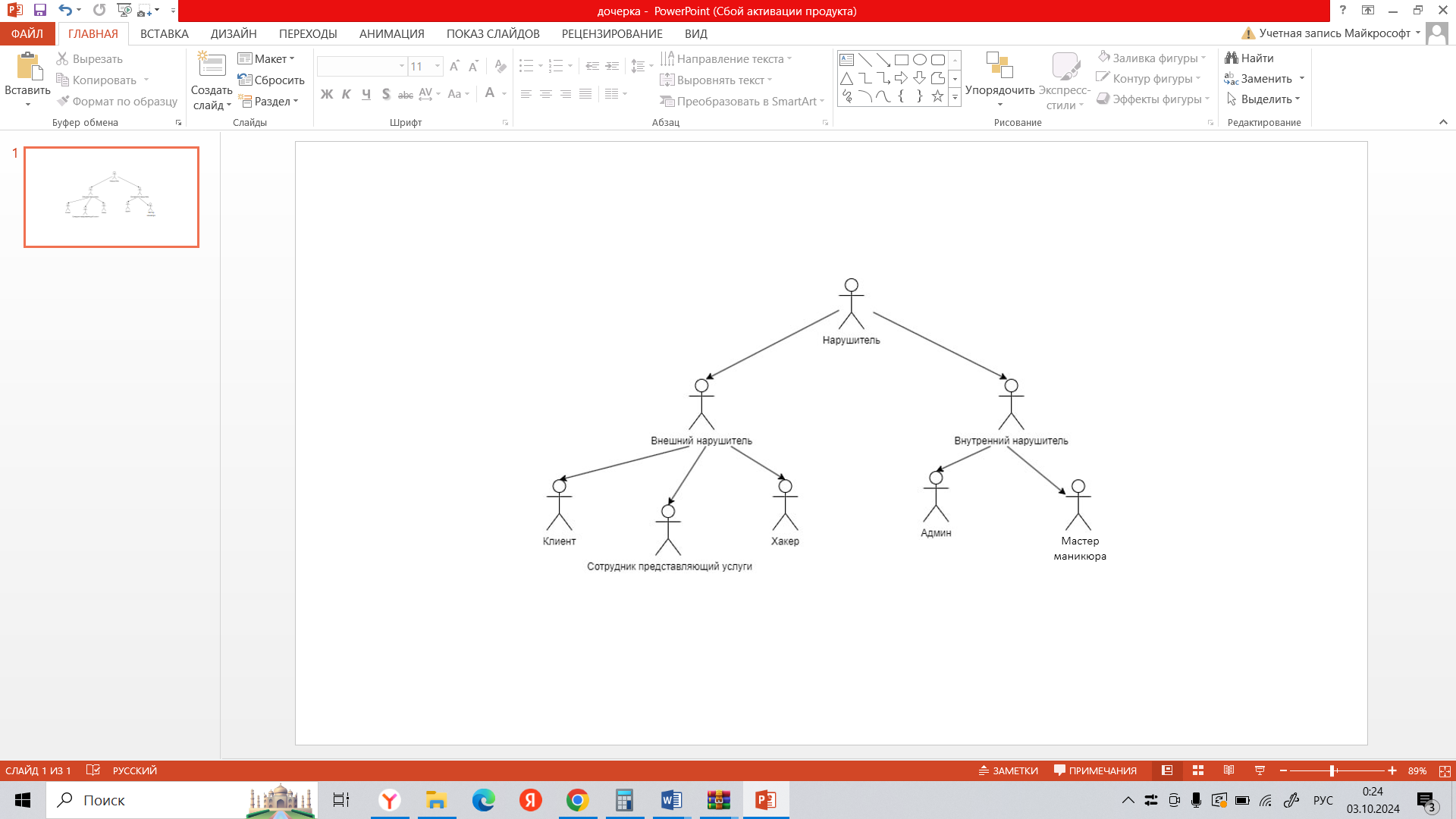
# РАЗРАБОТКА СЦЕНАРИЕВ MITRE ATT&CK

На данном этапе задачей является разработка 10-ти сценариев на основе Mitre ATT&CK, а также построение схемы взаимодействия компонентов системы и поднятие ИС. Я выбрала следующие сценарии – Компрометация, фишинг голосом, троян, вредоносное и вымогающее ПО (2, 3, 4, 5, 9 архив).

Сценарии в ATT&CK Navigator и их краткое объяснение приложены в работе в виде zip-файлов.



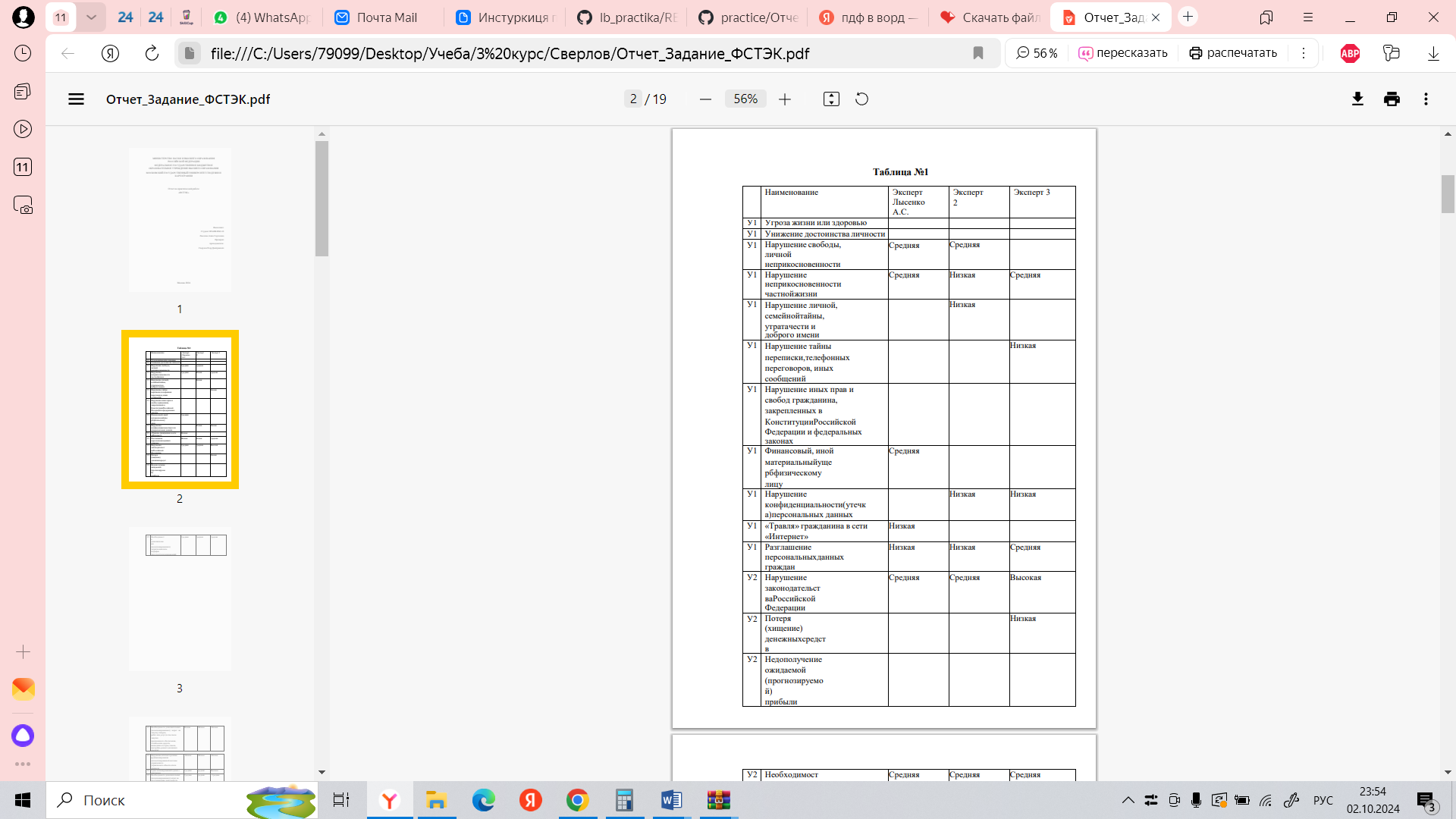


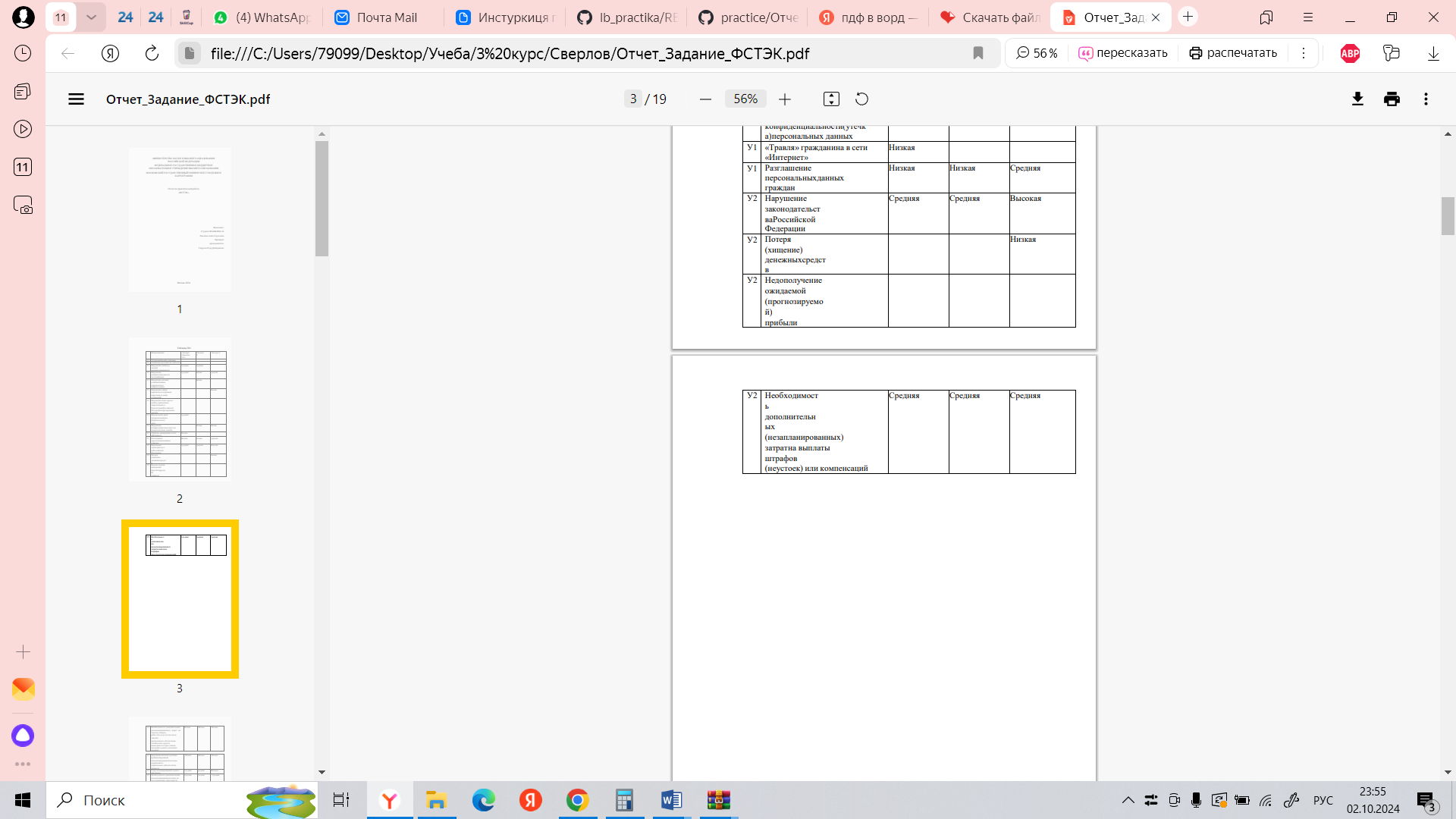


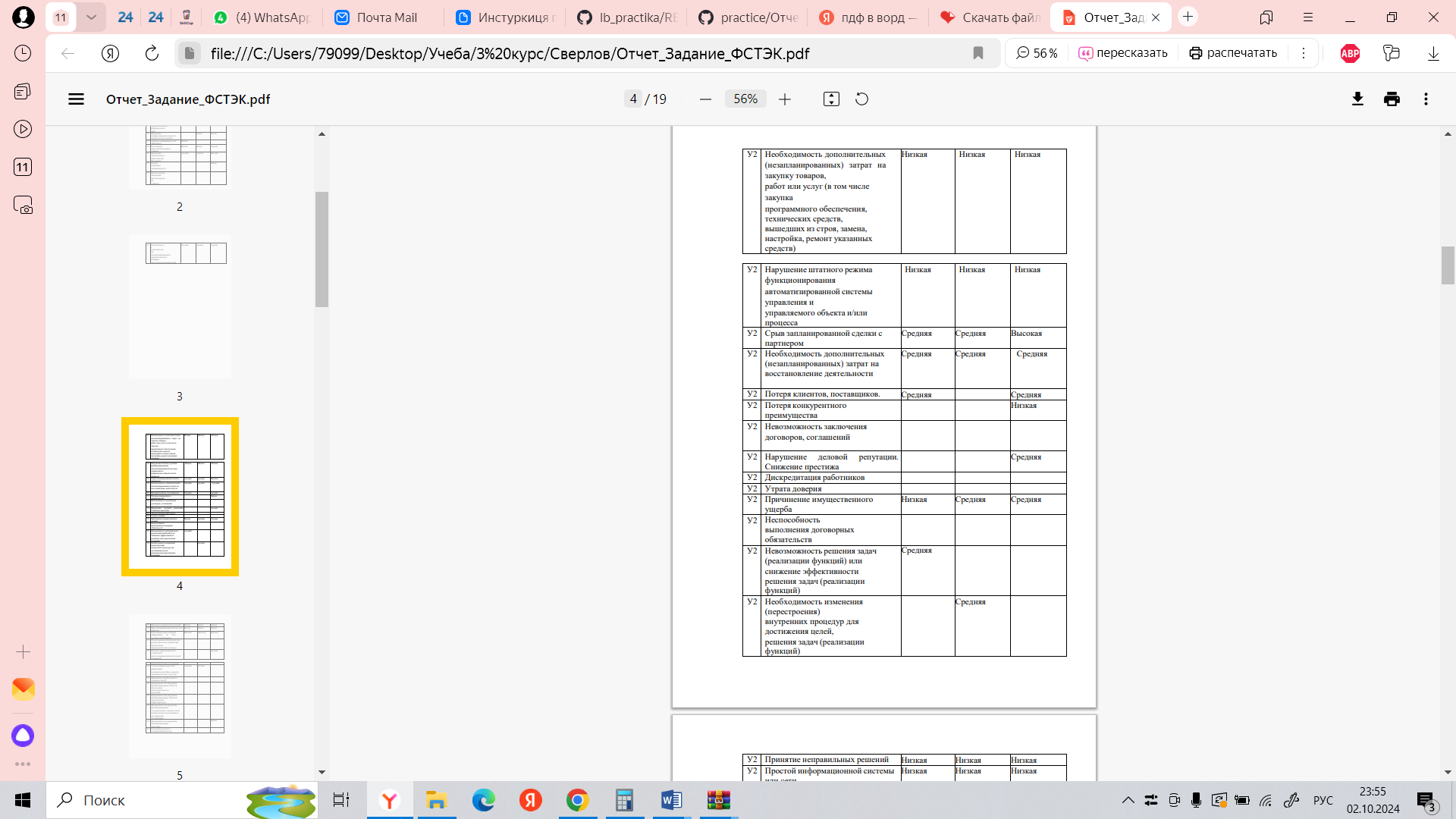
# РАБОТА С БДУ ФСТЭК

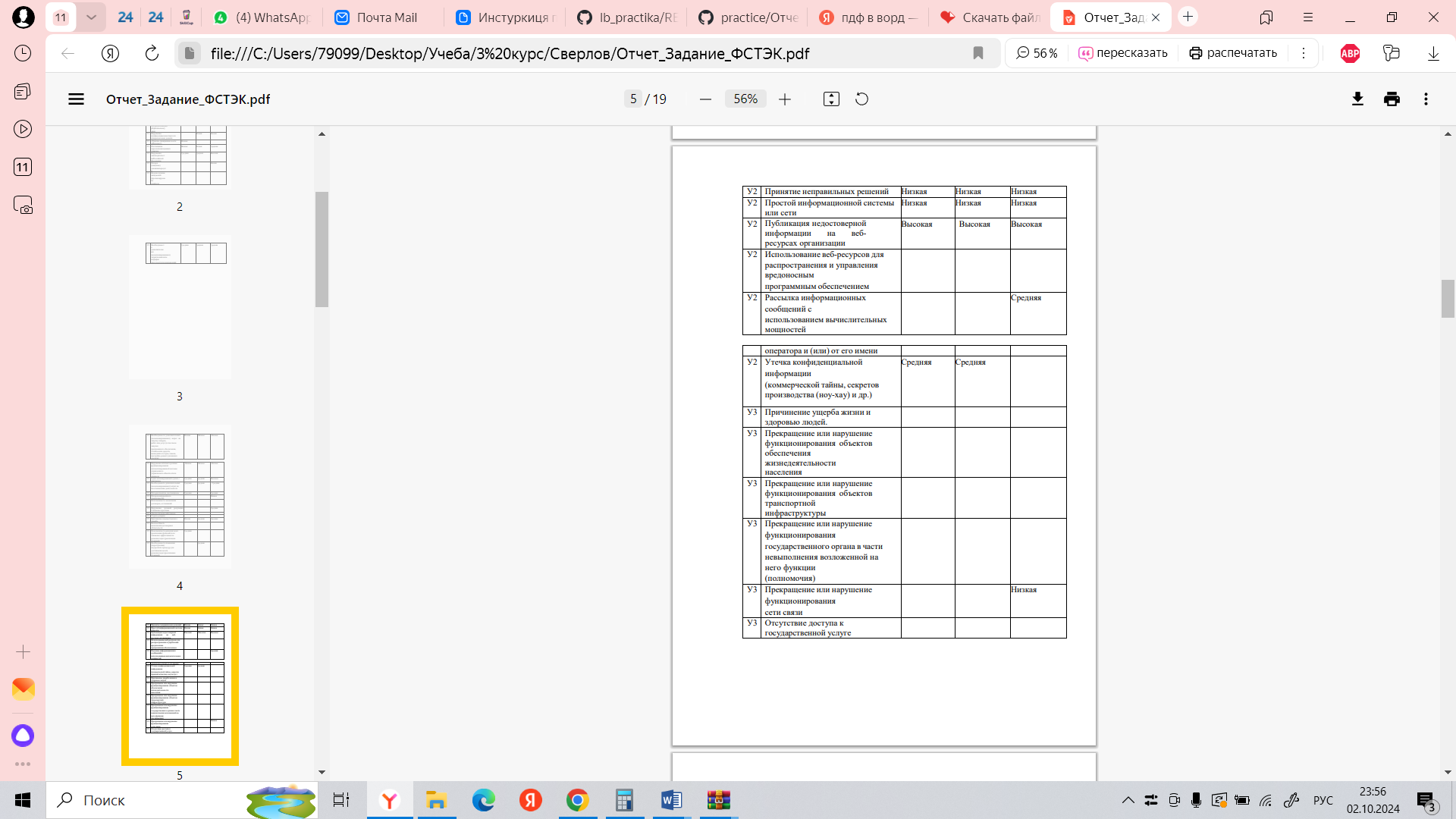
При выполнении данной задачи я использовала различные методические материалы, а также информацию, полученную с профессиональных веб-ресурсов. Ознакомившись с необходимыми источниками и проанализировав полученные данные, я приступила к созданию таблиц, и свой результат я представила в таблице 1

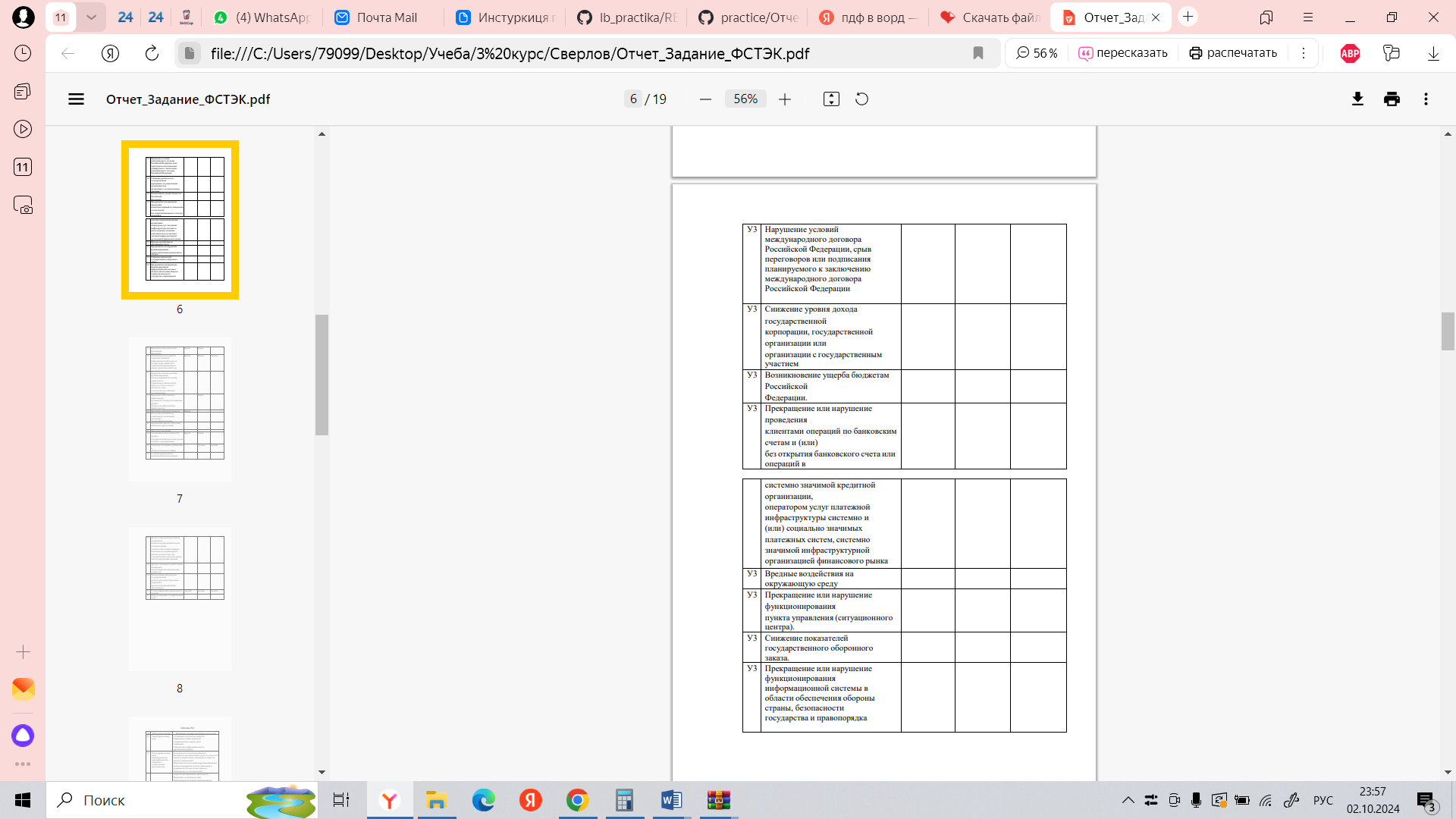
Таблица 1- оценка рисков

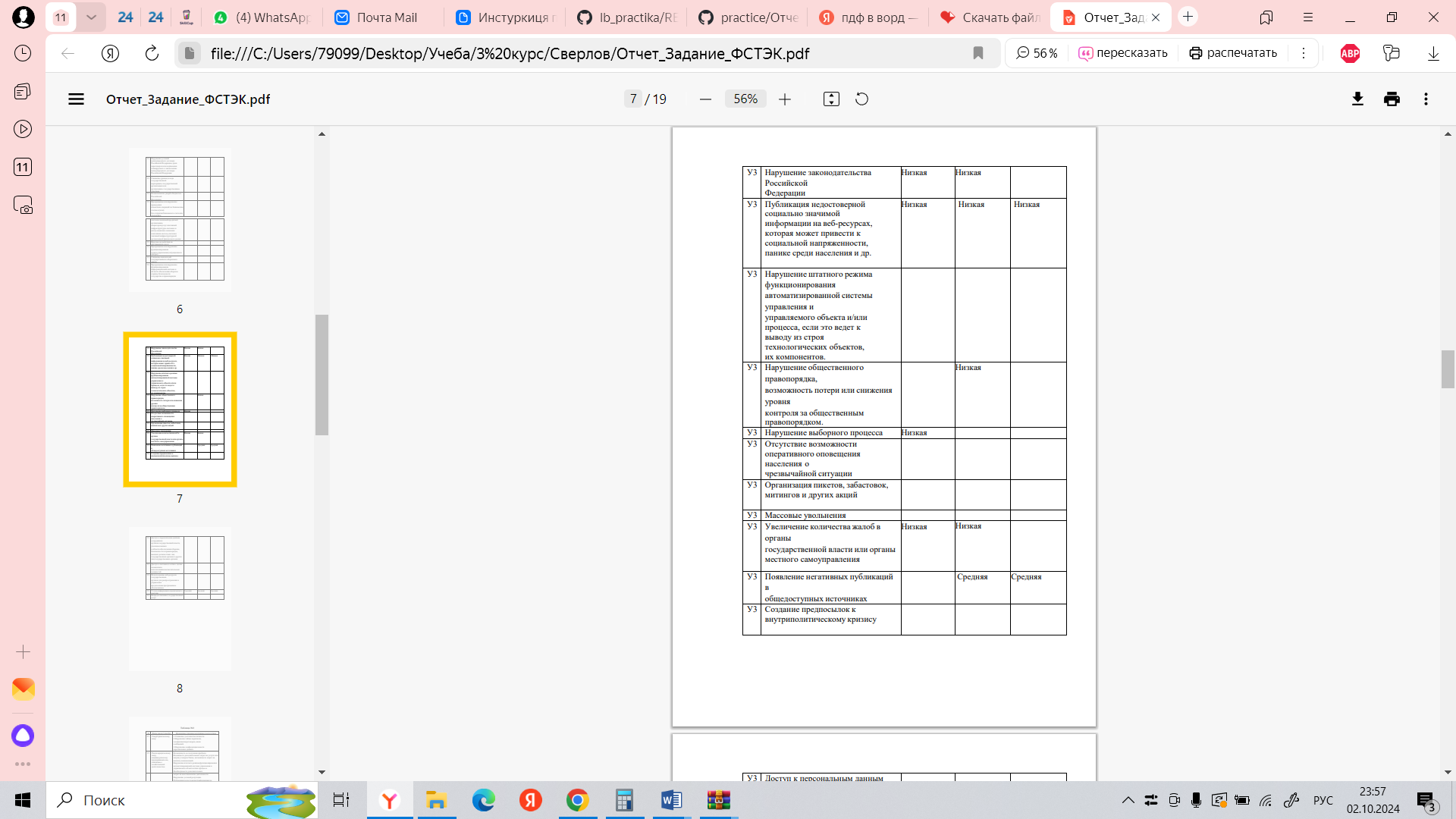


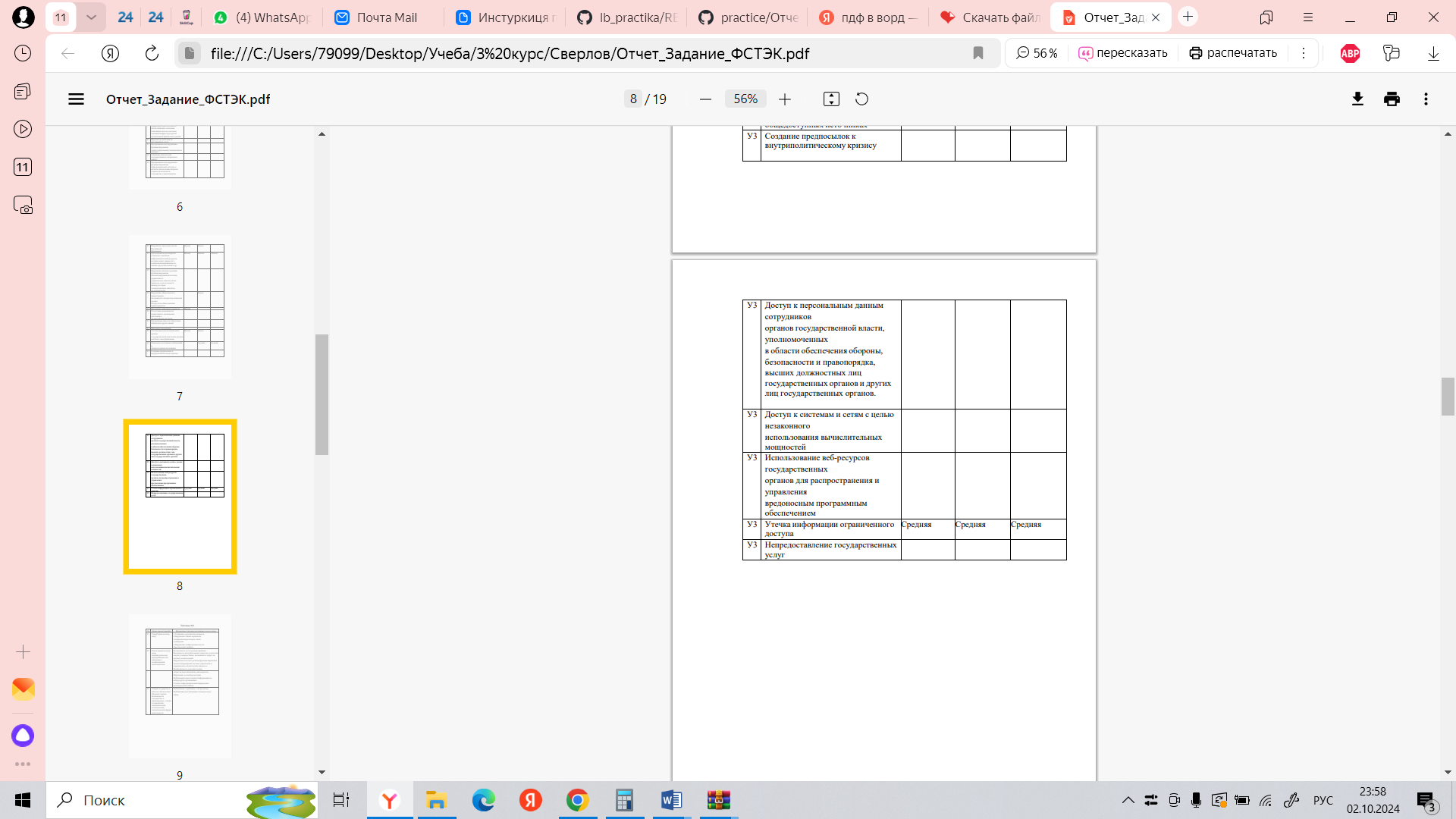












Далее по видам риска (ущерба) были даны возможные негативные последствия, а по виду нарушителя определила цели реализации угроз – Таблица 2

Таблица 2

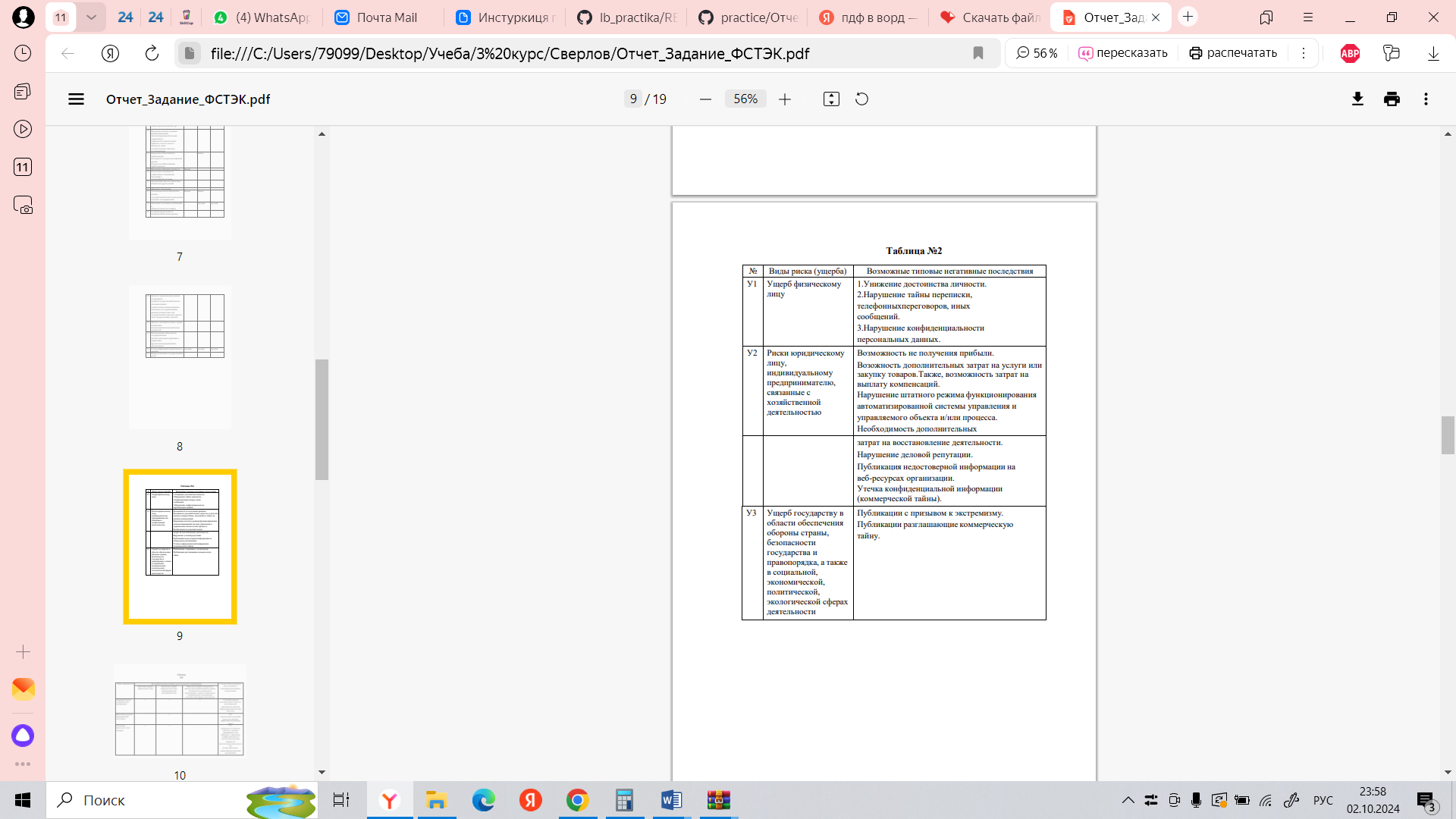
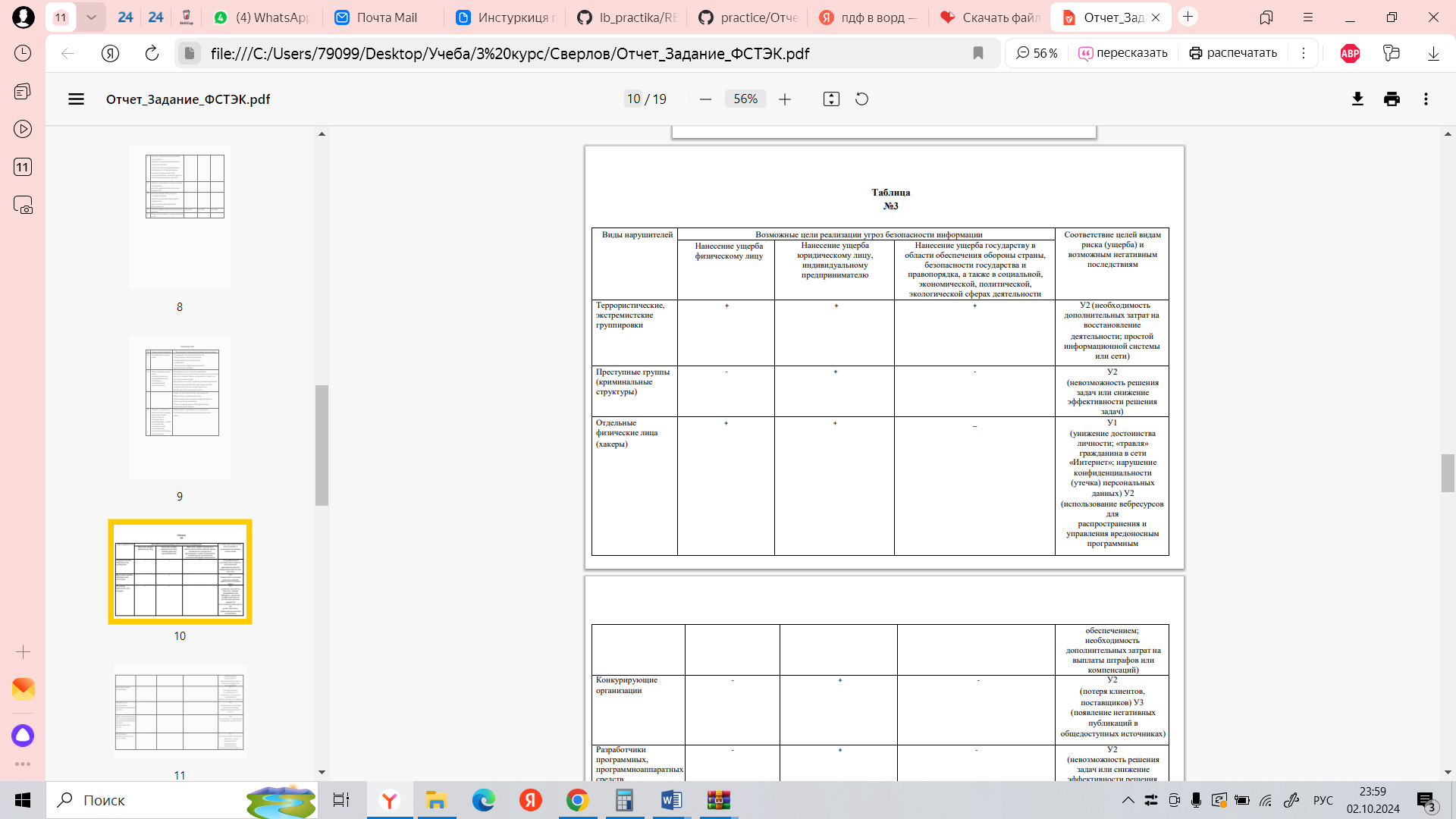
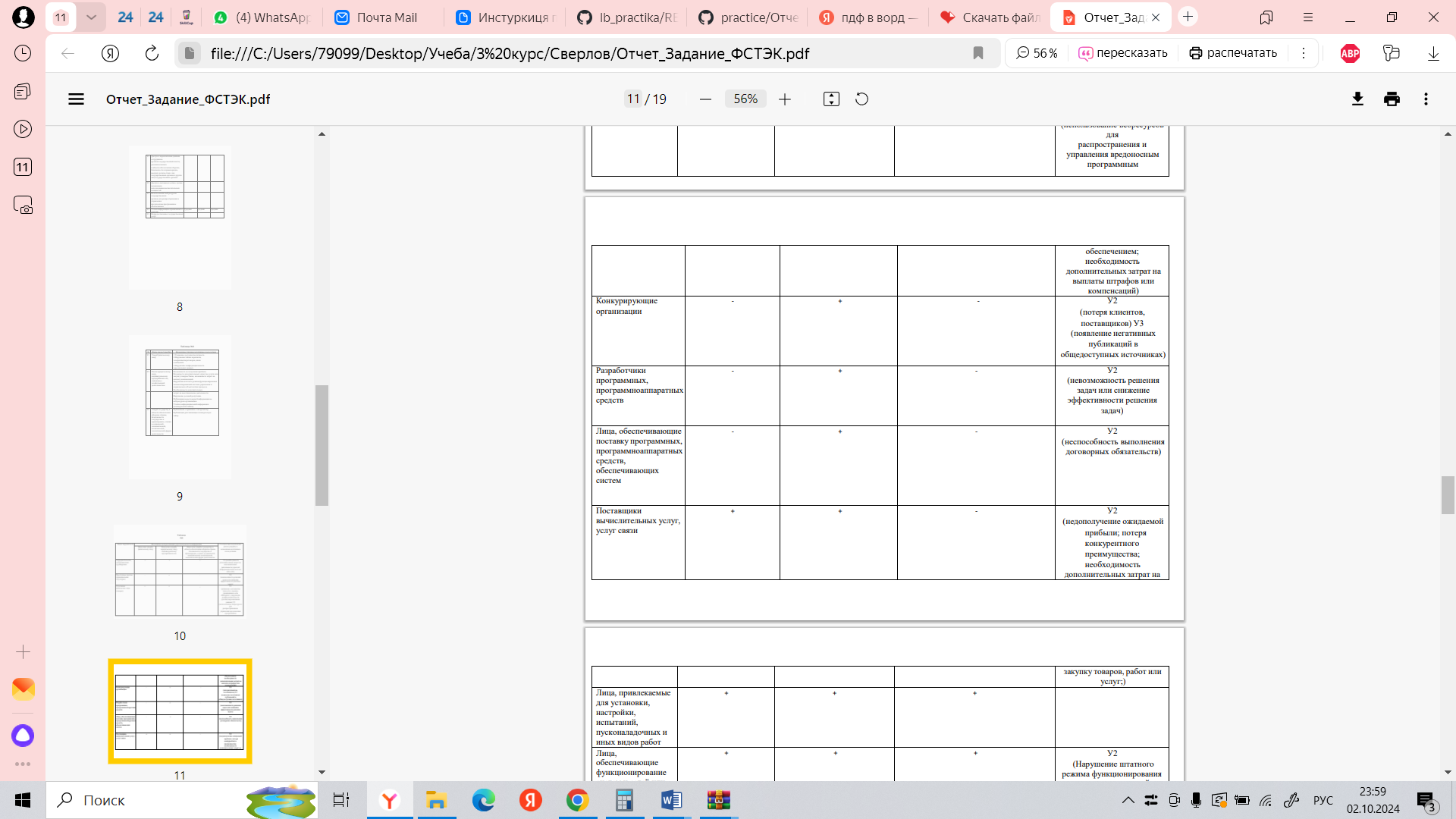
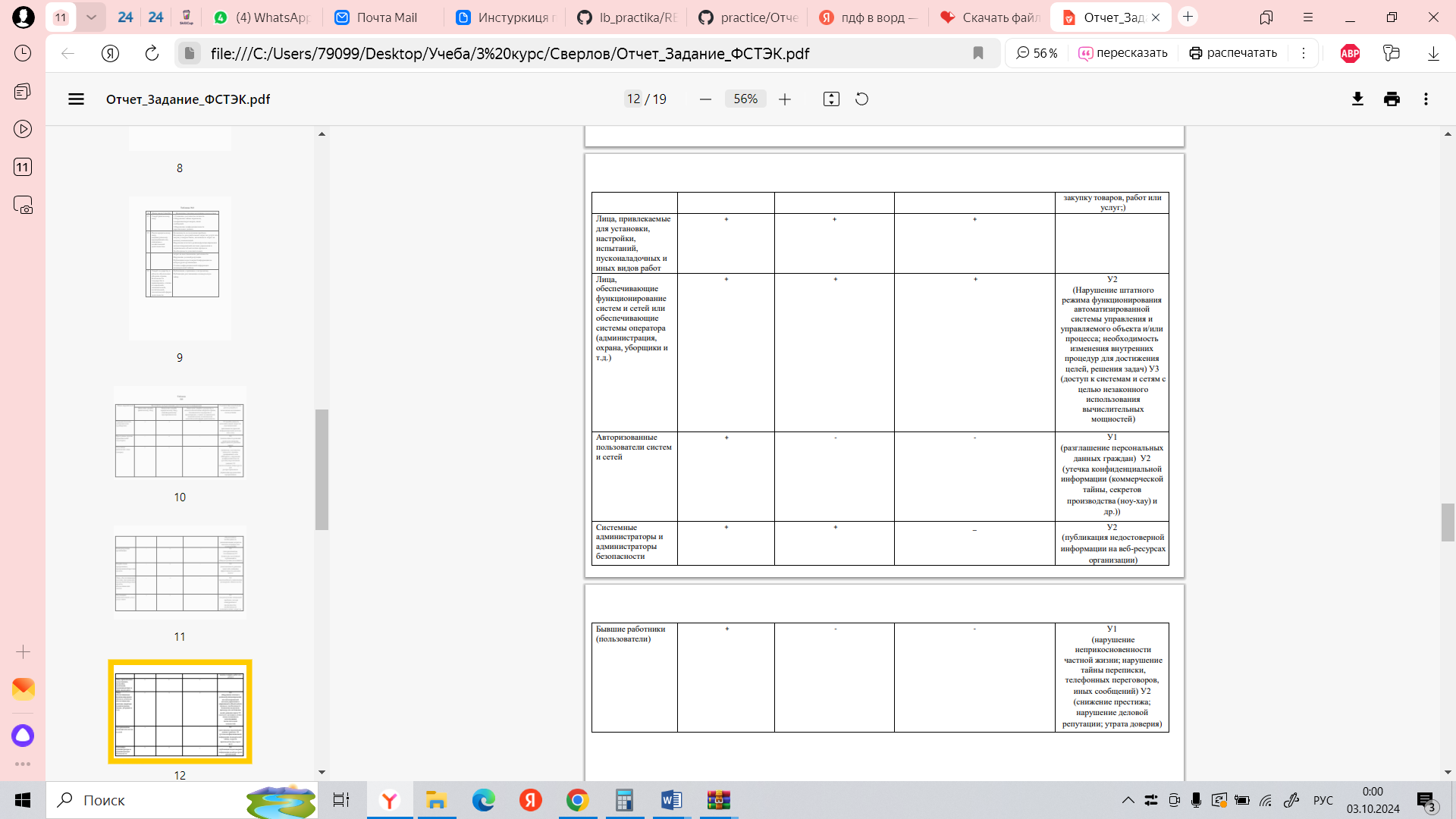


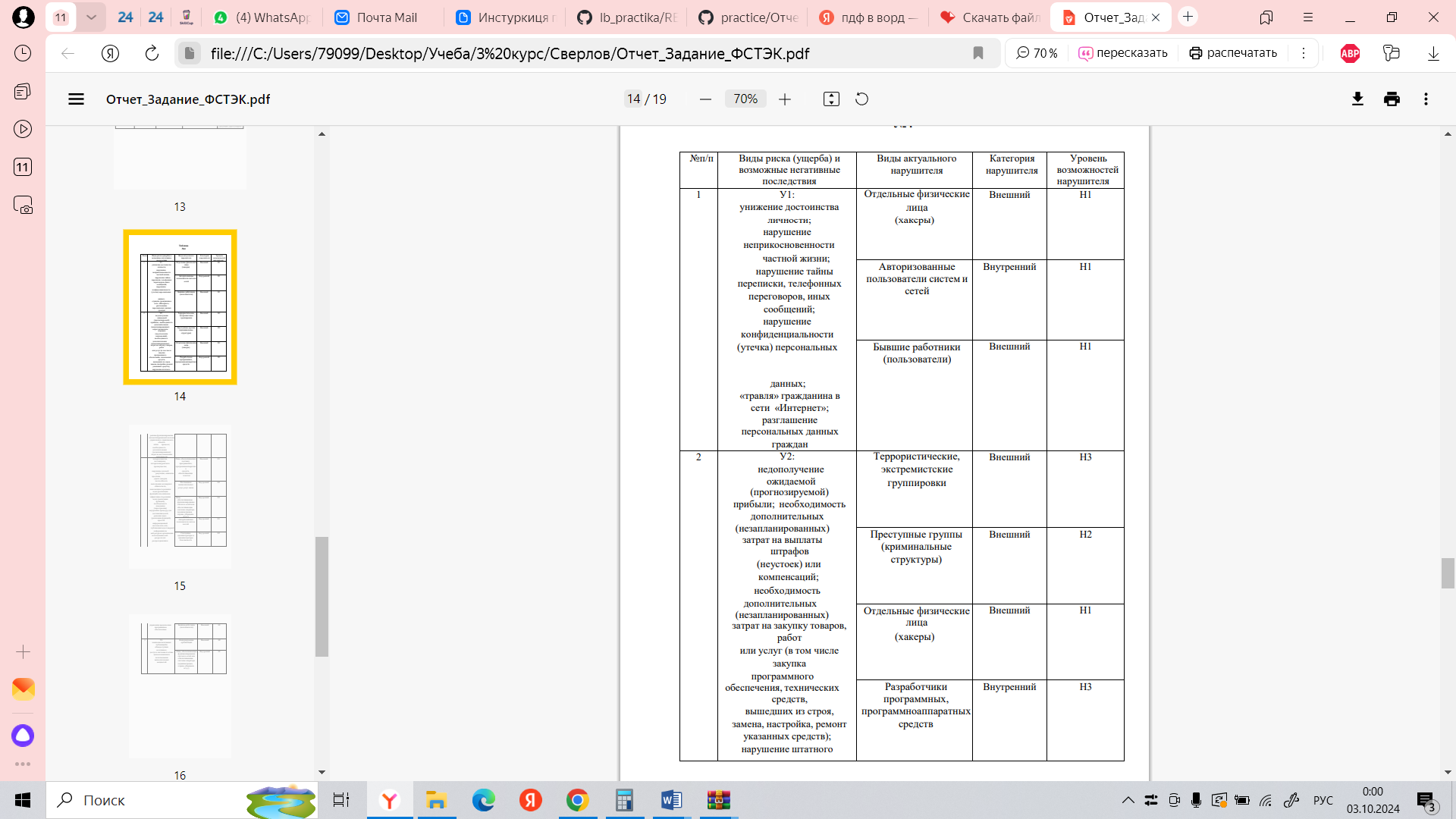
Рисунок 3

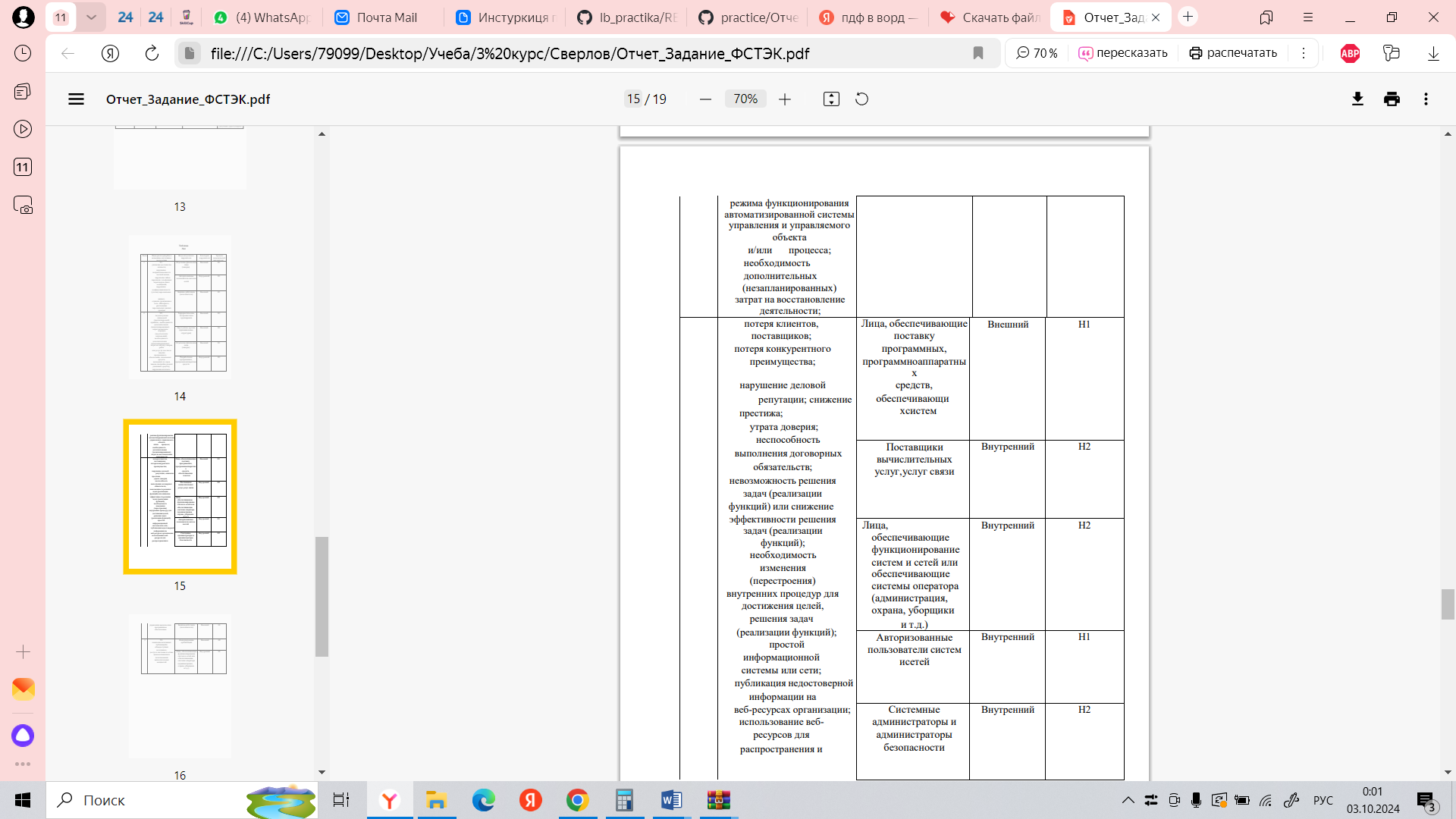


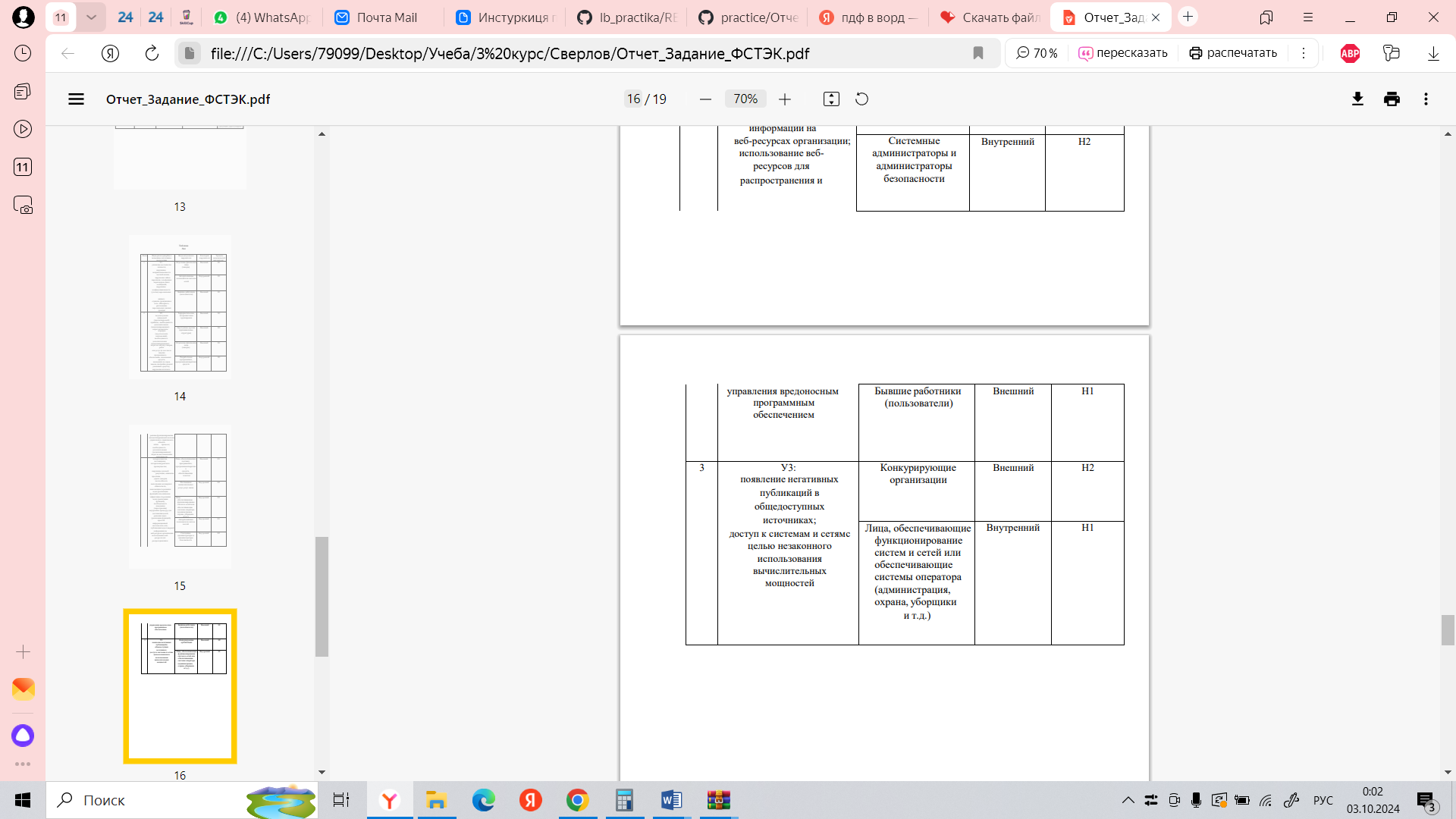




Далее я выделила виды, категорию и уровень нарушителя – Таблица 2

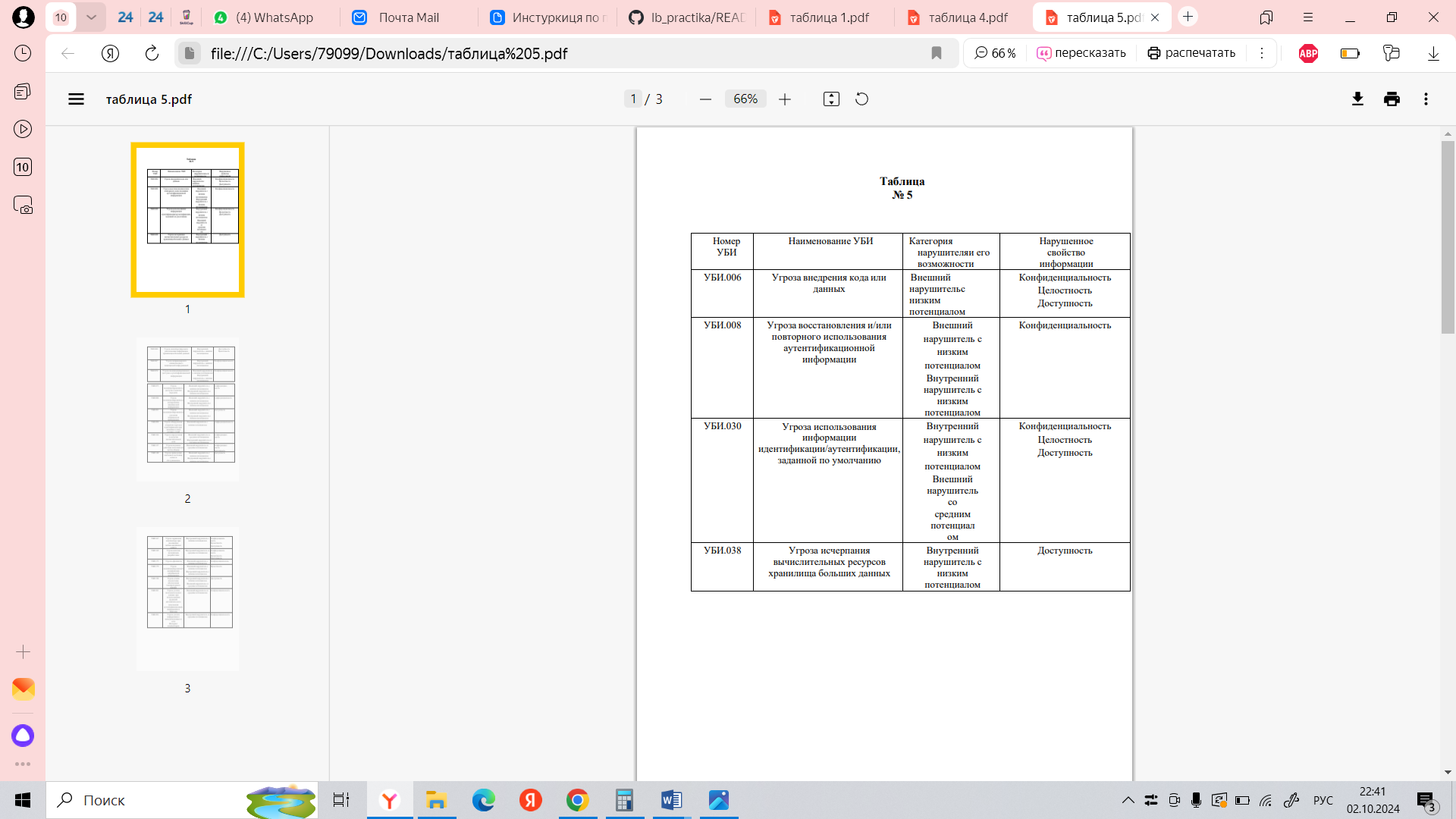
Таблица 2- Виды, категорию и уровень нарушителя

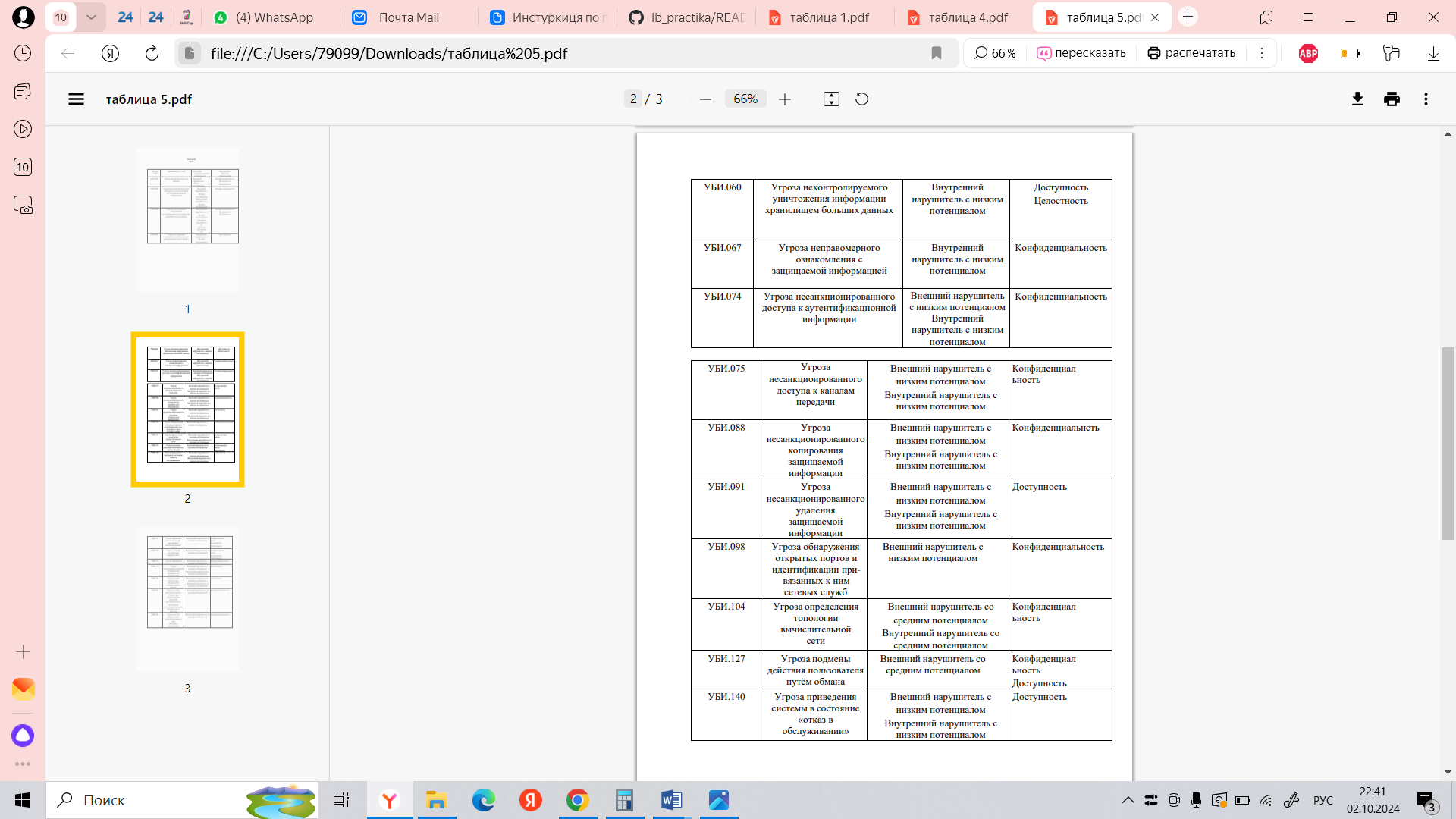


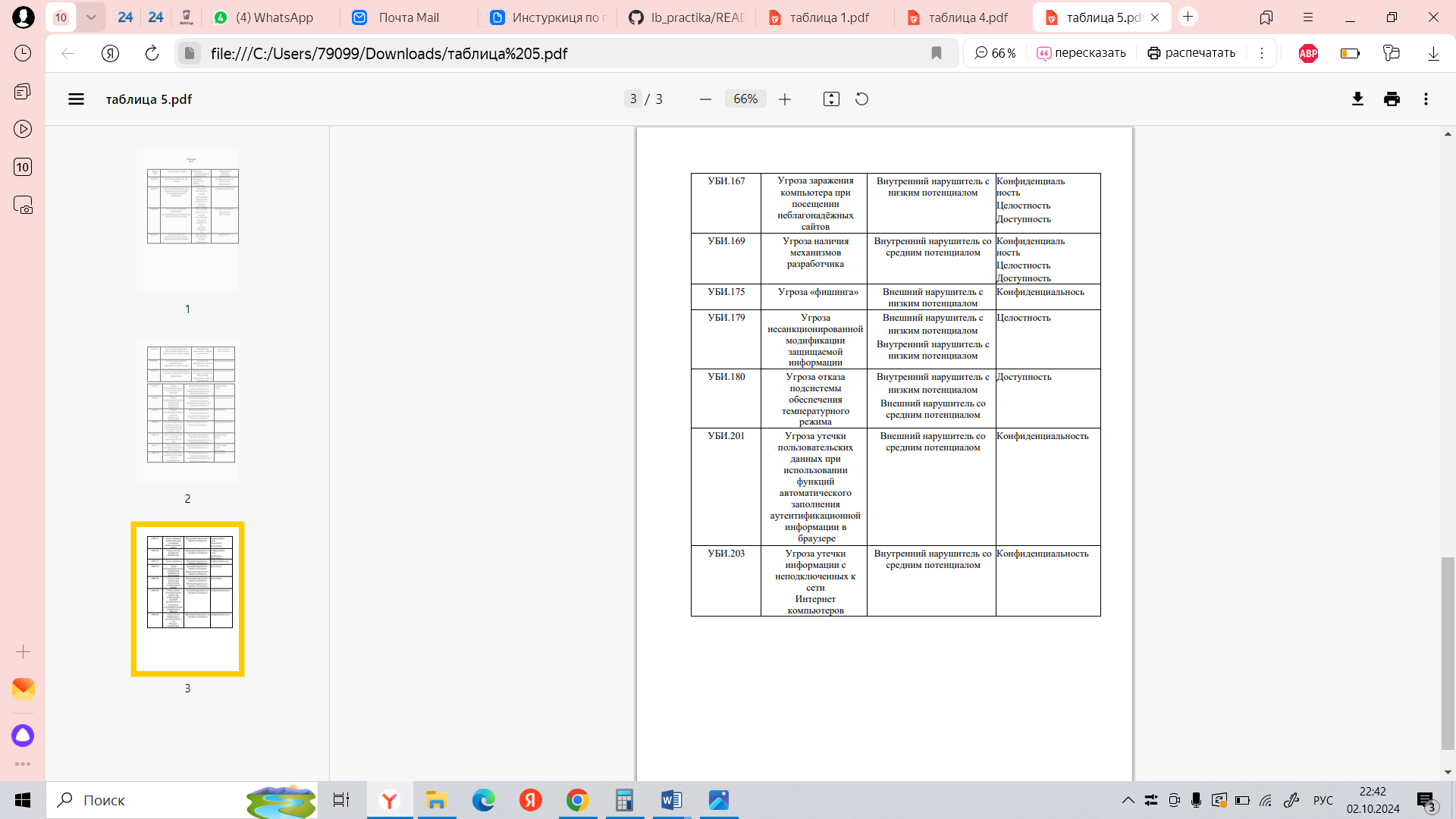


Далее я сформировала перечень возможных к реализации угроз безопасности- Таблица 3

Таблица 3- Перечень возможных к реализации угроз безопасности







# ПОДНЯТИЕ СИСТЕМЫ

В ходе работы я столкнулась с проблемой: после регистрации нового пользователя в системе Akkoma подтверждающее письмо на электронную почту не пришло. Я предположила, что проблема может быть в SMTP.

Сначала я решила просмотреть журналы Docker, чтобы найти дополнительные сведения о проблеме. Выполнив команду sudo docker-compose logs akkomaв терминале, я увидела сбой в соединении с SMTP-сервером (может быть адрес сервера или порт подключения)

Далее я решила подключить вручную . Для этого я ввела команду telnet. Соединение не удалось установить.

Таким образом, оба способа подтвердили, что проблема связана с некорректными настройками SMTP. Из-за этого я не смогла получить подтверждающее письмо и провести проверку системы.

# ВЫВОД

В результате выполнения работы я получила практический опыт в развёртывании и настройке информационных систем. Выполнение задания с матрицей Mitre ATT&CK дало возможность подробно проработать сценарии атак, улучшить понимание структуры стратегии и методов их моделирования. Также я изучала методику ФСТЭК для построения моделей угроз и нарушителей, что укрепило мои навыки анализа и оценки риска