УДК 004.81

Вестник УрФО № 4(50) / 2023, с. 43–52

Палютина Г.Н.

DOI: 10.14529/secur230404

О ПРИМЕНЕНИИ КОГНИТИВНОГО МОДЕЛИРОВАНИЯ В АДАПТИВНОЙ ОЦЕНКЕ РИСКОВ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ[1]

В статье обсуждаются результаты анализа возможности применения технологий когнитивного моделирования (КМ), а именно нечетких когнитивных карт (НКК) в различных этапах оценки рисков информационной безопасности (РИБ).

Были проанализированы ГОСТы, международные стандарты, различные научные публикации в области оценки РИБ, и была сформирована функциональная модель процесса оценки РИБ.

Продемонстрировано внедрение в один из этапов данной функциональной модели элементов КМ. Предложено на этапе «Идентификации угроз» использовать НКК для анализа необходимых исключительно для текущей ситуации факторов угроз, выраженных в виде концептов НКК.

Ключевые слова: *информационная безопасность, оценка информационных рисков, адаптивная оценка рисков информационной безопасности, когнитивное моделирование, нейронные сети, нечеткие когнитивные карты.*

[1] В рамках исполнения гранта ИБ МТУСИ № 40469-23/2022-к 15.06.2022г. протокол №2

ON THE APPLICATION OF COGNITIVE MODELING IN ADAPTIVE ASSESSMENT OF INFORMATION SECURITY RISKS

The article discusses the results of an analysis of the possibility of using cognitive modeling (CM) technologies, namely fuzzy cognitive maps (FCMs) in various stages of information security risk assessment (ISS).

GOSTs, international standards, various scientific publications in the field of RIB assessment were analyzed, and a functional model of the RIB assessment process was formed.

The implementation of CM elements into one of the stages of this functional model is demonstrated. It is proposed to use the NCC at the stage of "Threat Identification" to analyze the threat factors necessary exclusively for the current situation, expressed in the form of NCC concepts.

Keywords: *information security, information risk assessment, adaptive information security risk assessment, cognitive modeling, neural networks, fuzzy cognitive maps.*

Введение

В современном информационном обществе обеспечение защищённости информации становится все более важной и актуальной задачей. Угрозы кибербезопасности постоянно эволюционируют, традиционные статичные методы оценки рисков ИБ и противодействия им оказываются недостаточными. Отсюда вытекает актуальность поиска новых подходов и методов, позволяющих адаптивно оценивать риски ИБ и эффективно предотвращать их реализацию.

Одним из перспективных направлений в данном вопросе является применение КМ, которое позволяет учитывать неопределенность, сложность и динамичность информационной среды, а также факторы человеческого поведения и принятия решений.

Напомним, что процесс оценки рисков ИБ включает несколько этапов [1-4]. Сперва осуществляется идентификация и анализ уязвимостей информационной системы, а также оценка вероятности их возникновения. Затем проводится анализ потенциальных последствий этих уязвимостей, включая потерю конфиденциальности, целостности и доступности данных. Далее происходит определение уровня рисков и разработка мер по управлению рисками, включая рекомендации по применению комплекса мероприятий по защите информации.

Цель данной работы в исследовании применения технологий КМ в вышеупомянутых этапах оценки рисков ИБ с целью придания ему свойств адаптивности.

В статье проведен анализ ГОСТов, международных стандартов, научных публикаций по оценке рисков ИБ и КМ, сформирована функциональная модель оценки рисков ИБ, построена НКК, применимая на одном из этапов оценки рисков ИБ.

Формирование функциональной модели процесса оценки рисков ИБ и особенности внедрения в модель технологий КМ

Понятие управления и оценки рисков ИБ, подходы к организации этих процессов, методы, которые могут быть применены, общие рекомендации к проведению оценки рисков описываются в ГОСТах, международных стандартах, руководящих и прочих документах [1-3]. Опираясь на определения оценки риска, определим этот процесс как процесс, состоя-

щий из идентификации риска, анализа и оценки опасности риска, также можно использовать подход PDCA, который отмечает следующие этапы [4-5]:

1) идентификация контекста;
2) оценка рисков;
3) разработка плана обработки рисков;
4) принятие рисков;
5) ввод сформированного перечня действий по обработке рисков;
6) мониторинг и обновление рисков;
7) модернизация процесса риск-менеджмента.

Подробное описание данных этапов приведено в таблице 1 [5].

Опираясь на вышеперечисленные опре-

Таблица 1

Этапы оценки рисков информационной безопасности

№	Этапы	Характеристики
1	Идентификация риска	Классификация методов: – основанные на документальных свидетельствах: анализ контрольных листов, анализ экспериментальных данных, а также данных и событий, произошедших в прошлом; – посредством структурированного множества подсказок или вопросов; – индуктивные методы
2	Анализ риска	– Оценка методов управления; – анализ последствий реализации риска; – анализ и оценка вероятности; – предварительный анализ; – определение неопределенности и чувствительности. Классификация методов: качественные, количественные, смешанные.
3	Сравнительная оценка риска	Сопоставление уровня риска с критериями риска, установленными при определении области применения менеджмента риска, для определения типа риска и его значимости.

деления управления и оценки рисков ИБ, была сформирована функциональная модель данного процесса. В качестве основных этапов были определены следующие: идентификация активов; идентификация угроз; оценка уязвимостей; оценка вероятностей и воздействия; определение уровня рисков; формирование мер по снижению рисков; мониторинг и обновление.

Сформированная модель в нотации IDEF0 отображена на рисунке 1. В качестве управления используются приказы и методические документы ФСТЭК России. Остальные данные для входа, выхода и механизмы управления отражены в таблице 2.

Настоящая модель представляет собой стандартный статический подход к оценке рисков ИБ. Усовершенствование модели технологиями КМ позволит добавить ей свойства адаптивности. Эти вопросы рассмотрены авторами работ [6-8]. Отмечены основные проблемы оценки рисков ИБ: из-за недостаточности и противоречивости статистической информации об угрозах и уязвимостях, достоверная оценка рисков информационной безопасности затрудняется. Успешность такой оценки значительно зависит от качества экспертных оценок, полученных в ходе аудита информационной безопасности.

В [9] приведен сравнительный анализ методов КМ: сети Байеса; НКК; серые НКК. НКК выделен как ключевой метод КМ, однако у них есть недостатки. Эти недостатки включают необходимость ввода экспертной оценки вероятности активации входного концепта и невозможность комплексной оценки влияния нескольких факторов на один узел. Для решения этих проблем предложено использование серых НКК, которые позволяют более точно отражать вероятность реализации атаки на данный узел. В [10] рассмотрены алгоритмы построения и оптимизации структуры НКК. Нечеткость НКК позволяет включать в модель большое количество переменных с нечеткими значениями. НКК моделируют системы, в которых объем точной информации ограничен, но доступны экспертные знания о причинно-следственных связях концептов. Авторы отмечают, что НКК можно охарактеризовать как интерпретируемые рекуррентные НС, включающие элементы нечеткой логики. В отличие от классических НС, НКК не содержат

Таблица 2

Элементы функциональной модели оценки рисков ИБ

№	Этап	Вход	Выход	Механизм
1	Идентификация активов	Документация на системы и сети	Результаты анализа документации на системы и сети	Эксперты и специалисты по ИБ
2	Идентификация угроз	1.БДУ ФСТЭК России; 2.Открытые базы угроз; 3.Результаты анализа документации на системы и сети	Модель угроз безопасности информации, модель нарушителя	Эксперты и специалисты по ИБ
3	Оценка уязвимостей	пункты; 4.Информация об имеющихся угрозах, модель нарушителя	Информация по уязвимостям	Программное обеспечение по поддержке принятия решения
4	Оценка вероятностей и воздействия	пункты; 5.Информация по уязвимостям	Информация о рисках	Программное обеспечение по поддержке принятия решения
5	Определения уровня рисков	1-5 пункты; 6.Информация о рисках	Информация об уровне рисков	Программное обеспечение по поддержке принятия решения
6	Формирование мер по снижению рисков	6 пункт; 7.Информация об уровне рисков	План по снижению рисков	Эксперты и специалисты по ИБ
7	Мониторинг и обновление	6, 7 пункты; 8.План по снижению рисков	–	Эксперты и специалисты по ИБ

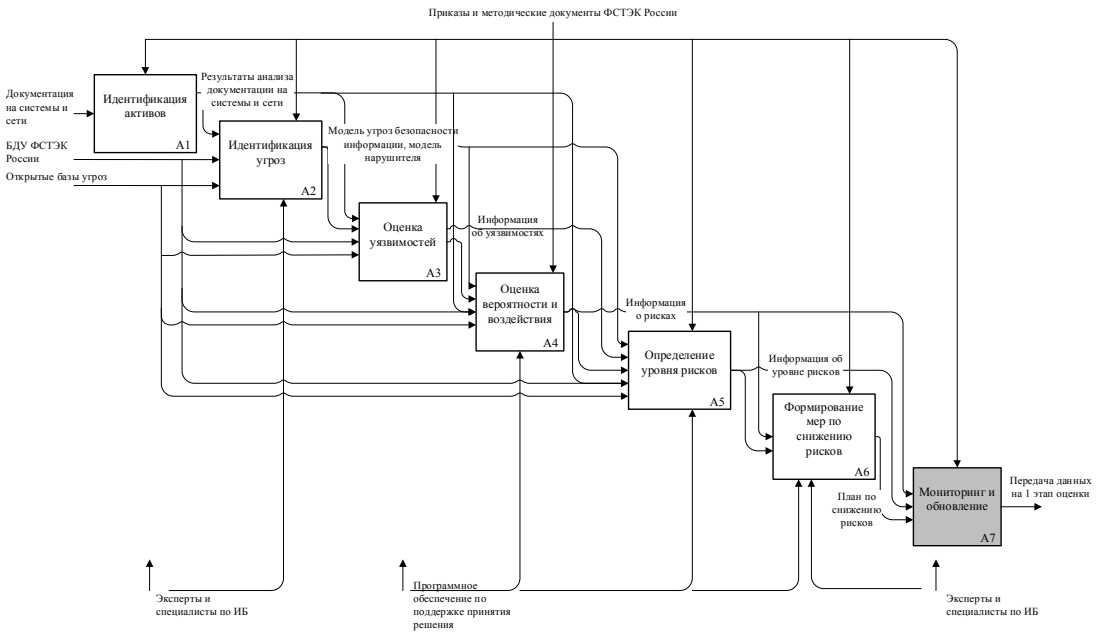

Рис. 1. Функциональная модель оценки рисков ИБ

скрытых нейронов, что позволяет им быть более интерпретируемыми. Однако, существуют проблемы, такие как выбор функции активации и правила обновления, а также сложности с обобщением и интерпретацией НКК. Авторы выделяют несколько актуальных направлений исследований: учет задержки распространения влияния и динамического изменения структуры НКК; создание методов, которые учитывают экспертные знания и ретроспективные данные, а также обнаружение предвзятости в экспертном мнении.

В [11] представлены результаты анализа рисков кибербезопасности с использованием НКК, построенных на основе знаний и опыта экспертов-специалистов. Упоминаются различные типы НКК, связанных с представлением силы связей в виде интервальных оценок: серые, интервально-значные и интуиционистские НКК. Для оценки силы связей между концептами в НКК с учетом возникающей неопределенности во мнениях экспертов при оценке локального риска рассматриваются различные подходы к формализации знаний экспертов, в том числе применение ансамбля НКК. В [12] представлена методика оценки актуальных угроз и уязвимостей, основанная на применении комбинации технологий КМ и Text-Mining. В работе подчеркивается важность автоматизации моделирования сценариев эксплуатации уязвимостей и реализации угроз на основе описания шаблонов компьютерных атак из различных БД и открытых источников. Одним из главных недостатков текущих текстовых описаний безопасности программного и аппаратного обеспечения информационной инфраструктуры является их недостаточная структурированность и фрагментированность. Анализ таких данных требует больших временных затрат и определенных профессиональных навыков.

Таким образом, анализ научных публикаций позволил выделить существующие недостатки в вопросах оценки рисков ИБ и технологий КМ:

– необходимость обработки большого количества данных;

– необходимость правильного формирования источников этих данных: недостаток данных или неправильная представительность обучающей выборки может повлиять на качество модели и ее способность к обобщению на новые данные;

– доступная информация об имеющихся угрозах и уязвимостях недостаточна;

– сложности формального определения функции итогового показателя оценки;

– необходима высокая квалификация экспертов, специалистов по ИБ;

– возможная разрозненность и несогласованность мнений нескольких экспертов;

– Сложность интерпретации топологии НКК и ограничения в возможности комплексной оценки воздействия множества концептов на один узел представляют вызовы в данной области.

В настоящей работе взят вектор на исследование внедрения НКК для снижения рассогласованности и разрозненности мнений экспертов и устранения необходимости работать с большими объемами данных. Для этого предложено модернизировать функциональную модель оценки рисков ИБ, внедрив элементы КМ на этапе «Идентификация угроз», что может помочь качественнее определить концепты, влияющие на эффективность и точность процесса идентификации угроз.

Когнитивное моделирование в адаптивной оценке рисков ИБ

Среди технологий КМ наиболее распространенными являются: сети Байеса; НКК; системы экспертных знаний [9]. НКК обладают определенными преимуществами: удобство использования, визуального восприятия, возможность учитывать неопределённость и нечеткость в процессе оценки рисков, способность изменяться и адаптироваться в соответствии с новыми данными и требованиями. НКК используется для решения задач, связанных с определением и оценкой влияния факторов ситуации, а также для получения прогнозов развития ситуации на основе вычисленных влияний. Основные элементы, необходимые при создании НКК, приведены в таблице 3.

НКК для анализа рисков ИБ является набором множеств:

$$НКК = \{C, F, W\}, \quad (1)$$

где C – множество концептов, F – множество связей между концептами, W – множество весов этих связей.

Чтобы сформировать перечень концептов НКК, были приглашены эксперты университета, преподаватели и специалисты по ИБ в ВУЗе. Основываясь на данных из открытых источников: отчеты по утечкам информации ограниченного доступа, утечкам данных, статистика по киберугрозам, БДУ ФСТЭК России, эксперты сформировали факторы риска (таблица 4), которые могут стать концептами разрабатываемой НКК [13-15].

Из этих данных сформированы концепты и построена НКК (рисунок 2). Ниже приведена матрица ВС НКК, определенная экспертами.

C1 – Управление доступом;

C2 – Конфиденциальность персональных данных студентов;

C3 – Физическая безопасность;

C4 – Сетевая безопасность;

C5 – Мошенничество в области исследований и публикаций;

Таблица 3

Архитектура нечеткой когнитивной карты

№	Элемент НКК	Описание
1.	Узлы	Переменные или концепты, которые моделируются в НКК. Каждый узел имеет свою активацию, отражающую текущее состояние переменной. Узлы могут быть бинарными (0 или 1) или иметь непрерывные значения.
2.	Связи	Взаимодействие между узлами в НКК, определяют направление и силу влияния одного узла на другой. Каждая связь имеет вес, указывающий на важность влияния. Связи могут быть однонаправленными или двунаправленными.
3.	Матрица весов связей (ВС)	Содержит значения ВС между узлами. Представляет собой двумерный массив, где каждый элемент указывает на силу и направление связи между двумя узлами.
4.	Функция активации	Определяет, как изменяется активация узла в зависимости от активаций связанных с ним узлов. Могут использоваться в зависимости от требований моделирования.
5.	Обучение и обновление	В процессе обучения НКК, активации узлов обновляются на основе входных данных и текущих активаций связанных с ними узлов. Это позволяет модели НКК адаптироваться к новым данным и улучшать свою производительность.
6.	Распространение активации	Происходит через связи между узлами, где активация одного узла передается другим узлам, влияя на их активации. Распространение активации может быть односторонним или многосторонним, в зависимости от архитектуры.

Таблица 4

Факторы риска для оценки рисков ИБ в образовательной сфере

№	Фактор риска	Подробнее по фактору
1.	Управление доступом	НСД к системам и данным; Неправильное управление аккаунтами пользователей; Недостаточная защита паролей и учетных записей.
2.	Конфиденциальность данных (персональных данных) студентов	Утечка конфиденциальных данных студентов: личная информация, оценки, финансовая информация; Нарушение правил регулирования в области защиты ПД.
3.	Физическая безопасность	НСД к физическим активам: компьютеры, серверы, хранилища данных, помещения с конфиденциальными документами.
4.	Сетевая безопасность	Атаки на сетевую инфраструктуру, уязвимости в системах, недостаточное обновление и патчинг ПО, атаки на сетевые устройства: маршрутизаторы и коммутаторы.
5.	Мошенничество в области исследований и публикаций	Подделка научных результатов, нарушение правил публикаций, плагиат.
6.	Управление уязвимостями	Недостаточное обнаружение и исправление уязвимостей в системах и приложениях, неправильная конфигурация сетевого оборудования.
7.	Социальная инженерия	Манипуляции для получения конфиденциальных данных или выполнения нежелательных действий путем обмана персонала или студентов.
8.	Отказ в обслуживании (DoS)	Атаки на системы, направленные на перегрузку ресурсов и приведение к отказу в обслуживании.
9.	Безопасность мобильных устройств	Утеря или кража мобильных устройств с конфиденциальной информацией, уязвимости мобильных приложений.
10.	Обучение и осведомленность	Недостаточное обучение персонала и студентов в области ИБ, недостаточное осведомление о правилах безопасного поведения в сети.

С6 – Управление уязвимостями;
С7 – Социальная инженерия;
С8 – Отказ в обслуживании (DoS);
С9 – Безопасность мобильных устройств;
С10 – Обучение и осведомленность.

Матрица W с экспертными оценками ВС, в которой принималось с = 1, имеет следующий вид:

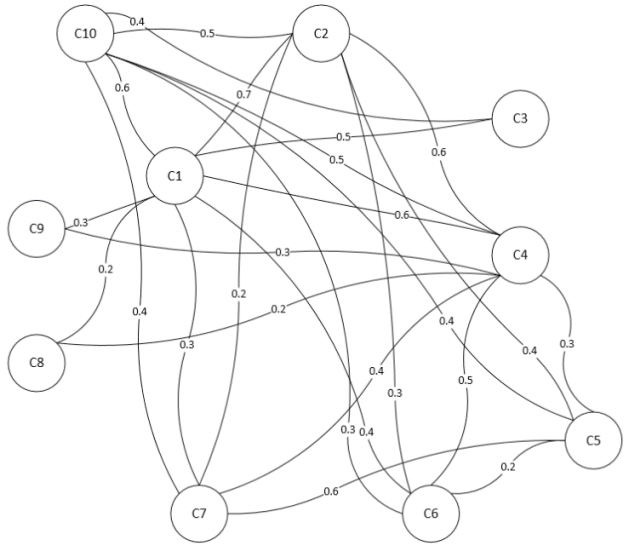

Рис. 2. НКК модели пространства рисков

$$W = \begin{bmatrix} 1 & 0.7 & 0.5 & 0.6 & 0 & 0.4 & 0.3 & 0.2 & 0.3 & 0.6 \\ 0.7 & 1 & 0 & 0.6 & 0.4 & 0.3 & 0.2 & 0 & 0 & 0.5 \\ 0.5 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0.4 \\ 0.6 & 0.6 & 0 & 1 & 0.3 & 0.5 & 0.4 & 0.2 & 0.3 & 0.5 \\ 0 & 0.4 & 0 & 0.3 & 1 & 0.2 & 0.6 & 0 & 0 & 0.4 \\ 0.4 & 0.3 & 0 & 0.5 & 0.2 & 1 & 0 & 0 & 0 & 0.3 \\ 0.3 & 0.2 & 0 & 0.4 & 0.6 & 0 & 1 & 0 & 0 & 0.4 \\ 0 & 0 & 0 & 0.4 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0.3 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0.6 & 0.5 & 0.4 & 0.5 & 0.4 & 0.3 & 0.4 & 0 & 0 & 1 \end{bmatrix}$$

Сформирована НКК и матрица ВС для одного из этапов оценки рисков ИБ, которая показывает, какие факторы могут иметь высокое или низкое значение при оценке рисков ИБ конкретно в имеющейся ситуации. При формировании этой НКК автоматически, мы получаем возможность адаптивно оценивать риски ИБ, приспосабливаясь к изменяющимся условиям. Ключевым моментом является корректное определение ВС, чаще всего это происходит в виде экспертной оценки. Но при росте количества концептов данный подход усложняется, и повышается вероятность субъективных ошибок. Для решения этой проблемы можно использовать автоматическую подстройку весов связей с помощью нейронных сетей (НС). В [16] рассмотрено обучение НКК с помощью нейросетевого подхода. Смысл данного подхода в том, чтобы позволить ВС изменяться так, будто они являются синапсами НС. Дальнейшее исследование направлено на применение нейронных сетей в оценке ВС НКК.

Заключение

Результаты проведенного анализа ГОСТов, международных стандартов, методик, освещающих вопросы оценки рисков ИБ, позволили сформировать функциональную модель оценки рисков ИБ, реализующую статический подход. В процессе исследования были обнаружены проблемные моменты такого подхода: сложность проведения оценки рисков за счет необходимости высоких компетенций экспертов, возможная рассогласованность и разрозненность их мнений, большие объемы входных данных, что усложняет и значительно замедляет сам процесс оценки рисков. Для устранения этого предложено применение технологий КМ, а именно НКК, для придания процессу оценки рисков ИБ

свойств адаптивности, что способствует более быстрой адаптации модели оценки к изменяющимся условиям.

Предложено внедрить на одном из этапов функциональной модели оценки рисков ИБ – «Идентификация угроз» НКК, содержащую в себе концепты по возможным угрозам ИБ в образовательной сфере. Были приглашены 10 экспертов ВУЗа из области ИБ: преподаватели, специалисты по ЗИ. Опираясь на открытые источники данных: отчеты компаний, занимающихся вопросами ИБ, статистика утечек данных за крайние годы, БДУ ФСТЭК России, а также на свой опыт, эксперты сформировали 10 концептов для НКК в сфере образования, а также расставили ВС между ними. Предложен задел для обучения НС расставлять ВС автоматически. Дальнейшее развитие данного исследования заключается в проведении экспериментов по созданию и обучению НС выставлять ВС, подбора оптимальной архитектуры НС, размерности слоев с целью подбора наиболее оптимальной версии, а также поиск других блоков из предложенной функциональной модели, в которых можно использовать такую комбинацию технологий как НС и КМ.

Литература

1. ISO/IEC 31010:2019 Менеджмент риска. Принципы и руководство. 2019.

2. ГОСТ Р ИСО/МЭК 31010-2011. Менеджмент риска. Методы оценки риска. 2011. – 4 с.

3. ГОСТ Р № ИСО/МЭК 27001-2021 от 01.01.2022. Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования. 2022.

4. ISO 27001 Системы менеджмента информационной безопасности. 2021.

5. ISO/IEC 27005:2018 «Информационные технологии. Методы обеспечения безопасности. Менеджмент рисков информационной безопасности». 2018.

6. Фомин Г. П., Сухорукова И. В., Грибов А. Ф Адаптивная многокритериальная система управления рисками/ Вестник ростовского государственного экономического университета (РИНХ), 2022. № 1 (77). С. 98-103. URL: https://www.elibrary.ru/item.asp?id=49424923 (дата обращения 30.06.2023 г.)

7. Глушенко С. А. Адаптивная нейро-нечеткая система оценки рисков информационной безопасности организации/ Бизнес-информатика, 2017. № 1 (39). С. 68-77. URL: https://bijournal.hse.ru/data/2017/08/30/1173956328/%D0%93%D0%BB%D1%83%D1%88%D0%B5%D0%BD%D0%BA%D0%BE%20%D0%A0%D0%A3%D0%A1%D0%9F%D0%95%D0%A0%D0%95%D0%92%D0%9E%D0%94%20-%20v2F.pdf (дата обращения 30.06.2023 г.)

8. Джамай Е. В., Зинченко А. С. Разработка адаптивной многокомпонентной системы управления риском высокотехнологичных предприятий/ Вестник Московского государственного областного университета. Серия: Экономика, 2022. № 2. URL: https://cyberleninka.ru/article/n/razrabotka-adaptivnoy-mnogokomponentnoy-sistemy-upravleniya-riskom-vysokotehnologichnyh-predpriyatiy (дата обращения 30.06.2023 г.)

9. 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 ИСА РАН, 2019. № 4. Том 69. URL: http://www.isa.ru/proceedings/images/documents/2019-69-4/62-69.pdf (дата обращения 25.07.2023 г.)

10. Петухова А. В., Коваленко А. В., Теунаев Д. М. Обзор динамических свойств и алгоритмов обучения нечетких когнитивных карт/ Политематический сетевой электронный научный журнал Кубанского государственного аграрного университета, 2021. № 163. Том 3. URL: https://cyberleninka.ru/article/n/obzor-dinamicheskih-svoystv-i-algoritmov-obucheniya-nechetkih-kognitivnyh-kart (дата обращения 28.07.2023 г.)

11. Васильев В. И., Вульфин А. М., Герасимова И. Б., Картак В. М. Анализ рисков кибербезопасности с помощью нечетких когнитивных карт/DOI:10.21681/2311-3456-2020-2-11-21. URL: https://cyberrus.com/wp-content/uploads/2020/06/11-21-236-20_2.-Vasilyev.pdf (дата обращения 28.07.2023 г.)

12. Васильев В. И., Вульфин А. М., Кириллова А. Д., Кучкарова Н. В. Методика оценки актуальных угроз и уязвимостей на основе технологий когнитивного моделирования и Text Mining/ Системы управления, связи и безопасности, 2021. № 3. URL: https://cyberleninka.ru/article/n/metodika-otsenki-aktualnyh-ugroz-i-uyazvimostey-na-osnove-tehnologiy-kognitivnogo-modelirovaniya-i-text-mining (дата обращения 29.07.2023 г.)

13. Отчет об исследовании утечек информации ограниченного доступа в I половине 2022 года.

Экспертно-аналитический центр InfoWatch. 2022 г. URL: https://www.infowatch.ru/sites/default/files/analytics/files/otchyot-ob-utechkakh-dannykh-za-1-polugodie-2022-goda_1.pdf (accessed: 12.09.2023)

14. Утечки данных. TAdviser. 2022. URL: https://www.tadviser.ru/index.php/%D0%A1%D1%82%D0%B0%D1%82%D1%8C%D1%8F:%D0%A3%D1%82%D0%B5%D1%87%D0%BA%D0%B8_%D0%B4%D0%B0%D0%BD%D0%BD%D1%8B%D1%85 (accessed: 16.09.2023)

15. Актуальные киберугрозы: I квартал 2022 года. Positive Technologies. URL: https://www.ptsecurity.com/ru-ru/research/analytics/cybersecurity-threatscape-2022-q1/ (accessed: 17.09.2023)

16. Ефремова Н. А., Аверкян А. Н., Ярушев С. А. Гибридные нечеткие когнитивные карты в задачах поддержки принятия решений и прогнозирования/ Software journal theory and applications, 2017. № 4. DOI: 10.15827/2311-6749.25.291 URL: http://swsys-web.ru/hybrid-fuzzy-cognitive-maps-in-decision-support-tasks.html (дата обращения 19.09.2023 г.)

References

1. ISO/IEC 31010:2019 Menedzhment riska. Printsipy i rukovodstvo. 2019.

2. GOST R ISO/MEK 31010-2011. Menedzhment riska. Metody otsenki riska. 2011. – 4 s.

3. GOST R № ISO/MEK 27001-2021 ot 01.01.2022. Informatsionnaya tekhnologiya. Metody i sredstva obespecheniya bezopasnosti. Sistemy menedzhmenta informatsionnoy bezopasnosti. Trebovaniya. 2022.

4. ISO 27001 Sistemy menedzhmenta informatsionnoy bezopasnosti. 2021.

5. ISO/IEC 27005:2018 «Informatsionnyye tekhnologii. Metody obespecheniya bezopasnosti. Menedzhment riskov informatsionnoy bezopasnosti». 2018.

6. Fomin G. P., Sukhorukova I. V., Gribov A. F Adaptivnaya mnogokriterial'naya sistema upravleniya riskami/ Vestnik rostovskogo gosudarstvennogo ekonomicheskogo universiteta (RINKH), 2022. № 1 (77). S. 98-103. URL: https://www.elibrary.ru/item.asp?id=49424923 (data obrashcheniya 30.06.2023 g.) 7. Glushenko S. A. Adaptivnaya neyro-nechetkaya sistema otsenki riskov informatsionnoy bezopasnosti organizatsii/ Biznes-informatika, 2017. № 1 (39). S. 68-77. URL: https://bijournal.hse.ru/data/2017/08/30/1173956328/%D0%93%D0%BB%D1%83%D1%88%D0%B5%D0%BD%D0%BA%D0%BE%20%D0%A0%D0%A3%D0%A1%D0%9F%D0%95%D0%A0%D0%95%D0%92%D0%9E%D0%94%20-%20v2F.pdf (data obrashcheniya 30.06.2023 g.)

8. Dzhamay Ye. V., Zinchenko A. S. Razrabotka adaptivnoy mnogokomponentnoy sistemy upravleniya riskom vysokotekhnologichnykh predpriyatiy/ Vestnik Moskovskogo gosudarstvennogo oblastnogo universiteta. Seriya: Ekonomika, 2022. № 2. URL: https://cyberleninka.ru/article/n/razrabotka-adaptivnoy-mnogokomponentnoy-sistemy-upravleniya-riskom-vysokotehnologichnyh-predpriyatiy (data obrashcheniya 30.06.2023 g.)

9. Guzairov M. B., Vul'fin A. M., Kartak V. M., Kirillova A. D., Mironov K. V. Sravnitel'nyy analiz algoritmov kognitivnogo modelirovaniya pri otsenke riskov informatsionnoy bezopasnosti/ Trudy ISA RAN, 2019. № 4. Tom 69. URL: http://www.isa.ru/proceedings/images/documents/2019-69-4/62-69.pdf (data obrashcheniya 25.07.2023 g.)

10. Petukhova A. V., Kovalenko A. V., Teunayev D. M. Obzor dinamicheskikh svoystv i algoritmov obucheniya nechetkikh kognitivnykh kart/ Politematicheskiy setevoy elektronnyy nauchnyy zhurnal Kubanskogo gosudarstvennogo agrarnogo universiteta, 2021. № 163. Tom 3. URL: https://cyberleninka.ru/article/n/obzor-dinamicheskih-svoystv-i-algoritmov-obucheniya-nechetkih-kognitivnyh-kart (data obrashcheniya 28.07.2023 g.)

11. Vasil'yev V. I., Vul'fin A. M., Gerasimova I. B., Kartak V. M. Analiz riskov kiberbezopasnosti s pomoshch'yu nechetkikh kognitivnykh kart/DOI:10.21681/2311-3456-2020-2-11-21. URL: https://cyberrus.com/wp-content/uploads/2020/06/11-21-236-20_2.-Vasilyev.pdf (data obrashcheniya 28.07.2023 g.)

12. Vasil'yev V. I., Vul'fin A. M., Kirillova A. D., Kuchkarova N. V. Metodika otsenki aktual'nykh ugroz i uyazvimostey na osnove tekhnologiy kognitivnogo modelirovaniya i Text Mining/ Sistemy upravleniya, svyazi i bezopasnosti, 2021. № 3. URL: https://cyberleninka.ru/article/n/metodika-otsenki-aktualnyh-ugroz-i-uyazvimostey-na-osnove-tehnologiy-kognitivnogo-modelirovaniya-i-text-mining (data obrashcheniya 29.07.2023 g.)

13. Otchet ob issledovanii utechek informatsii ogranichennogo dostupa v I polovine 2022 goda. Ekspertno-analiticheskiy tsentr InfoWatch. 2022 g. URL: https://www.infowatch.ru/sites/default/files/analytics/files/otchyot-ob-utechkakh-dannykh-za-1-polugodie-2022-goda_1.pdf (accessed: 12.09.2023)

14. Utechki dannykh. TAdviser. 2022. URL: https://www.tadviser.ru/index.php/%D0%A1%D1%82%D0%B0%D1%82%D1%8C%D1%8F:%D0%A3%D1%82%D0%B5%D1%87%D0%BA%D0%B8_%D0%B4%D0%B0%D0%BD%D0%BD%D1%8B%D1%85 (accessed: 16.09.2023)

15. Aktual'nyye kiberugrozy: I kvartal 2022 goda. Positive Technologies. URL: https://www.ptsecurity.com/ru-ru/research/analytics/cybersecurity-threatscape-2022-q1/ (accessed: 17.09.2023)

16. Yefremova N. A., Averkyan A. N., Yarushev S. A. Gibridnyye nechetkiye kognitivnyye karty v zadachakh podderzhki prinyatiya resheniy i prognozirovaniya/ Software journal theory and applications, 2017. № 4. DOI: 10.15827/2311-6749.25.291 URL: http://swsys-web.ru/hybrid-fuzzy-cognitive-maps-in-decision-support-tasks.html (data obrashcheniya 19.09.2023 g.)

ПАЛЮТИНА Галия Наилевна, аспирант, младший научный сотрудник Федерального государственного бюджетного образовательного учреждения высшего образования «Ростовский государственный экономический университет (РИНХ)». 344002, г. Ростов-на-Дону, ул. Большая Садовая, д. 69. E-mail: hello616@yandex.ru

PALYUTINA Galiya Nailevna, postgraduate student, junior researcher at the Federal State Budgetary Educational Institution of Higher Education "Rostov State Economic University (RINH)". 344002, Rostov-on-Don, st. Bolshaya Sadovaya, 69. E-mail: hello616@yandex.ru