УДК 004.056.5 Вестник УрФО № 4(58) / 2025, с. 53–63

Корженевский Д. А., Зырянова Т. Ю. 10.14529/secur250406

МЕТОДИКА ОЦЕНКИ РИСКОВ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ КООРДИНАТНО-ГРАФОВЫМ МЕТОДОМ

В статье рассматривается связь оценки риска информационной безопас-ности и бизнес-процессов, которые определяют шаги для достижения бизнес-цели. Рассматриваются составляющие, необходимые для оценки риска инфор-мационной безопасности при учете потребности организации как выстроенного менеджмента. Рассмотрены различные подходы к оценке информационной безопасности и определен приоритетный в данной работе.

Предложен метод оценки информационной безопасности, использующий количественный подход. Метод отражает взаимосвязь активов организации и выполняемых бизнес-операций и ущерба, который является составляющей риска. Описываются шаги, в рамках предлагаемого метода оценки рисков информационной безопасности, результатом выполнения которых является показатель риска информационной безопасности для рассматриваемой системы.

Ключевые слова: *риск информационной безопасности, оценка риска информационной безопасности, бизнес-процесс, бизнес-операция, аппроксимация.*

METHODOLOGY FOR ASSESSING INFORMATION SECURITY RISKS USING THE COORDINATE GRAPH METHOD

The article examines the relationship between information security risk as-sessment and business processes that determine the steps to achieve a business goal. The components necessary for assessing information security risk are considered, taking into account the needs of the organization as a structured management. Various approaches to information security assessment are considered and a priority one is identified in this work.

A method for assessing information security using a quantitative approach is proposed. The method reflects the relationship between the assets of the organization and the business operations performed and the damage that is part of the risk. The steps described within the framework of the proposed method for assessing information security risks are described, the result of which is an indicator of information security risk for the system in question.

Keywords: *information security risk, information security risk assessment, business process, business operation, approximation.*

Деятельность любой организации направлена на достижение бизнес-целей, для обеспечения которых могут применяться средства автоматизации. Средства автоматизации используются в бизнес-процессах, а каждому бизнес-процессу соответствует некоторый набор бизнес-операций. В данной работе под бизнес-операцией подразумевается совершение совокупности действий, которые являются составляющими бизнес-процесса. Бизнес-операция, в данной работе, – это минимальная единица совершения действий и минимальная составляющая бизнес-процесса. Определение термина «бизнес-процесс» содержится в ГОСТ Р ИСО 19439-2022 «Интеграция предприятия. Основа моделирования предприятия»: бизнес-процесс – частично установленный набор видов деятельности предприятия, который может быть выполнен для достижения определенного желаемого конечного результата во исполнение данной цели предприятия или части предприятия [1].

Применение средств автоматизации для выполнения и ускорения бизнес-операций, сопряжено с рисками информационной безопасности. В соответствии с текущим законодательством (ГОСТ Р ИСО/МЭК 27005-2010), риск информационной безопасности – возможность того, что данная угроза сможет воспользоваться уязвимостью актива или группы активов и тем самым нанесет ущерб организации [2]. В случае реализации риска информационной безопасности, возникает остановка выполнения бизнес-операций, как следствие невозможно выполнить бизнес-процесс или выполнение бизнес-процесса осуществляется с неудовлетворительными результатами. Остановленные бизнес-процессы не позволяют достичь бизнес-целей. Конечным результатом реализации риска информационной безопасности является ущерб, который может быть выражен во временном или денежном эквиваленте. Временной показатель ущерба оценивает время простоя актива или предприятия в целом, а время необходимое на возобновление выполнения бизнес-операций.

В качестве определения термина «ущерб» будет использоваться пояснение Банка России: ущерб – утрата активов, повреждение (утрата свойств) активов и (или) инфраструктуры организации или другой вред активам и (или) инфраструктуре организации БС РФ, наступивший в результате реализации угроз ИБ через уязвимости ИБ [3].

Определение «риск информационной безопасности» коррелирует с определением «ущерб». Согласно обоим определениям, существуют активы организации, которые содержат уязвимости, и эксплуатация которых приводит к реализации угроз информационной безопасности. Под активами организации в данной работе подразумевается следующее определение из ГОСТ Р 53114-2008: активы организации: все, что имеет ценность для организации в интересах достижения целей деятельности и находится в ее распоряжении [4]. Актив организации в данной работе – минимальная единица имущества, обладающая самостоятельной ценностью и функциональностью.

Исходя из вышеизложенного, риск информационной безопасности напрямую связан с активами организации, которые участвуют в обеспечении бизнес-операций.

Оценивать риски информационной безопасности можно м помощью нескольких подходов:

1. Качественная оценка риска информационной безопасности;
2. Количественная оценка риска информационной безопасности;
3. Метод, комбинирующий элементы качественной и количественной оценки рисков информационной безопасности.

Каждый подход обладает своими достоинствами и недостатками, что обуславливает необходимость выбора в зависимости от специфики информационной системы или сферы применения. Качественная оценка рисков информационной безопасности предназначена для общей идентификации риска с категоризацией выявленных рисков посредством присвоения им одного или нескольких атрибутов на основе оценочных шкал. Ключевым преимуществом данного подхода является его относительная простота и оперативность проведения анализа, что позволяет обеспечить быстрое получение интерпретируемых результатов. Также данный подход отличается высокой степенью доступности для широкого круга пользователей, включая лиц, не обладающих специализированными знаниями в области информационной безопасности. Однако ключевыми недостатками метода, которые ставят под сомнение результаты оценивания, являются:

1. Субъективность при оценивании риска ИБ – эксперт может субъективно подходить к оценке конкретного риска в зависимости от большого количества обстоятельств: уровень компетенций, опыт работы, различный уровень информированности о рассматриваемой системе и т.д.
2. Ограниченный спектр категорий – распределение оценки по небольшому количеству категорий приводит к ухудшению качества оценки риска и накоплению погрешности. Увеличение количества категорий может ввести в заблуждение экспертов при оценивании, так и непрофессионалов при принятии решения.
3. Трудности интерпретации результатов с существенной разницей в оценке – в случае получения от разных экспертов диаметральных оценок, сложно принять итоговое решение. Предположим, что эксперты дали оценки «низкий риск» и «высокий риск». Использование среднего значения может еще сильнее увеличить погрешность оценки и привести к необоснованно низкой оценке. А принятие версии одной из сторон может также привести к неверной оценке риска, так как эксперт выставляет субъективную оценку, которая может быть завышена.
4. Необходимость регулярного повторного оценивания – качественный подход не позволяет осуществлять точное прогнозирование изменения риска информационной безопасности. Также учитывая вышеописанные недостатки, повторная оценка необходима для корректировки произведенных ранее оценок.

Количественная оценка риска информационной безопасности представляет собой присвоение некоторого значения вероятности реализации риска в числовом формате. В ГОСТ Р ИСО/МЭК 27005-2010 определяется, что, помимо значения вероятности, необходимо рассматривать некоторую количественную оценку последствий риска [2]. Последствием риска будем считать воздействие на бизнес-операции и бизнес-процессы организации.

Количественная оценка риска информационной безопасности обладает рядом преимуществ, которые способствуют достижению высокой степени точности и объективности в анализе. Одним из ключевых преимуществ данного подхода является отсутствие

шкал оценивания, что позволяет минимизировать влияние человеческого фактора и повысить объективность результатов. Оценка с помощью количественного подхода позволяет получить точное числовое значение риска информационной безопасности. Данный подход позволяет проводить прогнозирование изменения риска информационной безопасности.

Недостатки, которые можно выделить для количественного подхода оценки рисков информационной безопасности:

1. Необходимость наличия достоверных данных – искаженные входные параметры приводят к неверному определению итогового результата, а также могут привести к ошибкам при расчете формул в автоматизированном режиме;
2. Сложность интерпретации итоговой оценки риска информационной безопасности – полученное значение может сложно интерпретироваться и непонятно человеку, не вовлеченному в процесс оценки рисков информационной безопасности.
3. Приведение входных параметров к определенной форме – подход использует числовые значения, которые в зависимости от метода подсчета, должны быть представлены в той или иной форме, а также возможно не все входные параметры поддаются конвертации в числовую величину.

Учитывая ключевые преимущества метода – точная оценка риска и возможность прогнозирования изменения риска информационной безопасности, будем считать метод количественной оценки приоритетным.

Предлагается новый метод оценки рисков информационной безопасности, основное внимание которого сконцентрировано на взаимосвязях: активов предприятия, бизнес-операциях (выполняемых с помощью активов), ущерба от прекращения бизнес-процессов, актуальной экспертной оценки опасности фактора риска. Перечисленные составляющие также являются входными данными метода.

Основные преимущества метода: возможность выполнения расчетов для любого количества входных параметров, что означает масштабируемость метода; возможность прогнозирования изменения рисков информационной безопасности с течением времени.

Для выполнения оценки риска информационной безопасности, необходимо последовательно выполнить следующие шаги:

1. Сформировать перечень бизнес-процессов и соответствующих им перечень бизнес-операций.
2. Сформировать перечень активов организации, которые обеспечивают выполнение бизнес-операций.
3. Составить структуру в виде графа, которая отображала связь активов и бизнес-операций.
4. Оценить минимальное количество активов для выполнения бизнес-операций.
5. Оценить необходимое время на восстановление выполнения бизнес-операции для каждой группы объектов.
6. Оценить с помощью экспертов существенность влияния факторов на указанные активы.
7. Построить в пространстве точки, которые отражали состояние активов по трем координатам: коэффициент показателя бизнес-операций (КПБО), ущерб, совокупная экспертная оценка.
8. Провести аппроксимацию указанных точек с целью получения полиномиальной функции.
9. Выполнить аналогичные действия для показателей с минимальным количеством активов, с целью определения приемлемого риска.
10. Определить соотношение объемов фигур и вычислить риск.

Для первого этапа необходимо, чтобы специалисты организации, где оценивается риск информационной безопасности, определили перечень рассматриваемых бизнес-процессов. Именно набор бизнес-процессов задает первый параметр масштаба оценивания. Затем необходимо проделать декомпозицию для каждого бизнес-процесса с целью определения бизнес-операций. Бизнес-операция в данном методе, как уже упоминалось ранее, минимальная единица действия. После получения перечня бизнес-операций необходимо перейти ко второму этапу.

Необходимо определить перечень активов предприятия, которые участвуют в выполнении бизнес-операций. Организация сама принимает решение, что включить в перечень, так как согласно ГОСТ Р 53114-2008, только организация определяет поставленные цели и соответствующую ценность. Вели-

чина перечня, которая является вторым параметром масштаба оценивания, задает объем последующих вычислений.

Третий этап — это построение графа, где для каждого актива определяется связь с бизнес-операцией. При этом один актив может быть связан с несколькими бизнес-операциями. Для каждой связи – ребра графа, необходимо определить важность (вовлеченность) актива в выполнении бизнес-операции. Актив может обеспечивать выполнение нескольких бизнес-операций с разной степенью вовлеченности. Результатом данного этапа является коэффициент показателя бизнес-операции (КПБО), и значение данного коэффициента будет располагаться на оси Ох, при выполнении шага под номером семь.

Дополнительно введем показатель сложности актива. Под сложностью актива понимается коэффициент, отражающий совокупность свойств и признаков актива, а также степень их влияния. Числовое значение характеризует насколько составляющей элемент отличается по некоторым критериям от других составляющих. Рекомендуется рассматривать элементы, которые непосредственно задействованы при осуществлении бизнес-операции. Предлагается использовать следующие критерии для оценки показателя сложности актива:

1. Стоимость актива;
2. Аппаратная сложность;
3. Количество обеспечиваемых операций и функций;
4. Отказоустойчивость и время беспрерывной работы актива;
5. Сложность администрирования актива;
6. Порог компетенций для работы с активом;
7. Ценность актива с точки зрения нарушителя.

Вышеперечисленные показатели не являются конечными и могут быть дополнены организацией, выполняющей оценку риска, дополнительными критериями, которые отвечали бы интересам организации и сфере деятельности.

В общем виде показатель сложности рассчитывается по формуле:

$$D = k \prod_{i=1}^{n} {x_i}^{w^i},$$

где k – константа нормализации, x_i – признаки и их значения, w^i – весовой коэффициент признака.

Например, для некоторого автоматизированного рабочего места (АРМ) бухгалтера, которое участвует в бизнес-операции «отправка файла xml во внешнюю систему», необходимо рассмотреть следующие составляющие элементы: операционная система, клиент базы данных, браузер, подключение к внешней системе, аппаратная составляющая АРМ.

Итоговая координата для каждой бизнес-операции находится по формуле:

$$\text{КПБО}_n = (e_1 * D_1) + \cdots + (e_i * D_k),$$

где e_i - вес ребра, D_k - сложность актива.

Четвертый этап предполагает нахождение показателя КПБО$_{min}$, который отражает необходимое минимальное количество активов, для выполнения бизнес-операции с наихудшими возможными и допустимыми результатами, но без прерывания операции. В отдельных случаях минимальное количество активов может совпадать с количеством активов в штатном режиме работы, в этом случае КПБО$_{min}$ будет равен 0. Показатель КПБО$_{min}$ необходим для оценивания приемлемого (допустимого) риска, по отношению к которому оценивается недопустимый (фактический) риск. Под допустимым риском понимается риск, который в данной ситуации считают приемлемым при существующих общественных ценностях [5].

Пятый этап предполагает определение показателя ущерба. Результатом данного этапа является коэффициент ущерба – располагается на оси Оу, при выполнении этапа под номером семь. Согласно определению, описанному в Стандарте Банка России СТО БР ИББС-1.0-2014, утрата актива ведет к ущербу. В предлагаемом методе утрата актива ведет к прекращению выполнения бизнес-операции, а следовательно, наступает ущерб, который можно измерить в денежном эквиваленте или временном эквиваленте. Ущерб будет оцениваться по времени, затраченному на восстановление выполнения БО с наихудшими допустимыми результатами, т.е. с минимальным количеством активов. Среди перечня возможных временных значений выбирается максимальное.

Единицы измерения определяются заранее и дальнейшие расчеты конвертируются в выбранную величину, например, часы. Действия совершаемые с активами для восстановления бизнес-операции:

1. Устранение нарушения работоспособности (например, время восстановления функционирования тонкого клиента 1С занимает 1 час);
2. Замена актива на резервный (например, в случае выхода из строя АРМ, замена займет 0,6 часа).

Стоит отметить, что замена на резервный актив не всегда является лучшим выбором, так как резервное устройство может нуждаться в настройке, которое займет больше времени, чем устранение причин неработоспособности основного устройства.

В последующем теоретически возможно рассчитать ущерб в денежном эквиваленте, основываясь на временном ущербе: время, затраченное персоналом на восстановление работоспособности; время простоя персонала, из-за невозможности работать с активом; стоимость актива (в случае полного уничтожения); стоимость компенсаций контрагентам и т.д.

Шестой этап направлен на получение экспертной оценки. Показатель экспертной оценки – представляет собой числовое значение, которое описывает величину фактора риска. Под фактором риска понимается фактор, который оказывает существенное влияние на риск [6]. Эксперт, руководствуясь своим профессиональным опытом, актуальным перечнем угроз и уязвимостей для активов, формирует некоторое положительное действительное число, отражающее величину существенности влияния фактора риска. Эксперту доступны сведения о предыдущих этапах, с целью осведомления обо всех влияющих факторах подлежащих оцениванию. Следует отметить, что количество экспертов, производящих оценку, должно быть не менее двух, чтобы избежать некорректных расчетов и субъективности мнения.

После получения данных от экспертов, необходимо произвести некоторые проверки: нахождение коэффициента конкордации, стандартизацию данных для поиска аномалий.

Для нахождения коэффициента конкордации, который используется для оценки согласованности мнений нескольких экспертов относительно ранжирования объектов, необходимо:

1. Составить таблицу, где для каждого фактора риска будут соотнесены экспертные оценки. Пример выполнения данного шага представлен в таблице 1, где m – количество экспертов, n – количество факторов риска. Фактором риска в данных вычислениях является комбинация сведений об активах, коэффициентах показателя бизнес-операции, коэффициент сложности каждого актива и показатель ущерба. Предполагается, что наименьшим значениям соответствуют наименьшие ранги, т.е. минимальное значение в столбце эксперта получит 1, а наибольшее будет равняться значению количества факторов.

2. Найти сумму ранжированных оценок экспертов для каждого фактора

$$R_i = \sum_{i=1}^{n} r_{mn},$$

где r_{mn} – оценка каждого эксперта по каждому фактору

Данные удобно привести к виду таблицы (таблица 2).

Таблица 1

Составление таблицы ранжирования экспертных оценок

Фактор риска	**Оценка эксперта 1**	**Оценка эксперта 2**	**Оценка эксперта 3**	**…**	**Оценка эксперта m**
Фактор 1	$r_{1;1}$	$r_{2;1}$	$r_{3;1}$	…	$r_{m;1}$
Фактор 2	$r_{1;2}$	$r_{2;2}$	$r_{3;2}$	…	$r_{m;2}$
Фактор 3	$r_{1;3}$	$r_{2;3}$	$r_{3;3}$	…	$r_{m;3}$
…	…	…	…	…	…
Фактор n	$r_{1;n}$	$r_{2;n}$	$r_{3;n}$	…	$r_{m;n}$

Таблица 2

Сумма ранжированных оценок

Фактор риска	Сумма оценок экспертов
Фактор 1	R_1
Фактор 2	R_2
…	…
Фактор n	R_n

3. Необходимо оценить среднюю сумму ранжированных оценок и сумму квадратов отклонений.

$$\bar{R} = \frac{\sum_{n=1}^{n} R_n}{n};$$

$$SS = \sum_{n=1}^{n} (R_n - \bar{R})^2.$$

4. Определение величины коэффициента конкордации Кендалла:

$$W = \frac{12 * SS}{m^2(n^3 - n)}$$

Величина изменяется от 0 (полная несогласованность) до 1 (полная согласованность). При значениях коэффициента, приближенных к 1, должно быть выдвинуто предположение о сговоренности экспертов, а значит, оценки могут быть некорректными. Оптимальным диапазоном величины коэффициента является 0,7…0,9. Если коэффициент определяется ниже порогового уровня в 0,7, то необходимо провести проверку экспертных оценок и определить аномалии.

Для поиска аномалий используется метод стандартизации данных. Основываясь на выполнении расчетов при нахождении коэффициента конкордации, определяется стандартное отклонение.

$$\sigma = \sqrt{\frac{SS}{n-1}}$$

Затем для каждого фактора и соответствующего ему экспертной оценки находится показатель z, который при превышении установленного порога означает аномалию. Установленный порог может изменяться по решению эксперта, проводящего оценку, однако рекомендуемый порог $|z_i|>3$.

$$z_i = \frac{x_i - \mu}{\sigma}$$

Аномальные оценки экспертов должны быть исключены из построения точек в трехмерном пространстве. Результатом данного этапа является получение экспертной оценки R_i для каждой комбинации КПБО и ущерба. Оценка R_i располагается по оси Oz.

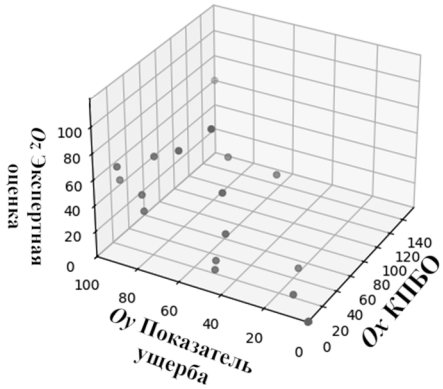

Рис. 1. Визуализация точек в пространстве

Седьмой этап предполагает, что полученные значения (связка КПБО-ущерб-экспертная оценка) являются координатами точек, которые располагаются в трехмерном пространстве: коэффициент показателя бизнес-операции (КПБО) – располагается на оси Ox, коэффициент ущерба – располагается на оси Oy, коэффициент экспертной оценки R_i – располагается на оси Oz. Визуализация данного этапа представлена на рисунке 1.

Восьмой этап предполагает работу с точками, расположенными в пространстве. После построения точек необходимо рассчитать аппроксимирующую поверхность. Аппроксимирующей функцией в данной работе будет являться полиномиальная функция.

Ключевой показатель полиномиальной функции – степень. Именно от данного показателя зависит точность аппроксимации, а также способность не учитывать некоторые значения «шума».

Для поиска оптимального значения степени полинома необходимо сравнить критерии Akaike Information Criterion (AIC) и Bayesian Information Criterion (BIC) для найденных значений точек в пространстве.

Нахождение критерия Акаике (AIC) выполняется по формуле:

$$AIC = n\,ln\left(\frac{RSS}{n}\right) + 2k,$$

где RSS – сумма квадратов остатков, n – общее количество наблюдений, k – количество параметров модели (включая свободный член).

Нахождение критерия Байеса (BIC) выполняется по формуле:

$$BIC = n\,ln\left(\frac{RSS}{n}\right) + k\,\ln(n).$$

Полученные значения для разных степеней полинома необходимо сравнить и выбрать наименьшие значения. Наименьшее значение определяет оптимальное соотношение точности аппроксимации и сложности модели, но без переобучения модели. Переобучением модели считается излишнее воздействие данных (шум) на полином.

Для нахождения RSS необходимо для каждой степени найти:

$$RSS = \sum_{i=1}^{n}[z_i - f(x_i, y_i)]^2,$$

где $f(x_i,y_i)$ значение полинома в точке (x_i,y_i).

Для нахождения AIC и BIC необходимо решение уравнения полиномов с первой до восьмой степени:

$$z = a_0 + a_1x + a_2y;$$

$$z = a_0 + a_1x + a_2y + a_3xy + a_4x^2 + a_5y^2;$$

$$z = a_0 + a_1x + a_2y + a_3xy + a_4x^2 + a_5y^2 + a_6x^2y + a_7xy^2 + a_8x^3 + a_9y^3;$$

$$z = a_0 + a_1x + a_2y + a_3xy + a_4x^2 + a_5y^2 + a_6x^2y + a_7xy^2 + a_8x^3 + a_9y^3 + a_{10}x^3y + a_{11}xy^3 + a_{12}x^4 + a_{13}y^4;$$

$$z = a_0 + a_1x + a_2y + a_3xy + a_4x^2 + a_5y^2 + a_6x^2y + a_7xy^2 + a_8x^3 + a_9y^3 + a_{10}x^3y + a_{11}xy^3 + a_{12}x^4 + a_{13}y^4 + a_{14}x^4y + a_{15}xy^4 + a_{16}x^5 + a_{17}y^5;$$

$$z = a_0 + a_1x + a_2y + a_3xy + a_4x^2 + a_5y^2 + a_6x^2y + a_7xy^2 + a_8x^3 + a_9y^3 + a_{10}x^3y + a_{11}xy^3 + a_{12}x^4 + a_{13}y^4 + a_{14}x^4y + a_{15}xy^4 + a_{16}x^5 + a_{17}y^5 + a_{18}x^5y + a_{19}xy^5 + a_{20}x^6 + a_{21}y^6;$$

$$z = a_0 + a_1x + a_2y + a_3xy + a_4x^2 + a_5y^2 + a_6x^2y + a_7xy^2 + a_8x^3 + a_9y^3 + a_{10}x^3y + a_{11}xy^3 + a_{12}x^4 + a_{13}y^4 + a_{14}x^4y + a_{15}xy^4 + a_{16}x^5 + a_{17}y^5 + a_{18}x^5y + a_{19}xy^5 + a_{20}x^6 + a_{21}y^6 + a_{22}x^6y + a_{23}xy^6 + a_{24}x^7 + a_{25}y^7;$$

$$z = a_0 + a_1x + a_2y + a_3xy + a_4x^2 + a_5y^2 + a_6x^2y + a_7xy^2 + a_8x^3 + a_9y^3 + a_{10}x^3y + a_{11}xy^3 + a_{12}x^4 + a_{13}y^4 + a_{14}x^4y + a_{15}xy^4 + a_{16}x^5 + a_{17}y^5 + a_{18}x^5y + a_{19}xy^5 + a_{20}x^6 + a_{21}y^6 + a_{22}x^6y + a_{23}xy^6 + a_{24}x^7 + a_{25}y^7 + a_{26}x^7y + a_{27}xy^7 + a_{28}x^8 + a_{29}y^8;$$

Ввиду того, что значения функции не проходят через координаты $(0;0;z_0)$, следовательно, $a_0 \neq z_0$. В связи с этим необходимо найти a0, а затем найти решение уравнения для оставшихся членов.

В общем виде решение предлагается строить в матричной форме, вида:

$$X = \begin{pmatrix} 1 & x_{11} & x_{12} & \dots & x_{1m} & x_{11}^2 & x_{12}^2 & \dots & x_{11}x_{12} & \dots & x_{11}^d & x_{12}^d & \dots & x_{11}^d x_{12}^d \\ 1 & x_{21} & x_{22} & \dots & x_{2m} & x_{21}^2 & x_{22}^2 & \dots & x_{21}x_{22} & \dots & x_{21}^d & x_{22}^d & \dots & x_{21}^d x_{22}^d \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\ 1 & x_{n1} & x_{n2} & \dots & x_{nm} & x_{n1}^2 & x_{n2}^2 & \dots & x_{n1}x_{n2} & \dots & x_{n1}^d & x_{n2}^d & \dots & x_{n1}^d x_{n2}^d \end{pmatrix};$$

$$Z = \begin{pmatrix} z_1 \\ z_2 \\ \vdots z_n \end{pmatrix}.$$

Для решения уравнения с применением метода Гаусса необходимо: перемножить обе стороны матричного уравнения слева на транспонированную матрицу $X^{\top}Xa = X^{\top}Z$. Найдем матрицу $C=X^{\top}X$ и вектор $b=X^{\top}Z$, а затем решим систему $Ca=b$. Решение системы $Ca=b$ выполнить методом Гаусса с приведением к верхней треугольной форме.

При наличии информации о числе наблюдений (n), количестве параметров (k), и величинах ошибок (RSS) допустимо вычислить критерии — AIC и BIC, а затем составить сравнительную таблицу. Итоговым результатом вычислений является степень полинома, оптимальная для аппроксимации построенных точек в пространстве.

Построение полинома удобнее выполнять автоматизированным способом. Визуализация аппроксимации для некоторых точек в пространстве представлена на рисунке 2.

Девятый этап выполняется для определения аппроксимирующей поверхности для КПБО$_{min}$ и ничем не отличается от выполняемых ранее вычислений. Задача данного этапа – построение аппроксимирующей поверхности допустимого риска.

Десятый этап заключается в получении значения объема фигуры, которую образует: полиномиальная поверхность (ограничение сверху), плоскость $z=0$ (ограничение снизу), плоскости, образуемые нормалями к координатным плоскостям крайних точек (боковые

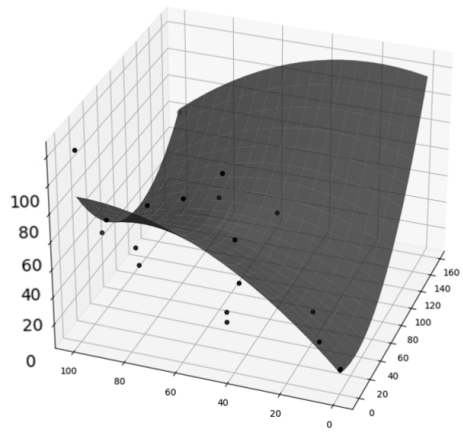

Рис. 2. Визуализация аппроксимирующей поверхности для точек в пространстве

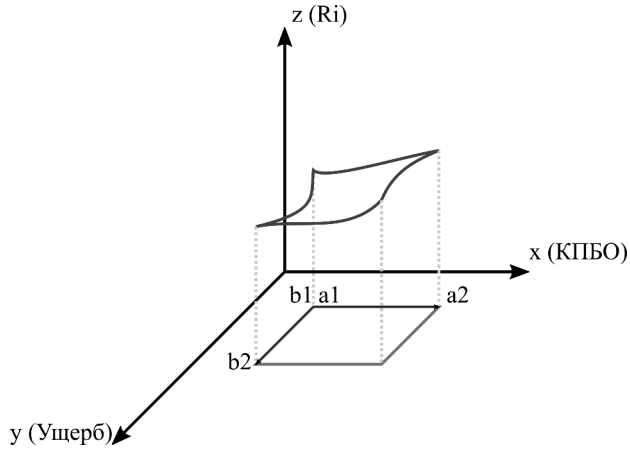

Рис. 3. Графическое представление по нахождению объема фигуры

грани). Для нахождения объема фигуры используется двойной интеграл, интегрируемый по координатам x и y, при фиксированном значении z.

Пусть границы фигуры заданы отрезками [a1, a2] вдоль оси x, [b1, b2] вдоль оси y, а поверхность, задаваемая полиномом, расположена целиком выше плоскости z. Начальной и конечной точками отрезков a1, a2, b1, b2 должны стать крайние точки, спроецированные на Oxy. Тогда нахождение объема производится по формуле:

$$V = \int_{a1}^{a2} \int_{b1}^{b2} f(x, y)\, dx\, dy\,.$$

Графическое представление по нахождению объема представлено на рисунке 3.

Заключительным этапом является определение объема фигуры оцениваемого риска и объема фигуры допустимого риска. Соотношение объемов фигур будет являться рассчитанным показателем риска, относительно приемлемого риска.

Предлагаемый метод позволяет проводить прогнозирование изменения рисков информационной безопасности с течением времени. Ввиду наличия математической функции, если предположить, что технические средства организации могут выходить из строя согласно теории надежности, то возможно произвести расчет рисков информационной безопасности через некоторый промежуток времени.

Предлагаемый метод имеет перспективы для дальнейшего исследования. Предполагается, что точки в координатном пространстве позволят построить векторы, что будет являться дополнительным фактором для анализа данных. Также предполагается, что полученные данные позволят построить градиент, что будет отображать тенденцию развития риска информационной безопасности и позволит проводить действия для минимизации риска.

Литература

1. ГОСТ Р ИСО 19439-2022 // Федеральное агентство по техническому регулированию и метрологии – [сайт] – URL: https://protect.gost.ru/document1.aspx?control=31&baseC=6&page=7&month=12&year=2022&search=&id=248845 (дата обращения 02.10.2025). – Режим доступа: свободный.

2. ГОСТ Р ИСО/МЭК 27005-2010 // РосГОСТ – [сайт] – URL: https://rosgosts.ru/file/gost/35/040/gost_r_iso!mek_27005-2010.pdf (дата обраще-ния: 10.10.2025). – Режим доступа: свободный.

3. СТО БР ИББС-1.0-2014 «Обеспечение информационной безопасности организаций банковской системы Российской Федерации» // Центральный банк Российской Федерации URL: https://cbr.ru/Crosscut/LawActs/File/446 (дата обращения: 18.10.2025). – Режим доступа: свободный.

4. ГОСТ Р 53114-2008 // Федеральное агентство по техническому регулированию и метрологии – [сайт] – URL: https://protect.gost.ru/document.aspx?control=7&id=174974 (дата обраще-ния 02.11.2025). – Режим доступа: свободный.

5. ГОСТ Р 51898—2002 «Аспекты безопасности. Правила включения в стандарты» Федеральное агентство по техническому регулированию и метро-логии. – 2002. 8 с.

6. ГОСТ Р 58771—2019 «Менеджмент риска. Технологии оценки рис-ка» // Электронный фонд правовых и нормативно-технических документов URL: https://docs.cntd.ru/document/1200170253 (дата обращения: 20.10.2025).

References

1. GOST R ISO 19439-2022 // Federal'noye agentstvo po tekhnicheskomu regulirovaniyu i metrologii – [sayt] – URL: https://protect.gost.ru/document1.aspx?control=31&baseC=6&page=7&month=12&year=2022&search=&id=248845 (data obrashcheniya 02.10.2025). – Rezhim dostupa: svobodnyy.

2. GOST R ISO/MEK 27005-2010 // RosGOST – [sayt] – URL: https://rosgosts.ru/file/gost/35/040/gost_r_iso!mek_27005-2010.pdf (data obra-shcheniya: 10.10.2025). – Rezhim dostupa: svobodnyy.

3. STO BR IBBS-1.0-2014 «Obespecheniye informatsionnoy bezopasno-sti organizatsiy bankovskoy sistemy Rossiyskoy Federatsii» // Tsentral'-nyy bank Ros-siyskoy Federatsii URL: https://cbr.ru/Crosscut/LawActs/File/446 (data obrashche-niya: 18.10.2025). – Re-zhim dostupa: svobodnyy.

4. GOST R 53114-2008 // Federal'noye agentstvo po tekhnicheskomu regu-lirovaniyu i metrologii – [sayt] – URL: https://protect.gost.ru/document.aspx?control=7&id=174974 (data obrashche-niya 02.11.2025). – Rezhim dostupa: svobodnyy.

5. GOST R 51898—2002 «Aspekty bezopasnosti. Pravila vklyucheniya v standarty» Federal'noye agentstvo po tekhnicheskomu regulirovaniyu i met-rologii. – 2002. 8 s.

6. GOST R 58771—2019 «Menedzhment riska. Tekhnologii otsenki ris-ka» // Elektronnyy fond pravovykh i normativno-tekhnicheskikh dokumentov URL: https://docs.cntd.ru/document/1200170253 (data obrashcheniya: 20.10.2025).

КОРЖЕНЕВСКИЙ Денис Алексеевич, аспирант, старший преподава-тель кафедры «Информационные технологии и защита информации» ФГБОУ ВО «Уральский государственный университет путей сообщения». 650034, г. Екатеринбург, ул. Колмогорова, 66. E-mail: DKorzhenevskiy@usurt.ru

ЗЫРЯНОВА Татьяна Юрьевна, кандидат технических наук, доцент, заведующий кафедрой «Информационные технологии и защита информации» ФГБОУ ВО «Уральский государственный университет путей сообщения». 650034, г. Екатеринбург, ул. Колмогорова, 66. E-mail: TZyryanova@usurt.ru

KORZHENEVSKIY Denis Alekseevich, post-graduate, Senior Lecturer at the Department of Information Technology and Information Security of the Federal State Budgetary Educational Institution of Higher Education «Ural State University of Railway Transport». 620034, Yekaterinburg, str. Kolmogorova, 66. E-mail: DKorzhenevskiy@usurt.ru

ZYRYANOVA Tatyana Yuryevna, Candidate of Technical Sciences, Associate Professor, Head of the Department of Information Technology and Information Security of the Federal State Budgetary Educational Institution of Higher Education «Ural State University of Railway Transport». 620034, Yekaterinburg, str. Kolmogorova, 66. E-mail: TZyryanova@usurt.ru