DOI 10.37882/2223-2966.2024.10-2.02

# АЛГОРИТМ ОЦЕНИВАНИЯ БЕЗОПАСНОСТИ ИНФОРМАЦИОННЫХ АКТИВОВ ПАССАЖИРСКИХ ПЕРЕВОЗОК ЖЕЛЕЗНОДОРОЖНЫМ ТРАНСПОРТОМ ПРИ НЕЧЕТКИХ ДАННЫХ

## AN ALGORITHM FOR EVALUATING THE SECURITY OF INFORMATION ASSETS OF PASSENGER TRANSPORTATION BY RAIL WITH FUZZY DATA

***E. Belova***
***A. Glukhov***
***S. Kornienko***
***A. Glukhov***

*Summary*. The article considers a variant of constructing an algorithm for assessing the information security of passenger transportation assets, taking into account the relationship between information security indicators of information assets, which is based on a hierarchical fuzzy production model of assets. This approach makes it possible to assess the information security of automated control systems for passenger transportation using vector safety indicators and the possibility of conducting security assessments of critical business processes based on statistical data and expert assessments.

*Keywords*: information security, hierarchical model, critical processes, management system, computer attacks.

***Белова Елена Ивановна***
*Аспирант, Петербургский государственный университет путей сообщения Императора Александра I*
*elenabelovavm@yandex.ru*
***Глухов Александр Петрович***
*доктор технических наук, Петербургский государственный университет путей сообщения Императора Александра I*
*apg606@yandex.ru*
***Корниенко Светлана Владимировна***
*кандидат технических наук, Петербургский государственный университет путей сообщения Императора Александра I*
*sv.diass99@yandex.ru*
***Глухов Александр Александрович***
*директор программ по информационно-телекоммуникационным системам, АО «Научно-производственное объединение «Критические информационные системы»*
*alexander.glukh0v@yandex.ru*

*Аннотация*. В статье рассмотрен вариант построения алгоритма оценивания информационной безопасности активов пассажирских перевозок, в основе которого лежит иерархическая нечетко-продукционная модель активов, а также учитываются взаимосвязи между показателями информационной безопасности информационных активов, Данный подход позволяет оценивать информационную безопасность АСУ пассажирских перевозок с использованием векторных показателей безопасности и возможностью проведения оценок безопасности критических бизнес- процессов на основе статистических данных и экспертных оценок.

*Ключевые слова*: информационная безопасность, иерархическая модель, критические процессы, система управления, компьютерные атаки.

Безопасность информационной инфраструктуры (ИИ) железнодорожного транспорта (ЖТ) в современных условиях непрерывного повышения интенсивности, разнообразия и результативности компьютерных атак (КА), определяется эффективностью и адекватностью реализуемых мер защиты информации на всех уровнях ИИ.

Деятельность по обеспечению информационной безопасности (ИБ) должна быть направлена на поддержание основных бизнес-процессов организаций ЖТ. Рассмотрение процесса создания (совершенствования) системы обеспечения информационной безопасности (СОИБ) организаций ЖТ как одного из обеспечивающих процессов, обеспечивающего основные процессы предприятия дает возможность разработки СОИБ в тесной взаимосвязи с проектированием других бизнес-процессов, что увеличит их интегрированность, гибкость, сбалансированность и управляемость.

Со стороны государственных регуляторов в области ИБ осуществляется переход от оценок воздействий

компьютерных инцидентов (КИ) на такие свойства информации, как конфиденциальность, целостность и доступность, к оценкам влияния КИ на бизнес-процессы организаций [1,2].

Реализация такого перехода требует разработки соответствующего методического аппарата, в том числе порядка (алгоритма) оценивания информационной безопасности АСУ пассажирских перевозок (АСУ ПП) железнодорожного транспорта на уровне безопасности следующих информационных активов (ИА) пассажирских перевозок:

— бизнес — процессов (БП) ПП,
— функциональных задач (ФЗ), решаемых при обеспечении БП;
— программных модулей АСУ ПП, обеспечивающих решение этих задач,
— программно-технических комплексов АСУ ПП [3].

В работе [4] была предложена иерархическая модель показателей безопасности информационных активов пассажирских перевозок и соответствующая ей иерархическая нечетко-продукционная модель [5] оценивания безопасности ИА ПП железнодорожного транспорта (рисунок 1).

В представленной модели на нижнем уровне находятся продукционные правила (ПрПр) для оценивания показателей качества функционирования (ПКФ) программно-технических комплексов АСУ ПП (например: производительность, коэффициент готовности, количество нормально функционирующих в сети интернет-терминалов продажи билетов и др.) в зависимости от компьютерных инцидентов в результате компьютерных атак.

В данных ПрПр условия (антецеденты) формируются на основе данных о компьютерных инцидентах, выводы (консеквенты) — значения ПКФ АСУ ПП.

На втором уровне — ПрПр для оценивания показателей безопасности программных модулей АСУ ПП (например: непротиворечивость данных нормативно-справочной информации (НСИ) для всего пассажирского комплекса (ПМ 1.1), полнота данных НСИ для всего пассажирского комплекса (ПМ 1.2); актуальность данных НСИ для всего пассажирского комплекса (ПМ 1.3); сохранность данных НСИ для всего пассажирского комплекса (ПМ.1.4) и другие.

Здесь антецеденты — значения ПКФ АСУ ПП, консеквенты — значения показателей безопасности модулей АСУ ПП.

На третьем уровне в ПрПр антецеденты — значения показателей безопасности модулей АСУ ПП, консеквенты — значения показателей выполнения функциональных задач (например: своевременность формирования данных о потребностях на перевозку (ПЗ 1.1), полнота формирования данных о потребностях на перевозку (ПЗ 1.2), достоверность формирования данных о потребностях на перевозку (ПЗ 1.3) другие.

На четвертом уровне антецедентами выступают значения показателей выполнения функциональных за-

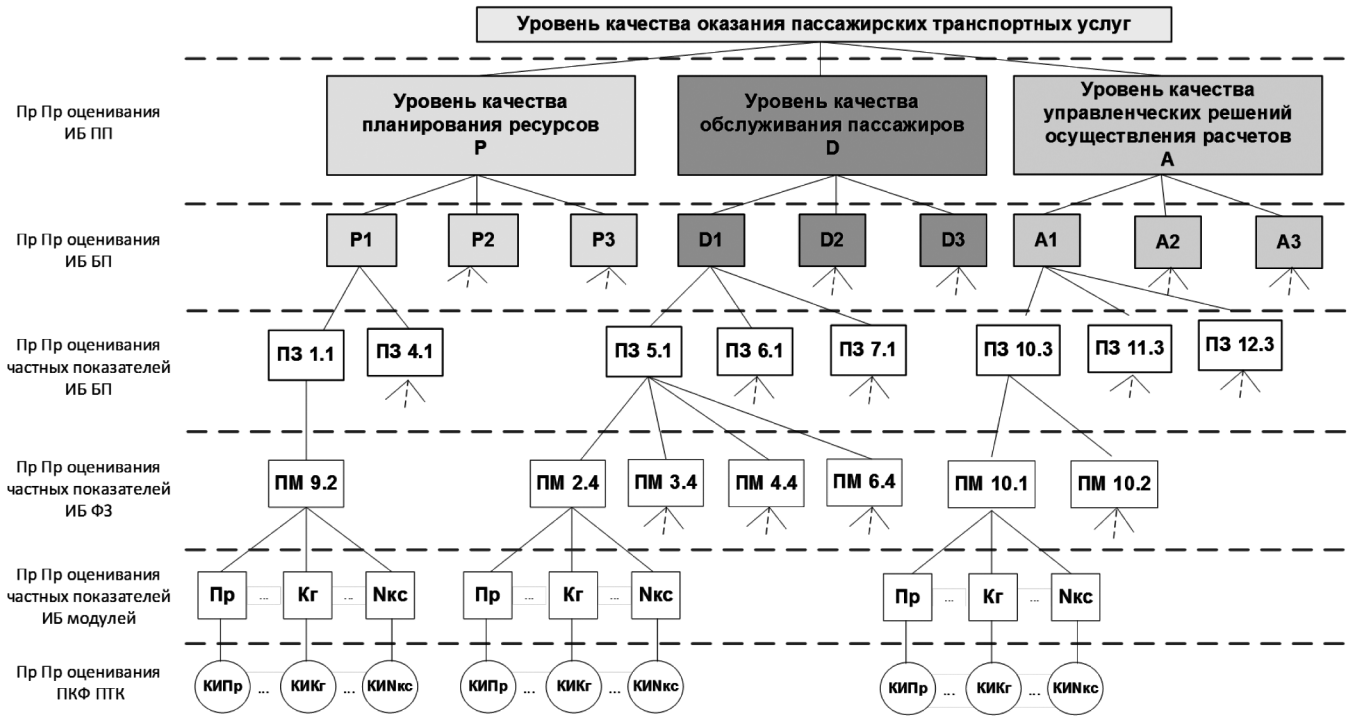


Рис. 1. Иерархическая модель нечетко-продукционных правил оценивания ИБ пассажирских перевозок

дач, а консеквентами значения частных показателей критических бизнес-процессов (например: количество отправленных пассажиров (D1), полнота данных, включающих информацию о поездах, тарифах, объектах сети и иной нормативно-справочной информации, необходимой для обслуживания пассажиров (D2), достоверность данных о номерах поездов возможности проезда на запрашиваемом маршруте, наличия мест в выбранных поездах, стоимости проезда (D3) и другие.

На пятом уровне в ПрПр антецеденты — значения показателей критических бизнес-процессов, консеквенты — значения показателей безопасности критических бизнес-процессов (уровень качества планирования ресурсов, уровень качества обслуживания пассажиров, уровень качества управленческих решений осуществления взаиморасчетов), определяющих в конечном итоге состояние интегрального показателя пассажирских перевозок — уровень качества оказания пассажирских транспортных услуг.

На рисунке 2 представлена блок-схема алгоритма оценивания информационной безопасности АСУ ПП по уровню безопасности критического бизнес-процесса.

Предлагается следующий порядок оценивания безопасности ИА ПП:

На Шаге 1 данного порядка производится формирование экспертной группы для определения нечетких множеств текущего состояния показателей информационной безопасности (ПБ) и формирования продукционных правил (ПрПр) для ПБ.

На Шаге 2 экспертами формируется исходный набора правил для каждого ПБ информационных активов пассажирских перевозок.

Шаг 3. Анализ и устранение противоречивых и избыточных правил.

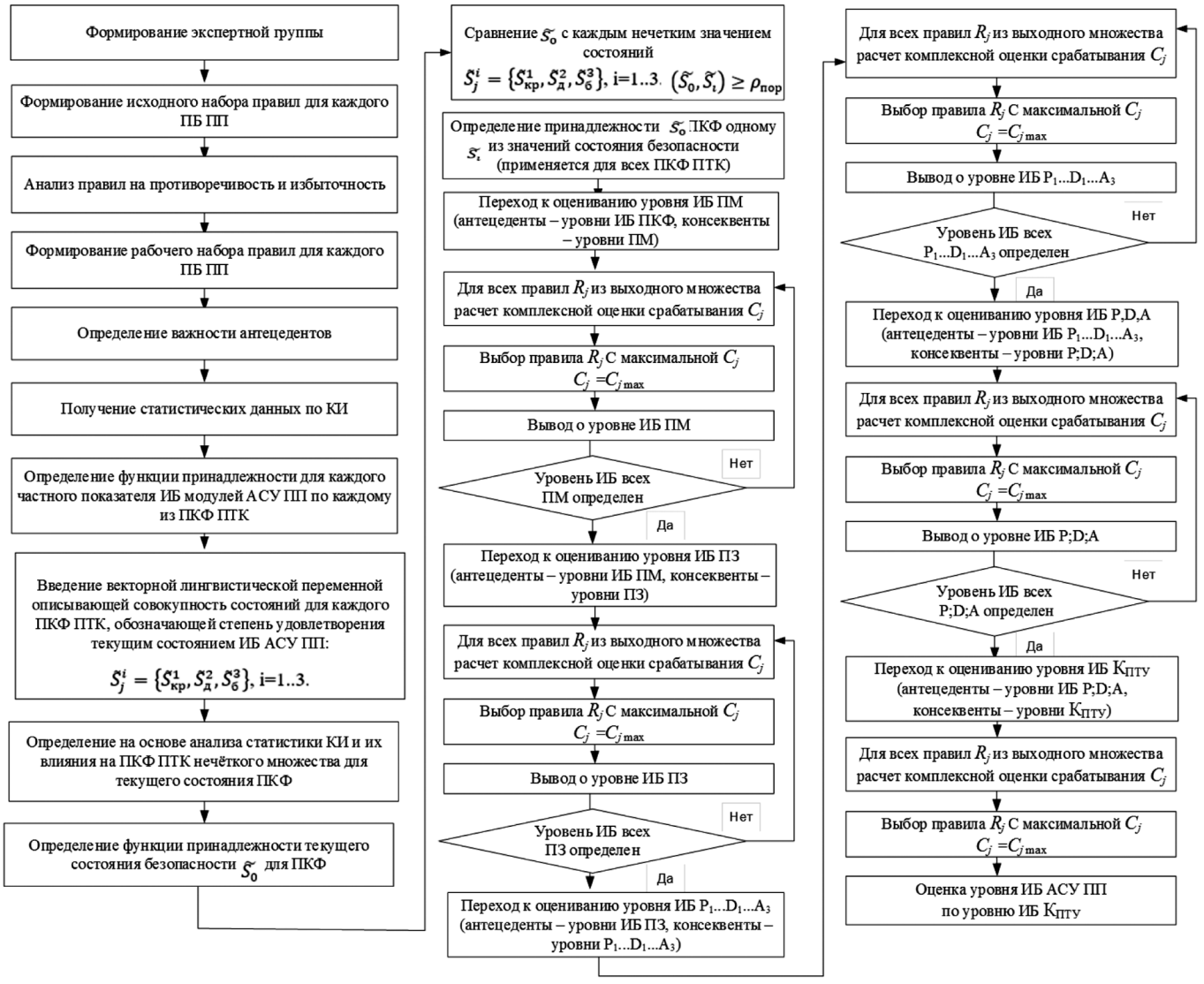


Рис. 2. Блок-схема алгоритма оценивания информационной безопасности АСУ ПП

Шаг 4. Формирование набора продукционных правил для каждого ПБ ПП иерархической модели.

Шаг 5. Определение важности ПБ в рамках введенных продукционных правил.

Шаг 6. Построение иерархической модели нечетко-продукционных правил оценивания ИБ пассажирских перевозок.

Шаг 7. Получение из систем мониторинга ИБ и IT - инфраструктуры статистических данных по компьютерным инцидентам (КИ), связанных с изменением (ухудшением) показателей качества функционирования программно-технических комплексов (ПКФ ПТК) АСУ ПП.

Шаг 8. Определение функции принадлежности для каждого частного показателя ИБ модулей $\left(i = 1\ldots K_{\text{ПМ}}\right)$ по каждому из ПКФ ПТК $\left(j_{ij} = 1\ldots K_{\text{ПКФ}ij}\right)$.

Шаг 9. Введение векторной лингвистической переменной, описывающей совокупность состояний для каждого ПКФ ПТК в пределах $[\,\text{ПКФ}_{min_{ij}}; \text{ПКФ}_{max_{ij}}\,]$, обозначающей степень удовлетворения текущим состоянием информационной безопасности АСУ ПП. При пятиуровневом нечетком классификаторе «критическое» (К), «близкое к критическому» (БК), «допустимое» (Д), «близкое к безопасному» (ББ), «безопасное» (Б) рассматриваются пять соответствующих функций принадлежности $\left\{\tilde{S}^1_{\text{кр}}, \tilde{S}^2_{\text{бк}}, \tilde{S}^3_{\text{д}}, \tilde{S}^4_{\text{ббз}}, \tilde{S}^5_{\text{б}}\right\}$, $i$=1..5.

Шаг 10. Определение на основе статистики КИ и влияния на $\text{ПКФ}_{il}$ нечёткого множества для текущего состояния $\text{ПКФ}_{ij}$.

Шаг 11. Определение функции принадлежности текущего значения безопасности ($\tilde{S}_0$) для $\text{ПКФ}_{ij}$.

Шаг 12. Сравнение текущего значения ($\tilde{S}_0$) $\text{ПКФ}_{ij}$ с каждым нечетким значением состояний $\left\{\tilde{S}^1_{\text{кр}}, \tilde{S}^2_{\text{бк}}, \tilde{S}^3_{\text{д}}, \tilde{S}^4_{\text{ббз}}, \tilde{S}^5_{\text{б}}\right\}$, $i$=1..5. путем расчета степени включения текущего состояния $S_0$ в состояние $\tilde{S}^i_j\left\{\tilde{S}^1_{\text{кр}}, \tilde{S}^2_{\text{бк}}, \tilde{S}^3_{\text{д}}, \tilde{S}^4_{\text{ббз}}, \tilde{S}^5_{\text{б}}\right\}$ и проверки ее соответствия порогу включения ситуаций ($0{,}6 \le \rho \le 1$), т.е. $\left(\tilde{S}_0, \tilde{S}_i\right) \ge \rho_{\text{пор}}$.

Шаг 13. Определяется принадлежность текущего состояния ($\tilde{S}_0$) $\text{ПКФ}_{ij}$ одному из значений состояния безопасности ($\tilde{S}_i$). Снятие «нечеткости» с определения уровня текущей ситуации снимается. Шаг 13 применяется для всех ПКФ ПТК.

Шаг 14. Переход к оцениванию состояния ИБ частных показателей ИБ модулей АСУ ПП ($\text{ПМ}_i$) исходя из сформированных продукционных правил, где антецеденты — уровни ИБ $\text{ПКФ}_{ij}$, а консеквенты — уровни $\text{ПМ}_i$.

Шаг 15. Для всех правил $R_j$ из выходного множества производится расчет их комплексной оценки срабатывания $C_j$.

Шаг 16. Выбирается правило $R_j$ с максимальной комплексной оценкой срабатывания $C_j = C_{\text{jmax}}$.

Шаг 17. Вывод о уровне ИБ частного показателя безопасности модуля АСУ ПП ($\text{ПМ}_i$).

Шаг 18. Выполнение шагов 15–17 для определения уровней ИБ всех частных показателей модулей АСУ ПП ($\text{ПМ}_i$).

Шаг 19. Переход к оцениванию состояния ИБ частных показателей функциональных задач АСУ ПП (ПЗ) исходя из сформированных продукционных правил, где антецеденты — уровни ИБ $\text{ПМ}_i$, а консеквенты — уровни ПЗ.

Шаг 20. Выполнение шагов 15–16 для определения уровня ИБ частного показателя функциональной задачи АСУ ПП.

Шаг 21. Вывод о уровне ИБ частного показателя безопасности функциональной задачи АСУ ПП.

Шаг 22. Выполнение шагов 20–21 для определения уровня ИБ всех частных показателей функциональных задач АСУ ПП (ПЗ).

Шаг 23. Переход к оцениванию состояния ИБ частных показателей бизнес-процессов АСУ ПП ($P_1,P_2,P_3$; $D_1,D_2,D_3$; $A_1,A_2,A_3$) исходя из сформированных продукционных правил, где антецеденты — уровни ИБ ПЗ, а консеквент — уровни частных показателей ИБ бизнес-процессов ($P_1,P_2,P_3$; $D_1,D_2,D_3$; $A_1,A_2,A_3$).

Шаг 24. Выполнение шагов 15–16 для определения уровня ИБ частного показателя бизнес-процесса.

Шаг 25. Вывод о уровне ИБ частного показателя безопасности бизнес-процесса АСУ ПП.

Шаг 26. Выполнение шагов 24–25 для определения уровня ИБ всех частных показателей бизнес-процессов АСУ ПП ($P_1,P_2,P_3$; $D_1,D_2,D_3$; $A_1,A_2,A_3$).

Шаг 27. Переход к оцениванию состояния ИБ показателей бизнес-процессов АСУ ПП (P; D; A) исходя из сформированных продукционных правил, где антецеденты — уровни ИБ $P_1,P_2,P_3$; $D_1,D_2,D_3$ и $A_1,A_2,A_3$, а консеквент — уровни ИБ показателей бизнес-процессов (P; D; A).

Шаг 28. Выполнение шагов 15–16 для определения уровня ИБ показателя бизнес-процесса.

Шаг 29. Вывод о уровне ИБ показателя безопасности бизнес-процесса АСУ ПП.

Шаг 30. Выполнение шагов 28–29 для определения уровней ИБ всех показателей бизнес-процессов АСУ ПП (P; D; A).

Шаг 31. Переход к оцениванию состояния ИБ «Уровня качества оказания пассажирских транспортных услуг» АСУ ПП ($К_{ПТУ}$) исходя из сформированных продукционных правил, где антецеденты — уровни ИБ P; D; A, а консеквент — уровень ИБ $К_{ПТУ}$.

Шаг 32. Выполнение шагов 15–16 для определения уровня ИБ $К_{ПТУ}$.

Шаг 33. Вывод о уровне ИБ «Качество предоставления пассажирских транспортных услуг» ($К_{ПТУ}$) АСУ ПП.

Рассмотрим частный пример оценки ИБ АСУ ПП по уровню безопасности бизнес-процесса «Обслуживание пассажиров» по показателю «Количество отправленных пассажиров».

В случае, когда для показателя безопасности какого-либо информационного актива (ИА) возможно (например, экспертным путем) определить влияние основных показателей качества функционирования ПТК АСУ ПП, (производительность — Пр, коэффициент готовности — $К_г$, количество работоспособных каналов самообслуживания — $N_{кс}$), предлагается следующая нечеткая модель на основе определения функции принадлежности состояния ИА в зависимости от ПКФ, характеризующая плавное изменение ПБ ИА от «критического» состояния к «безопасному», представленная на рисунке 3 [6].

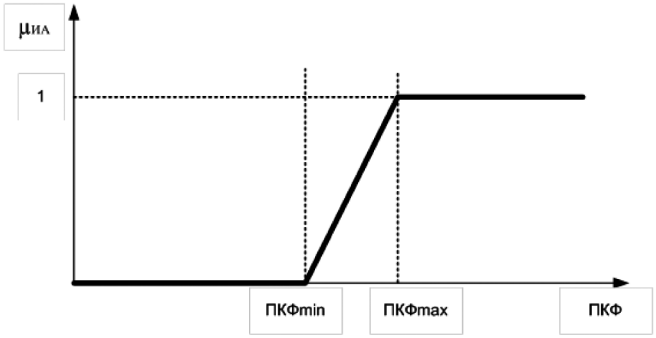


Рис. 3. Функция принадлежности для информационных активов и ПКФ ПТК
($\mu_{иа} = 1$ — безопасное состояние ИА, $\mu_{иа} = 0$ — критическое состояние ИА)

На основе анализа исходных данных, в которые входят:

— средняя стоимость билета;
— количество пассажиров, отправленных в дальнем следовании;
— доход от пассажирских перевозок;
— доля пассажиров, которые приобрели билеты через каналы самообслуживания;
— количество пассажиров, которые приобрели билеты через каналы самообслуживания;
— доход компании от продажи билетов через каналы самообслуживания;
— количество запросов через каналы самообслуживания на одно место;
— критический уровень недополучения доходов;
— критический уровень доходов от пассажирских перевозок пассажиров с билетами, приобретенными через каналы самообслуживания;
— минимально требуемое количество перевезенных пассажиров с билетами, приобретенными через каналы самообслуживания

можно определить максимальные и минимальные значения для основных ПКФ ПТК АСУ ПП, влияющих на информационную безопасность основного коммерческого показателя БП ПП - доход компании от ПП.

Допустим, например, что:

1. Производительность АСУ ПП в количестве запросов:
— требуемая производительность в количестве запросов ($Пр_{max}$) — 16,8 млрд запросов/год;
— минимальная производительность в количестве запросов ($Пр_{min}$) — 15,1 млрд запросов/год.

При оценивании ИБ учитывается текущая оценка экспертов, которая представлена на рис. 2 в виде функции принадлежности текущей ситуации. Для определения уровня безопасности ПБ необходимо сравнить текущее значение $\tilde{S}_0$ с каждым нечетким значением состояний: $\tilde{S}_j^i = \left\{ \tilde{S}_{кр}^1, \tilde{S}_{бк}^2, \tilde{S}_{д}^3, \tilde{S}_{бб}^4, \tilde{S}_{б}^5 \right\}$, $i$=1..5.

Пример оценивания ИБ при заданных функциях принадлежности представлен ниже.

Оценим ИБ основного коммерческого показателя БП ПП — доход компании от ПП на ПКФ ПТК АСУ ПП «Производительность АСУ ПП в количестве запросов».

Пусть, например, $\mu_s(y_i) = \{y_1, y_2, y_3, y_4, y_5\}$ — функция принадлежности лингвистической переменной $y_i$ при $i$=5: $y_1$ — «критическое», $y_2$ — «близкое к критическому», $y_3$ — «допустимое», $y_4$ — «близкое к безопасному», $y_5$ — «безопасное», $\tilde{S}_0$ — «текущее состояние» ПКФ ПТК АСУ ПП (Пр) по мнению экспертов.

Рассчитываем значения функций принадлежности для ПКФ ПТК АСУ ПП (Пр) (таблица 1).

Таблица 1.

Значения функций принадлежности

| № п/п | Функция принадлежности | |
|---|---|---|
| 1 | $\mu_{к}(\text{Пр}) = \begin{cases} 1 \\ \frac{15.56 - \text{Пр}}{15,56 - 15,1} \\ 0 \end{cases}$ | при $0 \le \text{Пр} \le 15,1$;<br>при $15,1 < \text{Пр} < 15,56$;<br>при $\text{Пр} \ge 15,56$; |
| 2 | $\mu_{бк}(\text{Пр}) = \begin{cases} 0 \\ \frac{\text{Пр} - 15,1}{15,56 - 15,1} \\ \frac{16 - \text{Пр}}{16 - 15,56} \\ 0 \end{cases}$ | при $0 \le \text{Пр} \le 15,1$;<br>при $15,1 \le \text{Пр} \le 15,56$;<br>при $15,56 < \text{Пр} \le 16$;<br>при $\text{Пр} > 16$; |
| 3 | $\mu_{д}(\text{Пр}) = \begin{cases} 0 \\ \frac{\text{Пр} - 15,56}{16 - 15,56} \\ \frac{16,45 - \text{Пр}}{16,45 - 16} \\ 0 \end{cases}$ | при $0 \le \text{Пр} \le 15,56$;<br>при $15,56 \le \text{Пр} \le 16$;<br>при $16 < \text{Пр} \le 16,45$;<br>при $\text{Пр} > 16,45$; |
| 4 | $\mu_{ББ}(\text{Пр}) = \begin{cases} 0 \\ \frac{\text{Пр} - 16}{16,45 - 16} \\ \frac{16,8 - \text{Пб}}{16,8 - 16,45} \\ 0 \end{cases}$ | при $0 \le \text{Пр} \le 16$;<br>при $16 \le \text{Пр} \le 16,45$;<br>при $16,45 < \text{Пр} \le 16,8$.<br>при $\text{Пр} > 16,8$; |
| 5 | $\mu_{Б}(\text{Пр}) = \begin{cases} 0 \\ \frac{\text{Пр} - 16,45}{16,8 - 16,45} \\ 1 \end{cases}$ | при $0 \le \text{Пр} \le 16,45$;<br>при $16,45 < \text{Пр} \le 16,8$;<br>при $\text{Пр} > 16,8$. |

Результаты расчетов показали (рисунок 4), что функция принадлежности «текущего состояния» ($\tilde{S}_0$) (полученная по результатам обработки мнений экспертов) информационной безопасности ПКФ ПТК АСУ ПП «Производительность АСУ ПП в количестве запросов» (Пр) с учетом компьютерных инцидентов, влияющих на данный показатель, соответствует значению {15,56; 15,92; 16,27}.

Производим анализ состояния текущей ситуации и проверяем степень включения состояния $\tilde{S}_0$ в состояние $\tilde{S}^2_{бк}$ и $\tilde{S}^3_{д}$: $v\left(\tilde{S}_0, \tilde{S}^2_{бк}\right) = 0,2 < \rho_{пор}$; $v\left(\tilde{S}_0, \tilde{S}^3_{д}\right) = 0,8 > \rho_{пор}$.

Таким образом, состояние $\tilde{S}_0$ нечетко включается в состояние $\tilde{S}^3_{д}$, что соответствует «допустимому» состоянию.

Определим абсолютное и относительное расстояния Хемминга $\rho_{АВ}$ и $\sigma_{АВ}$ между $\mu_{тек}(\text{Пр}) - \mu_{БК}(\text{Пр})$ и $\mu_{тек}(\text{Пр}) - \mu_{Д}(\text{Пр})$ (табл. 2).

В данном случае результаты расчётов показали, что минимум ФП $\mu_{тек}$ также соответствует «допустимому» состоянию.

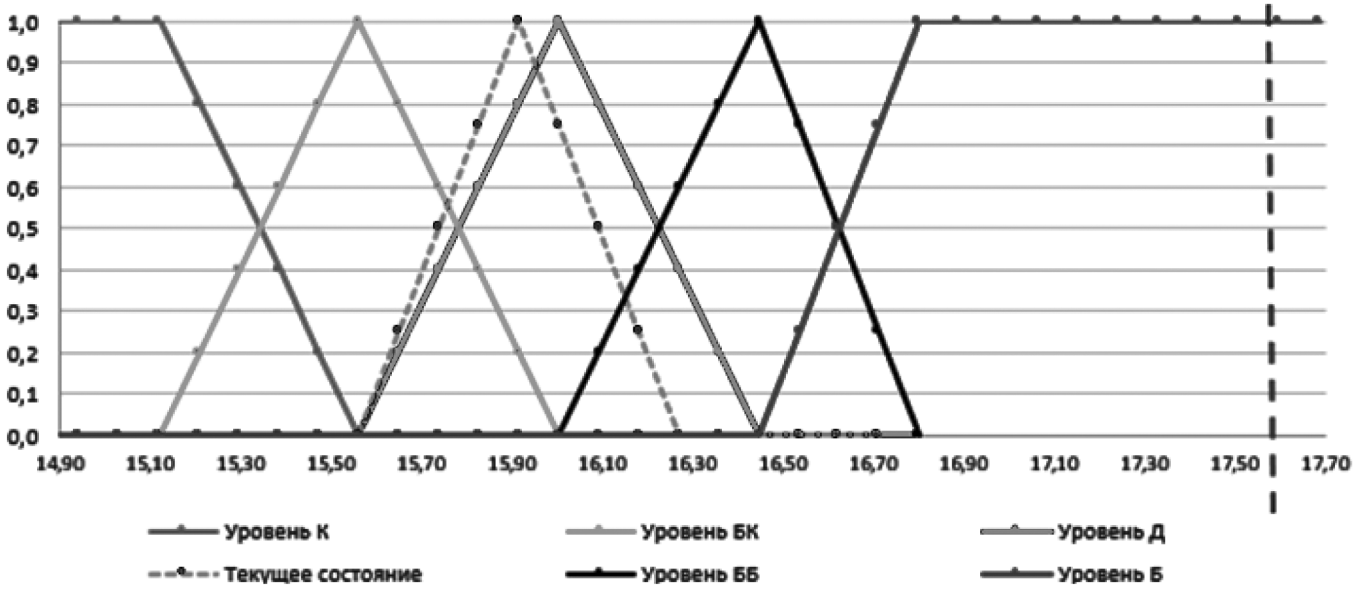


Рис. 4. Функции принадлежности для лингвистической переменной ПКФ ПТК АСУ ПП «Производительность АСУ ПП в количестве запросов» (Пр)

Таблица 2.
Результаты расчётов абсолютного и относительного расстояния Хемминга

| | $\rho_{АВ}$ | $\sigma_{АВ}$ |
|---|---|---|
| $\mu_{тек}(Пр) - \mu_{БК}(Пр)$ | 6,30 | 0,23 |
| $\mu_{тек}(Пр) - \mu_{Д}(Пр)$ | 2,00 | 0,07 |

Аналогичным образом проводятся расчеты для ПКФ $N_{кс}$ и $K_{г}$, что в итоге позволит выполнить векторную оценку показателя безопасности информационного актива.

Предлагаемый порядок оценивания информационной безопасности информационных активов пассажирских перевозок и нечетко определенных параметров может быть использован в системе управления информационной безопасностью железнодорожного транспорта.

ЛИТЕРАТУРА


1. Глухов А.П., Корниенко А.А., Белова Е.И. Подход к оцениванию информационной безопасности автоматизированных систем управления пассажирским перевозками железнодорожного транспорта // Двойные технологии. — 2023. — №1 (102). — С. 71–77.
2. Глухов А.П., Корниенко А.А., Ададуров С.Е., Белова Е.И. Оценивание информационной безопасности бизнес-процессов // Автоматика, связь, информатика. — 2023. — №7. — С. 17–20.
3. Белова, Е.И. Модели и алгоритмы оценивания информационной безопасности автоматизированной системы управления пассажирскими перевозками железнодорожного транспорта / Е.И. Белова // Двойные технологии. — 2023. — № 2. — С.48–54.
4. Белова Е.И., Корниенко С.В., Глухов А.П. Иерархическая нечетко-продукционная модель оценивания безопасности информационных активов пассажирских перевозок // В сборнике: Цифровые системы и модели: теория и практика проектирования, разработки и применения. Материалы национальной (с международным участием) научно-практической конференции. Казань. — 2024. — С. 1240–1244.
5. Катасев А.С., Емалетдинова Л.Ю. Нечетко-продукционная каскадная модель диагностики состояния сложного объекта // Программные системы и вычислительные методы . — 2013. — № 1(2). — С. 69–81.
6. Долженко А.И. Оценка нефункциональных характеристик качества информационной системы на основе теории нечетких чисел // Известия ВУЗов. Северо-Кавказский регион. Естественные науки. Приложение. — 2006. — №8. — С. 3–9.
7. Глухов А.П. Подходы к управлению информационной безопасностью в ОАО «РЖД» и модель ситуационного управления в нечеткой среде // Естественные и технические науки. — 2015. — № 9(87). — С. 127–136.