Руководство пользователя

Arachnid Threat Modeling

2025 год

Оглавление

1 Введение

1.1 Описание приложения

Приложение Arachnid Threat Modeling (далее Arachnid.TM) предназначено для поддержки специалистов по информационной безопасности и информационным технологиям (далее Пользователь) при решении задач – моделирования киберугроз.

1.2 Цели и преимущества

Arachnid.TM позволяет Пользователю построить диаграмму из узлов и их связей, представляющих модель информационной инфраструктуры. Для узлов провести анализ возможных кибератак и оценить вероятности. Для выявленных и указанных атак, система помогает рассчитать вероятности и диапазоны потерь в финансовых показателях.

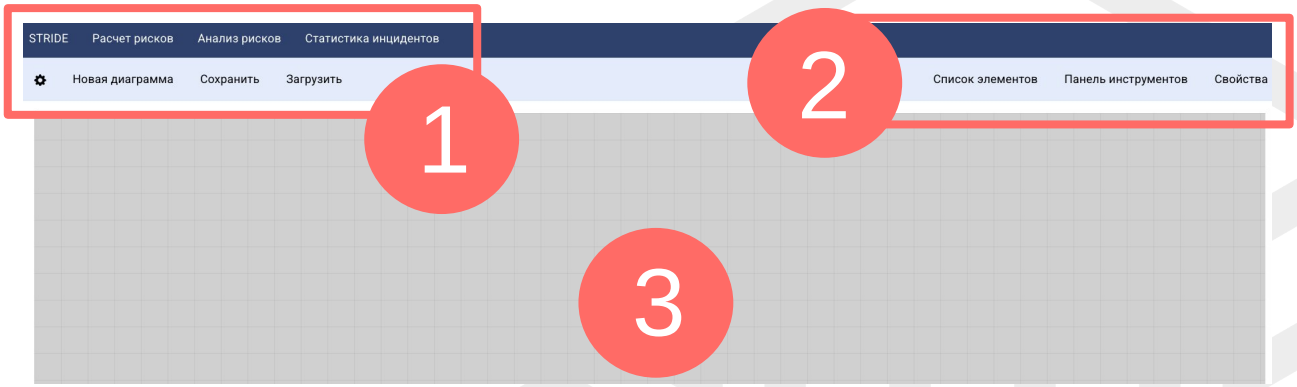
Для визуализации расчетов используется табличное и интерактивное графическое представление. Для более эффективного использования Arachnid.TM рекомендуется ознакомится с литературой в открытых источниках о методологиях моделирования угроз типа: STRIDE & LINDDUN.

1.3 Обзор интерфейса

Основное меню

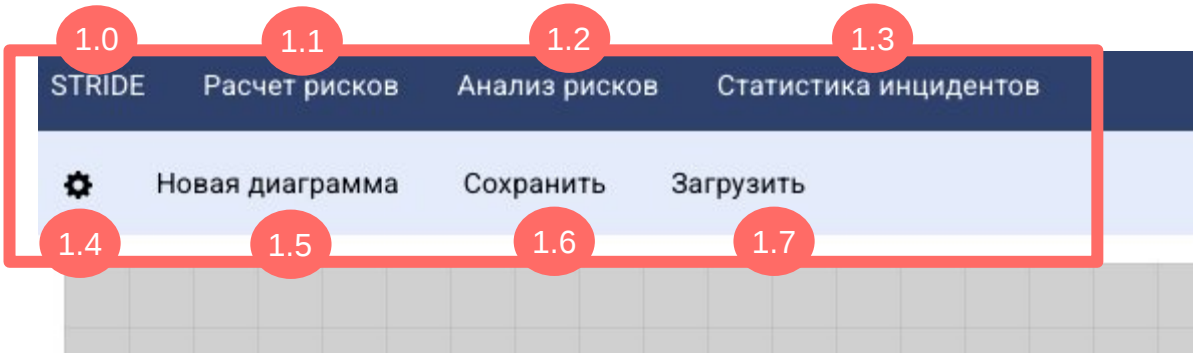
Для удобства разбора возможностей решения мы условно разделим экрана на три области (см. Скриншот 1):

1 Область навигации и глобальных настроек (прим. отмечено цифрой 1)
2 Область локальных настроек для элементов (прим. отмечено цифрой 2)
3 Область для работы и отображения диаграмм, таблиц и графиков (прим. Отмечено цифрой 3)



Скриншот 1

1.3.1 Область навигации и глобальных настроек (см. Скриншот 2):



Скриншот 2

1.0 **STRIDE** – вкладка, перейдя на которую, пользователь может начать (продолжить) проектирование диаграмм для создания модели инфраструктуры и анализа возможных кибератак.

1.1 **Расчёт рисков** – вкладка, перейдя на которую, пользователь может увидеть результаты расчёта и введённые данные по атакам с предыдущей вкладки (Расчет рисков).

1.2 **Анализ рисков** – вкладка, перейдя на которую, пользователь может увидеть результаты расчёта и введённые данные по атакам с предыдущей вкладки (Расчет рисков).

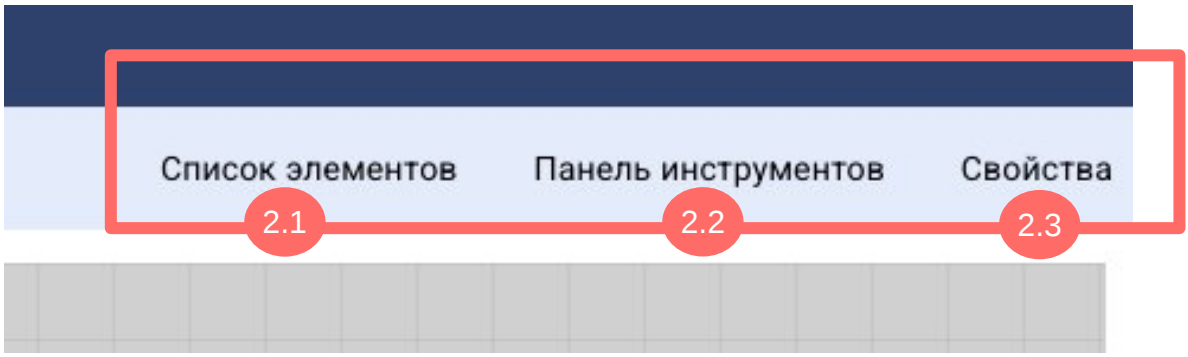
1.3 **Статистика инцидентов -** вкладка, перейдя на которую, пользователь может начать работу с отдельным инструментом “распределения частоты инцидентов”.
1.4 **Новая диаграмма –** система предложит пользователю ввести имя для новой модели угроз и продолжить работу уже с ней.

1.5 **Настройки -** система предложит пользователю выбрать таксономию угроз для моделирования (нужно выбрать один из двух вариантов STRIDE и LINDDUN, по умолчанию выбран STRIDE).

1.6 **Сохранить –** система сохраняет текущую модель со всеми данными.

1.7 **Загрузить -** пользователь сохраняет текущую модель со всеми данными.

1.3.2 Область локальных настроек для элементов



Скриншот 3

2.1 **Список элементов -** вкладка, выбрав которую, пользователь может увидеть все добавленные элементы на рабочую область в виде списка. При отсутствии добавленных элементов список будет пустым.

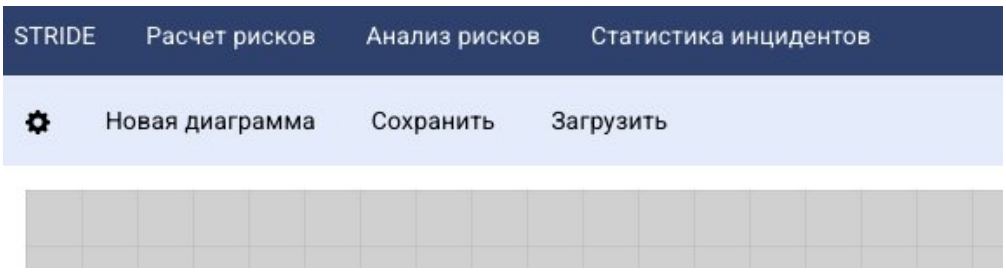
2.2 **Панель инструментов** - вкладка, на которой отображаются иконки всех доступных из библиотеки элементов для моделирования диаграммы и анализ угроз. Выбирая из этого списка и добавляя на рабочую область, пользователь формирует необходимую ему топологию (связность) анализируемой модели угроз.

2.3 **Свойства** - вкладка, на которой пользователю доступны для ввода поля характеризующие атаку (тип, вероятность, ущерб и так далее.)

2 Практические примеры

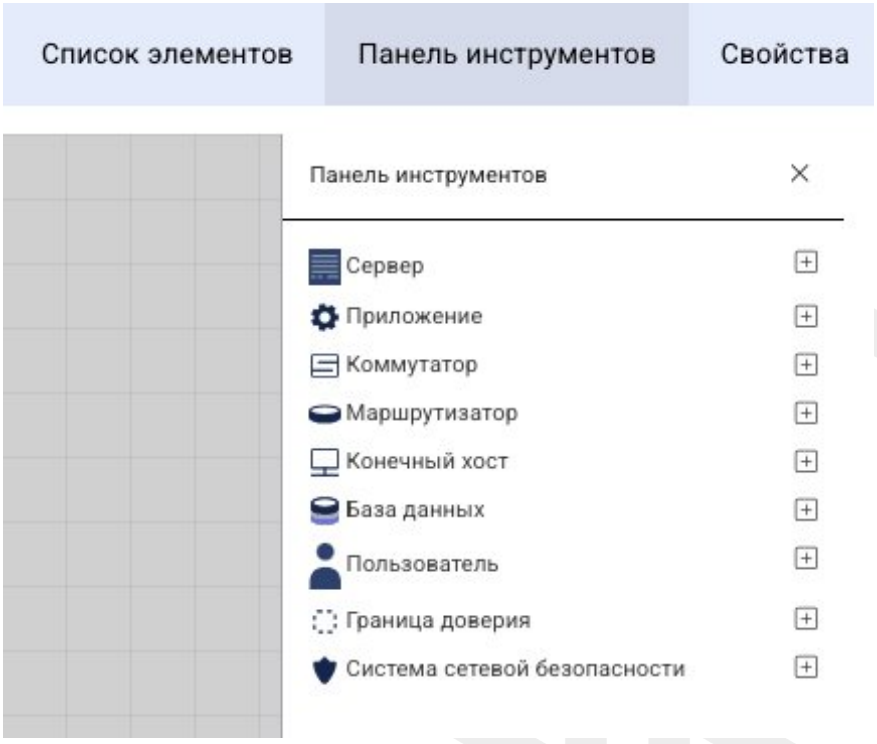
2.1 Создание модели угроз

1. **Шаг 1** - Пользователь нажимает “Новая диаграмма” чтобы создать новую диаграмму



Скриншот 4

2. **Шаг 2** - Пользователю указывает имя для новой диаграммы и нажимает “ok”
3. **Шаг 3** - Пользователь выбирает необходимые элементы инфраструктуры в Панели инструментов

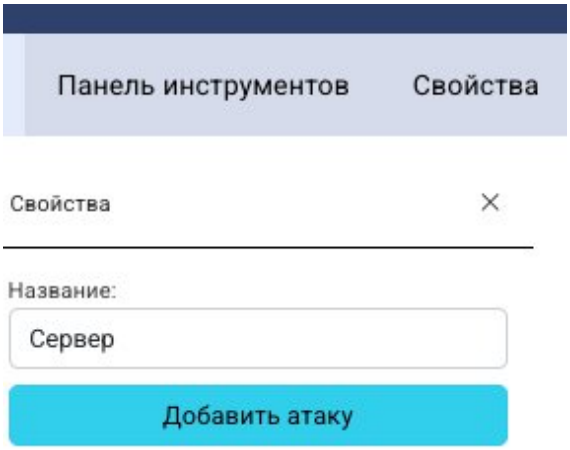


Скриншот 5

4. Система отображает выбранные элементы из Панели инструментов на рабочей области

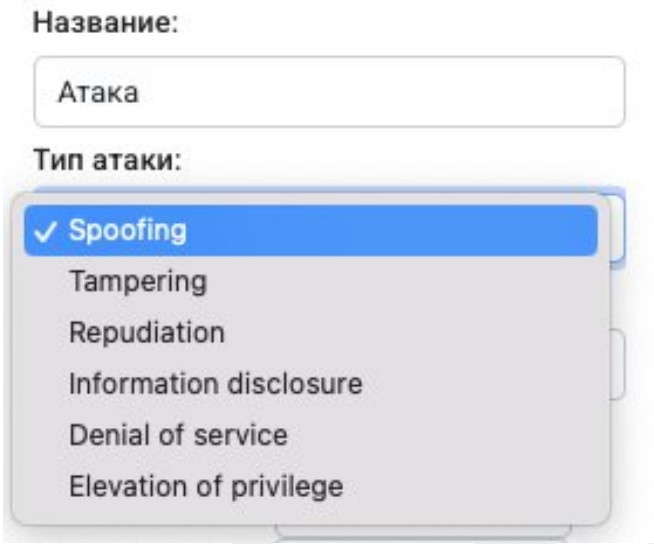
Скриншот 6

5. **Шаг 4** - Пользователь выбирает элемент на схеме, чтобы перейти в свойства для анализа вероятности кибератаки



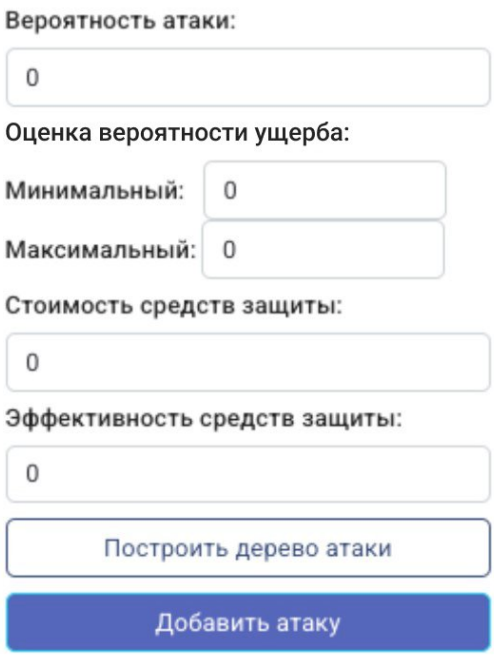
Скриншот 7

6. **Шаг 5** - Пользователь выбирает тип атаки из списка по STRIDE



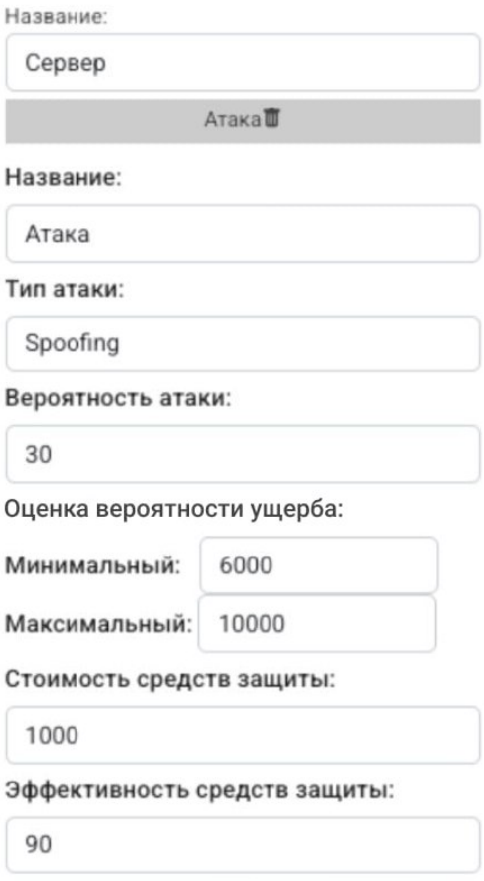
Скриншот 8

7. Система предлагает заполнить следующие поля



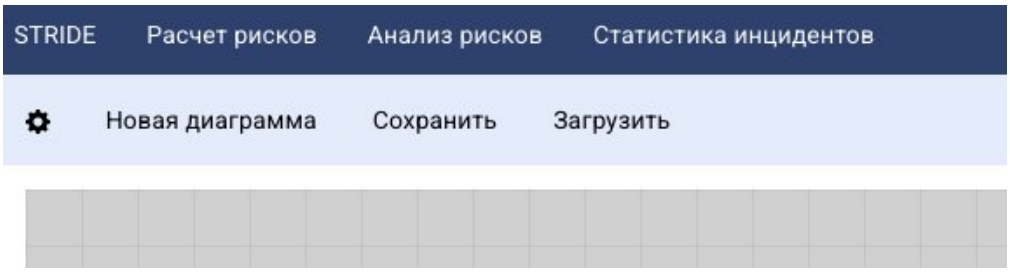
Скриншот 9

8. **Шаг 6** - Пользователю указывает данные в полях для ввода



Скриншот 10

9. Система осуществляет расчёт
10. **Шаг 7** - Пользователь переходит на следующую вкладку – Расчет рисков

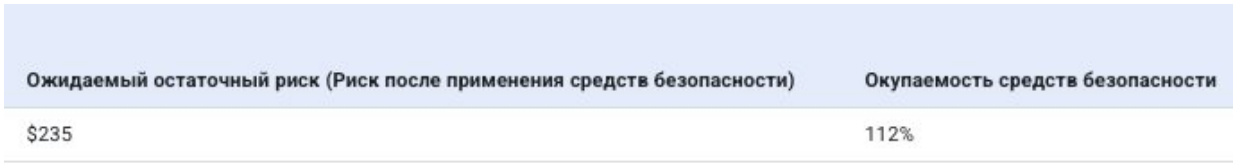


Скриншот 11

11. Система демонстрирует результаты расчета в таблице

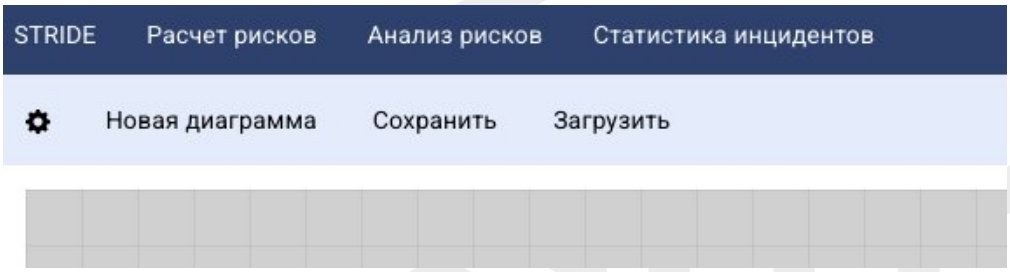
Скриншот 12

Скриншот 13



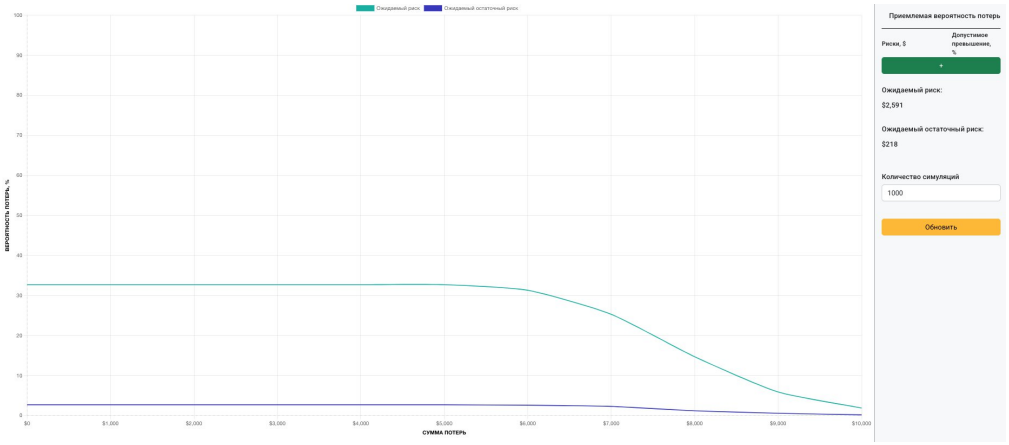
Скриншот 14

12. **Шаг 8** - Пользователь переходит на следующую вкладку – Анализ рисков



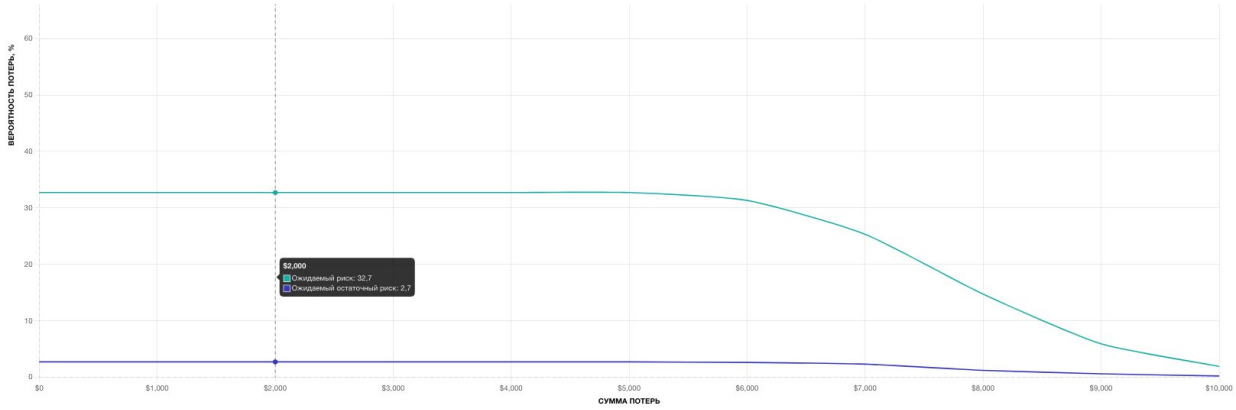
Скриншот 15

13. Система отображает область с графиком расчета “ожидаемого и ожидаемого остаточного риска” – 1, а также панель с уточнением “Приемлемой вероятностью потерь” – 2 (см. Скриншот 16)



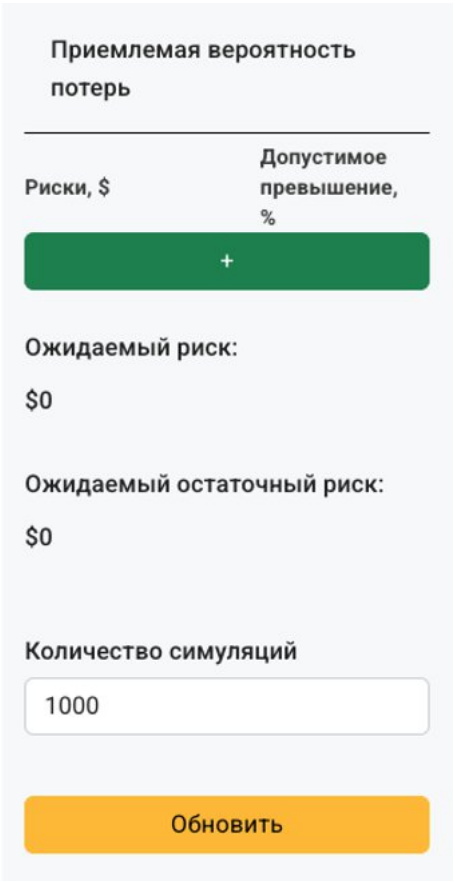
Скриншот 16

14. **Шаг 9** – Пользователь может изучить зависимость вероятность потерь и суммы потерь на графике



Скриншот 17

15. **Шаг 10** - Пользователь может изменить значения для рисков и их вероятности и запустить пересчет по методу Монте-Карло (количество симуляций по умолчанию = 1000)



Скриншот 18

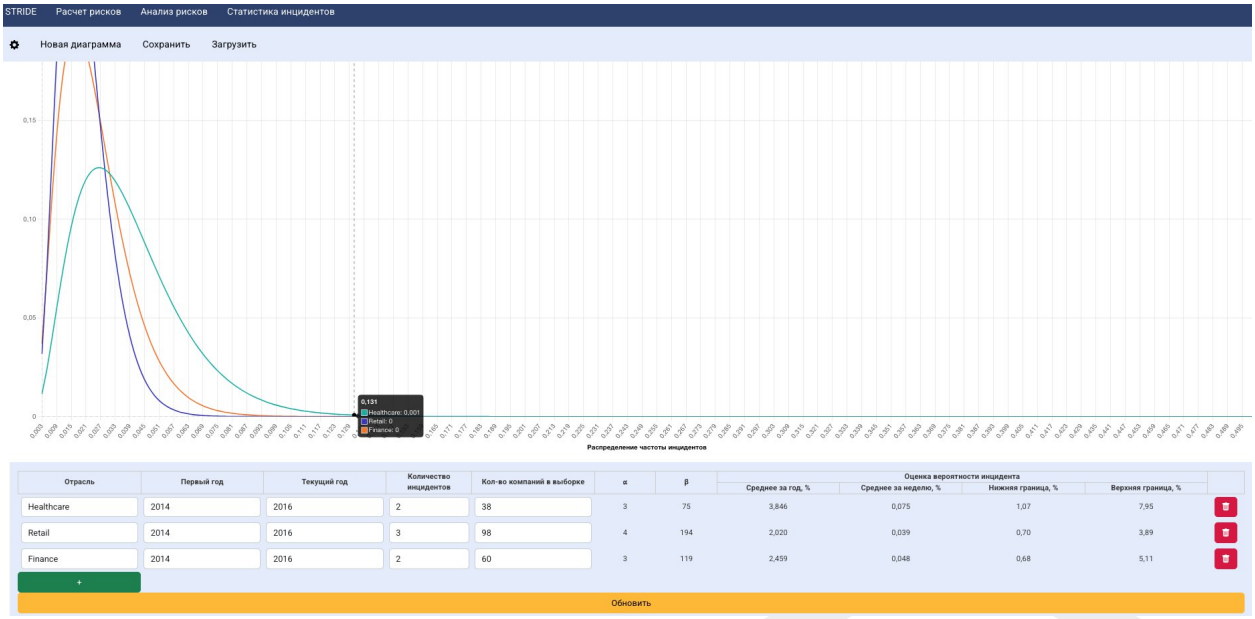
16. Отлично! Вы только что закончили основной путь пользователя при работе с Arachnid.TM.

2.2 Расчёт статистики инцидентов

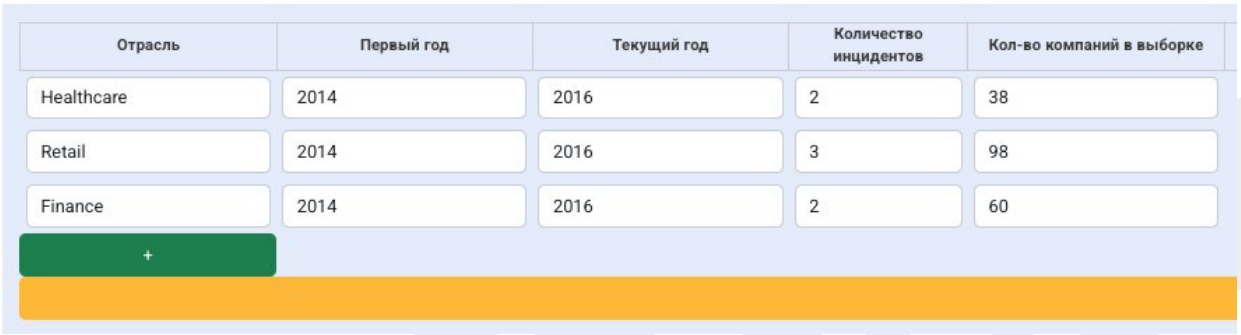
Пользователю доступен дополнительный инструмент, несвязанный с предыдущим рассмотренным анализом угроз и рисков по STRIDE.

Расчёт статистики инцидентов - позволяет ввести вручную данные по инцидентам для различных отраслей, предприятий или других исследуемых субъектов. Используя алгоритмы, альфа и бета распределений из математической статистики можно получить расчёты для вероятности появления инцидентов.

1. **Шаг 1** - Пользователь вводит имеющиеся у него данные по статистике инцидентов (см. Скриншоты 19,20) и нажимает “Обновить”



Скриншот 19



Скриншот 20

2. Система отображает результаты расчётов на графике и в таблице

Оценка вероятности инцидента			
Среднее за год, %	Среднее за неделю, %	Нижняя граница, %	Верхняя граница, %
3,846	0,075	1,07	7,95
2,020	0,039	0,70	3,89
2,459	0,048	0,68	5,11

Скриншот 21

3. Отлично! Вы только что закончили дополнительный путь пользователя при работе с Arachnid.TM.

3 Контакты поддержки

По вопросам эксплуатации решения **Arachnid.TM** вы можете обратиться в нашу службу поддержки - hello@arachnd.ru

Пожалуйста, указывайте в теме письма – **threat modelling** если у вас есть вопросы именно по использованию решения **Arachnid.TM**
Удачи!