УДК 004.56
DOI 10.33764/2618-981X-2025-8-246-252

*А. А. Киселев[1]✉, В. М. Белов[2]*

# Методика оценивания уровня защищенности объектов КИИ с использованием нечеткой логики

[1] Новосибирский государственный технический университет,
г. Новосибирск, Российская Федерация
[2] Сибирский государственный университет геосистем и технологий,
г. Новосибирск, Российская Федерация
e-mail: anton.kiselev@corp.nstu.ru

**Аннотация.** Настоящая методика предназначена для оценивания уровня защищенности объектов критической информационной инфраструктуры (ОКИИ) с использованием нечеткой логики с целью своевременного выявления, оценивания и прогнозирования источников угроз информационной безопасности (ИБ), причин и условий, способствующих нанесению ущерба обладателю информации и ее оператору, нарушению нормального функционирования и развития информационно-телекоммуникационных систем (ИТКС) при проведении аудиторских проверок внутреннего аудита организации работы ОКИИ на соответствие требованиям безопасности информации.

**Ключевые слова:** методика оценивания, уровень защищенности, критическая информационная инфраструктура, нечеткая логика, лингвистическая шкала

*A. A. Kiselev[1]✉, V. M. Belov[2]*

# Methodology for assessing the security level of critical information infrastructure facilities using fuzzy logic

[1] Novosibirsk State Technical University, Novosibirsk, Russian Federation
[2] Siberian State University of Geosystems and Technologies, Novosibirsk, Russian Federation
e-mail: anton.kiselev@corp.nstu.ru

**Abstract.** This methodology is designed to assess the security level of critical information infrastructure objects (OCII) in order to timely identify, assess and predict sources of information security threats, causes and conditions that contribute to damage to the information owner and operator, disruption of the normal functioning and development of information and telecommunications systems when conducting audits of the internal audit organization of the OCII for compliance with information security requirements.

**Keywords:** assessment methodology, security level, critical information infrastructure, fuzzy logic, linguistic scale

## *Введение*

Анализ опубликованных работ наглядно демонстрирует важность и обстоятельность исследований по теме статьи. В конечном итоге точность результата оценивания напрямую зависит от количества учтенных факторов, что приводит и к возрастанию трудоемкости расчетов.

Настоящая методика предназначена для оценивания уровня защищенности ОКИИ [1-5] с целью своевременного выявления, оценивания и прогнозирования источников угроз ИБ, причин и условий, способствующих нанесению ущерба обладателю информации и ее оператору, нарушению нормального функционирования и развития ИТКС при проведении аудиторских проверок внутреннего аудита организации работы ОКИИ по направлению «Организация и состояние работы по защите информации», самооценки защищенности ОКИИ (планового периодического контроля ИБ) на соответствие требованиям документов по ИБ. Оценивание уровня защищенности ОКИИ проводят с использованием балльной и лингвистической шкал в рамках нечеткого логического вывода.

***Представление методики оценивания уровня защищенности ОКИИ***

Методика оценивания уровня защищенности ОКИИ заключается в определении коэффициента важности (КВ) вопросов и разделов методом парного сравнения, по которым проводят оценивание уровня защищенности ОКИИ, в построении эталонных значений всех уровней защищенности ОКИИ методом лингвистических термов (допускается применение и других методов построения функций принадлежности (ФП) для построения эталонных значений), в обработке значений результатов ответов сотрудников отдела информационной безопасности (ОИБ), сотрудника, ответственного за обеспечение ИБ с использованием теории нечетких множеств (ТНМ): определение суммарной оценки уровня защищенности ОКИИ (показателя уровня защищенности) и в сравнении со всеми эталонными значениями уровней защищенности ОКИИ, на основании которого определяют уровень защищенности ОКИИ.

Оценка уровня защищенности ОКИИ строится на сформированном перечне вопросов, касающихся разных влияющих на уровень безопасности параметров безопасности. Ответы на вопросы (по разделам) позволяют получить представление о степени выполняемости требований нормативных источников, что в совокупности позволяет получить интегральную оценку. При этом проводят расчет КВ для каждого вопроса внутри разделов, соответственно, эталонных значений, определяющих уровни защищенности ОКИИ. Расчет КВ разделов и вопросов осуществляют компетентные специалисты в области ИБ (вышестоящих подразделений ОКИИ или коллегиально).

При оценивании уровня защищенности ОКИИ вопросы, по которым проводят оценивание, должны охватывать все составляющие ИБ. Варианты ответов (шкалы ответов) строятся таким образом, чтобы учесть все возможные исходы в каждом случае оценивания. При оценивании для объективности привлекаются любые сведущие специалисты организации.

Критерии оценивания и значения соответствия балльных ответов лингвистическим значениям (термам) нечеткой переменной «Уровень защищенности» приведены в табл. 1.

*Таблица 1*

Критерии оценивания и значения соответствия балльных ответов лингвистическим значениям (термам) нечеткой переменной «Уровень защищенности»

| Балльная оценка | Лингвистическая оценка | Соответствие текущему состоянию вопроса |
|---|---|---|
| 0 | полное отсутствие защищенности на ОКИИ | Требования, степень выполнения которых не установлена во внутренних нормативных документах ОКИИ, не выполняются |
| 0-0,08 | очень низкая оценка уровня защищенности (ОНОУЗ) | Требования, степень выполнения которых не в полном объеме установлена во внутренних нормативных документах ОКИИ, неактуальны и не выполняются |
| 0,09-0,25 | низкая оценка уровня защищенности (НОУЗ) | Требования, степень выполнения которых полностью установлена во внутренних нормативных документах ОКИИ, неактуальны и выполняются не в полном объеме |
| 0,26-0,42 | средняя оценка уровня защищенности (СОУЗ) | Требования, степень выполнения которых полностью установлена во внутренних нормативных документах ОКИИ, неактуальны и выполняются в полном объеме |
| 0,43-0,58 | неизменная оценка уровня защищенности (НеОУЗ) | Требования, степень выполнения которых не в полном объеме установлена во внутренних нормативных документах ОКИИ, актуальны и выполняются не в полном объеме |
| 0,59-0,75 | нормальная оценка уровня защищенности (НоОУЗ) | Требования, степень выполнения которых полностью установлена во внутренних нормативных документах ОКИИ, актуальны и выполняются не в полном объеме |
| 0,76-0,92 | высокая оценка уровня защищенности (ВОУЗ) | Требования, степень выполнения которых не в полном объеме установлена во внутренних нормативных документах ОКИИ, актуальны и выполняются своевременно в полном объеме |
| 0,93-1 | очень высокая оценка уровня защищенности (ОВОУЗ) | Требования, степень выполнения которых полностью установлена во внутренних нормативных документах ОКИИ, актуальны и выполняются своевременно в полном объеме |
| 1 | полная защищенность ОКИИ | Требования, степень выполнения которых полностью установлена во внутренних нормативных документах ОКИИ, актуальны и выполняются своевременно в полном объеме |

Оценивание уровня защищенности ОКИИ должно основываться на свидетельствах аудита, в качестве основных источников которых рекомендуется использовать:

– внутренние нормативные документы ОКИИ и, при необходимости, документы третьих лиц, относящиеся к обеспечению защищенности ОКИИ;

– устные высказывания сотрудников, ответственных за обеспечение ИБ в процессе проводимых опросов;

– результаты наблюдений за деятельностью сотрудников ОКИИ в области ИБ;

– соответствие описанных требований в нормативных документах положению дел на местах;

– настройки и функционирование средств защиты информации (СЗИ) на ОКИИ.

В процессе проведения опроса сотрудников, ответственных за обеспечение ИБ ОКИИ и наблюдений за деятельностью сотрудников ОКИИ проверяющие должны сделать вывод о степени соответствия оцениваемой деятельности требованиям внутренних нормативных документов ОКИИ, документов РФ по ИБ.

***Этапы проведения оценивания уровня защищенности ОКИИ***

1. Проведение осмотра ОКИИ, анализ документов по ИБ, их актуальность, достоверность, соответствие положений дел в ОКИИ требованиям документов по ИБ, опрос сотрудников ОИБ (сотрудника по ИБ) и аудит ИБ, оценивание и прогнозирование источников угроз ИБ, причин и условий, способствующих нанесению ущерба оператору и обладателю информации, нарушению нормального функционирования и развития ИТКС.

2. Составление вопросов по различным направлениям ИБ ОКИИ. Помимо нормативных источников по ИБ РФ дополнительно использовать в случае проведения аудиторской проверки внутреннего аудита организации работы ОИБ по направлению «Организация и состояние работы по защите информации» утвержденную программу проверки, а при проведении самооценки защищенности ОКИИ (планового периодического контроля уровня защищенности) – рекомендации ФСТЭК России.

3. Определение КВ, используя метод относительного ранжирования, или руководствуясь требованиями, определенными для коэффициентов вышестоящей организацией.

4. Определение и формирование эталонных значений всех уровней защищенности ОКИИ методом лингвистических термов (определить термы для лингвистической переменной «Уровень защищенности»).

5. При проведении аудиторской проверки внутреннего аудита организации работы ОКИИ по направлению «Организация и состояние работы по защите информации» провести опрос ОИБ (сотрудника по ИБ), в случае необходимости – специалистов других подразделений по подготовленным разделам ИБ. При проведении самооценки уровня защищенности ОКИИ (планового периодического контроля защищенности) ответить на вопросы разделов ИБ самостоятельно. Ответы давать в лингвистической или балльной форме в зависимости от выбранной модели оценивания уровня защищенности ОКИИ.

6. Определить суммарную оценку уровня защищенности ОКИИ (показателя уровня защищенности) и провести сравнение со всеми эталонными значениями уровней защищенности ОКИИ.

7. На основании результатов сравнения суммарной оценки уровня защищенности ОКИИ (показателя уровня защищенности) с эталонными значениями уровней защищенности ОКИИ определить уровень защищенности ОКИИ.

8. Проанализировать уровень защищенности ОКИИ.

### *Нечеткие модели оценивания уровня защищенности ОКИИ*

1. Нечеткая модель оценивания уровня защищенности ОКИИ с использованием балльной шкалы.

ОИБ (сотрудник по ИБ) отвечает на предварительно ранжированные вопросы. Вопросы охватывают всю программу аудиторской проверки внутреннего аудита ОКИИ по направлению «Организация и состояние работы по защите информации» и проранжированы по степени важности по *N*-балльной шкале.

По истечении определенного времени сотрудники, осуществляющие проверку, просматривают вопросы, варьируют диапазон шкалы ответов и рассчитывают КВ для каждого вопроса в зависимости от актуальности моделей угроз и технических каналов утечки информации (ТКУИ) ОКИИ, нормативных документов по ИБ. Далее осуществляют опрос сотрудников по ИБ. Пользователи в качестве ответов приводят балльные оценки из диапазона ответов.

На завершающей стадии определяют показатель уровня защищенности ОКИИ. Если распределение КВ по разделам различно, то необходимо предварительно определить значимость каждого раздела ИБ.

2. Нечеткая модель оценивания уровня защищенности ОКИИ с использованием лингвистической шкалы (НМЛШ).

Состояние защищенности ОКИИ в соответствии с НМЛШ определяют по результатам опроса сотрудников ОИБ (сотрудника по ИБ) согласно программе аудиторской проверки внутреннего аудита ОКИИ по направлению «Организация и состояние работы по защите информации», разделы (вопросы) которой предварительно ранжируют через определение КВ. Для достижения этой цели используют метод ранжирования на основе преобразованной матрицы, полученной на основании матрицы парных сравнений (суждений) (табл. 2).

*Таблица 2*

Шкала для построения матрицы суждений

| Оценка значимости | Качественная оценка | Примечание |
|---|---|---|
| 1 | Одинаковая значимость | Альтернативы имеют одинаковый ранг |
| 3 | Слабое преимущество | Преимущество одной альтернативы перед другой малоубедительное |
| 5 | Сильное преимущество | Есть надежные доказательства существенного преимущества одной альтернативы |
| 7 | Очевидное преимущество | Существуют убедительные свидетельства в пользу одной альтернативы |
| 9 | Абсолютное преимущество | Свидетельство в пользу преимущества одной альтернативы над другой с наибольшей мерой убедительности |
| 2, 4, 6, 8 | Промежуточные значения | Используется, если необходим компромисс |

Сотрудники, осуществляющие проверку, просматривают вопросы, рассчитывают КВ для каждого вопроса в зависимости от актуальности моделей угроз и ТКУИ ОКИИ, нормативных документов по ИБ.

Далее осуществляется опрос пользователей. Модель НМЛШ предполагает, что группа из *N* сотрудников ОИБ (сотрудник по ИБ) отвечает на *n* вопросов (*n*-компонентный экспертный запрос), соответственно составленных проверяющим сотрудником по нечеткой шкале.

На завершающей стадии определяют показатель уровня защищенности ОКИИ. Если распределение КВ по разделам различно, то необходимо определить значимость каждого раздела ИБ.

Кроме ранжирования разделов (вопросов) по степени важности, сотрудники, осуществляющие проверку, также строят нечеткие эталоны, которые отображают лингвистическую переменную «Уровень защищенности», являющуюся образцом для сравнения нечетких чисел, задают базовое терм-множество лингвистической переменной (ЛП), которое определяет уровень защищенности ОКИИ нечеткими термами, выбирают вид ФП, метод реализации операций нечеткой арифметики.

### *Представление и анализ полученных результатов оценивания уровня защищенности ОКИИ*

После получения итоговых оценок уровня защищенности ОКИИ (итоговых и по разделам) выполняется анализ результатов.

Рекомендуется проводить сравнение результатов оценивания уровня защищенности ОКИИ, полученных при проведении самооценки и оценивания в результате проверки внутреннего аудита ОКИИ.

Полученные по результатам аудиторских проверок внутреннего аудита организации работы ОКИИ по направлению «Организация и состояние работы по защите информации», самооценки защищенности (планового периодического контроля уровня защищенности на соответствие требованиям документов по ИБ), значение уровня защищенности ОКИИ должно соответствовать требованиям нормативных документов по ИБ и высокой (0,76-0,92) или очень высокой (0,93-1) оценке уровня защищенности ОКИИ.

### *Заключение*

Возможное изменение внешней среды ведения деятельности ОКИИ, изменение и возрастание рисков ИБ вследствие естественных и/или преднамеренных изменений во внешней и внутренней среде ОКИИ является причиной для регулярного периодического проведения аудиторских проверок внутреннего аудита организации работы ОКИИ по направлению «Организация и состояние работы по защите информации» и самооценок уровня защищенности ОКИИ, что позволяет своевременно принимать меры по поддержанию защищенности ОКИИ на необходимом уровне. С помощью самооценки уровня защищенности ОКИИ самостоятельно оценивают соответствие защищенности ОКИИ критериям проверок и проводят анализ недостатков системы обеспечения защищенности ОКИИ.

Результаты самооценки уровня защищенности ОКИИ могут служить основанием для устранения выявленных недостатков системы обеспечения защищенности ОКИИ.

## БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Алгоритмическое и методическое обеспечение оценивания защищенности объектов критических инфраструктур: монография / В.М. Белов, А.А. Киселев, А.Б. Архипова, Т.М. Пестунова. — Москва: РУСАЙНС, 2025. — 190 с.

2. Белов В. М. Подход к оценке уровня информационной безопасности в территориальных налоговых органах / В. М. Белов, Е. Н. Пивкин // Математические методы в технике и технологиях – ММТТ-20 : XX Междунар. науч. конф. : в 10 т. Т. 10. – Ростов-на-Дону, 2007. – С. 239–240.

3. Корченко А. Г. Построение систем защиты информации на нечетких множествах: теория и практические решения / А. Г. Корченко. – Киев: МК-Пресс, 2006. – 320 с.

4. Дойникова Е. В. Оценивание защищенности и выбор контрмер для управления кибербезопасностью: монография / Е. В. Дойникова, И. В. Котенко. – Санкт-Петербург: РАН, 2021. – 197 с.

5. Интеллектуальные сервисы защиты информации в крити-ческих инфраструктурах / И. В. Котенко, И. Б. Саенко, А. А. Чечулин [и др.]; под общ. ред. И. В. Котенко, И. Б. Саенко. – Санкт-Петербург: БХВ-Петербург, 2019. – 400 с. – ISBN 978-5-9775-3968-5.