DOI: 10.18721/JE.13502
УДК 336.6

СОЗДАНИЕ СИСТЕМЫ УПРАВЛЕНИЯ ЭКОНОМИЧЕСКИМ РИСКОМ С ИСПОЛЬЗОВАНИЕМ ИСКУССТВЕННЫХ НЕЙРОННЫХ СЕТЕЙ

Слепцова Ю.А.[1], Качалов Р.М.[1], Шокин Я.В.[2]

[1] Центральный экономико-математический институт РАН, Москва, Российская Федерация;

[2] Государственный университет «Дубна», Московская обл., Российская Федерация

При избытке и, в то же время, фрагментарности информации в современной экономике система управления уровнем риска предприятия и его социально-экономической экосистемы должна опираться на такие цифровые технологии, при использовании которых можно получить выигрыш во времени для оценки и анализа изменений в окружающей экономической среде. Цель настоящей статьи — сформулировать базовые подходы к созданию системы управления уровнем риска, в том числе процессов идентификации, оценки и минимизации уровня риска при подготовке управленческих решений, разработанных с помощью искусственных нейронных сетей. Используя методы операциональной теории управления уровнем риска, системной экономической теории и теории алгоритмов, в частности, искусственных нейронных сетей, и моделирования иммунного ответа, в данном исследовании показано, что система управления уровнем риска современного предприятия и его социально-экономической экосистемы будет опираться на принципы функционирования иммунной системы по аналогии с подобными системами в живых организмах. Процессы управления экономическим риском моделируются в рамках четырех основных трансграничных подсистем: интенциональной, экспектационной, когнитивной и функциональной. Выделены принципы, соблюдение которых необходимо для корректного использования искусственных нейронных сетей в подготовке управленческих решений и для накопления информации об уровне возможного риска. Показано, что для широкого применения аппарата искусственных нейронных сетей в системе управления предприятием необходимо достичь определенного уровня развития применяемых цифровых технологий. Показано, что для создания специализированной операционной системы управления уровнем риска индустриального интернета вещей (IoT) предприятия или цифровой многосторонней бизнес-платформы в целом может потребоваться отдельная цифровая экосистема. Представленное исследование может оказаться полезным для специалистов и руководителей предприятий при создании систем управления уровнем риска и систем поддержки принятия управленческих решений с использованием алгоритмов искусственных нейронных сетей. Ограничением применения полученных результатов является недостаточное развитие базового уровня информационных технологий на предприятии.

Ключевые слова: система управления уровнем риска, интенциональная, экспектационная, когнитивная и функциональная подсистемы, факторы риска, антирисковые управленческие воздействия, искусственные нейронные сети

Ссылка при цитировании: Слепцова Ю.А., Качалов Р.М., Шокин Я.В. Создание системы управления экономическим риском с использованием искусственных нейронных сетей // Научно-технические ведомости СПбГПУ. Экономические науки. 2020. Т. 13, № 5. С. 24–37. DOI: 10.18721/JE.13502

CREATION OF AN ECONOMIC RISK MANAGEMENT SYSTEM USING ARTIFICIAL NEURAL NETWORKS

Yu.A. Sleptsova[1], R.M. Kachalov[1], Ya.V. Shokin[2]

[1] Central Economics and Mathematics Institute of the RAS,
Moscow, Russian Federation;

[2] Dubna State University,
Moscow region, Russian Federation

Due to the abundance and fragmentation of information in the digital economy, the risk management system of an enterprise and its socio-economic ecosystem should rely on such digital technologies, which can be used to gain time to assess and analyze changes in the economic environment. The purpose of this article is to formulate basic approaches to creating a risk level managerial system, including processes for identifying, evaluating and minimizing the risk level in management decision-making developed using artificial neural networks. Using the methods of operational risk management theory, system economic theory, algorithm theory, in particular, artificial neural networks, and immune response modeling, this study shows that the risk management system of a modern enterprise and its socio-economic ecosystem will be based on the principles of functioning of the immune system by analogy with similar systems in living organisms. We model economic risk management processes within four main interacting subsystems: intentional, expectational, cognitive, and functional. The principles that must be observed for the correct use of artificial neural networks in decision-making and for the accumulation of information about the level of possible risk are highlighted. For wide application of artificial neural networks in enterprises, it is necessary to reach a certain level in digital technologies. It is shown that to create a specialized operating system for managing the risk level of an industrial Internet of things (IoT), enterprise or a digital multi-party business platform as a whole may require a separate digital ecosystem. The presented research may be useful for specialists and managers of enterprises when creating risk management systems and management decision support systems using artificial neural network algorithms. The lack of development of the basic level of information technologies at an enterprise limits the application of the results obtained.

Keywords: risk level managerial system, intentional, expectational, cognitive and functional subsystems, risk factors, anti-risk impact actions, artificial neural networks

Citation: Yu.A. Sleptsova, R.M. Kachalov, Ya.V. Shokin, Creation of an economic risk management system using artificial neural networks, St. Petersburg State Polytechnical University Journal. Economics, 13 (5) (2020) 24–37. DOI: 10.18721/JE.13502

Введение

С появлением новых цифровых технологий отчасти происходит проникновение технического знания к рядовым пользователям — помимо прочего, с точки зрения организационной структуры. Это приводит к тому, что происходит переход от так называемого дисциплинарного общества к «обществу контроля» [1]. Каждый сотрудник предприятия или единица оборудования становятся источником генерирования разнообразных данных, что приводит к сочетанию двух как бы противоположных феноменов: с одной стороны, ощущения практически безграничных возможностей в цифровой среде, а, с другой стороны, глобального контроля любого действия человека в сети со стороны заинтересованных лиц. Использование искусственных нейронных сетей (ИНС) подразумевает развитие таких алгоритмических методов прогнозирования, которые могли бы способствовать повышению качества принимаемых управленческих решений. Но надо заметить, что, в случае применения инструментария ИНС, получаемое техническое знание не может быть исключительно рациональным, поэтому вопрос о возможности следования этическим нормам при принятии решений с помощью ИНС может рассматриваться как предмет отдельной дискуссии [2].

В процессе подготовки управленческих решений могут быть идентифицированы следующие факторы риска стратегических решений, подготовленных при помощи искусственных нейронных сетей: увеличение неравенства между людьми, нарушение прав сотрудников или необоснованное расширение их обязанностей [3]. Другими словами, совершенствование социальных институтов в области взаимоотношения между людьми и создания нового знания могут не успевать за логикой эволюции цифровых технологий. В результате цифровые технологии развиваются в отсутствии необходимого знания об этих технологиях, позволяющего контролировать обоснованность сделанного алгоритмом выбора [4].

Технологический дизайн искусственной нейронной сети опирается на стохастическое знание, т.е. используемые в этих сетях алгоритмы работают со случайными процессами, например, с цепью Маркова. Они моделируют усредненное поведение экономических агентов по образцу, предложенному в обучающей выборке, и разрабатывают на основании этого прогнозы. В процессе настройки алгоритм ИНС не подбирает целевую функцию задачи, а формирует некоторое множество функций, которые реализуются этой совокупностью экономических агентов и генерируют некоторый набор значений, близкий к заданному обучающей выборкой. Поэтому важно, чтобы обучающая выборка формировалась для задачи, решаемой именно данной искусственной нейронной сетью [5].

Таким образом, если обучающую выборку формирует один специалист, то эта выборка может быть ограничена его опытом и знанием. Если же обучающая выборка генерируется автоматически с помощью специализированных алгоритмов, то она может содержать избыточную информацию, так называемый «шум», поэтому на практике лучше использовать опыт и знание нескольких экспертов или фильтры, представляющие собой специализированные программные комплексы первичной обработки данных, которые подавляют шумовые помехи.

Алгоритмы ИНС концептуально имитируют работу нейронных сетей в мозгу человека, по аналогии с этим можно рассмотреть иммунную систему живого организма и перенести принципы ее функционирования в систему управления уровнем риска в деятельности как отдельного предприятия, так и его предпринимательской экосистемы. Использование понятия «иммунитет» в гуманитарных науках не является чем-то принципиально новым. Например, оно используется в политическом и в юридическом смысловых полях, в дипломатии и юриспруденции, где под иммунитетом понимается изъятие из-под конкретной юрисдикции [6]. Понятие «иммунитет» в дальнейшем может иметь ключевое значение в становлении новой теории управления уровнем риска в цифровых социально-экономических экосистемах.

Постановка задачи

Непредвиденные события наступают неожиданно и могут допускать неоднозначную трактовку, т.е. могут быть рассмотрены, с одной стороны, как возможности для бизнеса предприятия, а, с другой стороны, как препятствие для достижения поставленных целей, так называемые «черные лебеди» [7]. Но времени на принятие позитивного управленческого решения может оказаться недостаточно, поэтому система управления уровнем риска в деятельности предприятия должна опираться на такие цифровые технологии, которые позволят получить выигрыш во времени для оценки и анализа сложившейся ситуации риска. Таким образом, проблема настоящего исследования состоит в том, насколько бизнес-процессы с использованием искусственных нейронных сетей в системе управления уровнем риска в деятельности предприятия могут быть настроены аналогично процессам в модели адаптивного иммунного ответа в живом организме [8].

Объектом настоящего исследования является управление уровнем риска на современном предприятии в условиях цифровизации внешней среды, предметом исследования — процессы управления уровнем риска.

Цель исследования — сформулировать основные подходы к созданию системы управления уровнем риска, в том числе процессов идентификации, оценки и минимизации уровня риска при подготовке управленческих решений, разработанных с помощью ИНС, для прогнозирования и анализа последствий их реализации для деятельности предприятия.

Методика исследования

Данная работа опирается на методы операциональной теории управления уровнем риска, системной экономической теории и теории алгоритмов, в частности, искусственных нейронных сетей, и методы моделирования иммунного ответа. Операциональная теория управления уровнем риска выделяет основные структурные составляющие процесса управления риском, использованные в данной работе, а именно, ситуацию риска, факторы риска, уровень риска, антирисковые управленческие воздействия [9,10].

На основании системной экономической теории в структуре системы управления предприятия выделяют четыре основные трансграничные подсистемы, каждая из которых соответствующим образом взаимодействует с предпринимательской экосистемой этого предприятия [11]:

- *интенциональная подсистема*, включающая в себя все процессы, связанные с формированием и анализом актуальности целей деятельности предприятия;
- *экспектационная подсистема*, формирующая ожидания относительно реакций внешней среды на те или иные действия или события, инициированные подразделениями предприятия;
- *когнитивная подсистема*, отвечающая за процессы формирования базы знаний о предприятии и его предпринимательской экосистеме;
- *функциональная подсистема*, отвечающая за действия, необходимые для выполнения системой своего целевого назначения.

Также эти четыре трансграничные подсистемы используются для организации системы управления данными, созданной для описания процедурных норм и правил, обеспечивающих надлежащее хранение и конфиденциальность данных, собираемых предприятием. Использование многослойных нейронных сетей позволяет включить создание функций в процесс обучения ИНС, тем самым резко увеличивая их производительность [12].

Взаимодействие этих подсистем реализует, соответственно, четыре стороны функционирования предприятия: плановую, прогнозную, информационную и операционную.

Главной особенностью моделей с использованием ИНС является построение системы рассуждений непосредственно на основе большого массива данных, без явных правил генерации результата процесса. Универсальность этих моделей делает их очень привлекательными для широкого спектра применений. Кроме того, исследователи ИНС с самого начала приняли открытый подход к сотрудничеству и распространению большого набора ресурсов: от программного обеспечения с открытым кодом до наборов данных, документации, свободно доступных каждому. Этот подход способствовал росту популярности алгоритмов ИНС в научных и инженерных сообществах и использованию преимуществ огромных объемов данных, собранных в цифровых системах. В то же время, со стороны пользователей возникли конкретные требования предоставлять понятные разъяснения при автоматизированном принятии решений без участия человека [13].

Методы обучения ИНС адаптированы для изучения новых видов представления данных, которые являются более компактными и более информативными и подходят для решения задач, связанных с классификацией, распознаванием, генерацией данных и т. д.

Обучение ИНС состоит из набора математических методов, объединяющих различные алгоритмические языки, теории статистического обучения и оптимизации. Цель такого объединения заключается в том, что информация для решения проблем извлекается из множества видов данных (изображений, записи датчиков, текстов и т. д.), что обычно происходит в условиях одной из трех типов парадигмальных сред [14]:

- в контролируемой среде каждый пример включает в себя метку, которая может быть категориальной или скалярной, причем для входного набора данных модель настроена на предсказание правильного обозначения или класса такой метки;

- в условиях неконтролируемой (или самоконтролируемой) среды маркировка не предусмотрена, модель ориентирована на изучение нового представления данных, группирующего примеры на основе их сходства;

- последняя группа методов обучения, так называемое обучение с подкреплением, при которых модель обучается выполнять сложную последовательность действий автономно в сложной среде.

Методы контролируемой среды при обучении ИНС являются преобладающими и, в основном, применяются для систем принятия решений. Например, в банках методы ИНС используются в маркетинговых целях. На основании операций, сделанных клиентами, извлекаются несколько предопределенных атрибутов: количество платежей в день, общая сумма расходов в день и т. д. На основе этих данных ИНС классифицируют клиентов в различные категории в зависимости от их поведенческой деятельности, эти категории затем используются для разработки индивидуальных маркетинговых стратегий. Фактором риска для клиента при применении таких стратегий может быть его «оппортунистическое» поведение, которое не позволит ему претендовать на выгодные условия сотрудничества с банком [15].

Модели ИНС по своей природе более сложны, чем классические системы принятия решений, так как они обладают нелинейной системой обратной связи между алгоритмом и набором данных, которые вместе составляют модель обучения, действующей как настоящая система рассуждений, выводящая прогнозы на основе входных данных в совокупности с прогнозами, сделанными на предыдущей итерации [16]. Эта модель затем встраивается в более традиционный программный комплекс, нередко в сочетании с другими частями кода или программного обеспечения, архитектура которого реализуется с использованием инструментов программирования, отличных от тех, которые использовались для разработки моделей ИНС. Если эти системы вводятся небрежно, то целостность всей архитектуры системы может оказаться под угрозой, так как результаты контроля безопасности теряют свою адекватность.

Особенностью моделей ИНС является их сервисный характер, что приводит к необходимости косвенного оценивания их эффективности через терминальный положительный эффект воздействия на предприятие, в интересах которого данная система была создана или адаптирована [17]. В качестве критерия оценки эффективности модели ИНС может быть использована возможность превышения достигнутого положительного эффекта минимального порогового значения, которое можно трактовать как вероятность успешного выполнения стоящей перед моделью ИНС задачи.

Методы построения моделей иммунного ответа, описывающие иерархически сложную иммунную систему, которые используются в биологии для выявления антигенов (генетически чужеродных агентов) и их уничтожения или для нейтрализации их патогенного действия, совместно с методами ИНС могут быть также применены для идентификации факторов риска, оценки уровня риска и разработки антирисковых управленческих воздействий в условиях цифрового взаимодействия в системе управления уровнем риска в деятельности предприятия и его предпринимательской экосистемы [8].

Результаты исследования

Проведенное исследование позволяет предложить новую структуру системы управления уровнем риска, основанную на приведенной выше структуре системы управления предприятием, которая включает в свой состав четыре трансграничные подсистемы: *интенциональную*, *экспектационную*, *когнитивную* и *функциональную*. Рассмотрим теперь каждую из этих подсистем в контексте системы управления уровнем риска.

А) *Интенциональная подсистема* системы управления уровнем риска предприятия охватывает намерения относительно будущей деятельности предприятия и включает в себя описание желаемых результатов в соответствии с целями предприятия. Описание целей помогает сократить время, необходимое для принятия последующих управленческих решений, например, увеличение объемов продаж или завоевание доли рынка (в количественных показателях). Если цели не сформулированы корректно и точно, то выработка антирискового управленческого решения может занять неограниченный период времени, поскольку каждый участник процесса принятия решения не будет проинформирован о том, какой результат необходимо достичь за определенный период деятельности. В связи с этим следует заметить, что на качество формирования целей предприятия (и косвенно на проявление факторов риска) значительное влияние оказывают мотивация руководителей предприятия, а также принятые на предприятии — в рамках сложившейся культуры управления риском — традиции определения стратегических целей и способы их реализации [18].

Б) В рамках *экспектационной подсистемы* использование моделей ИНС для прогнозирования может быть затруднено недостаточной интерпретируемостью применения аппарата ИНС. Следует обратить внимание на то, что для прогнозирования с помощью моделей ИНС существует два подхода.

При использовании первого подхода идентификация факторов риска осуществляется на каждом этапе обработки данных в процессе обучения ИНС. При этом этапы обработки данных при обучении ИНС на специальной выборке данных включают:

- описание функций, использующихся для получения результатов; логика модели может быть основана на правилах, полученных в результате сравнения значений признаков, на линейных или нелинейных операциях этих функций;
- описание вида данных, которые предполагается использовать в модели, включая границы пространства ввода; надо отметить, что наборы данных часто содержат смещения, которые могут оказать сильное влияние на результаты;
- описание способов принятия решения с использованием выходных значений в задачах классификации факторов риска.

Второй подход фокусируется на предоставлении объяснения прогноза, сделанного с помощью алгоритма ИНС на основе конкретных входных данных и выделения наиболее значимых параметров решения или путем формулирования специальных пояснений, которые будут показывать, на каких признаках следует сосредоточиться, чтобы изменить решение. Например, в случае кредитного скоринга поясняется, какие требования не были выполнены клиентом, чье заявление было отклонено [19].

В) К факторам риска *когнитивной подсистемы* системы управления уровнем риска можно отнести фактор риска смещения характеристик массива входных данных, обусловленных наличием ограниченного множества примеров в обучающей выборке данных, которое не отражает разнообразие и сложность ситуаций, т.е. обучающая выборка данных фактически не описывает реальное количество всех возможных вариантов. Это означает, что хороших результатов на очевидных примерах недостаточно для оценки способности модели ИНС правильно обрабатывать более неоднозначные ситуации [20].

В рамках когнитивной подсистемы выделены три принципа, соблюдение которых важно для корректного использования ИНС при подготовке управленческих решений и для накопления знаний об уровне возможного риска:

- *прозрачность моделей ИНС*, подразумевающая формирование подробной документации и цепочек обработки информации, включая описание данных, использованных в модели;
- *надежность моделей ИНС*, которая касается избегания сбоев или неисправностей, возникающих по причине либо форс-мажора, либо некорректности обучающей выборки;

• *защита данных в моделях ИНС*, подразумевающая безопасность и конфиденциальность данных, например, персональных данных.

Г) Управление уровнем риска и реализация антирисковых управленческих воздействий строится с помощью надлежащего организационного и технического контроля в рамках *функциональной подсистемы* системы управления уровнем риска. Функциональная подсистема включает оценку существенных изменений деятельности предприятий, мониторинг факторов риска. В эту же подсистему могут быть включены процедуры привлечения, развития и удержания квалифицированных сотрудников предприятия. Использование цифровых технологий, и, в частности, инструментов искусственных нейронных сетей позволит в рамках функциональной подсистемы системы управления уровнем риска перейти к проактивному управлению уровнем риска.

В отличие от традиционно используемого на практике реактивного управления, базирующегося на оперативном реагировании на негативные события и последующей компенсации негативных последствий, проактивное управление уровнем риска предполагает предотвращение возникновения инцидентов за счет создания в соответствующей системе управления уровнем риска принципиально новых упреждающих возможностей —например, параметрической адаптации моделей ИНС к прошлому, настоящему и будущему при формировании и реализации антирисковых управленческих воздействий на основе парирования не следствий, а причин, вызывающих ситуации риска и, соответственно, негативные события и их последствия на предприятии [21].

Схематически структура системы управления уровнем риска изображена на рис. 1.

В результате проведенного исследования также показано, что становление таких явлений, как индустриальный интернет вещей (Internet of Things, IoT), беспилотный транспорт, онлайн-банкинг, т.е. внедрение цифровых технологий в различных отраслях экономики обусловливает появление факторов риска некорректной реализации алгоритмов, в частности, ИНС, и может причинить не только экономический ущерб, но и инициировать угрозы жизни и здоровью людей — в первую очередь, работников предприятий, потребителей и т.п. Принципиальная схема архитектуры цифровой системы управления риском IoT или индустриального интернета вещей на производственном предприятии включает в себя датчики, сбор данных, коммуникации типа M2M — процессы обмена информацией между машинами и механизмами, и облачные хранилища [22].

На более ранних этапах развития информационных технологий при автоматизации производственных и бизнес-процессов на предприятиях компьютерная безопасность была частью системы управления уровнем риска. Если рассматривать предприятия различных отраслей экономики, например, крупный банк или большое производственное предприятие, то наборы факторов риска, связанных с компьютерной безопасностью, у таких компаний были разные, хотя

Рис. 1. Структура системы управления уровнем риска.
Fig. 1. Structure of the risk level management system

количество сотрудников и подразделений могло совпадать, так как по-разному были устроены информационные потоки и информационные системы [23]. Ключи доступа к информационной системе могли храниться на дискете или на USB-устройстве, а информация накапливалась на носителях, которые, как правило, были локализованы на территории предприятия. Комплекс антирисковых мероприятий разрабатывался индивидуально для каждого предприятия, вследствие чего и перечни, и стоимость таких мер были различными для каждого предприятия.

При переходе на новые цифровые технологии хранение персональных, индустриальных и корпоративных данных переносится в специализированные облачные хранилища или дата-центры. Традиционные концепции управления уровнем риска, связанные с компьютерной безопасностью, при переходе на технологии IoT могут оказаться недееспособными или неэффективными [24]. На предприятиях, объединенных на базе многосторонних платформ в предпринимательские экосистемы, выпускающих продукцию или услуги в цифровом формате и при этом использующих технологию IoT, также появляется новая концепция управления уровнем риска — концепция иммунитета.

Иммунная система, которая обеспечивает иммунитет, в данном случае, понимается как множественная гетерогенная конструкция в предпринимательской экосистеме, состоящая из компонентов, принадлежащих различным онтологическим порядкам [25]. Работа иммунной системы заключается в подготовке иммунного ответа до какого-либо внешнего воздействия. Собственно, иммунная система или система управления уровнем риска цифровой экосистемы обычно содержат компоненты, участвующие в иммунном ответе, возможно, с избытком [6]. В экономических терминах иммунитет цифровой предпринимательской экосистемы можно признать высоким в том случае, если затраты на выполнение успешной атаки извне на такую систему окажется выше потенциального ущерба, нанесенного цифровой предпринимательской экосистеме.

Принцип действия цифровых предпринимательских экосистем, или многосторонних платформ, обычно состоит в предоставлении одним предприятием, владельцем платформы, доступа заинтересованным партнерам к своим контрагентам с предложениями цифровых продуктов или услуг, которые дополняют предложения самого базового предприятия. Партнеры могут также рассматриваться как контрагенты предприятия, поскольку приносят доход, оплачивая дополнительные услуги, связанные с использованием платформы. Другими словами, предприятия, которые с помощью различных продуктов, услуг, сетей или их комбинаций исполняют роль посредников и объединяют контрагентов в группы, называются многосторонними платформами [26]. Таким образом, базовые предприятия создают платформу, другие предприятия могут создавать различные специализированные приложения, расширяя возможности платформы, добавляя свои данные и новые функции, тем самым повышая ее привлекательность для новых участников. Одной из основных стратегических задач многосторонней платформы является привлечение как можно большего количества пользователей, потому что только в таком случае уменьшение транзакционных издержек, которые распределяются между всеми пользователями платформы, становится привлекательным для всех сторон.

При разработке стратегии развития системы управления уровнем риска предприятий-участников многосторонних платформ на разных уровнях необходимо рассматривать несколько классов задач. Для самих многосторонних платформ — это достижение оптимального уровня риска процессов ценообразования, маркетинговых мероприятий и управление качеством. Для потенциальных пользователей многосторонних платформ — это, с одной стороны, оценка риска дополнительных издержек, а, с другой, учет сетевых эффектов интенциональной и экспектационной подсистем системы управления уровнем риска, возникающих между пользователями платформы. Фактически происходит минимизация степени влияния факторов риска роста продолжительности и затрат на исследование рынков, на поиск поставщиков и покупателей и т.п.

В функциональной подсистеме в рамках многосторонней цифровой платформы многие программные комплексы или приложения будут работать изолированно, и так будет осуществляться некоторая фрагментация и разделение сценариев работы устройств — для диссипации факторов риска сбоя вследствие внешней, так называемой хакерской атаки.

В таком случае снизить возможные негативные последствия потенциальных компьютерных атак можно, используя превентивные антирисковые управленческие воздействия — например, защищенные контроллеры для передачи данных, специализированные операционные системы и защищенные облачные хранилища. Усиленные меры безопасности как на предприятии, так и в рамках его предпринимательской экосистемы должны быть направлены на объекты критической инфраструктуры: системы электро- и водоснабжения, связь, газопроводы, — так как именно эти объекты в последнее время снабжают удаленными системами управления.

Специализированная операционная система управления уровнем риска для комплекса IoT, действующего в рамках предприятия или его предпринимательской экосистемы, может иметь упрощенную, и, вследствие этого, менее уязвимую структуру. Однако, создание специализированной операционной системы для индустриального интернета вещей может потребовать разработки отдельной цифровой экосистемы, аналогичной, например, цифровой экосистеме ПАО «Сбербанк» [27].

Общим трендом в условиях развивающейся цифровой экономики можно назвать формирование сложных цифровых многосторонних платформ, которые объединяют множество предприятий и экономических агентов, позволяя им получить доступ к ресурсам, потребителям или маркетинговым каналам. На практике это может означать, что предприятия вынуждены строить информационные системы таким образом, чтобы постепенно интегрироваться или синхронизироваться с процессами своих покупателей и поставщиков для формирования общих баз данных, что позволит намного точнее строить прогнозы и стратегии разного уровня с помощью технологий искусственных нейронных сетей. Степень свободы выбора решения каждого предприятия и экономического агента находится в обратном отношении к вероятности получения приемлемой для цифровой платформы в целом стратегии [28].

Вариант повышения такой вероятности заключается в создании специализированных правил или институтов в рамках цифровой платформы как некоторого своеобразного инструмента ограничения в ситуации выбора. Новые способы коллективного взаимодействия при координации усилий по созданию обучающих выборок для искусственных нейронных сетей могут предложить социальные сети нового типа. Если рассмотреть, например, сеть Facebook, то ее модель социальных отношений строится на основе протокола Open Graph, который позволяет любой веб-странице стать полноценным объектом в сети. Другой пример содержится в социометрии Морено, описывающей сообщество как собрание изолированных индивидов или атомов. Социометрия при этом предлагает такие способы измерения межличностных отношений, которые помогают обнаружить реальную структуру группы, в отличие от формальной ее структуры [29]. Но индивид или отдельный сотрудник могут рассматриваться как часть коллектива. Поэтому в настоящее время предпринимаются попытки, например, Б. Стиглером [30], разработать иную модель социальной сети, которая смогла бы отразить другую структуру социальных отношений.

Основной единицей в этой новой модели социальной сети выступает не индивидуальный пользователь, а группа или временный трудовой коллектив. Пользователь получает возможность использовать все функции такой сети только при вступлении в группу, которая, в отличие от группы в Facebook, объединена в некоторое сообщество с такими инструментами, которые допускают коллективное написание текстов и наборы специализированных меток. Такая сеть может использоваться для производства нового знания в когнитивной подсистеме системы управления уровнем риска и работы с ним — например, в случае создания обучающих выборок для ИНС в экспертных группах представителей различных предприятий или научных ор-

ганизаций. Алгоритмы ИНС могут сами стать источниками факторов риска в ситуациях, когда не приняты надлежащие меры безопасности для мониторинга их деятельности, независимо от специфики модели [31].

Ограниченность применения полученных результатов

Для широкого применения аппарата ИНС на производственных предприятиях им необходимо достичь базового уровня в цифровых технологиях, т.е. создать современную систему управления производственными и бизнес-процессами, автоматизировать управление ресурсами, как трудовыми, так и материальными, внедрить специализированные информационные решения для взаимоотношений с поставщиками и покупателями, реализовать систему бюджетирования, управления производством и качеством и создать системы управленческой отчетности.

Одна цифровая технология, в том числе исследуемые в этой работе искусственные нейронные сети, не может рассматриваться в качестве универсального инструмента при решении задач управления уровнем риска на различных предприятиях. В отличие от автоматизации, которую можно рассматривать как предыдущий этап развития информационных технологий, в рамках цифровой экономики еще не выработаны единые стратегии построения системы управления уровнем риска. Каждое предприятие на микроуровне, или отрасль на мезоуровне, будут искать свое направление устойчивого развития системы управления уровнем риска, адаптируя свои бизнес-модели к меняющейся среде. Поэтому рекомендации об установке датчиков на все агрегаты и счетчики всех видов ресурсов нельзя признать состоятельными с точки зрения экономики предприятия.

Коротко результаты данного исследования можно сформулировать следующим образом:

1) предложена структура системы управления уровнем риска, которая включает в свой состав четыре подсистемы (интенциональную, экспектационную, когнитивную и функциональную);

2) показано, что внедрение цифровых технологий в различных отраслях экономики обусловливает появление факторов риска некорректной реализации алгоритмов, в частности, ИНС, и может причинить не только экономический ущерб, но и инициировать угрозы жизни и здоровью людей;

3) отмечено, что с развитием цифровизации, появляется новая концепция управления уровнем риска — концепция иммунитета;

4) рассмотрены новые способы практической реализации коллективных действий экономических агентов, как предприятий, так и физических лиц в современных условиях.

Заключение

В итоге хотелось бы отметить, что при накоплении огромных массивов данных, как персональных, так и индустриальных, корпоративных, государственных и т.п. в цифровой предпринимательской экосистеме назревает необходимость дополнения стратегии развития предприятия созданием специальной иммунной подсистемы, которая будет подключаться в случае возникновения существенных помех работе информационных систем как на отдельном предприятии, так и в пределах всей его цифровой экосистемы. В данном случае функциональный контекст иммунной системы может помочь объяснить функции противоречии в социальных системах [32].

Как показало проведенное исследование, технологический дизайн и цифровые технологии будут способствовать снижению вероятности реализации негативных последствий предлагаемых управленческих решений как для отдельного предприятия, так и для его предпринимательской экосистемы.

Анализ сложившейся ситуации свидетельствует о том, что при увеличении общего количества информации остается неочевидной возможность преодоления проблемы получения необходимой и релевантной для принятия решений информации. Кроме того, при возрастании скорости

изменений и степени неопределенности внешней среды, в которой осуществляется деятельность предприятия и его предпринимательской экосистемы, могут получить существенное преимущество только те из них, которые в силах синхронизировать темп внешних изменений с темпом адаптации к ним. В случае слишком высокой скорости внешних изменений и низком темпе приспособления к ним, могут наступить неблагоприятные последствия для предприятия в виде дестабилизации его деятельности, поэтому есть основания предполагать, что использование ИНС в системе управления уровнем риска будет способствовать преодолению фрагментарности данных, имеющихся в распоряжении предприятия, и в том числе благодаря этому ускорит процессы принятия решений.

Таким образом, реализация антирисковых управленческих решений в условиях развития многосторонних платформ и применения технологий ИНС открывает широкие перспективы для использования технологических преимуществ анализа и обработки больших массивов информации для снижения затрат на подбор поставщиков и маркетинговые исследования, а также позволяет в целом уменьшить риск неблагоприятного развития событий.

Представленное исследование может оказаться полезным для исследователей предприятий в задачах моделирования процессов принятия решений и построения систем управления уровнем риска с использованием принципов и технологий искусственных нейронных сетей.

Благодарности

Финансовая поддержка РФФИ (проект 18-010-01042 "Экономическая рациональность менеджеров современных предприятий при принятии решений: исследование с применением инструментария операциональной теории риска и нейросетевого компьютерного моделирования").

СПИСОК ЛИТЕРАТУРЫ

1. **Делез Ж.** Переговоры. 1972–1990. СПб.: Наука. 2004. 235 с.

2. **Карпов В.Э., Готовцев П.М., Ройзензон Г.В.** К вопросу об этике и системах искусственного интеллекта // Философия и общество. 2018. № 2. С. 84–105. DOI: 10.30884/jfio/2018.02.07

3. **Малышкин А.В.** Интегрирование искусственного интеллекта в общественную жизнь: некоторые этические и правовые проблемы // Вестник Санкт-Петербургского университета. Право. 2019. № 10–3. С. 444–460. DOI: 10.21638/spbu14.2019.303

4. **Ложкин А.Г., Божек П., Майоров К.Н.** Исследование внутренних связей нейронной сети // Информационные технологии в науке, промышленности и образовании. Сб. трудов Всероссийской научно-технической конференции / Отв. ред. К.Ю. Петухов. Ижевск, ИжГТУ, 2019. С. 48–52.

5. **Червяков Н.И., Ляхов П.А. и др.** Архитектура сверхточной нейронной сети с вычислениями в системе остаточных классов с модулями специального вида // Нейрокомпьютеры: разработка, применение. 2017. № 1. С. 3–15.

6. **Сивков Д.** Свое или чужое? Создание тела в иммунологии // Логос. 2018. № 28–5. С. 249–286.

7. **Талеб Н.Н.** Черный лебедь. Под знаком непредсказуемости. М.: Колибри, 2009. 528 с.

8. **Кузнецов С.Р.** Математическая модель иммунного ответа // Вестник Санкт-Петербургского университета. Прикладная математика. Информатика. Процессы управления. 2015. № 4. С. 72–87.

9. **Качалов Р.М.** Управление экономическим риском: теоретические основы и приложения. СПб.: Нестор-История. 2012. 288 с.

10. **Качалов Р.М., Слепцова Ю.А., Шокин Я.В.** Оценка риска реализации инновационных проектов предприятий с помощью искусственных нейронных сетей // Вестник Волгоградского государственного университета. Экономика. 2019. № 21–4. С. 171–181. DOI: 10.15688/ek.jvolsu.2019.4.17

11. **Клейнер Г.Б., Рыбачук М.А., Ушаков Д.В.** Психологические факторы экономического поведения: системный взгляд // Terra Economicus. 2018. № 16–1. С. 20–36. DOI: 10.23683/2073-6606-2018-16-1-20-36

12. **Горбачевская Е.Н.** Классификация нейронных сетей // Вестник Волжского университета им. В.Н. Татищева. 2012. № 2(19). С. 128–134.

13. **Kaminski M.E.** The right to explanation, explained. Berkeley Technology Law Journal. 2019, no. 34, pp. 189–218. DOI: 10.15779/Z38TD9N83H

14. **Shalev-Shwartz S., Ben-David S.** Understanding machine learning: From theory to algorithms. Cambridge University Press, 2014. 397 p. DOI: 10.1017/CBO9781107298019

15. **Hamon R., Junklewitz H., Sanchez I.** Robustness and explainability of artificial intelligence - From technical to policy solutions. Luxembourg, Publications Office of the EU, 2020. DOI: 10.2760/57493

16. **Brundage M., Avin S., et al.** The malicious use of artificial intelligence: Forecasting, prevention, and mitigation. Technical Reports. Future of Humanity Institute, 2018. 101 p.

17. **Юсупов Р.М., Мусаев А.А.** Особенности оценивания эффективности информационных систем и технологий // Труды СПИИРАН. 2017. № 2(51). С. 5–34.

18. **Baum J.R., Locke E.A., Smith K.G.** A multidimensional model of venture growth. Academy of Management Journal, 2001, no. 44–2, pp. 292–303. DOI:10.5465/3069456

19. **Wachter S., Mittelstadt B., Russell C.** Counterfactual explanations without opening the black box: Automated decisions and the GPDR. Harvard Journal of Law & Technology, 2018, no. 31–2.

20. **Park S.H., Han K.** Methodologic guide for evaluating clinical performance and effect of artificial intelligence technology for medical diagnosis and prediction. Radiology, 2018, no. 286–3, pp. 800–809.

21. **Скатков А.В., Воронин Д.Ю. и др.** Проактивный и реактивный риск-менеджмент IT-сервисов облачных сред // Информационно-управляющие системы. 2017. № 3(88). С. 25–33. DOI: 10.15217/issn1684-8853.2017.3.25

22. **Куприяновский В.П., Намиот Д.Е. и др.** Интернет Вещей на промышленных предприятиях // International Journal of Open Information Technologies. 2016. № 4(12). С. 69–78.

23. **Слепцова Ю.А.** Методы выбора антирисковых управленческих воздействий // Научно-технические ведомости Санкт-Петербургского государственного политехнического университета. Экономические науки. 2015. № 6. С. 222–232. DOI: 10.5862/JE.233.23

24. **Петров В.Ю., Рудашевская Е.А.** Технология «Интернет Вещей» как перспективная современная технология // Фундаментальные исследования. 2017. № 9–2. С. 471–476.

25. **Martin E.** Toward an anthropology of immunology: The body as nation state. Medical Anthropology Quarterly, 1990, no. 4–4, pp. 410–426.

26. **Яблонский С.А.** Многосторонние платформы и рынки: основные подходы, концепции и практики // Российский журнал менеджмента. 2013. № 11–4. С. 57–78.

27. **Бердышев А.В.** Открытая платформа как технологическая основа развития ПАО «Сбербанк» // Вестник университета. 2018. № 11. С. 154–158. DOI: 10.26425/1816-4277-2018-11-154-158

28. **Шаститко А.Е., Курдин А.А.** В ожидании непредвиденного // Вопросы теоретической экономики. 2020. № 2. С. 36–50. DOI: 10.24411/2587-7666-2020-10202

29. **Морено Я.Л.** Социометрия: Экспериментальный метод и наука об обществе. М.: Академический проект, 2001. 383 с.

30. **Stiegler B.** Etats de choc: Bêtise et savoir au XXIe siècle. Paris, Fayard, 2012. 360 p.

31. **Russell S.J., Dewey D., Tegmark M.** Research priorities for robust and beneficial artificial intelligence. Artificial intelligence Magazine, 2015, no. 36–4, pp. 105–114. DOI: 10.1609/aimag.v36i4.2577

32. **Луман Н.** Социальные системы: Очерк общей теории. СПб.: Наука, 2007. 484 с.

REFERENCES

1. **Zh. Delez,** Peregovory. 1972–1990 [Conversation. 1972–1990]. St. Petersburg, Nauka, 2004. 235 pp. (rus)

2. **V.E. Karpov, P.M. Gotovtsev, G.V. Royzenzon,** K voprosu ob etike i sistemakh iskusstvennogo intellekta [On ethics and artificial intelligence systems]. Filosofiya i obshchestvo, 2018, no. 2, pp. 84–105. (rus). DOI: 10.30884/jfio/2018.02.07

3. **A.V. Malyshkin,** Integration of artificial intelligence into public life: some ethical and legal problems. Vestnik of Saint Petersburg University. Law, no. 10–3, pp. 444–460. (rus). DOI: 10.21638/spbu14.2019.303

4. **A.G. Lozhkin, P. Bozhek, K.N. Mayorov,** Issledovaniye vnutrennikh svyazey neyronnoy setiseti [Investigation of the internal connections of a neural network]. Petukhov K.Yu. (Ed.). Informatsionnyye tekhnologii v nauke, promyshlennosti i obrazovanii [Information technology in science, industry and education]. Proceedings of the All-Russian scientific and technical conference. Izhevsk, IzhGTU, 2019, pp. 48–52. (rus)

5. **N.I. Chervyakov, P.A. Lyakhov, et al.,** Arkhitektura svertochnoy neyronnoy seti s vychisleniyami v sisteme ostatochnykh klassov s modulyami spetsialnogo vida [Hardware implementation of a convolutional neural network using calculations in the residue number system]. Neyrokompyutery: razrabotka, primeneniye, 2017, no. 1, pp. 3–15. (rus)

6. **D. Sivkov,** Svoye ili chuzhoye? Sozdaniye tela v immunologii. [Yours or someone else's? Building a body in immunology]. Logos, 2018, no. 28–5, pp. 249–286. (rus)

7. **N.N. Taleb,** Chernyy lebed. Pod znakom nepredskazuyemosti [The Black Swan: The Impact of the highly improbable]. Moscow, Kolibri, 2009. 528 p. (rus)

8. **S.R. Kuznetsov,** Matematicheskaya model immunnogo otveta [Mathematical model of the immune response]. Vestnik Sankt-Peterburgskogo universiteta. Prikladnaya matematika, informatika, processy upravlenia, 2015, no. 4, pp. 72–87. (rus)

9. **R.M. Kachalov,** Upravleniye ekonomicheskim riskom: teoreticheskiye osnovy i prilozheniya [Economic risk management: Theory and applications]. St. Petersburg, Nestor-Istoriya, 2012. 288 p. (rus)

10. **R.M. Kachalov, Yu.A. Sleptsova, Ya.V. Shokin,** Risk assessment of implementing innovative projects in enterprises using artificial neural networks. Journal of Volgograd State University. Economics, 2019, no. 21–4, pp. 171–181. (rus). DOI: 10.15688/ek.jvolsu.2019.4.17

11. **G.B. Kleiner, M.A. Rybachuk, D.V. Ushakov,** Psychological factors of economic behavior: a systemic view. Terra Economicus, 2018, no. 16–1, pp. 20–36. DOI: 10.23683/2073-6606-2018-16-1-20-36

12. **E.N. Gorbachevskaya,** Klassifikatsiya neyronnykh setey [Classification of neural networks]. Vestnik Volzhskogo universiteta im. V.N. Tatishcheva, 2012, no. 2(19), pp. 128–134. (rus)

13. **M.E. Kaminski,** The right to explanation, explained. Berkeley Technology Law Journal. 2019, no. 34, pp. 189–218. DOI: 10.15779/Z38TD9N83H

14. **S. Shalev-Shwartz, S. Ben-David,** Understanding machine learning: From theory to algorithms. Cambridge University Press, 2014. 397 p. DOI: 10.1017/CBO9781107298019

15. **R. Hamon, H. Junklewitz, I. Sanchez,** Robustness and explainability of artificial intelligence – From technical to policy solutions. Luxembourg, Publications Office of the EU, 2020. DOI: 10.2760/57493

16. **M. Brundage, S. Avin, et al.,** The malicious use of artificial intelligence: Forecasting, prevention, and mitigation. Technical Reports. Future of Humanity Institute, 2018. 101 p.

17. **R.M. Yusupov, A.A. Musaev,** Osobennosti otsenivaniya effektivnosti informatsionnykh sistem i tekhnologiy [Features of evaluating the effectiveness of information systems and technologies]. Trudy SPIIRAN, 2017, no. 2(51), pp. 5–34. (rus)

18. **J.R. Baum, E.A. Locke, K.G. Smith,** A multidimensional model of venture growth. Academy of Management Journal, 2001, no. 44–2, pp. 292–303. DOI:10.5465/3069456

19. **S. Wachter, B. Mittelstadt, C. Russell,** Counterfactual explanations without opening the black box: Automated decisions and the GPDR. Harvard Journal of Law & Technology, 2018, no. 31–2.

20. **S.H. Park, K. Han,** Methodologic guide for evaluating clinical performance and effect of artificial intelligence technology for medical diagnosis and prediction. Radiology, 2018, no. 286–3, pp. 800–809.

21. **A.V. Skatkov, D.Yu. Voronin, et al.,** Proaktivnyy i reaktivnyy risk-menedzhment IT-servisov oblachnykh sred [Proactive and reactive risk management of IT services in cloud environments]. Informatsionno-upravlyayushchiye sistemy, 2017, no. 3(88), pp. 25–33. (rus). DOI: 10.15217/issn1684-8853.2017.3.25

22. **V.P. Kupriyanovskiy, D.E. Namiot, et al.,** Internet Veshchey na promyshlennykh predpriyatiyakh. [Internet of things in industrial plants]. International Journal of Open Information Technologies, 2016, no. 4(12), pp. 69–78. (rus)

23. **Iu.A. Sleptsova,** Methods of selecting antirisk controlling actions. St. Petersburg State Polytechnical University Journal. Economics, 2015, no. 6, pp. 222–232. (rus). DOI: 10.5862/JE.233.23

24. **V.Yu. Petrov, E.A. Rudashevskaya,** Tekhnologiya "Internet Veshchey" kak perspektivnaya sovremennaya tekhnologiya [The technology of "internet of things" as a perspective for modern information technology]. Fundamentalnyye issledovaniya, 2017, no. 9–2, pp. 471–476. (rus)

25. **E. Martin,** Toward an anthropology of immunology: The body as nation state. Medical Anthropology Quarterly, 1990, no. 4–4, pp. 410–426.

26. **S.A. Yablonskiy,** Mnogostoronniye platformy i rynki: osnovnyye podkhody, kontseptsii i praktiki [Multisided platforms and markets: Basic approaches, concepts and practices]. Rossiyskiy zhurnal menedzhmenta, 2013, no. 11–4, pp. 57–78. (rus)

27. **A. Berdyshev,** Open platform as a technological basis for the development of Sberbank. Vestnik Universiteta, 2018, no. 11, pp. 154–158. (rus). DOI: 10.26425/1816-4277-2018-11-154-158

28. **A.E. Shastitko, A.A. Kurdin,** V ozhidanii nepredvidennogo [Expecting unpredictable]. Voprosy teoreticheskoy ekonomiki, 2020, no. 2, pp. 36–50. DOI: 10.24411/2587-7666-2020-10202

29. **Ya.L. Moreno,** Sotsiometriya: Eksperimentalnyy metod i nauka ob obshchestve [Sociometry: Experimental method and the science of society]. Moscow, Akademicheskiy proyekt, 2001. 383 p. (rus)

30. **B. Stiegler,** Etats de choc: Bêtise et savoir au XXIe siècle. Paris, Fayard, 2012. 360 p.

31. **S.J. Russell, D. Dewey, M. Tegmark,** Research priorities for robust and beneficial artificial intelligence. Artificial intelligence Magazine, 2015, no. 36–4, pp. 105–114. DOI: 10.1609/aimag.v36i4.2577

32. **N. Luman,** Sotsialnyye sistemy: Ocherk obshchey teorii [Social systems: An outline of general theory]. St. Petersburg, Nauka, 2007. 484 p. (rus)

Статья поступила в редакцию 28.08.2020.

СВЕДЕНИЯ ОБ АВТОРАХ / THE AUTHORS

СЛЕПЦОВА Юлия Анатольевна
E-mail: julia_sleptsova@mail.ru
SLEPTSOVA Yulia A.
E-mail: julia_sleptsova@mail.ru

КАЧАЛОВ Роман Михайлович
E-mail: kachalov1ya@ya.ru
KACHALOV Roman M.
E-mail: kachalov1ya@ya.ru

ШОКИН Ян Вячеславович
E-mail: yshokin@mail.ru
SHOKIN Yan V.
E-mail: yshokin@mail.ru