ISSN 2658-5014 (Print) СИИТ ISSN 2686-7044 (Online)
2023. Т. 5, № 3 (12). С. 93–113 http://siit.ugatu.su
СИСТЕМНАЯ ИНЖЕНЕРИЯ И ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ

УДК 004.056.5 DOI 10.54708/2658-5014-SIIT-2023-no3-p93

Методы и алгоритмы количественной оценки и управления рисками безопасности в корпоративных информационных сетях на основе нечеткой логики

И. В. Аникин

Аннотация. В статье представлен обзор результатов исследования количественной оценки и управления рисками безопасности в корпоративных информационных сетях (КИС). Объектом исследования являются корпоративные информационные сети как объект защиты информации. Предмет исследования — модели, методы и алгоритмы нечеткой оценки и управления рисками информационной безопасности КИС. Цель — повышение эффективности защиты корпоративных информационных сетей на основе применения научно обоснованных методов, алгоритмов, технологических решений и инструментальных программных комплексов количественной оценки и управления рисками информационной безопасности в условиях возможной нечеткости, противоречивости, неполноты и качественного характера исходной информации. Достижение поставленной цели потребовало решения следующих задач разработки: 1) формальной модели КИС, описывающей различные виды активов и особенности их взаимодействия для решения задачи количественной оценки рисков ИБ; 2) метода и алгоритмов нечеткой оценки ущерба от реализации угроз при отсутствии защитных мер на основе подходов к количественной оценке частных показателей ущерба, нечеткой оценке уровней критичности активов и формальной модели КИС; 3) методов и алгоритмов нечетких оценок возможностей реализации угроз и использования уязвимостей при отсутствии защитных мер в условиях неопределенности исходной информации; 4) метода повышения эффективности защиты информации в КИС на основе управления рисками ИБ, с учетом модели защитных мер, нечеткой оценки рисков ИБ; 5) технологии количественной оценки и управления рисками ИБ в КИС; 6) инструментального комплекса программ для нечеткой оценки и управления рисками информационной безопасности в КИС, реализующего разработанные технологию, методы и алгоритмы. Для решения поставленных задач были использованы методы математического моделирования, системного анализа, теории нечетких множеств и нечеткой логики, теории графов, защиты информации, экспертного оценивания.

Ключевые слова: информационная безопасность; оценка рисков; управление рисками; нечеткая логика; моделирование; комплекс программ.

Введение

Бурное развитие вычислительной техники привело к значительному увеличению степени автоматизации современных предприятий. Повсеместное применение информационных технологий (ИТ) позволило им, с одной стороны, выйти на качественно новый уровень производства, с другой – привело к чрезвычайной уязвимости их бизнес-процессов по отношению угрозам информационной безопасности (ИБ) [1]. Растущая сложность информационных систем только усугубляет ситуацию [2]. В современных условиях эффективность функционирования предприятий напрямую зависит от степени защищенности корпоративных информационных сетей (КИС), посредством которых осуществляется автоматизация бизнес-процессов, а защита информации должна рассматриваться как важнейший фактор, влияющий на функционирование КИС. Под КИС будем понимать составную часть корпоративных информационных систем, включающую в себя техническое, информационное и программное обеспечение [1].

Выделяются два основных подхода к обеспечению ИБ КИС [3]: на основе реализации базового уровня ИБ и на оценке и управлении рисками ИБ. Второй подход приобретает особую

значимость для современных КИС, так как позволяет строить эффективные системы защиты информации (СЗИ) с позиции потенциально возможного ущерба, а также исследовать экономические аспекты реализации защитных мероприятий [4]. Однако при этом актуализируется вопрос формирования корректных оценок факторов риска [5].

Степень разработанности темы и обсуждение решаемой задачи

Исследованиям в области оценки и управления рисками ИБ посвящены работы многих известных российских и зарубежных ученых [6–11]. Однако, несмотря на значительное количество проводимых исследований и опубликованных работ, в настоящее время существуют значительные сложности количественной оценки рисков ИБ в современных КИС.

К достоинствам методов количественной оценки рисков ИБ следует отнести хорошую интерпретируемость данных оценок в рамках экономических моделей, а также простоту применения математического аппарата для формирования оптимальной совокупности защитных мероприятий. Однако практическое применение данных методов часто осложняется следующими обстоятельствами [1, 12]:

- сложностью практического использования и необходимостью детального анализа всех процессов, происходящих в КИС;
- неточностью количественных оценок факторов риска ИБ, их зависимостью от глубины анализа КИС и квалификации эксперта;
- сложной природой оцениваемых объектов, недостаточностью и неопределенностью исходной информации;
- качественным (не количественным) характером факторов риска ИБ;
- отсутствием статистической информации по реализации ряда угроз ИБ.

Для анализа объектов и явлений в указанных условиях в настоящее время активно применяются методы экспертного оценивания и теории нечетких множеств. Исследованиям в этой области посвящено множество работ [13–17]. Вопросы применения данных методов для решения задач защиты информации, в том числе для количественной оценки рисков ИБ, исследовались такими учеными, как В. И. Васильев, М. Б. Гузаиров, И. В. Машкина, И. В. Котенко, И.Б. Паращук, И. М. Ажмухамедов и др. [10, 18–21].

Однако, несмотря на значительный объем исследований, в настоящее время отсутствует единый подход к решению задач количественной оценки и управления рисками ИБ, способный работать в условиях нечеткости, неполноты и качественного характера исходной информации, а также противоречивости экспертных оценок. Основными факторами, характеризующими риски информационной безопасности, являются ущерб от реализации угроз, возможность реализации угроз, возможность использования уязвимостей в КИС. В связи с этим необходима оценка данных факторов риска в указанных условиях, что требует разработки соответствующих методов и алгоритмов [22, 23].

Таким образом, научно-техническая проблема, решаемая в данной работе, заключается в создании теоретических основ количественной оценки и управления рисками информационной безопасности в условиях возможной нечеткости, противоречивости, неполноты и качественного характера исходной информации. Решение данной проблемы имеет научную и практическую ценность для построения эффективных систем защиты информации. Объект исследования: корпоративные информационные сети как объект защиты информации. Предмет исследования: модели, методы и алгоритмы нечеткой оценки и управления рисками информационной безопасности КИС. Цель – повышение эффективности защиты корпоративных информационных сетей на основе применения научно обоснованных методов, алгоритмов, технологических решений и инструментальных программных комплексов количественной оценки и управления рисками информационной безопасности в условиях возможной нечеткости, противоречивости, неполноты и качественного характера исходной информации.

Достижение поставленной цели потребовало решения следующих задач разработки:

1) *формальной модели КИС*, описывающей различные виды активов и особенности их взаимодействия для решения задачи количественной оценки рисков ИБ;

2) *метода и алгоритмов нечеткой оценки* ущерба от реализации угроз при отсутствии защитных мер на основе подходов к количественной оценке частных показателей ущерба, нечеткой оценке уровней критичности активов и формальной модели КИС;

3) *методов и алгоритмов нечетких оценок возможностей реализации угроз* и *использования уязвимостей* при отсутствии защитных мер в условиях неопределенности исходной информации;

4) *метода повышения эффективности защиты информации в КИС* на основе управления рисками ИБ, с учетом модели защитных мер, нечеткой оценки рисков ИБ;

5) *технологии количественной оценки и управления рисками ИБ* в КИС;

6) *инструментального комплекса программ* для нечеткой оценки и управления рисками информационной безопасности в КИС, реализующего разработанные технологию, методы и алгоритмы.

Для решения поставленных задач были использованы методы математического моделирования, системного анализа, теории нечетких множеств и нечеткой логики, теории графов, защиты информации, экспертного оценивания.

Основные вопросы и проблемы

Рассмотрим основные вопросы и проблемы, связанные с обеспечением ИБ в КИС, через оценку и управление рисками ИБ. Проведен сравнительный анализ основных подходов к решению задач оценки и управления рисками ИБ. Показано, что для формирования оценок факторов риска ИБ в условиях неопределенности, неполноты и качественности исходной информации об угрозах и уязвимостях целесообразно применять методы теории нечетких множеств [1]. Ставится задача разработки технологии количественной оценки и управления рисками ИБ, а также соответствующих методов, алгоритмов и инструментального комплекса программ.

Под *корпоративной информационной сетью* будем понимать составную часть корпоративных информационных систем, включающую в себя уровни технического (АРМ, серверы, телекоммуникационное оборудование), информационного (информационные ресурсы) и программного (ИТ-сервисы) обеспечения [1].

Под *риском ИБ* понимается возможный ущерб организации в результате реализации некоторой угрозы через уязвимость [24]. Выделяют два основных способа оценки рисков ИБ: двухфакторный (1) и трехфакторный (2):

$$R\,(T) = PossT(T) \times Impact(T), \tag{1}$$

$$R(V, T) = PossV(V) \times PossT(T) \times Impact(T), \tag{2}$$

где $PossV(V)$ – возможность использования уязвимости V, $PossT(T)$ – возможность реализации угрозы T, $Impact(T)$ – ущерб от реализации угрозы T.

На практике используют два основных подхода оценки рисков ИБ: качественной оценки и количественной оценки. Основной задачей первого подхода является экспресс-оценка рисков, нацеленная на быстрое определение актуальных угроз. При этом используются порядковые шкалы для оценки факторов риска, а также матрица для оценки уровней риска ИБ. Основной задачей второго подхода является детальный анализ процессов, происходящих в КИС, и формирование экономических оценок привлекательности проектов по защите информации на основе количественных оценок риска ИБ. При этом используются непрерывные числовые интервалы для оценки факторов риска ИБ с помощью аналитических либо экспертных методов.

Практическое применение методов количественной оценки рисков ИБ при построении экономически эффективных систем защиты информации является более предпочтительным. Однако при этом возникают ряд сложностей, связанных со следующими особенностями исходных данных:

- качественный (не количественный) характер многих частных показателей факторов риска ИБ;
- недостаточный объем или полное отсутствие статистической информации об отдельных угрозах и уязвимостях;
- отсутствие или нечеткость исходной информации;
- противоречивость оценок факторов риска, формируемых экспертами.

В связи с этим актуально решение научно-технической проблемы и задач, представленных в данной работе.

Моделирование КИС для задачи оценки рисков ИБ

При моделировании КИС для задачи оценки рисков ИБ особое внимание уделяется моделированию взаимодействия активов. Рассматриваются множество активов КИС, находящихся на уровнях технического, информационного и программного обеспечения. Разработана теоретико-множественная модель КИС, описывающая техническое и информационное взаимодействие разнотипных активов, подверженных угрозам ИБ [25–28].

Для моделирования КИС и ее компонентов предлагается использовать теоретико-множественный подход. Предлагаемая *модель КИС* представляет собой следующий набор элементов (3):

$$M_{КИС} = \{M_{ТО}, M_{ИО}, M_{ИТС}\}, \quad (3)$$

где $M_{ТО}$, $M_{ИО}$, $M_{ИТС}$ – модели технического обеспечения (ТО), использования информационного обеспечения (ИО) и ИТ-сервисов соответственно.

Модель ТО КИС определяется в виде кортежа (4):

$$M_{ТО} = \langle A_{ТО}, K_{АРМ}, K_{серв}, K_{ТК}, G_{ЛС} \rangle, \quad (4)$$

где $A_{ТО} = A_{АРМ} \cup A_{серв} \cup A_{ТК}$ – множество элементов ТО КИС, $A_{АРМ}$ – множество АРМ, $A_{серв}$ – множество серверов, $A_{ТК}$ – множество элементов ТО; $K_{АРМ} = \{(a^i_{АРМ}, \tilde{c}\tilde{c}^i_{АРМ}, \tilde{c}\tilde{i}^i_{АРМ})\}_{i=1}^{N_{АРМ}}$ – отношение, связывающее каждый АРМ $a^i_{АРМ} \in A_{АРМ}$ с нечеткими уровнями $\tilde{c}\tilde{c}^i_{АРМ}$, $\tilde{c}\tilde{i}^i_{АРМ}$ его конфиденциальности и целостности соответственно, $N_{АРМ}$ – количество АРМ; $K_{серв} = \{(a^i_{серв}, \tilde{c}\tilde{c}^i_{серв}, \tilde{c}\tilde{i}^i_{серв}, \tilde{c}\tilde{d}^i_{серв})\}_{i=1}^{N_{серв}}$ – отношение, связывающее каждый сервер $a^i_{серв} \in A_{серв}$ с нечеткими уровнями $\tilde{c}\tilde{c}^i_{серв}$, $\tilde{c}\tilde{i}^i_{серв}$, $\tilde{c}\tilde{d}^i_{серв}$ его конфиденциальности, целостности и доступности соответственно, $N_{серв}$ – количество серверов; $K_{ТК} = \{(a^i_{ТК}, \tilde{c}\tilde{d}^i_{ТК})\}_{i=1}^{N_{ТК}}$ – отношение, связывающее каждый элемент ТО $a^i_{ТК} \in A_{ТК}$ с нечетким уровнем $\tilde{c}\tilde{d}^i_{ТК}$ его доступности, $N_{ТК}$ – количество таких элементов; $G_{ЛС} = \langle V, E \rangle$ – формализация логической структуры ТО КИС в виде графа, где множество вершин соответствует сегментам КИС и ТО, ребра – каналам связи.

Модель использования ИО КИС определяется в виде кортежа (5):

$$M_{ИО} = \left\langle A_{инф}, K_{И}, A_{АС}, A'_{ИТС}, R^{АС}_{инф}, R^{инф}_{ИТС}, IP \right\rangle, \quad (5)$$

где $K_{И} = \{(a^i_{инф}, \tilde{c}\tilde{c}^i_{инф}, \tilde{c}\tilde{i}^i_{инф}, \tilde{c}\tilde{d}^i_{инф})\}_{i=1}^{N_{инф}}$ – отношение, связывающее каждый информационный актив $a^i_{инф} \in A_{инф}$ с нечеткими уровнями $\tilde{c}\tilde{c}^i_{инф}$, $\tilde{c}\tilde{i}^i_{инф}$, $\tilde{c}\tilde{d}^i_{инф}$ его конфиденциальности, целостности и доступности соответственно; $A_{АС} \subseteq A_{АРМ} \cup A_{серв}$ – множество активов ТО, хранящих или обрабатывающих информационные активы; $A'_{ИТС} \subseteq A_{ИТС}$ – множество ИТ-сервисов, участвующих в предоставлении информации; $R^{АС}_{инф}: A_{инф} \times A_{АС} \to \{0,1\}$ – отношение, определяющее факт хранения/обработки информации на АРМ или сервере; $R^{инф}_{ИТС}: A'_{ИТС} \times A_{инф} \to \{0,1\}$ – отно-

шение, определяющее факт предоставления информации посредством конкретного ИТ-сервиса; $IP = \left\{a^i_{инф}, a^i_{ИТС}, \{Path^i_j\}^h_{j=1}\right\}^{N_{IP}}_{i=1}$ – информационные потоки в КИС, определенные на графе $G_{ЛС}$, $a^i_{инф} \in A_{инф}$ – информационный актив; $a^i_{И\rightarrow ТС} \in A'_{ИТС}$ – ИТ-сервис КИС, предоставляющий на выходе потребителям информационный актив $a^i_{инф}$; $Path^i_j$ – маршрут в графе $G_{ЛС}$, отражающий движение информации в логической структуре КИС.

Модель использования ИТ-сервисов КИС определяется в следующем виде:

$$M_{ИТС} = \langle A_{ИТС}, K_{ИТС}, G_{ИТС}, R^{AO}_{ИТС}\rangle, \quad (6)$$

где $K_{ИТС} = \{(a^i_{ИТС}, \tilde{c}\tilde{d}^i_{ИТС})\}^{N_{ИТС}}_{i=1}$ – отношение, связывающее каждый ИТ-сервис $a^i_{ИТС} \in A_{ИТС}$ с нечетким уровнем $\tilde{c}\tilde{d}^i_{ИТС}$ его доступности, $N_{ИТС}$ – множество рассматриваемых ИТ-сервисов; $G_{ИТС} = \langle A_{ИТС}, E_{ИТС}\rangle$ – ориентированный граф – совокупность деревьев зависимостей ИТ-сервисов с точки зрения доступности; $R^{AO}_{ИТС}$: $A_{ИТС} \times A_{ТО} \rightarrow \{0,1\}$ – отношение, определяющее факт реализации ИТ-сервиса на базе конкретного элемента ТО.

Разработка метода и алгоритмов для нечеткой количественной оценки ущерба от реализации угроз

Рассмотрим задачу разработки метода и алгоритмов для нечеткой количественной оценки ущерба от реализации угроз при отсутствии защитных мер на основе подходов к количественной оценке частных показателей ущерба, нечеткой оценке уровней критичности активов и формальной модели КИС. Предложен состав частных показателей ущерба от реализации угроз. Для их оценки предложено использовать методы теории нечетких множеств и метод анализа иерархий (МАИ). Разработаны методы и алгоритмы оценки уровней критичности по конфиденциальности (К), целостности (Ц) и доступности (Д) активов КИС, основанные на количественной оценке частных показателей ущерба и формирования функций принадлежности на основе экспертных оценок [29–31].

Ущерб от реализации угроз ИБ определяется с помощью модели угроз, представленной в виде трехдольного графа $G_{угр}$=$A_{уязв} \times A_{угр} \times A_{акт}$, где $A_{уязв}$ – множество уязвимостей, $A_{угр}$ – множество угроз ИБ, $A_{акт}$ – множество активов КИС. Ущерб от реализации угрозы напрямую связан с критичностью активов, затрагиваемых ее реализацией. В связи с этим определение уровней критичности активов является одной из важнейших задач, требующих решения.

При оценке уровней критичности активов КИС учитываются особенности их взаимодействия, в соответствии с которыми выполняются следующие шаги:

1) оценка уровней критичности информационных активов по КЦД;

2) оценка уровней критичности неинформационных активов в следующей последовательности: Оценка уровней критичности АРМ (КЦ) $\rightarrow$ Оценка уровня критичности ИТ-сервисов (Д) $\rightarrow$ Оценка уровней критичности серверов (КЦД) $\rightarrow$ Оценка уровня критичности телекоммуникационного оборудования (Д).

Разработан метод оценки уровней критичности информационных активов (**метод 1)**, использующий технологию сбора экспертных мнений в группе, МАИ, методы теории нечетких множеств, включающий в себя следующие этапы:

1) составление перечня информационных активов на основе анализа бизнес-процессов;

2) определение множества частных показателей, влияющих на ущерб от реализации угроз;

3) количественная оценка уровней критичности информационных активов.

Для реализации Этапа 2 предложено множество из 29 частных показателей $\{\gamma_1, \ldots, \gamma_{29}\}$, характеризующих различные виды ущерба от реализации угроз. Данные частные показатели используются на Этапе 3 при оценке уровней критичности активов. Для формирования данных оценок в количественном виде при наличии частных показателей, имеющих качествен-

ный (не количественный) характер, был использован МАИ. Привлечение нескольких экспертов для оценки активов приводит к появлению множества экспертных оценок, которые преобразуются в функцию принадлежности (ФП) нечеткого числа, определяющего уровень критичности актива.

Для нечеткой оценки уровня каждого вида критичности информационных активов предложен обобщенный **алгоритм 1:**

1. Формируется экспертная группа, включающая в себя *N* экспертов.

2. Каждому *k*-му эксперту в сформированной группе назначается вес δ_k.

3. Для исследуемого вида критичности активов (К/Ц/Д) формируется дерево декомпозиции ущерба (4-уровневая иерархия), на верхнем уровне которого размещается исследуемый вид ущерба, на втором уровне – группы частных показателей ущерба, на третьем – частные показатели ущерба, на нижнем уровне – исследуемые активы $a^1, \ldots, a^{N_a}$, где N_a – количество исследуемых активов.

4. Для построенного дерева декомпозиции ущерба применяется МАИ. При этом для каждого из экспертов с номером k вычисляются количественные оценки $\left(w_i^C\right)_k, i = 1, N_a$, $\sum_{i=1}^{N_a}\left(w_i^C\right)_k = 1$ приоритетов исследуемых активов a^i по исследуемому виду критичности *C*.

5. Формируется нечеткий приоритет $\widetilde{w}_i^C$ актива a^i на основе экспертных данных $\left(w_i^C\right)_k$, $k = \overline{1, N}$. Функция принадлежности нечеткого приоритета $\widetilde{w}_i^C$ формируется с помощью предложенного алгоритма *FZ_STAT*, основанного на поиске треугольного нечеткого числа, наиболее точно аппроксимирующего полученные экспертные данные, с учетом веса эксперта. Для подбора параметров треугольного нечеткого числа использовался многопараметрический метод градиентного спуска.

6. Выбирается актив a^*, для которого экспертным путем оценивается уровень критичности $\tilde{I}^C(a^*)$ в условных единицах (например, в рублях) в виде нечеткого треугольного числа.

7. В соответствии со сформированными нечеткими приоритетами $\widetilde{w}_i^C$ вычисляется уровень критичности $\tilde{I}^C\left(a^i\right)$ в условных единицах остальных активов a^i относительно a^* по исследуемому виду критичности C. Для активов, не включенных в дерево декомпозиции конкретного ущерба, уровень критичности равен нулю.

На основе **алгоритма 1** разработаны алгоритм оценки уровней критичности КЦД информационных активов (**алгоритм 2**), а также метод оценки уровней критичности неинформационных активов КИС в виде нечетких чисел (**метод 2**), включающий в себя последовательную реализацию следующих алгоритмов:

- **алгоритм 3** оценки уровней критичности КЦ АРМ (при этом оценки конфиденциальности и целостности определяются путем суммирования соответствующих оценок критичностей информационных активов, хранимых и обрабатываемых на АРМ);
- **алгоритм 4** оценки уровня критичности (по доступности) ИТ-сервиса (при этом выбирается максимальная из следующих оценок: уровня доступности, сформированного путем анализа дерева ущерба и МАИ с помощью **алгоритма 1**, суммы оценок уровней критичностей (по доступности) информационных активов, предоставляемых ИТ-сервисом, уровня критичности ИТ-сервиса, сформированного на основе анализа дерева зависимостей ИТ-сервисов $G_{ИТС}$);
- **алгоритм 5** оценки уровней критичности КЦД сервера (при этом оценки конфиденциальности и целостности сервера определяются путем суммирования соответствующих оценок уровней критичности информационных активов, хранимых и обрабатываемых на сервере; оценка уровня доступности сервера определяется путем суммирования уровней доступности реализуемых на базе него ИТ-сервисов);

• **алгоритм 6** оценки уровня критичности (по доступности) телекоммуникационного оборудования определяется путем суммирования уровней доступности ИТ-сервисов, реализуемых на базе данного оборудования или использующих его в качестве посредника при передаче информации.

На основании полученных уровней критичностей активов КИС, используя модель угроз КИС в виде трехдольного графа $G_{угр}$, разработан метод нечеткой количественной оценки ущерба от реализации угрозы T_i (**метод 3**), включающий в себя следующие шаги:

Шаг 1. На модели угроз $G_{угр}$ определяются множества активов КИС $A^C(T_i)$, $A^I(T_i)$, $A^D(T_i)$, для которых угроза T_i нарушает конфиденциальность, целостность или доступность соответственно. Определяется множество всех активов $A(T_i) = \{a^j\}_{j=1}^{N_i}$ КИС, затрагиваемых реализацией угрозы T_i, $A(T_i) = A^C(T_i) \cup A^I(T_i) \cup A^D(T_i)$.

Шаг 2. С помощью **метода 1** осуществляется нечеткая оценка уровней критичности информационных активов.

Шаг 3. С помощью **метода 2** осуществляется нечеткая оценка уровней критичности неинформационных активов.

Шаг 4. Для каждого из активов $a^j \in A^C(T_i)$, $a^j \in A^I(T_i)$, $a^j \in A^D(T_i)$ экспертным путем определяются показатели в виде нечетких чисел $\tilde{pc}^j(T_i)$, $\tilde{pi}^j(T_i)$, $\tilde{pd}^j(T_i)$ – проценты нарушения конфиденциальности, целостности и доступности соответственно при реализации угрозы T_i.

Шаг 5. Производится нечеткая оценка суммарных ущербов, наносимых угрозой T_i по каждой из категорий.

$$\tilde{cc}(T_i) = \sum_{a^j \in A^C(T_i)} \tilde{pc}^j(T_i) \cdot \tilde{cc}_{a^j},$$
$$\tilde{ci}(T_i) = \sum_{a^j \in A^I(T_i)} \tilde{pi}^j(T_i) \cdot \tilde{ci}_{a^j},$$
$$\tilde{cd}(T_i) = \sum_{a^j \in A^D(T_i)} \tilde{pd}^j(T_i) \cdot \tilde{cd}_{a^j},$$

где $\tilde{cc}(T_i)$, $\tilde{ci}(T_i)$, $\tilde{cd}(T_i)$ – нечеткие количественные оценки ущерба, наносимого угрозой T_i по конфиденциальности, целостности и доступности соответственно.

Шаг 6. Нечеткая оценка ущерба, связанная с реализацией угрозы T_i, определяется в виде нечеткого числа: $Impact(T_i) = \tilde{cc}(T_i) + \tilde{ci}(T_i) + \tilde{cd}(T_i)$.

Методы нечетких количественных оценок возможности реализации угроз

Рассмотрим методы нечетких количественных оценок возможности реализации угроз и использования уязвимостей при отсутствии защитных мер в условиях неопределенности исходной информации, нечеткого и качественного характера частных показателей. Для количественной оценки частных показателей используется МАИ. Для учета неопределенности исходной информации и нечеткого характера частных показателей используются методы теории нечетких множеств. Предлагаются нечетко-продукционная модель представления знаний и схема нечеткого логического вывода, позволяющая оценивать уязвимости на основе нечетких оценок частных показателей с учетом их важности и в условиях отсутствия части информации [23]. Разработан метод количественной экспресс-оценки и ранжирования уязвимостей, а также нечеткой оценки возможности использования уязвимостей на основе нечетко-продукционной модели [32].

Получение количественных оценок для возможности реализации угроз на практике часто осложняется отсутствием статистических данных по реализации ряда угроз, зависимостью факторов, влияющих на возможность их реализации, личностными свойствами нарушителя,

качественным характером влияющих факторов. Для нечеткой количественной оценки возможности реализации угрозы $T_i \in T$ в указанных условиях предлагается **метод 4**, включающий два этапа.

Этап 1. Определение экспертным путем множества частных показателей $\{\alpha_1(T_i), \ldots, \alpha_{p_i}(T_i)\}$, влияющих на возможность реализации угрозы T_i,

Этап 2. Нечеткая оценка возможности реализации угрозы T_i на основе количественной оценки частных показателей.

Данную оценку предлагается выполнять с помощью опросных листов, включающих перечень вопросов с несколькими вариантами ответов. Каждому из ответов соответствует определенное количество баллов. Возможность реализации угрозы определяется общим количеством баллов после ответа экспертом на все вопросы. Рассмотрим формализацию постановки и решения данной задачи.

Дано:

$\alpha_j(T_i), j = 1,..,p_i$ – частные показатели возможности реализации угрозы T_i;

$Q_j(T_i)$ – вопрос опросного листа для оценки соответствующего частного показателя $\alpha_j(T_i)$;

$Answer_{jk}(T_i),\ k = \overline{1, k_j(T_i)}$ – возможные ответы на вопрос $Q_j(T_i)$, где $k_j(T_i)$ – количество возможных ответов;

$s_1 \in [1, k_1(T_i)]$, $s_2 \in [1, k_2(T_i)]$, …, $s_{p_i} \in \left[1, k_{p_i}(T_i)\right]$ – выбранные экспертом варианты ответов на каждый из вопросов.

Требуется определить:

$\overline{point}_{jk}(T_i)$ – количество баллов в виде нечеткого числа, соответствующее выбору ответа $Answer_{jk}(T_i)$;

$\overline{POINT}_j(T_i) = \sum_{k=1}^{k_j(T_i)} \overline{point}_{jk}(T_i)$ – количество баллов в виде нечеткого числа, отводимое на каждый из вопросов $Q_j(T_i)$;

$\tilde{P}_i = \sum_{j=1}^{p_i} \overline{point}_{js_j}(T_i)$ – общее количество баллов в виде нечеткого числа, набранных экспертом по результатам ответа на все вопросы $Q_j(T_i), j = 1,..,p_i$ теста.

Решение:

Для поиска значений $\overline{POINT}_j(T_i)$ и $\overline{point}_{jk}(T_i)$ применяется МАИ, в рамках которого сформирована 3-уровневая иерархия, на верхнем уровне которой располагается цель – возможность реализации угрозы, на втором – частные показатели $\alpha_j(T_i)$, соответствующие вопросам теста $Q_j(T_i)$, на нижнем уровне – ответы $Answer_{jk}(T_i)$.

Предложен алгоритм нечеткой оценки возможности реализации угроз (**алгоритм 7**), состоящий из следующих шагов:

1. Формируется экспертная группа, включающая в себя *N* экспертов. Каждому *k*-му эксперту в сформированной группе назначается вес δ_k.

2. Определяются приоритеты важности для вопросов. С помощью МАИ формируется вектор приоритетов $\left(wq^i\right)_z = \left(wq_1^i, \ldots, wq_{p_i}^i\right)_z$ вопросов $Q_j(T_i)$, где $z = \overline{1, N}$ – номер эксперта.

3. Формируются нечеткие приоритеты важности для вопросов $\tilde{w}\tilde{q}_j^i$ с помощью **алгоритма *FZ_STAT*** на основе оценок $\left\{\left(wq_j^i\right)_z\right\}$, полученных от *N* экспертов с учетом их веса δ_z.

4. Определяется количество баллов $\overline{POINT}_j(T_i)$ в виде нечеткого числа, отводимое на каждый из вопросов $Q_j(T_i)$. $\overline{POINT}_j(T_i) = P^i \bullet \tilde{w}\tilde{q}_j^i$, где P^i – максимальное количество баллов, отводимое на весь тест, $\bullet$ – операция умножения нечеткого числа на скаляр.

5. Оцениваются с помощью МАИ приоритеты важности $\left(wa_j^i\right)_z = \left(wa_{j1}^i, \ldots, wa_{jk_j(T_i)}^i\right)_z$ для ответов $Answer_{jk}(T_i)$ внутри вопросов, где $z = \overline{1, N}$ – номер эксперта.

6. Определяются приоритеты важности для ответов внутри вопросов $\widetilde{w}\tilde{a}_{jk}^{i}$ в виде нечетких чисел с помощью **алгоритма *FZ_STAT*** на основе оценок $\left\{\left(wa_{jk}^{i}\right)_{z}\right\}$, полученных от N экспертов с учетом их веса δ_z.

7. Определяются абсолютные значения баллов $\left|\overline{point}_{jk}(T_i)\right|$ в виде нечетких чисел, набираемых при выборе экспертом ответа $Answer_{jk}(T_i)$ на вопрос $Q_j(T_i)$. Количество баллов

$$\left|\overline{point}_{jk}\left(T_i\right)\right| = \overline{POINT}_j\left(T_i\right) \bullet \widetilde{w}\widetilde{a}_{jk}^{i},$$

где $\bullet$ – операция умножения нечетких чисел, реализуемая на базе принципа обобщения.

8. Определяются экспертным путем положительные (приводящие к увеличению) и отрицательные (приводящие к уменьшению возможности реализации угрозы T_i) значения баллов $\overline{point}_{jk}\left(T_i\right)$. Отрицательные значения баллов вычисляются как нечеткие числа, противоположные их абсолютным значениям.

9. Эксперт формирует варианты ответов s_j на каждый из вопросов $Q_j(T_i)$, $j = \overline{1, p_j}$.

10. Нормируется общее количество баллов $\tilde{P}_i = \sum_{j=1}^{p_i} \overline{point}_{js_j}$, набранное за ответы на вопросы теста, следующим образом:

$$\psi\left(\tilde{P}_i\right) = \frac{\left(\tilde{P}_i - P_i^{min}()\right)}{\left(P_i^{max_i^{min}}\right)},$$

где $Pmin_S\left(\sum_{j=\overline{1,p_i}}^{\Sigma} \tilde{P}_j^{min}()\right)_{min}$, $Pmax_S\left(\sum_{j=\overline{1,p_i}}^{\Sigma} \tilde{P}_j^{max}()\right)_{max}$, S – носитель нечеткого множества, нечеткие числа $\tilde{P}_j^{\min_{k=1,k_j(T_i)} \overline{point}_{jk}^{i}}$, $\tilde{P}_j^{\max_{k=1,k_j(T_i)} \overline{point}_{jk}^{i}}$ – минимальное и максимальное значения баллов соответственно при ответе на вопрос $Q_j(T_i)$.

11. Значение $\psi\left(\tilde{P}_i\right) = PossT(T_i)$ рассматривается в качестве нечеткой оценки возможности реализации угрозы T_i.

Мировым стандартом де-факто для оценки уязвимостей в настоящее время является метод CVSS V3, основанный на введении и оценке специализированных метрик уязвимостей. Однако данный метод обладает рядом недостатков.

1. Оценка метрик уязвимостей осуществляется в виде абстрактных количественных значений, которые жестко заданы. Метод не позволяет их изменить в случае, если эксперт не согласен с ними. У эксперта отсутствует возможность формирования нечетких оценок.

2. Отсутствует возможность отказа эксперта от оценки любой из базовых метрик уязвимостей, если у него отсутствует полная и достоверная информация.

3. Все метрики уязвимостей в данном методе являются равнозначными, в то время как они в различной степени влияют на результат реализации угроз через оцениваемые уязвимости.

Для устранения данных недостатков предложен метод оценки уязвимостей, основанный на базе знаний (7) и системе нечетко-продукционных правил (8)

$$KB = \left\{\left\{R^j\right\}_{j=1}^{s}, I\right\}, \tag{7}$$

где $\left\{R^j\right\}_{j=1}^{s}$ – множество нечетко-продукционных правил для нечеткой оценки уязвимостей со взвешенными параметрами $P_i^j \in P$, степенью универсальности правила, P – полное множество параметров (частных показателей уязвимостей, соответствующих метрикам CVSS v3), j – номер правила, I – схема нечеткого логического вывода с возможностью пропуска параметров правил и оценкой степени достоверности принятого решения.

R^j – нечеткое продукционное правило следующего вида:

$$\text{«ЕСЛИ } P_1^j \text{ есть} \tilde{A}_1^j(w_1^j) \text{ И … И } P_{s_j}^j \text{ есть} \tilde{A}_{s_j}^j(w_{s_j}^j) \text{ ТО Оценка уязвимости есть } \tilde{L}^j \text{» } [CF^j], \quad (8)$$

где $P^j = \{P_i^j\} \subset P, i = \overline{1, r_j}$ – множество частных показателей уязвимостей, заданных в виде лингвистических переменных (ЛП), на которые накладываются ограничения в условиях правила R^j; $A^j = \langle \tilde{A}_1^j, \ldots, A_{r_j}^j \rangle$ $A^j = \langle \widetilde{A}_1^j, \ldots, A_{r_j}^j \rangle$ – значения частных показателей уязвимостей (значения ЛП), определяющих нечеткие ограничения на параметры P_i^j; $w^j = \langle w_1^j, w_{r_j}^j \rangle$ – веса нечетких ограничений $\tilde{A}_i^j$ на параметры P_i^j в антецеденте правила R^j; $CF^j \in [0; 1]$ – степень уверенности эксперта в универсальности правила; $\tilde{L}^j$ – значение ЛП «Оценка уязвимости» при заданных значениях частных показателей в правиле R_j. Формализованы ЛП, соответствующие метрикам уязвимостей множества P, определенным в CVSS v3.

Для выполнения вывода на системе правил (8) разработана новая **схема нечеткого логического вывода**, формирующая оценку $RL(v)$ уязвимости v, а также оценку доли $D(v)$ использования информации при получении результата, на основании входных значений $\tilde{p}_i$ частных показателей $P_i \in P$, которые может оценить эксперт. Предложенная схема вывода включает следующие шаги.

Шаг 1. Реализуется нечеткий логический вывод на каждом правиле R^j.

1.1. Формируется ФП, определяющая результат вывода на правиле R^j согласно выражению $RL(R^j) = \min\limits_{z \in Z}(\mu_{\tilde{L}^j}(z), \hat{\eta}^j)$, где $\hat{\eta}^j = \frac{\sum_i \mu_t^j \cdot w_i^j}{\sum_t w_i^j}$ – степень срабатывания правила R^j, $\mu_i^j = \max\limits_U \left\{ min\left(\mu_{\tilde{A}_i^j}(u), \mu_{\tilde{p}_i}(u)\right)\right\}$, $\sum_t -$ сумма по индексам всех частных показателей множества P^j правила R^j, $\sum_i -$ сумма по индексам частных показателей множества P^j правила R^j с известными значениями.

1.2. Определяется доля использованной информации $D^j = \frac{\sum_i w_i^j}{\sum_t w_t^j}$ при получении результата $RL(R^j)$. Данное значение позволяет в дальнейшем судить о степени доверия к сформированному результату.

Шаг 2. Реализуется нечеткий логический вывод на множестве правил $\{R^j\}$.

$$RL(v) = Defuz\left(\bigcup_j RL(R^j)\right), \qquad D(v) = \frac{\sum_{Rj} D^j \cdot \hat{\eta}^j}{\sum_{Rj} \hat{\eta}^j},$$

где $RL(v)$ – оценка степени уязвимости v, *Defuz* – функция дефаззификации результата по методу центра тяжести, $D(v)$ – доля использования информации.

На основании схемы нечеткого логического вывода разработан метод количественной экспресс-оценки и ранжирования уязвимостей (**метод 5**), состоящий из следующих шагов.

Шаг 1. Строится модель базы знаний *KB* путем задания множества правил $\{R^j\}$ для оценки уязвимостей $v_1, \ldots, v_n$ в КИС, представленных в графе $G_{угр}$.

Шаг 2. Эксперт формирует нечеткие оценки $\tilde{p}_{i,1}, \ldots, \tilde{p}_{i,k_i}$ частных показателей $P_{i,1}, \ldots, P_{i,k_i}$ для уязвимости v_i, $i = \overline{1, n}$. Тогда для каждой уязвимости v_i вычисляются доли использования информации $D(v_1), \ldots, D(v_n)$, согласно **схеме нечеткого логического вывода.**

Шаг 3. Вычисляется оценка $RL(v_i)$ для каждой уязвимости v_i, $i = \overline{1, n}$. При этом возможны два случая.

Случай 1. Известны значения всех частных показателей для уязвимости v_i, то есть $D(v_i) = 1$. В этом случае оценка уязвимости вычисляется в виде четкого числа $RL(v_i) = Defuz\left(\bigcup_j RL(R^j)\right)$, согласно **схеме нечеткого логического вывода**.

Случай 2. Известны значения не всех частных показателей для уязвимости v_i. При этом возможно два варианта: вариант 2, *а* и вариант 2, *б*.

Вариант 2, *а*. Если $\alpha \le D(v_i) < 1$, где уровень α является пороговым уровнем неопределенности и определяется экспертом, то для оценки уязвимости v_i реализуется последовательность шагов 3.1–3.3 (рисунок 1 для случая одного неопределенного частного показателя).

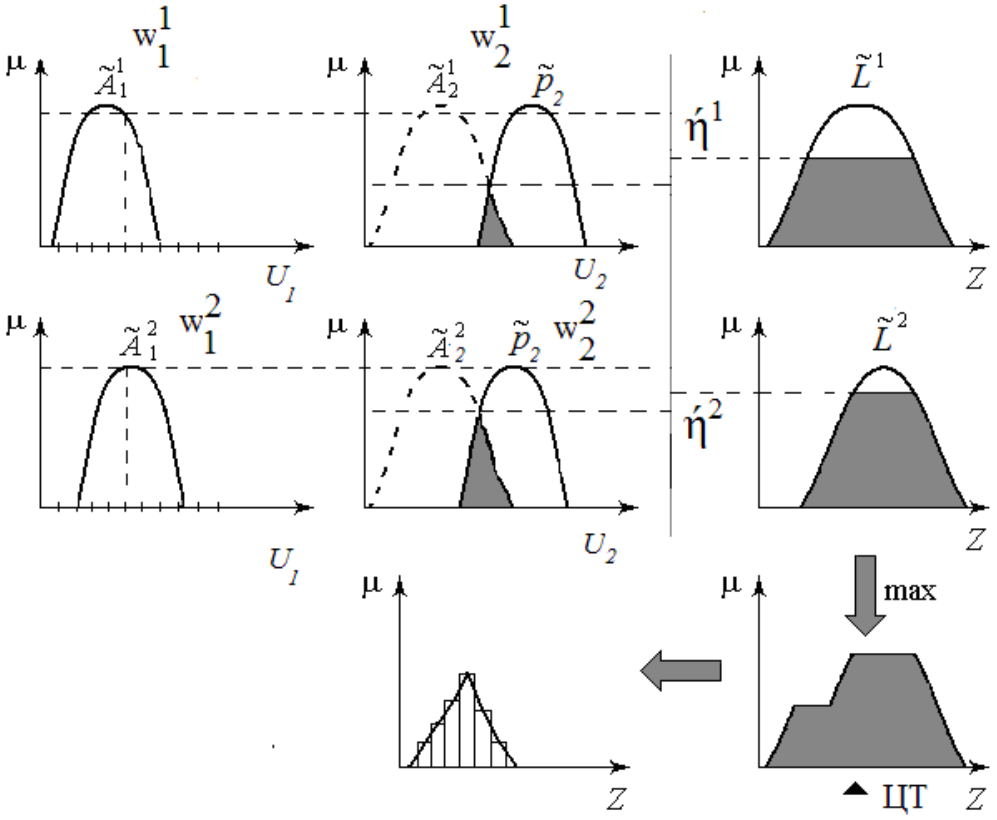

Рис. 1 Нечеткий логический вывод при неопределенном значении одного из частных показателей.

Пусть для уязвимости v_i не определено значение одного единственного частного показателя P_1 (также может быть получен обобщенный случай нескольких неопределенных частных показателей). Обозначим через U_1 универсальное множество, на котором задан P_1 с неопределенным значением. Тогда логический вывод будет осуществляться следующим образом.

Шаг 3.1. Пространство неопределенности U_1 равномерно разбивается на множество интервалов с одинаковым дискретным шагом точками $b_1, \ldots, b_S$.

Шаг 3.2. Вычисляются четкие значения оценок уязвимости $RL(v_i, b_j)$ в каждой из точек $b_1, \ldots, b_S$.

Шаг 3.3. Оценка уязвимости $\tilde{R}\tilde{L}(v_i)$ вычисляется в нечетком виде с помощью алгоритма *FZ_STAT* на основе распределения значений $RL(v_i, b_j)$, сформированных в пространстве неопределенности U_1 при $\delta_k = 1$.

Вариант 2, *б*. Если $D(v_i) < \alpha$, где уровень α определяется экспертным путем, то оценка уязвимости v_i не вычисляется в связи с отсутствием значительного количества информации о данной уязвимости.

Шаг 4. Ранжирование уязвимостей. Устанавливается отношение нестрогого порядка $\le$ между уязвимостями с оценками: $v_i \le v_j \Leftrightarrow R\tilde{L}(v_i) \le R\tilde{L}(v_j)$, где $\le$ – операция сравнения нечетких чисел, определяемая известным индексом ранжирования $H(\tilde{A}, \tilde{B}) = \sup_{a \ge b} min(\mu_{\tilde{A}}, \mu_{\tilde{B}})$.

Четкие оценки уязвимостей $RL(v_i)$ рассматриваются в качестве частного случая нечетких чисел с соответствующими ФП.

На базе **метода 5** разработан метод нечеткой оценки возможности использования уязвимостей (**метод 6**), включающий в себя следующие шаги:

1. Формируется модель базы знаний.

1.1. Рассматривается следующее множество частных показателей P для оценки возможности использования уязвимостей: P_1 = Способ получения доступа, P_2 = Сложность получения доступа, P_3 = Требуемые привилегии, P_4 = Необходимость взаимодействия с пользователем системы, P_{10} = Возможность использования, P_{11} = Уровень исправления, P_{12} = Уровень достоверности источника.

1.2. Экспертным путем формируется множество правил $\{R^j\}_{j=1}^{S}$ вида (8) на множестве параметров P для оценки возможности использования уязвимостей.

2. Пусть $v_1, \ldots, v_n$ – уязвимости в КИС, представленные в $G_{угр}$, через которые реализуется конкретная угроза T_i. Четкая $RL(v_i)$ или нечеткая $\tilde{R}\tilde{L}(v_i)$ оценка возможности использования уязвимости v_i определяется с помощью **метода 5** на сформированной базе знаний и принимается в качестве возможности $PossV(v_i)$ использования уязвимости v_i.

Полученные результаты позволили разработать следующий **метод нечеткой количественной оценки рисков ИБ** [33, 34].

1. С помощью метода нечеткой оценка ущерба для угрозы T_i (**метод 3**) определяется ущерб в виде нечеткого числа $Impact(T_i)$.

2. В случае двухфакторной оценки рисков применятся метод нечеткой оценки возможности реализации угрозы T_i (**метод 4**) и определяется возможность реализации в виде нечеткого числа $PossT(T_i)$. Далее оценка риска ИБ для угрозы T_i выполняется в виде нечеткого числа на основе принципа обобщения:

$$\boldsymbol{Risk(T_i) = Impact(T_i) \bullet PossT(T_i).}$$

3. В случае трехфакторной оценки применяется метод нечеткой оценки возможности реализации угрозы T_i (**метод 4**) и определяется возможность реализации в виде нечеткого числа $PossT(T_i)$. Далее применяется метод нечеткой оценки возможности использования уязвимости v_j (**метод 6**) и определяется возможность использования в виде нечеткого числа $PossV(v_j)$. Далее оценка риска ИБ для угрозы T_i, реализуемой через уязвимость v_j, выполняется в виде нечеткого числа на основе принципа обобщения следующим образом:

$$\boldsymbol{Risk(T_i, v_j) = Impact(T_i) \bullet PossT(T_i) \bullet PossV(v_j).}$$

Оценка риска ИБ для угрозы T_i выполняется следующим образом:

$$\boldsymbol{Risk(T_i) = Impact(T_i) \bullet PossT(T_i) \cdot\bullet \max_j PossV(v_j).}$$

Метод повышения защищенности КИС в условиях финансовых ограничений

Рассмотрим метод повышения защищенности КИС на основе управления рисками ИБ в условиях финансовых ограничений. Для этого разработаны модель защитных мер и метод нечеткой оценки рисков ИБ в условиях применения защитных мероприятий. Даны формальные постановки оптимизационных задач для управления рисками ИБ. Сформирована технология количественной оценки и управления рисками ИБ, способная работать в условиях неопределенности и неполноты информации об угрозах и уязвимостях, противоречивости оценок факторов риска, даваемых экспертами, нечеткого и качественного характера большинства частных показателей, влияющих на возможность реализации угроз, использования уязвимостей и определяющих ущерб.

Управление рисками ИБ предполагает реализацию непрерывного процесса последовательной оценки и дальнейшего снижения рисков ИБ в КИС в рамках допустимых затрат. Оценка рисков ИБ выполняется с помощью ранее разработанных методов и алгоритмов оценки ущерба, возможности реализации угроз, использования уязвимостей. Дальнейшее снижение рисков ИБ осуществляется путем построения модели защитных мер и решения оптимизационных задач по выбору наилучшей их группы в рамках допустимых затрат.

Разработан метод повышения защищенности КИС на основе управления рисками ИБ (**метод 7**) [1, 35, 36], включающий в себя три основных этапа.

Этап 1. Оценка рисков ИБ в денежном эквиваленте при условии реализации множества защитных мер.

Пусть $T = \{T_i\}$ – множество возможных угроз ИБ в КИС, определенных в графе $G_{угр}$. Предполагается, что угрозы действуют независимо друг от друга, и ущерб аддитивен, то есть $Risk = \sum_T Risk(T_i)$. Для учета при оценке рисков ИБ реализованных защитных мер предложена модель защитных мер КИС в виде кортежа (9)

$$M_{СЗИ} = \left\langle Z, R_{СЗИ}^{уязв}, R_{СЗИ}^{угр}, R_{СЗИ}^{ущерб\_C}, R_{СЗИ}^{ущерб\_I}, R_{СЗИ}^{ущерб\_D} \right\rangle, \quad (9)$$

где $Z = \{z_i\}_{i=1}^{n}$ – множество защитных мер, $R_{СЗИ}^{уязв}: \{Z \times A_{уязв}\} \to F([0,1])$, $R_{СЗИ}^{угр}: \{Z \times A_{угр}\} \to F([0,1])$ – нечеткие величины снижения возможности использования уязвимостей и реализации угроз соответственно при внедрении защитных мер, $F([0,1])$ – множество нечетких чисел, определенных на интервале [0,1], $R_{СЗИ}^{ущерб\_C}, R_{СЗИ}^{ущерб\_I}, R_{СЗИ}^{ущерб\_D}: \{Z \times A_{угр}\} \to F([0,1])$ – нечеткая величина снижения ущерба от реализации угроз при внедрении защитных мер.

На базе модели (9) разработан метод оценки риска ИБ с учетом множества реализованных защитных мер $z_i \in Z$ (**метод 8**), основанный на вычислении скорректированных уровней ущербов $Impact(T_i)_Z$, возможности реализации угроз $PossT(T_i)_Z$ и уязвимостей $PossV(v_j)_Z$ при условии реализации защитных мер.

Этап 2. Расчет экономической эффективности множеств защитных мер, предполагаемых к реализации. Оценка эффективности защитной меры $z_i \in Z$ определяется через уровень эффективности $K(z_i)$ следующим образом:

$$K(z_i) = \frac{Выгоды(z_i) - П\_Затраты(z_i)}{Е\_затраты(z_i)},$$

где $Выгоды(z_i) = \Delta R = Risk(T) - Risk(T)_{\{z_i\}}$ – выгоды от реализации защитной меры z_i в единицу времени (например, год), $Risk(T) = \sum_j Risk(T_j)$, $Risk(T)_{\{z_i\}} = \sum_j Risk(T_j)_{\{z_i\}}$ – нечеткие суммарные уровни риска в единицу времени по всем угрозам $T_j \in T$ без учета и с учетом реализации защитных мер соответственно, $Е\_затраты(z_i)$ – единовременные затраты на реализацию защитной меры z_i (оцениваются экспертом), $П\_Затраты(z_i)$ – дополнительные постоянные затраты на реализацию защитной меры z_i в единицу времени. Для оценки постоянных затрат предложен **метод 9**, основанный на МАИ.

Экономическая эффективность множества защитных мер Z' определяется в виде $K(Z') = \sum_{z_i \in Z'} K(z_i)$, а срок окупаемости инвестиций – в виде $1/K(Z')$.

Этап 3. Выбор оптимальной совокупности защитных мер.

Пусть $Z = \{z_i\}_{i=1,M}$ – множество всевозможных защитных мер, которые потенциально возможно использовать для защиты КИС. Поставим в соответствие каждому множеству $Z' \subseteq Z$ вектор $X = (x_1, \ldots, x_M)$ выбираемых для реализации защитных мер в КИС. Здесь x_i =1, если $z_i \in Z'$, то есть z_i выбрана для реализации, и x_i = 0, если $z_i \notin Z'$. Решаются следующие постановки оптимизационных задач на этапе выбора оптимальной совокупности защитных мер.

Постановка задачи № 1. Пусть $Risk^{пороговый}$ – пороговый уровень рисков, приемлемый для КИС.

Найти вектор $X = (x_1, \ldots, x_M)$, такой, что $\begin{cases} \overline{K}(x_1, \ldots, x_M) \to max, \\ \overline{Risk}(T, x_1, \ldots, x_M) \le Risk^{пороговый}, \\ x_i \in \{0,1\}. \end{cases}$

Здесь $\overline{K}(x_1, \ldots, x_M)$ – экономическая эффективность совокупности выбранных для реализации защитных мер, $\overline{Risk}(T, x_1, \ldots, x_M)$ – суммарный риск с учетом множества реализуемых защитных мер.

Постановка задачи № 2. Пусть Ω – максимальный срок окупаемости проекта, E – максимальные единовременные затраты на реализацию проекта по внедрению защитных мер множества Z', приемлемые для организации.

Найти вектор $X = (x_1, \ldots, x_M)$, такой, что $\begin{cases} \frac{1}{\overline{Risk}(T, x_1, \ldots, x_M)} \to max, \\ \frac{1}{\overline{K}(x_1, \ldots, x_M)} \le \Omega, \\ \overline{E_{Затраты}}(x_1, \ldots, x_M) \le E, \\ x_i \in \{0,1\}. \end{cases}$

Для решения поставленных оптимизационных задач разработан метод управления рисками ИБ в условиях финансовых ограничений (**метод 10**), основанный на генетическом алгоритме.

На основе полученных теоретических результатов была сформирована технология количественной оценки и управления рисками ИБ в КИС в условиях нечеткости и неполноты информации об угрозах и уязвимостях, возможной противоречивости оценок факторов риска, даваемых экспертами; нечеткого и качественного характера большинства частных показателей, определяющих ущерб, а также влияющих на возможность реализации угроз и использования уязвимостей (рисунок 2) [37]. Управление рисками ИБ в КИС рассматривается как непрерывный процесс (обратная связь на рисунке 2).

ИНСТРУМЕНТАЛЬНЫЙ КОМПЛЕКС ПРОГРАММ КОЛИЧЕСТВЕННОЙ ОЦЕНКИ И УПРАВЛЕНИЯ РИСКАМИ ИБ

Рассмотрим разработанный инструментальный комплекс программ количественной оценки и управления рисками ИБ в КИС. Рассматриваются примеры его использования для решения задач количественной оценки и управления рисками ИБ в различных КИС.

Представленные в предыдущих разделах модели, методы и алгоритмы реализованы в виде инструментального комплекса программ количественной оценки и управления рисками ИБ в КИС, структура которого в соответствии с решаемыми задачами представлена на рисунке 3.

Полученные результаты были внедрены в промышленную эксплуатацию в составе системы управления ИБ «Общероссийской системы электронной торговли zakazrf.ru» ГУП «Агентство по государственному заказу, инвестиционной деятельности и межрегиональным связям Республики Татарстан» для решения задачи оценки и управления рисками. Произведена оценка критичности активов КИС: 23 информационных актива, 3 типа АРМ, 6 серверов, 13 ИТ-сервисов. Проведен анализ 11 угроз ИБ, свойственных КИС. Результаты оценки рисков для угрозы УБИ.006 представлены в таблице 1. Конечные результаты оценки рисков для всех угроз представлены в таблице 2.

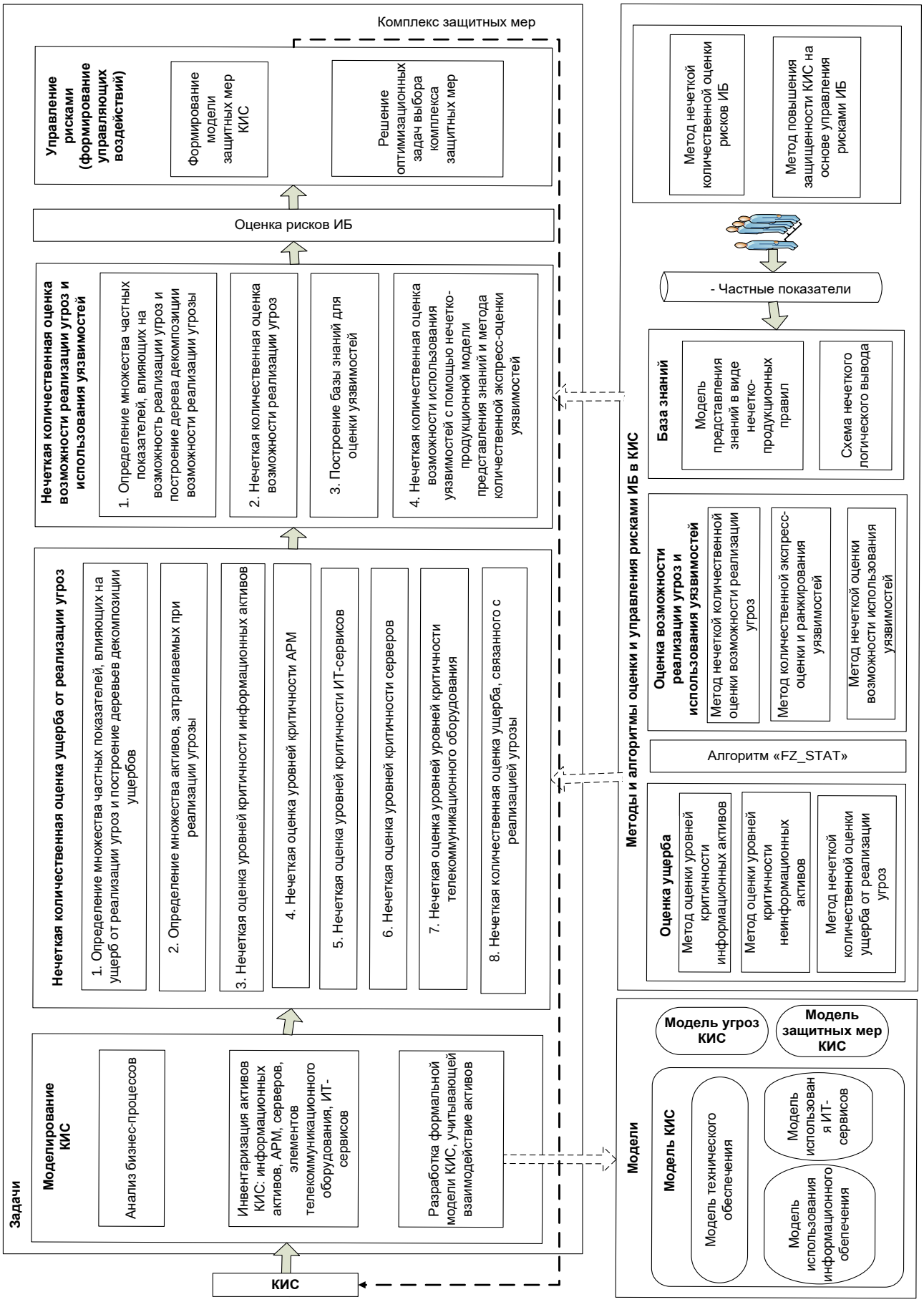

Рис. 2 Технология количественной оценки и управления рисками информационной безопасности.

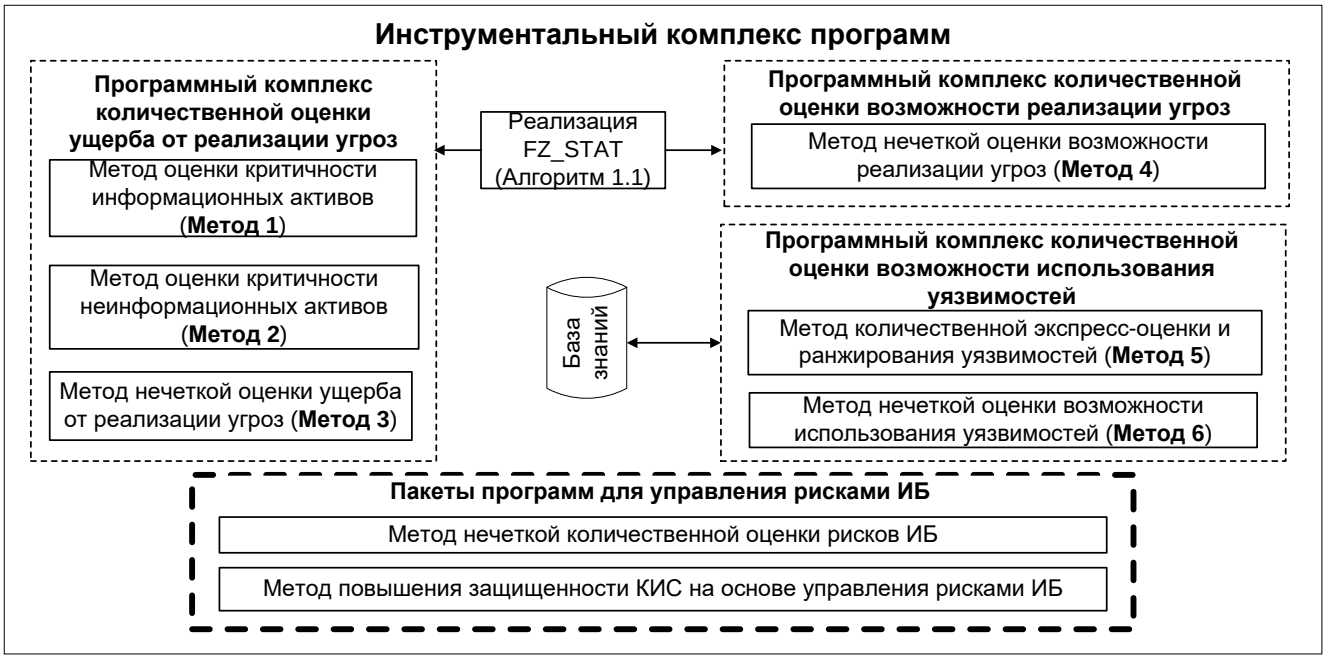

Рис. 3 Структура инструментального комплекса программ.

Таблица 1

Результаты оценки рисков для угрозы УБИ.006

Угроза	Актив	Ущерб, тыс. руб.	Возможность реализации	Риск, тыс. руб.
УБИ.006	АРМ Администраторов	(1538.7, 1540, 1540.7)	0.48	(738.6, 739.3, 739.6)
	Терминальный сервер teamRAY 2061L	(9375.9, 9821.9, 10364)	0.54	(5063, 5303.8, 5596.6)
	Сервер рабочей зоны поставщика	(2353.3, 2598.2, 2691.9)	0.54	(1270.8, 1403, 1453.7)
	Сервер WEB-зоны (рабочей зоны поставщика)	(2353.3, 2598.2, 2691.9)	0.54	(1270.8, 1403, 1453.6)

Таблица 2

Результаты оценки рисков для угроз информационной безопасности

Угроза	Риск, тыс. руб.
УБИ.006	(8343, 8849, 9243)
УБИ.008	(11294, 13467, 14961)
УБИ.018	(1000.2, 1001, 1001.5)
УБИ.067	(11750, 14075, 15638)
УБИ.091	(1935, 1978, 1999)
УБИ.116	(16517, 20073, 22576)
УБИ.128	(12545, 15245, 17146)
УБИ.140	(21099, 21565, 21769)
УБИ.157	(21366, 21838, 22044)
УБИ.167	(1230, 1232, 1232.6)
УБИ.179	(4630, 4733, 4778)

В качестве множества защитных мер для КИС ГУП «Агентство по государственному заказу, инвестиционной деятельности и межрегиональным связям Республики Татарстан» рассматривались: z_1 = “Комплекс СЗИ НСД”, z_2 = “Комплекс средств антивирусной защиты”, z_3 = “Комплекс встроенных СрЗИ сетевого оборудования”, z_4 = “Комплекс межсетевого экранирования”, z_5 = “Комплекс обнаружения и предотвращения вторжений”, z_6 = “Комплекс анализа защищенности”, z_7 = “Комплекс криптографической защиты”, z_8 = “Комплекс резервного копирования”, z_9 = “Комплекс средств анализа средств анализа и консолидации событий ИБ", z_{10} = “Комплекс защиты среды виртуализации".

Была проведена оценка остаточных рисков ИБ с учетом различных комбинаций реализованных защитных мер, расчет показателей экономической эффективности всех их комбинаций. Далее, на основании проведенных расчетов, были решены две задачи по выбору наилучшей совокупности защитных мер.

В результате решения оптимизационной задачи №1 при $Risk^{пороговый}$ = 6 млн руб. сформирована рекомендуемая группа защитных мер z_1 = ”Комплекс СЗИ НСД”, z_2 = ”Комплекс средств антивирусной защиты”, z_3 = ”Комплекс встроенных СрЗИ сетевого оборудования”, z_4 = ”Комплекс межсетевого экранирования”, z_6 = ”Комплекс анализа защищенности”, z_7 = ”Комплекс криптографической защиты”, z_{10} = ” Комплекс защиты среды виртуализации”. Данная группа мер обеспечивает остаточный уровень риска $\overline{Risk}(T, x_1, \ldots, x_{10})$ = 5734 тыс. руб., что составляет 4,7% от первоначального уровня.

В результате решения оптимизационной задачи № 2 при Ω = 1 год, E = 2 млн руб. сформирована рекомендуемая группа защитных мер z_1 = ”Комплекс СЗИ НСД”, z_2 = ”Комплекс средств антивирусной защиты”, z_3 = ”Комплекс встроенных СрЗИ сетевого оборудования”, z_4 = ”Комплекс межсетевого экранирования”, z_5 = ”Комплекс обнаружения и предотвращения вторжений”, z_6 = ”Комплекс анализа защищенности”, z_7 = ”Комплекс криптографической защиты”, z_{10} = ”Комплекс защиты среды виртуализации”. Данная группа мер обеспечивает остаточный уровень риска $\overline{Risk}(T, x_1, \ldots, x_{10})$ = 5655 тыс. руб., что составляет 4,6 % от первоначального уровня. Данный уровень риска на 79 тыс. руб. ниже остаточного уровня риска, достигаемого при реализации группы защитных мер, полученных при решении задачи № 1, однако это требует дополнительных единовременных затрат на реализацию в размере 970 тыс. руб., что видится необоснованным. Таким образом, следует склониться к реализации группы защитных мер, полученных при решении задачи № 1. Сравнение выбранных защитных мер с их полным составом, предполагаемым ранее к реализации (без учета уровней риска), позволяет утверждать, что применение разработанных технологий, методов и алгоритмов количественной оценки и управления рисками ИБ позволило сократить единовременные затраты на СЗИ КИС ГУП «Агентство по государственному заказу, инвестиционной деятельности и межрегиональным связям Республики Татарстан» на 2 млн 650 тыс. руб.

Результаты также были использованы для решения задач оценки уровней критичности активов и выбора эффективных защитных мер компанией АО «АйСиЭл – КПО ВС», а также использованы для количественной оценки и управления рисками, связанными с реализацией угроз ИБ на корпоративную информационную сеть ФГБОУ ВО «Казанский национальный исследовательский технический университет им. А. Н. Туполева – КАИ».

Заключение

1. Разработана теоретико-множественная модель КИС, *отличающаяся* наличием описания взаимодействия разнотипных активов КИС. Модель отражает логическую структуру КИС, информационные потоки в КИС, взаимозависимость ИТ-сервисов с точки зрения доступности, что *позволяет* выполнять детальный анализ информационных процессов КИС и использовать результаты данного анализа при оценке и управлении рисками ИБ.

2. Разработаны метод и алгоритмы нечеткой оценки ущерба от реализации угроз при отсутствии защитных мер, *отличающиеся* тем, что оценка уровней критичности активов и частных показателей ущерба выполняется в количественном виде с применением МАИ и методов теории нечетких множеств, что *позволяет* получить адекватные количественные оценки ущерба в условиях их качественного характера и в условиях противоречивости исходной информации.

3. Разработаны методы и алгоритмы нечетких оценок возможности реализации угроз и использования уязвимостей при отсутствии защитных мер и возможной неопределенности исходной информации, *отличающиеся* тем, что при оценке используются опросные листы и формальная модель базы знаний с новым видом нечетко-продукционных правил и новой схемой нечеткого логического вывода, что *позволяет* эксперту оперативно выполнять количественную оценку возможностей реализации угроз и использования уязвимостей в условиях нечеткости, неполноты и противоречивости части исходной информации, а также отсутствия статистических данных о реализации угроз и использования уязвимостей.

4. Разработан метод повышения эффективности защиты информации в КИС на основе модели защитных мер, решении оптимизационных задач выбора наилучшей группы защитных мероприятий, *отличающийся* учетом нечетких оценок рисков ИБ в КИС; введением нечетких величин снижения ущерба, возможностей реализации угроз и использования уязвимостей при реализации защитных мер; вычислением уровня эффективности в условиях нечеткости рисков и качественного характера частных показателей постоянных затрат, связанных с реализацией защитных мер, что *позволяет* оперативно выполнить оценку экономической эффективности различных вариантов СЗИ и сформировать наилучший комплекс защитных мер в условиях нечеткого и качественного характера исходной информации.

5. Разработана технология количественной оценки и управления рисками ИБ, *отличающаяся* используемым подходом к оценке рисков с применением теоретико-множественной модели КИС, базы знаний, методов и алгоритмов количественной оценки и управления рисками ИБ с применением методов теории нечетких множеств, что *позволяет* выполнять оценку и управление рисками ИБ в условиях нечеткости, неполноты информации об угрозах и уязвимостях, возможной противоречивости оценок факторов риска, даваемых экспертами; нечеткого и качественного характера частных показателей, определяющих ущерб, а также влияющих на возможность реализации угроз и использования уязвимостей.

6. Разработан инструментальный комплекс программ оценки и управления рисками информационной безопасности в КИС, реализующий разработанную технологию, методы и алгоритмы, позволяющий формировать оптимальный комплекс защитных мер в условиях нечеткости, неполноты, качественности и возможной противоречивости исходной информации. Комплекс программ был апробирован на примере решения задач по оценке и управлению рисками ИБ в КИС ГУП «Агентство по государственному заказу, инвестиционной деятельности и межрегиональным связям Республики Татарстан» с достижением остаточного риска 4,7% от максимального значения. Применение выбранной группы защитных мер позволило сократить единовременные затраты по сравнению с реализацией их полного состава на 2 млн 650 тыс. руб.

Таким образом, в работе решена научно-техническая проблема, заключающаяся в создании теоретических основ количественной оценки и управления рисками информационной безопасности в условиях возможной нечеткости, противоречивости, неполноты и качественного характера исходной информации. Решение данной проблемы имеет научную и практическую ценность для построения эффективных систем защиты информации.

СПИСОК ЛИТЕРАТУРЫ / REFERENCES

1. Аникин И. В. Методы оценки и управления рисками информационной безопасности в корпоративных информационных сетях. Казань: Школа, 2015. [[Anikin I. V. Methods for Assessing and Managing Information Security Risks in Corporate Information Networks. Kazan: School, 2015. (In Russian).]]

2. Fabarisov T., Siedel G., Vock S., Morozov A. “Aspects of industrial CPS critical for risk assessment methods” // Системная инженерия и информационные технологии. 2021. Т.3, № 3 (7). С. 23-29. [[In: System Engineering and Information Technologies. 2021. V. 3, No. 3 (7), pp. 23-29.]]

3. Аникин И. В., Глова В. И. К вопросу стандартизации в проблеме безопасности информационных технологий // Вестник КГТУ им. А. Н. Туполева. 2004. № 3. С. 68-63. [[Anikin I. V., Glova V. I. “On the issue of standardization in the problem of information technology security” // Bulletin of KSTU A. N. Tupolev. 2004. No. 3, pp. 68-63. (In Russian).]]

4. Аникин И. В. Метод управления рисками информационной безопасности в корпоративных информационных сетях // Инфокоммуникационные технологии. 2015. Т. 13. № 2. С. 215-221. [[Anikin I. V. “Information security risk management method in corporate information networks” // Info-communication Technologies. 2015. V. 13, No. 2, pp. 215-221. (In Russian).]]

5. Аникин И. В. Управление внутренними рисками информационной безопасности корпоративных информационных сетей // Научно-технические ведомости Санкт-Петербургского государственного политехнического университета. Информатика. Телекоммуникации. Управление. 2009. № 3 (80). С. 35-40. [[Anikin I. V. “Management of internal risks of information security of corporate information networks” // Scientific and Technical Statements of the St. Petersburg State Polytechnic University. Computer science. Telecommunications. Control. 2009. No. 3 (80), pp. 35-40. (In Russian).]]

6. Васильев В. И., Вульфин А. М., Кириллова А. Д. Анализ и управление рисками информационной безопасности АСУ ТП на основе когнитивного моделирования // Моделирование, оптимизация и информационные технологии. 2022. Т. 10. № 2 (37). С. 1-18. [[Vasiliev V. I., Vulfin A. M., Kirillova A. D. “Analysis and risk management of information security of process control systems based on cognitive modeling” // Modeling, Optimization, and Information Technologies. 2022. Vol. 10. No. 2 (37), pp. 1-18. (In Russian).]]

7. Гузаиров М. Б., Вульфин А. М., Картак В. М., Кириллова А. Д., Миронов К. В. Сравнительный анализ алгоритмов когнитивного моделирования при оценке рисков информационной безопасности // Труды Института системного анализа Российской академии наук. 2019. Т. 69. № 4. С. 62-69. [[Guzairov M. B., Vulfin A. M., Kartak V. M., Kirillova A. D., Mironov K. V. “Comparative analysis of cognitive modeling algorithms in assessing information security risks” // In: Proceedings of the Institute of System Analysis of the Russian Academy of Sciences. 2019. V. 69. No. 4, pp. 62-69. (In Russian).]]

8. Тулиганова Л. Р., Машкина И. В. Численная оценка риска нарушения информационной безопасности в сегменте виртуализации информационной системы предприятия // Безопасность информационных технологий. 2015. Т. 22. № 1. С. 113-114. [[Tuligova L. R., Mashkina I. V. “Numerical assessment of the risk of information security violations in the segment of enterprise information system virtualization” // Security of Information Technologies. 2015. V. 22. No. 1, pp. 113-114. (In Russian).]]

9. Львович Я. Е., Преображенский А. П., Преображенский Ю. П., Чопоров О. Н. Анализ подходов для оценки рисков в ходе внедрения корпоративных информационных систем в организациях // Вестник Воронежского института высоких технологий. 2019. № 4 (31). С. 56-58. [[Lvovich Ya. E., Preobrazhensky A. P., Preobrazhensky Yu. P., Choporov O. N. “Analysis of approaches for assessing risks during the implementation of corporate information systems in organizations” // Bulletin of the Voronezh Institute of High Technologies. 2019. No. 4 (31), pp. 56-58. (In Russian).]]

10. Ажмухамедов И. М., Выборнова О. Н., Брумштейн Ю. М. Управление рисками информационной безопасности в условиях неопределенности // Проблемы информационной безопасности. Компьютерные системы. 2016. № 1. С. 7-14. [[Azhmukhamedov I. M., Vybornova O. N., Brumshtein Yu. M. “Information security risk management in conditions of uncertainty” // Problems of Information Security. Computer Systems. 2016. No. 1, pp. 7-14. (In Russian).]]

11. Баранова Е. К., Мурзакова А. А., Мурзакова Е. А. Сравнительный анализ программного обеспечения для анализа рисков информационной безопасности в соответствии с ГОСТ Р ИСО/МЭК 27005-10 // Информационные технологии и вычислительные системы. 2019. № 2. С. 75-83. [[Baranova E. K., Murzakova A. A., Murzakova E. A. “Comparative analysis of software for risk analysis of information security in accordance with GOST R ISO/IEC 27005-10” // Information Technologies and Computing Systems. 2019. No. 2, pp. 75-83. (In Russian).]]

12. Аникин И. В., Гильмуллин Т. М. Моделирование объектов информационной безопасности для задачи оценки рисков // Научно-технические ведомости Санкт-Петербургского государственного политехнического университета. Информатика. Телекоммуникации. Управление. 2009. Т. 5. № 86. С. 151-155. [[Anikin I. V., Gilmullin T. M. “Modeling of information security objects for the problem of risk assessment” // Scientific and Technical Statements of the St. Petersburg State Polytechnic University. Computer science. Telecommunications. Control. 2009. V. 5, No. 86, pp. 151-155. (In Russian).]]

13. Аникин И. В., Зиновьев И. П. Усовершенствование системы нечеткого вывода Такаги–Сугено // Вестник КГТУ им. А. Н. Туполева. 2009. № 3. С. 84–88. [[Anikin I. V., Zinoviev I. P. “Improvement of the Takagi–Sugeno fuzzy inference system” // Bulletin of KSTU A. N. Tupolev. 2009. No. 3, pp. 84-88. (In Russian).]]

14. Аникин И. В., Зиновьев И. П. Модель логического вывода на основе нечеткой линейной регрессии // Научно-технические ведомости Санкт-Петербургского государственного политехнического университета. Информатика. Телекоммуникации. Управление. 2010. № 5. С. 139-145. [[Anikin I. V., Zinoviev I. P. “An inference model based on fuzzy linear regression” // Scientific and Technical Bulletin of the St. Petersburg State Polytechnic University. Computer science. Telecommunications. Control. 2010. No. 5, pp. 139-145. (In Russian).]]

15. Anikin I. V., Alnajjar K. “Pseudo-random number generator based on fuzzy logic” // In: 2016 International Siberian Conference on Control and Communications, SIBCON 2016. Proceedings.2016, pp. 1-4, doi: 10.1109/SIBCON.2016.7491667.

16. Anikin I. V., Zinoviev I. P. “Fuzzy control based on new type of Takagi-Sugeno fuzzy inference system” // In: 2015 International Siberian Conference on Control and Communications, SIBCON 2015. Proceedings. 2015, doi: 10.1109/SIBCON.2015.7146977.

17. Anikin I., Zinoviev I. “New type of Takagi-Sugeno fuzzy inference system as universal approximator” // Applied Mechanics and Materials. 2014. V. 598, pp. 453-458.

18. Васильев В. И., Вульфин А. М., Гузаиров М. Б., Картак В. М., Черняховская Л. Р. Оценка рисков кибербезопасности АСУ ТП промышленных объектов на основе вложенных нечетких когнитивных карт // Информационные технологии. 2020. Т. 26. № 4. С. 213-221. [[Vasiliev V. I., Vulfin A. M., Guzairov M. B., Kartak V. M., Chernyakhovskaya L. R. “Assessing cybersecurity risks for automated process control systems for industrial facilities based on nested fuzzy cognitive maps” // Information Technologies. 2020. V. 26. No. 4, pp. 213-221. (In Russian).]]

19. Машкина И. В., Сенцова А. Ю., Степанова Е. С. Разработка нечетких когнитивных карт и искусственной нейронной сети для оперативной оценки информационных рисков в системе облачных вычислений // Нейрокомпьютеры: разработка, применение. 2013. № 3. С. 026-030. [[Mashkina I. V., Sentsova A. Yu., Stepanova E. S. “Development of fuzzy cognitive maps and an artificial neural network for the operational assessment of information risks in a cloud computing system” // Neurocomputers: Development, Application. 2013. No. 3, pp. 026-030. (In Russian).]]

20. Kotenko I. V., Parashchuk I. B. “Evaluation of information security of industrial automation systems using fuzzy algorithms and predicates” // International Russian Automation Conference (RusAutoCon), Sochi, Russia (5-11 Sept. 2021). IEEE Xplore Digital Library: Browse Conferences, 2021. V. (Doc.) 9537332, pp. 261-266.

21. Васильев В. И., Картак В. М. Применение методов искусственного интеллекта в задачах защиты информации (по материалам научной школы УГАТУ) // Системная инженерия и информационные технологии. 2020. Т. 2. № 2 (4). С. 43-50. [[Vasiliev V. I., Kartak V. M. “Application of artificial intelligence methods in information security problems (based on the materials of the scientific school of the USATU)” // System Engineering and Information Technologies. 2020. V.2, No. 2 (4), pp. 43-50. (In Russian).]]

22. Аникин И. В. Метод оценки внутренних рисков информационной безопасности корпоративных информационных сетей // Информация и безопасность. 2014. Т. 17. № 2. С. 320–323. [[Anikin I. V. “Method for assessing internal risks of information security of corporate information networks” // Information and Security. 2014. V. 17, No. 2, pp. 320-323. (In Russian).]]

23. Аникин И. В. Метод оценки рисков для уязвимостей информационных систем, основанный на нечеткой логике // Информация и безопасность. 2014. Т. 17. № 3. С. 468–471. [[Anikin I. V. “Risk assessment method for information systems vulnerabilities based on fuzzy logic” // Information and Security. 2014. V. 17, No. 3, pp. 468-471. (In Russian).]]

24. Аникин И. В., Потапов А. С. Программный комплекс оценки рисков информационной безопасности на основе продукционно-фреймовой модели // Научно-технические ведомости Санкт-Петербургского государственного политехнического университета. Информатика. Телекоммуникации. Управление. 2010. № 5. С. 98-102. [[Anikin I. V., Potapov A. S. “A software package for assessing information security risks based on a production-frame model” // Scientific and Technical Bulletin of the St. Petersburg State Polytechnic University. Computer Science. Telecommunications. Control. 2010. No. 5, pp. 98-102. (In Russian).]]

25. Аникин И. В., Емалетдинова Л. Ю., Кирпичников А. П. Обеспечение информационной безопасности корпоративных информационных сетей через оценку и управление рисками // Вестник Казанского технологического университета. 2015. Т. 18. № 7. С. 247-250. [[Anikin I. V., Emaletdinova L. Yu., Kirpichnikov A. P. “Ensuring information security of corporate information networks through risk assessment and management” // Bulletin of the Kazan Technological University. 2015. V. 18, No. 7, pp. 247-250. (In Russian).]]

26. Аникин И. В., Емалетдинова Л. Ю., Кирпичников А. П. Методы оценки и управления рисками информационной безопасности в корпоративных информационных сетях // Вестник Казанского технологического университета. 2015. Т. 18. № 6. С. 195-197. [[Anikin I. V., Emaletdinova L. Yu., Kirpichnikov A. P. “Methods for assessing and managing information security risks in corporate information networks” // Bulletin of the Kazan Technological University. 2015. V. 18, No. 6, pp. 195-197. (In Russian).]]

27. Аникин И. В., Газимов Р. М. Практика применения моделирующих структур для исследования защищенности информационных активов предприятий // Информация и безопасность. 2015. Т. 18. № 4. С. 376–379. [[Anikin I. V., Gazimov R. M. “The practice of using modeling structures to study the security of information assets of enterprises” // Information and Security. 2015. V. 18, No. 4, pp. 376-379. (In Russian).]]

28. Anikin I. V. “Information security risks assessment in telecommunication network of the university” // In: IEEE Conference 2016 Dynamics of Systems, Mechanisms and Machines (Omsk, 2016), pp. 1-4, doi: 10.1109/Dynamics.2016.7818967 .

29. Аникин И. В. Метод количественной оценки уровня ущерба от реализации угроз на корпоративную информационную сеть // Информационные технологии. 2010. № 1. С. 2-6. [[Anikin I. V. “Method for quantitative assessment of the level of damage from the implementation of threats to the corporate information network” // Information Technologies. 2010. No. 1, pp. 2-6. (In Russian).]]

30. Аникин И. В. Метод анализа иерархий в задачах оценки и анализа рисков информационной безопасности // Вестник КГТУ им. А. Н. Туполева. 2006. № 3. С. 11-18. [[Anikin I. V. “The method of analysis of hierarchies in the tasks of assessing and analyzing risks of information security” // Bulletin of KSTU A. N. Tupolev. 2006. No. 3, pp. 11-18. (In Russian).]]

31. Аникин И. В. Метод нечеткой оценки критичности активов корпоративной информационной сети // Информационные системы и технологии. 2015. № 4. С. 111-120. [[Anikin I. V. “A fuzzy assessment method for the criticality of corporate information network assets” // Information Systems and Technologies. 2015. No. 4, pp. 111-120. (In Russian).]]

32. Аникин И. В. Нечеткая оценка уязвимостей, основанная на метриках CVSS V.2.0 // Проблемы информационной безопасности. Компьютерные системы. 2015. № 3. С. 111-117. [[Anikin I. V. “Fuzzy vulnerability assessment based on CVSS V.2.0 metrics” // Problems of Information Security. Computer Systems. 2015. No. 3, pp. 111-117. (In Russian).]]

33. Аникин И. В. Нечеткая оценка факторов риска информационной безопасности // Безопасность информационных технологий. 2016. № 1. С. 78-87. [[Anikin I. V. “Fuzzy assessment of information security risk factors” // Security of Information Technologies. 2016. No. 1, pp. 78-87. (In Russian).]]

34. Anikin I. V. “Information security risk assessment and management method in computer networks” // In: 2015 International Siberian Conference on Control and Communications (SIBCON). Proceedings. Omsk State Technical University. Russia, Omsk, May 21–23, 2015. IEEE Catalog Number: CFP13794–CDR. doi: 10.1109/SIBCON.2015.7146975 .

35. Anikin I. V., Emaletdinova L. Yu. “Information security risk management in computer networks based on fuzzy logic and cost/benefit ration estimation” // In: Proceedings of the 8th International Conference on Security of Information and Networks (SIN’15). September 8–10, 2015, Sochi/Russia, pp. 8-11.

36. Аникин И. В., Кирпичников А. П. Применение метода анализа иерархий для решения задачи выбора антивирусных продуктов // Вестник Казанского технологического университета. 2014. Т. 17. № 12. С. 187-189. [[Anikin I. V., Kirpichnikov A. P. “Application of the hierarchy analysis method for solving the problem of choosing anti-virus products” // Bulletin of the Kazan Technological University. 2014. V. 17, No. 12, pp. 187-189. (In Russian).]]

37. Аникин И. В., Емалетдинова Л. Ю. Методология количественной оценки и управления рисками информационной безопасности // Информация и безопасность. 2016. Т. 19. № 4. С. 539-542. [[Anikin I. V., Emaletdinova L. Yu. “Methodology of quantitative assessment and risk management of information security” // Information and Security. 2016. V. 19, No. 4, pp. 539-542. (In Russian).]]

Поступила в редакцию 14 августа 2023 г.

МЕТАДАННЫЕ / METADATA

Title: Methods and algorithms for quantitative assessment and management of security risks in corporate information networks based on fuzzy logic.

Abstract: The article presents an overview of the results of a study on the quantitative assessment and management of security risks in corporate information networks (CIS). The object of research is corporate information networks as an object of information protection. The subject of the study is models, methods and algorithms for fuzzy assessment and risk management of CIS information security. The goal is to increase the efficiency of protecting corporate information networks based on the use of evidence-based methods, algorithms, technological solutions, and instrumental software systems for quantifying and managing information security risks in the face of possible fuzziness, inconsistency, incompleteness, and qualitative nature of the initial information. Achieving this goal required solving the following development tasks: 1) a formal CIS model that describes various types of assets and features of their interaction to solve the problem of quantitative IS risk assessment; 2) a method and algorithms for fuzzy assessment of damage from the implementation of threats in the absence of protective measures based on approaches to the quantitative assessment of partial damage indicators, fuzzy assessment of asset criticality levels and a formal CIS model; 3) methods and algorithms for fuzzy assessments of the possibilities of implementing threats and exploiting vulnerabilities in the absence of protective measures in the conditions of uncertainty of the initial information; 4) a method for improving the efficiency of information protection in CIS based on information security risk management, taking into account the model of protective measures, fuzzy assessment of information security risks; 5) technologies for quantitative assessment and risk management of information security in CIS; 6) an instrumental set of programs for fuzzy assessment and management of information security risks in the CIS, which implements the developed technology, methods and algorithms. To solve the tasks set, methods of mathematical modeling, system analysis, fuzzy set theory and fuzzy logic, graph theory, information security, and expert evaluation were used.

Key words: information security; risk assessment; risk management; fuzzy logic; modeling; software framework.

Язык статьи / Language: русский / Russian.

Об авторе / About the author:

АНИКИН Игорь Вячеславович
ФГБОУ ВО «Казанский национальный исследовательский технический университет им. А. Н. Туполева — КАИ», Россия.
Зав. каф. систем информационной безопасности. Дипл. спец. по математ., информат. и выч. технике (Елабужск. гос. пед. ин-т, 1997). Д-р техн. наук по методам и системам защиты информации, инф. безопасности (Уфимск. гос. авиац. техн. ун-т, 2018). Иссл. в обл. информационной безопасности, интеллектуальных систем, нечеткого и нейросетевого моделирования.
E-mail: IVAnikin@kai.ru
ORCID: https://orcid.org/0000-0001-9478-4894
URL: https://elibrary.ru/author_profile.asp?authorid=260371

ANIKIN Igor Vyacheslavovich
Kazan National Research Technical University named after A. N. Tupolev — KAI, Russia.
Head Department of Information Security Systems. Dipl. Specialist in Mathematics, Informatics and Computer Engineering (Elabuga State Pedagogical Institute, 1997). Dr. Tech. Sciences on Methods and Systems of Information Security (Ufa State Aviation Technical University, 2018). Research in the field of information security, intelligent systems, fuzzy and neural network modeling.
E-mail: IVAnikin@kai.ru
ORCID: https://orcid.org/0000-0001-9478-4894
URL: https://elibrary.ru/author_profile.asp?authorid=260371