Алгоритм представления математической модели остаточного риска

**Человек:** Большинство современных методик оценки и управления рисками используют значение остаточного риска как числовой показатель, характеризующий риск угрозы после применения всех контрмер, при этом не уделяют ему должного внимания. В работе изображен алгоритм позволяющий представить остаточный риск угрозы информационной безопасности в виде математической модели, что в свою очередь дает возможность более подробно проанализировать рассматриваемый параметр и саму модель, коэффициенты в которой показывают на сколько сильно входные параметры влияют на итоговый результат. Алгоритм получения математической модели остаточного риска строился на базе полного факторного эксперимента, с учетом особенностей рассматриваемого параметра. Данное представление позволит анализировать значение остаточного риска не только как некоторого числового показателя, но и как математическую модель, что в дальнейшем может помочь методикам оценки и управления рисками гораздо шире использовать остаточный риск для улучшения качества системы защиты информации на предприятии.

**Key words:** алгоритм, угрозы информационной безопасности, система защиты информации, математическая модель, остаточный риск, полный факторный эксперимент, коэффициенты модели, риск угрозы, прочность механизмов защиты, методы оценки риска

=================================

**FastText\_KMeans\_Clean:** Далее нам необходимо перейти к нормированным значениям для упрощения расчета коэфициентов. Нормированные величины. Расчитываем коэффициенты математической модели при нормированных значениях по следующей формуле `bara\_(g)=1/N\*sum\_(i=1)^N <<y\_(i)>>\*barx\_(gi)` , где индекс `g` указывает номер столбца, индекс `i` - номер строки. Рассмотренный в работе алгоритм позволяет представить значение осаточного риска для любой угрозы информационной безопаснсоти в виде математической модели, что можно использовать для улучшения качества системы защиты информации, с учетом рассмотрения остаточного риска не только как числового показателя, но и как математическую функцию.

**Key words part:** 0.696969696969697

=================================

**FastText\_KMeans\_Raw/:** В матрице эксперимента количество столбцов равно числу коэффициентов функции, а количество строк определяется по формуле `N=2^(n)` , где `n` ` ` - число входных параметров. На основе матрицы эксперимента составляется система уравнений, которая используется для расчета коэффициентов. Нормированные величины. Рассмотренный в работе алгоритм позволяет представить значение осаточного риска для любой угрозы информационной безопаснсоти в виде математической модели, что можно использовать для улучшения качества системы защиты информации, с учетом рассмотрения остаточного риска не только как числового показателя, но и как математическую функцию.

**Key words part:** 0.7272727272727273

=================================

**FastText\_PageRank\_Clean/:** Управление рисками строится на их оценки, которая включает в себя анализ и оценивание. Алгоритм строится на базе полного факторного эксперимента [6,7]. Проведение параллельных опытов используется для получения более точного результата. Проведем аппроксимацию нашей функции `y=f(x\_(1),x\_(2))` линейной`y=a\_(0)+a\_(1)\*x\_(1)+a\_(2)\*x\_(2)` . Матрицу эксперимента представим в виде таблицы. Дисперсия определяется по формуле:` S\_(i)^(2)=(1)/(1-n)\*sum\_(i=1)^n (y\_(i) - << y>>)^(2)`, где `n` - число параллельных опытов. При переходе верхние значения параметров приравниваются к 1, а нижние к -1. Нормированные величины.

**Key words part:** 0.4545454545454545

=================================

**FastText\_PageRank\_Raw/:** Алгоритм строится на базе полного факторного эксперимента [6,7]. Проведение параллельных опытов используется для получения более точного результата. Рассмотрим произвольную угрозу информационной безопасности, для которой: `P=0,38, Z=53, m=0,8, R=0,38\*53=20, deltaR=2, deltam=0,1`. Матрицу эксперимента представим в виде таблицы. Столбоц `x\_(0)` добавлен для возможности расчета коэффициента`a\_(0)`. При переходе верхние значения параметров приравниваются к 1, а нижние к -1. Нормированные величины. В результате расчетов получилась следующая математическая модель: `y=-3,9+0,2\*x\_(1)+20\*x\_(2)`.

**Key words part:** 0.6363636363636364

=================================

**Mixed\_ML\_TR/:** Существуют различные методы направленные на поиск оптимального значения оценки рисков информационной безопасности и их анализа: метод нечёткой кластеризации и вычисления взаимной информации[1], матричный подход[2], нечёткий всесторонний метод[3], на основе предикатов и логического вывода[4] и т.д. Результатом оценки риска после внедрения мер противодействия угрозе информационной безопасности является значение остаточного риска. Остаточный риск расчитывается по формуле `R\_(ost)=R\*(1-m) ` , где `R` - риск угрозы, `m` - прочность механизмов защиты и представляет из себя остающийся, потенциальный риск после применения всех контрмер[5], он является важным показателем качества механизмов противодействия и как следствие играет важную роль в управлении рисками информационной безопасности, что делает вопрос математического описания остаточных рисков актуальным. На основе матрицы эксперимента составляется система уравнений, которая используется для расчета коэффициентов. Проведем аппроксимацию нашей функции `y=f(x\_(1),x\_(2))` линейной`y=a\_(0)+a\_(1)\*x\_(1)+a\_(2)\*x\_(2)` . Далее нам необходимо перейти к нормированным значениям для упрощения расчета коэфициентов. При расчетах все условия проверки алгоритма были соблюдены, что говорит об адекватности расчитанных коэффициентов и самой математической содели. В результате использования алгоритма мы получаем линейную функцию остаточного риска`R\_(ost)=-3,9+0,2\*x\_(1)+20\*x\_(2)` с рассчитанными коэффициентами, которые показывают насколько сильно каждый параметр оказывает влияние на итоговый результат. Рассмотренный в работе алгоритм позволяет представить значение осаточного риска для любой угрозы информационной безопаснсоти в виде математической модели, что можно использовать для улучшения качества системы защиты информации, с учетом рассмотрения остаточного риска не только как числового показателя, но и как математическую функцию.

**Key words part:** 0.9393939393939394

=================================

**MultiLingual\_KMeans/:** Существуют различные методы направленные на поиск оптимального значения оценки рисков информационной безопасности и их анализа: метод нечёткой кластеризации и вычисления взаимной информации[1], матричный подход[2], нечёткий всесторонний метод[3], на основе предикатов и логического вывода[4] и т.д. Результатом оценки риска после внедрения мер противодействия угрозе информационной безопасности является значение остаточного риска. На основе матрицы эксперимента составляется система уравнений, которая используется для расчета коэффициентов. Проведем аппроксимацию нашей функции `y=f(x\_(1),x\_(2))` линейной`y=a\_(0)+a\_(1)\*x\_(1)+a\_(2)\*x\_(2)` . Далее нам необходимо перейти к нормированным значениям для упрощения расчета коэфициентов. При расчетах все условия проверки алгоритма были соблюдены, что говорит об адекватности расчитанных коэффициентов и самой математической содели.

**Key words part:** 0.7575757575757576

=================================

**Multilingual\_PageRank/:** На основе матрицы эксперимента составляется система уравнений, которая используется для расчета коэффициентов. Проведение параллельных опытов используется для получения более точного результата. Если хоть одно условие не выполняется, то необходимо перейти к предыдущим шагам алгоритма для внесения изменений. Рассмотрим произвольную угрозу информационной безопасности, для которой: `P=0,38, Z=53, m=0,8, R=0,38\*53=20, deltaR=2, deltam=0,1`. Матрицу эксперимента представим в виде таблицы. Нормированные величины. После чего необходимо вернуться к ненормированным значениям:`a\_(0)=bara\_(0)-bara\_(1)\*(x\_(v1)+x\_(n1))/(x\_(v1)-x\_(n1))-bara\_(2)\*(x\_(v2)+x\_(n2))/(x\_(v2)-x\_(n2))` , `a\_(1)=(2\*bara\_(1))/(x\_(v1)-x\_(n1))` , `a\_(2)=(2\*bara\_(2))/(x\_(v2)-x\_(n2))` , где `x\_(v)` и `x\_(n)` верхнее и нижнее значение входных параметров. При расчетах все условия проверки алгоритма были соблюдены, что говорит об адекватности расчитанных коэффициентов и самой математической содели.

**Key words part:** 0.5454545454545454

=================================

**RuBERT\_KMeans\_Without\_ST/:** Остаточный риск расчитывается по формуле `R\_(ost)=R\*(1-m) ` , где `R` - риск угрозы, `m` - прочность механизмов защиты и представляет из себя остающийся, потенциальный риск после применения всех контрмер[5], он является важным показателем качества механизмов противодействия и как следствие играет важную роль в управлении рисками информационной безопасности, что делает вопрос математического описания остаточных рисков актуальным. Для начала нам необходимо определить характеристики угрозы безопасности, такие как вероятность и критичность. Аппроксимация представляет собой замену нашей функции остаточного риска от двух переменных другой, при этом замена может происходить различными вариантами:`y=a\_(0)+a\_(1)\*x\_(1)+a\_(2)\*x\_(2) `, `y=a\_(0)+a\_(1)\*x\_(1)+a\_(2)\*x\_(2)+a\_(12)\*x\_(1)\*x\_(2)`, `y=a\_(0)+a\_(1)\*x\_(1)+a\_(2)\*x\_(2)+a\_(3)\*x\_(1)^(2)` и тд. Проведение параллельных опытов используется для получения более точного результата. Нормированные величины.

**Key words part:** 0.6666666666666666

=================================

**RuBERT\_KMeans\_With\_ST/:** Управление рисками строится на их оценки, которая включает в себя анализ и оценивание. Существуют различные методы направленные на поиск оптимального значения оценки рисков информационной безопасности и их анализа: метод нечёткой кластеризации и вычисления взаимной информации[1], матричный подход[2], нечёткий всесторонний метод[3], на основе предикатов и логического вывода[4] и т.д. Результатом оценки риска после внедрения мер противодействия угрозе информационной безопасности является значение остаточного риска. На основе матрицы эксперимента составляется система уравнений, которая используется для расчета коэффициентов. Далее нам необходимо перейти к нормированным значениям для упрощения расчета коэфициентов. Расчитываем коэффициенты математической модели при нормированных значениях по следующей формуле `bara\_(g)=1/N\*sum\_(i=1)^N <<y\_(i)>>\*barx\_(gi)` , где индекс `g` указывает номер столбца, индекс `i` - номер строки.

**Key words part:** 0.7878787878787878

=================================

**RUBERT\_page\_rank\_Without\_ST/:** Управление рисками строится на их оценки, которая включает в себя анализ и оценивание. Для начала нам необходимо определить характеристики угрозы безопасности, такие как вероятность и критичность. Столбоц `x\_(0)` добавлен для возможности расчета коэффициента`a\_(0)`. При переходе верхние значения параметров приравниваются к 1, а нижние к -1. Нормированные величины.

**Key words part:** 0.4545454545454545

=================================

**RUBERT\_page\_rank\_With\_ST/:** Управление рисками строится на их оценки, которая включает в себя анализ и оценивание. Проведение параллельных опытов используется для получения более точного результата. Матрицу эксперимента представим в виде таблицы. Далее нам необходимо перейти к нормированным значениям для упрощения расчета коэфициентов. Нормированные величины.

**Key words part:** 0.3636363636363637

=================================

**RUSBERT\_KMeans\_Without\_ST/:** Существуют различные методы направленные на поиск оптимального значения оценки рисков информационной безопасности и их анализа: метод нечёткой кластеризации и вычисления взаимной информации[1], матричный подход[2], нечёткий всесторонний метод[3], на основе предикатов и логического вывода[4] и т.д. Результатом оценки риска после внедрения мер противодействия угрозе информационной безопасности является значение остаточного риска. Доверительный интервал для входных параметров алгоритма: риск угрозы `deltaR` ,прочность механизмов защиты `deltam` , может варьироваться от 10% до 30% от значения входного параметра. В матрице эксперимента количество столбцов равно числу коэффициентов функции, а количество строк определяется по формуле `N=2^(n)` , где `n` ` ` - число входных параметров. Нормированные величины.

**Key words part:** 0.8181818181818182

=================================

**RUSBERT\_KMeans\_With\_ST/:** Целью данной работы является представление алгоритма получения математического описания остаточного риска. Аппроксимация представляет собой замену нашей функции остаточного риска от двух переменных другой, при этом замена может происходить различными вариантами:`y=a\_(0)+a\_(1)\*x\_(1)+a\_(2)\*x\_(2) `, `y=a\_(0)+a\_(1)\*x\_(1)+a\_(2)\*x\_(2)+a\_(12)\*x\_(1)\*x\_(2)`, `y=a\_(0)+a\_(1)\*x\_(1)+a\_(2)\*x\_(2)+a\_(3)\*x\_(1)^(2)` и тд. В матрице эксперимента количество столбцов равно числу коэффициентов функции, а количество строк определяется по формуле `N=2^(n)` , где `n` ` ` - число входных параметров. Если хоть одно условие не выполняется, то необходимо перейти к предыдущим шагам алгоритма для внесения изменений. При переходе верхние значения параметров приравниваются к 1, а нижние к -1.

**Key words part:** 0.4545454545454545

=================================

**RUSBERT\_page\_rank\_Without\_ST/:** Для начала нам необходимо определить характеристики угрозы безопасности, такие как вероятность и критичность. Рассмотрим произвольную угрозу информационной безопасности, для которой: `P=0,38, Z=53, m=0,8, R=0,38\*53=20, deltaR=2, deltam=0,1`. При переходе верхние значения параметров приравниваются к 1, а нижние к -1. Нормированные величины. После чего необходимо вернуться к ненормированным значениям:`a\_(0)=bara\_(0)-bara\_(1)\*(x\_(v1)+x\_(n1))/(x\_(v1)-x\_(n1))-bara\_(2)\*(x\_(v2)+x\_(n2))/(x\_(v2)-x\_(n2))` , `a\_(1)=(2\*bara\_(1))/(x\_(v1)-x\_(n1))` , `a\_(2)=(2\*bara\_(2))/(x\_(v2)-x\_(n2))` , где `x\_(v)` и `x\_(n)` верхнее и нижнее значение входных параметров.

**Key words part:** 0.3939393939393939

=================================

**RUSBERT\_page\_rank\_With\_ST/:** Управление рисками строится на их оценки, которая включает в себя анализ и оценивание. Проведение параллельных опытов используется для получения более точного результата. При переходе верхние значения параметров приравниваются к 1, а нижние к -1. Нормированные величины. После чего необходимо вернуться к ненормированным значениям:`a\_(0)=bara\_(0)-bara\_(1)\*(x\_(v1)+x\_(n1))/(x\_(v1)-x\_(n1))-bara\_(2)\*(x\_(v2)+x\_(n2))/(x\_(v2)-x\_(n2))` , `a\_(1)=(2\*bara\_(1))/(x\_(v1)-x\_(n1))` , `a\_(2)=(2\*bara\_(2))/(x\_(v2)-x\_(n2))` , где `x\_(v)` и `x\_(n)` верхнее и нижнее значение входных параметров.

**Key words part:** 0.3333333333333333

=================================

**Simple\_PageRank/:** Существуют различные методы направленные на поиск оптимального значения оценки рисков информационной безопасности и их анализа: метод нечёткой кластеризации и вычисления взаимной информации[1], матричный подход[2], нечёткий всесторонний метод[3], на основе предикатов и логического вывода[4] и т.д. Результатом оценки риска после внедрения мер противодействия угрозе информационной безопасности является значение остаточного риска. Остаточный риск расчитывается по формуле `R\_(ost)=R\*(1-m) ` , где `R` - риск угрозы, `m` - прочность механизмов защиты и представляет из себя остающийся, потенциальный риск после применения всех контрмер[5], он является важным показателем качества механизмов противодействия и как следствие играет важную роль в управлении рисками информационной безопасности, что делает вопрос математического описания остаточных рисков актуальным. Доверительный интервал для входных параметров алгоритма: риск угрозы `deltaR` ,прочность механизмов защиты `deltam` , может варьироваться от 10% до 30% от значения входного параметра. В матрице эксперимента количество столбцов равно числу коэффициентов функции, а количество строк определяется по формуле `N=2^(n)` , где `n` ` ` - число входных параметров. В алгоритме присутствуют три условия, которые должны быть соблюдены при проведении расчетов: проверка однородности оценок дисперсии по критерию Кохрэна `G<G\_(kr)` ` ` , проверка нуль гипотез для коэффициентов модели с помощью критерия Стьюдента `t>t\_(kr)` ` ` и проверка адекватности самой математической модели по критерию Фишера `F<F\_(kr)` ` ` . В результате использования алгоритма мы получаем линейную функцию остаточного риска`R\_(ost)=-3,9+0,2\*x\_(1)+20\*x\_(2)` с рассчитанными коэффициентами, которые показывают насколько сильно каждый параметр оказывает влияние на итоговый результат.

**Key words part:** 0.9090909090909092

=================================

**TextRank/:** Существуют различные методы направленные на поиск оптимального значения оценки рисков информационной безопасности и их анализа: метод нечёткой кластеризации и вычисления взаимной информации[1], матричный подход[2], нечёткий всесторонний метод[3], на основе предикатов и логического вывода[4] и т.д. Результатом оценки риска после внедрения мер противодействия угрозе информационной безопасности является значение остаточного риска. Остаточный риск расчитывается по формуле `R\_(ost)=R\*(1-m) ` , где `R` - риск угрозы, `m` - прочность механизмов защиты и представляет из себя остающийся, потенциальный риск после применения всех контрмер[5], он является важным показателем качества механизмов противодействия и как следствие играет важную роль в управлении рисками информационной безопасности, что делает вопрос математического описания остаточных рисков актуальным. Нахождение всех коэффициентов является основной задачей в ходе получения математической модели, которые покажут, на сколько каждый из входных параметров влияет на результат. В алгоритме присутствуют три условия, которые должны быть соблюдены при проведении расчетов: проверка однородности оценок дисперсии по критерию Кохрэна `G<G\_(kr)` ` ` , проверка нуль гипотез для коэффициентов модели с помощью критерия Стьюдента `t>t\_(kr)` ` ` и проверка адекватности самой математической модели по критерию Фишера `F<F\_(kr)` ` ` . В результате использования алгоритма мы получаем линейную функцию остаточного риска`R\_(ost)=-3,9+0,2\*x\_(1)+20\*x\_(2)` с рассчитанными коэффициентами, которые показывают насколько сильно каждый параметр оказывает влияние на итоговый результат. Рассмотренный в работе алгоритм позволяет представить значение осаточного риска для любой угрозы информационной безопаснсоти в виде математической модели, что можно использовать для улучшения качества системы защиты информации, с учетом рассмотрения остаточного риска не только как числового показателя, но и как математическую функцию.

**Key words part:** 0.9090909090909092

=================================

**TF-IDF\_KMeans/:** Целью данной работы является представление алгоритма получения математического описания остаточного риска. На основе матрицы эксперимента составляется система уравнений, которая используется для расчета коэффициентов. В алгоритме присутствуют три условия, которые должны быть соблюдены при проведении расчетов: проверка однородности оценок дисперсии по критерию Кохрэна `G<G\_(kr)` ` ` , проверка нуль гипотез для коэффициентов модели с помощью критерия Стьюдента `t>t\_(kr)` ` ` и проверка адекватности самой математической модели по критерию Фишера `F<F\_(kr)` ` ` . Проведем аппроксимацию нашей функции `y=f(x\_(1),x\_(2))` линейной`y=a\_(0)+a\_(1)\*x\_(1)+a\_(2)\*x\_(2)` . Среднее значение итогового результата образуется из за вероятности преодоления механизмов защиты, которое принимает значенияе не более 1% , в результате чего нам необходимо провести параллельные опыты и усреднить полученные значения. Дисперсия определяется по формуле:` S\_(i)^(2)=(1)/(1-n)\*sum\_(i=1)^n (y\_(i) - << y>>)^(2)`, где `n` - число параллельных опытов. Далее нам необходимо перейти к нормированным значениям для упрощения расчета коэфициентов.

**Key words part:** 0.6666666666666666

=================================

**Текст:** Управление рисками строится на их оценки, которая включает в себя анализ и оценивание. Существуют различные методы направленные на поиск оптимального значения оценки рисков информационной безопасности и их анализа: метод нечёткой кластеризации и вычисления взаимной информации[1], матричный подход[2], нечёткий всесторонний метод[3], на основе предикатов и логического вывода[4] и т.д.. Результатом оценки риска после внедрения мер противодействия угрозе информационной безопасности является значение остаточного риска. Большинство современных методик используют остаточный риск как числовой показатель, который по результатам проведенных мер противодействия должен входить в заранее определенный доверительный интервал , устраивающий конкретную компанию. Остаточный риск расчитывается по формуле `R\_(ost)=R\*(1-m) ` , где `R` - риск угрозы, `m` - прочность механизмов защиты и представляет из себя остающийся, потенциальный риск после применения всех контрмер[5], он является важным показателем качества механизмов противодействия и как следствие играет важную роль в управлении рисками информационной безопасности, что делает вопрос математического описания остаточных рисков актуальным.. Целью данной работы является представление алгоритма получения математического описания остаточного риска.. . Рис.1 Алгоритм получения математической модели остаточного риска. Алгоритм строится на базе полного факторного эксперимента [6,7].. Для начала нам необходимо определить характеристики угрозы безопасности, такие как вероятность и критичность. Зная данные характеристики можно вычислить значение риска угрозы `R=P\*Z` ` ` , где `P` ` ` - вероятность а `Z` ` ` - критичность угрозы. Доверительный интервал для входных параметров алгоритма: риск угрозы `deltaR` ,прочность механизмов защиты `deltam` , может варьироваться от 10% до 30% от значения входного параметра. Аппроксимация представляет собой замену нашей функции остаточного риска от двух переменных другой, при этом замена может происходить различными вариантами:`y=a\_(0)+a\_(1)\*x\_(1)+a\_(2)\*x\_(2) `, `y=a\_(0)+a\_(1)\*x\_(1)+a\_(2)\*x\_(2)+a\_(12)\*x\_(1)\*x\_(2)`, `y=a\_(0)+a\_(1)\*x\_(1)+a\_(2)\*x\_(2)+a\_(3)\*x\_(1)^(2)` и тд. Нахождение всех коэффициентов является основной задачей в ходе получения математической модели, которые покажут, на сколько каждый из входных параметров влияет на результат. В матрице эксперимента количество столбцов равно числу коэффициентов функции, а количество строк определяется по формуле `N=2^(n)` , где `n` ` ` - число входных параметров. На основе матрицы эксперимента составляется система уравнений, которая используется для расчета коэффициентов. Проведение параллельных опытов используется для получения более точного результата.. В алгоритме присутствуют три условия, которые должны быть соблюдены при проведении расчетов: проверка однородности оценок дисперсии по критерию Кохрэна `G<G\_(kr)` ` ` , проверка нуль гипотез для коэффициентов модели с помощью критерия Стьюдента `t>t\_(kr)` ` ` и проверка адекватности самой математической модели по критерию Фишера `F<F\_(kr)` ` ` . Если хоть одно условие не выполняется, то необходимо перейти к предыдущим шагам алгоритма для внесения изменений.. Рассмотрим произвольную угрозу информационной безопасности, для которой: `P=0,38, Z=53, m=0,8, R=0,38\*53=20, deltaR=2, deltam=0,1`. Проведем аппроксимацию нашей функции `y=f(x\_(1),x\_(2))` линейной`y=a\_(0)+a\_(1)\*x\_(1)+a\_(2)\*x\_(2)` .. Матрицу эксперимента представим в виде таблицы. Среднее значение итогового результата образуется из за вероятности преодоления механизмов защиты, которое принимает значенияе не более 1% , в результате чего нам необходимо провести параллельные опыты и усреднить полученные значения. Столбоц `x\_(0)` добавлен для возможности расчета коэффициента`a\_(0)`. Дисперсия определяется по формуле:` S\_(i)^(2)=(1)/(1-n)\*sum\_(i=1)^n (y\_(i) - << y>>)^(2)`, где `n` - число параллельных опытов.. Таблица 1. Эксперимент. Далее нам необходимо перейти к нормированным значениям для упрощения расчета коэфициентов. При переходе верхние значения параметров приравниваются к 1, а нижние к -1.. Таблица 2. Нормированные величины. Расчитываем коэффициенты математической модели при нормированных значениях по следующей формуле `bara\_(g)=1/N\*sum\_(i=1)^N <<y\_(i)>>\*barx\_(gi)` , где индекс `g` указывает номер столбца, индекс `i` - номер строки. После чего необходимо вернуться к ненормированным значениям:`a\_(0)=bara\_(0)-bara\_(1)\*(x\_(v1)+x\_(n1))/(x\_(v1)-x\_(n1))-bara\_(2)\*(x\_(v2)+x\_(n2))/(x\_(v2)-x\_(n2))` , `a\_(1)=(2\*bara\_(1))/(x\_(v1)-x\_(n1))` , `a\_(2)=(2\*bara\_(2))/(x\_(v2)-x\_(n2))` , где `x\_(v)` и `x\_(n)` верхнее и нижнее значение входных параметров.. В результате расчетов получилась следующая математическая модель: `y=-3,9+0,2\*x\_(1)+20\*x\_(2)`. При расчетах все условия проверки алгоритма были соблюдены, что говорит об адекватности расчитанных коэффициентов и самой математической содели.. В результате использования алгоритма мы получаем линейную функцию остаточного риска`R\_(ost)=-3,9+0,2\*x\_(1)+20\*x\_(2)` с рассчитанными коэффициентами, которые показывают насколько сильно каждый параметр оказывает влияние на итоговый результат. Рассмотренный в работе алгоритм позволяет представить значение осаточного риска для любой угрозы информационной безопаснсоти в виде математической модели, что можно использовать для улучшения качества системы защиты информации, с учетом рассмотрения остаточного риска не только как числового показателя, но и как математическую функцию.