

УДК 004.414.28, 004.415.23, 004.418
DOI: [10.26102/2310-6018/2023.40.1.001](https://doi.org/10.26102/2310-6018/2023.40.1.001)

Подход к управлению виртуальной компьютерной лабораторией на основе концептуальной модели операционных рисков

М.А. Белов[✉], А.В. Живетьев, С.А. Подгорный, Н.А. Токарева, Е.Н. Черемисина

Государственный университет «Дубна», Дубна, Российская Федерация
belov@uni-dubna.ru[✉]

Резюме. Статья посвящена совершенствованию системы управления учебным дата-центром «Виртуальная Компьютерная Лаборатория» на основе концептуальной модели операционных рисков. Виртуальная Компьютерная Лаборатория представляет собой интегрированный комплекс аппаратных и программных средств виртуализации и контейнеризации, в форме облачных сервисов с интегрированной системой управления знаниями. Виртуальная Компьютерная Лаборатория используется для освоения многокомпонентных информационных систем и формирования набора сложных знаний, умений и навыков у учащихся в области ИТ в рамках аудиторной и самостоятельной практической работы. Система управления знаниями и принципы самоорганизации, заложенные в основу Виртуальной Компьютерной Лаборатории, позволяют сформировать однородную образовательную среду. Для надежного функционирования Виртуальной Компьютерной Лаборатории с минимальным количеством простоев выполнен анализ влияния рисков на ее работу, а также предлагается подход к созданию системы управления рисками. Рассматриваемый в статье подход позволяет лучше оценивать узкие места Виртуальной Компьютерной Лаборатории и комплексно решать ключевые проблемы, увеличивать время доступности, улучшать качество ее работы и уменьшать количество сбоев за счет использования превентивных механизмов, успешно выявлять риски, которые в наибольшей степени влияют на результаты ее работы и разрабатывать эффективную систему мероприятий по их минимизации. В статье подробно рассматриваются такие элементы риск-менеджмента, как определение и оценка рисков, стратегическое управление рисками, мониторинг и анализ рисков, обеспечение безопасности и управление изменениями.

Ключевые слова: образование, информационные технологии, Виртуальная Компьютерная Лаборатория, управление рисками, риск менеджмент, операционные риски, управление социотехническими системами на основе модели рисков, цифровая трансформация, облачный дата-центр, современные методы управления, электронное обучение, ИТ-образование, дистанционное обучение.

Для цитирования: Белов М.А., Живетьев А.В., Подгорный С.А., Токарева Н.А., Черемисина Е.Н. Подход к управлению виртуальной компьютерной лабораторией на основе концептуальной модели операционных рисков. *Моделирование, оптимизация и информационные технологии.* 2023;11(1). URL: <https://moitvvt.ru/ru/journal/pdf?id=1254> DOI: 10.26102/2310-6018/2023.40.1.001

An approach to managing a virtual computer lab based on the conceptual model of operational risks

M.A. Belov[✉], A.V. Zhivetyev, S.A. Podgorny, N.A. Tokareva, E.N. Cheremisina

Dubna State University, Dubna, Russian Federation
belov@uni-dubna.ru[✉]

Abstract. The article presents the results of a research on improving the management system of Virtual Computer Lab educational data center based on the conceptual model of operational risks. Virtual

Computer Lab is an integrated assembly of virtualization and containerization hardware and software tools in the form of cloud services with an integrated knowledge management system. Virtual Computer Lab is used to master multicomponent information systems for developing students' complex knowledge, skills and abilities in the field of IT in a classroom context and as part of independent learning. The knowledge management system and the principles of self-organization, which are the integral parts of Virtual Computer Laboratory, make it possible to create a homogeneous educational environment. For the reliability and durability of using the Virtual Computer Laboratory with a minimal downtime, an analysis of the impact of risks on its operation was carried out, and an approach to designing a risk management system was proposed. The approach considered in the article enables better assessment of performance bottlenecks of the Virtual Computer Lab as well as its key problems in a comprehensive manner, increase service uptime, enhance performance quality and reduce the number of failures by means of preventive mechanisms, successfully identify the risks that significantly affect its output and develop an effective system of measures to minimize them. The article discusses in detail such elements of risk management as risk identification and assessment, strategic risk management, risk monitoring and analysis, security and change management.

Keywords: education, information technology, Virtual Computer Lab, risk management, operational risks, management of sociotechnical systems based on a risk model, digital transformation, cloud data center, modern management methods, digital learning, IT-education, distance learning, e-learning.

For citation: Belov M.A., Zhivetyev A.V., Podgorny S.A., Tokareva N.A., Cheremisina E.N. An approach to managing a virtual computer lab based on the conceptual model of operational risks. *Modeling, Optimization and Information Technology*. 2023;11(1). URL: <https://moitvvt.ru/ru/journal/pdf?id=1254> DOI: 10.26102/2310-6018/2023.40.1.001 (In Russ.).

Введение

Для работы с современными информационными технологиями и сложными программно-технологическими решениями, обладающими свойством нелинейности, выпускникам ИТ направлений необходимо иметь глубокие теоретические знания, а также практические умения и навыки. Для подготовки таких специалистов требуется глубокое понимание предметной области, платформенное или даже экосистемное мышление на уровне концепций и методологий, владение последними технологиями, а также использование эффективных и инновационных инструментов, одним из которых является учебный дата-центр «Виртуальная Компьютерная Лаборатория». Учебный центр является гиперконвергентным комплексом, который обеспечивает предоставление вычислительных ресурсов в форме облачных сервисов, позволяет контролировать учебные активности учащихся, управлять их поведением внутри лаборатории, выдавать рекомендации и готовые шаблоны с помощью экспертной системы, а также интегрирует систему управления знаниями, что позволяет говорить об однородной образовательной среде, в которой, например, присутствуют элементы наглядного пиктографического представления внутренних операционных ресурсов, снижающие порог вхождения, а также реализована частичная автоматизация основных технологических операций. Это способствует снижению порога вхождения и способствует более быстрому получению образовательных результатов. Такая облачная образовательная среда позволяет предоставлять учащимся возможности для развертывания и изучения современных информационных систем и новейших достижений информационных технологий, сопутствующих теорем и алгоритмов для создания перспективных программно-технологических решений в области цифровой трансформации и ИТ-сервисов массового обслуживания. Причем учащиеся могут делать это как самостоятельно, так и посредством совместной работы в рамках аудиторных практических занятий и их последующего продолжения посредством онлайн коллаборации. Принципиально важной и отличительной чертой учебного дата-центра «Виртуальная Компьютерная

Лаборатория» являются принципы самоорганизации, которые предоставляют возможность перейти от системы жестких политик безопасности, без которых не может нормально функционировать ни один классический компьютерный класс, к системе без каких-либо ограничений прав и свобод учащихся в области развертывания и использования программного обеспечения, что позволяет не только продуктивно учиться, но и развивать чувство личной ответственности, уважение к коллегам, а также развивать и укреплять основные культурные ценности в университетской среде [1-10].

Однако существуют различные операционные риски и проблемные ситуации, являющиеся неотъемлемой частью любой человеческой деятельности, которые могут оказывать негативное влияние на продуктивное использование Виртуальной Компьютерной Лаборатории (ВКЛ) в образовательном процессе. Именно из-за этого возникает необходимость и потребность разработки системы управления рисками, построенной на основе результатов сбора, систематизации и обобщения коллективных знаний всех участников и заинтересованных субъектов, позволяющей избежать возникновения проблемных и непредвиденных ситуаций, препятствующих организации учебного процесса, позволяющего обучать профессионалов в области современных информационных технологий. Целеполаганием исследования являются формирование концепции по совершенствованию системы управления сложной системы – учебного дата-центра «Виртуальная Компьютерная Лаборатория», ориентированной на уменьшение количества сбоев, повышение стабильности функционирования и, как следствие, повышение продуктивности работы преподавателей и учащихся.

Анализ влияния рисков на функционирование Виртуальной Компьютерной Лаборатории, подход к проектированию системы управления рисками (концептуальная модель)

В рамках контекста управления Виртуальной Компьютерной Лабораторией, рисками признаются события, способные, в случае их реализации, оказывать негативное влияние на функционирование системы. Риск, которому удалось реализоваться, превращается в проблему или, иными словами, последствие риска, где вероятностью риска является вероятность, с которой конкретный риск может превратиться в проблему.

Очевидно, что управление тем или иным риском состоит из действия или процедуры действий, которые позволяют выявить и оценить риски до или во время их превращения в проблему, тем самым обеспечивая их своевременное отслеживание и устранение. Необходимо прилагать максимум усилий, чтобы выявить основные риски как можно раньше и желательного до того, как они превратились в проблемы. Сразу после того, как риск выявлен и идентифицирован, принимается взвешенное решение об ответных действиях, призванных снизить вероятность возникновения неблагоприятного события или уменьшить деструктивные последствия в случае реализации риска, задействуя минимально необходимые и достаточные ресурсы.

В процессе эксплуатации Виртуальной Компьютерной Лаборатории в образовательном процессе мы использовали три стратегии противодействия рискам: избегание риска, переадресация риска и согласие с присутствием риска. Избегание риска связано с исключением программных компонентов ВКЛ и оборудования, на поддержку стабильной работы которых недостаточно ресурсов или выведение из эксплуатации устройств, выработавших двойной ресурс при отсутствии финансирования на амортизацию. Такой подход мы применяли к катастрофическим рискам. Переадресация рисков, по сути, являлась для нас привлечением внешних экспертов или компаний, у которых достаточно технических ресурсов для гарантированного поддержания работоспособности программного обеспечения или вспомогательных устройств,

например, таких как система кондиционирования серверной. Но чаще всего, приходилось соглашаться с присутствием риска и пассивно ожидать его реализации, при этом имея план альтернативных действий на случай реализации риска, предпринимая действия (если таковые были возможны), ориентированные на уменьшение вероятности его проявления или минимизации его последствий. В условиях неопределенности, вызванной асимметричным распределением информации, отсутствием знаний о будущих переменных или недостатком информации о событиях и зачастую их вероятностной природе, нам приходилось составлять список выявленных и отслеживаемых рисков, упорядоченных по степени важности и критичности, которые, по сути и формируют приоритет, определяемый как произведение вероятности на величину воздействия, выраженную в условных единицах. При этом нам приходилось сталкиваться с тем, что ситуации с неопределенностью усугублялись из-за искажения имеющейся информации за счёт ее субъективной оценки участниками Виртуальной Компьютерной Лаборатории, что порой затрудняло экспозицию рисков во времени, связанную с организацией проведения ключевых и опасных, с точки зрения возникновения рисков, мероприятий в разное время.

В большинстве систем риск-менеджмента все многообразие рисков можно разбить на три группы: операционные риски (на которые мы сделали основной акцент в исследовании, а также бизнес-риски и финансовые риски. С точки зрения эксплуатации Виртуальной Компьютерной Лаборатории в магистерских программах Института Системного Анализа и Управления, наиболее важными и актуальными для нас являются операционные риски, т. е. риски, которые связаны с персоналом, преподавателями и учащимися, технологические риски, риски процессов, а также внешние риски.

Например, к рискам персонала, преподавателей и студентов можно отнести риски нехватки квалифицированных сотрудников, выполняющих весь необходимый спектр обеспечивающих процессов, связанных с функционированием ВКЛ, недостаточной квалификацией молодых преподавателей и ассистентов, недобросовестным исполнением операций, связанных с модернизацией и поддержкой оборудования, несвоевременную установку патчей безопасности, создание групповых политик безопасности ненадлежащего качества, которые или могут иметь бреши в сетевой защите и внутренней безопасности, или не позволяют полноценно проводить как аудиторные занятия, так и самостоятельную исследовательскую и проектную работы. Также существуют риски, связанные с перегрузкой преподавателей больше, чем это допускается психофизиологическими нормами, риски ошибок студентов с возможным безалаберным отношением к вычислительным ресурсам.

К рискам процессов можно отнести риск неверной методологии осуществления образовательных процессов, например, когда методология устарела и не позволяет подготавливать специалистов, востребованных ведущими отраслевыми компаниями, или, когда инновационная методология требует дорогостоящих серверов и программного обеспечения, но не поддерживается руководством вуза, в силу нехватки средств или желания сэкономить. Сюда можно отнести и риск неверной организационной структуры обеспечивающих подразделений, а также недостатки в системе защиты информации и порядка доступа к информации или неправильной организации информационных потоков внутри организации.

Технологические риски связаны с отказами серверов, сетевой инфраструктуры, перебоями в электроснабжении, отсутствием исправных источников бесперебойного питания и дизель генераторов, а также сбоями в программном обеспечении.

К внешним рискам относятся риски хакерского проникновения или вирусной атаки, а также маловероятные риски, связанные с несанкционированным проникновением, хищением активов и неблагоприятные ситуации из-за техногенных

катастроф или выхода из строя критически важного оборудования, например, кондиционера в серверной и отсутствием средств на его замену или ремонт в условиях летней жары.

Мы рассматриваем Виртуальную Компьютерную Лабораторию как организацию, поэтому управление рисками является процессом, который затрагивает всю деятельность лаборатории, начиная от разработки стратегии и заканчивая выполнением отдельных функций всеми вовлеченными лицами. Фактически, процесс управления рисками сводится к тому, что принимаются и выполняются такие управленческие решения, которые позволяют существенно снизить неблагоприятное влияние операционных рисков на учебный процесс из-за ненадлежащего функционирования Виртуальной Компьютерной Лаборатории, которое может быть вызвано случайными событиями.

Однако, для того чтобы деятельность по управлению рисками была эффективной, она должна быть систематической и комплексной. При построении системы управления рисками проводится углубленное исследование совокупности всех рисков как единого целого, с учетом всех ключевых взаимосвязей и возможных последствий. Помимо понимания общих закономерностей, следует также учитывать воздействие средств и инструментов управления риском (как положительное, так и отрицательное) на тот риск, для борьбы с которым они предназначены, но и анализировать их влияние (положительное или отрицательное) на другие риски в зависимости от их места и связей внутри Виртуальной Компьютерной Лаборатории, а также на возможное появление новых рисков.

Затем мы разделили процесс управления рисками на несколько этапов:

1. *Системное планирование управления рисками* – выбор методов и подходов для управления рисками Виртуальной Компьютерной Лаборатории, а затем планирование всей последующей деятельности.

2. *Идентификация и исследование (анализ) рисков* – определение рисков, которые способны оказывать негативное влияние на функционирование Виртуальной Компьютерной Лаборатории в образовательном процессе, с обязательным последующим документированием всех рисков и их характеристик.

3. *Оценка рисков* – качественное и/или количественное определение риска, его углубленный анализ, а также анализ сопутствующих условий и причин их возникновения с целью определения влияния на функционирование Виртуальной Компьютерной Лаборатории.

4. *Прогноз и планирование реагирования на риски* – определение методов и процедур, которые помогут минимизировать негативные последствия рисков событий и обоснование потенциально возможных преимуществ выбранного решения (если это возможно).

5. *Контроль рисков на основе мониторинга* – мониторинг рисков, определение оставшихся угроз, реализация плана и выполнение необходимых действий для управления рисками, в том числе и оценки эффективности действий по минимизации рисков (в случае необходимости).

Тут следует отметить, что этапы управления рисками представлены как дискретные элементы с четко определенными характеристиками, но на практике они могут частично совпадать и взаимодействовать.

При создании программно-технологического решения управления рисками, необходимо иметь в виду 5 уровней развертывания, представленных аналитической компанией Gartner, которые можно рассматривать как стадии внедрения системы управления рисками, а также уровень ее зрелости.

1. *Уровень 1.* Наличие достоверной информации и общая осведомленность всех заинтересованных лиц в проблематике операционных рисков, назначение ответственных по обеспечению соответствия стандартам и надзору за состоянием операционных рисков.

2. *Уровень 2.* Оценка уязвимостей и узких мест Виртуальной Компьютерной Лаборатории, с точки зрения операционных рисков, разработка плана действий по обеспечению соответствия стандартам, оценка соответствия существующей системы управления рисками принимаемым стандартам.

3. *Уровень 3.* Оценка уровня сложности системы и, как следствие, анализ прямых и косвенных затрат на обеспечение соответствию стандартам и сравнение их с потенциальными преимуществами (иными словами, сравнение стоимости управления операционными рисками с результатом, который будет достигнут).

4. *Уровень 4.* Разработка групповых политик и процедур управления операционными рисками Виртуальной Компьютерной Лаборатории, включая все необходимые для этого средства, а также информацию и знания по процессам.

5. *Уровень 5.* Оценка полученных результатов, достигнутых с помощью реализованной системы управления операционными рисками (внешний и внутренний аудит).

Развертывание системы управления рисками в среду Виртуальной Компьютерной Лаборатории позволяет более оперативно и своевременно выявлять угрозы и возможности, влияющие на качество ее функционирования, что способствует повышению прозрачности управления, росту доверия руководства вуза к проекту ВКЛ, развиваемому в виде гибрида плюралистической и эволюционной организаций, получению новых знаний и опыта вовлеченными в проект сотрудниками вуза, привлечению более мотивированных и достойных абитуриентов, минимизации затрат на использование Виртуальной Компьютерной Лаборатории, а также коммерциализации проекта.

Первой и ключевой задачей создания системы риск-менеджмента является идентификация, анализ и оценка рисков и угроз, возникающих при использовании Виртуальной Компьютерной Лаборатории в учебном процессе, от правильной организации и решения которой в значительной степени будет зависеть то, насколько эффективными будут управленческие решения и, в конечном итоге, подойти к стабильной, продуктивной и бесбойной эксплуатации Виртуальной Компьютерной Лаборатории. Благодаря успешному выполнению данного этапа появляется возможность сформировать целостную картину (карту) рисков. Для этого необходимо выполнить осмысление каждого риска, т. е. провести качественный анализ структурных характеристик риска, таких как уязвимость, опасность, подверженность риску, а затем более детально проанализировать конкретные причины неблагоприятных событий, а также их отрицательных последствий для всех ключевых рисков в целом. Для идентификации и анализа рисков могут применяться различные методы, от широко применяемой экспертной оценки, до более формализованных вариантов, таких как контроллинг ключевых показателей или проверочные списки рисков, содержащие вопросы, отвечая на которые делается проверка того, все ли необходимые критерии учтены, также может проводиться анализ видов, вариантов и последствий отказов, описание сценариев возникновения риска и его дальнейшего развития (так называемый анализ «что если»), предупредительный анализ человеческих ошибок.

Методы оценки рисков в контексте функционирования Виртуальной Компьютерной Лаборатории важны для нас не столько с точки зрения определения величины ущерба, обусловленного конкретным риском, сколько для выяснения того, какую опасность несет в себе этот риск, и стоит ли с ним бороться. В процессе

эксплуатации Виртуальной Компьютерной Лаборатории мы столкнулись с проблемой проведения количественного анализа рисков, из-за того, что для построения вероятностной модели требуется провести связывание событий и ущерба с вероятностью этих событий на основе исторической информации, которую достаточно сложно собрать в условиях дефицита ресурсов, с которым мы столкнулись. Модели оценки без учета вероятности, такие как, имитационное моделирование, анализ чувствительности, стресс анализ, анализ сценариев, на наш взгляд, основываются на субъективных оценках определения ущерба, поэтому применять их не всегда целесообразно.

Нехватка ресурсов требует качественного анализа, который предполагает обнаружение рисков, исследование их особенностей и выявление последствий реализации этих рисков в форме потенциального или нанесенного ущерба, а также идентификацию источников информации по каждому риску.

При этом работая с информацией необходимо соблюдать принципы полезности, доступности и достоверности, руководствуясь текущими параметрами встроенных систем мониторинга, опросами, документацией, накопленным опытом из уже произошедших аварий и нестандартных ситуаций.

О мероприятиях по планированию и реагированию на риски, а также их минимизации мы уже говорили в начале данной статьи, это избегание риска, снижение риска, передача риска и принятие риска. Поэтому мы сразу переходим к заключительному этапу мониторинга и проверки рисков. Мониторинг операционных рисков включает в себя наблюдение за появлением проблемных ситуаций, идентификацию оставшихся угроз для предотвращения рисков, что является необходимым для полного контроля за ситуацией и формирования управляющих воздействий. Также очень важно правильно определить ключевые индикаторы рисков. Они должны объективно отражать уровень каждого конкретного риска, т. к. среди множества действующих факторов, большинство из которых являются случайными, существуют и такие, которые во многом определяют вероятность наступления неблагоприятного события и потенциальный размер ущерба. При анализе таких показателей можно с большей или меньшей уверенностью отслеживать и прогнозировать не только уровень риска, но и прогнозировать масштаб проблем, а также потенциальные убытки. К типичным, наиболее часто используемым индикаторам риска можно отнести простой, количество жалоб, количество и типы ошибок в лог-файлах, частоту ручных исправлений и корректировок системы. Изменение ключевых индикаторов риска может являться сигналом возникновения рисков ситуации и, соответственно, сигналом к запуску мероприятий по минимизации данного риска.

Информационная система управления рисками ВКЛ должна поддерживать полный жизненный цикл управления рисками, предоставляя возможность формирования политики управления рисками, генерации отчетов поддержки принятия решений, а также мониторинга и контроля всех рисков в Виртуальной Компьютерной Лаборатории. Также информационная система управления рисками должна содержать детальное описание сценариев, процедур и их ресурсного окружения в виде шаблонов документов, контрольных листов, процессных моделей и референтных примеров, позволяющих по аналогии находить ответы на важные вопросы, возникающие в процессе эксплуатации. Система должна предоставлять риски не только по процессам, категориям, ответственным и индикаторам рисков, но и таким образом, чтобы каждый пользователь мог видеть только ту информацию, которая предназначена для него. Такое представление позволяет всем участникам Виртуальной Компьютерной Лаборатории получить наиболее полную информацию (в рамках полномочий системной роли) о том, в каких процессах возникает данный риск, какое место он занимает в дереве рисков лаборатории, кто является ответственным за его контроль, и какие индикаторы

используются для его мониторинга и анализа. Каждый пользователь Виртуальной Компьютерной Лаборатории в любой момент может выяснить, какие меры применяются для минимизации данного риска, а также посмотреть их на карте рисков, чтобы иметь представление о наиболее значимых рисках, а также наблюдать изменения положений различных рисков вследствие проведения мероприятий по их минимизации. Более того, система управления рисками должна предоставлять возможность студентам и преподавателям участвовать в идентификации и анализе рисков ВКЛ, а также давать рекомендации по их минимизации или устранению.

Однако очень важно, чтобы в конечном итоге не получилось так, что затраты на управление рисками превысили бы эффект от снижения рисков и их неблагоприятных последствий.

Заключение

Ключевая стратегия для сохранения лидерства – экспериментировать и двигаться вперед, поэтому данное исследование ориентировано на эволюционное развитие и совершенствование системы управления Виртуальной Компьютерной Лабораторией, что позволяет лучше оценивать узкие места лаборатории и решать ключевые проблемы комплексно, предоставлять возможность управления ВКЛ всем заинтересованным лицам, повышать надежность и качество ее работы за счет использования превентивных механизмов, успешно выявлять риски, которые в наибольшей степени влияют на результаты использования Виртуальной Компьютерной Лаборатории в учебном процессе, разработать и непрерывно актуализировать эффективную систему мероприятий по их минимизации, привлекать новых заинтересованных в развитии ВКЛ пользователей к процессам управления и совершенствования, использовать технологию минимизации операционных рисков как инструмент управления лабораторией и положительно повлиять на динамику ее развития.

Предлагаемый подход к управлению Виртуальной Компьютерной Лабораторией является частью методологии подготовки квалифицированных ИТ-профессионалов, обеспечивая Институту Системного Анализа и Управления (ИСАУ) Университета «Дубна» уверенное лидерство в создании оптимальной и устойчивой образовательной среды, на основе применения самых современных методов и технологий.

СПИСОК ИСТОЧНИКОВ

1. Grishko S., Belov M., Cheremisina E., Sychev P. Model for creating an adaptive individual learning path for training digital transformation professionals and big data engineers using Virtual Computer Lab. *Communications in Computer and Information Science*. 2021;1448:496–507.
2. Белов М.А., Гришко С.И., Лишилилин М.В., Осипов П.А., Черемисина Е.Н. Стратегия подготовки ИТ-специалистов с применением инновационного учебного дата-центра «виртуальная компьютерная лаборатория» для эффективного решения задач цифровой трансформации и акселерации цифровой экономики. *Современные информационные технологии и ИТ-образование*. 2021; 17:134–144.
3. Белов М.А., Гришко С.И., Черемисина Е.Н., Токарева Н.А. Подготовка ИТ-специалистов в условиях глобальной цифровой трансформации. Концепция автоматизированного управления профилями компетенций в образовательных программах будущего. *Современные информационные технологии и ИТ-образование*. 2021;20:658–669.

4. Cheremisina E.N., Belov M.A., Tokareva N.A., Nabiullin A.K., Grishko S.I., Sorokin A.V. Embedding of containerization technology in the core of the virtual computing lab. *CEUR Workshop Proceedings. 26. Ser. «Selected Papers of the 26th International Symposium on Nuclear Electronics and Computing, NEC 2017»*. 2017; 2023:299–302.
5. Belov M., Grishko S., Cheremisina E., Tokareva N. *Concept of peer-to-peer caching database for transaction history storage as an alternative to blockchain in digital economy. CEUR Workshop Proceedings. 9. Ser. «GRID 2021 - Proceedings of the 9th International Conference «Distributed Computing and Grid Technologies in Science and Education»*. 2021;3041:494–497.
6. Cheremisina E., Tokareva N., Kirpicheva E., Kreider O., Milovidova A., Potemkina S. The concept of training it professionals in the cross-cutting digital technologies. *CEUR Workshop Proceedings. 9. Ser. «GRID 2021 - Proceedings of the 9th International Conference «Distributed Computing and Grid Technologies in Science and Education»*. 2021;3041:525–529.
7. Миловидова А.А., Черемисина Е.Н., Добрынин В.Н. Алгоритм определения типа и параметров функции принадлежности нечёткого измерителя. *Современная наука: актуальные проблемы теории и практики. Серия: Естественные и технические науки*. 2019;9:69–74.
8. Добрынин В.Н., Миловидова А.А., Соколов И.А. Оценка адекватности модели и объекта исследования. *Информационно-телекоммуникационные технологии и математическое моделирование высокотехнологичных систем. Материалы Всероссийской конференции с международным участием*. М: Издательство РУДН; 2018. С. 252–256.
9. Митрошин П.А. Автоматизация процесса измерения уровня развития компетенций в компетентностно-ориентированной модели обучения. *Метрологическое обеспечение инновационных технологий. Международный форум*. СПб: Санкт-Петербургский государственный университет аэрокосмического приборостроения; 2020. С. 204–205.
10. Митрошин П.А. Модели и алгоритмы поддержки управления процессом обучения. *Информатизация образования и методика электронного обучения: цифровые технологии в образовании. Материалы IV Международной научной конференции*. Красноярск: Красноярский государственный педагогический университет им. В.П. Астафьева; 2020. С. 263–268.
11. Белов М.А., Антипов О.Е. Контрольно-измерительная система оценки качества обучения в виртуальной компьютерной лаборатории, качество. *Наука. Инновации. Образование*. 2012;3:28–37.
12. Черемисина Е.Н., Белов М.А., Антипов О.Е., Сорокин А.В. Инновационная практика компьютерного образования в университете "Дубна" с применением виртуальной компьютерной лаборатории на основе технологии облачных вычислений. *Программная инженерия*. 2012;5:34–41.
13. Черемисина Е.Н., Крамаров Н.Л., Белов М.А. *Практический системный анализ. Построение моделей понятий в проектах повышения эффективности деятельности организаций*. Учебное пособие для студентов высших учебных заведений. Дубна: Государственный Университет «Дубна»; 2012. 149 с.
14. Черемисина Е.Н., Белов М.А., Лишин М.В. Интеграция виртуальной компьютерной лаборатории и знаниевого пространства – новый взгляд на подготовку высококвалифицированных ИТ-специалистов. *Системный анализ в науке и образовании*. 2014;1:97–104.

15. Сидоров Д.С., Белов М.А. Проектирование аппаратно-программных комплексов в учебном процессе с применением виртуальной компьютерной лаборатории. *Системный анализ в науке и образовании*. 2020;2:70–82.

REFERENCES

1. Grishko S., Belov M., Cheremisina E., Sychev P. Model for creating an adaptive individual learning path for training digital transformation professionals and big data engineers using Virtual Computer Lab. *Communications in Computer and Information Science*. 2021;1448:496–507.
2. Belov M.A., Grishko S.I., Lishilin M.V., Osipov P.A., Cheremisina E.N. Strategy for training IT specialists using the innovative training data center «virtual computer laboratory» to effectively solve the problems of digital transformation and acceleration of the digital economy. *Modern information technology and IT education*. 2021;17:134–144.
3. Belov M.A., Grishko C.I., Cheremisina E.N., Tokareva N.A. Training IT specialists in a global digital transformation. The concept of automated management of competency profiles in educational programs of the future. *Modern information technology and IT education*. 2021;20:658–669.
4. Cheremisina E.N., Belov M.A., Tokareva N.A., Nabiullin A.K., Grishko S.I., Sorokin A.V. Embedding of containerization technology in the core of the virtual computing lab. *CEUR Workshop Proceedings. 26. Ser. «Selected Papers of the 26th International Symposium on Nuclear Electronics and Computing, NEC 2017»*. 2017; 2023:299–302.
5. Belov M., Grishko S., Cheremisina E., Tokareva N. *Concept of peer-to-peer caching database for transaction history storage as an alternative to blockchain in digital economy*. *CEUR Workshop Proceedings. 9. Ser. «GRID 2021 - Proceedings of the 9th International Conference «Distributed Computing and Grid Technologies in Science and Education»*. 2021;3041:494–497.
6. Cheremisina E., Tokareva N., Kirpicheva E., Kreider O., Milovidova A., Potemkina S. The concept of training it professionals in the cross-cutting digital technologies. *CEUR Workshop Proceedings. 9. Ser. «GRID 2021 - Proceedings of the 9th International Conference «Distributed Computing and Grid Technologies in Science and Education»*. 2021;3041:525–529.
7. Milovidova A.A., Cheremisina E.N., Dobrynin V.N. Algorithm for determining the type and parameters of the function of belonging to an odd meter. *Modern science: current problems of theory and practice. Series: Natural and Technical Sciences*. 2019;9:69–74.
8. Dobrynin V.N., Milovidova A.A., Sokolov I.A. Assessment of the adequacy of the model and the study object. Information and telecommunication technologies and mathematical modeling of high-tech systems. *Materials of the All-Russian Conference with international participation*. M: RUDN Publishing House; 2018:252–256.
9. Mitroshin P.A. Automation of the process of measuring the level of development of competencies in a competence-oriented training model. *Metrological support of innovative technologies. International Forum*. St. Petersburg State University of Aerospace Instrumentation; 2020. P. 204–205.
10. Mitroshin P.A. Models and algorithms to support the management of the learning process. *Informatization of education and the methodology of e-learning: digital technologies in education. Proceedings of the IV International Scientific Conference*.

- Krasnoyarsk: V.P. Astafiev Krasnoyarsk State Pedagogical University; 2020. P. 263–268.
11. Belov MA, Antipov O.E. Control and measurement system for assessing the quality of training in a virtual computer laboratory, quality. *Science. Innovation. Education*. 2012;3:28–37.
 12. Cheremisina E.N., Belov MA, Antipov O.E., Sorokin A.V. Innovative practice of computer education at Dubna University using a virtual computer laboratory based on cloud computing technology. *Software engineering*. 2012;5:34–41.
 13. Cheremisina E.N., Kramarov N.L., Belov M.A. *Practical system analysis. Building models of concepts in projects to improve the efficiency of organizations*. A textbook for students of higher education institutions. Dubna: State University «Dubna»; 2012. 149 p.
 14. Cheremisina E.N., Belov MA, Lishilin M.V. Integration of a virtual computer laboratory and a knowledge space is a new look at the training of highly qualified IT specialists. *Systems analysis in science and education*. 2014;1:97–104.
 15. Sidorov D.S., Belov M.A. Design of hardware and software systems in the educational process with the use of a virtual computer laboratory. *Systems analysis in science and education*. 2020;2:70–82.

ИНФОРМАЦИЯ ОБ АВТОРАХ / INFORMATION ABOUT THE AUTHORS

Белов Михаил Александрович, кандидат технических наук, доцент Государственного университета «Дубна», Дубна, Российская Федерация.
e-mail: belov@uni-dubna.ru
ORCID: [0000-0003-0678-3344](https://orcid.org/0000-0003-0678-3344)

Mikhail Aleksandrovich Belov, Candidate of Technical Sciences, Associate Professor at Dubna State University, Dubna, Russian Federation.

Живетьев Александр Викторович, ассистент, Государственный университет «Дубна», Дубна, Российская Федерация.
e-mail: zhivetyev@gmail.com
ORCID: [0000-0002-8202-6428](https://orcid.org/0000-0002-8202-6428)

Aleksandr Viktorovich Zhivetyev, Assistant Lecturer, Dubna State University, Dubna, Russian Federation.

Подгорный Сергей Александрович, доктор технических наук, профессор Государственного университета «Дубна», Дубна, Российская Федерация.
e-mail: saptich@rambler.ru
ORCID: [0000-0001-6842-270X](https://orcid.org/0000-0001-6842-270X)

Sergey Aleksandrovich Podgorny, Doctor of Technical Sciences, Professor at Dubna State University, Dubna, Russian Federation.

Токарева Надежда Александровна, кандидат физико-математических наук, доцент Государственного университета «Дубна», Дубна, Российская Федерация.
e-mail: tokareva@uni-dubna.ru
ORCID: [0000-0002-0798-2276](https://orcid.org/0000-0002-0798-2276)

Nadezhda Alexandrovna Tokareva, Candidate of Physical and Mathematical Sciences, Associate Professor at Dubna State University, Dubna, Russian Federation.

Черемисина Евгения Наумовна, доктор технических наук, профессор

Evgeniya Naumovna Cheremisina, Doctor of Technical Sciences, Professor at Dubna State University, Dubna, Russian Federation.

Государственного университета «Дубна»,
Дубна, Российская Федерация.
e-mail: chere@uni-dubna.ru
ORCID: [0000-0002-6041-8359](https://orcid.org/0000-0002-6041-8359)

*Статья поступила в редакцию 24.11.2022; одобрена после рецензирования 03.12.2022;
принята к публикации 11.01.2023.*

*The article was submitted 24.11.2022; approved after reviewing 03.12.2022;
accepted for publication 11.01.2023.*