

Использование соревновательных и рейтинговых систем при оценке рисков нарушения информационной безопасности организаций

А. С. Поморцев, С. Н. Новиков

В статье представлено решение проблемы использования метода парных сравнений при оценке рисков нарушения информационной безопасности организаций, позволяющее сократить количество необходимых операций сравнения, на основе соревновательных и рейтинговых систем.

Ключевые слова: информационная безопасность, оценка рисков, рейтинговые системы.

1. Введение

В работах [1, 2] была предложена методика оценки рисков нарушения информационной безопасности (ИБ) организаций, включающая перечень параметров оценки. С точки зрения обеспечения ИБ данные параметры неравнозначны. В этой связи необходимо разработать систему весовых коэффициентов, характеризующих, какие из этих параметров более важные, а какие – менее важные. Для этого существуют точные и приближённые методы. Точным методом в данном случае является метод парных сравнений. Проблема заключается в том, что количество необходимых операций сравнения возрастает квадратично. В предложенной методике содержится 721 параметр, следовательно, необходимо 259560 операций парного сравнения. Все операции парного сравнения выполняются экспертом, проводящим оценку вручную, что затратно по времени. В будущем с появлением новых угроз и требований к системам обеспечения информационной безопасности количество параметров будет увеличиваться.

В данной статье предложено решение на основе соревновательных и рейтинговых систем, позволяющее сократить количество необходимых операций сравнения.

2. Анализ систем проведения соревнований

Система проведения соревнований – это порядок, в соответствии с которым проводятся соревнования (матчи, турниры). Выбор системы проведения соревнования зависит от целей и задач, которые преследует данное соревнование, числа участников и сроков проведения.

Круговая система проведения соревнований работает следующим образом: все участники (команды) играют друг с другом поочередно в порядке, определяемом таблицами очередности игры. По сравнению с другими системами соревнований она отличается наименьшим влиянием случайности на итоги соревнования [3]. Данная система соревнований позволяет наиболее полно оценить силы соперников, однако при большом количестве участников проведение соревнований по данной системе займет большое количество времени. Данная система проведения соревнований подходит для оценки рисков нарушения ИБ, по своей сути повторяя метод парных сравнений.

Соревнования по Швейцарской системе проводятся с любым числом участников (команд) в ограниченные сроки. Для составления пар перед началом каждого тура производится жеребьёвка. В каждом туре встречаются участники с равным или почти равным числом очков, повторные встречи не проводятся. При подведении итогов в случае равенства очков у двух или более участников для определения мест чаще всего применяется система коэффициентов Бухгольца [3]. Коэффициент Бухгольца участника складывается из суммы всех очков соперников, с которыми данный участник играл, независимо от результата встреч между ними. Идея применения коэффициента: участнику, игравшему с более сильными соперниками, набравшими в сумме больше очков, присуждается более высокое итоговое место [3]. Данная система проведения соревнований подходит для оценки рисков нарушения ИБ, так как позволяет оценить соотношения сил соперников и определить распределение мест, занятых участниками турнира, начиная с лидера и заканчивая участником, проигравшим все партии.

Олимпийская система проведения соревнований предполагает выбывание участника или команды из соревнования после проигрыша определенного количества партий (матчей) или после потери определённого числа очков в личных соревнованиях. При ничейном результате партия (матч) переигрывается (возможен также жребий). Личная встреча обычно играется до конца, исход командного матча решают коэффициенты. Применяется для массовых соревнований [3]. Данная система проведения соревнований повторяет Швейцарскую систему, отличаясь тем, что позволяет в кратчайшие сроки оценить распределение первых мест, но не позволяет оценить выбывших игроков. Олимпийская система проведения соревнований не подходит для использования при оценке рисков нарушения ИБ, так как необходимо определить полное распределение мест.

При проведении соревнований по Схевенингенской системе все участники (команды) делятся на две группы. Представители одной группы играют поочередно со всеми представителями другой группы. При наличии двух команд результат командного матча определяется суммой очков, набранных участниками каждой команды. Применяется для тренировочных соревнований между молодыми и опытными шахматистами, а также в международных командных встречах [3]. Данная система проведения соревнований подходит для использования в разрабатываемой системе оценки. Однако возможна ситуация, когда представители одной группы окажутся сильнее представителей другой группы.

Анализ систем проведения соревнований показал, что для оценки рисков нарушения ИБ подойдут Швейцарская, круговая и Схевенингенская системы проведения соревнований. Характер зависимости количества партий от числа участников показан на рис 1. Результаты анализа сведены в табл. 1.

Таблица 1. Результаты анализа систем проведения соревнований

Параметры сравнения	Система проведения соревнований		
	Швейцарская	Круговая	Схевенингенская
Вычислительная сложность	$Q = f\left(\frac{N}{2} \log_2 N\right)$	$Q = f\left(\frac{N}{2}(N-1)\right)$	$Q = f\left(\frac{N}{2}\right)^2$
Количество операций сравнения при $N = 721$	3423	259560	129961

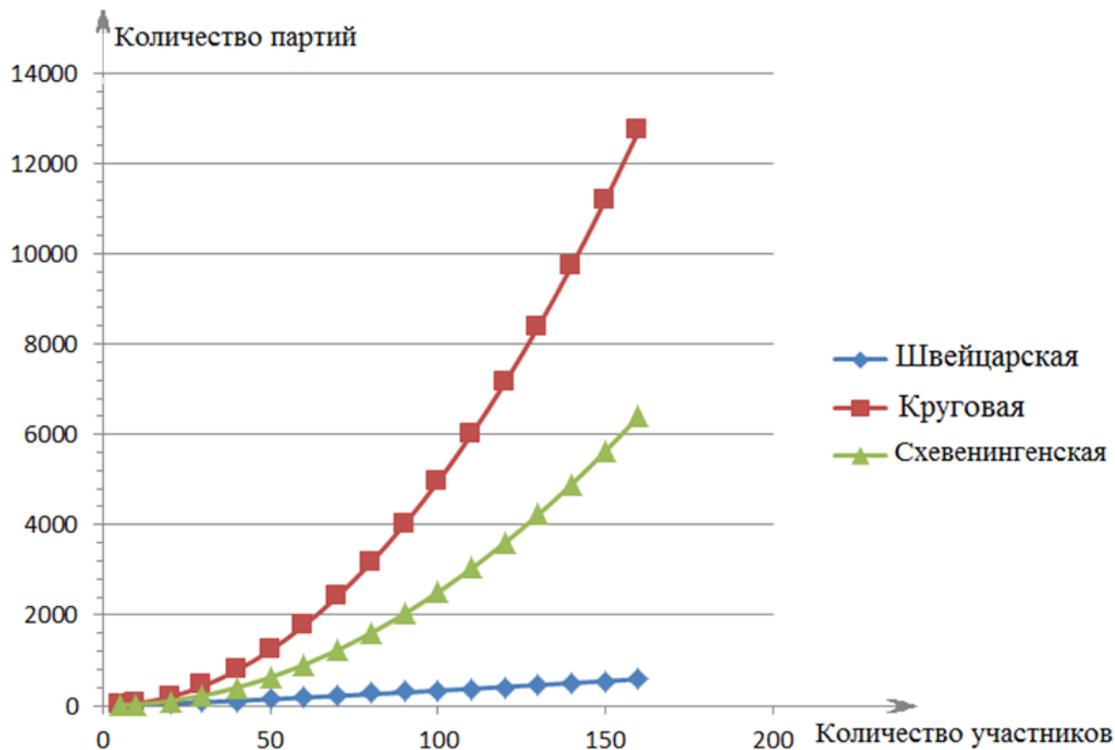


Рис. 1. Зависимость количества партий от количества участников

Как видно из табл. 1 и рис. 1, Швейцарская система позволяет произвести сравнение и определить распределение мест за меньшее количество операций.

При использовании Схевенингенской системы проведения соревнований возможен случай, когда задача распределения мест становится нерешаемой. Круговая система повторяет метод парных сравнений и не дает никакого выигрыша по времени. В этой связи при оценке рисков нарушения ИБ целесообразно использовать Швейцарскую систему проведения соревнований. Для того чтобы дополнительно сократить количество необходимых операций сравнения, необходимо разделить параметры оценки на 25 функциональных групп, предложенных в статье [2].

3. Анализ системы рейтингов Эло

Рейтинг – это числовой или порядковый показатель, отображающий важность или значимость определенного объекта или явления.

Система рейтингов Эло была разработана американским профессором физики Арпадом Эло. Эта система представляет собой метод расчёта относительной силы игроков в играх, в которых участвуют двое игроков (например, сёги, го или шахматы) [4].

Для определения нового рейтинга после проведения партии вычисляется математическое ожидание количества очков, которое наберёт игрок А в партии с В:

$$E_A = \frac{1}{1 + 10^{\frac{R_B - R_A}{400}}}, \quad (1)$$

где E_A – математическое ожидание количества очков, которое наберёт игрок А в партии с В; R_A – рейтинг игрока А; R_B – рейтинг игрока В; 400 – максимально возможная разница рейтингов соперников.

Новый рейтинг игрока А рассчитывается по формуле:

$$R'_A = R_A + K(S_A - E_A) \quad (2)$$

где K – коэффициент, значение которого равно 10 для сильнейших игроков (рейтинг 2400 и выше), 15 – для игроков с рейтингом меньше чем 2400 и 30 (было 25) – для новых игроков

(первые 30 партий с момента получения рейтинга ФИДЕ); S_A – фактически набранное игроком А количество очков (1 очко за победу, 0.5 – за ничью и 0 – за поражение); R'_A – новый рейтинг игрока А.

Система рейтингов Эло очень популярна и применяется во многих сферах. Если модифицировать данную систему рейтингов, то её можно применить при оценке рисков нарушения информационной безопасности организаций.

4. Разработка системы оценки весовых коэффициентов

4.1. Модификация рейтинговой системы

При разработке системы оценки весовых коэффициентов за основу была взята система рейтингов Эло для ФИДЕ. В предложенной рейтинговой системе возможна ситуация проведения партии между игроками с разницей рейтингов более 400. Поэтому преобразуем (1), заменив число 400 в знаменателе показателя степени 10 на среднее арифметическое рейтингов соперников. Получим новую формулу:

$$E_A = \frac{1}{1 + 10^{\frac{2(R_B - R_A)}{R_B + R_A}}}, \quad (3)$$

где E_A – математическое ожидание количества очков, которое наберёт игрок А в партии с В; R_A – рейтинг игрока А; R_B – рейтинг игрока В.

Тем самым мы учитываем влияние разницы рейтингов. Новый рейтинг игрока А рассчитывается по (2). При этом расчёт значения коэффициента K проводится следующим образом:

$$K = \frac{R_{нач}}{N}, \quad (4)$$

где $R_{нач}$ – начальное значение рейтинга; N – количество раундов.

Также было принято решение определить пять вариантов исхода сравнения, то есть S будет принимать одно из пяти значений: 0; 0.25; 0.5; 0.75; 1.

4.2. Разработка алгоритма расчёта весовых коэффициентов

Для сокращения количества операций сравнения решено использовать Швейцарскую систему проведения соревнований, так как она в совокупности с рейтинговой системой позволяет проранжировать множество критериев за меньшее количество операций сравнения. Опишем подробнее разработанную систему.

Все объекты будут разбиты на пары и будут сравниваться между собой. Было определено пять вариантов сравнения:

– значимость первого объекта значительно превышает значимость второго объекта: $S_A = 1, S_B = 0$;

– значимость первого объекта превышает значимость второго объекта: $S_A = 0.75, S_B = 0.25$;

– первый и второй объект равнозначны: $S_A = 0.5, S_B = 0.5$;

– значимость второго объекта превышает значимость первого объекта: $S_A = 0.25, S_B = 0.75$;

– значимость второго объекта значительно превышает значимость первого объекта: $S_A = 0, S_B = 1$.

В зависимости от результата сравнения будет произведен пересчет рейтингов. После того как все пары пройдут этап сравнения, все объекты должны быть упорядочены в порядке убывания рейтинга и начинается новый раунд. Формируется новый состав пар и далее идет сравнение и пересчет рейтинга. Количество раундов определяется как округленное вверх до целых число, равное двоичному логарифму от количества сравниваемых объектов.

Формирование пар происходит следующим образом. Берем первый в списке объект и определяем, сравнивался ли он с объектом, который занимает второе положение в списке. Если эти объекты ранее не сравнивались, то формируется новая пара, иначе – просматриваем следующий объект, и так далее, пока не найдем пару для первого. Затем переходим к следующей паре объектов, проводим аналогичную проверку и формируем пару.

При проверке работы данного алгоритма формирования пар возникла проблема: проверка и формирование пар происходит по списку сверху вниз и возможна ситуация, когда последняя пара сравнивалась между собой ранее, а так как они последние в списке, то нет возможности подыскать для них новых «соперников». Поэтому алгоритм был доработан. Был добавлен похожий цикл формирования, работающий снизу вверх. Если последние два объекта сравнивались ранее, то пробуем составить пары из последних четырех объектов. Если и теперь хотя бы одна из пар не удовлетворяет необходимому условию, то берем последние шесть объектов, и так далее.

В итоге алгоритм формирования пар работает следующим образом: в цикле, который повторяется до тех пор, пока хотя бы одна из пар не удовлетворяет условию, что объекты пары ранее не сравнивались между собой, сперва выполняется алгоритм формирования сверху вниз, затем идет проверка всех пар; если существует хотя бы одна пара, не удовлетворяющая условию, что объекты пары ранее не сравнивались между собой, то дальше работает алгоритм формирования снизу вверх, затем начинается новая итерация цикла формирования.

Возможна ситуация, когда количество объектов является нечетным числом и один объект остается без пары. Для решения данной проблемы был разработан следующий алгоритм. В первом раунде не участвует объект, находящийся в списке на последней позиции. В начале каждого нового раунда, после того как объекты были упорядочены по рейтингу, выбирается объект, занимающий положение посередине списка. Его место занимает объект, который не участвовал в предыдущем раунде. Затем идет алгоритм формирования пар и алгоритм сравнения.

При выполнении алгоритма сравнения рейтинг объекта, не участвующего в сравнении, не остается неизменным: его рейтинг изменяется на среднее арифметическое различных долей от прироста рейтинга объектов, с которыми он сравнивался ранее. То есть если объект, который пропускает раунд, ранее оказался более значим или равнозначен по сравнению с объектом, участвующим в раунде, то половина изменения рейтинга второго будет учтена в расчете рейтинга пропускающего объекта при условии, что второй объект оказался более значим или равнозначен по сравнению со своим соперником.

В случае если второй объект оказался менее значим по сравнению со своей парой, то в расчете нового рейтинга пропускающего раунд объекта учитываться будет только десятая часть изменения рейтинга второго.

В ситуации, когда объект, который пропускает раунд, ранее оказался менее значим, чем объект, участвующий в раунде, возможны два исхода событий. Первый из них, когда участвующий в раунде объект оказался менее значим по сравнению со своим соперником, – в данном случае половина изменения его рейтинга будет учитываться при расчете рейтинга пропускающего раунд объекта. Второй случай, когда участвующий в раунде объект оказался более значим или равнозначен по отношению к своему сопернику, – десятая часть изменения его рейтинга будет учитываться при расчете рейтинга пропускающего раунд объекта.

5. Заключение

В данной статье рассмотрено использование соревновательных и рейтинговых систем для сокращения количества необходимых операций парного сравнения при оценке рисков нарушения ИБ организаций. Также в статье предложено решение проблемы с нечётным количеством параметров оценки.

В табл. 2 приведены расчеты необходимого количества операций сравнения для метода парных сравнений и разработанной системы оценки весовых коэффициентов для случая, когда оценивается 721 частный показатель, и случая, когда показатели разбиты на 25 групп.

Таблица 2. Количество операций сравнения для разных методов оценки

Ситуация	Количество операций сравнения	
	Метод парных сравнений	Разработанная система
721 частный показатель	259560	3423
25 групповых параметров	11809	1796

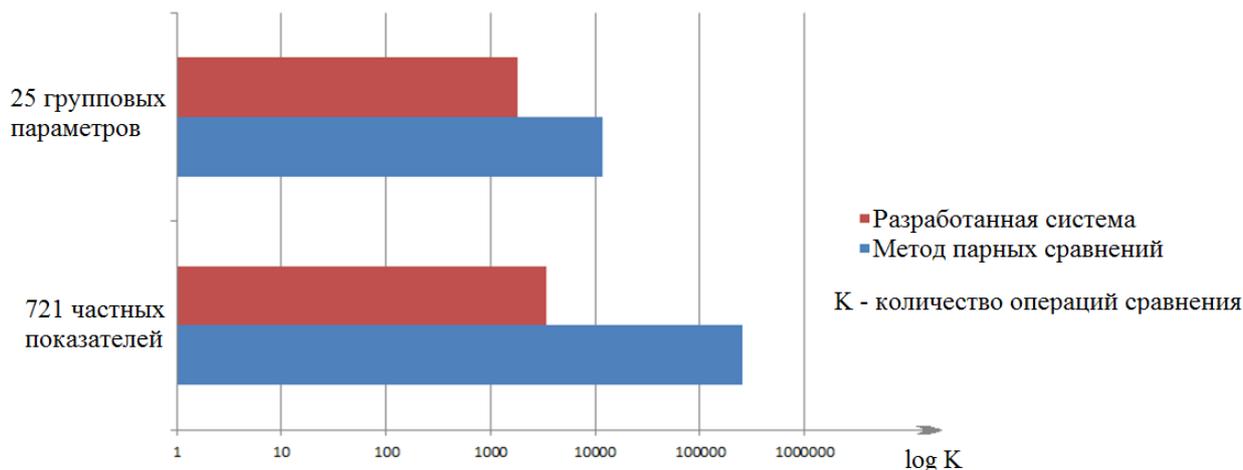


Рис. 2. Количество операций сравнения для разных методов оценки

На рис. 2 представлены гистограммы, отображающие необходимое для оценки объектов количество операций сравнения. Так как значения имеют большой разброс, для их отображения была взята логарифмическая шкала. Как видно из гистограмм, объединение частных показателей в группы и использование разработанной системы оценки весовых коэффициентов позволяет сократить количество операций сравнения в 144 раза по сравнению с оценкой 721 частного показателя методом парных сравнений.

Литература

1. Поморцев А. С. Методика оценки рисков нарушения информационной безопасности организации с учётом квалификации экспертов // Доклады ТУСУР. 2014. № 2 (32). С. 167–169.
2. Поморцев А. С, Новиков С. Н. Разработка системы параметров оценки рисков нарушения информационной безопасности организаций // Доклады ТУСУР. 2014. № 2 (32). С. 170–174.
3. Руководство для арбитров FIDE. Русская версия. / под ред. А. В. Ткачёва. М., 2014. 186 с.
4. Что такое рейтинг Эло [Электронный ресурс]. URL: <http://chessworldweb.com/articles/144-what-is-an-elo-rating.html> (дата обращения: 02.03.2016).

Статья поступила в редакцию 12.09.2017.

Поморцев Антон Сергеевич

аспирант кафедры безопасности и управления в телекоммуникациях СибГУТИ, тел. 8 (383) 269-82-45, e-mail: pomortsev.anton@gmail.com.

Новиков Сергей Николаевич

д.т.н., доцент, заведующий кафедрой безопасности и управления в телекоммуникациях СибГУТИ (630102, Новосибирск, ул. Кирова, 86), тел. 8 (383) 269-82-45, e-mail: snovikov@ngs.ru.

Competition and rating systems in the assessment of organizations risks of violation of information security

A. Pomortsev, S. Novikov

This article presents a solution to the problem of using the method of paired comparisons when evaluating the risks of violation of information security organizations, which allows us to reduce the number of required comparisons on the basis of competition and rating systems.

Keywords: information security, risk assessment, rating systems.