ПРОЕКТ НА КОНКУРС «УЧИ-ИТ»:

«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
(Д.Э.Н, ДОЦ. КАФЕДРЫ ИТЭУ)

АКТУАЛЬНОСТЬ И ПРОБЛЕМА

Актуальность проекта обусловлена рядом факторов:

- Рост количества и усложнение способов кибератак
- Классические экспертные методы не учитывают многокомпонентный характер ущерба в соответствии с приоритетами конкретной ИТ-организации
- Исходные данные для анализа могут быть неактуальными, недостоверными и/или неполными
- Качественные методы оценки рисков преобладают над количественными, что приводит к субъективизму, сложностям при ранжировании угроз и обосновании инвестиций на организацию защиты
- Текущие решения зачастую реализуют лишь отдельные этапы анализа рисков, а не все процессы – от сбора данных до формирования рекомендаций по их обработке

Основная проблема

- Обеспечение баланса между точностью прогноза, прозрачностью алгоритма и учётом специфики бизнеса.

ПРАКТИКО-ОРИЕНТИРОВАННОСТЬ И ЦЕЛЕВАЯ АУДИТОРИЯ

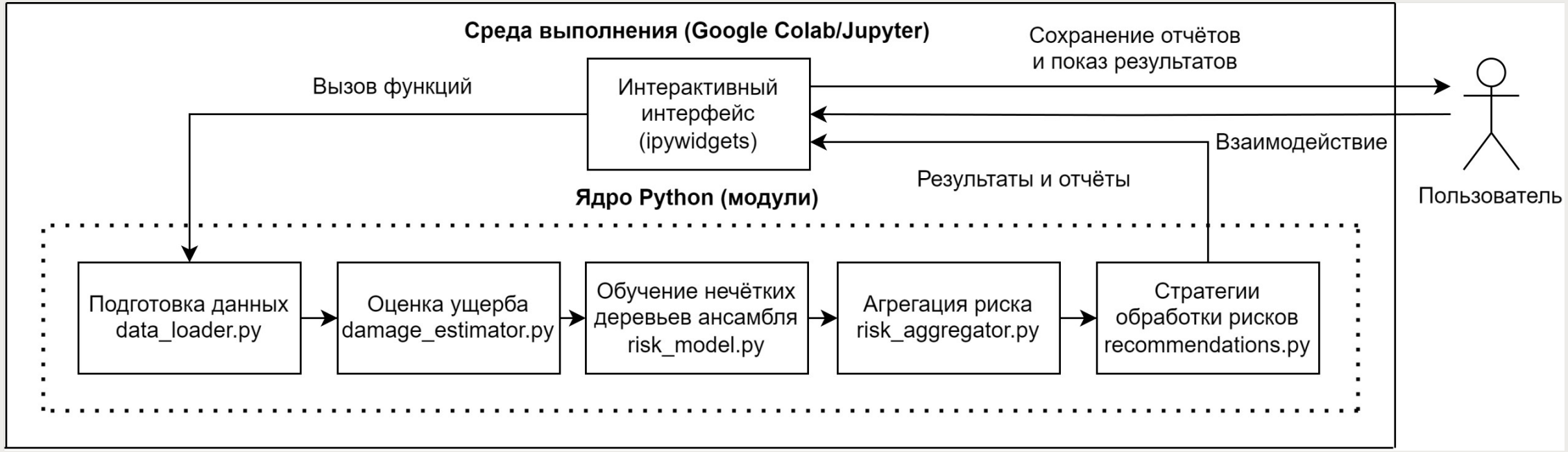
Практическая польза

- Автоматизация анализа рисков ИБ, предложение стратегий их обработки и возможных решений
- Обоснование бюджета на защиту
- Снижение влияния человеческого фактора
- Интерпретируемость

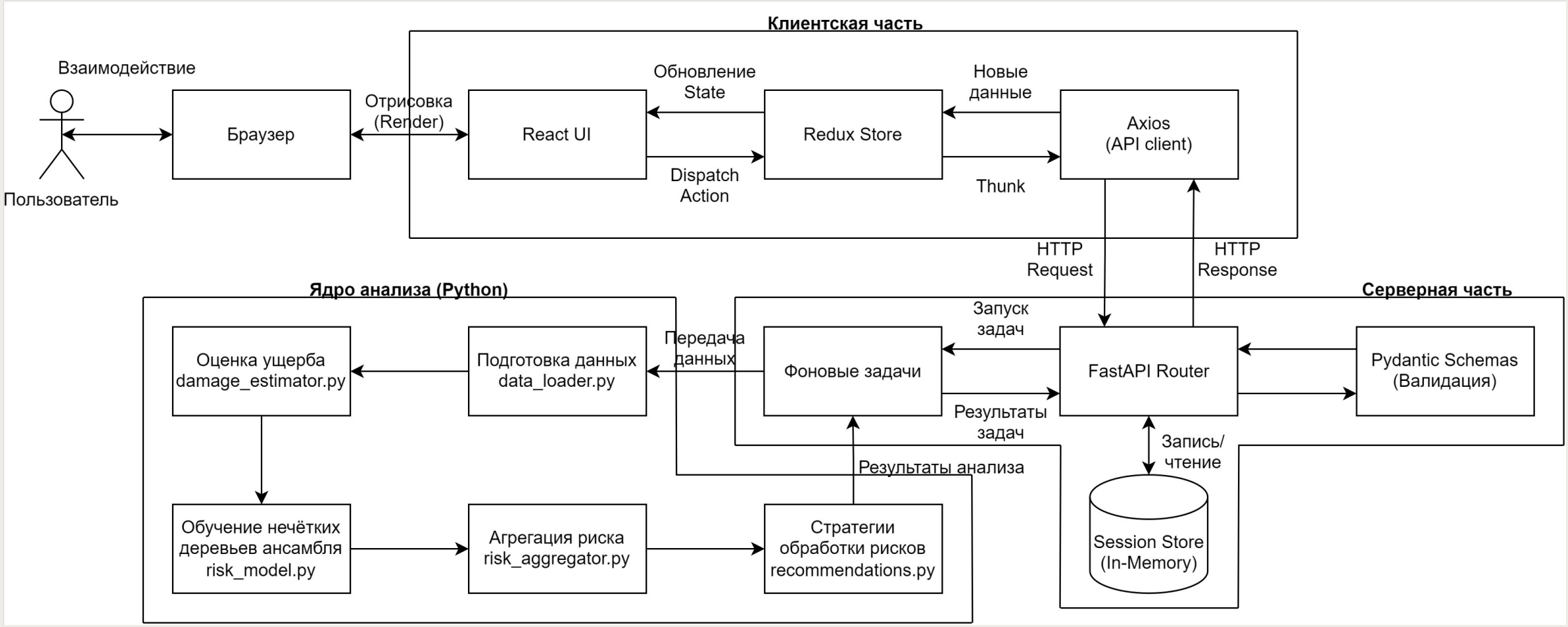
Целевая аудитория

- Студенты (бакалавры и магистры)
- Аспиранты
- Специалисты по ИБ
- Аналитики центров мониторинга безопасности
- Риск-менеджеры
- Аналитики данных

АРХИТЕКТУРА РЕШЕНИЯ
GOOGLE COLAB И ЛОКАЛЬНЫЙ JUPYTER



АРХИТЕКТУРА РЕШЕНИЯ
ВЕБ-ПРИЛОЖЕНИЕ



ТЕОРИЯ
МАТЕМАТИЧЕСКАЯ МОДЕЛЬ ОЦЕНКИ РИСКА

$\mathbf{R = P \times D}$, где

R – совокупный риск

P – вероятность реализации риск-события, прогнозируется моделью

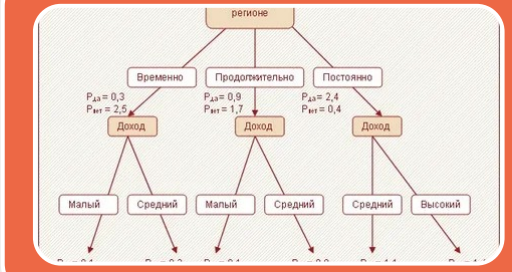
D – нормированный ущерб

$\mathbf{D = \sum_{i=1}^{5}(w_i \times d_i)}$, где

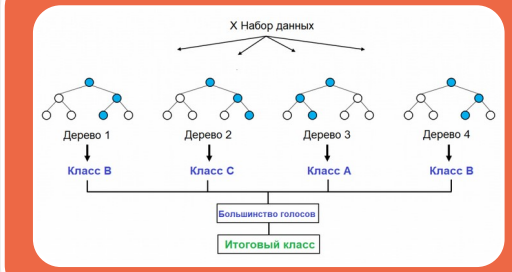
$\mathbf{w_i}$ – экспертный вес категории ущерба

$\mathbf{d_i}$ – оценка ущерба

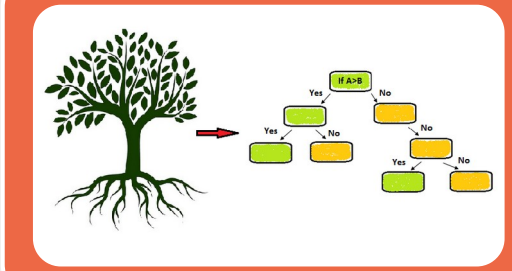
ТЕОРИЯ
НЕЧЁТКИЕ ДЕРЕВЬЯ И ИХ АНСАМБЛЬ



Нечёткое дерево решений – это метод машинного обучения, который объединяет классическую структуру деревьев решений с принципами нечёткой логики. Его ключевое отличие в том, что он использует функции принадлежности вместо жёстких порогов. Объект распределяется по ветвям с определёнными вероятностями



Ансамбль нечётких деревьев решений – это метод машинного обучения, который объединяет несколько моделей в виде «леса» нечётких решающих деревьев. Происходит усреднение прогнозов для снижения дисперсии и обучение множества деревьев на случайных подвыборках данных и признаков



Преимущества подхода:

- Устойчивость к шумам, выбросам и переобучению
- Работа с размытыми экспертными понятиями
- Интерпретируемость полученных результатов

ТЕОРИЯ
МАТЕМАТИЧЕСКАЯ РЕАЛИЗАЦИЯ

$$\mathbf{P}(\hat{y}|\mathbf{x}) = \sum_{l=1}^{L} \boldsymbol{\pi}_l(\mathbf{x}) \times \mathbf{P}_l(\hat{y}|\mathbf{x})$$, где

$\mathbf{L}$ – количество листьев в дереве

$\boldsymbol{\pi}_l(\mathbf{x})$ – вероятность достижения листа $\mathbf{l}$ (произведение нечётких условий)

$\mathbf{P}_l$ – распределение классов в листе

Механизм мягкого вывода

$$\mathbf{P}_{final} = \frac{1}{T}\sum_{t=1}^{T} \mathbf{P}_t$$, где

$\mathbf{T}$ – количество деревьев в ансамбле

Ансамблирование (бэггинг)

ТЕОРИЯ
МНОГОКРИТЕРИАЛЬНАЯ ОЦЕНКА УЩЕРБА

Ущерб от реализации риска носит многокритериальный характер в ИТ-организации. Для этого он был разделён на пять категорий: потери данных, финансовый, репутационный, операционный и юридический.

Также ущерб может быть задан экспертом различным образом:

Числовой режим –
эксперт задаёт веса категорий ущерба ползунками

Лингвистический режим –
эксперт задаёт ущерб через термы, которые переводятся в баллы

РЕАЛИЗАЦИЯ

GOOGLE COLAB И ЛОКАЛЬНЫЙ JUPYTER

- Монолитная архитектура (всё в одном окне)
- Интерактивные виджеты (ipywidgets)
- Мгновенный экспорт (CSV, HTML, PDF)
- Быстрый запуск без установки ПО

Интеллектуальный анализ рисков ИБ

Данные | Анализ

Данные

Источник: Сгенерировать / Загрузить файл

Сценарий: Сбалансированный

Записей: 500

Сгенерировать данные

Предпросмотр датасета

◀ Назад | Страница 1 / 50 | Вперёд ▶ | Перейти к странице: 1 | Перейти

Показаны записи 1–10 из 500

	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	Security	DB_Query	3.012354	5	9	2	1	18.757193	4	1	
2	2025-01-01 00:05:00	IT_Ops	Config_Change									
3	2025-01-01 00:10:00	HR	Config_Change									

Результаты анализа рисков

◀ Назад к настройкам

Метрики качества модели

- **Accuracy (Точность)** – доля правильных ответов: 0.647
- **F1-score (F1-мера, баланс точности и полноты):** 0.701
- **AUC-ROC (площадь под ROC-кривой):** 0.733
- **Порог классификации:** 0.45

Экспертные веса ущерба

Категория	Вес
Финансовый	0.250000
Репутационный	0.250000
Операционный	0.200000
Юридический	0.150000
Потеря данных	0.150000

Рекомендации по обработке рисков

◀ Назад | Страница 1 / 15 | Вперёд ▶ | Перейти к странице: 1 | Перейти

Показаны записи 1–10 из 150

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 Development. CVSS-оценка 8.5 указывает на высокую критичность.	0.527000	28.800000	15.160000	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. Проводить статический и динамический анализ кода, использовать безопасные фреймворки, обновлять библиотеки Учитывая высокий CVSS-скор, приоритизировать исправление уязвимости в течение 48 часов.
							Внедрить дополнительные средства

Визуализация результатов

◀ Назад к результатам

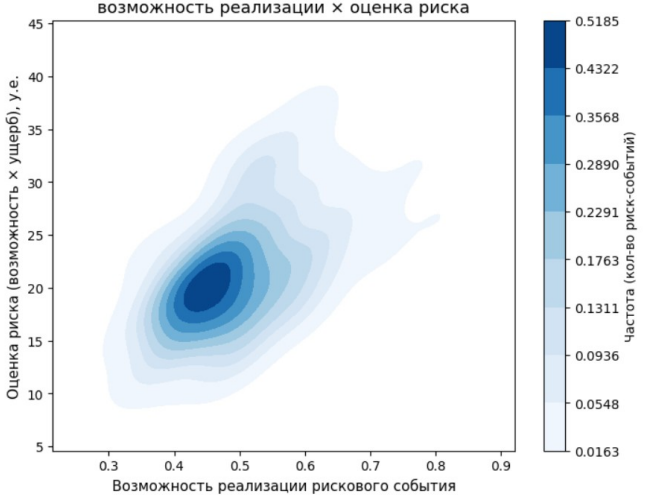
Фильтры данных

Отдел: Все

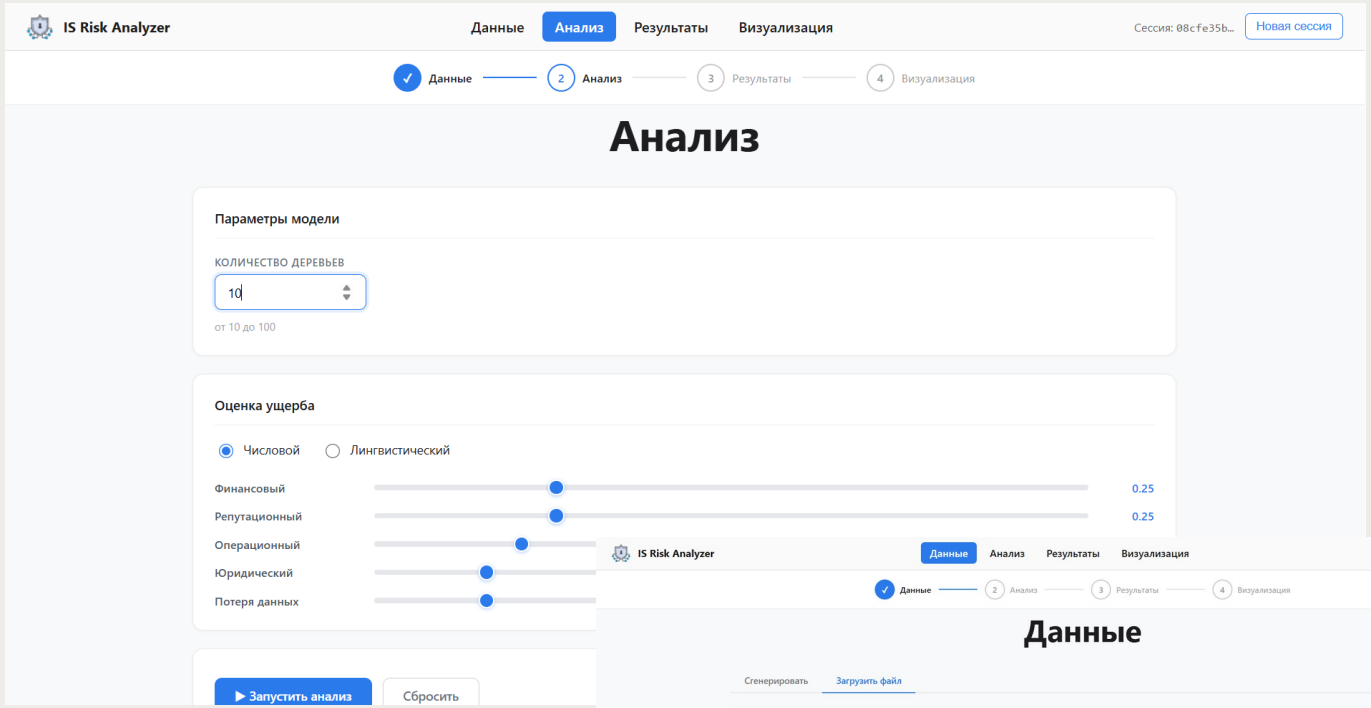
Событие: Все

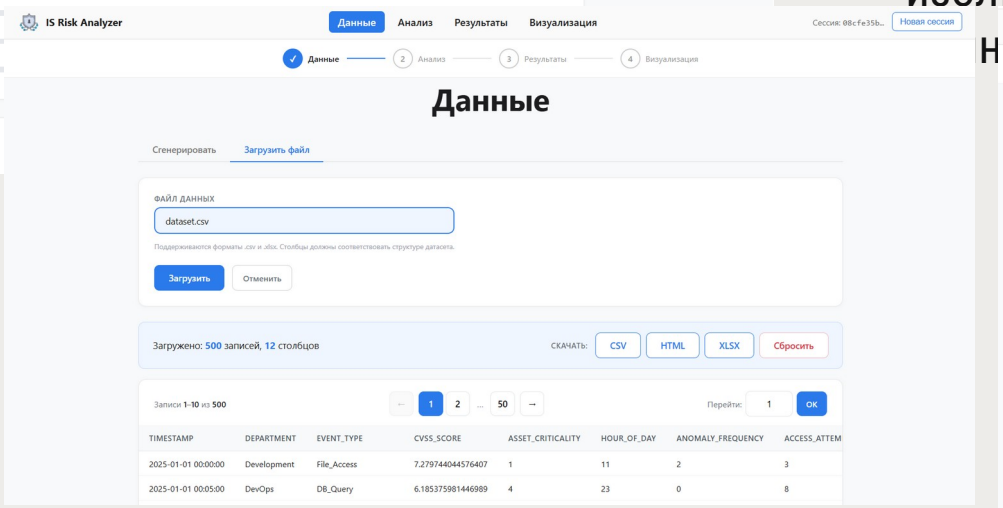
Уровень р… Все

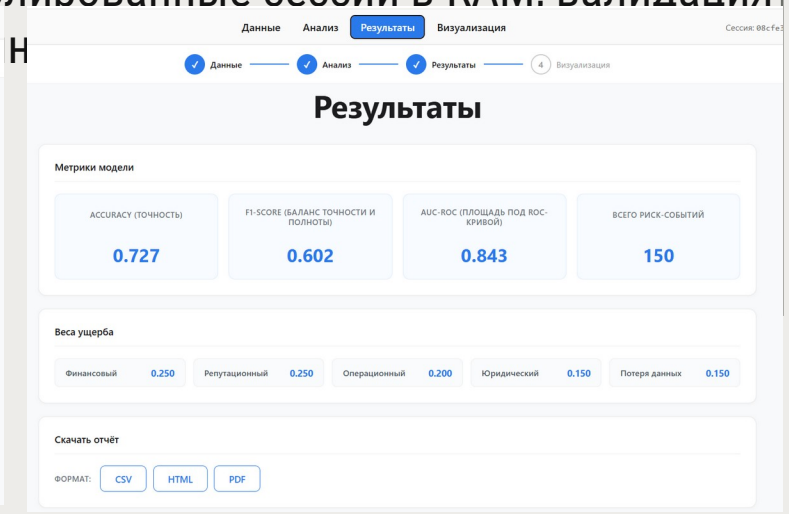
Визуализация результатов



РЕАЛИЗАЦИЯ
ВЕБ-ПРИЛОЖЕНИЕ







Реализовано в дополнение к указанному в заявке.
Стек: React и Redux Toolkit, Python, FastAPI.
UX-решения:
- Пошаговый мастер (Stepper)
- Прогресс-бар выполнения задач
- Блокировка интерфейса во время вычислений (защита от ошибок)
4 вкладки: Данные, Анализ, Результаты, Визуализация
Фоновая обработка задач, изолированные сессии в RAM, валидация

РЕАЛИЗАЦИЯ
РЕЗУЛЬТАТЫ И ВИЗУАЛИЗАЦИЯ

Скачать отчёт

ФОРМАТ: CSV HTML PDF

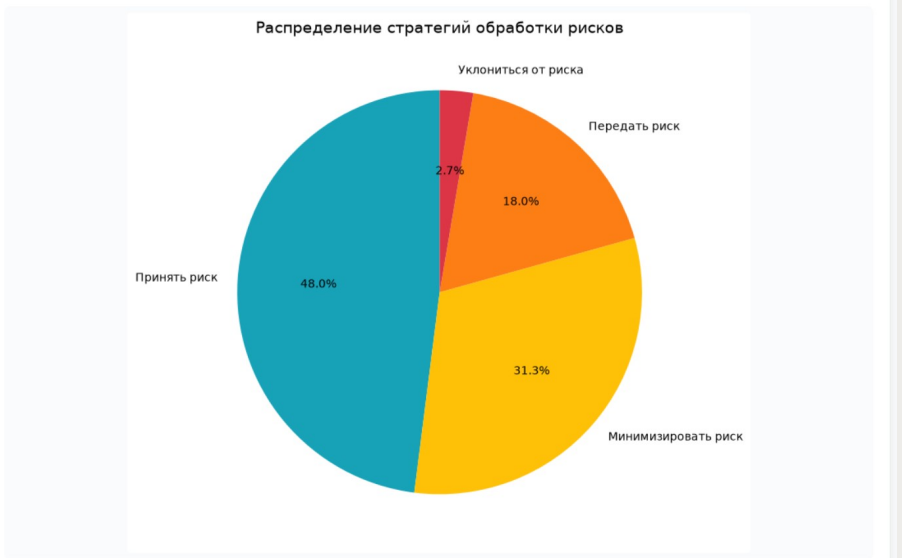
Рекомендации по обработке рисков — Всего записей: 150

Записи 1–10 из 150 ← 1 2 ... 15 → Перейти: 1 OK

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 Auth_Attempt в отделе Security. CVSS-оценка 7.9 указывает на высокую критичность.	0.648	53.4	34.56	Высокий	Минимизировать риск	Внедрить дополнит… Рекомендуемые мер… аутентификацию, ус… для обнаружения ан… безопасности, пров… кибербезопасности… приоритизировать …
Событие №2	Выявлена уязвимость в ИТ-архитектуре: обнаружены подозрительные DB_Query в отделе HR. CVSS-оценка 4.2 требует внимания.	0.441	45.0	19.82	Низкий	Принять риск	Мониторить в рамк… не требуются. Реком… данных, настроить а… параметризованны… Защитить персонал… конфиденциальност… данных. Учитывая ср… исправление в ближ…

- 11 графиков с фильтрацией по отделам и типам событий
- Суррогатное дерево
- Таблица с рекомендациями по обработке рисков
- Оценка качества модели (AUC, F1, Accuracy)
- Экспорт всех графиков одним ZIP-архивом
- Экспорт отчётов в форматах CSV, HTML и PDF

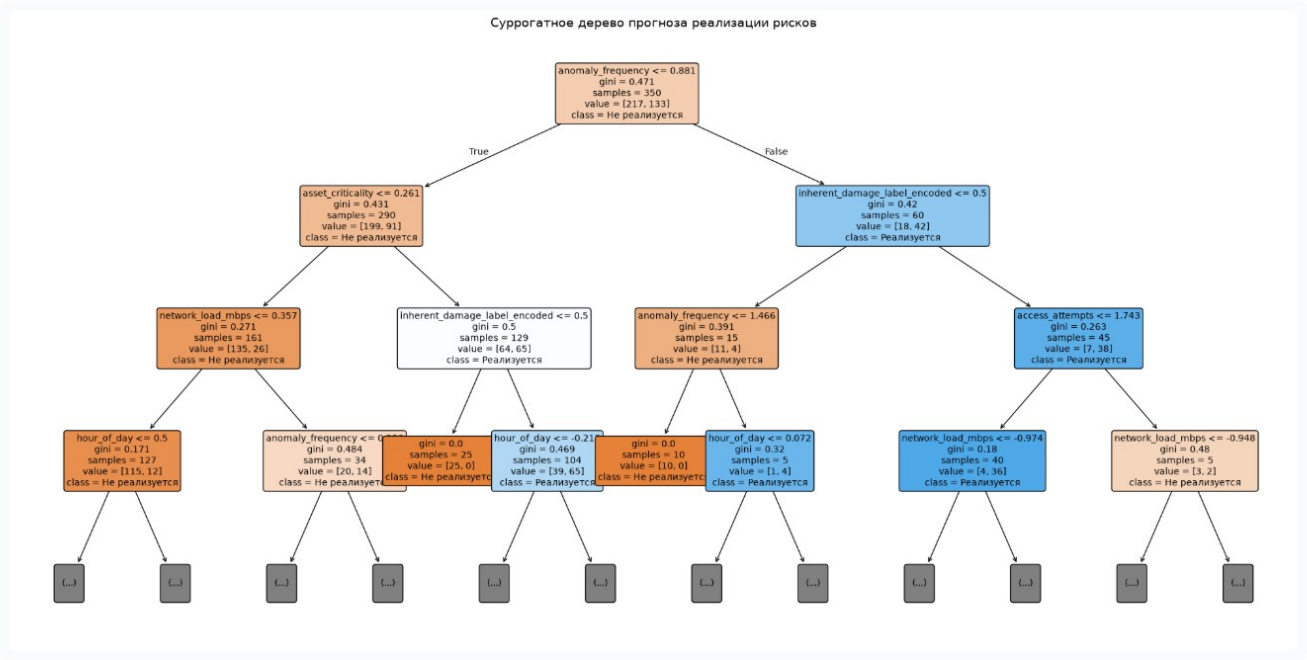
8. Распределение стратегий обработки рисков



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

РЕАЛИЗАЦИЯ
ОБЪЯСНИМОСТЬ МОДЕЛИ (СУРРОГАТНОЕ ДЕРЕВО)

12. Суррогатное дерево прогноза реализации рисков



Суррогатное дерево - это обычное решающее дерево, обученное на прогнозах ансамбля нечётких деревьев. Служит для визуализации логики работы модели.

- Решение проблемы «чёрного ящика»
- Имитация логики ансамбля простым деревом решений
- Прозрачность – аналитик видит вклад каждого признака

ТЕХНИЧЕСКАЯ ВОСПРОИЗВОДИМОСТЬ ПРОЕКТА



латформенность и изоляция окружения: поддержка Windows, macOS, Linux; зование venv для исключения конфликтов системных библиотек; файл ments.txt с жёсткой фиксацией версий (pandas, scikit-learn, fuzzytree, FastAPI).



минированность ML-модели: фиксация seed для бэггинга и генерации ущерба, ение эффекта «скачущих» результатов (одинаковые данные всегда дают чные метрики).



матизация развертывания: Скрипт start.bat для Windows (автосоздание окружения, вка Python/Node.js зависимостей, запуск FastAPI и React), готовый архив files.zip для мгновенного развертывания в Google Colab или Jupyter (ячейки здают структуру папок и модули), наличие Swagger UI и готовых коллекций для ирования API.

МЕТОДИЧЕСКАЯ ГОТОВНОСТЬ К ВНЕДРЕНИЮ

Полный комплекс документации – методические указания и инструкции по запуску, Readme-файлы для разработчиков, видеоматериалы

Интеграция (готовность API) – встроенная интерактивная документация Swagger UI, возможность тестирования всех эндпоинтов без написания кода

Модульность архитектуры – ML-ядро изолировано от веб-интерфейса и работает как независимо, возможно встроить в существующие SOAR- и SIEM-системы через REST API

Внедрение в образовательный процесс – изучение ML и нечёткой логики, принципов веб-и бэкенд разработки, основа для проведения практических занятий

БЕЗОПАСНОСТЬ ПРЕДЛАГАЕМЫХ РЕШЕНИЙ

- Конфиденциальность данных – локальные вычисления, отсутствие передачи корпоративных данных на сторонние API
- Изоляция пользовательских сессий – уникальный идентификатор для каждой сессии, хранение данных в оперативной памяти сервера без пересечения между разными аналитиками
- Безопасность ввода – строгая типизация и валидация загружаемых CSV/XLSX файлов на уровне бэкенда, защита от инъекций, вредоносного кода и превышения лимитов памяти
- Объяснимый ИИ – прозрачность модели исключает скрытые уязвимости «чёрного ящика», возможность аудита (специалист по ИБ всегда может проверить, на основании каких признаков модель присвоила риск)

ЗАКЛЮЧЕНИЕ И ПОТЕНЦИАЛЬНЫЕ НАПРАВЛЕНИЯ РАЗВИТИЯ





Разработан метод интеллектуального анализа рисков ИБ в ИТ-организации, который реализован в двух вариантах и обеспечивает высокую интерпретируемость результатов. Проект полностью готов к внедрению и масштабированию

Направления развития:
- Разработка коннекторов к реальным SIEM-системам (Splunk, QRadar, MaxPatrol) для автоматического сбора логов
- Переход от In-Memory сессий к СУБД для работы в крупных сетях
- Интеграция с базами знаний об угрозах для повышения точности ML-модели