УДК 004.056.5 Вестник УрФО № 2(52) / 2024, с. 56–67

Ожгибесова А. С., Шабуров А. С., Южаков А. А. DOI: 10.14529/secur240206

ОБ ОЦЕНКЕ РИСКОВ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ НА ОСНОВЕ ПРИМЕНЕНИЯ НЕЧЕТКИХ КОГНИТИВНЫХ КАРТ В ИНТЕЛЛЕКТУАЛЬНЫХ ТРАНСПОРТНЫХ СИСТЕМАХ УПРАВЛЕНИЯ ДОРОЖНЫМ ДВИЖЕНИЕМ

В статье проанализирована проблема оценки рисков безопасности информации в условиях внедрения интеллектуальных информационных систем, а также роста количества и сложности кибератак. Приведен состав интеллектуальной транспортной системы, а также математическое описание нечеткой когнитивной карты и последовательность ее разработки. Проанализирована структура информационных потоков одной из транспортных систем и основные задачи ее функционирования. На основе анализа векторов атак на информационную транспортную систему определены необходимые концепты для разработки нечеткой когнитивной карты оценки рисков. Приведена количественная оценка программного обеспечения, с использованием которого разработана модель оценки рисков на основе нечеткой когнитивной модели

Ключевые слова: *риск информационной безопасности, защита информа-ции, интеллектуальная транспортная система, нечеткая когнитивная карта*

ABOUT ASSESSING INFORMATION SECURITY RISKS BASED ON THE APPLICATION OF FUZZY COGNITIVE MAPS IN INTELLIGENT TRANSPORT TRAFFIC MANAGEMENT SYSTEMS

The article analyzes the problem of assessing information security risks in the context of the implementation of intelligent information systems, as well as the growth in the number and complexity of cyberattacks. The composition of an intelligent transport system is presented, as well as a mathematical description of a fuzzy cognitive map and the sequence of its development. The structure of information flows of one of the transport systems and the main tasks of its functioning are analyzed. Based on the analysis of attack vectors on the information transport system, the necessary concepts for developing a fuzzy cognitive risk assessment map are identified. A quantitative as-sessment of the software is provided, using which a risk assessment model has been de-veloped based on a fuzzy cognitive model

Keywords: *information security risk, information protection, intelligent transport system, fuzzy cognitive map*

Введение

На этапе оценки рисков информационной безопасности возникают достаточно сложные проблемы, обусловленные необходимостью принятия оперативных решений[1]. Данные решения требуют адекватного оценивания параметров и характеристик векторов информационных атак, что также обусловленоразнообразием, сложностью и непредсказуемостью как самих атак, так и прочих деструктивных информационных воздействий. Особенно актуальна данная проблема в условиях внедрения и развития интеллектуальных информационных систем, обеспечивающих функционирование различных, в том числе и критически важных процессов и систем[2]. Необходимость оперативного принятия решений по защите информации требует совершенствования процесса оценки рисков, в том числе и за счет автоматизации с использованием компьютерных средств моделирования.

Прикладной характер процесса оценки рисков предполагает формирование необходимой и достаточной инструментальной базы, позволяющей оперативно формировать требуемые модели угроз безопасности информации. Например, внедрение концепции «умного города» предполагает использование подобных автоматизированных решений для инфраструктурных транспортных решений на основе интеллектуальной поддержки[3].

Современные интеллектуальныетранспортныесистемы (ИТС) представляют собой интеграцию информационных и коммуникационных технологий и средств автоматизации с транспортной инфраструктурой, транспортными средствами и их пользователями[4]. Внедрение подобных систем позволяет реализовать с заданным качеством процессы управления транспортной системой региона, населенного пункта, или отдельной дороги, а также группой транспортных средств, или отдельным средством. Основной целью внедрения подобных систем является обеспечения качественного использования дорожной сети, повышения ее безопасности, а также повышение эффективности транспортного процесса. Достижение цели предполагает использование значительного количества про-

граммно-аппаратурных средств, технических, периферийных устройств, каналов связи для осуществления сбора, обработки и передачи значительных объемов данных.

К основным компонентам ИТС, как правило, относятся следующие компоненты и системы[3]:

1) Транспортные средства, оборудованные средствами для коммуникации и управления.

2) Средства связи и коммуникации, включающие системы передачи данных, электронные сайты, приложения и сети.

3) Системы мониторинга дорожной ситуации, включающие оконечные устройства для мониторинга: видеокамеры, датчики, придорожные метеостанции.

4) Системы общего управления, включающие средства контроля дорожного трафика, паркинга, управления ремонтом и строительством дорожной инфраструктуры, средства управления общественным транспортом.

5) Системы управления движением, включающие средства управления светофорными объектами, шлагбаумами, электронными дорожными знаками.

6) Платежные системы и приложения, включающие платежные автоматы, системы продажи электронных билетов, средства бесконтактной идентификации (RFID-метки).

Сложность взаимодействия и реализация функционального предназначения ИТС, неопределенность и непредсказуемость ситуаций транспортного обеспечения обуславливает значительное количество уязвимостей и векторов информационных атак. Последствия подобных атак сложно предсказуемы и в совокупности влекут за собой значительный экономический ущерб, а также возможный ущерб безопасности жизни и здоровья всех участников дорожного движения.

Противодействие подобным информационным атакам на ИТС предполагается на основе внедрения системы защиты информации. В свою очередь система защиты информации, а также эффективность мер по обеспечению информационной безопасности напрямую зависит от оперативности и адекватности оценки рисков, основанной на автоматизированных методах[5]. Одним из проверенных инструментов подобной оценки является использование метода на основе нечетких когнитивных карт [6].

Метод оценки рисков информационной безопасности на основе нечетких когнитивных карт

Как правило, нечеткая когнитивная карта (НКК) – это ориентированный граф, заданный с помощью множеств[6]:

$$\text{НКК}=<C,F,W>,$$

где $C=\{C_i\}$ – множество концептов – вершин графа, которые в данном случае выступают в качестве факторов, наиболее значимых для оценки угроз безопасности информации;

$F=\{F_i\}$ – множество направленных дуг графа – связей между концептами;

$W=\{W_i\}$ – множество весов связей графа, которые могут быть положительными ($W_{ij}>0$) или отрицательными ($W_{ij}<0$) в зависимости от того, усиливают или ослабляют влияние концепта на концепт.

Разработка НКК предполагает реализацию нескольких обязательных этапов, с учетом специфики решаемых задач, а также используемых инструментов моделирования.

На первоначальном этапе определяются цели и задачи моделирования, которые достигаются и решаются посредством разработки НКК.

На втором этапе определяются исходные данные, которые, как правило, носят статистический характер, представляют собой результаты исследований, или экспертных оценок.

На третьем этапе определяются правила вывода результатов моделирования, обусловленные логическими законами принятия решений и основанные на имеющейся базе данных. Правила вывода определяют связи получаемых решений, основанных на множестве входных параметров.

На четвертом этапе разработки НКК предполагается применение специализированного программного обеспечения, с целью проверки работоспособности модели.

На заключительном этапе проводится тестирования и валидация разработанной модели на основе созданных разнообразных сценариев, в меняющихся условиях. Валидация модели осуществляется с учетом экспертных оценок и реальных условий функционирования моделируемых систем. Внедрение разработанной модели предполагает ее применение в предметной области для решения конкретных задач[7].

Выбор программного обеспечения для моделирования НКК

Выбор программного обеспечения для реализации модели напрямую зависит от целей и задач, которые преследуются в работе, а также от финансовых ограничений и технических возможностей.

Проанализировав информацию о существующих программных продуктах, можно выделить следующие наиболее важные критерии выбора[8-11]:

1. Простота использования программы. Интуитивно понятный интерфейс позволит пользователям быстро освоить процесс создания моделей, что в свою очередь приведет к экономии времени оценки угроз информационной безопасности.

2. Возможность визуального представления моделей, что позволяет сделать модели более наглядными добавлению цветовых эффектов, текста и мультимедийных объектов. Таким образом, упрощается проведение анализа и интерпретация полученных результатов.

3. Широкое разнообразие инструментов форматирования и стилизации обеспечивает большую гибкость и творческие возможности при создании моделей, что сделает их более информативными и удобными для восприятия.

4. Возможность экспорта данных в различные форматы для использования полученных исследований в проектах, при добавлении в отчеты и интеграции с другими приложениями.

5. Открытый исходный код, обеспечивающий прозрачность в отношении функциональности и безопасности программного обеспечения. Код можно проверить на наличие ошибок, дополнить или модифицировать в соответствии с потребностями организации.

6. Поддержка разработчиками и периодические обновления (сопровождение) позволяют избавляться от возникающих ошибок функционирования, увеличивать возможности моделирования и совершенствовать продукт.

7. Мультиплатформенность, что делает программу доступной для широкого круга пользователей не зависимо от операционной системы или устройства, которые он использует.

Кроме того, необходимо ввести количественную оценку критериев для получения объективных результатов. Оптимальное решение принимается при точном расчете и сравнении различного программного обеспечения (ПО) на основе одних и тех же мер или показателей[12].

Для удобства представления критериев выбора ПО разработана сводная таблица характеристик программных решений, на основе присвоения им одного из следующих значений:

0 – критерий отсутствует в программе;

1 – критерий присутствует, но функционально ограничен;

2 – критерий присутствует и имеет полную функциональность.

Полученные оценки значений критериев ПО, потенциально используемых для разработки НКК, представлены в таблице 1. Итоговый суммарный результат оценки критериев позволяет осуществить выбор наиболее эффективное ПО для разработки НКК.

Таблица 1.

Количественная оценка программного обеспечения

	FCMapper	CmapTools	XMind	Visual Understanding Environment
Простота использования	1	2	2	2
Возможности визуального представления моделей	1	2	2	2
Разнообразие функций	0	2	2	2
Экспорт данных	1	1	1	2
Открытый исходный код	2	0	0	2
Поддержка и обновления	0	1	2	1
Мультиплатформенность	1	2	2	2
Итоговая оценка	6	10	11	13

Результаты количественной оценки критериев позволяет выбрать ПО Visual Understanding Environment (VUE), являющееся оптимальным для решения поставленных задач текущего исследования.

Разработка нечеткой когнитивной модели для автоматизации оценки рисков

1. Цель и задачи моделирования

Целью моделирования является наглядное представление метода оценки рисков на основе НКК для конкретного примера в организации, управляющей интеллектуальной транспортной системой.

Задачи:

- анализ особенностей организации, актуальных угроз (дестабилизирующих факторов), информационных ресурсов, наиболее значимых рисков, являющихся целевыми факторами;
- построение графа связности концептов и определение их весов;
- расчет относительного уровня риска информационной безопасности (целевых факторов).

2. Определение входных данных

В качестве предметной области в данной работе рассматривается одна из транспортных систем, предназначенная для контроля и обеспечения безопасности дорожного движения, функционирующая на базе государственного краевого учреждения «Центр безопасности дорожного движения» (ГКУ ЦБДД). Оценка рисков осуществляется на примере одного из значимых объектов КИИ. На рис. 1 представлена структура информационных потоков ГКУ «ЦБДД».

По результатам экспертной оценки функционирования систем ГКУ «ЦБДД» определен перечень информационных систем - объектов КИИ, к которым относятся:

1. Информационная система «Метеорологическое обеспечение»;
2. Информационная система «Фотовидеофиксация»;
3. Информационная система «Видеонаблюдение»;
4. Информационная система «Весовой и габаритный контроль».

В качестве примера для построенияНКК определена информационная система (ИС) «Метеорологическое обеспечение», предназначенная для выполнения следующих функций:

- получение оперативной информации о погодных условиях и состоянии дорожного покрытия на сети автомобильных дорог Пермского края;
- прогнозирование возможных опасных метеорологических условий на дорожном полотне;
- принятие решений по проведению необходимых работ по содержанию дорог.

В состав ИС входят комплексные посты дорожного контроля (КПДК), основу которых составляют 59 датчиков, распределенных по дорожной сети региона.

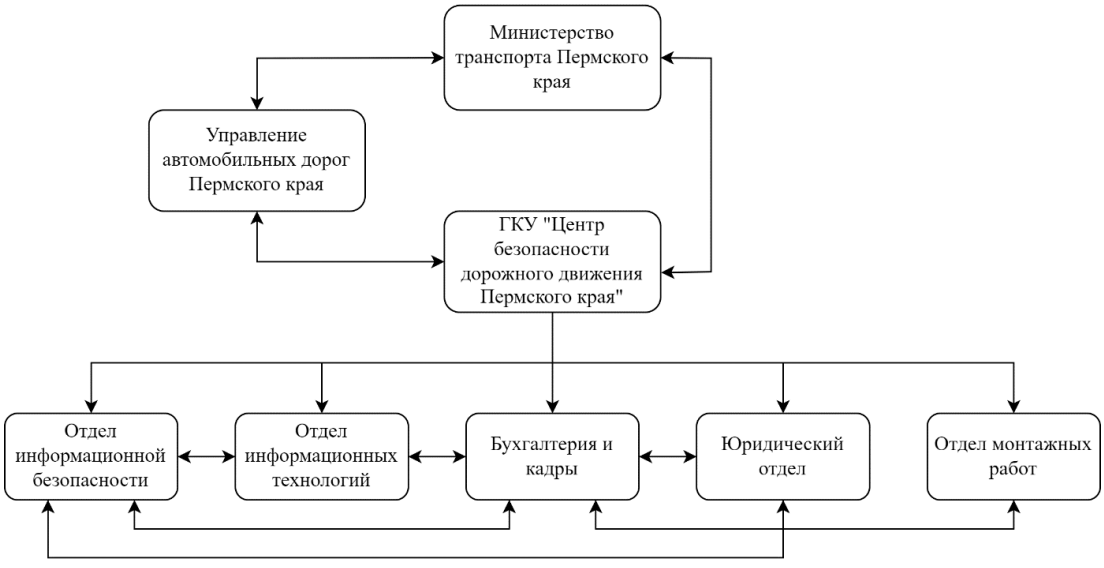

Рисунок 1 – Структура информационных потоков ГКУ «ЦБДД»

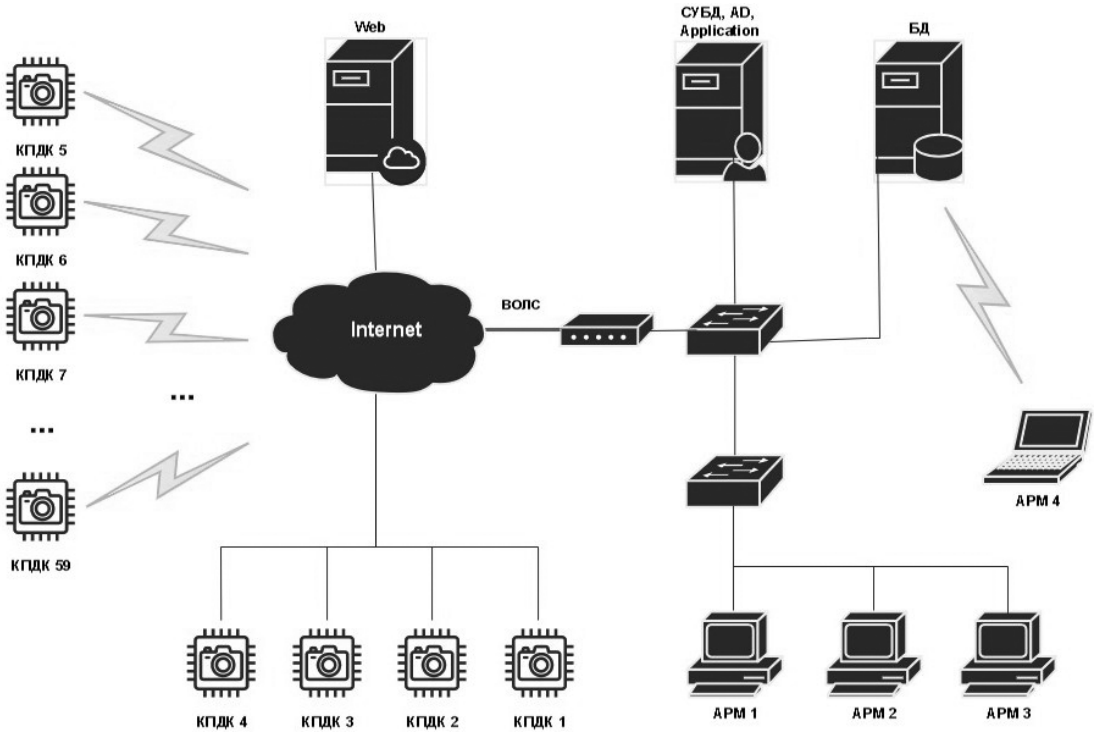

Рис. 2. Общая схема ИС «Метеорологическое обеспечение»

Структурная схема ИС «Метеорологическое обеспечение», включающая 4-е автоматизированных рабочих места (АРМ) операторов ИС, объединенных в одну локальную сеть.

Управление ИС осуществляется на основе 3-х серверных станций, обеспечивающих выполнение всех вышеперечисленных функций.

В ИС «Метеорологическое обеспечение» обрабатываютсяследующие виды информации:

• видовая информация о погодной обстановке на дорожном полотне в зоне обозрения видеокамеры (формируется КПДК во взаимодействии с подключенными к ним камерами видеонаблюдения);

• информация в числовом и текстовом виде о погодных условиях, в которых располагается станция (формируется КПДК во взаимодействии с подключенными к ним датчиками).

Полученная от датчиков информация направляется по каналам связи через КПДК для хранения на сервере баз данных. В дальнейшем данная информация используется оператором диспетчерского центра, отделом эксплуатации автомобильных дорог для принятия решения по управлению дорожным движением.

Основными задачами обработки информации в системе являются: составление статистики погодных условий с целью предварительной оценки затрат на обслуживание дорожного полотна, уведомление подрядных организаций о необходимости принять меры по уходу за дорожным полотном, общедоступное доведение до автовладельцев сведений о погодных условиях на дорожном полотне. Рассматриваемая сеть относится к сетям электросвязи 2 категории (выделенная)[13].

К основным последствиям реализации компьютерных атак (КА) на ИС «Метеорологическое обеспечение» относятся следующие:

• прекращение или нарушение функционирования объектов транспортной инфраструктуры (автомобильных дорог), так как объект обеспечивает осведомление подрядных организаций, ответственных за обеспечение надлежащего состояния дорожного полотна;

• нарушение функционирования Министерства транспорта Пермского края в части выполнения возложенной на него функции по осуществлению государственного контроля (надзора) за соблюдением требований технического регламента Таможенного союза «Безопасность автомобильных дорог».

Анализ деструктивных информационных воздействий на ИС «Метеорологическое обеспечение» предполагающий оценку потенциально возможных векторов КА, которые могут быть реализованы злоумышленником, представлены на рис. 3.

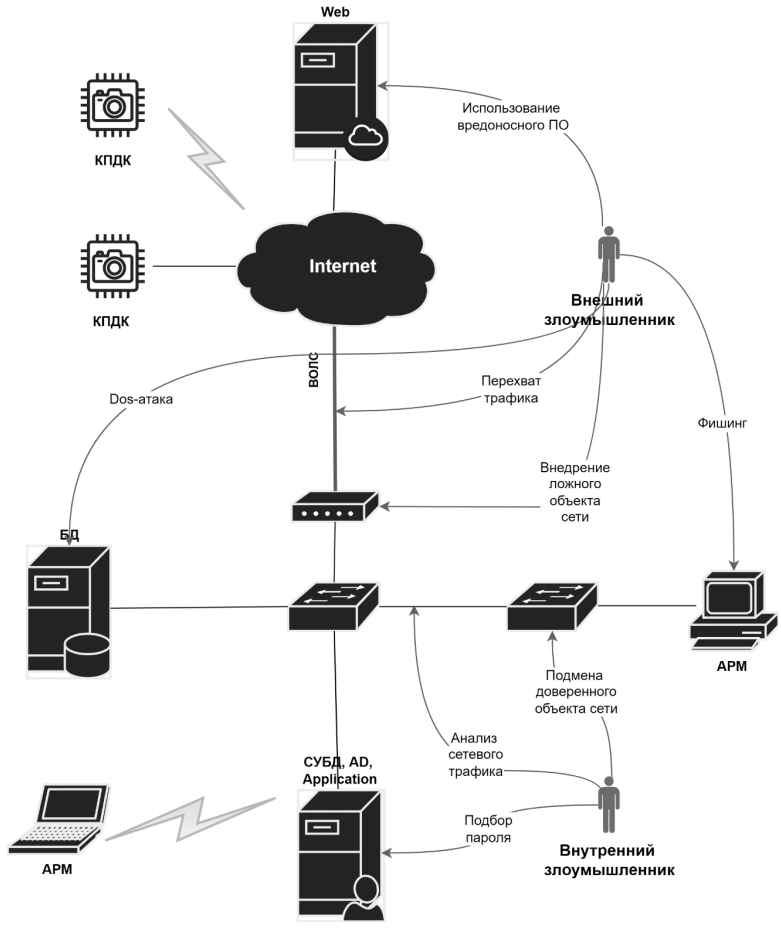

Рис. 3. Вектора атак на ИТС

Внутренний злоумышленник, действующий из корпоративного сегмента сети, может проникнуть в технологическую сеть предприятия и скомпрометировать технологический процесс, получить и повысить привилегий в ОС на узлах ИС.

Внешний злоумышленник, обнаруживший доступные интерфейсы администрирования серверов ИС и удаленного доступа к СУБД в совокупности с повсеместным использованием словарных и стандартных паролей привилегированных пользователей, может в один шаг получить полный контроль как над веб-приложениями, так и над серверами, получить доступ к БД и файлам, развивать атаку на другие ресурсы. Хранящиеся в открытом доступе важные данные, например учетные записи, исходный код веб-приложений, персональные данные пользователей, могут быть использованы при атаках.

Процесс работы ИТС начинается со сбора информации о состоянии трафика. Данные собираются непосредственно от пользователей по средствам GPS на смартфонах или других устройств, а такжес использованием видеокамер с высоким разрешением и дорожных радаров.

Использование подобных технологий позволяет получить информацию о скорости, расстоянии между транспортными средствами, маршрутах, движении через перекрестки, задержках и распределении между отдельными полосами движения и т.п. Затем данные попадают в центры управления дорожным движением, где происходит их анализ, и выстраиваются дальнейшие решения по оптимизации трафика. После этого обработанная информация отправляется на «умные» светофоры для смены сигналов в зависимости от загруженности соседних перекрестков, в случае ДТП на мобильные приложения для предупреждения о затруднениях проезда и координации общественного транспорта, а также др.

В качестве основных угроз, при оценке рисков функционирования ИСвыделим возможные векторы атак рассматриваемого фрагмента организации:

- анализ сетевого трафика;
- сканирование сети;
- угроза выявления пароля;
- подмена доверенного объекта сети;
- фишинг;
- внедрение ложного объекта сети;
- отказ в обслуживании;
- угрозы внедрения по сети вредоносных программ.

Исходя из сформированного списка векторов атак и последствий их реализации, вы-

Таблица 2.

Список концептов НКК

Концепт	Класс	Название концепта	Переменные состояния
C_1	Дестабилизирующие факторы (угрозы)	Угроза анализа сетевого трафика	Среднее количество реализации несанкционированного доступа, в ед. времени
C_2		Угроза сканирования сети	Среднее количество обнаруженных узлов, в ед. времени
C_3		Угроза выявления пароля	Среднее количество подобранных паролей, в ед. времени
C_4		Угроза подмены доверенного объекта сети	Среднее количество подмененных объектов, в ед. времени
C_5		Фишинг	Среднее количество фишинговых атак, в ед. времени
C_6		Угроза внедрения по сети вредоносных программ	Среднее количество вирусных атак, в ед. времени
C_7		Угроза физического выведения из строя средств хранения, обработки и (или) ввода/вывода/передачи информации	Среднее количество средств, выведенных из строя, в ед. времени
C_8		Угроза отказа в обслуживании	Среднее количество отказов, в ед. времени
C_9	Информационные ресурсы	АРМ сотрудников	Количество работоспособных АРМ, ед.
C_{10}		КПДК	Количество работоспособных КПДК, ед.
C_{11}		Программное обеспечение	Количество видов ПО, ед.
C_{12}		База данных	Объем информации, содержащейся в БД, Гбайт
C_{13}	Целевые факторы	Репутация организации	Число негативных высказываний, ед.
C_{14}		Качество предоставляемых услуг	Точность метеорологических показаний, %
C_{15}		Материальный ущерб	Финансовые потери, направленные на восстановление работоспособности, руб.

деляются концепты НКК карты ИС, актуальные для ИС «Метеорологическое обеспечение». Основные концепты когнитивной карты приведены в таблице 2.

Зададим веса W_{ij} с помощью нечеткой лингвистической шкалы, которая представляет собой упорядоченное множество лингвистических знаний (термов)[14]. Каждому из термов поставим в соответствие некоторый числовой диапазон, принадлежащий отрезку $[0;1]$ для обозначения положительного влияния или отрезку $[-1;0]$ - для отрицательных.

Таким образом, определяются входные данные для моделирования нечеткой когнитивной карты.

3. Построение графа с учетом особенностей ИС «Метеорологическое обеспечение»

В программной среде VUE построим модель оценки рисков НКК (рис. 4), в которой концепты обозначены номерами, а на связях между концептами определены значения весов. Значения весов определяются экспертным методом.

Рис. 4. Модель оценки рисков на основе НКК

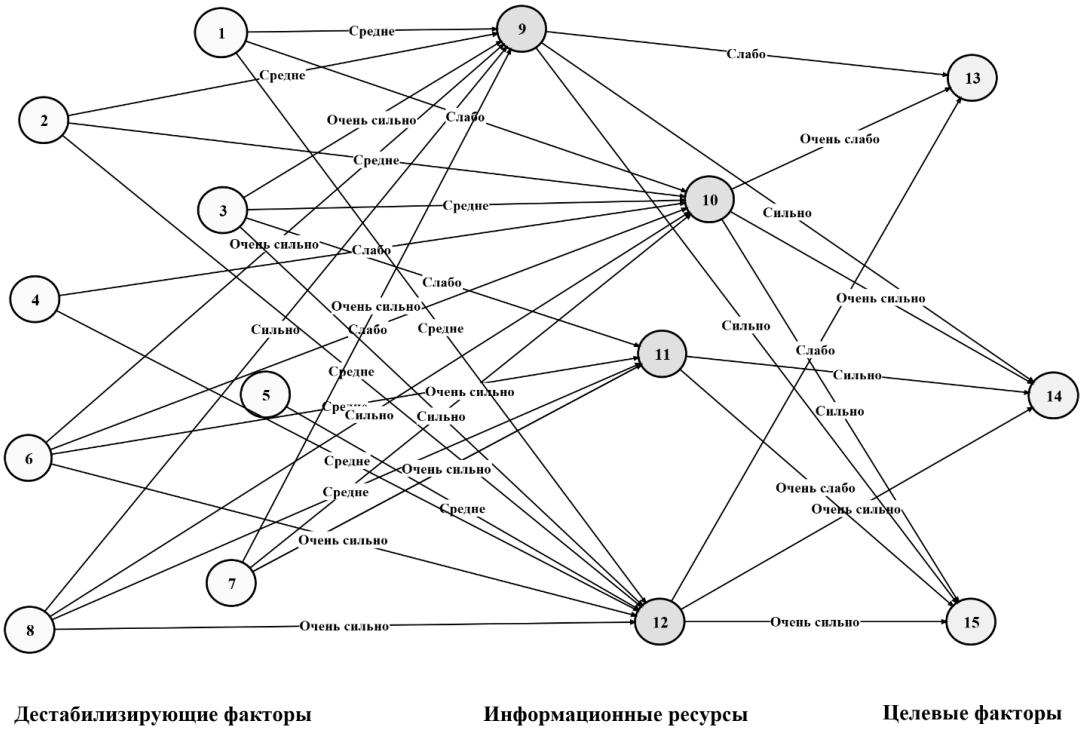

Рис. 4. Модель оценки рисков на основе НКК

Переведенныечисленные значения лингвистических термвесов связей НКК представлены в таблице 3.

Расчет состояния i-го концепта НКК производится уравнением вида[15]:

$$X_i(t+1) = f(\sum_{j=1}^{n} W_{ji}X_j(t) + X_i(t)) \qquad (1)$$

где $X_i(t+1)$ и $X_i(t)$ - значения переменной X_i, на $(t+1))$-м и t-м шаге соответственно, $(k = 1,2,...)$; W_{ji}- вес связи между концептами C_i и C_j; f - некоторая нелинейная функция, принимающая значения в интервале [0,1].

Таблица 3.

Веса связей между концептами НКК

Вес связи $C_i \rightarrow C_j$	НКК	Вес связи $C_i \rightarrow C_j$	НКК	Вес связи $C_i \rightarrow C_j$	НКК
W_{ij}	W_{ij}	$W_{4\rightarrow12}$	0,475	$W_{8\rightarrow12}$	0,925
$W_{1\rightarrow9}$	0,475	$W_{5\rightarrow12}$	0,475	$W_{9\rightarrow13}$	0,25
$W_{1\rightarrow10}$	0,25	$W_{6\rightarrow9}$	0,925	$W_{9\rightarrow14}$	0,725
$W_{1\rightarrow12}$	0,475	$W_{6\rightarrow10}$	0,25	$W_{9\rightarrow15}$	0,725
$W_{2\rightarrow9}$	0,475	$W_{6\rightarrow11}$	0,475	$W_{10\rightarrow13}$	0,1
$W_{2\rightarrow10}$	0,475	$W_{6\rightarrow12}$	0,925	$W_{10\rightarrow14}$	0,925
$W_{2\rightarrow12}$	0,475	$W_{7\rightarrow9}$	0,925	$W_{10\rightarrow15}$	0,725
$W_{3\rightarrow9}$	0,925	$W_{7\rightarrow10}$	0,925	$W_{11\rightarrow14}$	0,925
$W_{3\rightarrow10}$	0,925	$W_{7\rightarrow11}$	0,925	$W_{11\rightarrow15}$	0,1
$W_{3\rightarrow11}$	0,25	$W_{8\rightarrow9}$	0,725	$W_{12\rightarrow13}$	0,25
$W_{3\rightarrow12}$	0,725	$W_{8\rightarrow10}$	0,725	$W_{12\rightarrow14}$	0,925
$W_{4\rightarrow10}$	0,25	$W_{8\rightarrow11}$	0,475	$W_{12\rightarrow15}$	0,925

Таблица 4.

Результаты моделирования угроз

R_{13}	R_{14}	R_{15}
0,245	0,647	0,925

4. Расчет относительного уровня рисков для целевых факторов

Рассчитаем относительный уровень риска R_i для целевых факторов: репутация организации (C_{13}), качество предоставляемых услуг (C_{14}), материальный ущерб (C_{15}). Значение уровня угрозы рассчитывается как $R_i=X_i^*$, где X_i^* - установившееся значения состояния i-го целевого концепта, в данном случае i=13,14,15. Результаты моделирования уровня угроз целевых факторов показаны в таблице 4.

Для удобства интерпретации представим значения уровней угроз целевых концептов в виде диаграммы (рис. 5).

Полученные значения целевых факторов рисков информационной безопасности на целевые факторы позволяют выработать рекомендации по приоритетным направлениям для создания и/или совершенствования системы защиты информации. На основании диаграммы значений целевых факторов можно сделать вывод, что наиболее важным является необходимость проведения мероприятий по снижению риска, влекущего материальный ущерб организации. Следующим шагом по рейтингу опасности необходимо снизить уровень риска, влияющий на качество предоставляемых услуг. Уровень риска для репутации организации является приемлемым, поэтому, в данном случае, можно вынести решение о принятии риска.

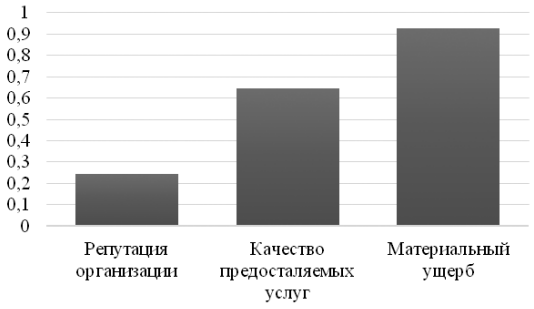

Рисунок 5 – Диаграмма значений целевых факторов

Заключение

Таким образом, приведенный в статье пример применения методики оценки рисков безопасности информации для критически важной информационной инфраструктуры ИС «Метеорологическое обеспечение» в организации ГКУ «ЦБДД» показывает, что оценка рисков, основанная на построении НКК– это эффективный инструмент для анализа нечеткости и неопределенности в оценке угроз безопасности информации и принятия обоснованных решений, что повышает эффективность системы безопасности, в целом. Кроме того, моделирование на основе НКК позволяет учитывать широкий спектр факторов и их взаимосвязей, а также использовать возможность визуализации оценки рисков информационной безопасности. Применение НКК может быть расширено, с учетом новых факторов, характеристик ИС и изменений предметной области. НКК предоставляют собой фундаментальную основу для дальнейшего развития и усовершенствования процесса оценки рисков информационной безопасности.

Литература

1. Шабуров, А.С. Разработка нечеткой когнитивной модели для автома-тизации оценки угроз безопасности информации / А.С. Шабуров, А.С. Ожгибесова // Master'sJournal. – 2023. –№ 2. – Art. № 05.

2. Ожгибесова А.С., Шабуров А.С.Метод автоматизации оценки угроз безопасности информации на основе нечетких когнитивных моделей // Иннова-ционные технологии: теория, инструменты, практика. – 2022. – Т.1. – С. 290-296.

3. Курчеева Г.И., Денисов В.В. Угрозы для информационной безопасности в высокоорганизованных системахтипа «Умный город» // Интернет-журнал «НАУКОВЕДЕНИЕ» Том 8, №3 (2016) http://naukovedenie.ru/PDF/146EVN316.pdf (доступ свободный). (Дата обращения: 02.03.2024).

4. М.Р. Якимов. Транспортное планирование: терминологический сло-варь / М. Р. Якимов. – М: Агентство РАДАР, 2022. – 87 с. (Дата обращения: 29.02.2024).

5. Булдакова Т. И., Миков Д. А. Обеспечение согласованности и адек-ватности оценки факторов риска информационной безопасности // Вопросы ки-бербезопасности. 2017. №3 (21). URL: https://cyberleninka.ru/article/n/obespechenie-soglasovannosti-i-adekvatnosti-otsenki-faktorov-riska-informatsionnoy-bezopasnosti (дата обращения: 04.03.2024).

6. Васильев В.И. Интеллектуальные системы защиты информации: учебное пособие/. 2 е изд., испр. и доп. М.: Машиностроение, 2013. 172 с. (Дата обращения: 05.03.2024).

7. Васильев В.И., Вульфин А.М., Герасимова И.Б., Картак В.М. Анализ рисков кибербезопасности с помощью нечетких когнитивных карт.// Вопросы кибербезопасности. 2020. №2 (36). (дата обращения: 21.03.2024).

8. FCMapper // [Электронный ресурс] – Режим доступа: https://www.fcmappers.net/joomla/index.php (Дата обращения: 15.03.2024).

9. CmapTools // [Электронный ресурс] – Режим доступа: https://cmap.ihmc.us/ (Дата обращения: 16.03.2024).

10. XMind // [Электронный ресурс] – Режим доступа: https://xmind.app/ (Дата обращения: 17.03.2024).

11. VisualUnderstandingEnvironment// [Электронный ресурс] – Режим доступа: https://vue.tufts.edu/ (Дата обращения: 18.03.2024).

12. Федеральный закон от 07.07.2003 N 126-ФЗ (ред. 14.11.2023) "О связи". (Дата обращения: 09.03.2024).

13. Корнев, Л. В. Определение уровня безопасности системы защиты ин-формации на основе когнитивного моделирования / Л. В. Корнев. —— Текст: непосредственный // Молодой ученый. —— 2021. —— № 33 (375). —— С. 9--14. —— URL: https://moluch.ru/archive/375/83624/ (Дата обращения: 12.03.2024).

14. Васильев В. И., Вульфин А. М., Кудрявцева Р. Т. Анализ и управление рисками информационной безопасности с использованием технологий когнитивного моделирования // Доклады ТУСУР. 2017. №4. (Дата обращения: 19.03.2024).

15. Васильев В.И. Автоматизация процесса оценки информационных рисков с использованием нечетких когнитивных карт / В.И. Васильев, Р.Т., Кудрявцева, В.А. Юдинцев // Вестник УГАТУ, 2014. Т. 18, № 3 (64). С. 253 260. (дата обращения: 15.03.2024).

References

1. SHaburov, A.S. Razrabotkanechetkojkognitivnojmodelidlyaavto-matizaciiocenkiugrozbezopasnosti informacii / A.S. SHaburov, A.S. Ozhgibesova // Master'sJournal. – 2023. –№ 2. – Art. № 05.

2. Ozhgibesova A.S., SHaburov A.S. Metodavtomatizaciiocenkiugrozbezopasnostiinformaciinaosnove nechetkihkognitivnyhmodelej // Innovacionnyetekhnologii: teoriya, instrumenty, praktika. – 2022. – T.1. – S. 290-296.

3. Kurcheeva G.I., Denisov V.V. Ugrozydlyainformacionnojbezopas-nosti v vysokoorganizovannyhsiste mahtipa «Umnyjgorod» // Internet-zhurnal «NAUKOVEDENIE» Tom 8, №3 (2016) http://naukovedenie.ru/PDF/146EVN316.pdf (dostupsvobodnyj). (Data obrashche-niya: 02.03.2024).

4. M.R. YAkimov. Transportnoe planirovanie: terminologicheskij slo-var' / M. R. YAkimov. – M: Agentstvo RADAR, 2022. – 87 s. (Data obrashcheniya: 29.02.2024).

5. Buldakova T. I., Mikov D. A. Obespecheniesoglasovannosti i adek-vatnostiocenkifaktorovriskainformacionnojbezopasnosti // Voprosyki-berbezopasnosti. 2017. №3 (21). URL: https://cyberleninka.ru/article/n/obespechenie-soglasovannosti-i-adekvatnosti-otsenki-faktorov-riska-informatsionnoy-bezopasnosti (data obrashcheniya: 04.03.2024).

6. Vasil'ev V.I. Intellektual'nye sistemy zashchity informacii: uchebnoe posobie/. 2 e izd., ispr. i dop. M.: Mashinostroenie, 2013. 172 s. (Data obrashcheniya: 05.03.2024).

7. Vasil'ev V.I., Vul'fin A.M., Gerasimova I.B., Kartak V.M. Ana-liz riskov kiberbezopasnosti s pomoshch'yu nechetkih kognitivnyh kart. // Vo-prosy kiberbezopasnosti. 2020. №2 (36). (data obrashcheniya: 21.03.2024).

8. FCMapper // [Elektronnyj resurs] – Rezhim dostupa: https://www.fcmappers.net/joomla/index.php (Data obrashcheniya: 15.03.2024).

9. CmapTools // [Elektronnyj resurs] – Rezhim dostupa: https://cmap.ihmc.us/ (Data obrashcheniya: 16.03.2024).

10. XMind // [Elektronnyj resurs] – Rezhim dostupa: https://xmind.app/ (Data obrashcheniya: 17.03.2024).

11. Visual Understanding Environment // [Elektronnyj resurs] – Rezhim dostupa: https://vue.tufts.edu/ (Data obrashcheniya: 18.03.2024).

12. Federal'nyj zakon ot 07.07.2003 N 126-FZ (red. 14.11.2023) "O svyazi". (Data obrashcheniya: 09.03.2024).

13. Kornev, L. V. Opredelenie urovnya bezopasnosti sistemy zashchity informacii na osnove kognitivnogo modelirovaniya / L. V. Kornev. —— Tekst: neposredstvennyj // Molodoj uchenyj. —— 2021. —— № 33 (375). —— S. 9--14. —— URL: https://moluch.ru/archive/375/83624/ (Data obrashcheniya: 12.03.2024).

14. Vasil'ev V. I., Vul'fin A. M., Kudryavceva R. T. Analiz i uprav-lenie riskami informacionnoj bezopasnosti s ispol'zovaniem tekhnologij ko-gnitivnogo modelirovaniya // Doklady TUSUR. 2017. №4. (Data obrashcheniya: 19.03.2024).

15. Vasil'ev V.I. Avtomatizaciyaprocessaocenkiinformacionnyhriskov s ispol'zovaniemnechetkihkognit ivnyhkart / V.I. Vasil'ev, R.T., Kudryavceva, V.A. YUdincev // Vestnik UGATU, 2014. T. 18, № 3 (64). S. 253 260. (dataobrashcheniya: 15.03.2024).

ОЖГИБЕСОВА Анна Сергеевна, аспирант кафедры Автоматики и теле-механики, Пермский национальный исследовательский политехнический универ-ситет. 614990, Пермский край, г. Пермь, Комсомольский проспект, д. 29. E-mail: aozgibesova@pstu.ru

ШАБУРОВ Андрей Сергеевич, кандидат технических наук, доцент, доцент кафедры Автоматики и телемеханики, Пермский национальный исследовательский политехнический университет. 614990, Пермский край, г. Пермь, Комсомольский проспект, д. 29. E-mail: shans@at.pstu.ru

ЮЖАКОВ Александр Анатольевич, доктор технических наук, профессор, заведующий кафедры Автоматики и телемеханики, Пермский национальный исследовательский политехнический университет. 614990, Пермский край, г. Пермь, Комсомольский проспект, д. 29. E-mail: uz@at.pstu.ru

OZHGIBESOVA Anna Sergeevna, graduatestudent, Department of Automation and Telemechanics, Perm National Research Polytechnic University. 614990, Perm Krai, Perm, Komsomolsky Prospekt, 29. E-mail: aozgibesova@pstu.ru

SHABUROV Andrey Sergeevich, Candidate of Technical Sciences, Associate Professor of the Department of Automation and Telemechanics, Perm National Research Polytechnic University. 614990, Perm Krai, Perm, Komsomolsky Prospekt, 29. E-mail: shans@at.pstu.ru

YUZHAKOV Alexander Anatolyevich, Doctor of Technical Sciences, Profes-sor, Head of the Department of Automation and Telemechanics, Perm National Re-search Polytechnic University. 614990, Perm Krai, Perm, Komsomolsky Prospekt, 29. E-mail: uz@at.pstu.ru