МЕТОДИЧЕСКИЕ УКАЗАНИЯ ПО ИСПОЛЬЗОВАНИЮ КОНКУРСНОГО ПРОЕКТА
«Разработка метода интеллектуального анализа рисков информационной безопасности в ИТ-организации»

Образовательная организация: филиал ФГБОУ ВО «НИУ «МЭИ» в г. Смоленске
Автор: Дроздов Никита Владимирович
Куратор: Булыгина Ольга Валентиновна (доктор экономических наук, доцент кафедры Информационных технологий в экономике и управлении)

СОДЕРЖАНИЕ

1 Работа с интерфейсом в Google Colab и локальном Jupyter.....1
2 Работа с интерфейсом через веб-приложение.....14
Важные моменты.....26

1 Работа с интерфейсом в Google Colab и локальном Jupyter

После успешного выполнения 12-й ячейки в Google Colab или ячейки в файле «interface.ipynb» при локальном запуске (см. п. 1 и 2 инструкции) под блоком кода появится интерактивная панель управления. Интерфейс в обоих случаях абсолютно идентичен и состоит из двух основных вкладок: «Данные» и «Анализ» (рисунки 1 и 2).

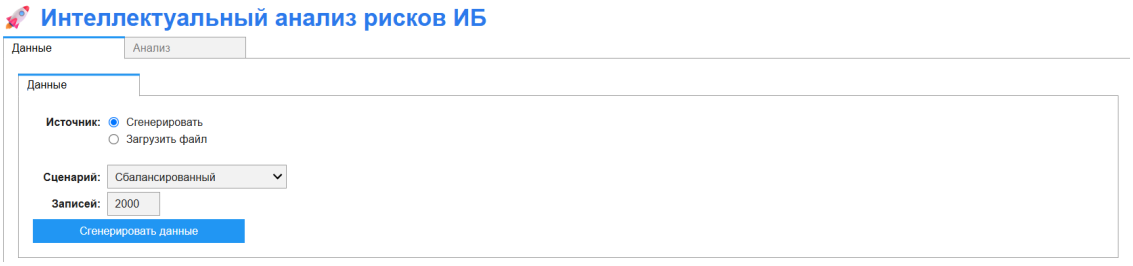


Рисунок 1 – Вкладка «Данные»

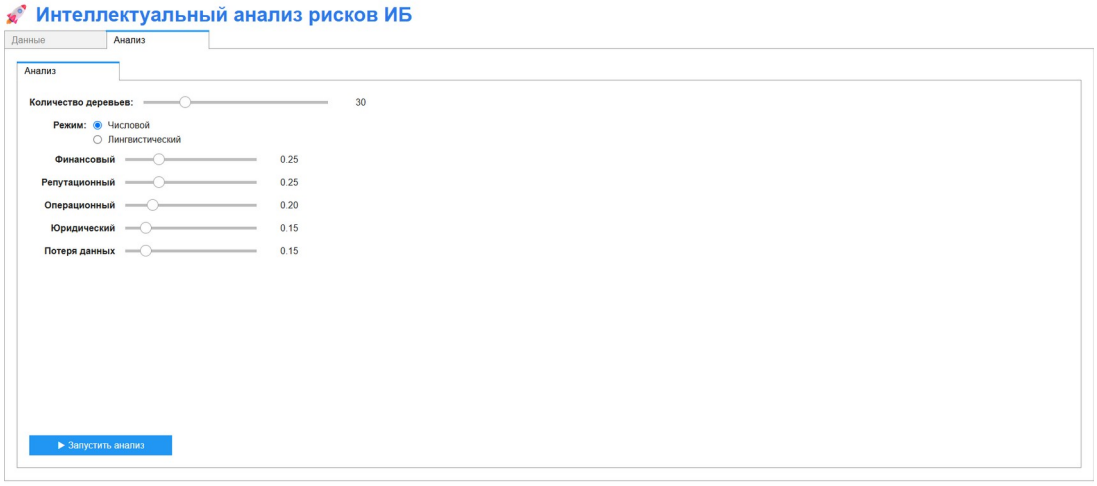


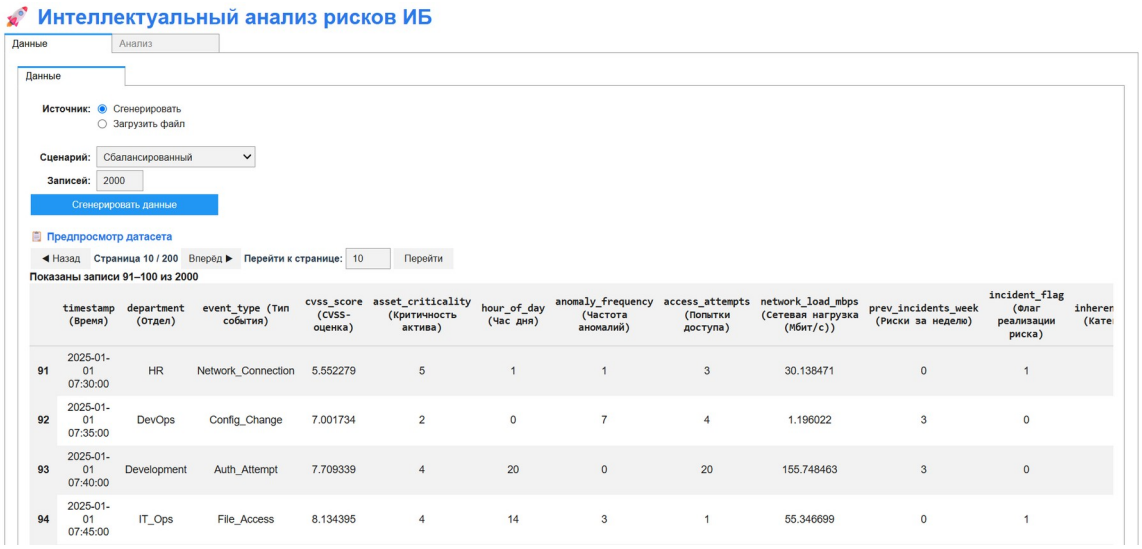
Рисунок 2 – Вкладка «Анализ»

Вкладка «Данные» – на данной вкладке осуществляется подготовка исходной информации для анализа.

В блоке «Источник» выберите один из двух режимов:

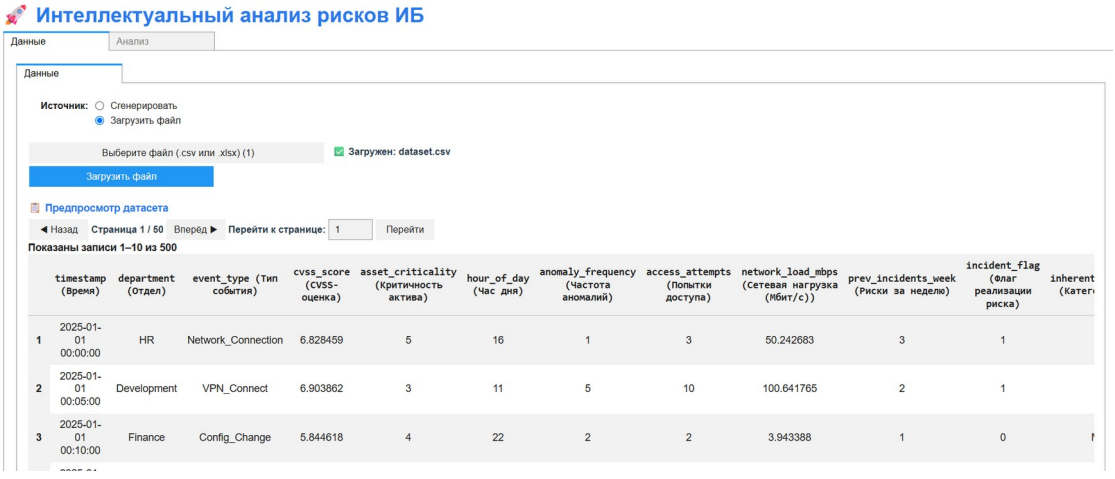
- «Сгенерировать» – позволяет создать синтетический датасет. В открывшемся меню выберите сценарий (Сбалансированный, Высокие риски или Низкие риски) и укажите необходимое количество записей (от 100 до 100 000).
- «Загрузить файл» – позволяет использовать собственные данные. Нажмите на кнопку выбора файла и укажите документ в формате «.csv» или «.xlsx». Загружаемый файл должен содержать обязательные столбцы (время, отдел, тип события, CVSS-оценка, критичность актива и др.).

Нажмите кнопку «Сгенерировать данные» или «Загрузить файл». Дождитесь появления таблицы предпросмотра датасета. Для навигации по строкам используйте кнопки «Назад» и «Вперед» или введите номер страницы вручную. На рисунках 3 и 4 представлены режимы работы и таблицы предпросмотров.



	timestamp (Время)	department (Отдел)	event_type (Тип события)	cvss_score (CVSS-оценка)	asset_criticality (Критичность актива)	hour_of_day (Час дня)	anomaly_frequency (Частота аномалий)	access_attempts (Попытки доступа)	network_load_mbps (Сетевая нагрузка (Мбит/с))	prev_incidents_week (Риски за неделю)	incident_flag (Флаг реализации риска)	inherer (Кате
91	2025-01-01 07:30:00	HR	Network_Connection	5.552279	5	1	1	3	30.138471	0	1	
92	2025-01-01 07:35:00	DevOps	Config_Change	7.001734	2	0	7	4	1.196022	3	0	
93	2025-01-01 07:40:00	Development	Auth_Attempt	7.709339	4	20	0	20	155.748463	3	0	
94	2025-01-01 07:45:00	IT_Ops	File_Access	8.134395	4	14	3	1	55.346699	0	1	

Рисунок 3 – Режим генерации датасета



	timestamp (Время)	department (Отдел)	event_type (Тип события)	cvss_score (CVSS-оценка)	asset_criticality (Критичность актива)	hour_of_day (Час дня)	anomaly_frequency (Частота аномалий)	access_attempts (Попытки доступа)	network_load_mbps (Сетевая нагрузка (Мбит/с))	prev_incidents_week (Риски за неделю)	incident_flag (Флаг реализации риска)	inherent (Катег
1	2025-01-01 00:00:00	HR	Network_Connection	6.828459	5	16	1	3	50.242683	3	1	
2	2025-01-01 00:05:00	Development	VPN_Connect	6.903862	3	11	5	10	100.641765	2	1	
3	2025-01-01 00:10:00	Finance	Config_Change	5.844618	4	22	2	2	3.943388	1	0	

Рисунок 4 – Режим загрузки датасета

Вкладка «Анализ» – данная вкладка предназначена для конфигурирования параметров модели и запуска расчетов.

С помощью ползунка задайте «Количество деревьев» в ансамбле (от 10 до 100). В блоке «Режим» выберите способ задания экспертной оценки ущерба:

- «Числовой» – используйте ползунки для каждой из пяти категорий ущерба (финансовый, репутационный, операционный, юридический, потеря данных), чтобы задать их веса. Программа автоматически нормирует значения.
- «Лингвистический» – выберите качественные оценки (от «Очень низкого» до «Критического») из выпадающих списков для каждой категории.

Нажмите кнопку «Запустить анализ». Ожидайте конца анализа, в это время над полосой прогресса будут сменяться сообщения о статусе (например, «Обучение деревьев (15/30)...»). Дождитесь заполнения шкалы на 100% и появления сообщения об успешном завершении. На рисунках 5-8 представлены режимы задания экспертной оценки и процесс анализа.

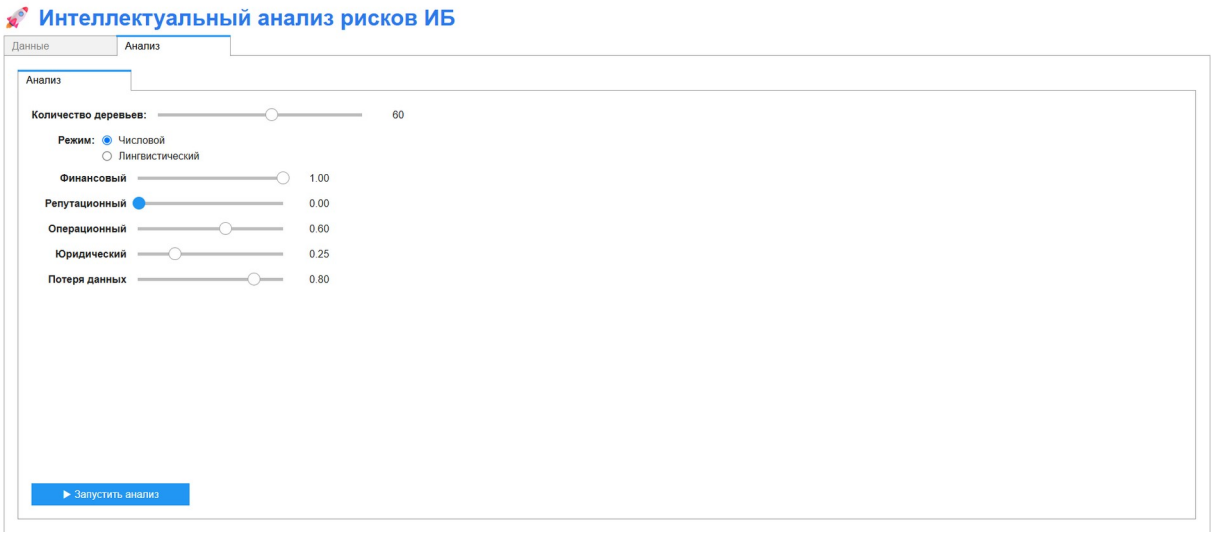


Рисунок 5 – Задание экспертной оценки в числовом режиме

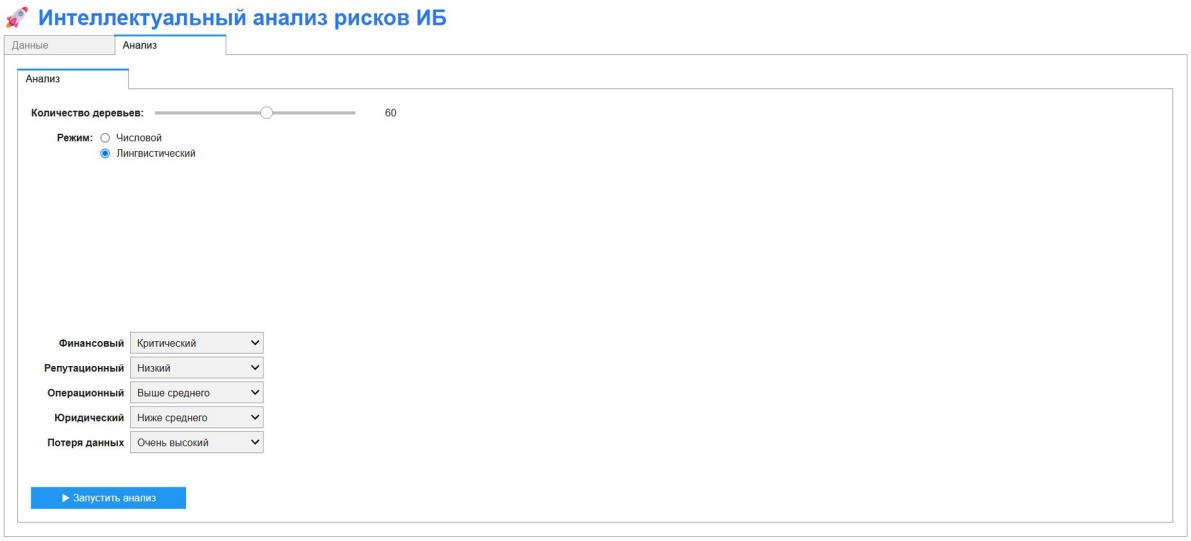


Рисунок 6 – Задание экспертной оценки в лингвистическом режиме

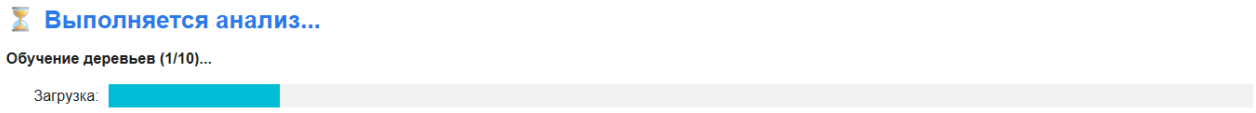


Рисунок 7 – Выполнение анализа



Рисунок 8 – Завершение анализа

Просмотр результатов – после завершения анализа автоматически откроется страница результатов.

В верхней части страницы отображаются метрики качества модели (Accuracy, F1, AUC), таблица экспертных весов ущерба и таблица рекомендаций по обработке рисков. Для скачивания отчетов используйте кнопки «Скачать CSV», «Скачать HTML» или «Скачать PDF» (рисунки 9-14).

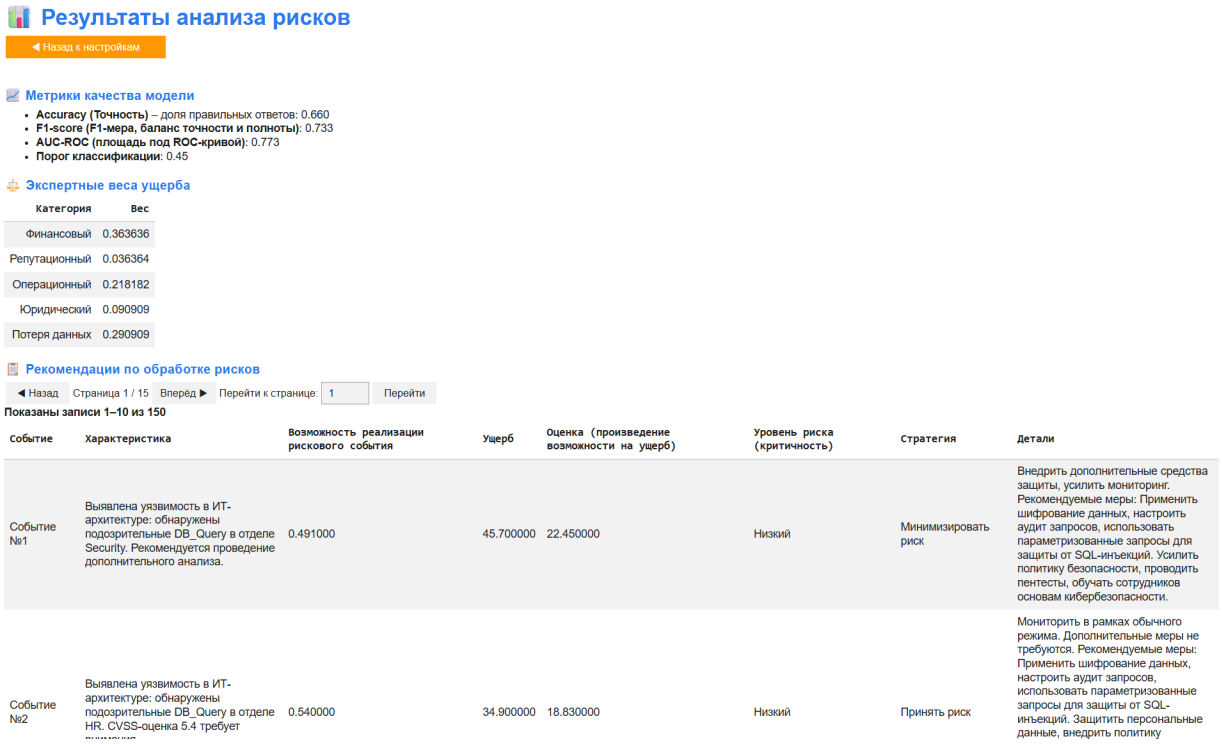


Рисунок 9 – Метрики, веса ущерба и рекомендации по обработке рисков

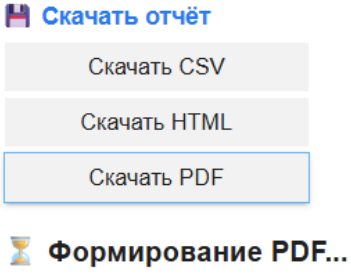


Рисунок 10 – Формирование отчета

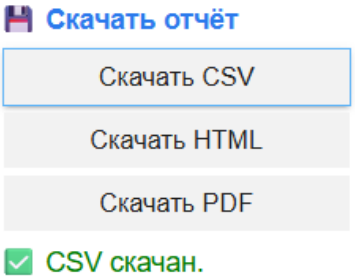


Рисунок 11 – Скачивание отчета

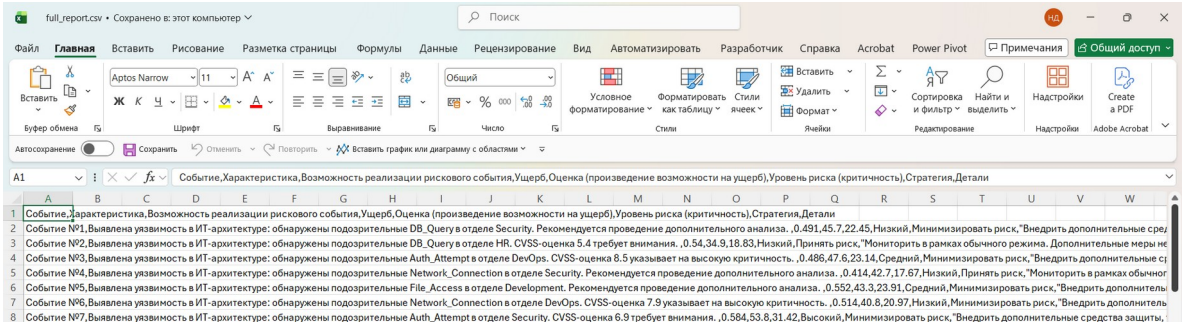
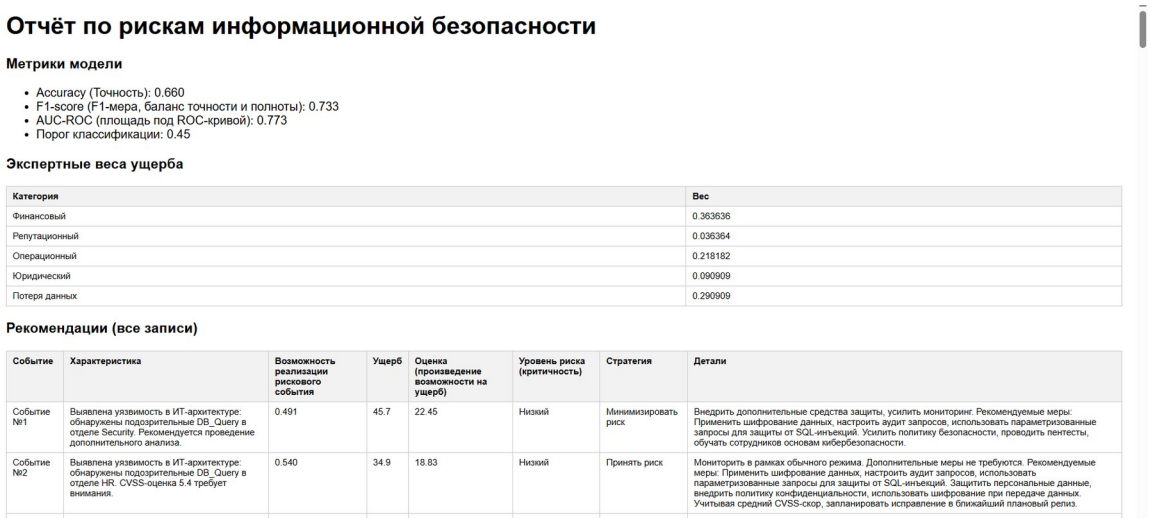


Рисунок 12 – Отчет в формате CSV



Отчёт по рискам информационной безопасности

Метрики модели

- Accuracy (Точность): 0.660
- F1-score (F1-мера, баланс точности и полноты): 0.733
- AUC-ROC (площадь под ROC-кривой): 0.773
- Порог классификации: 0.45

Экспертные веса ущерба

Категория	Вес
Финансовый	0.363636
Репутационный	0.036364
Операционный	0.218182
Юридический	0.090909
Потеря данных	0.290909

Рекомендации (все записи)

Событие	Характеристика	Возможность реализации рискового события	Ущерб	Оценка (произведение возможности на ущерб)	Уровень риска (критичность)	Стратегия	Детали
Событие №1	Выявлена уязвимость в ИТ-архитектуре: обнаружены подозрительные DB_Query в отделе Security. Рекомендуется проведение дополнительного анализа.	0.491	45.7	22.45	Низкий	Минимизировать риск	Внедрить дополнительные средства защиты, усилить мониторинг. Рекомендуемые меры: Применить шифрование данных, настроить аудит запросов, использовать параметризованные запросы для защиты от SQL-инъекций. Усилить политику безопасности, проводить пентесты, обучать сотрудников основам кибербезопасности.
Событие №2	Выявлена уязвимость в ИТ-архитектуре: обнаружены подозрительные DB_Query в отделе HR. CVSS-оценка 5.4 требует внимания.	0.540	34.9	18.83	Низкий	Принять риск	Мониторить в рамках обычного режима. Дополнительные меры не требуются. Рекомендуемые меры: Применить шифрование данных, настроить аудит запросов, использовать параметризованные запросы для защиты от SQL-инъекций. Защитить персональные данные, внедрить политику конфиденциальности, использовать шифрование при передаче данных. Учитывая средний CVSS-скор, запланировать исправление в ближайший плановый релиз.

Рисунок 13 – Отчет в формате HTML

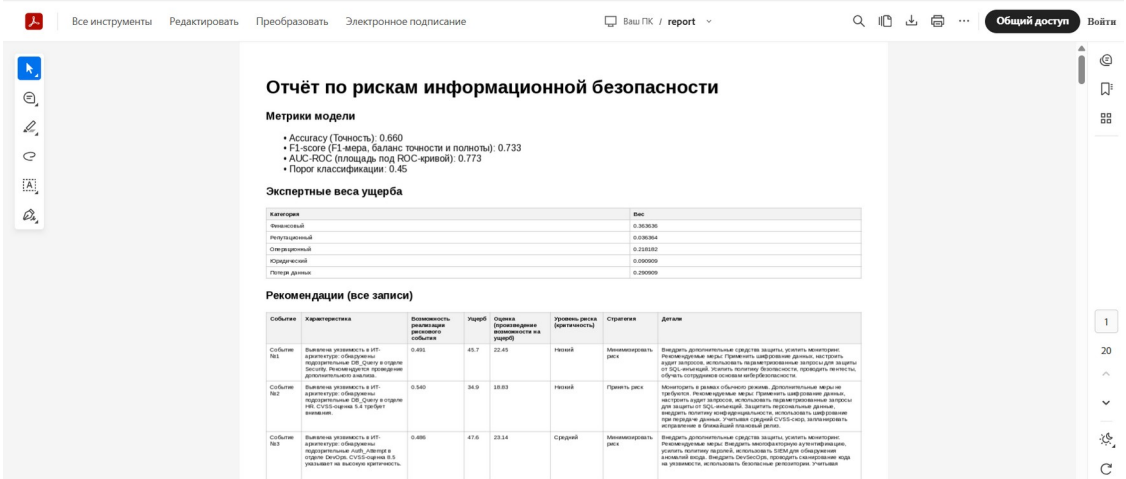


Рисунок 14 – Отчет в формате PDF

Также на странице результатов представлено суррогатное дерево, которое представляет собой обычное дерево, обученное на данных ансамбля, для визуализации логики работы модели (рисунок 15). Для удобства на данной странице представлен датасет и кнопки для его скачивания в форматах CSV, HTML и XLSX (рисунки 16-20). Процесс формирования и скачивания схож с отчетами по обработке рисков.

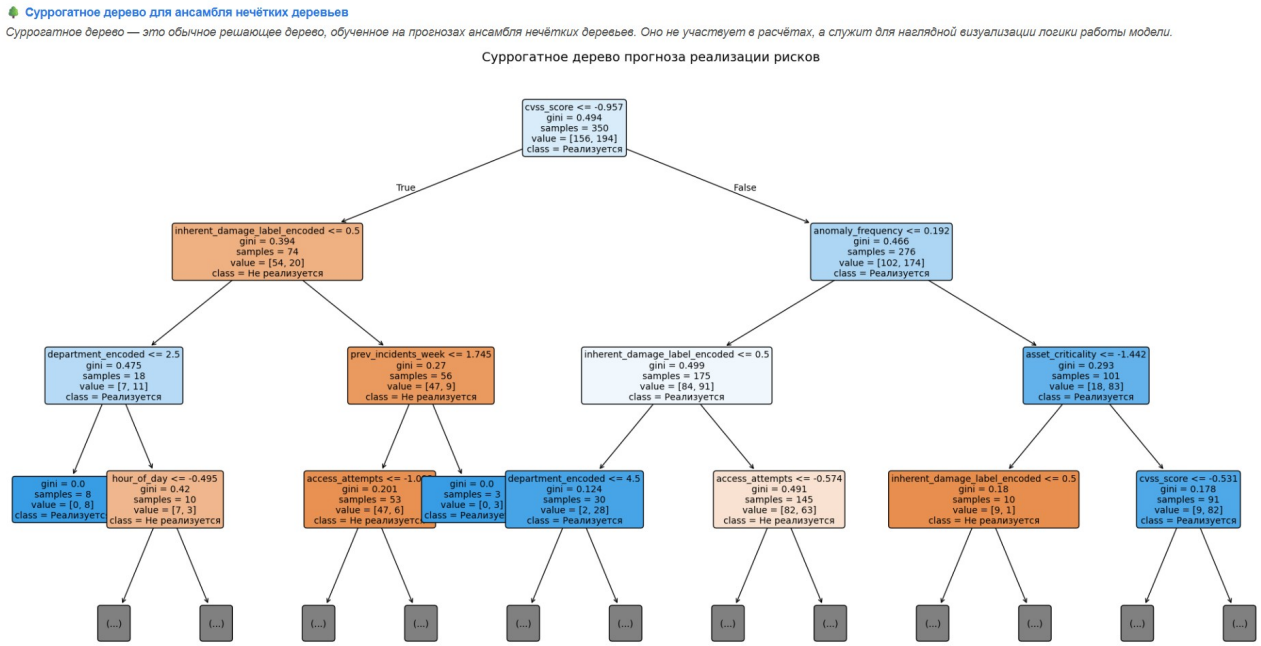
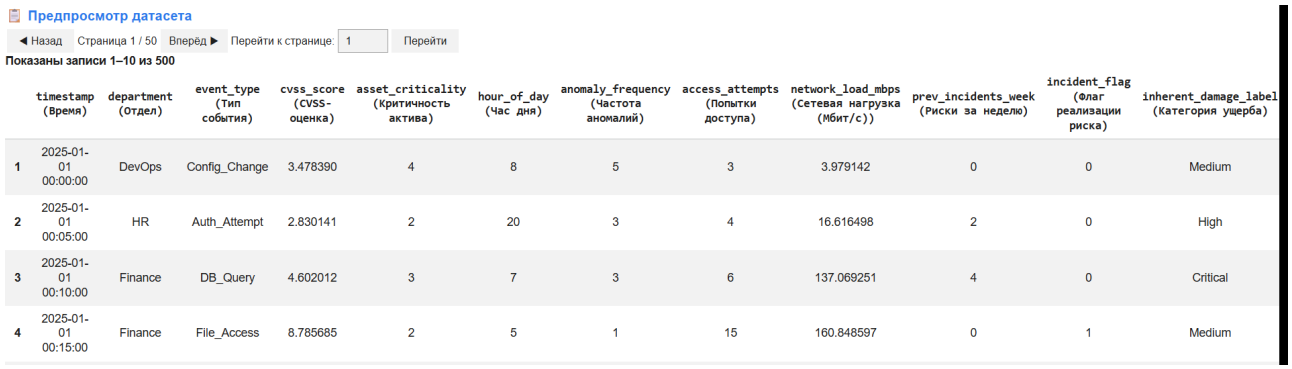


Рисунок 15 – Суррогатное дерево



	timestamp (Время)	department (Отдел)	event_type (Тип события)	cvss_score (CVSS-оценка)	asset_criticality (Критичность актива)	hour_of_day (Час дня)	anomaly_frequency (Частота аномалий)	access_attempts (Попытки доступа)	network_load_mbps (Сетевая нагрузка (Мбит/с))	prev_incidents_week (Риски за неделю)	incident_flag (Флаг реализации риска)	inherent_damage_label (Категория ущерба)
1	2025-01-01 00:00:00	DevOps	Config_Change	3.478390	4	8	5	3	3.979142	0	0	Medium
2	2025-01-01 00:05:00	HR	Auth_Attempt	2.830141	2	20	3	4	16.616498	2	0	High
3	2025-01-01 00:10:00	Finance	DB_Query	4.602012	3	7	3	6	137.069251	4	0	Critical
4	2025-01-01 00:15:00	Finance	File_Access	8.785685	2	5	1	15	160.848597	0	1	Medium

Рисунок 16 – Датасет

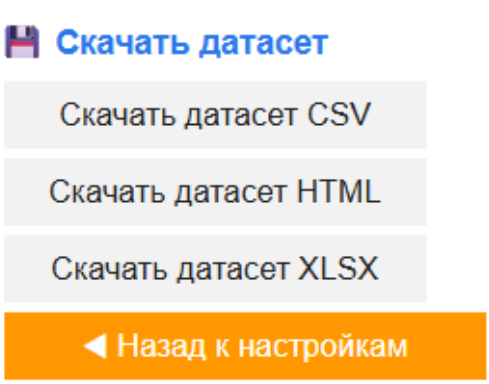
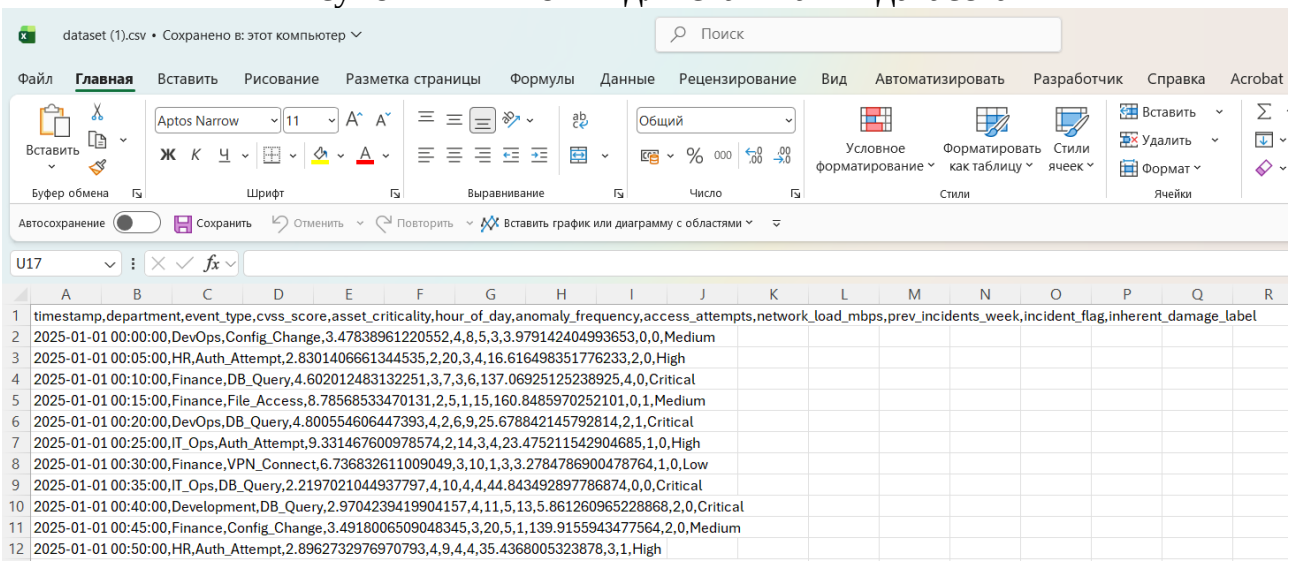


Рисунок 17 – Кнопки для скачивания датасета



dataset (1).csv • Сохранено в: этот компьютер

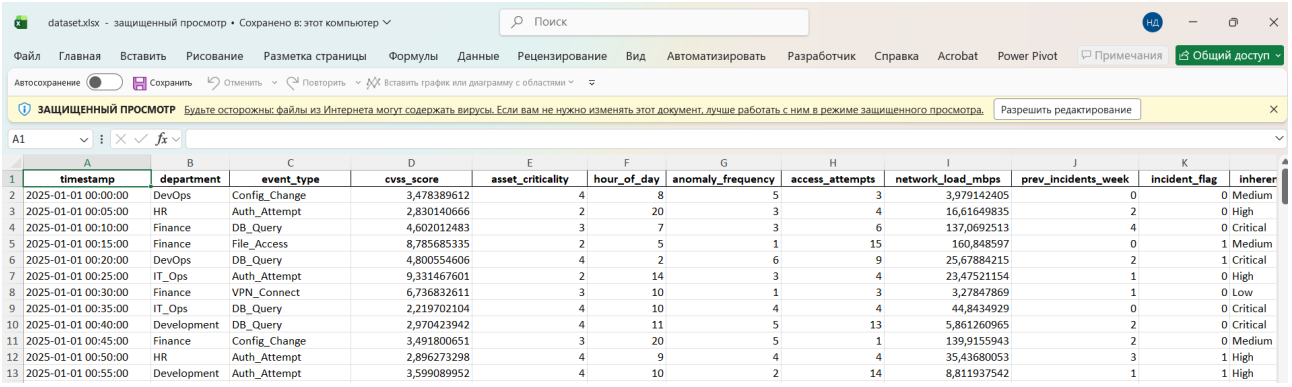
	A
1	timestamp,department,event_type,cvss_score,asset_criticality,hour_of_day,anomaly_frequency,access_attempts,network_load_mbps,prev_incidents_week,incident_flag,inherent_damage_label
2	2025-01-01 00:00:00,DevOps,Config_Change,3.47838961220552,4,8,5,3,3.979142404993653,0,0,Medium
3	2025-01-01 00:05:00,HR,Auth_Attempt,2.8301406661344535,2,20,3,4,16.616498351776233,2,0,High
4	2025-01-01 00:10:00,Finance,DB_Query,4.602012483132251,3,7,3,6,137.06925125238925,4,0,Critical
5	2025-01-01 00:15:00,Finance,File_Access,8.78568533470131,2,5,1,15,160.8485970252101,0,1,Medium
6	2025-01-01 00:20:00,DevOps,DB_Query,4.800554606447393,4,2,6,9,25.678842145792814,2,1,Critical
7	2025-01-01 00:25:00,IT_Ops,Auth_Attempt,9.331467600978574,2,14,3,4,23.475211542904685,1,0,High
8	2025-01-01 00:30:00,Finance,VPN_Connect,6.736832611009049,3,10,1,3,3.2784786900478764,1,0,Low
9	2025-01-01 00:35:00,IT_Ops,DB_Query,2.2197021044937797,4,10,4,4,44.843492897786874,0,0,Critical
10	2025-01-01 00:40:00,Development,DB_Query,2.9704239419904157,4,11,5,13,5.861260965228868,2,0,Critical
11	2025-01-01 00:45:00,Finance,Config_Change,3.4918006509048345,3,20,5,1,139.9155943477564,2,0,Medium
12	2025-01-01 00:50:00,HR,Auth_Attempt,2.8962732976970793,4,9,4,4,35.4368005323878,3,1,High

Рисунок 18 – Датасет в формате CSV

Датасет для анализа рисков

timestamp	department	event_type	cvss_score	asset_criticality	hour_of_day	anomaly_frequency	access_attempts	network_load_mbps	prev_incidents_week	incident_flag	inherent_damage_label
2025-01-01 00:00:00	DevOps	Config_Change	3.478390	4	8	5	3	3.979142	0	0	Medium
2025-01-01 00:05:00	HR	Auth_Attempt	2.830141	2	20	3	4	16.616498	2	0	High
2025-01-01 00:10:00	Finance	DB_Query	4.602012	3	7	3	6	137.069251	4	0	Critical
2025-01-01 00:15:00	Finance	File_Access	8.785685	2	5	1	15	160.848597	0	1	Medium
2025-01-01 00:20:00	DevOps	DB_Query	4.800555	4	2	6	9	25.678842	2	1	Critical
2025-01-01 00:25:00	IT_Ops	Auth_Attempt	9.331468	2	14	3	4	23.475212	1	0	High
2025-01-01 00:30:00	Finance	VPN_Connect	6.736833	3	10	1	3	3.278479	1	0	Low
2025-01-01 00:35:00	IT_Ops	DB_Query	2.219702	4	10	4	4	44.843493	0	0	Critical
2025-01-01 00:40:00	Development	DB_Query	2.970424	4	11	5	13	5.861261	2	0	Critical
2025-01-01 00:45:00	Finance	Config_Change	3.491801	3	20	5	1	139.915594	2	0	Medium
2025-01-01 00:50:00	HR	Auth_Attempt	2.896273	4	9	4	4	35.436801	3	1	High
2025-01-01 00:55:00	Development	Auth_Attempt	3.599090	4	10	2	14	8.811938	1	1	High
2025-01-01 01:00:00	IT_Ops	File_Access	6.972053	3	18	4	5	163.573031	1	1	Medium
2025-01-01 01:05:00	Finance	Config_Change	2.511278	4	16	7	2	49.586156	1	0	Medium
2025-01-01 01:10:00	DevOps	VPN_Connect	5.811823	2	16	5	1	45.130947	1	0	Low
2025-01-01 01:15:00	Development	Network_Connection	6.759260	1	18	0	1	69.014012	2	1	Low

Рисунок 19 – Датасет в формате HTML



dataset.xlsx - защищенный просмотр • Сохранено в: этот компьютер

	A	B	C	D	E	F	G	H	I	J	K	L
1	timestamp	department	event_type	cvss_score	asset_criticality	hour_of_day	anomaly_frequency	access_attempts	network_load_mbps	prev_incidents_week	incident_flag	inherer
2	2025-01-01 00:00:00	DevOps	Config_Change	3,478389612	4	8	5	3	3,979142405	0	0	Medium
3	2025-01-01 00:05:00	HR	Auth_Attempt	2,830140666	2	20	3	4	16,61649835	2	0	High
4	2025-01-01 00:10:00	Finance	DB_Query	4,602012483	3	7	3	6	137,0692513	4	0	Critical
5	2025-01-01 00:15:00	Finance	File_Access	8,785685335	2	5	1	15	160,848597	0	1	Medium
6	2025-01-01 00:20:00	DevOps	DB_Query	4,800554606	4	2	6	9	25,67884215	2	1	Critical
7	2025-01-01 00:25:00	IT_Ops	Auth_Attempt	9,331467601	2	14	3	4	23,47521154	1	0	High
8	2025-01-01 00:30:00	Finance	VPN_Connect	6,736832611	3	10	1	3	3,27847869	1	0	Low
9	2025-01-01 00:35:00	IT_Ops	DB_Query	2,219702104	4	10	4	4	44,8434929	0	0	Critical
10	2025-01-01 00:40:00	Development	DB_Query	2,970423942	4	11	5	13	5,861260965	2	0	Critical
11	2025-01-01 00:45:00	Finance	Config_Change	3,491800651	3	20	5	1	139,9155943	2	0	Medium
12	2025-01-01 00:50:00	HR	Auth_Attempt	2,896273298	4	9	4	4	35,43680053	3	1	High
13	2025-01-01 00:55:00	Development	Auth_Attempt	3,599089952	4	10	2	14	8,811937542	1	1	High

Рисунок 20 – Датасет в формате XLSX

Для перехода *к графическому анализу* нажмите кнопку «Показать визуализацию» на странице результатов (рисунок 21). На открывшейся странице представлены 11 интерактивных графиков (распределение рисков, топ-20 событий, матрица ошибок, ROC-кривая и др.) и суррогатное дерево решений (рисунки 22-33). Для сохранения всех графиков нажмите «Скачать все графики», после которой они выгрузятся в ZIP-архиве (рисунки 34 и 35).

Используйте выпадающие списки в верхней части страницы для фильтрации данных по отделам, типам событий и уровням критичности рисков (рисунок 36).



Рисунок 21 – Кнопка «Показать визуализацию»

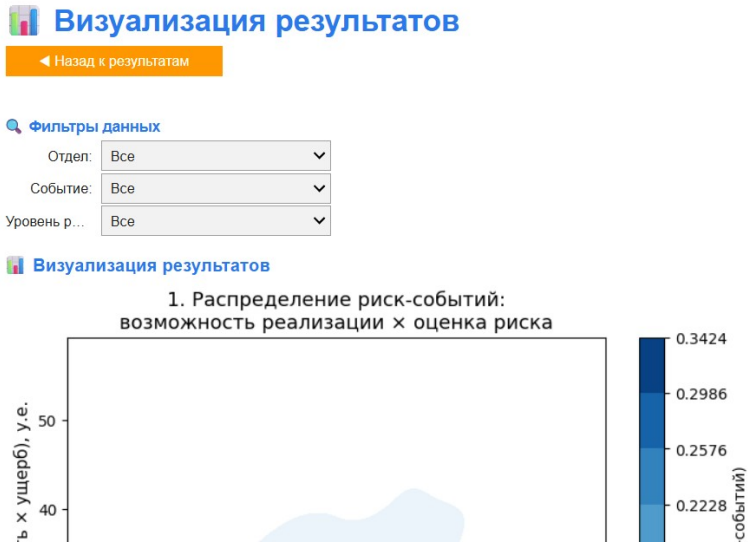
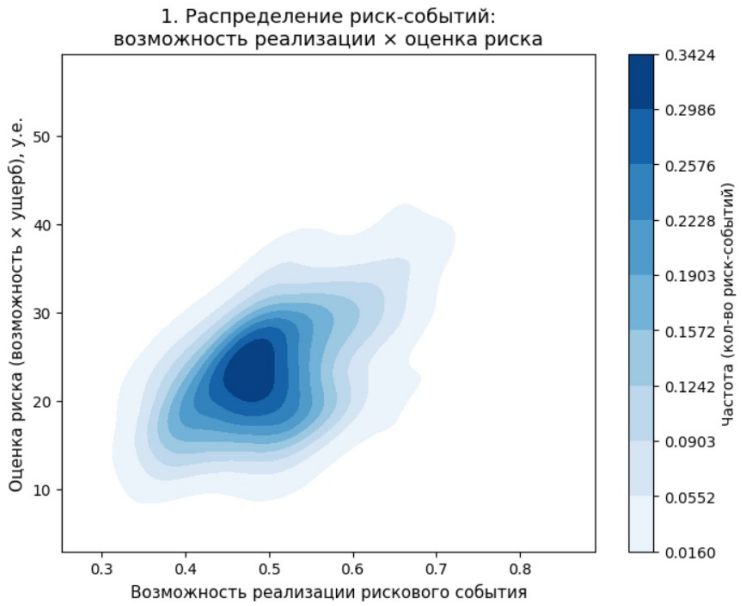
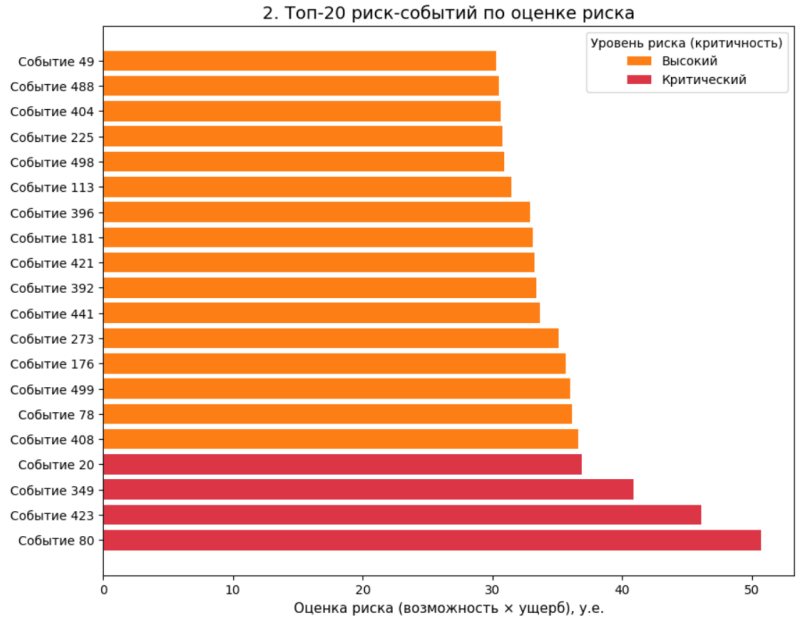


Рисунок 22 – Страница визуализации



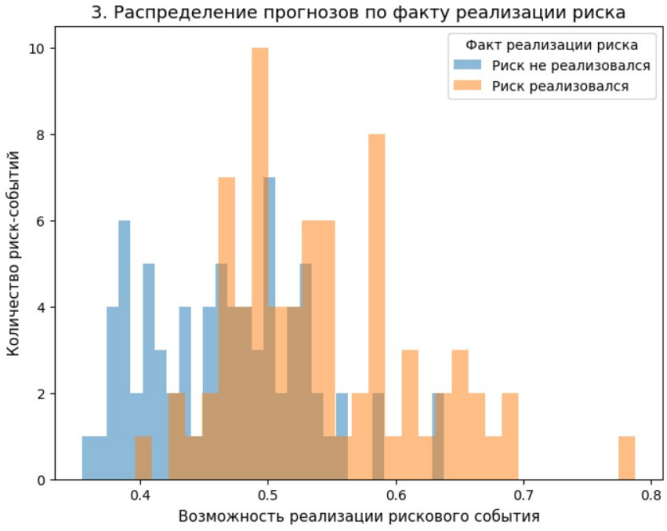
Совместное распределение риск-событий по прогнозируемой возможности реализации и оценке риска. Чем темнее область, тем чаще в неё попадают риск-события.

Рисунок 23 – Распределение риск-событий



Самые критичные риск-события с наибольшей оценкой риска. Цвет соответствует уровню риска (критичности).

Рисунок 24 – Топ-20 риск-событий по оценке риска



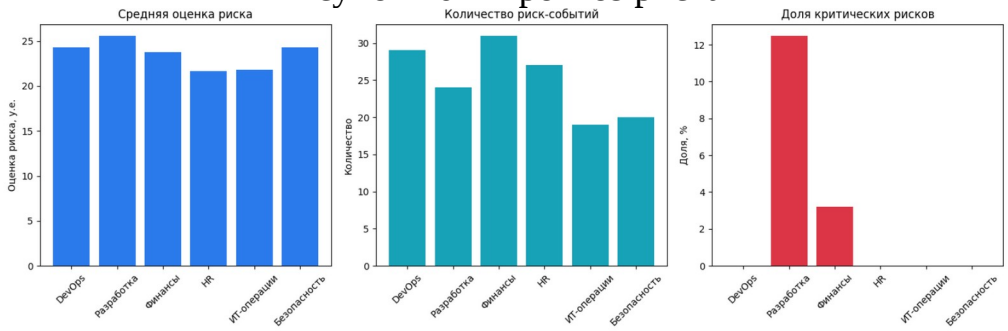
Распределение прогнозируемой возможности реализации для риск-событий, которые фактически реализовались и не реализовались.

Рисунок 25 – Распределение прогнозов по факту реализации риска



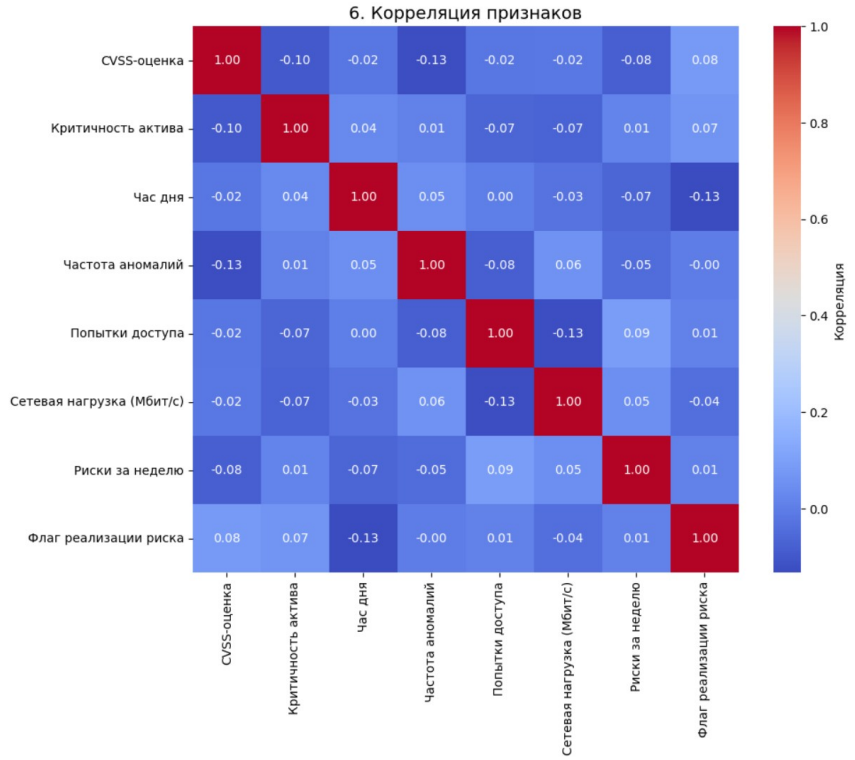
Прогноз риска: по оси X — прогнозируемая возможность реализации, по оси Y — ущерб. Цвет точки отражает итоговую оценку риска.

Рисунок 26 – Прогноз риска



Сводка по отделам: средняя оценка риска, количество риск-событий и доля критических рисков.

Рисунок 27 – Сводка по отделам ИТ-организации



Показывает, какие числовые признаки сильно коррелируют между собой.

Рисунок 28 – Корреляция признаков



Динамика количества риск-событий и средней оценки риска по часам суток.

Рисунок 29 – Временной профиль риск-событий по часам суток



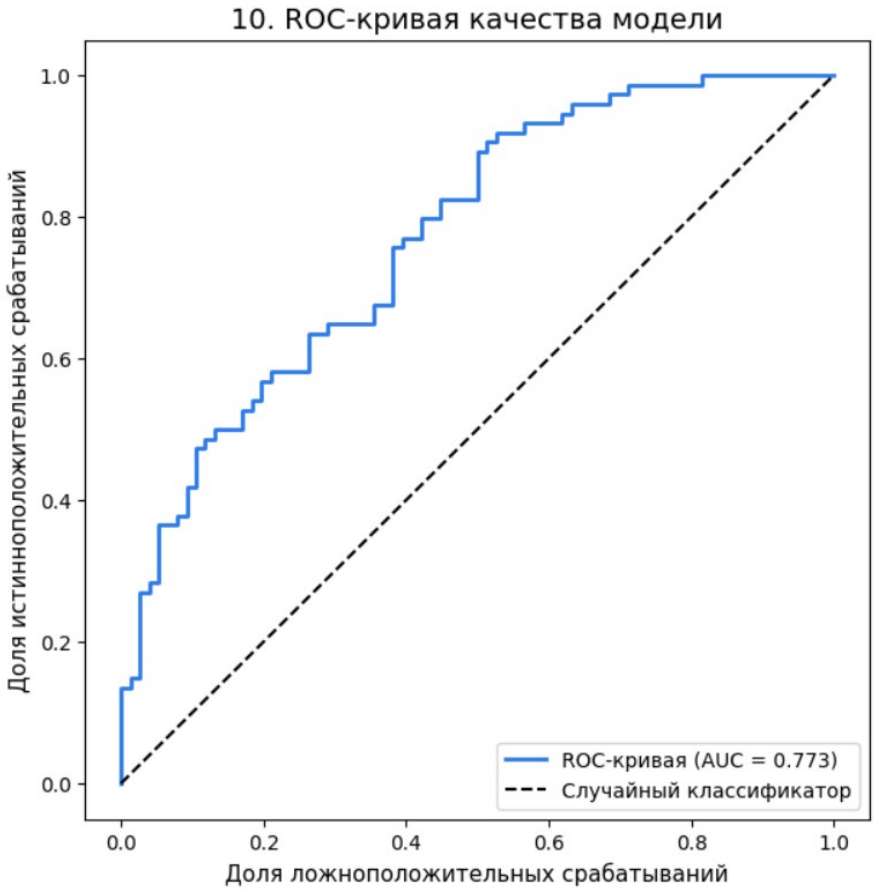
Доли риск-событий по стратегиям обработки: принять, минимизировать, передать или уклониться.

Рисунок 30 – Распределение стратегий обработки рисков



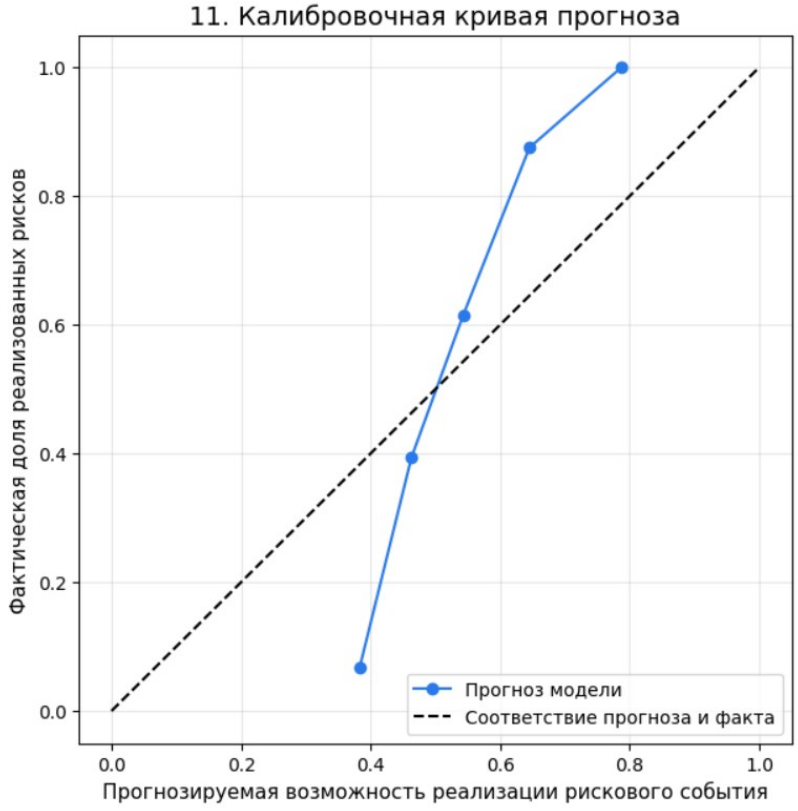
Сравнение прогноза модели с фактической реализацией рисков.

Рисунок 31 – Матрица ошибок



Качество разделения классов: чем выше кривая и больше площадь под ней (AUC), тем лучше модель.

Рисунок 32 – ROC-кривая



Соответствие между прогнозируемой возможностью реализации и фактической долей реализованных рисков.

Рисунок 33 – Калибровочная кривая

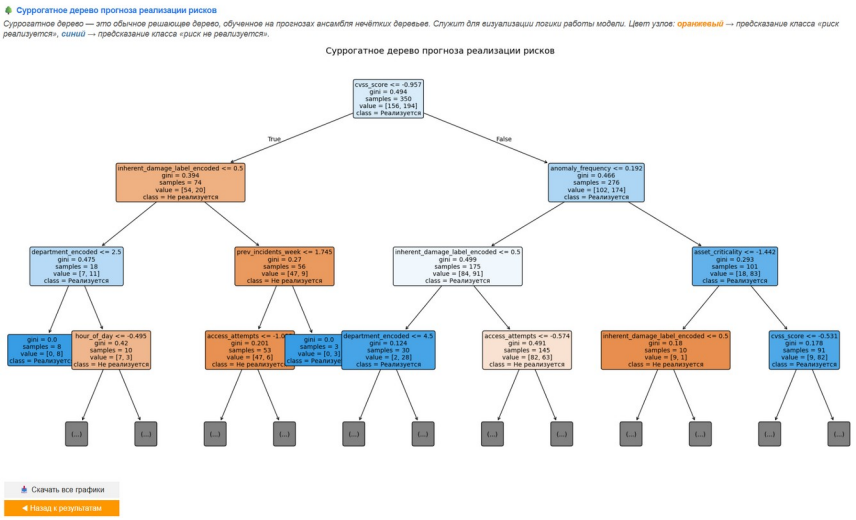


Рисунок 34 – Суррогатное дерево и кнопка скачивания графиков

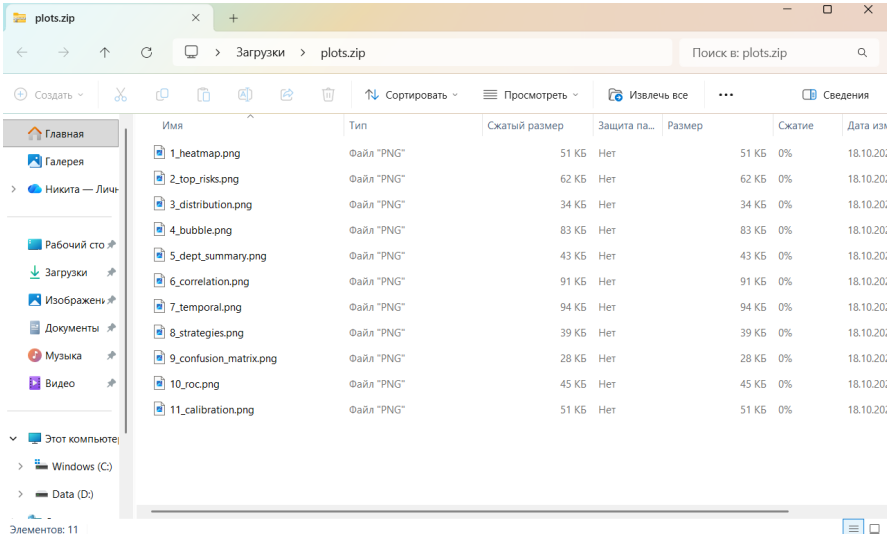


Рисунок 35 – ZIP-архив графиков

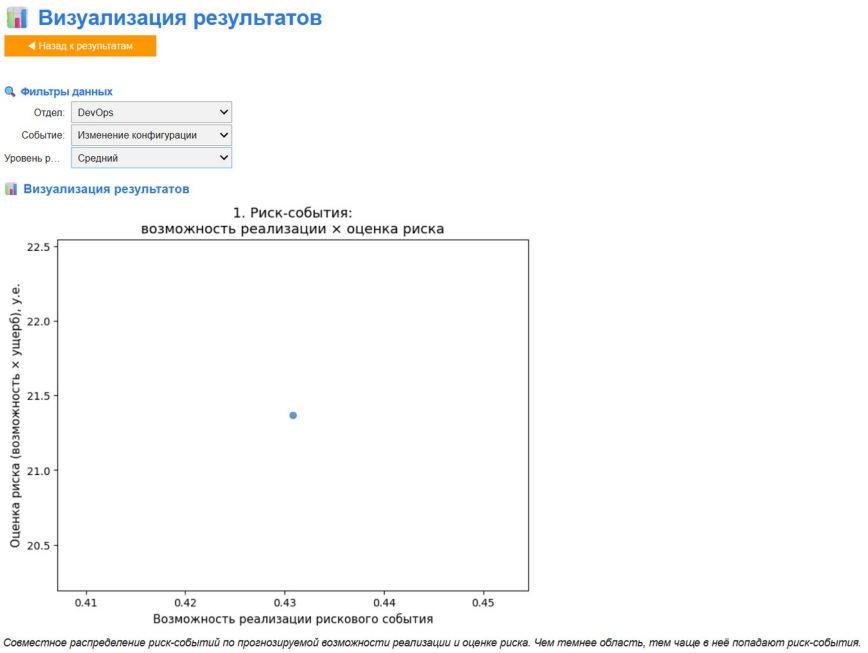


Рисунок 36 – Применение фильтров

Для перехода к предыдущим этапам или проведения нового анализа с новыми или старыми данными используйте кнопки навигации на страницах.

Примечания: для проведения анализа с использованием предыдущего датасета сохраните его в формате CSV или XLSX и загрузите на вкладке данных.

2 Работа с интерфейсом через веб-приложение

Интерфейс веб-приложения разделен на 4 логические вкладки, переключение между которыми осуществляется через верхнее меню навигации. Ниже меню представлен прогресс-бар, который отражает текущий этап. Справа от меню навигации расположена кнопка «Новая сессия», о которой будет рассказано далее, а рядом с ней идентификатор текущей сессии. Главная страница веб-приложения представлена на рисунке 37.

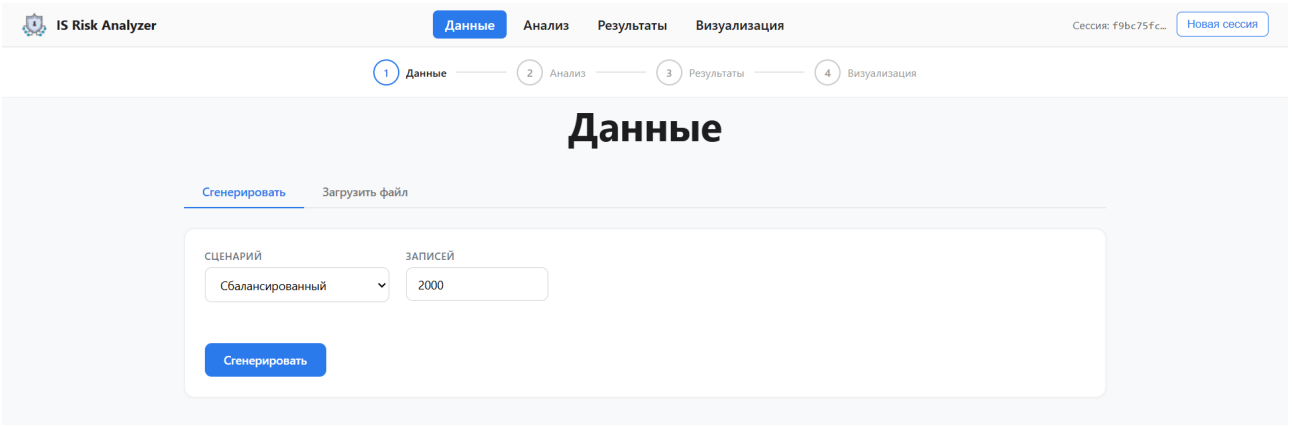


Рисунок 37 – Главная страница веб-приложения

Вкладка «Данные» – при открытии приложения сессия создается автоматически, о чем свидетельствует соответствующий статус. Аналогично версии для Colab и локальным Jupyter, выберите режим:

- «Сгенерировать» – настройка сценария (Сбалансированный, Высокие риски или Низкие риски) и количества записей (от 100 до 100 000).
- «Загрузить файл» – выбор CSV/XLSX документа. Загружаемый файл должен содержать обязательные столбцы (время, отдел, тип события, CVSS-оценка, критичность актива и др.).

После нажатия кнопки генерации или загрузки появится таблица предпросмотра датасета с пагинацией, а этап «Данные» в прогресс-баре будет отображаться, как выполненный. Рядом с таблицей располагаются кнопки скачивания и сброса датасета. Приложение позволяет сохранить исходные данные в форматах CSV, HTML и XLSX.

Режимы генерации и загрузки файла, изменение статуса этапа в прогресс-баре, а также таблицы предпросмотра исходных данных для анализа представлены на рисунках 38 и 39.

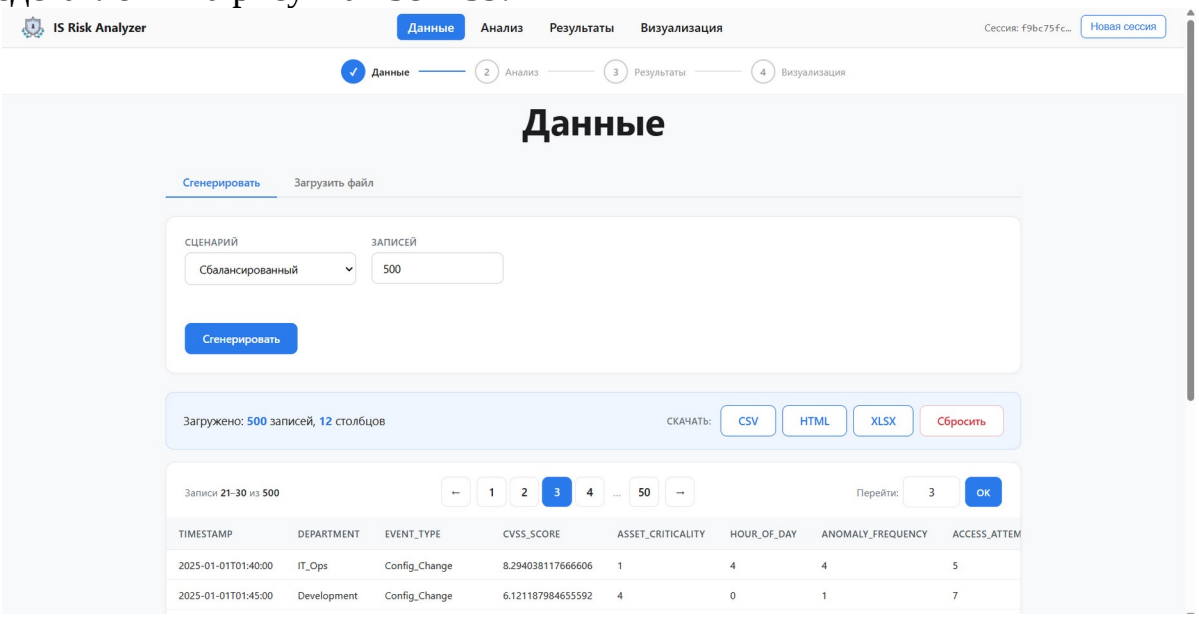


Рисунок 38 – Режим «Сгенерировать»

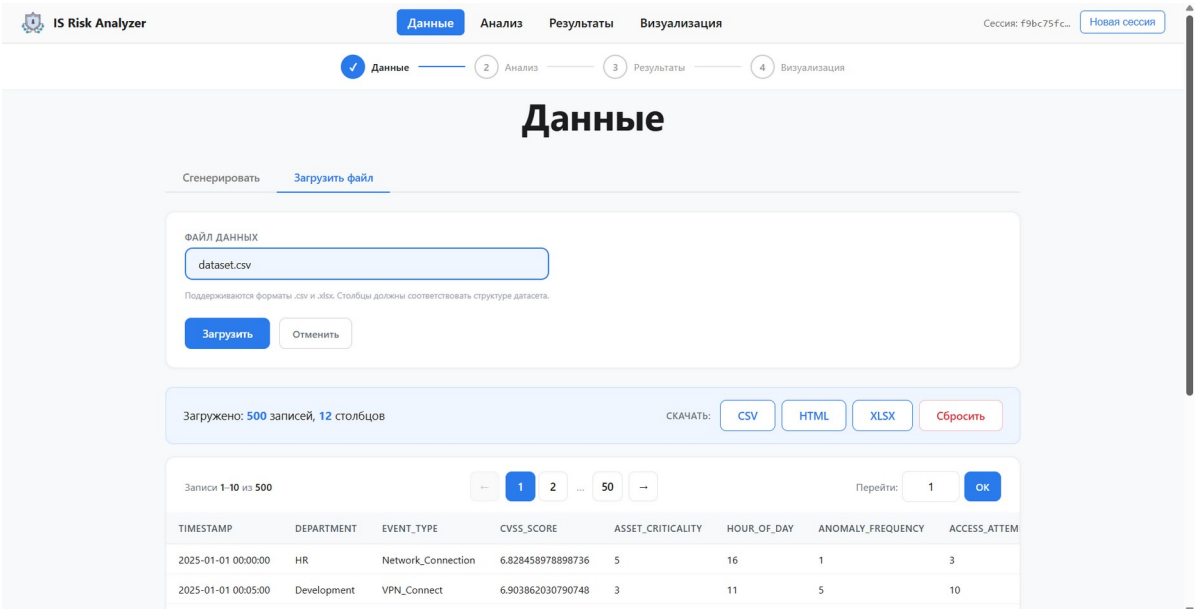


Рисунок 39 – Режим «Загрузить файл»

Файлы сохраненных датасетов идентичны тем, что формируются в Google Colab или локальном Jupyter (рисунки 18-20). При скачивании датасета все кнопки на странице становятся неактивными, а кнопка с выбранным форматом меняет название на «…».

После успешного завершения этапа с подготовкой данных внизу страницы появляется надпись о возможности перехода на следующий этап (рисунок 40).

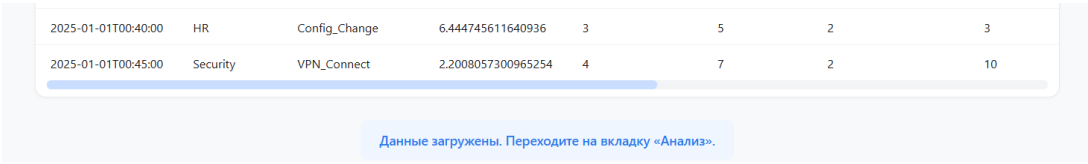


Рисунок 40 – Надпись о возможности перехода на этап анализа

Вкладка «Анализ» – до того момента, пока не будет завершена подготовка датасета, на данном этапе ничего не отображается, кроме сообщения о необходимости завершения предыдущего этапа (рисунки 41).

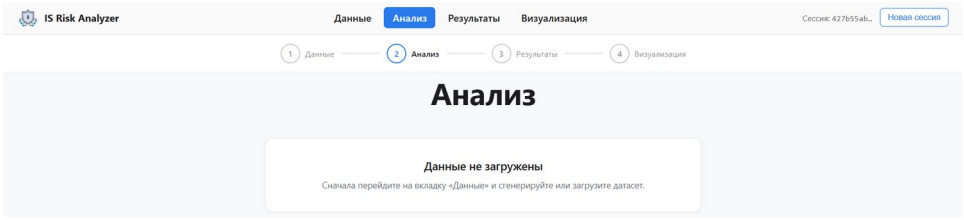


Рисунок 41 – Переход на вкладку «Анализ» до завершения загрузки данных

Задайте количество нечетких деревьев в ансамбле (от 10 до 100). Настройте экспертные веса категорий ущерба в одном из двух режимов:

- «Числовой» – используйте ползунки для каждой из пяти категорий ущерба (финансовый, репутационный, операционный, юридический, потеря данных), чтобы задать их веса. Программа автоматически нормирует значения.
- «Лингвистический» – выберите качественные оценки (от «Очень низкого» до «Критического») из выпадающих списков для каждой категории.

Указание количества деревьев ансамбля и режимы экспертных заданий весов ущерба представлены на рисунках 42 и 43.

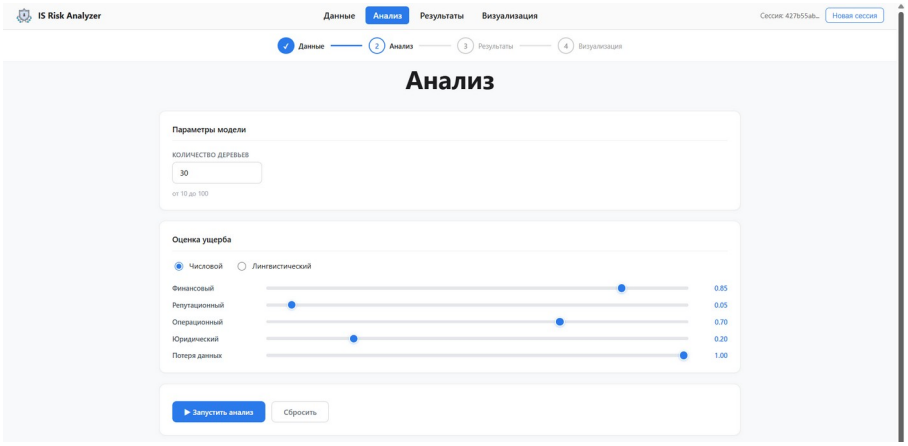


Рисунок 42 – Режим «Числовой» в веб-приложении

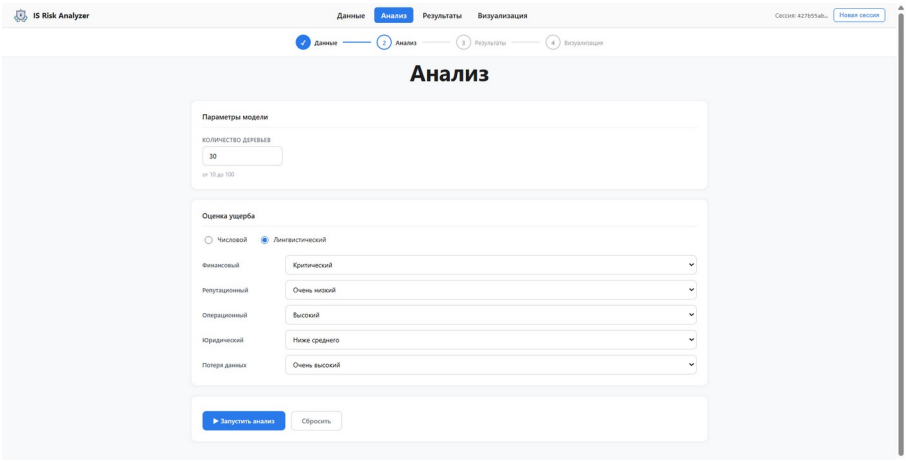


Рисунок 43 – Режим «Лингвистический» в веб-приложении

Нажмите кнопку «Запустить анализ». Внизу страницы появится прогресс-бар, отображающий текущий этап анализа, подобно версии в Google Colab и локальном Jupyter (рисунок 44). Дождитесь завершения анализа, после которого прогресс-бар будет заполнен на 100% и внизу появится надпись о возможности перехода на следующий этап (рисунок 45).

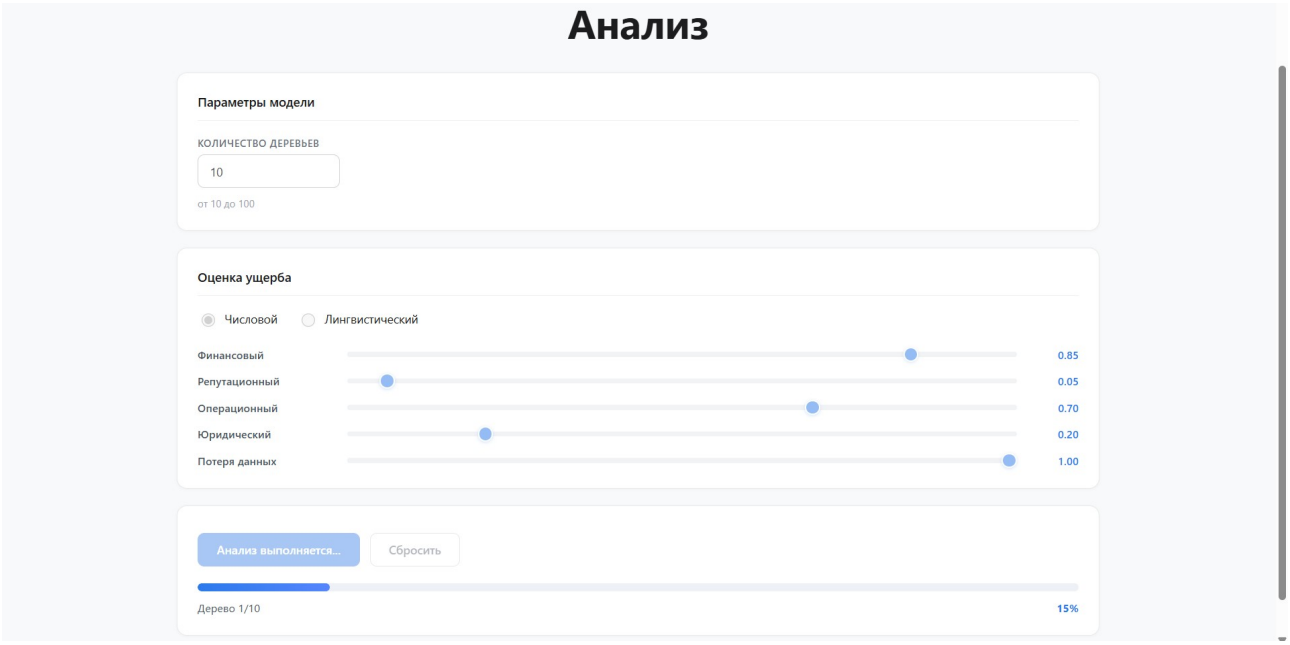


Рисунок 44 – Проведение анализа

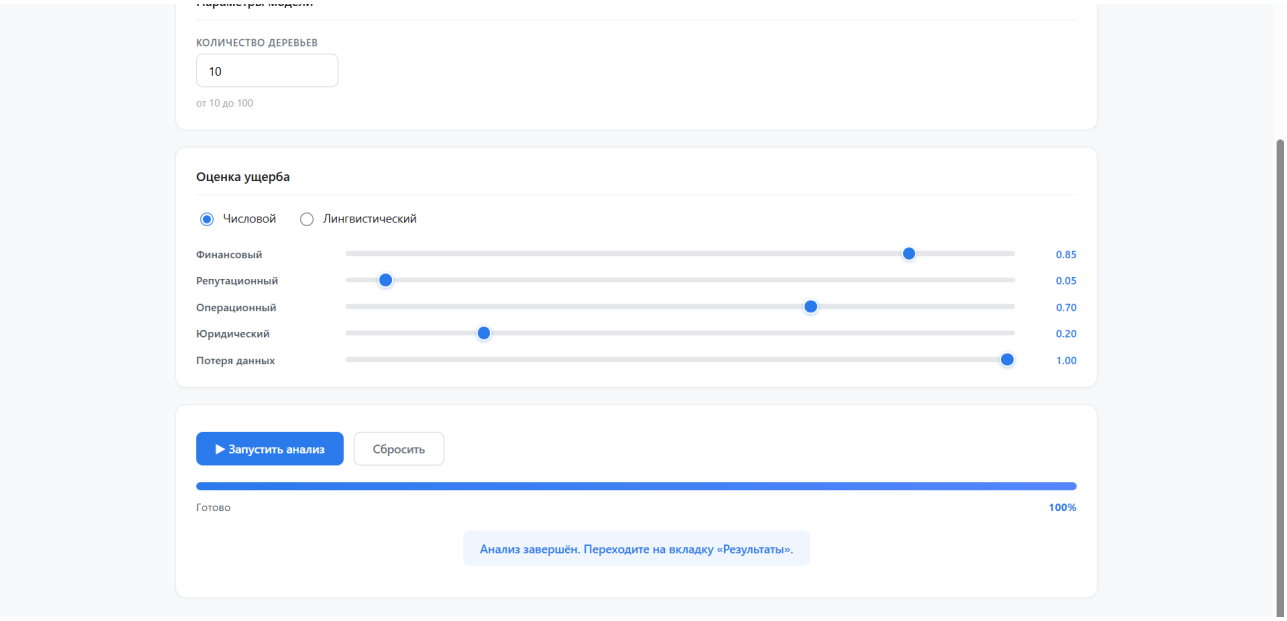


Рисунок 45 – Завершение анализа и сообщение о переходе к результатам

Вкладка «Результаты» – до того момента, пока не будет завершен анализ, на данном этапе ничего не отображается, кроме сообщения о необходимости завершения предыдущего этапа (рисунки 46). На странице отображаются карточки с метриками качества модели (Accuracy, F1, AUC), весами ущерба по категориям и таблица с рекомендациями по обработке рисков (рисунки 47 и 48). Над таблицей доступны кнопки для скачивания итогового отчета в форматах CSV, HTML и PDF. Внизу страницы отображается сообщение о возможности перехода на этап визуализации (рисунок 49).

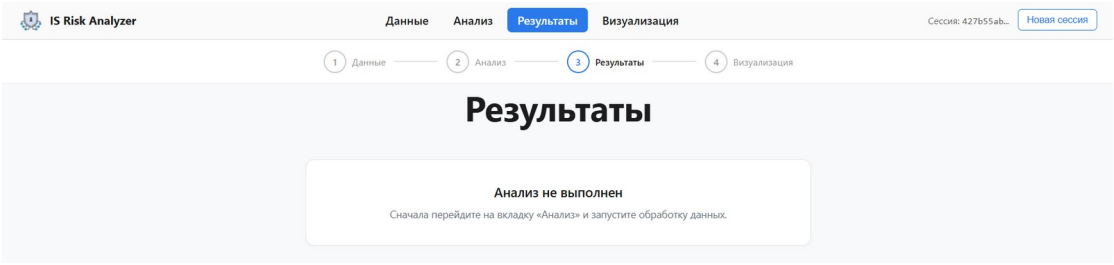


Рисунок 46 – Переход на вкладку «Результаты» до завершения анализа

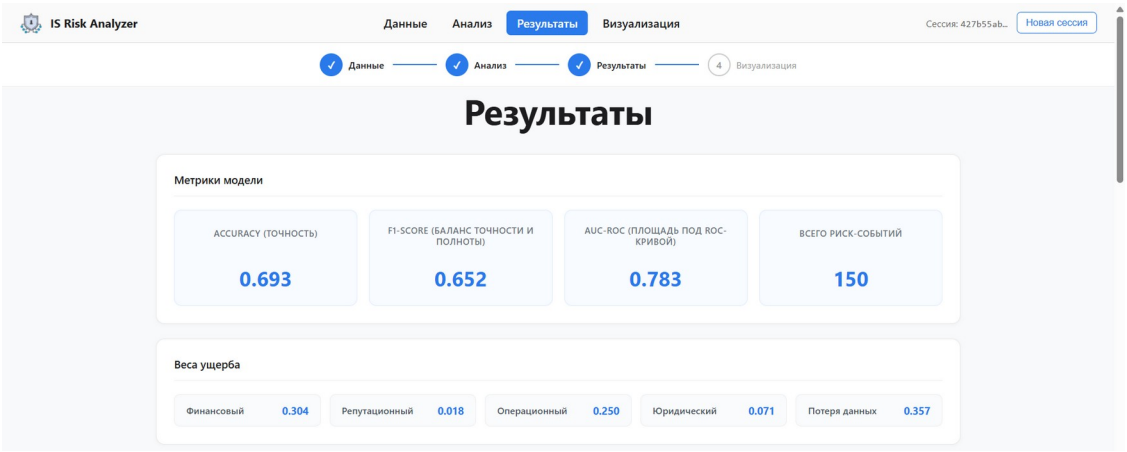


Рисунок 47 – Метрики модели и веса ущерба по категориям

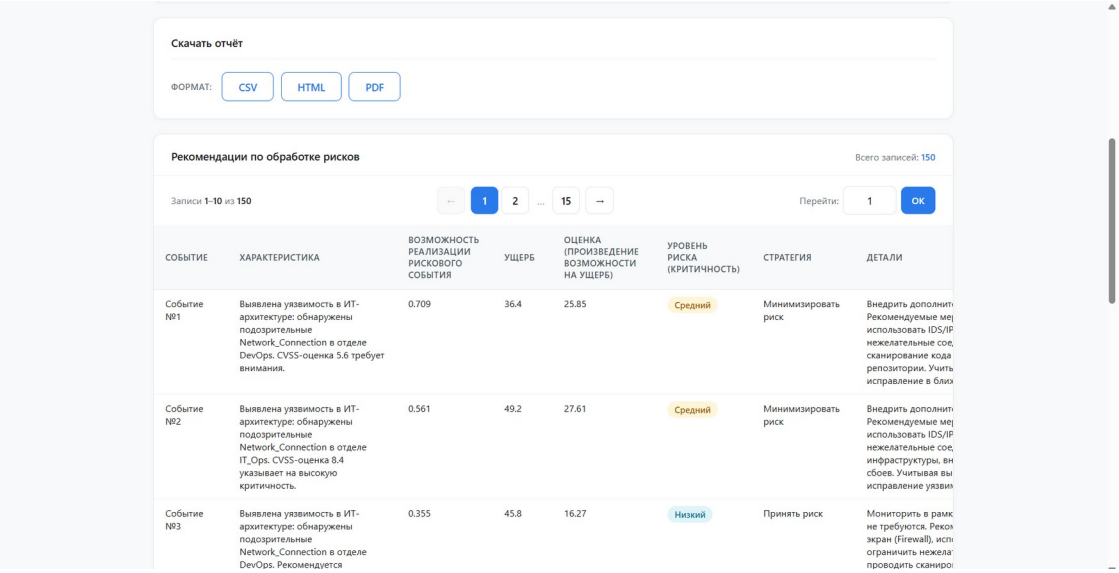


Рисунок 48 – Кнопки скачивания отчетов и таблица рекомендаций

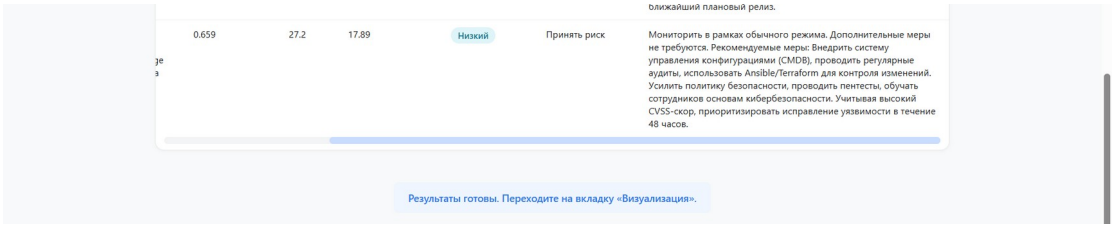


Рисунок 49 – Сообщение о переходе на вкладку визуализации

Файлы сохраненных отчетов идентичны тем, что формируются в Google Colab или локальном Jupyter (рисунки 12-14). При скачивании отчета все кнопки на странице становятся неактивными, а кнопка с выбранным форматом меняет название на «…».

Вкладка «Визуализация» – до того момента, пока не будет завершен анализ, на данном этапе ничего не отображается, кроме сообщения о необходимости завершения предыдущего этапа (рисунки 50).

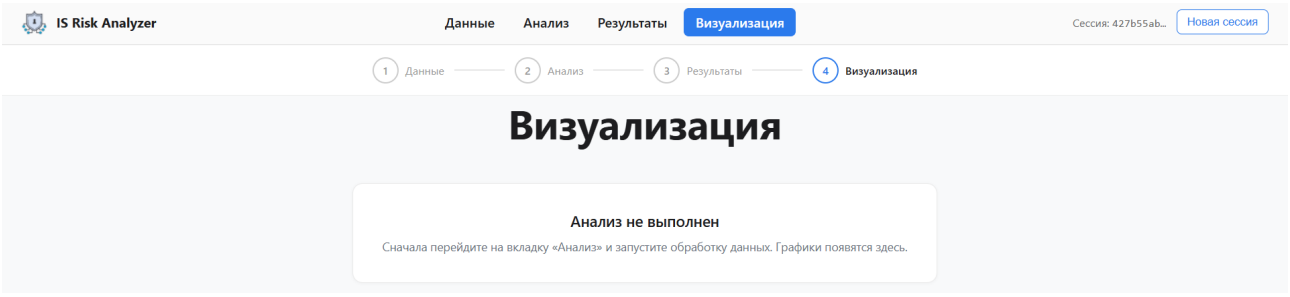


Рисунок 50 – Переход на вкладку «Визуализация» до завершения анализа

Перейдите на данную вкладку и дождитесь конца формирования и загрузки графиков (рисунок 51).

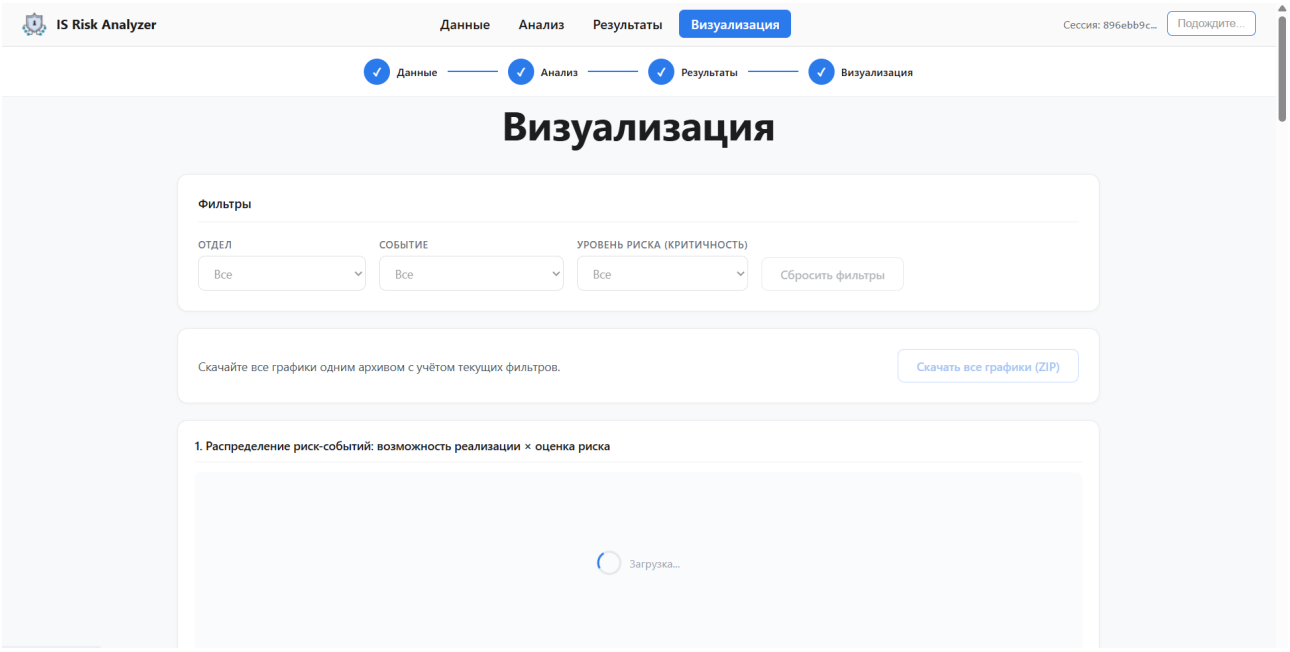


Рисунок 51 – Загрузка графиков

Изучите представленные графики (их набор идентичен Google Colab или локальном Jupyter) и суррогатное дерево (все они представлены на рисунках 52-63). Для сохранения всех материалов нажмите кнопку скачивания ZIP-архива (рисунки 64 и 65). Используйте выпадающие списки для фильтрации данных по отделам, типам событий и уровням риска. Графики будут перестраиваться динамически (рисунок 66). Для очистки фильтров используйте кнопку «Сбросить фильтры».

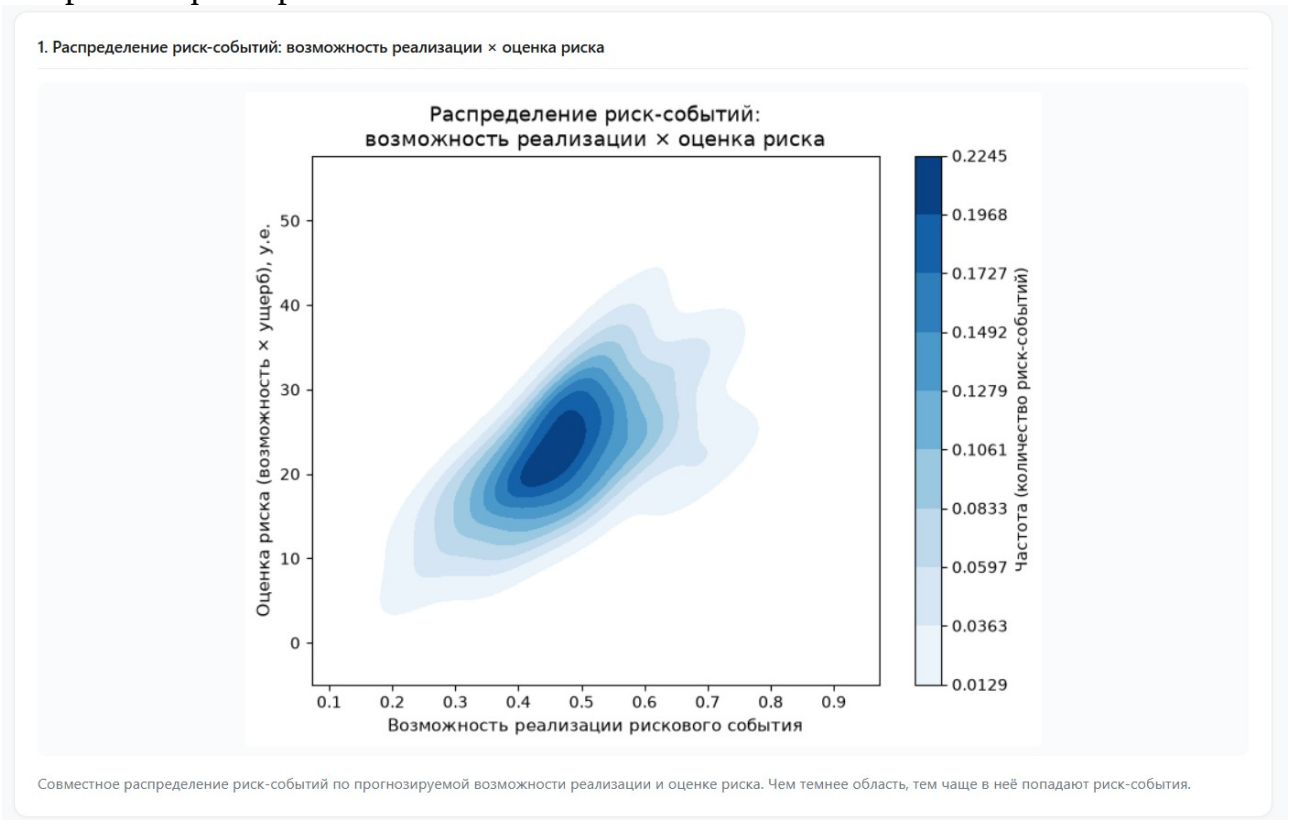


Рисунок 52 – График распределения риск-событий

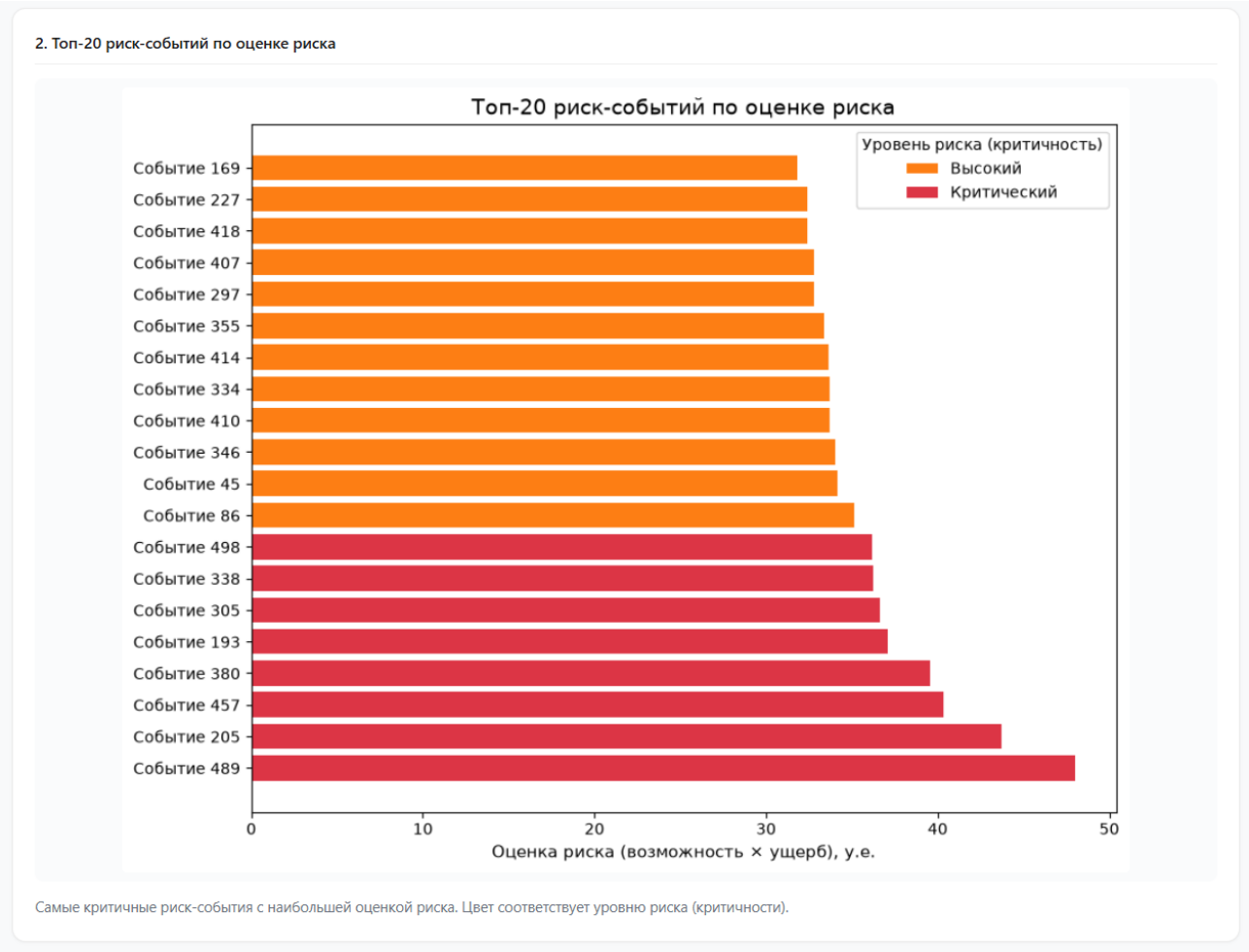


Рисунок 53 – График топ-20 риск-событий по оценке риска

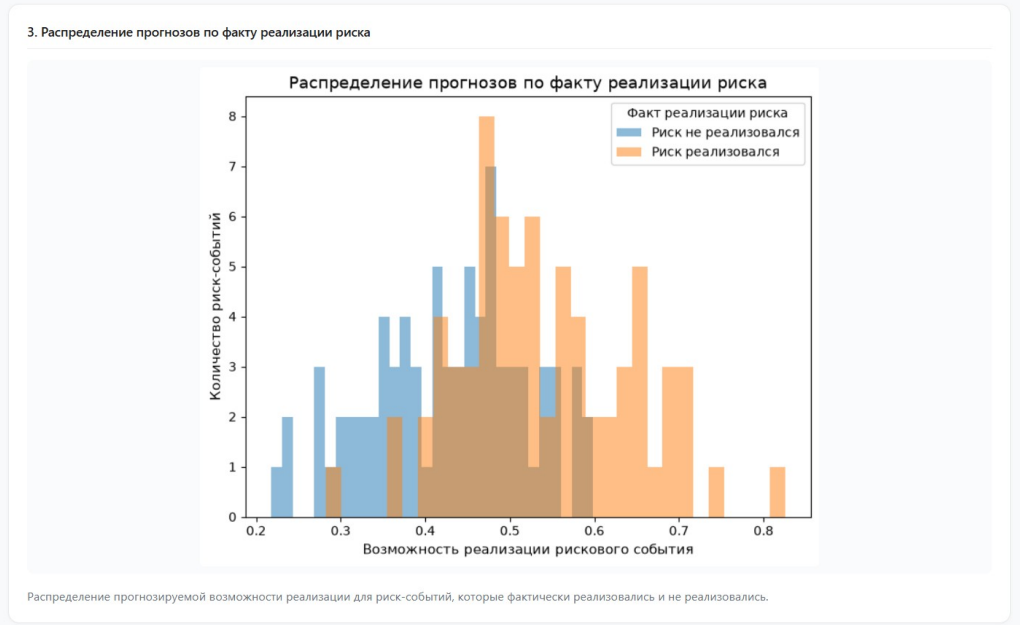


Рисунок 54 – График распределения прогнозов по факту реализации риска

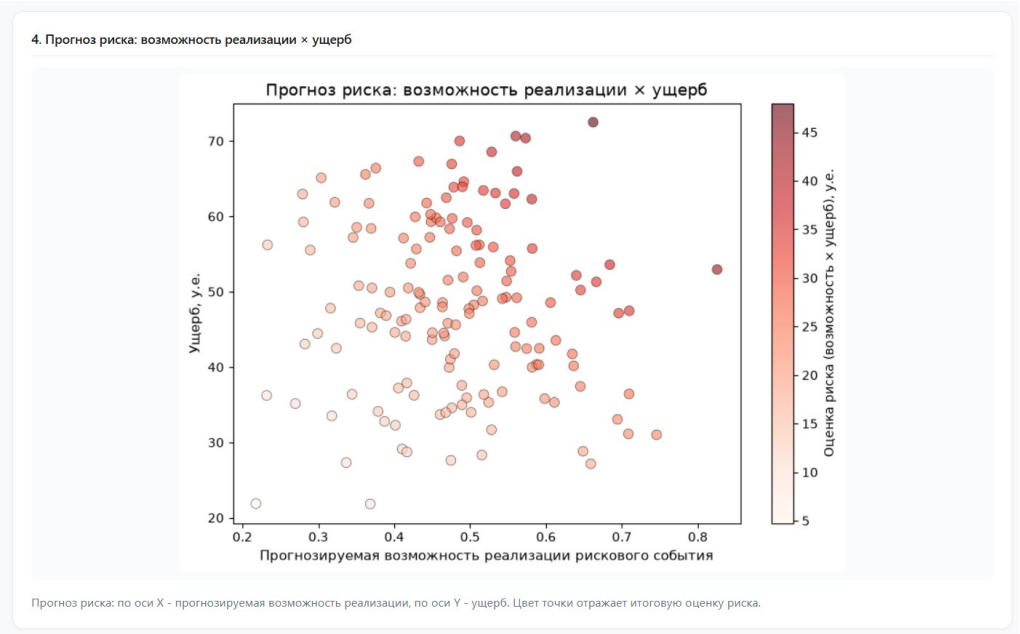


Рисунок 55 – График прогноза риска

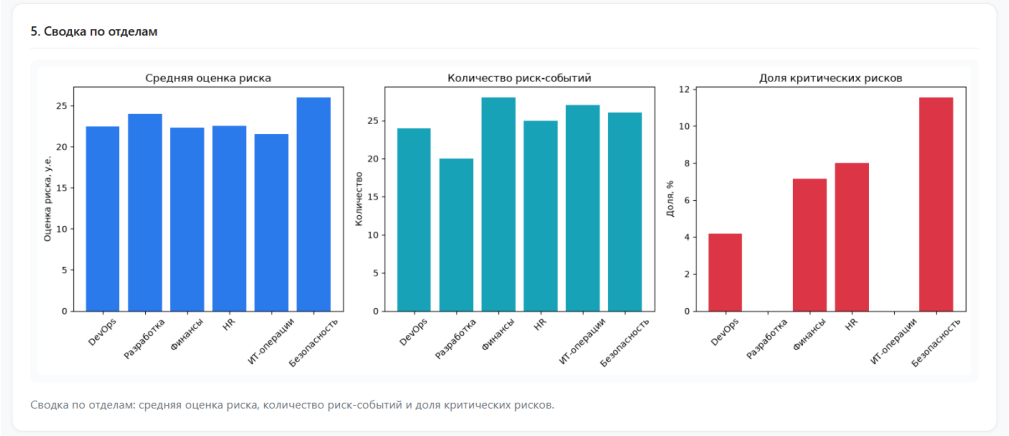


Рисунок 56 – Графики сводки по отделам

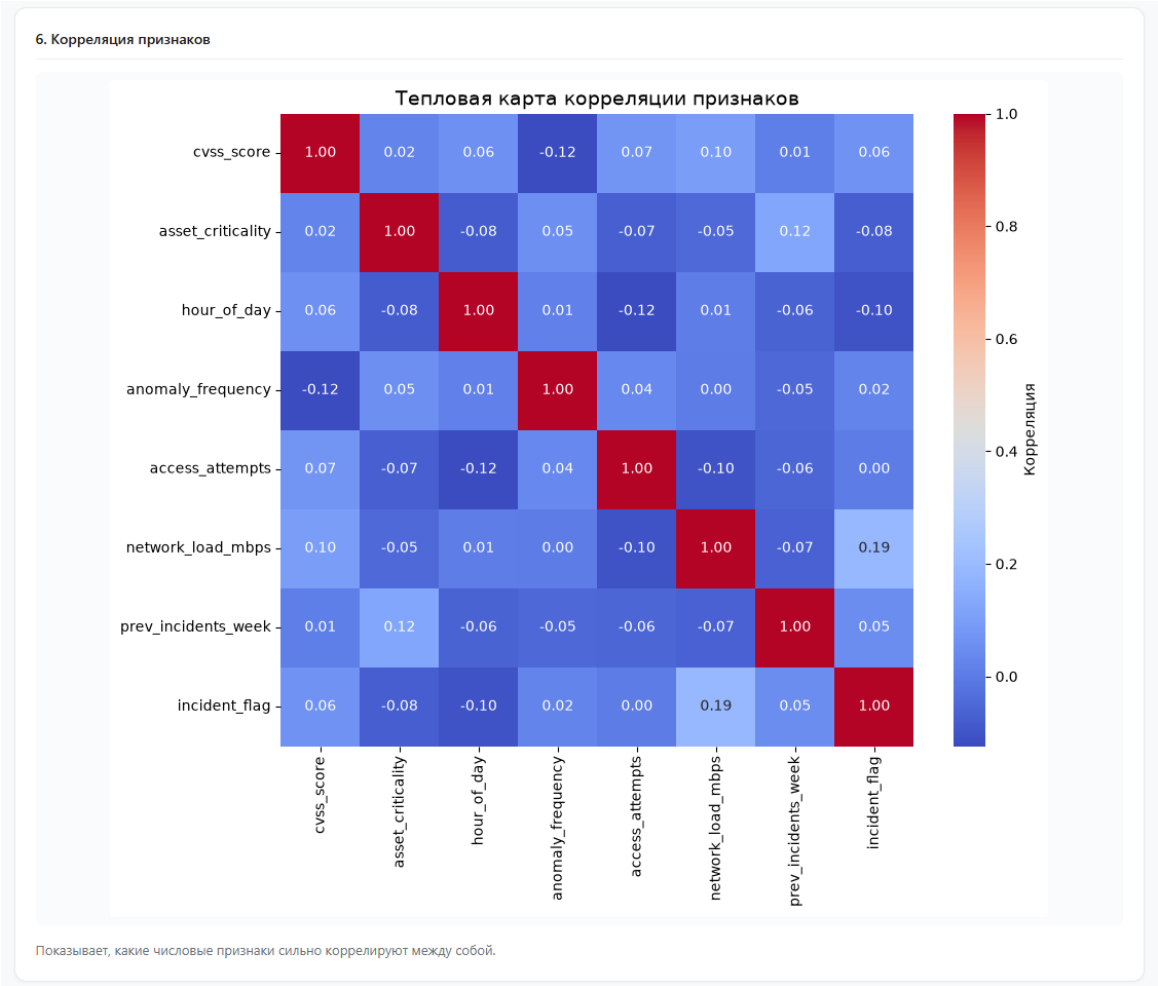


Рисунок 57 – График корреляции признаков

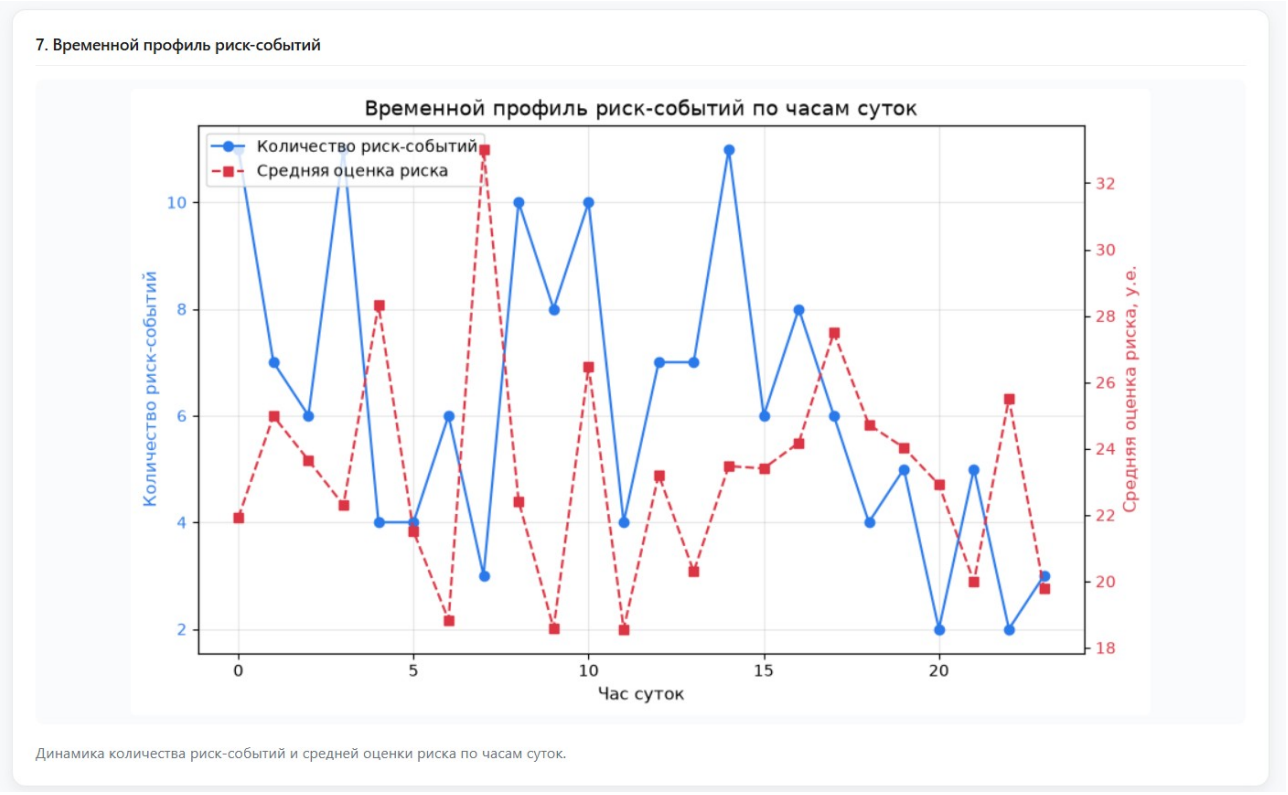


Рисунок 58 – График временного профиля риск-событий по часам суток

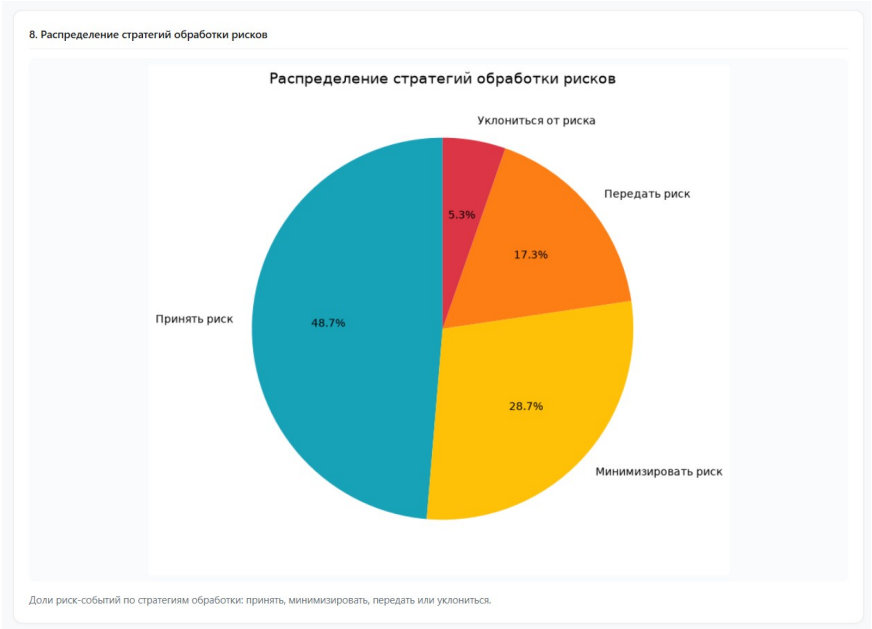


Рисунок 59 – График распределения стратегий обработки рисков

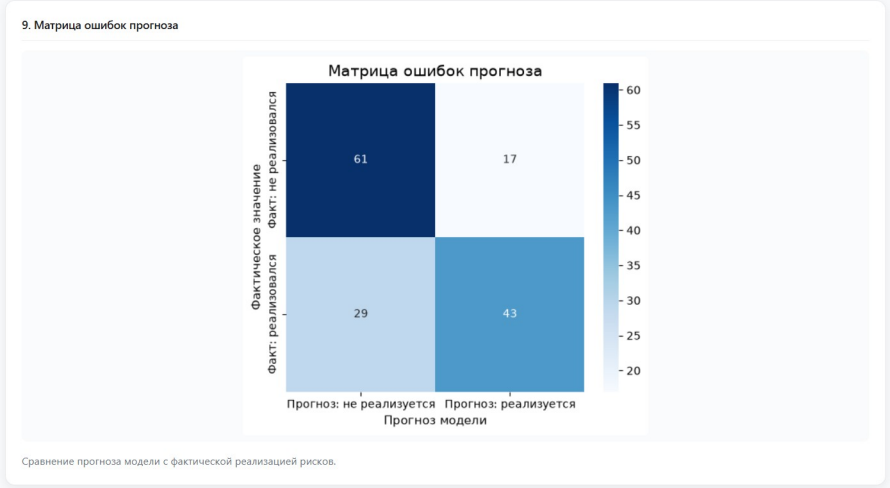


Рисунок 60 – График матрицы ошибок

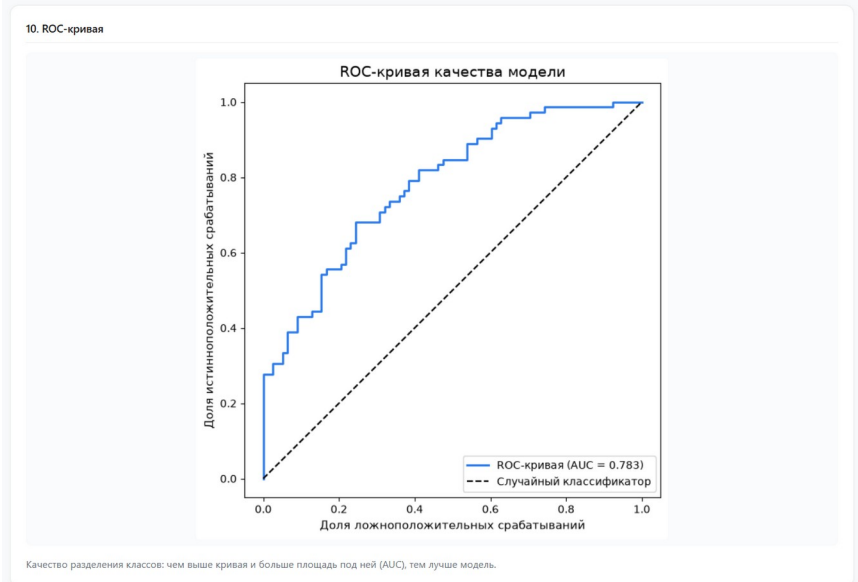


Рисунок 61 – График ROC-кривой

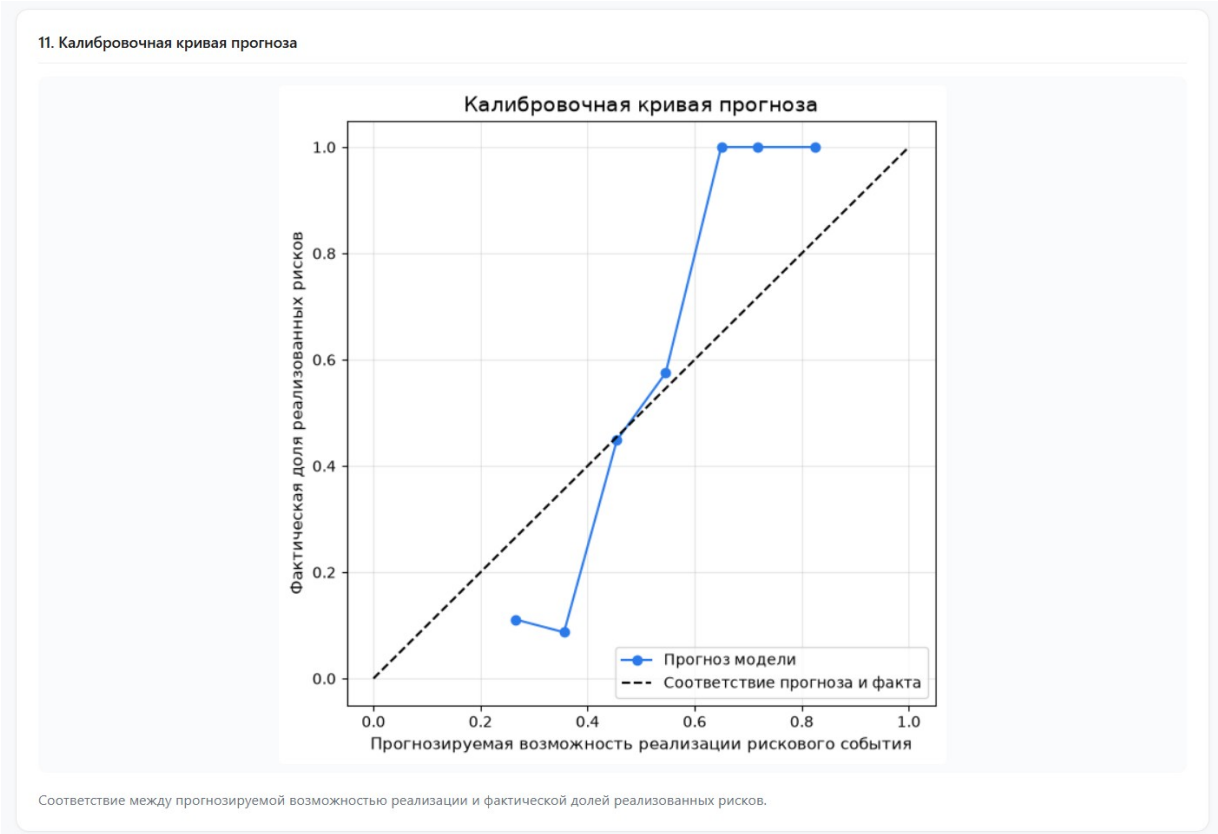


Рисунок 62 – График калибровочной кривой

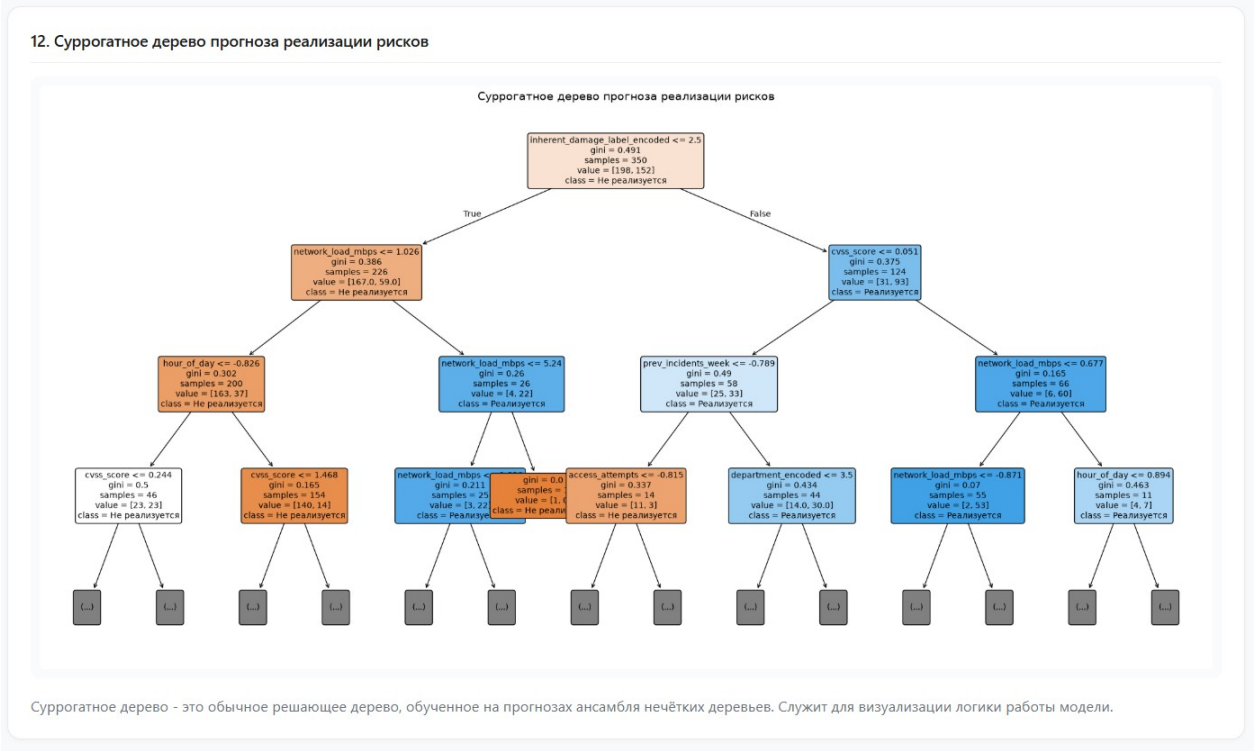


Рисунок 63 – Суррогатное дерево в веб-приложении

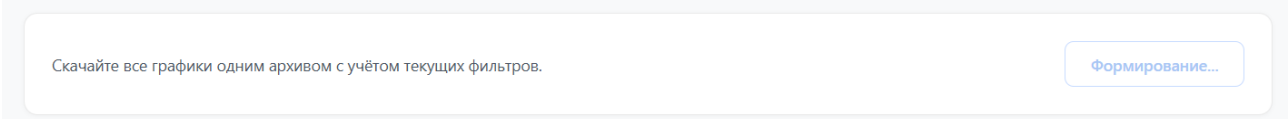


Рисунок 64 – Формирование ZIP-архива

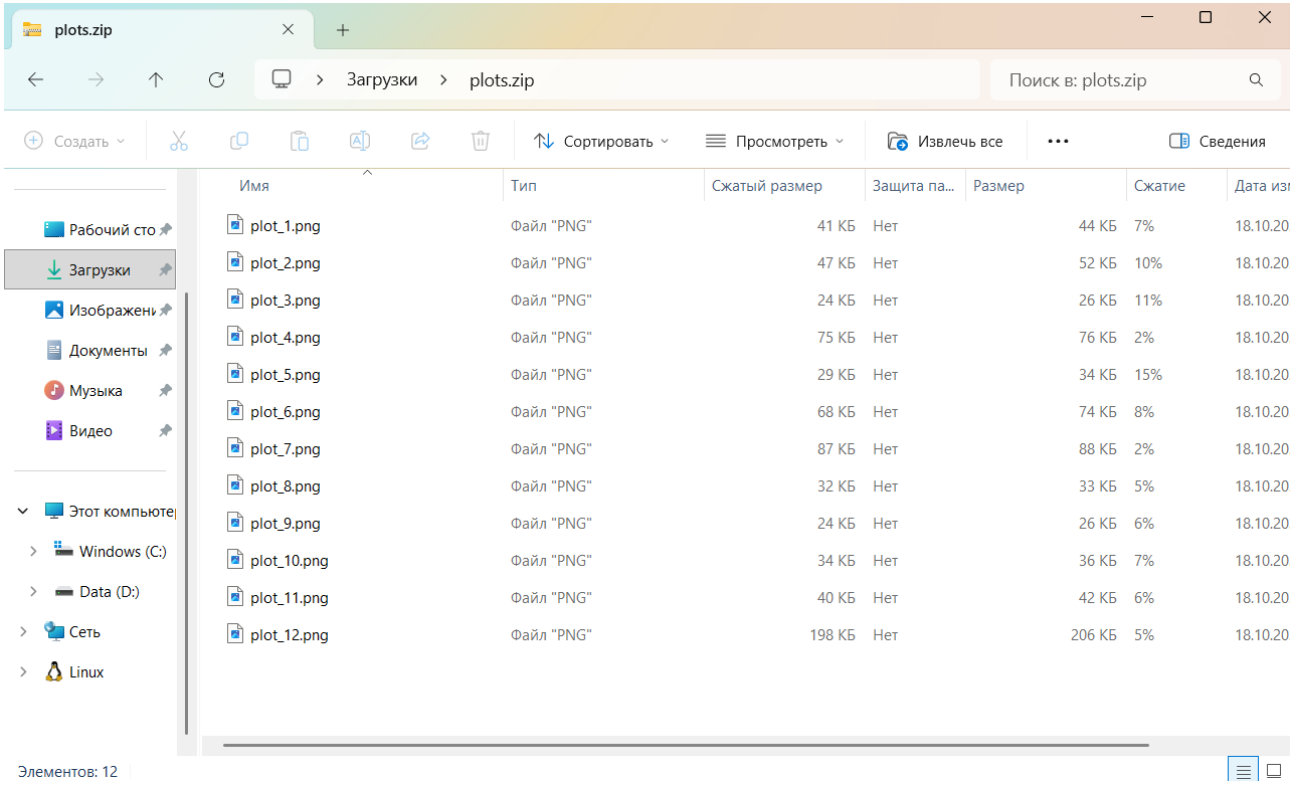


Рисунок 65 – ZIP-архив с графиками и суррогатным деревом

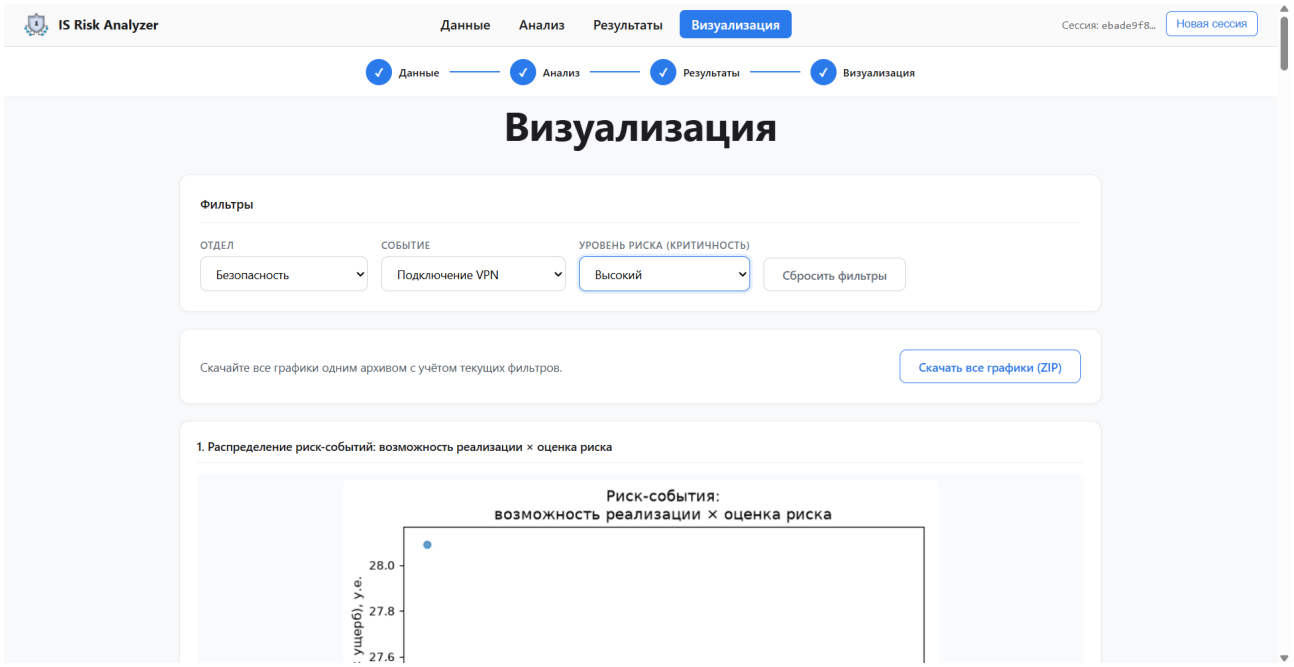


Рисунок 66 – Перерисовка графиков при выборе фильтров

При загрузке страницы, изменении или очистке фильтров выпадающий список и скачивание графиков блокируется до момента, пока не загрузятся все графики на странице.

Во время выполнения некоторых процессов в системе кнопки блокируются, а ряд возможностей становятся недоступными до завершения данных процессов, что можно заметить на некоторых приведенных ранее рисунках.

Управление сессиями – для сброса текущих результатов и проведения нового анализа на тех же данных воспользуйтесь кнопкой «Сбросить» на вкладке «Анализ» или просто запустите его заново. Для проведения анализа на новом датасете нажмите кнопку «Сбросить» на вкладке «Данные» или сгенерируйте или загрузите датасет. Также для этих целей доступна кнопка «Новая сессия» в правом верхнем углу страницы. В дополнение к этому кнопка «Новая сессия» генерирует новый идентификатор, полностью очищая текущее состояние в оперативной памяти сервера.

Важные моменты

- Обучение нечетких деревьев – это трудоемкий процесс, который прямо пропорционально зависит от размера датасета и количества деревьев в ансамбле. При большом объеме данных и количестве деревьев процесс обучения может занимать длительное время и использовать огромные вычислительные ресурсы, поэтому советуется использовать оптимальные значения. Для стабильной работы в браузере и предотвращения переполнения оперативной памяти сервера (особенно при одновременной работе нескольких пользователей) рекомендуется загружать датасеты объемом не более 10 000-20 000 записей и использовать от 30 до 50 деревьев в ансамбле. Этого достаточно для получения статистически значимых результатов.

- Загружаемый файл датасета должен содержать следующие обязательные столбцы: timestamp, department, event_type, cvss_score, asset_criticality, hour_of_day, anomaly_frequency, access_attempts, network_load_mbps, prev_incidents_week, incident_flag. При отсутствии хотя бы одного из них система выдаст ошибку.

- Формирование PDF-отчета в локальном веб-приложении требует наличия системных библиотек WeasyPrint (GTK3). При их отсутствии воспользуйтесь форматами CSV или HTML, которые формируются без ограничений.

- При генерации синтетического датасета в режиме «Сбалансированный» система использует адаптивные квантильные пороги для наглядной демонстрации работы модели на всех уровнях критичности рисков. При загрузке внешнего файла (даже если это скачанный ранее сгенерированный датасет) система применяет алгоритм без искусственной подгонки под квантили. Это сделано для того, чтобы при анализе реальных корпоративных данных программа не «придумывала» критические риски там, где их нет.