СЕВАСТОПОЛЬСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

Перспективные направления развития отечественных информационных технологий

Материалы VIII межрегиональной научно-практической конференции

Севастополь, 20-24 сентября 2022

Федеральное государственное автономное образовательное
учреждение высшего образования
«Севастопольский государственный университет»

Перспективные направления развития отечественных информационных технологий

Материалы VIII межрегиональной научно-практической конференции
(Севастополь 20 - 24 сентября 2022 года)

Advanced national information systems and technologies

Materials of VIII interregional scientific-practical conference
(Sevastopol, September 20–24, 2022)

Севастополь 2022

УДК 658.52.011.56(06)
ББК 34.6-5-05
А 224

Научный редактор: Б.В. Соколов, проф., д-р техн. наук, главный научный сотрудник СПИИРАН Санкт-Петербургского Федерального исследовательского центра Российской академии наук

Соорганизаторами конференции являются:
Министерство науки и высшего образования Российской Федерации,
Правительство Севастополя,
Законодательное Собрание Севастополя,
Правительство Санкт-Петербурга,
Севастопольский государственный университет,
Санкт-Петербургский Федеральный исследовательский центр Российской академии наук (СПб ФИЦ РАН)

А 224 **Перспективные направления развития отечественных информационных технологий: материалы VIII межрегиональной научно-практической конф. Севастополь, 20-24 сентября 2022 г. /** Севастопольский государственный университет; науч. ред. : Б.В. Соколов. – Севастополь: СевГУ, 2022. – 252с.
ISBN 978-5-6049992-2-6

В сборнике представлены научные работы из разных отраслей науки и техники. Предназначен для научных сотрудников, студентов и преподавателей.
Материалы докладов публикуются в авторской редакции.

УДК 658.52.011.56(06)
ББК 34.6-5-05

ISBN 978-5-6049992-2-6

ОРГАНИЗАЦИОННЫЙ КОМИТЕТ КОНФЕРЕНЦИИ

Сопредседатели

Нечаев Владимир Дмитриевич	Ректор Севастопольского государственного университета
Юсупов Рафаэль Мидхатович	Научный руководитель СПИИРАН Санкт-Петербургского Федерального исследовательского центра Российской академии наук (СПб ФИЦ РАН), заслуженный деятель науки и техники РФ, член-корреспондент РАН

Заместитель председателя

Бондарев Владимир Николаевич	Директор института информационных технологий Севастопольского государственного университета

ПРОГРАММНЫЙ КОМИТЕТ КОНФЕРЕНЦИИ

Председатель

Советов Борис Яковлевич	Сопредседатель Научного совета по информатизации Санкт-Петербурга, заслуженный деятель науки и техники РФ, академик Российской академии образования

Заместители председателя

Моисеев Дмитрий Владимирович	Профессор кафедры «Информационные технологии и компьютерные системы» Севастопольского государственного университета
Жигадло Валентин Эдуардович	Заместитель генерального директора ЗАО «Институт телекоммуникаций», председатель Санкт-Петербургского отделения Академии информатизации образования

ТЕМАТИЧЕСКИЕ НАПРАВЛЕНИЯ КОНФЕРЕНЦИИ

- Проблемы развития информационного общества. Цифровая экономика
- Фундаментальные проблемы развития информационных технологий
- Искусственный интеллект и технологии «Умного города»
- Информационная среда и телекоммуникационная инфраструктура
- Информационные технологии в критических инфраструктурах. Информационная безопасность
- Информационные технологии в машиностроении
- Информационные технологии в морехозяйственной деятельности
- Геоинформационные системы и спутниковый мониторинг
- ИТ-продукты и услуги
- Импортозамещение и технологическая безопасность ИТ-сферы
- ИТ в образовании, подготовка и переподготовка ИТ-специалистов

ПЛЕНАРНОЕ ЗАСЕДАНИЕ

УДК 629.735.33

Н.Н. Мошак, д-р техн. наук, профессор
Санкт-Петербургский государственный университет телекоммуникаций им. проф.М.А. Бонч-Бруевича

КОНВЕРГЕНЦИЯ МОБИЛНЫХ И ФИКСИРОВАННЫХ СЕТЕЙ СВЯЗИ НА ОСНОВЕВЕ СИСТЕМЫ IMS

Аннотация
Анализируются концепция реализации архитектуры NGN, предложенный группой 3GPP. Обсуждаются способы обеспечения услуг сквозного качества передачи изохронного трафика в сети LTE/IMS в режиме установленного соединения E2E.
Ключевые слова: архитектура NGN, IMS, LTE, соединение E2E в LTE, качество передачи VoLTE/IPTV.
Abstract
The concept of implementing the NGN architecture proposed by the 3GPP group is analyzed. Methods of providing end-to-end isochronous traffic quality services in an LTE/IMS network in established connection mode E2E are discussed.
Key words: NGN architecture, IMS, LTE, LTE E2E connection, VoLTE/IPTV transmission quality.

В основу концепции построения сети связи следующего поколения NGN (Next Generation Network) на базе коммутации пакетов положена идея о создании универсальной сети, которая бы позволяла переносить любые виды информации, а также обеспечивать возможность предоставления широкого спектра инфокоммуникационных услуг в рамках Глобального информационного общества GIS (Global Information Society) с соответствующей Глобальной информационной инфраструктурой GII (Global Information Infrastructure) [1]. Согласно принятой концепции GII должна стать инфраструктурой, которая облегчает развитие, реализацию и взаимодействие существующих и будущих информационных служб, и применений с помощью индустрии телекоммуникаций, информационных технологий, бытовой электроники и производства контента. В рекомендации МСЭ-Т Y.2001 в 2004 году дается определение NGN: «Сеть следующих поколений (Next Generation Network, NGN) – это сеть с пакетной коммутацией, способной предоставлять услуги электросвязи и использующей нескольких широкополосных технологий транспортировки, поддерживающих требуемое качество обслуживания (QoS), в которой связанные с обслуживанием функции не зависят

от примененных технологий, обеспечивающих транспортировку информации. Она обеспечивает свободный доступ пользователей к различным поставщикам услуг и/или выбираемым ими услугами. Она поддерживает универсальную мобильность, которая обеспечивает постоянное и повсеместное предоставление услуг пользователям». Одним из основных свойств NGN является уровневая архитектура. Базовым принципом архитектуры NGN является разделение функции управления и переноса информации, а также функции услуг и приложений от функций сети [2]. Наиболее значимым достоинством такой архитектуры является возможность построения конвергентной сети для всех типов доступа, поскольку уровневая конструкция обеспечивает эффективное введение новых мультимедийных приложений.

Отличительной особенностью логической структуры сетей NGN, является тот факт, что в ней всегда должны быть реализованы три новых базовых функции [3, 4]: функции «управления резервированием ресурса», функции «контроля резервирования ресурса» и функции «совмещения» сервисных информационных потоков SDF (Service Data Flow) в общей физической среде.

В телекоммуникационной индустрии сети следующего поколения NGN разрабатываются, начиная с 90-х годов прошлого столетия, причем каждая из них имеет различное происхождение и проектное решение (ITU-T, 3GPP, ETSI TISPAN, CableLabs, MSF), целью которых является построение полностью конвергированной сети NGN. При этом, она должна не только предоставлять пользователю инфоуслуги современного общества, но также и сетевые услуги существующих сетей связи в рамках новой сетевой парадигмы. В настоящее время архитектура IMS (IP Multimedia Subsystem) рассматривается многими операторами и сервис-провайдерами, а также поставщиками оборудования как возможное решение для построения сетей следующего поколения NGN и как основа конвергенции мобильных и стационарных сетей на платформе IP, т.е. в современном телекоммуникационном мире, идет постепенная миграция к IMS [5]. Сеть IMS строится на архитектуре NGN. Ее авторство принадлежит международному партнерству 3-d Generation Partnership Project (3GPP), объединившему European Telecommunications Standardization Institute (ETSI) и несколько национальных организаций стандартизации. Концепция IMS поддерживает все технологии доступа и обеспечивающая реализацию большого числа инфокоммуникационных услуг, в также дает возможность традиционным телефонным операторам, операторам мобильной связи и различным сервис-провайдерам предлагать свои услуги пользователям всех

типов сетей доступа и всех типов терминалов через единую транспортную сеть на базе протокола IP-MPLS. В IMS применен новый подход к предоставлению услуг, позволяющий оператору внедрять услуги, созданные сторонними разработчиками, не имеющими отношения к поставщикам оборудования. IMS позволяет использовать в системе тарификации более эффективные бизнес-модели.

Основным протоколом плоскости управления IMS является SIP (Session Initiation Protocol), позволяющий устанавливать сессии E2E между пользователями сети и использовать IMS лишь как систему, предоставляющую сервисные функции по безопасности, авторизации, доступу к услугам и т. д. При этом обеспечивается заданное качество услуг QoS (Quality of Services) в сессии E2E. Несколько ролей SIP-серверов или прокси, которые вместе называются функцией управления сеансом вызова CSCF (Call Session Control Function), используются для обработки пакетов сигнализации SIP в IMS. Функция управления сеансом вызова CSCF в зависимости от выполняемой задачи принимает на себя различные роли. Логически он разделяется на прокси-CSCF или посредник для взаимодействия UE с P-CSCF (Proxy-CSCF), посредник для взаимодействия с внешними сетями I-CSCF (Interrogating CSCF) и центральный узел сети IMS обрабатывает все SIP-сообщения, которыми обмениваются оконечные устройства S-CSCF (Serving CSCF). Серверы приложений AS (Application Server) размещают и выполняют службы, а также взаимодействуют с S-CSCF с помощью SIP.

В докладе обсуждаются проблемы и способы обеспечения услуг сквозного качества передачи изохронного трафика в сети LTE/IMS в режиме установленного соединения E2E в развитии идей, изложенных в [6-9].

Библиографический список

1. ITU-T Recommendation Y. 110. Global Information Infrastructure principles and framework architecture. –1998
2. Росляков А. В., Ваняшин С. В., Самсонов М.Ю. и др. Сети следующего поколения NGN/Под ред. А.В. Рослякова. – М.: Эко-Трендз, 2008. – 424с.
3. Мошак Н. Н. Защищенные инфотелекоммуникации. Анализ и синтез. – СПб.: ГУАП, 2014. – 193 с.
4. Мошак Н.Н. Структурный метод анализа базовых функций архитектур сетей LTE и IMS // Перспективные направления развития отечественных информационных технологий: материалы VII межрегиональной научно-практической конф. Севастополь, 21-25 сентября 2021 г. /

Севастопольский государственный университет; науч. ред. Б..В. Соколов. – Севастополь: СевГУ, 2021. – 201с. ISBN 978-5-6044481-1-3 . С.26-37
5. Г.Г. Яновский. Статья «IP Multimedia Subsystem: принципы, стандарты и архитектура». 2006г. Вестник связи URL:http://greenmount.narod.ru/qnowskijGG.html (дата обращения 14.08.2022)
6. Мошак Н.Н., Щербак В.И. Проблемы обеспечения сквозного качества услуг B2C в сети LTE // Информационная безопасность регионов России (ИБРР-2021). XII Санкт-Петербургская межрегиональная конференция. Санкт-Петербург, 27-29 октября 2021 г.: Материалы конференции / СПОИСУ. – СПб., 2021. – 427 с. ISBN 978-5-00182-019-2, с. 177-179. URL: https://pureportal.spbu.ru › files › ibrr2021_materials
7. Мошак Н.Н., Щербак В.И. Способы обеспечения сквозного качества услуг в сети LTE // Региональная информатика и информационная безопасность. Сборник трудов. Выпуск 10 / СПОИСУ. – СПб., 2021. – 406 с. ISBN 978-5-001820-20-8, с 47-53 URL: http://spoisu.ru › riib (дата обращения 14.08.2022)
8. Мошак Н.Н., Харитонов Г.Д. МЕХАНИЗМЫ ОБЕСПЕЧЕНИЯ QOS В СЕТИ LTE. Региональная информатика (РИ-2020). XVII Санкт-Петербургская международная конференция «Региональная информатика (РИ-2020)». Санкт-Петербург, 28-30 октября Р32 2020 г.: Материалы конференции. Часть 2. \ СПОИСУ. – СПб, 2020. – 335 с.
9. ISBN 978-5-907223-86-8, с. 296-297 URL: http://www.spoisu.ru/conf/ri2020/materials (дата обращения 14.08.2022)
10. Н.Н. Мошак, Л.К. Птицына, С.Р. Рудинская. Вербальная модель процесса предоставления услуги VoLTE // Материалы XXVI Международной науч.-техн. конф., «Современные средства связи», 21-22 окт. 2021 года. Минск, Респ. Беларусь; редкол.: А.О. Зенкевич [и др.]. – Минск: Белорусская государственная академия связи, 2021 – 388 с. – с.231-233 ISBN 978-985-585-076-3 URL: bsac.by›sites…basic…conference/sss…2020_10_23.pdf (дата обращения 14.08.2022)

УДК 005.07:004.05.

С. В. Микони, д-р техн. наук, профессор
Санкт-Петербургский Федеральный исследовательский Центр РАН
Санкт-Петербургский институт информатики и автоматизации РАН 14 линия 39, г. 199178, Санкт-Петербург, Россия, 199178
e-mail: smikoni@mail.ru

МОДЕЛЬ МНОГОМЕРНОГО ОЦЕНИВАНИЯ ОБЪЕКТОВ В ЗАДАЧАХ ПРИНЯТИЯ РЕШЕНИЙ

Аннотация
Обосновывается необходимость разделения модели многомерного оценивания на две части – модель предметной области и модель предпочтений ЛПР. Модель ПрО не зависит от решаемой задачи оценивания. Модель предпочтений ЛПР содержит информацию, предназначенную для решения конкретной задачи оценивания. Такое разделение моделей упрощает построение и отладку модели многомерного оценивания объекта для решения задач классификации и упорядочения конечного множества объектов.
Ключевые слова: модель, оценивание, предметная область, предпочтение ЛПР, классификация, упорядочение.

THE MODEL OF MULTIDIMENSIONAL ESTIMATION OF OBJECTS IN DECISION-MAKING TASKS

Abstract
The necessity of dividing the multivariate estimation model into two parts is substantiated – the model of the subject area and the model of preferences of the decision maker. The SbA model does not depend on the estimation problem being solved. The decision maker's preference model contains information intended for solving a specific evaluation problem. This separation of models simplifies the construction and debugging of a multidimensional object estimation model for solving problems of classifying and ordering a finite set of objects.
Key words: model, estimation, subject area, decision maker's preference, classification, ordering.

В работах, посвящённых принятию решений на конечном множестве альтернатив, описание этапов принятия решения слабо увязывается с проектированием модели многомерного оценивания (ММО) [1]. Между тем, трудоёмкость проектирования модели ММО несоизмеримо больше трудоёмкости других этапов принятия решения. Её проектирование осуществляется в два этапа [2].

На первом из них изучаются свойства объекта оценивания и выбираются те из них, которые существенны для решения поставленной задачи. Эту работу выполняют специалисты-предметники.

На втором этапе ЛПР задаёт требования к показателям, отражающим выбранные свойства объекта. Оба этапа выполняются под руководством системного аналитика, отвечающего за качество модели ММО. Сообразно такой последовательности создания модель ММО делится на две части: модель предметной области (ПрО) и модель предпочтений ЛПР.

Модель ПрО представляет собой структуру показателей $R \subseteq J \times J$. В зависимости от числа показателей и их различия определяется число уровней этой структуры, отражающей дерево целей выбора. Узлам нижнего уровня этой структуры соответствуют таблицы «Объекты/ Показатели». Они имеют одинаковое количество строк, именуемых оцениваемыми объектами X, $|X| = N$ и в общем случае разное количество столбцов, именуемых показателями J. Суммарное количество столбцов в таблицах нижнего уровня иерархии равно $n = |J|$. На этом же этапе задаются границы шкалы $[y_{j,\min}, y_{j,\max}]$ j-го показателя, $j \in J$.

Модель предпочтений ЛПР в задаче упорядочения объектов характеризуется следующими параметрами:

1) *важность* (вес) w_j j-го показателя;
2) *целевое значение* c_j j-го показателя;
3) *оценочная функция* $u_j = f_н(y_j)$ полезности j-го показателя;
4) *вид* обобщающей функции.

В задаче определения принадлежности оцениваемого объекта одному из заданных классов параметром 2 являются границы между смежными классами, а параметром 3 – функции принадлежности этим классам. Предлагаемое деление модели ММО на две части позволяет создавать модели разнообразных задач классифицирования и упорядочения объектов на общей модели предметной области. Это создаёт предпосылки для экономичного решения разнообразных задач принятия решений и упрощения отладки их моделей.

Исследования, выполненные по данной тематике, проводились в рамках бюджетной темы FFZF–2022–0004.

Библиографический список

1. Рамеев О.А., Корнеенко В.П. Основы теории многокритерального оценивания объектов с многоуровневой структурой показателей эффективности. –М.: МаксПресс, 2018. –413 с.
2. Микони С.В. Теория принятия управленческих решений: учебное пособие для вузов / С.В. Микони. – 2-е изд. испр. и доп. – СПб.: Лань, 2022. – 384 с.

УДК 004.056

В.С. Сторожик, кандидат технических наук, доцент
Арктический и антарктический научно-исследовательский институт

ТРЕБОВАНИЯ НОРМАТИВНЫХ ПРАВОВЫХ АКТОВ К ОРГАНИЗАЦИОННО-РАСПОРЯДИТЕЛЬНЫМ ДОКУМЕНТАМ ДЛЯ ИНФОРМАЦИОННЫХ СИСТЕМ ПЕРСОНАЛЬНЫХ ДАННЫХ

Аннотация
Рассматриваются нормативные правовые акты, определяющие особенности реализации требований к организационно-распорядительным документам по обеспечению безопасности персональных данных при их обработке в информационных системах.
Ключевые слова: безопасность, защита, информация, информационная система, оператор, мера защиты, персональные данные, система безопасности, средства защиты, требование, уровень защищенности.

Annotation
The normative legal acts defining the specifics of the implementation of the requirements for organizational and administrative documents to ensure the security of personal data during their processing in personal data information systems are considered.
Keywords: security, protection, information, information system, operator, security measure, personal data, security system, means of protection, requirement, security level.

В Стратегии национальной безопасности Российской Федерации поставлена задача обеспечения защиты конституционных прав и свобод человека и гражданина при обработке персональных данных [1].

В докладе Президента Российской Федерации на заседании Совета Безопасности Российской Федерации 20 мая 2022 г. «О повышении устойчивости и безопасности функционирования информационной инфраструктуры государства» подчеркнуто, что принципиально важно свести на нет риски утечек конфиденциальной информации и персональных данных граждан [2].

Требования по обеспечению безопасности персональных данных (ПДн) регулируются российским и международным законодательством.

Федеральный закон от 27 июля 2006 г. № 152-ФЗ «О персональных данных» содержит нормы, соответствующие основным положениям Конвенции Совета Европы о защите физических лиц при автоматизированной обработке персональных данных 1981 г. [3, 4],

Уполномоченным органом Российской Федерации по защите прав субъектов ПДн является Федеральная служба по надзору в сфере связи,

информационных технологий и массовых коммуникаций (Роскомнадзор), подведомственная Министерству цифрового развития, связи и массовых коммуникаций Российской Федерации (Минцифры России) [5].

В рамках своих полномочий [6] во исполнение 152-ФЗ Правительством Российской Федерации постановлением от 1 ноября 2012 г. № 1119 установлены уровни защищенности ПДн при их обработке в информационных системах персональных данных (ИСПДн) в зависимости от угроз безопасности этих данных и требования к защите ПДн при их обработке в ИСПДн, исполнение которых обеспечивает установленные уровни защищенности ПДн [7], а постановлением от 6 июля 2008 г. № 512 установлены требования к материальным носителям биометрических ПДн и технологиям хранения таких данных вне ИСПДн [8].

В соответствии со статьей 19 152-ФЗ меры обеспечения безопасности ПДн устанавливают в пределах своих полномочий ФСТЭК России (не криптографическими способами) и ФСБ России (при использовании криптографических методов защиты информации) [9, 10].

Приказом ФСТЭК России от 17 февраля 2013 г. № 21 утверждены Состав и содержание конкретных организационных и технических мер по обеспечению безопасности ПДн при их обработке в ИСПДн для обеспечения соответствующего уровня защищенности ПДн [11].

Если ПДн обрабатываются в государственной информационной системе (ГИС), то меры по обеспечению безопасности должны приниматься в соответствии с требованиями приказа ФСТЭК России от 11 февраля 2013 г. № 17 [12].

Если защищаемая ИСПДн является значимым объектом критической информационной инфраструктуры [13, 14], то меры по обеспечению безопасности должны приниматься в соответствии с требованиями приказа ФСТЭК России от 25 декабря 2017 г. № 239 [15].

Для определения угроз безопасности ПДн при их обработке в ИСПДн оператору следует опираться на методические документы ФСТЭК России:

1. Базовую модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных [16].

2. Методику оценки угроз безопасности информации [17].

ФСБ России во исполнение части 4 статьи 19 152-ФЗ приказом от 10 июля 2014 г. № 378 утвержден Состав и содержание организационных и технических мер по обеспечению безопасности ПДн при их обработке в ИСПДн с использованием средств криптографической защиты информации (СКЗИ), необходимых для выполнения установленных Правительством Российской Федерации требований к защите ПДн для

каждого из уровней защищенности [18].

Методические рекомендации ФСБ России по разработке нормативных правовых актов, определяющих угрозы безопасности персональных данных, актуальные при обработке персональных данных в информационных системах персональных данных, эксплуатируемых при осуществлении соответствующих видов деятельности, утвержденные руководством 8 Центра ФСБ России 31 марта 2015 г., предназначены для государственных органов и операторов, использующих СКЗИ и разрабатывающих соответствующие модели угроз [19].

Операторам ИСПДн также необходимо руководствоваться следующими методическими документами ФСБ России:

1. Типовыми требованиями по организации и обеспечению функционирования шифровальных (криптографических) средств, предназначенных для защиты информации, не содержащей сведений, составляющих государственную тайну, в случае их использования для обеспечения безопасности персональных данных при их обработке в информационных системах персональных данных [20].

2. Методическими рекомендациями по обеспечению с помощью крипто средств безопасности ПДн при их обработке в ИСПДн с использованием средств автоматизации [21].

С целью обеспечения безопасности ПДн при их обработке в ИСПДн оператором должны быть разработаны организационно-распорядительные документы, предусмотренные нормативными правовыми актами, перечень которых представлен в Таблице.

Разработанные и реализованные оператором организационно-распорядительные документы, предусмотренные нормативными правовыми актами в области обеспечения безопасности ПДн, создают предпосылки для качественного решения задачи обеспечения защиты конституционных прав и свобод человека и гражданина при обработке ПДн в ИСПДн.

Таблица - Организационно-распорядительные документы по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных

№ п/п Наименование организационно-распорядительного документа Ссылка на требования нормативного правового акта – основание для разработки документа

1. Акт определения уровня защищенности ПДн при их обработке в информационной системеПункт 8 Постановления Правительства Российской Федерации от 01.11.2012 № 1119 [7]

2. Документ о назначении должностного лица (работника) опера-

тора, ответственного за обеспечение безопасности ПДн в информационной системе Пункт 14. Постановления Правительства Российской Федерации от 01.11.2012 № 1119 [7];

Пункт 16 Приказа ФСБ России от 10.07.2014 N 378 [18]

3. Перечень лиц, доступ которых к ПДн, обрабатываемым в информационной системе, необходим для выполнения ими служебных (трудовых) обязанностей Пункт 14. Постановления Правительства Российской Федерации от 01.11.2012 № 1119 [7];

Пункт 16 Приказа ФСБ России от 10.07.2014 N 378 [18]

4. Правила доступа в помещения, где размещены используемые средства криптографической защиты информации (СКЗИ), хранятся СКЗИ и (или) носители ключевой, аутентифицирующей и парольной информации СКЗИ, в рабочее и нерабочее время, а также в нештатных ситуациях Пункт 13 Постановления Правительства Российской Федерации от 01.11.2012 № 1119 [7];

Пункт 6 Приказа ФСБ России от 10.07.2014 N 378 [18]

5. Перечень лиц, имеющих право доступа в помещения, где размещены используемые СКЗИ, хранятся СКЗИ и (или) носители ключевой, аутентифицирующей и парольной информации СКЗИ Пункт 6 Приказа ФСБ России от 10.07.2014 N 378 [18]

6. Правила доступа к персональным данным, обрабатываемым в информационной системе персональных данных Статья 19 Федерального закона от 27.07.2006 N 152-ФЗ [3];

Пункт 8.2 Приказа ФСТЭК России от 18.02.2013 № 21 [12]

7. Определение границ контролируемой зоныПункт 10 Приказа ФСБ России от 10.07.2014 N 378 [18]

8. Журнал учета носителей персональных данных с использованием регистрационных (заводских) номеров Пункт 7 Приказа ФСБ России от 10.07.2014 N 378 [18];

ЗНИ.1 Приказа ФСТЭК России от 18.02.2013 N 21 [12]

9. Совокупность предположений о возможностях, которые могут использоваться при создании способов, подготовке и проведении атак, и определение на этой основе и с учетом типа актуальных угроз требуемого класса СКЗИ п. 9 Приказа ФСБ России от 10.07.2014 N 378 [18]

10 Правила генерации и смены паролей пользователей Мера АНЗ.5 раздела VIII. Контроль (анализ) защищенности персональных данных (АНЗ) Приложения к Приказу ФСТЭК России от 18.02.2013 N 21 [12]

Библиографический список

1. Стратегия национальной безопасности Российской Федерации (утв. Указом Президента Российской Федерации от 2 июля 2021 г. № 400).

2. Доклад Президента Российской Федерации В.В. Путина 20 мая 2022 г. на заседании Совета Безопасности Российской Федерации «О повышении устойчивости и безопасности функционирования информационной инфраструктуры государства».
3. Федеральный закон от 27 июля 2006 г. № 152-ФЗ «О персональных данных» (с изменениями и дополнениями).
4. Конвенция Совета Европы о защите физических лиц при автоматизированной обработке персональных данных (Страсбург, 28 января 1981 г.).
5. Постановление Правительства Российской Федерации от 16 марта 2009 г. № 228 «О Федеральной службе по надзору в сфере связи, информационных технологий и массовых коммуникаций».
6. Федеральный конституционный закон от 6 ноября 2020 г. № 4-ФКЗ «О Правительстве Российской Федерации».
7. Постановление Правительства Российской Федерации от 1 ноября 2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных».
8. Постановление Правительства Российской Федерации от 6 июля 2008 г. № 512 «Об утверждении требований к материальным носителям биометрических персональных данных и технологиям хранения таких данных вне информационных систем персональных данных».
9. Указ Президента Российской Федерации от 16 августа 2004 г. № 1085 «Вопросы Федеральной службы по техническому и экспортному контролю».
10. Указ Президента Российской Федерации от 11 августа 2003 г. № 960 «Вопросы Федеральной службы безопасности Российской Федерации».
11. Приказ ФСТЭК России от 17 февраля 2013 г. № 21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных».
12. Приказ ФСТЭК России от 11 февраля 2013 г. № 17 «Об утверждении требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах».
13. Федеральный закон от 26 июля 2017 г. N 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации».
14. Постановление Правительства Российской Федерации от 8 февраля 2018 г. № 127 «Об утверждении Правил категорирования объектов критической информационной инфраструктуры Российской Федерации, а

также перечня показателей критериев значимости объектов критической информационной инфраструктуры Российской Федерации и их значений».

15. Приказ ФСТЭК России от 25 декабря 2017 г. № 239 «Об утверждении Требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации» (в ред. приказа ФСТЭК России от 26 марта 2019 г. № 60).

16. Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных, утверждена ФСТЭК России 15 февраля 2008 г.

17. Методика оценки угроз безопасности информации, утверждена ФСТЭК России 5 февраля 2021 г.

18. Приказ ФСБ России от 10 июля 2014 г. № 378 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных Правительством Российской Федерации требований к защите персональных данных для каждого из уровней защищенности».

19. Методические рекомендации по разработке нормативных правовых актов, определяющих угрозы безопасности персональных данных, актуальные при обработке персональных данных в информационных системах персональных данных, эксплуатируемых при осуществлении соответствующих видов деятельности, утверждены руководством 8 Центра ФСБ России 31 марта 2015 г. № 149/7/2/6-432.

20. Типовые требования по организации и обеспечению функционирования шифровальных (криптографических) средств, предназначенных для защиты информации, не содержащей сведений, составляющих государственную тайну, в случае их использования для обеспечения безопасности персональных данных при их обработке в информационных системах персональных данных», утверждены руководством 8 Центра ФСБ России 21 февраля 2008 г. № 149/6/6-622.

21. Методические рекомендации по обеспечению с помощью крипто средств безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств автоматизации, утверждены 8 Центром ФСБ России 21 февраля 2008 г. № 149/54-144.

УДК 623.41: 681.3
Д.В.Моисеев, доктор технических наук, профессор
Севастопольский государственный университет
ул. Университетская 33, г. Севастополь, Россия, 299053

ПРЕИМУЩЕСТВА ПРИМЕНЕНИЯ НЕПОЗИЦИОННОЙ ФОРМЫ ПРЕДСТАВЛЕНИЯ ИНФОРМАЦИИ В ВИДЕ ВЕРОЯТНОСТНЫХ ОТОБРАЖЕНИЙ В СИСТЕМАХ УПРАВЛЕНИЯ РАКЕТНЫМ ОРУЖИЕМ

Аннотация

В работе рассматривается принципиальная возможность применения вероятностной формы представления информации в системах управления ракетным оружием с целью значительного сокращения аппаратного объема бортовых систем управления, повышения их быстродействия и помехозащищенности.

Annotation

The paper considers the fundamental possibility of using a probabilistic form of information representation in missile weapon control systems in order to significantly reduce the hardware volume of on-board control systems, increase their performance and noise immunity.

Введение. Настоящий период развития вычислительной техники характеризуется интенсивным поиском принципиально новых методов обработки и хранения информации, построения универсальных и специализированных вычислительных архитектур, и систем на их основе с привлечением современных технологий, среди которых цифровая обработка сигналов является одной из наиболее востребованных [1].

Благодаря современным достижениям в области нано- и микроэлектроники в новейших информационно-измерительных и управляющих системах цифровая обработка сигналов, как известно, успешно применяется для фильтрации и кодирования речевых и звуковых сигналов, обработки изображений и измерительной информации, спектрального анализа цифровой звуко- и видеозаписи, в радиотехнических системах и системах телекоммуникаций, управления и робототехники, защиты информации в таких областях, как связь, мультимедиа, телефония и телевидение, радиолокация и радионавигация, гидроакустика, медицина и системах управления ракетным оружием всех уровней.

Для цифровой обработки сигналов, используемой в последние десятилетия, характерно наличие огромных объемов вычислений над массивами данных большой разрядности, проводимых в реальном масштабе времени [2].

Стремление к улучшению энергетической эффективности и универсальности устройств цифровой обработки сигналов приводит к усложнению вычислительных алгоритмов, обострению проблемы аппаратурных затрат, быстродействия, точности и повышению требований к отказоустойчивости устройств и помехоустойчивости каналов связи при передаче данных, что особо остро начинает ощущаться в условиях наложений санкций на высокотехнологические решения, а также необходимостью выполнения импортозамещения отечественных микросхем и элементной базы, используемых, в частности, в системах управления ракетным оружием.

В связи с этим особую актуальность приобретают исследования в области одного из направлений развития параллельных вычислительных технологий, связанные с разработкой методов, алгоритмов и устройств вычислительной техники для цифровой обработки сигналов с применением непозиционных систем счисления, наиболее перспективной из которых является вероятностная форма представления информации.

С развитием цифровой вычислительной техники и методов имитационного моделирования стал широко использоваться метод статистических испытаний, основная идея которого – связь между вероятностными характеристиками случайных процессов и величинами, являющимися решениями задач математического анализа [3].

Постановка задачи. В настоящий момент, в связи с достижениями научно-технического прогресса четко прослеживаются следующие тенденции в развитии систем управления ракетным оружием:

1. Переход на цифровую обработку сигналов.

2. Импортозамещение элементной базы в отечественной микроэлектронике.

3. Реализация «Сетецентрического» принципа управления в возможных военных конфликтах.

Данные требования времени, в свою очередь, требуют от разработчиков и проектировщиков систем управления ракетным оружием:

- уменьшения на порядки времени реакции БЦВМ для возможности управления в режиме реального времени;

- необходимости повышения пропускной способности и защищенности каналов связи, что выражается:

а) необходимостью внедрения новых протоколов передачи данных;

б) повышением помехозащищенности существующих и перспективных каналов передачи данных;

в) криптографической стойкостью информации, передаваемой по закрытым каналам связи.

- необходимости увеличения времени автономной работы мобильных устройств (таких как БПЛА);

- повышения надёжности и стойкости к внешним воздействиям схемотехнических решений, блоков и элементов.

Решение задачи. Как известно, основными достоинствами вероятностных вычислительных устройств, обрабатывающих информацию, представленную в непозиционной форме в виде вероятностных отображений, являются: простота схемных решений; высокая помехозащищённость; низкий, сравнительно с аналогичными цифровыми устройствами, аппаратный объём [3].

В качестве примера, для анализа преимуществ, получаемых от использования вероятностной формы представления информации, предлагаем рассмотреть типовой пример вероятностной вычислительной машины.

В общем случае схема типовой вероятностной машины предполагает наличие следующих устройств [3-4]: устройства ввода информации, служащие для преобразования дискретной и аналоговой информации в непозиционное представление в виде вероятностных отображений; стохастические вычислительные устройства (СВУ); устройства вывода информации, преобразовывающие результирующие вероятности случайных двоичных символов в цифровую или аналоговую форму; генераторы случайных и псевдослучайных чисел (ГСЧ и ГПСЧ), служащие для формирования стохастических констант и случайных сигналов; устройство управления.

Сердцем любой БЦВМ, является микропроцессор, в случае вероятностной схемотехники – стохастические вычислительные устройства, ядром которого выступает вероятностное арифметическое устройство (см. Рис. 1.).

В состав схемы вероятностного арифметического устройства входят: генератор тактовых импульсов (ГТИ), выполняющий задающую и синхронизирующую функции; дешифратор команд (ДК) на три входа; четырехвходовой дизъюнктор; счетчик результата; блок переписи результата; регистр результата; генератор случайных равномерно распределенных чисел (ГСРРЧ), а также блоки выполнения арифметических операций: блок деления; блок умножения; блок сложения; блок вычитания; блок возведения в целую положительную степень.

Как известно, в существующих универсальных процессорах реализация всего имеющегося функционала производится через выполнения

операции сложения и сдвига, что в значительной степени замедляет их работу.

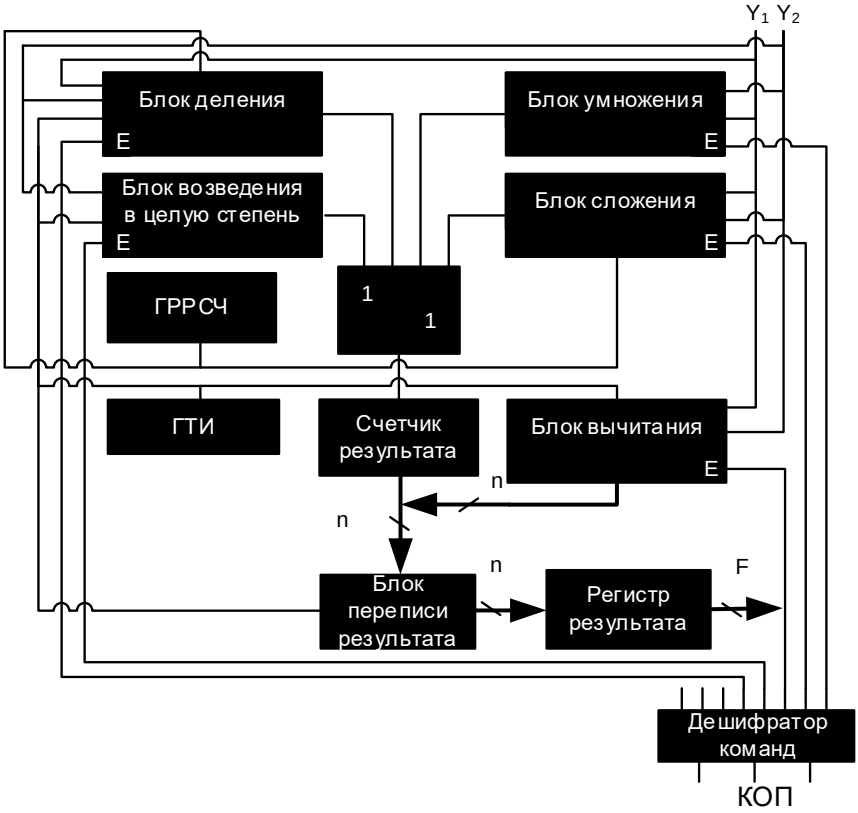


Рис. 1 – Вероятностное арифметическое устройство.

В качестве основного преимущества применения непозиционного вероятностного представления информации при реализации цифровой обработки сигналов можно выделить многократное уменьшение аппаратного объема вычислительных устройств, входящих в состав вероятностного арифметического устройства:

– при выполнении сложения двух операндов аппаратурный объем вероятностного сумматора составит 13 базовых логических элементов,

в то время как аппаратурный объем параллельного 16-разрядного комбинационного сумматора составит 181 элемент, что на уровне логического элемента превышает предложенное решение в 14 раз;

– при умножении двух двухбайтовых двоичных чисел потребуется множительное устройство, число элементов булева базиса, в котором составит около 700, в то время как вероятностное множительное устройство будет реализовано на трех конъюнкторах;

– схема возведения в квадрат в вероятностной форме реализуется на двух элементах, а с увеличением степени количество элементов будет равно 2^n, где n – это степень, что дает преимущество по сравнению с цифровым устройством приблизительно в 300 раз;

– аппаратурный объем предложенного вероятностного делителя по сравнению с цифровым меньше примерно в 6 раз.

Таким образом суммарный аппаратный объём вероятностного арифметического устройства в целом меньше в 150 раз по сравнению с цифровыми аналогами.

В качестве примера преимуществ, получаемых от специализированных вероятностных процессоров, рассмотрим схемотехнические ращения вероятностного коррелометра и вероятностного спектрометра. Первый может быть использован в корреляционно-экстремальных системах наведения крылатых ракет, что повысит точность их выхода к цели [4]. Его аппаратный объём меньше цифрового аналога на два порядка, а производительность выше на один порядок.

Вероятностный спектрометр меньше классического цифрового в 20 раз и быстрее в 6 раз и может быть использован в оптических или тепловых головках наведения ЗУР и повысить их вероятность поражения цели [3].

Выводы. Таким образом, становится очевидным тот факт, что применение в системах управления ракетным оружием непозиционной формы представления информации в виде вероятностных отображений позволит:

1) Уменьшить аппаратный объём бортовых вычислительных устройств и тем самым:

- повысить мощность боевой части ракет;
- увеличить время автономной работы мобильных устройств (например, БПЛ);
- увеличить запас топлива, тем самым увеличив радиус поражения;
- повысить надёжность блоков, микросхем и элементов;
- уменьшить стоимость проектирования, производства и эксплуатации изделий.

2) Повысить быстродействие при решении специфических вычислительных задач и, как следствие:

- повысить точность наведения КР и ЗУР;
- увеличить количество поражаемых целей и скорострельность.

3) Повысить помехозащищённость каналов связи и повысить криптографическую стойкость информации, передаваемой по ним.

ЛИТЕРАТУРА

1. Лебедев Е.К., Галанина Н.А. Сравнительный анализ позиционной и непозиционной обработки информации сигнальными процессорами // Динамика нелинейных дискретных электротехнических и электронных систем: материалы V Всерос. науч. конф. – Чебоксары: Изд-во Чуваш. ун-та, 2003. – С. 193–196.

2. . Дзегеленок И.И, Оцоков Ш.А. Алгебраизация числовых представлений в обеспечении высокоточных суперкомпьютерных вычислений // Вестник МЭИ. – 2010. – № 3. – С. 107–116.

3. Моисеев Д.В. Сравнение различных форм непозиционного вероятностного отображения информации / Д.В. Моисеев, О.Д. Чужикова-Проскурнина, Н.Е. Сапожников // Системы контроля окружающей среды, ФГБНУ «Институт природно-технических систем» – Севастополь, 2016. – № 4 (24). – С. 68–74.

4. Моисеев Д.В. Применение вероятностной формы представления данных в корреляционно-экстремальных системах / Д.В. Моисеев, О.Д. Чужикова-Проскурнина, Н.Е. Сапожников // Системы контроля окружающей среды, ФГБНУ «Институт природно-технических систем» – Севастополь, 2016. – № 5 (25). – С. 47–52.

ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ В КРИТИЧЕСКИХ ИНФРАСТРУКТУРАХ. ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

УДК 004.056.53

А.В. Селезнев, канд. техн. наук, В.А. Саяркин, И.Б. Паращук, д-р техн. наук, профессор
Военная академия связи
г. Санкт-Петербург, Россия

АНАЛИЗ ТРЕБОВАНИЙ К ПРОГРАММНО-АППАРАТНОЙ РЕАЛИЗАЦИИ И ОБЗОР ПРИНЦИПОВ ПОСТРОЕНИЯ СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ ДЛЯ СОВРЕМЕННЫХ СИСТЕМ ЭЛЕКТРОННОГО ДОКУМЕНТООБОРОТА

Аннотация
Доклад посвящен анализу концептуальных и целевых требований к программно-аппаратной реализации средств обеспечения безопасности информации для современных систем электронного документооборота. Рассмотрены базовые принципы, обуславливающие набор требований к построению и функционированию средств и комплексов такого класса. Результаты анализа призваны помочь при разработке и технической реализации высокоэффективных средств защиты информации для современных систем обработки электронных документов, использующих различные каналы и тракты информационного обмена.
Ключевые слова: средства защиты информации, система электронного документооборота, электронный документ, принципы, требования.

Annotation
The report is devoted to the analysis of conceptual and target requirements for software and hardware implementation of information security tools for modern electronic document management systems. The basic principles that determine the set of requirements for the construction and operation of facilities and complexes of this class are considered. The results of the analysis are intended to help in the development and technical implementation of highly effective information security tools for modern electronic document processing systems using various channels and paths of information exchange.
Keywords: information security tools, electronic document management system, electronic document, principles, requirements.

Развитие современного информационного общества невозможно без инновационных решений в рамках совершенствования IT-

инфраструктуры. При этом различные грани совершенствования IT-инфраструктуры отражают как эволюционные процессы в информационном пространстве страны, так и частные процессы развития инфокоммуникаций в экономике, здравоохранении и в других областях деятельности. Одним из ключевых элементов построения современной IT-инфраструктуры практически любого масштаба, являются системы электронного документооборота (ЭДО) [1].

Системы ЭДО представляют собой совокупность взаимосвязанных программных средств, предназначенных для выполнения полного перечня работ с электронными документами, необходимых пользователю. Это комплексное общесистемное прикладное программное обеспечение, позволяющее организовать работу с электронными документами (создание, изменение, поиск), а также взаимодействие между должностными лицами (передачу документов, выдачу заданий, отправку уведомлений и т.п.). Системы ЭДО являются организационно-техническими объектами, предназначенными для обеспечения процессов создания, управления доступом и распространения электронных документов, а также для обеспечения контроля над потоками документов [2]. Рынок средств и технологий ЭДО стремительно развивается, но особое внимание специалистов сосредоточено на поиске новых технических и программных решений по защите информации, циркулирующей и хранящейся в системах ЭДО [3].

Обеспечение защиты информации в современных системах ЭДО предполагает создание препятствий для любых несанкционированных попыток хищения или модификации обрабатываемой, передаваемой или хранимой здесь информации. Рассмотрим требования к программно-аппаратной реализации средств защиты информации (СрЗИ), использующих методы и алгоритмы обеспечения защищенности электронных документов (ЭД) от нежелательного (для соответствующих субъектов информационных отношений) их разглашения (нарушения конфиденциальности), искажения (нарушения целостности), утраты или снижения степени доступности информации, а также незаконного их тиражирования.

Средства защиты информации, в самом общем виде, могут быть определены как организованная совокупность всех программно-аппаратных решений, методов и мероприятий, выделяемых (предусматриваемых) в современных системах ЭДО для решения в них выбранных задач защиты ЭД.

Важнейшим концептуальным требованием к программно-аппаратной реализации СрЗИ является требование адаптируемости, т.е., способность к целенаправленному их приспособлению при изменении

структуры, технологически схем или условий функционирования систем ЭДО.

К программно-аппаратной реализации СрЗИ предъявляется еще целый ряд более конкретных, целевых требований, которые могут быть разделены на функциональные, эргономические, экономические, технические и организационные. В процессе развития работ по защите информации, наряду с разработками конкретных вопросов защиты систем ЭДО, формировались общеметодологические принципы программно-аппаратной реализации СрЗИ. Перечень принципов программно-аппаратной реализации СрЗИ для систем ЭДО включает: концептуальное единство – архитектура, технология, организация и обеспечение функционирования СрЗИ и их компонентов должны реализовываться в строгом соответствии с положениями единой концепции защиты информации; адекватность требованиям – СрЗИ должны строиться в строгом соответствии с требованиями к защите и значениями параметров, влияющих на защиту информации; функциональная самостоятельность – предполагает, что СрЗИ должны быть самостоятельными обеспечивающими подсистемами систем ЭДО, должны не зависеть от других подсистем; удобство использования – СрЗИ не должны создавать дополнительных неудобств для пользователей и персонала систем ЭДО; минимизация предоставляемых прав – каждому пользователю систем ЭДО должны представляться лишь те полномочия на доступ к ЭД, которые ему действительно необходимы для выполнения своих функций; полнота контроля – все процедуры ЭДО должны контролироваться СрЗИ в полном объеме, причем основные результаты контроля должны фиксироваться в специальных регистрационных журналах; активность реагирования – СрЗИ должны реагировать на любые попытки несанкционированных действий; экономичность СрЗИ для систем ЭДО – при условии соблюдения основных требований всех предыдущих принципов расходы на такие средства должны быть минимальными.

Таким образом, рассмотрены концептуальные и целевые требования к программно-аппаратной реализации СрЗИ для современных систем ЭДО. Сформулированы принципы построения и функционирования средств такого класса. Предполагается, что следование данным принципам и выполнение рассмотренных требований позволит осуществить разработку и техническую реализацию высокоэффективных СрЗИ, нацеленных на защиту данных, циркулирующих в современных системах автоматизированной обработки ЭД.

Библиографический список

1. Коржук В. М., Попов И. Ю., Воробьева А. А., Защищенный документооборот. Часть 1: Учебно-методическое пособие – СПб: Университет ИТМО, 2021. 67 с.
2. Булдакова Т. И., Глазунов Б. В., Ляпина Н. С. Оценка эффективности защиты систем электронного документооборота // Доклады Томского государственного университета систем управления и радиоэлектроники, №1 (25), Ч. 2, 2012. С. 52–56.
3. Селезнев А. В., Паращук И. Б., Саяркин В. А. Современный электронный документооборот в автоматизированных системах диспетчерского управления движением поездов: вопросы защиты информации // Материалы V-й международной научно-практической конференции «Инновационная железная дорога. Новейшие и перспективные системы обеспечения движения поездов. Проблемы и решения». Сборник статей // Под общей редакцией Яшина М.Г. – СПб., Петергоф: ВИ (ЖДВ и ВОСО), 2022. С. 405–413.

УДК 004.056.53
И.В. Морозов, В.А. Сундуков, И.Б. Паращук, д-р техн. наук, профессор
Военная академия связи
г. Санкт-Петербург, Россия

ТРЕБОВАНИЯ К СРЕДСТВАМ МНОГОФАКТОРНОЙ АУТЕНТИФИКАЦИИ ПОЛЬЗОВАТЕЛЕЙ В ИНТЕРЕСАХ ЗАЩИТЫ ИНФОРМАЦИИ В КРИТИЧЕСКИХ ИНФРАСТРУКТУРАХ

Аннотация
Доклад посвящен анализу основных требований и критериев сравнительной оценки средств многофакторной аутентификации пользователей при доступе к информационным ресурсам критических инфраструктур. Проведен анализ классификационных признаков различных затрат на поддержание работоспособности таких систем, средств и комплексов, учитывая затраты на ликвидацию последствий нарушения политики информационной безопасности и последствий реализации угроз несанкционированного доступа в критических инфраструктурах.
Ключевые слова: критическая инфраструктура, система, средства, многофакторная аутентификация, пользователь, требования, критерии, информационные ресурсы.
Annotation
The report is devoted to the analysis of the main requirements and criteria for the comparative evaluation of the means of multi-factor authentication of users when accessing information resources of critical infrastructures. The analysis of classification features of various costs for maintaining the operability of such systems, facilities and complexes is carried out, taking into account the costs of eliminating the consequences of violating the information security policy and the consequences of the implementation of unauthorized access threats in critical infrastructures.
Keywords: critical infrastructure, system, tools, multi-factor authentication, user, requirements, criteria, information resources.

Анализ современных тенденций в формах и методах обеспечения защиты информации (ЗИ) в критических инфраструктурах (КИ) показывает, что по-прежнему наиболее важны такие аспекты безопасности, как предотвращение несанкционированного доступа нелегитимных пользователей к информационным ресурсам инфраструктур такого класса [1].

Эти целям традиционно служат современные средства многофакторной аутентификации (МФА) пользователей при их доступе к информационным ресурсам КИ, причем, к таким средствам предъявляются

особые критерии сравнительной оценки и особые требования. Подразумевается, что аутентификация – это проверка подлинности идентификации пользователя, процесса, устройства или другого компонента КИ (обычно осуществляется перед разрешением доступа к информационным ресурсам КИ).

К информационным ресурсам КИ относят всю совокупность данных, организованных для эффективного получения достоверной информации в интересах обеспечения бесперебойного функционирования таких инфраструктур. При этом МФА – метод контроля доступа, расширенная аутентификация, когда, прежде чем получить доступ к информационным ресурсам КИ, подтверждение пользователем своей личности происходит с использованием, как минимум, двух различных факторов проверки. Одна из основных задач средств МФА – обеспечение надежной проверки подлинности и верификации любого пользователя, которого можно однозначно аутентифицировать по тому, что он знает (имя и пароль); что он имеет (специальный ключ – уникальный идентификатор); что он из себя представляет (признаки, которые присущи только ему). Конкретные механизмы МФА пользователей могут быть реализованы на основе паролей; технических средств; средств биометрии; криптографии с уникальными ключами для каждого пользователя КИ.

С точки зрения детализации требований можно сформулировать систему (группы) требований к средствам МФА, а также к процессу их функционирования. Применение методов и мероприятий контроля несанкционированного доступа и диагностики систем защиты, выполнение их в установленные сроки и с наилучшим из возможных результатов рассматривается как одно из важнейших направлений для формирования ключевых критериев сравнительной оценки качества средств МФА пользователей при доступе к информационным ресурсам КИ. Предлагается выделять следующие группы критериев: событийные (смысловые, содержательные, процессные) – критерии оценки, отражающие выполнение или невыполнение МФА своей миссии; временные – критерии оценки, отражающие своевременность выполнения различных методов аутентификации (оценивается соблюдение сроков аутентификации); результативные – критерии оценки МФА, отражающие эффективность и результативность проведенной аутентификации при конкретной угрозе (оценивается достижение целевых значений исходов МФА).

В этой связи предлагается сформулировать и проанализировать базовые требования к современным средствам МФА, В частности, могут быть предъявлены функциональные требования: оповещение (должна

быть предусмотрена возможность отправки оповещений о происходящих событиях – нарушениях или попытках нарушений доступа к ресурсам); удаленное управление (возможность управления всеми средствами МФА с одного рабочего места); ведение журналов; производительность систем МФА (необходимо регулировать уровень нагрузки); защита от различных типов (факторов, признаков) несанкционированного доступа; постоянная защита рабочих станций КИ; автоматическое обновление базы типов (факторов, признаков) несанкционированного доступа [2, 3].

Кроме того, средства МФА должны обеспечивать регулярное обновление используемой базы шаблонов, содержать в себе механизмы поиска ранее неизвестных признаков пользователей при многофакторной аутентификации, как наиболее распространенных и опасных в настоящее время.

Особые требования предъявляются к затратам ресурсов на осуществление процедур МФА. Как правило, это затраты: на формирование и поддержание управления средствами МФА (организационные затраты); на контроль, то есть на подтверждение достигнутого уровня защиты; внутренние и внешние затраты на ликвидацию последствий нарушений политики информационной безопасности КИ; затраты на техническое обслуживание средств МФА [4].

Таким образом, проведен анализ основных критериев сравнительной оценки и требований к средствам МФА пользователей при их доступе к информационным ресурсам КИ. Рассмотрены вопросы классификации затрат на поддержание работоспособности таких средств, учитывая затраты на ликвидацию последствий нарушения политики информационной безопасности критических инфраструктур.

Библиографический список

1. Андриянова Т. А., Саломатин С. Б. Комплексная оценка безопасности ведомственных сетей // Доклады Белорусского государственного университета информатики и радиоэлектроники. 2017, Том 109, №7, С.40–44.
2. Виткова Л. А., Паращук И. Б. Анализ современных инновационных решений по выявлению отклонений в эвристиках трафика сверхвысоких объемов для обнаружения сетевых атак и защиты от них // Региональная информатика и информационная безопасность. Сборник трудов. Выпуск 8 / СПОИСУ. – СПб.: 2020. С. 99–102.
3. Бабошин В. А., Паращук И. Б., Сундуков В. А. Анализ общих требований к средствам многофакторной аутентификации пользователей

железнодорожных систем автоматики, телемеханики и связи // Материалы V-й международной научно-практической конференции «Инновационная железная дорога. Новейшие и перспективные системы обеспечения движения поездов. Проблемы и решения». Сборник статей // Под общей редакцией Яшина М.Г. – СПб, Петергоф: ВИ (ЖДВ и ВОСО), 2022. С. 89–98.
4. Цуканова О. А., Смирнов С. Б. Экономика защиты информации: учебное пособие, 2-е издание, измененное и дополненное. – СПб.: НИУ ИТМО, 2014. – 79 с.

УДК 591.6
Т.А. Агасиев, к.т.н., доцент, А.П. Карпенко, д. ф.-м. н., профессор, С.Ю. Чуриков, магистр
МГТУ им. Н.Э. Баумана

АДАПТАЦИИ ПЛАНА ЭКСПЕРИМЕНТА ДЛЯ ПОВЫШЕНИЯ КАЧЕСТВА СУРРОГАТНОЙ МОДЕЛИ В ЗАДАЧЕ ГЛОБАЛЬНОЙ ОПТИМИЗАЦИИ

Аннотация
Рассматриваем суррогатное моделирование в задаче глобальной оптимизации. Представляем авторский алгоритм, предназначенный для адаптивного улучшения плана эксперимента, на основе которого осуществляется построение начальной суррогатной модели целевой функции. Приводим описание программной реализации алгоритма, а также результаты вычислительных экспериментов.
Ключевые слова: глобальная оптимизация, суррогатное моделирование, адаптация плана эксперимента.
Annotation
We consider surrogate modeling in the global optimization problem. We present the author's algorithm for adaptive improvement of the experimental design, on the basis of which an initial surrogate model of the objective function is built. We present a description of the software implementation of the algorithm, as well as the results of computational experiments.
Keywords: global optimization, surrogate modeling, adaptive design of experiment.

В процессе решения многих практических задач глобальной оптимизации необходимо многократно определять значения целевой функции $f(X)$, имеющей высокую вычислительную сложность. С целью экономии вычислительных ресурсов в этом случае применяют быстро вычислимую аппроксимирующую (суррогатную) модель $\hat{f}(X,\theta)$ этой функции, где θ - вектор свободных параметров модели. Для построения этой модели, полагаем, имеется набор точек $\mathbf{X}$ в пространстве варьируемых переменных (план эксперимента) и значения целевой функции F в этих точках – обучающая выборка $S=\{X_i,\ f_i\}_{i=1}^{|S|}=\{\mathbf{X},F\}$. Здесь $f_i=f(X_i);\ X_i\in D_X\subset\Re_{|X|}$, где D_X - $|X|$-мерный параллелепипед допустимых значений варьируемых

параметров X. От плана эксперимента $\{X_i\}_{i=1}^{|S|} = \mathbf{X} \in \chi$ может существенно зависеть качество начальной суррогатной модели и, как следствие, эффективность решения задачи оптимизации с использованием этой модели [1] (здесь χ - множество допустимых планов).

Исходную (базовую) задачу глобальной параметрической оптимизации ставим в виде: $f(X) \to \min,\ X \in D_X$. Процесс построения суррогатной модели $\hat{f}(X,\theta)$ требует решения вспомогательной задачи оптимизации $\min\limits_{\theta} err(\hat{f}(X,\theta),\ f(X))$, где $err(\cdot,\cdot)$ - ошибка модели, в качестве которой рассматриваем среднеквадратичную ошибку аппроксимации функции $f(X)$ в точках плана эксперимента $\mathbf{X}$. Качество этого плана формализуем с помощью критерия $\Phi(\mathbf{X})$, так что искомый наилучший план эксперимента $\mathbf{X}^*$ определяет равенство $\mathbf{X}^* = \arg\min \Phi(\mathbf{X})$, $\mathbf{X} \in \chi$.

Предлагаем следующую схему адаптивного построения плана эксперимента $\mathbf{X}^*$ [2].

1) Генерируем начальный план эксперимента $\mathbf{X}$ с небольшим числом точек и вычисляем значения целевой функции $f(X)$ в точках этого плана.

2) Итерационно выполняем следующие действия.

а) Строим суррогатную модель с помощью текущей обучающей выборки $\{\mathbf{X}, F\}$.

б) Выбираем новую допустимую точку X^{new}, исходя из условия $X^{new} = \arg\min \Phi(\mathbf{X} \bigcup X),\ X \in D_X$.

в) Вычисляем значения целевой функции $f(X^{new})$ и дополняем обучающую выборку новым элементом: $S = S \bigcup \{X^{new},\ f(X^{new})\}$.

Возможные условия останова: число новых точек плана эксперимента превышает заданное максимальное число; ошибка *err* текущей суррогатной модели меньше допустимой; значение критерия $\Phi(\mathbf{X})$ меньше заданного.

Для реализации прототипа программной системы выбран язык программирования *Python*. В системе использованы известные библиотеки *numpy, scipy, Skikit Learn, jMetalPy, SMAC3, PyQt5, matplotlib.* В программной системе реализованы следующие суррогатные модели:

линейная регрессия на основе радиальных базисных функций; суррогатная модель на основе гауссовских процессов [3]; модель на основе решающих деревьев [4]. При построении суррогатной модели используем кросс-валидацию и регуляризацию на основе аддитивной штрафной функции. В качестве критерия качества плана эксперимента $\Phi(\mathbf{X})$ могут быть использованы [5]: наименьшее расстояние между точками плана эксперимента; наибольшее евклидово расстояние между соседними точками плана эксперимента; -критерий; отклонение оценки функции распределения точек плана от равномерного распределения; рассеяние расстояний до соседних точек плана.

Представляем некоторые результаты вычислительных экспериментов. В качестве суррогатной модели использована модель линейной регрессии с гауссовыми радиальными функциями в качестве базисных (два свободных параметра – параметр радиальной базисной функции и коэффициент регуляризации). Рассматриваем три тестовых функции: функция Розенброка; функция Стыбинского-Танга; функция Захарова. Начальный план эксперимента генерируем случайным образом; измерения повторяем 30 раз для каждой из тестовых функций с различным числом варьируемых параметров $|X| \in \{2, 4, 8\}$ и типом суррогатной модели, определяемым значениями свободных параметров. Для каждой такой комбинации варьируем число новых точек плана эксперимента от одной до 40. Точность полученных суррогатных моделей сравниваем с точностью моделей, полученных путем дополнения плана эксперимента случайным образом.

Результаты вычислительного эксперимента показывают, что предложенный в работе алгоритм коррекции плана эксперимента позволяет повысить точность начальной суррогатной модели целевой функции до 47% по сравнению с моделью, построенной на основе случайного плана эксперимента.

Работа поддержана грантом ФЗ-20200929364 Ministry of Innovative Development of the Republic of Uzbekistan.

Библиографический список

1. Díaz-Manríquez A., Toscano-Pulido G., Gómez-Flores W. On the selection of surrogate models in evolutionary optimization algorithms // IEEE congress of evolutionary computation. 2011. P. 2155-2162.
2. Bhosekar A., Ierapetritou M. Advances in surrogate-based modeling, feasibility analysis, and optimization: A review // Computers & Chemical Engineering. 2018. V. 108. P. 250-267.
3. Schulz E., Speekenbrink M., Krause A. A tutorial on Gaussian process

regression: Modelling, exploring, and exploiting functions // Journal of Mathematical Psychology. 2018. V. 85. P. 1-16.
4. Moisen G. G. Classification and regression trees // In: Jørgensen, Sven Erik; Fath, Brian D.(Editor-in-Chief). Encyclopedia of Ecology, volume 1. Oxford, UK: Elsevier. 2008. P. 582-588.
5. Pronzato L., Müller W. G. Design of computer experiments: space filling and beyond //Statistics and Computing. 2012. V. 22. №. 3. P. 681-701.

УДК 681.32

С.А. Державин, аспирант, А.С. Гейда, доктор технических наук, старший научный сотрудник Санкт-Петербургского федерального исследовательского центра РАН, доцент, И. П. Колосов, аспирант, В.С. Резанова, аспирант

Российская академия народного хозяйства и государственной службы

КОНЦЕПЦИЯ МАЙНИНГА ИНФОРМАЦИИ, ДЕЙСТВИЙ, СОСТОЯНИЙ ПРИ ИСПОЛЬЗОВАНИИ ИНФОРМАЦИИ ДЛЯ ФУНКЦИОНИРОВАНИЯ СИСТЕМ

Аннотация

Цифровая трансформация экономики и общества вызывает много задач, решаемых практиками и теоретикам при проектировании и использовании информационных технологий. Для успешного решения многих из этих задач требуется исследование результатов использования информационных технологий еще на стадии проектирования систем, в которых эти технологии используются, на математических моделях, описывающих будущее использование информационных технологий при функционировании систем. Однако, прогнозные математические модели, связывающие показатели успешности использования информационных технологий с характеристиками этих технологий и характеристиками функционирования систем пока еще не разработаны в должной мере. Недостаточно подробно описаны концептуальные и методологические основания такого моделирования. Моделирование использования информации связано с построением значительного числа возможных последовательностей причинно-следственных связей информационных и других действий, вызываемых ими цепочек событий и состояний при функционировании. Частично такие цепочки могут быть получены за счет майнинга процессов. Однако, множество всех возможных цепочек может быть получено на этапе проектирования лишь частично, в связи с тем, что такие цепочки могут быть новыми. Для получения множеств возможных цепочек действий, событий и состояний предложено разработать технологии синтеза множеств возможных цепочек действий, событий и состояний. Представленный в докладе материал должен позволить преодолеть имеющееся несоответствие и перейти к построению требуемых моделей цепочек действий, событий и состояний на этапе проектирования.

Ключевые слова: майнинг, процессный майнинг, майнинг информации, моделирование, методы, машинное обучение.

Annotation
The digital transformation of the economy and society caused many problems in the design and use of information technologies to be solved by practitioners and theorists. To successfully solve many of these problems, it is necessary to study the results of the use of information technologies at the design stage of the systems. Such results of the use of information technologies shall be studies on mathematical models predicting the future use of information technologies in the functioning of systems. However, predictive mathematical models linking indicators of the success of the use of information technologies with the characteristics of these technologies and the characteristics of the functioning of systems have not yet been adequately developed. The conceptual and methodological foundations of such modeling are not described in sufficient detail. Modeling the use of information is associated with the construction of a significant number of possible sequences of cause-and-effect relationships of information and other actions, chains of events and states caused by them during functioning. In part, such chains can be obtained by process mining. However, the set of all possible chains can be obtained by process mining only partially at the design stage, because such chains may be new, not ever recorded ones. To obtain sets of possible chains of actions, events, and states, it is proposed to develop new technologies for synthesizing sets of possible chains of actions, events and states. The research results, presented in the article should make it possible to overcome the existing gap and proceed to the construction of the required models of chains of actions, events and states at the design stage.
Key words: mining, process mining, information mining, modelling, methods, machine learning.

Введение. При реализации цифровой трансформации многих современных систем возникают разнообразные задачи проектирования и совершенствования использования цифровых информационных технологий (ИТ). Так, например, оказывается необходимым соотносить затраты на внедрение цифровых технологий сначала с характеристиками разрабатываемых и внедряемых ИТ, а затем с теми результатами, которые могут быть получены при использовании внедренных ИТ и наконец – с финансовыми результатами, достигаемыми благодаря использованию цифровых ИТ [1,2,3].

В ранее опубликованных авторами трудах [4,5,6] показано, что для получения математических моделей, позволяющих описать связи характеристик разрабатываемых и используемых ИТ с получаемыми результатами использования в будущей практике необходимо породить возможные последовательности связанных причинно-следственными

связями действий, событий и состояний в зависимости от получаемой, создаваемой и используемой информации о функционировании системы и ее среды.

Модели использования информации для функционирования системы. Возможные последовательности связанных причинно-следственными связями действий, событий и состояний [7] могут быть структурированы в виде теоретико-графовых моделей разного вида, а затем — функциональных и программных моделей использования информации при функционировании системы. Они дают далее возможность оценить результаты отдельных реализаций функционирования в изменяющихся условиях при соответствующих реализациях применения ИТ и меры возможности таких реализаций. Это, затем, дает возможность оценить показатели потенциала системы, функционирующей с использованием ИТ, в изменяющихся условиях, и показатели, описывающие изменение энтропии при использовании ИТ — синтропию систем [8]. Эти показатели, оцениваемые в зависимости от условий функционирования и от характеристик, используемых ИТ и позволяют далее перейти к функциональным моделям, описывающим связи характеристик, разрабатываемых и используемых ИТ с получаемыми результатами использования в будущей практике. Такие зависимости, в свою очередь, позволяют решать значительное число практических задач, в том числе – задач цифровизации, как математические задачи исследования операций, математического программирования [9].

Основная сложность при таком подходе к решению задач цифровой трансформации состоит в построении необходимых моделей, опирающихся на представление возможных последовательностей причинно-следственных связей между действиями разных видов, информацией об условиях, результатах и реализации действий, событиями в и результате и состояниями. Такие модели могут обладать разными особенностями и их возможно порождать разными методами. Рассмотрим особенности предложенных авторами моделей использования информации для функционирования систем, опирающихся на представление в виде цепочек причинно-следственных связей.

Особенности моделей использования информации для функционирования систем, опирающихся на представление в виде цепочек причинно-следственных связей. Нами предложены модели, опирающиеся на представления последовательностей причинно-следственных связей между действиями разных видов, информацией об условиях, результатах и реализации действий, событиями в их результате и состояниями (“цепочки причинно-следственных связей”). Такие модели предназначены далее для связывания характеристик информационных

технологий и систем, в которых они используются, с показателями, характеризующими разнообразные стороны успешности использования ИТ и для расчета этих показателей в зависимости от характеристик ИТ. При этом важной особенностью указанных моделей является то, что вычисления по этим моделям реализуются в соответствии с закономерностями природных явлений (по причинно-следственным связям), результаты вычислений имитируют результаты реализации того или иного функционирования системы в тех или иных условиях (по тем же причинам, модель обеспечивает подобие функционированию). Кроме того, модель информационной операции подобна информационной операции (и может непосредственно использоваться в системе при функционировании). Наконец, вычисление результатов функционирования задается последовательностью элементов в цепочках модели, а цепочки могут храниться в последовательности вычислений.

Несмотря на то, что модели указанного вида обладают указанными достоинствами, их построение связано с существенными затруднениями, вызванными масштабностью множества возможных цепочек, неопределенностями и случайностями при их формировании, сложностями корректного описания причинно-следственных связей в цепочках так, чтобы можно было достаточно просто перейти к вычислительным моделям.

В связи с этим остро встает вопрос о методах порождения моделей «цепочек» и методах автоматизации их порождения.

Методы порождения моделей использования информации для функционирования систем. Рассмотрим ряд основных методов порождения моделей, опирающихся на представления последовательностей причинно-следственных связей между действиями разных видов, информацией об условиях, результатах и реализации действий, событиями в их результате и состояниями (моделями «цепочек»).

Метод непосредственного построения модели экспертом. В соответствии с этим методом, цепочки порождаются специалистом по реализации процессов, хорошо знающим особенности моделируемых процессов. Метод трудоемок, однако позволяет описывать все элементы модели (в том числе информационные) подробно. При этом, однако, могут быть пропущены некоторые реализации цепочек в результате ошибки эксперта.

Метод порождения модели по заданным экспертом мета-описаниям (мета-модели) и алгоритмам порождения. В соответствии с этим методом, цепочки порождаются не непосредственно, а путем описания алгоритма их порождения, на основе некоторой мета-модели, описыва-

ющей сведения о совокупностях подобных элементов строящихся моделей в более сжатом виде (по отношению к строящейся модели) и алгоритма (правил) порождения модели. Так, например, путем обходов диаграммы, задающей мета-модель в виде графа, описывающего возможные реализации последовательностей причинно-следственных связей, которые могут перечисляются (для порождения модели) при обходе такой мета-модели с соблюдением заданных правил порождения. Метод характеризуется тем, что часть действий может быть автоматизирована. Однако он более сложен в конструировании корректной мета-модели и алгоритма. При его реализации алгоритм, если он корректен, гарантирует перечисление всех возможных цепочек. Описание информационных действий должно быть формализировано, что может вызывать сложности.

Указанные два метода порождения моделей – методы порождения человеком моделей применения информации в деятельности. Их отличие в том, что человеком в разных формах описываются возможные последовательности изменения (альтернирования) деятельности в различных условиях, в зависимости от выполняемых информационных действий. При этом при описании в форме мета-модели применение информации и возможности альтернирования необходимо формализовать, что и дает возможность поставить между человеком и моделью вычислительное устройство, на котором может быть выполнена часть действий по моделированию.

Майнинг процессов. В соответствии с этим методом log-файлы исследуются на предмет выявления цепочек причинно-следственных связей. По ним порождаются реализации цепочек (traces), которые затем следует систематизировать, породив модели процессов. Недостаток метода состоит в том, что в log файлах могут быть только те реализации процессов, которые были наблюдены. Однако это не все возможные реализации. Кроме того, на этапе проектирования никаких log-файлов функционирования проектируемой системы еще нет. Наконец, существующие log-файлы редко содержат сведения о выполненных информационных действиях, необходимые для майнинга использования информации для функционирования систем («майнинга использования информации»).

Метод обучения по log- файлам алгоритма непосредственного построения моделей, на основе порождаемых мета-моделей. Используя как имеющиеся построенные экспертами мета-модели, так и полученные из log- файлов реализации процессов следует уточнить мета-модель использования информации и, на основе log-файлов обучить алгоритм,

порождающий возможные цепочки в зависимости от условий. Алгоритм должен порождать корректные (с точки зрения эксперта) модели процессов в виде цепочек реализаций. В этом случае также говорят о майнинге использования информации. И в этом случае необходимо моделировать использование информации в log-файлах.

Указанные два метода порождения моделей – методы порождения моделей применения информации в деятельности из log-файлов. Их отличие в том, что последовательности изменения (альтернирования) деятельности в различных условиях заданы в log-файлах и в моделях использования информации при функционировании систем, построенных людьми. При этом, в настоящее время выстраивание цепочек деятельности в зависимости от выполняемых информационных действий не распространено достаточно широко и, как правило, игнорируется. Описывается только результат. Не практикуется формализация применения информации с использованием мета-моделей.

Метод обучения мета – модели и алгоритмов порождения. В рамках этого метода мета-модель и алгоритм ее использования для порождения модели создается машиной на основе данных, используемых и человеком, и машиной (в том числе и log-файлов) и аналогично тому, как это делает человек. Предполагается, что структура и характеристики информационных действий не меняются при машинном обучении, информационные действия заданы. Тем не менее, такие алгоритмы нам неизвестны.

Метод майнинга информационных действий. Метод состоит в обучении моделей информационных действий так, чтобы они реализовывали лучшие из возможных (по соответствию эффектов требованиям в возможных условиях) реакции на изменения системы и ее среды. При этом в качестве данных используются реализованные информационные действия, модели и мета-модели, процессов, описанные экспертами и log-файлы с записями о характеристиках информационных действий.

Указанные два метода порождения моделей – перспективные методы машинного порождения моделей применения информации в деятельности. Модели создаются машиной на основе данных, используемых и человеком, и машиной и аналогично тому, как это делает человек. Их отличие в том, что на основе как моделей, построенных человеком, так и log-файлов применяются алгоритмы создания возможных последовательностей изменения (альтернирования) деятельности, в зависимости от возможных выполняемых информационных действий в различных условиях и от характеристик этих действий. При этом применение информации и возможности альтернирования формализуются для

того, чтобы обеспечить их формирование разрабатываемым алгоритмом на основе уже имеющихся моделей (машинное обучение созданию моделей использования информации для деятельности).

Комплексные методы. Такие методы представляют собой систему методов 1–6, сформированную таким образом, чтобы с ее использованием могли создаваться требуемые модели использования информации для функционирования систем.

Заключение. Предложены направления построения и совершенствования прогнозных математических моделей, связывающие показатели успешности использования информационных технологий с характеристиками этих технологий и характеристиками функционирования систем. Описаны концептуальные и методологические трудности, связанные с таким моделированием. Показано, что моделирование использования информации связано с построением значительного числа возможных последовательностей причинно-следственных связей информационных и других действий, вызываемых ими цепочек событий и состояний при функционировании. Частично такие цепочки могут быть получены за счет майнинга процессов. Однако, множество всех возможных цепочек может быть получено на этапе проектирования лишь частично, в связи с тем, что такие цепочки могут быть новыми. Для получения множеств возможных цепочек действий, событий и состояний предложено разработать ряд концепций, методов и технологий моделирования множеств возможных цепочек действий, событий и состояний с использованием информационных действий. В докладе показаны основные направления создания таких моделей, в том числе и с использованием машинного обучения. Описано новое направление моделирования использования информации, представляющее собой майнинга информационных действий при функционировании систем и машинное обучение характеристик таких действий по имеющимся сведениям. Представленный в докладе материал должен позволить преодолеть имеющееся несоответствие и перейти к построению требуемых моделей использования информации для функционирования систем.

Работа проводилась при поддержке бюджетной НИР FFZF-2022–0003.

Библиографический список

1. Р. М. Юсупов, А. А. Мусаев. Проблема оценивания эффективности информационных технологий // Материалы конференции «Информационные технологии в управлении (ИТУ-2018)». Электроприбор. 2018.
2. Р. М. Юсупов, А. А. Мусаев. Особенности оценивания эффективности информационных систем и технологий// Тр. СПИИРАН. 51 (2017), p.p.5–34.

3. Юсупов Р. М., Мусаев А. А. К оцениванию эффективности информационных систем. Методологические аспекты // Информационные технологии. 2017. Том 23. №5. С. 323–332.
4. Ашимов, А. А., Гейда, А. С., Лысенко, И. В., & Юсупов, Р. М. Эффективность функционирования и другие операционные свойства систем: задачи и метод оценивания. Труды СПИИРАН, 5(60), 2018. p.p. 241–270.
5. Гейда А. С., Гурьева Т. Н., Наумов В. Н. Концептуальные и математические модели, методы и технологии исследования цифровой трансформации экономических и социальных систем: обзор предметного поля (часть I) // Управленческое консультирование. 2021. No 11. С. 95–108.
6. Гейда А. С., Гурьева Т. Н., Наумов В. Н. Концептуальные и математические модели, методы и технологии исследования цифровой трансформации экономических и социальных систем: обзор предметного поля (часть II) // Управленческое консультирование. 2021. No 12. С. 111–125.
7. M. Reichert, B. Weber. Enabling Flexibility in Process-Aware Information Systems, Springer-Verlag Berlin Heidelberg 2012. 511 P.
8. V. Vyatkin. "Syntropic criterion for removing restrictions during the COVID-19 pandemic," Политематический сетевой электронный научный журнал Кубанского государственного аграрного университета, no. 174, 2021, pp. 426–435.
9. Гейда А.С. Основы теории потенциала сложных технических систем: монография / А.С. Гейда. – М.: РАН, 2021. – 408 с.

УДК 004.056
В.С. Сторожик, к.т.н., доцент
Арктический и антарктический научно-исследовательский институт
ул. Беринга, д. 38, г. Санкт-Петербург, Россия, 199397
e-mail: vstorozhik@yandex.ru

ОСОБЕННОСТИ РЕАЛИЗАЦИИ ТРЕБОВАНИЙ НОРМАТИВНЫХ ПРАВОВЫХ АКТОВ К ОРГАНИЗАЦИОННО-РАСПОРЯДИТЕЛЬНЫМ ДОКУМЕНТАМ ДЛЯ ИНФОРМАЦИОННЫХ СИСТЕМ ПЕРСОНАЛЬНЫХ ДАННЫХ

Аннотация
Рассматриваются нормативные правовые акты, определяющие особенности реализации требований к организационно-распорядительным документам по обеспечению безопасности персональных данных при их обработке в информационных системах.
Ключевые слова: безопасность, защита, информация, информационная система, оператор, мера защиты, персональные данные, система безопасности, средства защиты, требование, угроза безопасности информации, уровень защищенности.

V. S. Storozhik
Arctic and Antarctic Research Institute,
38 Bering Street, Saint Petersburg, Russia, 199397
e-mail: vstorozhik@yandex.ru

FEATURES OF THE IMPLEMENTATION OF THE REQUIREMENTS OF REGULATORY LEGAL ACTS TO ORGANIZATIONAL AND ADMINISTRATIVE DOCUMENTS FOR PERSONAL DATA INFORMATION SYSTEMS

Annotation
The normative legal acts defining the specifics of the implementation of the requirements for organizational and administrative documents to ensure the security of personal data during their processing in information systems are considered.
Keywords: security, protection, information, information system, operator, security measure, personal data, security system, means of protection, requirement, threat to information security, security level.

В Стратегии национальной безопасности Российской Федерации поставлена задача обеспечения защиты конституционных прав и свобод человека и гражданина при обработке персональных данных [1].

В докладе Президента Российской Федерации на заседании Совета Безопасности Российской Федерации 20 мая 2022 г. «О повышении

устойчивости и безопасности функционирования информационной инфраструктуры государства» подчеркнуто, что принципиально важно свести на нет риски утечек конфиденциальной информации и персональных данных граждан [2].

Рассматриваются нормативные правовые акты, определяющие особенности реализации требований к организационно-распорядительным документам по обеспечению безопасности персональных данных при их обработке в информационных системах. [3 - 8].

Библиографический список

1. Стратегия национальной безопасности Российской Федерации (утв. Указом Президента Российской Федерации от 2 июля 2021 г. № 400).
2. Доклад Президента Российской Федерации В.В. Путина 20 мая 2022 г. на заседании Совета Безопасности Российской Федерации «О повышении устойчивости и безопасности функционирования информационной инфраструктуры государства».
3. Федеральный закон от 27 июля 2006 г. № 152-ФЗ «О персональных данных» (с изменениями и дополнениями).
4. Постановление Правительства Российской Федерации от 1 ноября 2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных».
5. Приказ ФСТЭК России от 17 февраля 2013 г. № 21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных».
6. Приказ ФСТЭК России от 11 февраля 2013 г. № 17 «Об утверждении требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах».
7. Приказ ФСБ России от 10 июля 2014 г. № 378 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных Правительством РФ требований к защите персональных данных для каждого из уровней защищенности».
8. Методические рекомендации по разработке нормативных правовых актов, определяющих угрозы безопасности персональных данных, актуальные при обработке персональных данных в информационных

системах персональных данных, эксплуатируемых при осуществлении соответствующих видов деятельности, утверждены руководством 8 Центра ФСБ России 31 марта 2015 г. № 149/7/2/6-432.

УДК 004.056

В.С.Сторожик, кандидат технических наук, доцент
Арктический и антарктический научно-исследовательский институт

ТРЕБОВАНИЯ НОРМАТИВНЫХ ПРАВОВЫХ АКТОВ К ОРГАНИЗАЦИОННО-РАСПОРЯДИТЕЛЬНЫМ ДОКУМЕНТАМ ДЛЯ ИНФОРМАЦИОННЫХ СИСТЕМ ПЕРСОНАЛЬНЫХ ДАННЫХ

Аннотация
Рассматриваются нормативные правовые акты, определяющие особенности реализации требований к организационно-распорядительным документам по обеспечению безопасности персональных данных при их обработке в информационных системах.
Ключевые слова: безопасность, защита, информация, информационная система, оператор, мера защиты, персональные данные, система безопасности, средства защиты, требование, уровень защищенности.
Annotation
The normative legal acts defining the specifics of the implementation of the requirements for organizational and administrative documents to ensure the security of personal data during their processing in personal data information systems are considered.
Keywords: security, protection, information, information system, operator, security measure, personal data, security system, means of protection, requirement, security level.

В Стратегии национальной безопасности Российской Федерации поставлена задача обеспечения защиты конституционных прав и свобод человека и гражданина при обработке персональных данных [1].

В докладе Президента Российской Федерации на заседании Совета Безопасности Российской Федерации 20 мая 2022 г. «О повышении устойчивости и безопасности функционирования информационной инфраструктуры государства» подчеркнуто, что принципиально важно свести на нет риски утечек конфиденциальной информации и персональных данных граждан [2].

Требования по обеспечению безопасности персональных данных (ПДн) регулируются российским и международным законодательством.

Федеральный закон от 27 июля 2006 г. № 152-ФЗ «О персональных данных» содержит нормы, соответствующие основным положениям Конвенции Совета Европы о защите физических лиц при автоматизированной обработке персональных данных 1981 г. [3, 4],

Уполномоченным органом Российской Федерации по защите прав субъектов ПДн является Федеральная служба по надзору в сфере связи,

информационных технологий и массовых коммуникаций (Роскомнадзор), подведомственная Министерству цифрового развития, связи и массовых коммуникаций Российской Федерации (Минцифры России) [5].

В рамках своих полномочий [6] во исполнение 152-ФЗ Правительством Российской Федерации постановлением от 1 ноября 2012 г. № 1119 установлены уровни защищенности ПДн при их обработке в информационных системах персональных данных (ИСПДн) в зависимости от угроз безопасности этих данных и требования к защите ПДн при их обработке в ИСПДн, исполнение которых обеспечивает установленные уровни защищенности ПДн [7], а постановлением от 6 июля 2008 г. № 512 установлены требования к материальным носителям биометрических ПДн и технологиям хранения таких данных вне ИСПДн [8].

В соответствии со статьей 19 152-ФЗ меры обеспечения безопасности ПДн устанавливают в пределах своих полномочий ФСТЭК России (не криптографическими способами) и ФСБ России (при использовании криптографических методов защиты информации) [9, 10].

Приказом ФСТЭК России от 17 февраля 2013 г. № 21 утверждены Состав и содержание конкретных организационных и технических мер по обеспечению безопасности ПДн при их обработке в ИСПДн для обеспечения соответствующего уровня защищенности ПДн [11].

Если ПДн обрабатываются в государственной информационной системе (ГИС), то меры по обеспечению безопасности должны приниматься в соответствии с требованиями приказа ФСТЭК России от 11 февраля 2013 г. № 17 [12].

Если защищаемая ИСПДн является значимым объектом критической информационной инфраструктуры [13, 14], то меры по обеспечению безопасности должны приниматься в соответствии с требованиями приказа ФСТЭК России от 25 декабря 2017 г. № 239 [15].

Для определения угроз безопасности ПДн при их обработке в ИСПДн оператору следует опираться на методические документы ФСТЭК России:

1. Базовую модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных [16].

2. Методику оценки угроз безопасности информации [17].

ФСБ России во исполнение части 4 статьи 19 152-ФЗ приказом от 10 июля 2014 г. № 378 утвержден Состав и содержание организационных и технических мер по обеспечению безопасности ПДн при их обработке в ИСПДн с использованием средств криптографической защиты информации (СКЗИ), необходимых для выполнения установленных

Правительством Российской Федерации требований к защите ПДн для каждого из уровней защищенности [18].

Методические рекомендации ФСБ России по разработке нормативных правовых актов, определяющих угрозы безопасности персональных данных, актуальные при обработке персональных данных в информационных системах персональных данных, эксплуатируемых при осуществлении соответствующих видов деятельности, утвержденные руководством 8 Центра ФСБ России 31 марта 2015 г., предназначены для государственных органов и операторов, использующих СКЗИ и разрабатывающих соответствующие модели угроз [19].

Операторам ИСПДн также необходимо руководствоваться следующими методическими документами ФСБ России:

1. Типовыми требованиями по организации и обеспечению функционирования шифровальных (криптографических) средств, предназначенных для защиты информации, не содержащей сведений, составляющих государственную тайну, в случае их использования для обеспечения безопасности персональных данных при их обработке в информационных системах персональных данных [20].

2. Методическими рекомендациями по обеспечению с помощью крипто средств безопасности ПДн при их обработке в ИСПДн с использованием средств автоматизации [21].

С целью обеспечения безопасности ПДн при их обработке в ИСПДн оператором должны быть разработаны организационно-распорядительные документы, предусмотренные нормативными правовыми актами, перечень которых представлен в Таблице.

Разработанные и реализованные оператором организационно-распорядительные документы, предусмотренные нормативными правовыми актами в области обеспечения безопасности ПДн, создают предпосылки для качественного решения задачи обеспечения защиты конституционных прав и свобод человека и гражданина при обработке ПДн в ИСПДн.

Таблица - Организационно-распорядительные документы по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных

№ п/п	Наименование организационно-распорядительного документа	Ссылка на требования нормативного правового акта – основание для разработки документа
1.	Акт определения уровня защищенности ПДн при их обработке в информационной системе	Пункт 8 Постановления Правительства Российской Федерации от 01.11.2012 № 1119 [7]
2.	Документ о назначении должностного лица (работника) оператора, ответственного за обеспечение безопасности ПДн в информационной системе	Пункт 14. Постановления Правительства Российской Федерации от 01.11.2012 № 1119 [7]; Пункт 16 Приказа ФСБ России от 10.07.2014 N 378 [18]
3.	Перечень лиц, доступ которых к ПДн, обрабатываемым в информационной системе, необходим для выполнения ими служебных (трудовых) обязанностей	Пункт 14. Постановления Правительства Российской Федерации от 01.11.2012 № 1119 [7]; Пункт 16 Приказа ФСБ России от 10.07.2014 N 378 [18]
4.	Правила доступа в помещения, где размещены используемые средства криптографической защиты информации (СКЗИ), хранятся СКЗИ и (или) носители ключевой, аутентифицирующей и парольной информации СКЗИ, в рабочее и нерабочее время, а также в нештатных ситуациях	Пункт 13 Постановления Правительства Российской Федерации от 01.11.2012 № 1119 [7]; Пункт 6 Приказа ФСБ России от 10.07.2014 N 378 [18]
5.	Перечень лиц, имеющих право доступа в помещения, где размещены используемые СКЗИ, хранятся СКЗИ и (или) носители ключевой, аутентифицирующей и парольной информации СКЗИ	Пункт 6 Приказа ФСБ России от 10.07.2014 N 378 [18]

6.	Правила доступа к персональным данным, обрабатываемым в информационной системе персональных данных	Статья 19 Федерального закона от 27.07.2006 N 152-ФЗ [3]; Пункт 8.2 Приказа ФСТЭК России от 18.02.2013 № 21 [12]
7.	Определение границ контролируемой зоны	Пункт 10 Приказа ФСБ России от 10.07.2014 N 378 [18]
8.	Журнал учета носителей персональных данных с использованием регистрационных (заводских) номеров	Пункт 7 Приказа ФСБ России от 10.07.2014 N 378 [18]; ЗНИ.1 Приказа ФСТЭК России от 18.02.2013 N 21 [12]
9.	Совокупность предположений о возможностях, которые могут использоваться при создании способов, подготовке и проведении атак, и определение на этой основе и с учетом типа актуальных угроз требуемого класса СКЗИ	п. 9 Приказа ФСБ России от 10.07.2014 N 378 [18]
10	Правила генерации и смены паролей пользователей	Мера АНЗ.5 раздела VIII. Контроль (анализ) защищенности персональных данных (АНЗ) Приложения к Приказу ФСТЭК России от 18.02.2013 N 21 [12]

Библиографический список

1. Стратегия национальной безопасности Российской Федерации (утв. Указом Президента Российской Федерации от 2 июля 2021 г. № 400).
2. Доклад Президента Российской Федерации В.В. Путина 20 мая 2022 г. на заседании Совета Безопасности Российской Федерации «О повышении устойчивости и безопасности функционирования информационной инфраструктуры государства».
3. Федеральный закон от 27 июля 2006 г. № 152-ФЗ «О персональных данных» (с изменениями и дополнениями).
4. Конвенция Совета Европы о защите физических лиц при автоматизированной обработке персональных данных (Страсбург, 28 января 1981 г.).
5. Постановление Правительства Российской Федерации от 16 марта 2009 г. № 228 «О Федеральной службе по надзору в сфере связи, информационных технологий и массовых коммуникаций».
6. Федеральный конституционный закон от 6 ноября 2020 г. № 4-ФКЗ

«О Правительстве Российской Федерации».
7. Постановление Правительства Российской Федерации от 1 ноября 2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных».
8. Постановление Правительства Российской Федерации от 6 июля 2008 г. № 512 «Об утверждении требований к материальным носителям биометрических персональных данных и технологиям хранения таких данных вне информационных систем персональных данных».
9. Указ Президента Российской Федерации от 16 августа 2004 г. № 1085 «Вопросы Федеральной службы по техническому и экспортному контролю».
10. Указ Президента Российской Федерации от 11 августа 2003 г. № 960 «Вопросы Федеральной службы безопасности Российской Федерации».
11. Приказ ФСТЭК России от 17 февраля 2013 г. № 21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных».
12. Приказ ФСТЭК России от 11 февраля 2013 г. № 17 «Об утверждении требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах».
13. Федеральный закон от 26 июля 2017 г. N 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации».
14. Постановление Правительства Российской Федерации от 8 февраля 2018 г. № 127 «Об утверждении Правил категорирования объектов критической информационной инфраструктуры Российской Федерации, а также перечня показателей критериев значимости объектов критической информационной инфраструктуры Российской Федерации и их значений».
15. Приказ ФСТЭК России от 25 декабря 2017 г. № 239 «Об утверждении Требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации» (в ред. приказа ФСТЭК России от 26 марта 2019 г. № 60).
16. Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных, утверждена ФСТЭК России 15 февраля 2008 г.
17. Методика оценки угроз безопасности информации, утверждена ФСТЭК России 5 февраля 2021 г.
18. Приказ ФСБ России от 10 июля 2014 г. № 378 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных

системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных Правительством Российской Федерации требований к защите персональных данных для каждого из уровней защищенности».

19. Методические рекомендации по разработке нормативных правовых актов, определяющих угрозы безопасности персональных данных, актуальные при обработке персональных данных в информационных системах персональных данных, эксплуатируемых при осуществлении соответствующих видов деятельности, утверждены руководством 8 Центра ФСБ России 31 марта 2015 г. № 149/7/2/6-432.

20. Типовые требования по организации и обеспечению функционирования шифровальных (криптографических) средств, предназначенных для защиты информации, не содержащей сведений, составляющих государственную тайну, в случае их использования для обеспечения безопасности персональных данных при их обработке в информационных системах персональных данных», утверждены руководством 8 Центра ФСБ России 21 февраля 2008 г. № 149/6/6-622.

21. Методические рекомендации по обеспечению с помощью крипто средств безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств автоматизации, утверждены 8 Центром ФСБ России 21 февраля 2008 г. № 149/54-144.

УДК 004.056.53
И.Б. Паращук, д-р техн. наук, профессор, И.В. Котенко, д-р техн. наук, профессор, И.Б. Саенко, д-р техн. наук, профессор
Санкт-Петербургский Федеральный исследовательский центр Российской академии наук (СПб ФИЦ РАН)
г. Санкт-Петербург, Россия

РАЗРАБОТКА ИСХОДНЫХ ДАННЫХ ДЛЯ АЛГОРИТМОВ НЕЧЕТКОГО УПРАВЛЕНИЯ ИНФОРМАЦИЕЙ И СОБЫТИЯМИ БЕЗОПАСНОСТИ В КИБЕРФИЗИЧЕСКИХ СИСТЕМАХ

Аннотация
Доклад посвящен вопросам формулировки и количественного обоснования исходных данных, необходимых для нечеткого управления информацией и событиями безопасности в современных киберфизических системах. Рассматриваются несколько альтернативных аналитических подходов к построению функций принадлежности в приложении к задачам нечеткого управления информацией и событиями безопасности систем такого класса.
Ключевые слова: функция принадлежности, метод, система, управление информацией и событиями безопасности, нечеткое управление.
Annotation
The report is devoted to the formulation and quantitative justification of the initial data necessary for the fuzzy management of information and security events in modern cyber-physical systems. Several alternative analytical approaches to the construction of membership functions in relation to the tasks of fuzzy information management and security events of systems of this class are considered.
Keywords: membership function, method, system, security information and event management, fuzzy management.

К киберфизическим системам (КФС) относятся масштабные технологические и крупные многоуровневые, многокомпонентные инженерные объекты, которые технически реализованы на базе «бесшовной» интеграции вычислительных алгоритмов и встроенных физических компонентов. Иными словами, это системы, в которых взаимосвязаны ресурсы, технологии, вычислительные элементы и элементы физической природы, служащие как потребителями, так и источниками информации. Применение КФС позволяет повысить адаптивность, масштабируемость, отказоустойчивость и безопасность инженерных систем, а также эргономичность (удобство) их использования. Принято считать, что в системах такого класса кибернетическая и физическая составляющие тесно интегрированы во всех масштабах и на всех уровнях в рамках

единого информационного пространства с помощью датчиков и сенсоров.

Ключевым элементом, обеспечивающим функционирование современных КФС, важнейшим основным и/или вспомогательным потребляемым и производимым «продуктом» для систем такого класса является информация. Подсистема обмена информацией в КФС – важнейшая подсистема, поэтому актуально направление исследований, связанное с управлением событиями и инцидентами информационной безопасности таких систем. Созданы и функционируют специализированные системы управления информацией и событиями безопасности (ИСБ), называемые SIEM-системами (Security Information and Event Management). Они служат для анализа в реальном масштабе времени событий (угроз) безопасности и позволяют быстро реагировать на эти угрозы. Их задача – не допустить существенного ущерба для целостности, конфиденциальности и доступности данных [1].

Задачи, которые решают SIEM-системы, заключаются в следующем: сбор, обобщение и хранение журналов событий и иной информации безопасности от множества разнородных источников; автоматическое оповещение и визуализация предупреждений; использование инструментов для и разбора инцидентов и анализа событий; анализ и обработка событий с использованием методов интеллектуального анализа данных; подготовка данных для проведения расследований и экспертиз. Основное преимущество SIEM-систем – обнаружение угроз безопасности и атак на ранних стадиях их проявления. Кроме того, SIEM-систем обеспечивают прогнозирование поведения КФС в ходе негативного воздействия, что позволяет своевременно вырабатывать адекватные меры противодействия атакам [1-3].

С учетом того факта, что почти все управленческие решения в рамках процедур обеспечения защищенности КФС принимаются в условиях неопределенности, принято считать, что одним из рациональных походов к реализации подобных задач является применение моделей и алгоритмов нечеткого управления. Вместе с тем, использование моделей и алгоритмов нечеткого управления невозможно без знаний о значениях функций принадлежности (ФП) нечетких множеств, лежащих в основе механизмов нечеткого управления. Функции принадлежности в исследуемой постановке определяться для задач принятия решений о принадлежности конкретной компьютерной атаки к нечеткому множеству опасных атак. Рассматриваются алгоритмы построения ФП по вероятностной схеме и с помощью метода, базирующегося на формировании ФП в виде функций от плотности вероятности [4, 5].

Вычислительные эксперименты показывают, что с использованием метода представления функций принадлежности в виде функций от плотности вероятности четких случайных границ между термами лингвистической переменной, а также на основе стандартного набора графиков функций принадлежности, можно получить значения ФП, например, для утверждения «величина *x* мала». Физический смысл этого утверждения для нашей практической задачи заключается в определении текущего уровне (степени) опасности конкретного типа компьютерных атак для информационной безопасности КФС – «уровень опасности конкретного типа компьютерных атак *x* мал».

Для определения текущего уровня (степени) опасности конкретного типа компьютерных атак – «уровень опасности конкретного типа компьютерных атак *x* большой», задачи поиска ФП решаются аналогично [5].

Теоретический анализ рассмотренных методов позволяет выдвинуть гипотезу о том, что эффективные подходы к построению ФП в задачах принятия решений по управлению информацией и событиями безопасности, могут быть найдены на пути сочетания простых вероятностных методов (по вероятностной схеме) и метода построения функций принадлежности на основе анализа функций от плотности вероятности.

Рассмотренные методы разработки исходных данных (писка ФП) имеют свои достоинства и недостатки, но не обладают большой математической и вычислительной сложностью. Эти методы, наряду с прочим, позволяют учесть неопределенность наблюдаемых и управляемых параметров безопасности, что обеспечит повышение достоверности контроля информации и событий безопасности в рамках нечеткого управления защищенностью киберфизических систем.

Исследования проводятся при поддержке гранта РНФ № 21-71-20078 в СПб ФИЦ РАН.

Библиографический список

1. Miller D. R., Harris S., Vandyke S. Security Information and Event Management (SIEM) implementation. – New York: McGrawHill. 2011. 345 p.
2. Kotenko I., Parashchuk I. Determining the Parameters of the Mathematical Model of the Process of Searching for Harmful Information. Cyber-Physical Systems: Industry 4.0 Challenges // Studies in Systems, Decision and Control 260. A.G. Kravets et al. (eds.). Springer Nature Switzerland AG, Cham 2020. pp. 225–236.
3. Vielberth M. Security Information and Event Management (SIEM) // Encyclopedia of Cryptography, Security and Privacy. Springer, Berlin, Heidelberg. 2021. pp. 1-16.

4. Паращук И. Б., Бобрик И. П. Нечеткие множества в задачах анализа сетей связи. – СПб.: ВУС. 2001. – 80 с.
5. Паращук И.Б., Котенко И.Б., Саенко И.Б. Управление информацией и событиями безопасности на основе нечетких алгоритмов // Перспективные направления развития отечественных информационных технологий: материалы VII межрегиональной научно-практической конференции. (Севастополь, 21-25 сентября 2021 г.) – Севастополь: СевГУ, 2021. С. 67–68.

УДК 629.735.33
Н. Н. Мошак[1], д-р техн. наук, профессор, В.В. Касаткин[2], доц., канд. техн. наук
[1]*Санкт-Петербургский государственный университет телекоммуникаций им. проф. М.А. Бонч-Бруевича*
e-mail: nnmoshak49@mail.ru
[2]*Санкт-Петербургский Федеральный исследовательский центр Российской академии наук*
e-mail: spiiras@iias.spb.su

СРАВНИТЕЛЬНЫЙ АНАЛИЗ МЕТОДИК АУДИТА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ИНФОРМАЦИОННЫХ СИСТЕМ

Аннотация
Анализируются методы аудита информационной безопасности, применяемые для оценки текущей защищенности информационных систем. Проводится их сравнительная оценка.
Ключевые слова: аудит информационной безопасности, информационная система, угрозы безопасности, система управления информационной безопасности.
Annotation
Information security audit methods used to assess the current security of information systems are analyzed. Their comparative assessment is carried out.
Key words: information security audit, information system, security threats, information security management system.

1 мая 2022 года Президентом РФ был подписан указ № 250, направленный на обеспечение информационной безопасности ряда ключевых организаций России. Одним из самых важных пунктов этого указа является установление перечня организаций, которым необходимо осуществить меры по оценке уровня защищенности своих информационных систем (ИС). К таким предприятиям относятся органы власти, госкорпорации, субъекты критических информационных инфраструктур (КИИ), стратегические и системообразующие организации и иные предприятия, созданные на основании Федерального закона. Одной из причин такой проверки могут служить требования регуляторов (например, ФСТЭК России) по проведению анализа защищенности государственных информационных систем (ГИС) и систем персональных данных (ИСПдн). Такой анализ должен быть проведен на момент формирования требований к защищенности инфраструктуры и выполняться периодически уже после проведения мероприятий по защите и использования сертифицированных средств защиты.

Основной целью информационной безопасности (защищенности) ИС организации – является понижение размера вероятного ущерба ценных активов до допустимых значений, а также надежная и качественная эксплуатация ИС в условиях возникающих угроз. Защищенность ИС достигается проведением руководством организации соответствующей политики информационной безопасности (далее – Политика) [1, 2]. Одноименный документ разрабатывается и принимается как официальный рабочий докумет (РД) организации в части ИБ ИС. Политика определяет, что нужно защищать. Поэтому после определения официальной Политики следует определить конкретные защитные меры и средства, а также меры контроля, реализующие практические процедуры защиты. Процедуры защиты определяют, как именно выполнять и контролировать требования Политики ИС. Требования ИБ, определяемые Политикой, являются основой построения системы информационной безопасности (СИБ) или системы защиты информации в организации. СИБ организации – это единый комплекс правовых норм, организационных и технических мер, обеспечивающий защищенность информации в соответствии с принятой Политикой. Организационные меры заключаются в формальных процедурах и правилах работы с важной информацией, информационными сервисами и средствами защиты. Технические меры включают в себя использование программных средств контроля доступа, мониторинг состояния ИБ информации, криптографическую и антивирусную защиту, защиту от электромагнитных излучений и т. д. Таким образом, СИБ – это совокупность защитных мер, средств и процессов их эксплуатации, включая ресурсное и административное (организационное) обеспечение, реализующая требования Политики. СИБ организации, как процесс защиты, относится к вспомогательным процессам, обеспечивающим качество ее основного бизнес-процесса.

Обеспечение ИБ организации – это непрерывный процесс, основное содержание которого составляет контроль и управление. Процедуры оперативного контроля состояния и управления ИБ реализует система управления ИБ (СУИБ) организации [3, 4].

СУИБ – часть менеджмента (скоординированной деятельности по руководству и управлению) организации, предназначенного для создания, эксплуатации, мониторинга, анализа и совершенствования системы обеспечения ИБ (СОИБ) организации. СОИБ организации объединяет как систему информационной защиты СИБ, так и систему управления «ИБ – СУИБ». При этом СУИБ является каркасом, который связывает различные компоненты средств ИБ организации и позволяет надежно и прозрачно управлять СОИБ организации.

Анализ или оценка уровня защищенности ИС — это анализ реализованных мер защиты информации, который позволит определить степень соответствия требованиям основных нормативно-правовых актов, а также оценить реальный уровень защищенности ИС организации от возможных угроз. Анализ защищенности ИС должен проводиться: в процессе разработки Политики и в процессе эксплуатации ИС в рамках осуществления функций СУИБ [3, 4].

Для объективной оценки текущего уровня безопасности ИС применяется аудит ИБ, который включает анализ рисков, связанных с возможностью осуществления угроз безопасности в отношении ценных активов ИС, оценку текущего уровня защищенности ИС, локализацию узких мест в системе их защиты, оценку соответствия ИС требованиям нормативных документов и существующим стандартам в области информационной безопасности и выработку рекомендаций по внедрению новых и повышению эффективности существующих механизмов безопасности ИС [5, 6]. В статье обсуждаются методы аудита ИБ, применяемые для оценки текущей защищенности ИС, и проводится их сравнительная оценка.

Цели и задачи аудита ИБ. Выделяют внутренний и внешний аудит информационной безопасности [3, 4].

Внутренний аудит регламентируется внутренними документами по ИБ (в том числе требованиями Политики) и нормативными документам по ИБ Регуляторов. Внутренний аудит проводится структурным подразделением организации по технической защите информации и выполняется на регулярной основе.

Внешний аудит проводится независимыми экспертами, которым по условиям договоров предоставляется доступ к ИС организации. Он может проводиться по требованию руководства, акционеров и правоохранительных органов. Как правило, привлечение внешних аудиторов ведет к более объективной оценке, существующей СУИБ, поскольку такие компании имеют штат квалифицированных аудиторов.

Общей задачей аудита ИБ является проверка и оценивание ИС на соответствие критериям, которые определяют требования к уровню ИБ [3, 4]. Частными задачами аудита являются [6, 7]:

– анализ рисков, связанных с возможностью реализации угроз безопасности;

– оценка текущего уровня защищенности;

– выявление уязвимостей в подсистеме защиты и «узких мест» системы;

– оценка соответствия системы и ее защиты существующим стандартам в области ИБ, а также политике безопасности;

– формирование рекомендаций по комплексу мер, направленных на повышение эффективности существующей системы защиты.

– Цели аудита можно подразделить на [7]:

– превентивные – направленные на превентивное выявление угроз и уязвимостей и предотвращение инцидентов ИБ;

– детектирующие – направленные на обнаружение новых или уточнение особенностей уже имеющихся угроз и уязвимостей системы защиты вовремя или после инцидентов ИБ;

– корректирующие – направленные на формирование комплекса мер повышения эффективности существующей системы защиты после инцидентов ИБ с учетом вновь выявленных угроз и уязвимостей.

Целью аудита может быть, как комплексный аудит системы защиты информации организации, так и аудит ИБ отдельных ИТ-систем (сетей передачи данных, вычислительных систем и систем хранения данных, и др.).

Виды аудита ИБ. Традиционно выделяют три типа аудита ИБ, которые различаются перечнем анализируемых компонентов СОИБ и получаемыми результатами:

– активный аудит;

– экспертный аудит;

– аудит на соответствие стандартам ИБ.

Активный аудит. Одним из самых распространенных видов аудита является активный аудит. Это исследование состояния защищенности информационной системы с точки зрения хакера (или некоего злоумышленника, обладающего высокой квалификацией в области информационных технологий). Активный аудит представляет собой обследование состояния защищенности ИС, относящихся к программно-техническому уровню [9, 10]. Активный аудит включает:

– анализ текущей архитектуры и настроек элементов системы защиты;

– интервьюирование ответственных и заинтересованных лиц;

– проведение инструментальных проверок, охватывающих определенные элементы системы защиты ИС.

Анализ архитектуры и настроек элементов системы защиты проводится специалистами, обладающими знаниями по конкретным подсистемам, представленным в обследуемой системе (например, могут требоваться специалисты по активному сетевому оборудованию или по ОС), а также системными аналитиками, которые выявляют возможные изъяны в организации подсистем. Результатом этого анализа является набор опросных листов и инструментальных тестов. Опросные листы

используются в процессе интервьюирования лиц, отвечающих за администрирование ИС, для получения субъективных характеристик ИС, для уточнения полученных исходных данных и для идентификации некоторых мер, реализованных в рамках СОИБ. Например, опросные листы могут включать вопросы, связанные с политикой смены и назначения паролей, жизненным циклом АИС и степенью критичности отдельных ее подсистем для ИС и бизнес-процессов организации в целом.

Параллельно с интервьюированием проводятся инструментальные проверки (тесты). Зачастую компании-поставщики услуг активного аудита именуют его именно как инструментальный анализ защищенности, чтобы отделить данный вид аудита от других. Аудиторы должны согласовывать каждый тест, модель знания, применяемую в тесте, и возможные негативные последствия теста с лицами, заинтересованными в непрерывной работе ИС (руководителями, администраторами системы и др.). Инструментальные проверки состоят из набора заранее согласованных тестов, направленных на получение характеристик об уровне защищенности ИС. Для проведения инструментальных проверок может быть использована методика, предполагающая тестирование возможности несанкционированного доступа (НСД) к информации, обрабатываемой или хранящейся в ИС, как изнутри организации, так и из внешних сетей [4, 9, 10]. Суть проверок состоит в том, что с помощью специального программного обеспечения (в том числе, с помощью систем анализа защищенности) и специальных методов осуществляется сбор информации о состоянии системы сетевой защиты. Под состоянием системы сетевой защиты понимаются лишь те параметры и настройки, использование которых помогает хакеру проникнуть в сети и нанести урон организации. При осуществлении данного вида аудита на систему сетевой защиты моделируется как можно большее количество таких сетевых атак, которые может выполнить хакер. При этом аудитор искусственно ставится именно в те условия, в которых работает хакер, – ему предоставляется минимум информации, только та, которую можно раздобыть в открытых источниках. Естественно, атаки всего лишь моделируются и не оказывают какого-либо деструктивного воздействия на информационную систему. Их разнообразие зависит от используемых систем анализа защищенности и квалификации аудитора. Результатом активного аудита является информация обо всех уязвимостях, степени их критичности и методах устранения, сведения о широкодоступной информации (информация, доступная любому потенциальному нарушителю) сети заказчика. По окончании активного аудита выдаются рекомендации по модернизации системы сетевой защиты, которые позво-

ляют устранить опасные уязвимости и тем самым повысить уровень защищенности информационной системы от действий «внешнего» злоумышленника при минимальных затратах на информационную безопасность. По результатам инструментальной проверки проводится пересмотр результатов предварительного анализа и, возможно, организуется дополнительное обследование.

Еще один вид услуг, предлагаемых в ходе активного аудита, - исследование производительности и стабильности системы, или стресс-тестирование. Оно направлено на определение критических точек нагрузки, при которой система вследствие атаки на отказ в обслуживании или повышенной загруженности перестает адекватно реагировать на легитимные запросы пользователей. Стресс-тест позволит выявить «узкие» места в процессе формирования и передачи информации и определить те условия, при которых нормальная работа системы невозможна. Тестирование включает в себя моделирование атак на отказ в обслуживании, пользовательских запросов к системе и общий анализ производительности.

Одной из самых «эффектных» услуг является тест на проникновение (Penetration Testing), который во многом похож на «внешний» активный аудит, но по своей сути аудитом не является. Однако ей свойственны множество ограничений и особенностей. Например, особенность технического характера: заказчик информируется только о факте уязвимости системы сетевой защиты, в то время как в результатах «внешнего» активного аудита заказчику сообщается не только факт уязвимости сети, но и информация обо всех уязвимостях и способах их устранения.

По результатам активного аудита создается аналитический отчет, состоящий из описания текущего состояния технической части СОИБ, списка найденных уязвимостей ИС со степенью их критичности и результатов упрощенной оценки рисков, включающей модель нарушителя и модель угроз.

Экспертный аудит. Экспертный аудит предназначен для оценивания текущего состояния ИБ на нормативно-методологическом, организационно-управленческом и процедурном уровнях [9-11]. Экспертный аудит проводится преимущественно внешними аудиторами, его выполняют силами специалистов по системному управлению. Сотрудники организации-аудитора совместно с представителями заказчика проводят следующие виды работ:

– сбор исходных данных об ИС, ее функциях и особенностях, используемых технологиях автоматизированной обработки и передачи информации (с учетом ближайших перспектив развития);

– сбор информации об имеющихся организационно-распорядительных документах по обеспечению ИБ и их анализ;

– определение защищаемых активов, ролей и процессов СОИБ.

Важнейшим инструментом экспертной оценки является сбор данных об ИС путем интервьюирования технических специалистов и руководства заказчика. Основные цели интервьюирования руководящего состава организации:

– определение политики и стратегии руководства в вопросах обеспечения ИБ;

– выявление целей, которые ставятся перед СОИБ;

– выяснение требований, которые предъявляются к СОИБ;

– получение оценок критичности тех или иных подсистем обработки информации, оценок финансовых потерь при возникновении тех или иных инцидентов.

Основные цели интервьюирования технических специалистов:

– сбор информации о функционировании ИС;

– получение схемы информационных потоков в ИС;

– получение информации о технической части СОИБ;

– оценка эффективности работы СОИБ.

Отметим, что сбор данных об ИС путем интервьюирования представителей заказчика и заполнения ими специальных анкет является одним из самых объемных видов работ, которые проводятся при экспертном аудите. В рамках экспертного аудита проводится анализ организационно распорядительных документов, таких как политика безопасности, план защиты, различного рода положения и инструкции. Организационно распорядительные документы оцениваются на предмет достаточности и непротиворечивости декларируемым целям и мерам ИБ, а также на предмет соответствия стратегической политике руководства в вопросах ИБ.

Экспертный аудит предполагает также проведение анализа информационных потоков организации. Определяются типы информационных потоков ИС организации и составляется их диаграмма, где для каждого информационного потока указывается его ценность (в том числе ценность передаваемой информации) и используемые методы обеспечения безопасности, отражающие уровень защищенности информационного потока. При этом особое внимание уделяется определению полномочий и ответственности конкретных лиц за обеспечение информационной безопасности различных участков/подсистем ИС.

Результаты экспертного аудита могут содержать рекомендации по совершенствованию нормативно-методологических, организационно управленческих и процедурных компонентов СОИБ.

Аудит на соответствие стандартам ИБ. Причины проведения аудита на соответствие стандарту можно условно разделить по степени обязательности данной услуги по отношению к организации: обязательная сертификация; сертификация, вызванная «внешними» объективными причинами; сертификация, позволяющая получить выгоды в долгосрочной перспективе; добровольная сертификация. Государственные организации, которые обрабатывают сведения, составляющие государственную тайну, в соответствии с российским законодательством обязаны проводить аттестацию информационной системы (во многом процедура аналогична сертификации). Однако такие организации чаще всего пользуются не услугой аудита на соответствие стандартам, а в обязательном порядке проводят аттестацию собственных ИС при участии аттестационных центров. Специально уполномоченные организации-аудиторы (аттестационные центры) по результатам аудита принимают решение и выдают документальное подтверждение о соответствии СОИБ тому или иному эталонному стандарту (проводят сертификацию) [9, 10].

Аудит на основе анализа стандартов информационной безопасности является самым практичным. Стандарты ИБ определяют базовый набор требований безопасности для широкого класса систем, который формируется в результате обобщения мировой практики. Стандарты ИБ могут определять разные наборы требований безопасности, в зависимости от уровня защищенности исследуемой системы, который требуется обеспечить, ее принадлежности (коммерческая организация, либо государственное учреждение), а также назначения (финансы, промышленности, связь и т. п.). От аудитора в данном случае требуется правильно определить набор требований стандарта, соответствие которым требуется обеспечить для конкретной исследуемой системы.

По результатам могут быть подготовлены отчеты, содержащие следующую информацию:

– степень соответствия проверяемой ИС выбранным стандартам;

– количество и категории полученных несоответствий и замечаний;

– рекомендации по построению или модификации СОИБ, позволяющие привести ее в соответствие с требованиями рассматриваемого стандарта.

Сравнение методик аудита ИБ. Сравнительный анализ методик аудита ИБ показан в таблицах 1-3.

Таблица 1 - Анализ методики активного аудита ИБ

Сильные стороны	Слабые стороны
• Автоматизация процесса аудита • В процессе проведения аудита не требуется участие сотрудников компании • Частота проведения аудита не регламентируется • Возможно проведение стресс тестирования для определения производительности и стабильности работы системы, а также проверки системы на устойчивость к DoS-атакам	• Требуется дополнительное программное обеспечение • На время проведения аудита необходимо прекратить работу • системы • Аудит направлен на выявление только известных уязвимостей
Возможности	**Угрозы**
• Высокий спрос на рынке • Аудит может быть осуществлен сотрудниками подразделения информационной безопасности предприятия • Большое количество программных продуктов различных организаций • Автоматизация большей части работы экспертов	• Высокая стоимость необходимого программного обеспечения • Для каждой системы необходимо подбирать программное обеспечение для проведения аудита • Отсутствие нормативной базы для проведения аудита • Возможны ошибки в используемом программном обеспечении

Таблица 2 - Анализ методики экспертного аудита ИБ

Сильные стороны	Слабые стороны
• Не требуется дополнительного программного обеспечения • Не требуется прекращение работы системы на время проведения аудита • Частота проведения аудита не регламентируется • Аудит исходит из угроз информационной безопасности, тем самым позволяет покрыть большое число уязвимостей	• Необходимо участие сотрудников организации в процессе проведения аудита • Высокие требования к качеству информации, предоставляемой компанией заказчиком • Длительные подготовительные работы • Процесс аудита может занять большое количество времени

Возможности	Угрозы
• Накопленный большой опыт экспертных знаний в сфере информационной безопасности • Наличие необходимых нормативно-правовых документов • Аудит может быть осуществлен сотрудниками подразделения информационной безопасности предприятия • Возможность автоматизации процесса аудита	• Отсутствуют средства автоматизации процесса • Необходимость доверия оценкам экспертов • Высокие требования к компетентности экспертов • Возможны противоречия во мнениях экспертов

Таблица 3 - Анализ методики аудита ИБ на соответствие стандартам

Сильные стороны	Слабые стороны
• Порядок проведения аудита регламентируется нормативными документами • В нормативных документах присутствует описание отчетных документов • Не требуется дополнительного программного обеспечения • Не требуется прекращение работы системы во время проведения аудита	• Необходимо участие сотрудников организации в процессе проведения аудита • Аудит необходимо проводить каждый раз при изменении системы • Высокие требования к качеству информации, предоставляемой организацией-заказчиком • Процесс аудита может занять большое количество времени • Большое количество нормативно-правовых документов
Возможности	**Угрозы**
• Сертификат безопасности, выдаваемый в результате проведения аудита, повышает престиж организации • В требованиях нормативных документов находят отражение лучшие практические выводы экспертов • Высокий спрос на рынке	• Нормативная база постоянно дорабатывается • Противоречия в нормативно-правовых документах • Невозможно выполнить аудит силами самой организации, т. к. сертификат соответствия выдает только аккредитованная организация

Этапы проведения аудита ИБ. На первом этапе совместно с заказчиком разрабатывается регламент, устанавливающий состав и порядок проведения работ. Основная задача регламента заключается в определении границ, в рамках которых будет проведено обследование. Регламент является тем документом, который позволяет избежать взаимных претензий по завершении аудита, поскольку чётко определяет обязанности сторон [4].

На этом этапе цели проведения аудита уточняются и планируются все последующие шаги. Проводятся сбор исходных данных от заказчика, их предварительный анализ, а также организационные мероприятия по подготовке проведения аудита:

– уточняются цели и задачи аудита;
– формируется рабочая группа;
– подготавливается и согласовывается техническое задание на проведение аудита.

В состав рабочей группы должны входить специалисты компании исполнителя (компании проводящей аудит) и сотрудники компании заказчика. Этап постановки задачи завершается разработкой, согласованием и утверждением технического задания (ТЗ). В ТЗ на аудит фиксируется состав и содержание работ по аудиту и требования к разрабатываемым документам. Кроме того, в ТЗ вносят сроки проведения работ, а при необходимости — план-график.

На втором этапе в соответствии с согласованным регламентом осуществляется сбор исходной информации. Методы сбора информации включают интервьюирование сотрудников заказчика, анализ предоставленной организационно-распорядительной и технической документации, использование специализированных инструментальных средств. На этом этапе собирается информация и дается оценка следующих мер и средств:

– организационных мер в области информационной безопасности;
– программно-технических средств защиты информации;
– обеспечения физической безопасности.

Анализируются следующие характеристики построения и функционирования корпоративной информационной системы:

– организационные характеристики;
– организационно-технические характеристики;
– технические характеристики, связанные с архитектурой ИС;
– технические характеристики, связанные с конфигурацией сетевых устройств и серверов ИС;

– технические характеристики, связанные с использованием встроенных механизмов информационной безопасности.

После получения исходных данных готовится отчет об обследовании. Отчет об обследовании является основой для последующих этапов аудита: анализа рисков и разработки рекомендаций.

Третий этап работ предполагает проведение анализа собранной информации с целью оценки текущего уровня защищённости автоматизированной системы заказчика. В процессе анализа *определяются риски информационной безопасности*, которым может быть подвержена организация. Фактически риск представляет собой интегральную оценку того, насколько эффективно существующие средства защиты способны противостоять атакам с использованием информационных технологий [1 2, 5]. Анализ рисков — это то, с чего должно начинаться построение любой системы информационной безопасности. Он включает в себя мероприятия по обследованию безопасности ИС, с целью определения того какие ресурсы и от каких угроз надо защищать, а также в какой степени те или иные ресурсы нуждаются в защите. Определение набора адекватных контрмер осуществляется в ходе управления рисками. Риск определяется вероятностью причинения ущерба и величиной ущерба, наносимого ресурсам ИС, в случае осуществления угрозы безопасности. Анализ рисков состоит в том, чтобы выявить существующие риски и оценить их величину (дать им качественную, либо количественную оценку). Задача управления рисками заключается в выборе обоснованного набора контрмер, позволяющих снизить уровни рисков до приемлемой величины. Стоимость реализации контрмер должна быть меньше величины возможного ущерба. Разница между стоимостью реализации контрмер и величиной возможного ущерба должна быть обратно пропорциональна вероятности причинения ущерба.

По результатам проведённого анализа на четвёртом этапе проводится разработка рекомендаций по повышению уровня защищённости от угроз информационной безопасности.

Как правило, разработанные рекомендации направлены не на полное устранение всех выявленных рисков, а лишь на их уменьшение до приемлемого остаточного уровня. При выборе мер по повышению уровня защиты автоматизированной системы учитывается одно принципиальное ограничение – стоимость их реализации не должна превышать стоимость защищаемых информационных ресурсов. В завершении процедуры аудита его результаты оформляются в виде отчётного документа, который предоставляется заказчику.

В зависимости *от вида аудита* используются две основные группы методов расчёта рисков безопасности. Первая группа методов

позволяет установить уровень риска путём оценки степени соответствия определённому набору требований по обеспечению ИБ. В качестве источников таких требований могут выступать документы, представленные на рисунке 1.

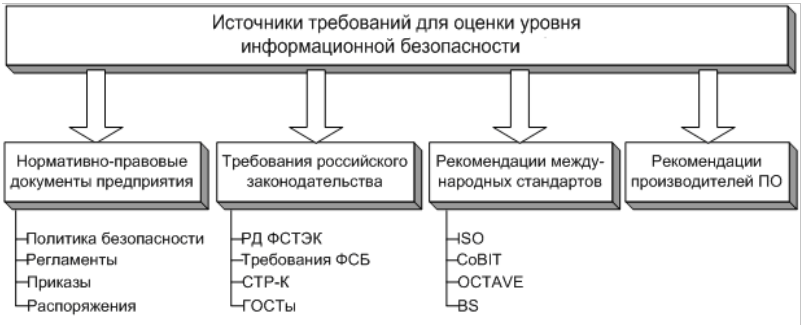


Рисунок 1 – Источники требований информационной безопасности, на основе которых может проводиться оценка рисков

Данная группа методов используется при проведении оценки ИС на предмет соответствия стандартам и руководящим документам.

Вторая группа методов оценки рисков информационной безопасности используется при проведении инструментального анализа защищенности и базируется на определении вероятности реализации атак, а также уровней их ущерба. В данном случае значение риска вычисляется отдельно для каждой атаки и в общем случае представляется как произведение вероятности проведения атаки на величину возможного ущерба от этой атаки. Значение ущерба определяется собственником информационного ресурса, а вероятность атаки вычисляется группой экспертов, проводящих процедуру аудита [1, 2, 5].

Выводы. Аудит информационной безопасности — один из эффективных методов получения объективной информации о текущем уровне защищенности организации от угроз информационной безопасности. Кроме того, результаты аудита являются основой для формирования стратегии развития СОИБ организации.

Активный аудит позволяет взглянуть на защищенность ИС со стороны хакера. Аудитор выполняет роль хакера. Из минусов подхода – необходимость установки дополнительного ПО и длительность проведения аудита.

Экспертный аудита ИБ позволяет наиболее комплексно оценить состояние рассматриваемой системы с точки зрения ИБ путем работы с

профессиональным экспертом, имеющим соответствующую квалификацию и обладающим объемными знаниями в области обеспечения информационной безопасности в системах разного уровня и назначения. Применение экспертных систем позволит, с одной стороны, компании-заказчику проводить аудит собственными силами, а экспертов по информационной безопасности приглашать только в критических ситуациях; с другой стороны, для компании-аудита экспертная система может выступать в качестве инструментального средства, позволяющего ускорить процесс проведения аудита и облегчить работу экспертов. Однако, проведение экспертного аудита информационной безопасности требует хорошей подготовки экспертов, а специалистов такого уровня очень мало. Кроме того, решение задачи плохо формализуется и в большей степени строится на личном опыте и интуиции. Поэтому в разных условиях можно использовать различные комбинации методик, в качестве метода проведения предварительного аудита или подтверждения и представления результатов, полученных посредством проведения экспертного аудита.

Аудит на основе анализа стандартов информационной безопасности является самым практичным. Стандарты ИБ определяют базовый набор требований безопасности для широкого класса систем, который формируется в результате обобщения мировой практики. От аудитора в данном случае требуется правильно определить набор требований стандарта, соответствие которым требуется обеспечить для конкретной исследуемой системы. Однако, этот аудит невозможно выполнить силами самой организации, т. к. сертификат соответствия выдает только аккредитованная организация-аудитор.

На практике может применяться и комплексный аудит ИБ с использованием нескольких методик сразу. Комплексный аудит безопасности ИС позволяет получить наиболее полную и объективную оценку защищенности системы, локализовать имеющиеся проблемы и разработать эффективную программу построения СОИБ организации [5]. Одним из минусов подхода является его дороговизна.

В заключении отметим, что аудит безопасности не является однократной процедурой, а должен проводиться на регулярной основе.

Библиографический список

1. Мошак Н. Н. Безопасность информационных систем: учеб. пособие. СПб.: ГУАП, 2019. 169 с.
2. Мошак Н. Н., Птицына Л. К. Защищенные информационные системы: учеб. пособие. СПб: СПбГУТ, 2020. 216 с.

3. Мошак Н.Н. Основы управления информационной безопасностью: Учеб. пособие/ Н.Н.Мошак; под ред. В.В. Овчинникова. – СПб.: ГУАП, 2022. – 141 с.
ISBN 978-5-8088-1711-1
4. А.В. Солодянников. Информационная безопасность автоматизированных систем. – СПб.: Изд-во СПбГЭУ, 2020. – 108 с.
5. Малыш В.Н., Фролов И.Н. Аудит информационной безопасности и консалтинг: Учебно-методическое пособие – Липецк: ЛГПУ, 2012. – 141с.
6. Аверичников В. И., Рытов М. Ю., Кувылкин А. В., Рудановский М. В. Аудит информационной безопасности органов исполнительной власти: учебное пособие. – М.: Флинта, 2011. – 100 с.
7. Астахов А. Введение в аудит информационной безопасности // GlobalTrust Solutions [Электронный ресурс]. 2018. – URL: http://globaltrust.ru (дата обращения: 09.12.2022).
8. Оценка состояния информационной безопасности за определенный период времени (URL - https://rtmtech.ru/services/otsenka-sostoyaniya-ib-za-period/).
9. А.Н. Андрончик, В.В. Богданов, Н.А. Домуховский, А.С. Коллеров, Н.И. Синадский, Д.А. Хорьков, М.Ю. Щербаков. Защита информации в компьютерных сетях. - Екатеринбург УГТУ–УПИ, 2008.
10. Фабричная, А. С. Аудит информационной безопасности: основные принципы проведения и методика / А. С. Фабричная // Учет и статистика. – 2008. – № 1(11). – С. 178-183. – EDN JUFVOF.
11. Курбатоввa, М. С. Обзор зарубежных методик аудита безопасности информационных систем / М. С. Курбатоввa, Е. С. Поликарпов // Актуальные проблемы кибербезопасности в сети Интернет: Сборник научных трудов Всероссийской конференции, Москва, 23 апреля 2020 года. – Москва: Московский университет Министерства внутренних дел Российской Федерации им. В.Я. Кикотя, 2020. – С. 157-160. – EDN KHFKAL.

УДК 621.311.23: 629.12
А.В. Михайличенко, И.Б. Паращук, д-р техн. наук, профессор
Военная академия связи
г. Санкт-Петербург, Россия

АНАЛИЗ НАДЕЖНОСТИ МОБИЛЬНЫХ ЦЕНТРОВ ОБРАБОТКИ ДАННЫХ: ПРОБЛЕМЫ И ПЕРСПЕКТИВЫ

Аннотация
Доклад посвящен анализу роли и места современных мобильных центров обработки данных в информационно-телекоммуникационной инфраструктуре, а также вопросам совершенствования методологии анализа надежности мобильных центров обработки данных. Основное содержание доклада составляет описание сущности современных проблем методологии анализа надежности объектов такого класса, а также формулировка основ нового, перспективного подхода, построенного на гранулярных вычислениях и позволяющего учитывать различного рода неопределенность исходных данных.
Ключевые слова: надежность, методика, мобильный центр обработки данных, гранулярные вычисления, показатель, анализ.
Annotation
The report is devoted to the analysis of the role and place of modern mobile data centers in the information and telecommunications infrastructure, as well as issues of improving the methodology for analyzing the reliability of mobile data centers. The main content of the report is a description of the essence of the modern problems of the methodology for analyzing the reliability of objects of this class, as well as the formulation of the foundations of a new, promising approach based on granular calculations and allowing for various kinds of uncertainty of the source data.
Keywords: reliability, methodology, mobile data center, granular computing, indicator, analysis.

В современных условиях эволюционного развития информационно-телекомуникационной сферы, как у нас в стране, так и в мире в целом, все большее значение приобретают центры обработки данных (ЦОД). При этом особую роль играют мобильные ЦОД, позволяющие хранить и обрабатывать большие массивы данных, максимально приближенных к местам расположения пользователей. Мобильные ЦОД представляют собой гибкие и масштабируемые системы, к которым относят контейнерные ЦОД и дата-центры на транспортной базе [1].

Высокий уровень требований к современному цифровому контенту предопределяет возросшие требования к надежности архитек-

туры мобильных ЦОД, к алгоритмам поддержания их работоспособности, ремонтопригодности и восстанавливаемости. Это, в свою очередь, обуславливает ужесточение требований к оперативности и достоверности методов и средств анализа надежности мобильных ЦОД, накладывает отпечаток на требования к алгоритмам оценивания технической надежности их программно-аппаратных средств. Иными словами, существует объективная необходимость в точных и оперативных методологических инструментах анализа надежности мобильных ЦОД.

Проблемы анализа надежности сложных технических систем связаны, в основном, с формулировкой системы показателей надежности, поиском критериев оценки вероятностной меры надежности и определением состава обобщенного, комплексного показателя надежности. Но системная, базовая проблема – необходимость учета динамики изменения условий применения таких систем (Арктика, пустыня и т.д.), а также необходимость учета различного рода неопределенности исходных данных для оценки и поддержанию надежности таких ЦОД.

В этой связи перспективным, на наш взгляд, является подход, ориентированный на алгоритмы гранулярных вычислений (ГВ) [2]. Эти алгоритмы позволяют решать задачи идентификации и оценки большого количества (массивов) нечетко, неполно и недостоверно заданных (наблюдаемых) параметров в интересах анализа надежности таких динамических систем с изменяющейся в процессе функционирования структурой, как мобильные ЦОД.

Иными словами, для решения задач интеллектуальной информационной оценки надежности мобильных ЦОД и формирования точных, формализованных и однозначных значений (на основе нечетких знаний) исходных данных для оценки надежности, могут использоваться методы и алгоритмы ГВ, иногда называемые fuzzy-granular computing – нечетко-гранулярные вычисления [2-4]. В рамках подобных задач также иногда говорят о «неточных множествах», как о широко известных в настоящее время подходах к гранулированию информации [3-5].

Под гранулой понимается группа информационных объектов (данных), объединяемых неразличимостью, сходством, близостью, т.е. отношениями, обладающими, по крайней мере, свойствами симметричности и рефлексивности. Термин «гранула» означает динамическую целостную информационную структуру, организованную для достижения некоторой цели, а гранулярные вычисления (методы математической обработки и преобразования информационных гранул) применяются наряду с методами обработки нечеткой информации [4, 5].

Гранулярное представление нечетких множеств для задач анализа надежности мобильных ЦОД в условиях неопределенности позволяет

операции оценивания осуществлять в соответствии с алгоритмами гранулярных (нечетко-гранулярных) вычислений [4, 5]. Алгоритмы ГВ в задачах интеллектуальной обработки данных при оценке надежности МЦОД включают два этапа: этап информационного гранулирования и этап гранулярных вычислений, в рамках которого реализуется математическая обработка информационных гранул с целью преобразования характеризующих их неточных, зашумленных, неупорядоченных и неформализованных нечетких исходных данных большой размерности (избыточных данных) к виду, пригодному для осуществления достоверной параметрической оценки надежности мобильных ЦОД.

Практическая реализация предложенного «гранулярного» подхода позволит устранить нечеткость, зашумленность, неупорядоченность и неформализованность при формировании исходных данных для анализа технической надежности объектов такого класса.

Это, в свою очередь, позволит повысить объективность задания этих исходных данных, и, в конечном итоге, повысить достоверность оценки степени технической надежности, реально присущей таким сложным информационным системам, как мобильные центры обработки данных.

Библиографический список

1. Докучаев В. А., Кальфа А. А., Маклачкова В. В. Архитектура центров обработки данных. М.: Горячая линия-Телеком, 2020. – 240 с.
2. Крюкова Е. С., Ткаченко В. В., Михайличенко А. В., Паращук И. Б. Вопросы оценки надежности современных систем хранения данных для мобильных дата-центров // Наукоемкие технологии в космических исследованиях Земли. 2021. Т. 13. № 5. С. 86–95.
3. Паращук И. Б., Михайличенко Н. В., Михайличенко А. В. Нейронечеткие сети и алгоритмы гранулярных вычислений в задачах интеллектуальной обработки данных для оценки надежности мобильных дата-центров // Применение искусственного интеллекта в информационно-телекоммуникационных системах. Сборник материалов научно-практической конференции. – СПб.: ВАС, 2021. – 174 с., С. 110–115.
4. Минаев Ю. Н., Филимонова О. Ю., Минаева Ю. И. Гранулярный компьютинг в системе нечетких множеств на уровне тензорных гранул // Проблемы информатизации и управления. 2012. №4(40). С. 51-61.
5. Бутакова М. А., Гуда А. Н., Иванченко О. В., Карпенко Е. В. Элементы теории гранулярных вычислений с нечеткими приближенными информационными гранулами. // Вестник Ростовского государственного университета путей сообщения. 2015. № 4(60). С. 27–33.

УДК 004.056
Е. К. Щелокова, А.В. Самойлов
Санкт-Петербургский государственный университет телекоммуникаций им. проф. М.А. Бонч-Бруевича
e-mail: kece7980@gmail.com
e-mail: nogginz1488@gmail.com

МЕХАНИЗМЫ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ В СЕТИ: КРИПТОГРАФИЯ

Аннотация
Рассматриваются понятие криптографии, история и сфера её применения, основные способы и алгоритмы шифрования данных. Оценивается эффективность применения средств криптографической защиты информации на примере DLP-системы «СёрчИнформ КИБ».
Ключевые слова: алгоритм, безопасность, данные, защита информация, криптография, сеть, система, средства защиты, угроза безопасности информации, шифрование, эффективность.
Annotation
This article discusses the concept of cryptography, what this science does and where it takes its history from. The objectives of the article will be the study of data encryption, their algorithms, as well as the consideration of cryptography in the modern world using the example of the SearchInform CIB DLP system.
Keywords: algorithm, security, data, information protection, cryptography, network, system, means of protection, threat to information security, encryption, efficiency.

В современном цифровом мире ключевую роль играет обеспечение безопасности компьютерных систем.

В настоящее время криптографические методы преимущественно используют для защиты информации от несанкционированного доступа. Они также являются основой ряда современных информационных технологий электронного документооборота, электронных денег, тайного электронного голосования и т.д. [1-3].

Рассматриваются работы, в которых предлагаются решения по борьбе с вирусами, направленные на снижение уровня уязвимости защищаемых информационных ресурсов и киберпреступности [4-6].

Анализируются эффективные механизмы обеспечения безопасности в сети за счет применения средств криптографической защиты информации [7].

Библиографический список

1. Волкогонов В. Н., Гельфанд А. М., Карамова М. Р. Обеспечение безопасности персональных данных при их обработке в информационных системах персональных данных // Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2019). – 2019. – С. 266-270.
2. Гельфанд А.М., Пешков А.И., Фадеев И.И., Лансере Н.Н., Система электронного документооборота. Заявка от 26.11.2021 № 2021669214.
3. Пестов И. Е., Кошелева С. А. Атаки на облачную инфраструктуру // Инновационные решения социальных, экономических и технологических проблем современного общества. – 2021. – С. 113-115.
4. Рыжиков А. А., Цветков А. Ю. Разработка программного комплекса по аудиту устройств в сетях // Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2020). – 2020. – С. 779-782.
5. Синельщиков В. С., Цветков А. Ю. Защита персональных данных на предприятии // Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2021). – 2021. – С. 653-657.
6. Темченко В. И., Цветков А. Ю. Проектирование модели информационной безопасности в операционной системе // Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2019). – 2019. – С. 740-745.
7. Кушнир Д. В., Шемякин С. Н. Особенности формирования ключевых данных в квантовой криптографической сети // Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2021). – 2021. – С. 560-564.

ПРОБЛЕМЫ РАЗВИТИЯ ИНФОРМАЦИОННОГО ОБЩЕСТВА. ЦИФРОВАЯ ЭКОНОМИКА

УДК 338.242

Д.Е. Бекбергенева, доктор экон. наук, доцент, М.Л. Слободян, канд. экон. наук, доцент

ФГБОУ ВО «Югорский государственный университет»

ПАРАДИГМА ЦИФРОВОЙ ТРАНСФОРМАЦИИ СОЦИАЛЬНО-ЭКОНОМИЧЕСКОГО РАЗВИТИЯ РЕГИОНА

Аннотация

Развитие цифровых технологий, цифровая трансформация региональной экономики, влияет на экономическое развитие региона в целом, за счет смены парадигмы развития. Цель исследования – стратегия цифровой трансформации региональной экономики. Объект исследования – парадигмы цифровой трансформации бизнес-процессов и предприятий.

Ключевые слова: цифровая трансформация, парадигма цифровизации, автоматизация, роботизация, оцифровывание бизнес-процессов, регион

Abstract

The development of digital technologies, the digital transformation of the regional economy, affects the economic development of the region as a whole, due to a change in the development paradigm. The purpose of the study is the strategy of digital transformation of the regional economy. The object of research is the paradigm of digital transformation of business processes and enterprises.

Keywords: digital transformation, digitalization paradigm, automation, robotization, digitization of business processes, region

Изучая научную литературу других стран, можно выделить сущность процесса цифровизации – трансформация не только экономической, но и социальной сфер общественной жизни [1]. Цифровая трансформация есть процесс постоянных изменений, обеспеченный внедрением различных цифровых решений, методов и технологий во всех сферах общественной жизни [2]. Современная парадигма цифровизации экономики региона должна основываться на данной концепции, чтобы соответствовать современным реалиям общества, поскольку технологии, реализуемые в рамках данной концепции, подразумевают методы и решения, которые обеспечивают формирование, обработку и реализацию больших объемов информации, а также алгоритмы, управляющие

производством за счет современных сенсоров, аддитивных технологий, виртуальных технологий и индивидуализации процесса взаимодействия с потребителем [3]. В данной сфере следует обратить внимания на исследования в области концепций «Индустрия 3.0» и «Индустрия 4.0», представленные в работах А. В. Шукалова, Д. А. Заколдаева, И. О. Жаринова. [4,5]

Автороми работы была построена диаграмма направлений современной парадигмы цифровой трансформации (рисунок 1).

Рисунок 1 - Ключевые направления парадигмы цифровой трансформации региональной экономики (составлено автором)

В результате данной работы были определены шесть ключевых направлений цифровой трансформации региональной экономики: трансформация процессов создания ценностей; виртуализация предприятий; автоматизация процессов обработки информации; взращивание современного цифрового менталитета населения; обеспечение стремительного роста производительности предприятий в области высоких технологий; взращивание цифрового менталитета среди стейкхолдеров, обеспечивающий региональное развитие.

По результатам исследования парадигмы цифровой трансформации региональной экономики можно сделать следующие выводы: цифровая трансформация региональной экономики за счет применения концепции развития «Индустрия 4.0», несет в себе положительную массу современных, технологических решений и методологий оптимизации, автоматизации и цифровизации ключевых бизнес-процессов региональной экономики. Рассматриваемая концепция адаптивна, поскольку

имеет значительный ряд направлений развития, стратегий внедрения изменений, что позволяет считать её практически полностью автономной, всесторонней, универсальной концепцией улучшений, способствующей значительному росту эффективности и качества делопроизводства бизнес-процессов.

Библиографический список

1. Кац Р.Л. Преобразующее экономическое воздействие цифровых технологий, Восемнадцатая сессия Комиссии по науке и технике в целях развития // 2015, с 1–13.
2. Стольтерман Э., Крун Ф.А. Исследование информационных систем: актуальная теория и обоснованная практика // Springer. 2004. С. 689
3. Бекбергенева, Д.Е. Ключевые направления развития Индустрии 4.0 в современных условиях цифровизации экономики // Экономические науки. 2020. № 185. С. 61-65. URL: https://ecsn.ru/files/pdf/202004/202004_61.pdf
4. Шукалов А.В., Заколдаев Д.А., Жаринов И.О. Алгоритмы проектирования механосборочного производства предприятий Индустрии 3.0 и Индустрии 4.0 // ТПУ. 2018. № 3-4 (117-118). С. 148-154.

УДК 004.056.53

А.М. Колбанёв, технический директор блока ООО «ЭР-1»

ПРОБЛЕМЫ И ЗАДАЧИ ЦИФРОВИЗАЦИИ ЖИЛИЩНО-КОММУНАЛЬНОГО ХОЗЯЙСТВА

Аннотация

Рассматривается жилищно-коммунальное хозяйство (ЖКХ) как предметная область внедрения информационных систем и технологий цифровой экономики. Формулируются цели цифровизации ЖКХ, направленные на повышение комфорта, безопасности и ресурсоэффективности как собственников квартир, так и управляющих организаций. Анализируются особенности цифровых продуктов, внедряемых для достижения поставленных целей.

Ключевые слова: ЖКХ, цифровой продукт, умный город, нематериальный актив, безопасность территории, комфорт, цифровизация.

Annotation

Housing and communal services (housing and communal services) are being considered as a subject area of the introduction of information systems and technologies of the digital economy. The goals of digitalization of housing and communal services aimed at improving the comfort, safety and resource efficiency of both apartment owners and management organizations are formulated. The features of digital products implemented to achieve the set goals are analyzed.

Keywords: housing and communal services, digital product, smart city, intangible asset, territory security, comfort, digitalization.

С развитием цифровых технологий, развитием общества, ростом благосостояния населения, возникают и дополнительные потребности в безопасности, комфорте, ресурсоэффективности, уже недостаточно базовых потребностей, которые были. Так, например, очень важно обеспечить безопасность на прилегающей территории к жилому комплексу и внутри дома, теперь каждый объект недвижимости должен быть оборудован системами умной домофонии, умной системой сбора показаний потребления электрической энергии с приборов учета согласно Постановлению Правительства № 890 [1], видеонаблюдения, организация закрытой территории жилого комплекса с калитками, воротами и/или шлагбаумами обеспечивающими разнообразные сценарии доступа на территорию и управления ими как для управляющей организации, так и сценариями для жителей. Для снятия показаний с приборов учета больше нет необходимости подходить к каждому из них и переписывать показания передавая затем эти данные также под запись в управляющею организацию. В режиме on-line из любой точки присутствия есть доступ

к видеокамерам, расположенным на территории ЖК, звонок в домофон теперь отражается в мобильном приложении телефона вне зависимости от местонахождения. Через единую цифровую среду выстраивается процесс взаимодействия жителя и управляющей организации, есть возможность контроля сроков выполнения работ по заявкам и контроль качества выполненных работ, выставление счетов за потребляемые услуги, проведения общих собраний собственников, информирования жителей посредством push уведомлений и много другое.

Разработка и внедрение новых цифровых продуктов позволяет также существенно повысить привлекательность объектов недвижимости для будущих собственников квартир и эффективность эксплуатации управляющей организации, позволяет обеспечить полный цикл контроля за объектом недвижимости, с момента начала строительства контролируя сроки строительства, с возможностью покупки и приемки квартир и последующею эксплуатацию.

В ЖКХ давно назрела необходимость цифровизации и внедрения новых цифровых продуктов [2], новых сценариев управления качеством жизни, цифровыми продуктами и возможностями для управляющих организаций в вопросах обслуживания объектов недвижимости, взаимодействия с собственниками. Цифровизация ЖКХ позволит выйти на новый качественный уровень взаимодействия жителя и управляющей организации обеспечивая растущие потребности в современных цифровых продуктах и качестве клиентского сервиса.

Цифровизация ЖКХ – это долгий и сложный процесс, который требует серьезной административной поддержки, большого объема инвестиций и существенного развития технологий [3].

Жилищно-коммунальное хозяйство России (ЖКХ России) – это совокупность отраслей российской экономики, обеспечивающих работу инженерной инфраструктуры зданий населённых пунктов, создающих удобства и комфортность проживания и нахождения в них граждан путем предоставления им широкого спектра жилищно-коммунальных услуг [4].

В ЖКХ входят жилищное хозяйство (капитальный и текущий ремонт зданий), теплоснабжение, водоснабжение, электроснабжение, ремонт инженерных коммуникаций, а также благоустройство территорий, утилизация мусора и уборка.

ЖКХ – это сложный многоотраслевой производственно-технический комплекс.

Социально-экономическая ситуация в России становится все более зависимой от состояния жизнеобеспечивающих инфраструктурных отраслей, особое место среди которых занимает жилищно-коммунальное

хозяйство (ЖКХ), поскольку от нее зависит нормальное самочувствие миллионов людей. [4]

Рынок ЖКХ огромен, по прогнозам аналитиков, в 2023 г. оборот рынка составит более 3,2 трлн. руб. Эта цифра касается только оборота по содержанию жилья, коммунальных платежей, и капремонту.

Когда мы говорим про цифровизацию ЖКХ России, то имеем в виду огромный комплекс решений, который позволит оптимизировать бюджеты, снизить издержки на содержание недвижимости как для управляющих организаций, так и для собственников помещений и повысить качество жизни.

Цифровизация должна улучшать жизнь, делать эффективными и прозрачными процессы взаимодействия между управляющей организации и жителями [5].

Цифровизация ЖКХ затронет:

– «Умный город»;
– «Умный район»;
– «Умный ЖК»;
– «Умный дом»;
– «Умный двор»;
– «Умная квартира».

Направления цифровизации ЖКХ:

– Информационные системы – информационные ресурсы, поставщики информации;

– Интеллектуальные системы управления – мобильное приложение, интерфейсы управления сбором данных показаний приборов учета, интерфейсы управления доступом, облачные хранилища и т.д.

Жилищно-коммунальное хозяйство России (ЖКХ России) затрагивает:

– 1 087 724 дома;
– 2 758,18 млн кв.м.;
– 48 999 шт., управляющих организаций;
– 32 098 шт., ТСЖ, ЖСК, и иных организаций;
– 145,6 млн. человек.

Одно из главных отличий цифровых продуктов от физических состоит в том, что они зачастую продолжают улучшаться уже будучи проданными потребителям – выходят обновления программного обеспечения, совершенствуются функции сервиса.

Цифровой продукт – нематериальный актив или контент.

Другая особенность цифровых продуктов от прочих заключается в том, что они легко масштабируются.

Цифровой актив как результат интеллектуальной деятельности можно запатентовать, тем самым ограничив свободу конкурентов по выводу на рынок похожих продуктов и получив возможность продавать право на его использование.

Сделать жилой комплекс/дом удовлетворяющей современным требованиям по комфорту, безопасности и ресурсоэффективности для собственников квартир и для управляющих организаций, предоставить им возможность пользоваться современными цифровыми продуктами это и есть задачи цифровизации ЖКХ.

Пользователи цифровых продуктов должны иметь постоянный доступ к модулям управления системами умной домофонии, контроля доступа на территорию ЖК, телеметрии, видеонаблюдения, оперативно получать информацию, со стороны управляющих организаций должны иметь возможность контроля, мониторинга и своевременного устранения возможных аварийных ситуаций.

Неотъемлемой частью становится взаимодействие жителей с управляющей организацией, для этого должна быть единая цифровая платформа, обеспечивающая взаимодействия всех элементов цифровых продуктов.

Цифровой продукт в зависимости от класса жилья, потребности застройщика, законодательства и в будущем управляющей организации должен иметь возможность легкого масштабирования продуктов и сценариев жизни от небольшого проникновения до максимального.

С внедрением цифровых продуктов в ЖКХ у жителей обеспечивается потребность в комфорте и безопасности, появляется возможность управлять потреблением ресурсов и наличием прозрачного взаимодействия с управляющей организацией в свою очередь управляющая организация более качественно управляет жилищным фондом, может улучшать качество клиентского сервиса, более тесно взаимодействуя с жителями.

Библиографический список

1. Постановление Правительства РФ от 19 июня 2020 г. N 890 "О порядке предоставления доступа к минимальному набору функций интеллектуальных систем учета электрической энергии (мощности)"
2. Куклина Е.А., Мицеловская О.С. Современные проблемы жилищно-коммунального хозяйства Российской Федерации и направления их решения // Экономика нового мира. 2019. №4 (16). URL: https://cyberleninka.ru/article/n/sovremennye-problemy-zhilischno-kommunalnogo-hozyaystva-rossiyskoy-federatsii-i-napravleniya-ih-resheniya (дата обращения: 08.03.2023).

3. Никифорова Т.И., Нижальская Н.И. Цифровизация ЖКХ как основа развития отрасли // Индустриальная экономика № 4, том 2, 2022. С. 125 – 129.
4. "Жилищный кодекс Российской Федерации" от 29.12.2004 N 188-ФЗ (ред. от 21.11.2022) (с изм. и доп., вступ. в силу с 01.03.2023)
5. Цифровизация ЖКХ: темпы, тренды и примеры внедрения умных решений. URL: https://roskvartal.ru/tehnologii-v-zhkh/13428-cifrovizaciya-zhkh-tempy-trendy-i-primery-vnedreniya-umnyh-resheniy (дата обращения: 08.03.2023).

УДК: 330.47
Н.А. Кузнецова, старший преподаватель
ФГБОУ ВО «Омский государственный аграрный университет имени П.А.Столыпина»

ВОЗМОЖНОСТИ ПРИМЕНЕНИЯ ЦИФРОВЫХ ТЕХНОЛОГИЙ В РАЗВИТИИ СИСТЕМЫ УПРАВЛЕНИЯ ОТХОДАМИ РАСТЕНИЕВОДСТВА

Аннотация: *Обеспечение деятельности организаций в области управления отходами растениеводства достоверными, актуальными и достаточными данными является важнейшим фактором принятия своевременных и эффективных управленческих решений. В статье рассмотрены основные тенденции применения цифровых технологий в системе управления отходами отрасли растениеводства, способы, с помощью которых цифровизация может повысить использование инновационных моделей по управлению отходами.*
Ключевые слова: цифровые технологии, цифровизация, отходы растениеводства, система управления отходами, регион.
Abstract: *Ensuring the activities of organizations in the field of crop waste management with reliable, relevant and sufficient data is the most important factor in making timely and effective management decisions. The article discusses the main trends in the use of digital technologies in the waste management system of the crop industry, the ways in which digitalization can increase the use of innovative waste management models.*
Key words: digital technologies, digitalization, crop waste, waste management system, region.

Основная цель системы управления отходами сельского хозяйства, в том числе и отходами растениеводства, на региональном уровне заключается в максимальном сокращении негативного влияния отходов на окружающую среду за счет эффективного использования ресурсов на всем протяжении их жизненного цикла, сокращения объемов производимых отходов и использования отходов как сырья для производства новой продукции. Сохранение ресурсов и использование технологий, связанных с повторным использованием и переработкой отходов, оказывают положительное влияние на развитие экономики региона. Очевидно, что региональные долгосрочные стратегии управления отходами должны предусматривать как совершенствование методов их сбора, так и использование инновационных моделей по управлению ими. Ключевым элементом повышения эффективности системы управления отходами растениеводства на региональном уровне может стать применение цифровых технологий [3].

По оценке Министерства сельского хозяйства России и экспертов, использование цифровых технологий в АПК позволяет повысить рентабельность сельхозпроизводства путем точечной оптимизации затрат и более эффективного распределения средств при комплексном подходе с внедрением элементов цифровой экономики [2, 5].

Одним из ключевых этапов решения проблемы управления отходами в России на национальном уровне было принятие в 2020 г. национальных целей развития до 2030 года и плана создания «устойчивой системы обращения с отходами» [4]. Законодательство Российской Федерации обязывает каждый регион разработать современную стратегию обращения с отходами для создания экологически безопасной и экономически эффективной системы потребления продуктов и товаров. При разработке стратегии особое внимание должно уделяться цифровизации не только технологических процессов переработки уже образованных отходов, но и предотвращения их формирования.

Для своевременного и эффективного принятия управленческого решения необходимо располагать данными о количестве образующихся отходов; вести учет сырья и материалов, извлеченных из отходов для вторичного использования; а также знать количество отходов, отправляющихся на дальнейшее обезвреживание и захоронение. В связи с этим, возникает необходимость получения информации, отражающей реальные показатели образования отходов.

С целью организации такого учета службой государственной статистики разработана формы статистической отчетности − №2-ТП (отходы) «Сведения об образовании, обработке, утилизации, обезвреживании, размещении отходов производства и потребления». Но такая форма отчетности имеет свои недостатки, к которым можно отнести: внесение недостоверной информации; ошибки в заполнении данной формы отчетности; высокие затраты труда на заполнение формы и предоставление ее в контролирующие органы; сложное взаимодействие лиц и ведомств, задействованных в сборе такой информации [1];

Таким образом, выявленные недостатки современной системы управления отходами актуализируют потребность к поиску новых подходов с использованием цифровых технологий.

Анализ, выполненный автором, показал, что исследования и разработки российских и зарубежных ученых в области цифровизации управления отходами сосредоточены на описании будущих цифровых технологий. К ним можно отнести концепции цифрового управления отходами в устойчивых городах, создание прототипов интеллектуальных контейнеров, цифровая классификация изображений для сорти-

ровки отходов и другие [1]. В отраслевом разрезе исследования в большей степени сосредоточены на решении вопроса в жилищно-коммунальной сфере, сельскому хозяйству уделяется очень мало внимания.

Вместе с тем, на рынке появляются новые эко-ориентированные подходы [7], бизнес-модели, например, платформы электронной торговли отходами. Отмечается тенденция расширения ассортимента программного обеспечения для работы с отходами и бизнес-аналитики в исследуемой сфере [1].

Следует отметить, что элементы цифровизации имеются на разных этапах процесса обращения с отходами, однако эффекты их использования неоднородны: разные технологии применяются в разных масштабах.

Очевидно, что эффективная региональная система управления отходами должна создавать прозрачную систему, в которой возможно эффективное взаимодействие всех заинтересованных сторон. Цифровизация этого процесса поможет улучшить экологическую обстановку и создаст основу для построения эффективной системы переработки отходов [6]. Причем информационно-коммуникационные технологии могут выступать не только основными инструментами, помогающими улучшить управление отходами, но и способом информирования населения о решении проблем в этой сфере.

Библиографический список:

1. Колесников Р.В. Совершенствования статистического обеспечения деятельности по управлению твердыми коммунальными отходами с использованием процессов цифровизации // Научный журнал НИУ ИТМО. Серия «Экономика и Экологический менеджмент». № 4. 2021. С. 131-141.

2. Кузнецова Н.А., Зинич Л.В., Асташова Е.А. Оценка потенциала цифровизации сельского хозяйства Омской области // Креативная экономика. 2022. Том 16. № 11. URL: https://creativeconomy.ru/lib/116572

3. Печенкина, А. В. Роль цифровизации в развитии системы управления отходами: региональный аспект / А. В. Печенкина, Т. Г. Краснова // Конкурентный потенциал региона: оценка и эффективность использования: Сборник статей XIII Международной научно-практической конференции, Абакан, 09–12 ноября 2022 года. – Абакан: Издательство ФГБОУ ВО «Хакасский государственный университет им. Н. Ф. Катанова». 2022. С. 239-241.

4. Утилизационные амбиции требуют амуниции // URL: https://www.kommersant.ru/doc/5667389 (дата обращения 20.09.2022 г.)

5. Цифровая трансформация сельского хозяйства России: офиц. изд. – М.: ФГБНУ «Росинформагротех». 2019. 80 с. URL: https://mcx.gov.ru/upload/iblock/28f/28f56de9c3d40234dbdcbfac94787558.pdf (дата обращения 20.09.2022 г.)
6. Цифровизация - драйвер развития отрасли обращения с отходами // URL: https://www.comnews.ru/content/216919/2021-10-14/2021-w41/cifrovizaciya-drayver-razvitiya-otrasli-obrascheniya-otkhodami (дата обращения 21.09.2022 г.)
7. Козлова О.А. Экологический маркетинг: новый концептуальный подход и стратегический потенциал производителей// Вестник ОмГУ. Серия «Экономика». – 2011. – № 1. С. 146–156

УДК 621.311.23: 629.12
С.А. Шинкарев, канд. техн. наук, доцент, И.Б. Паращук, д-р техн. наук, профессор, Е.С. Крюкова, канд. техн. наук
Военная академия связи
г. Санкт-Петербург, Россия

ВЛИЯНИЕ СТРУКТУРНЫХ ПАРАМЕТРОВ НА ОЦЕНКУ КАЧЕСТВА СЕТЕЙ ПЕРЕДАЧИ ДАННЫХ И ЭЛЕКТРОННЫХ БИБЛИОТЕК

Аннотация
Рассмотрены ключевые понятия, особенности структуры и базовые компоненты современных сетей передачи данных и электронных библиотек. Проведен анализ видов и особенностей их структуры, определяющих пригодность данных объектов к применению по назначению. Выдвинута гипотеза о возможности построения интеллектуального алгоритма, который бы при оценке качества объектов такого класса производил выборку тех элементов, а значит и тех показателей качества структуры и компонентов, которые вносят наибольший вклад в качество сетей передачи данных и электронных библиотек в целом.
Ключевые слова: структура, сеть передачи данных, компонент, показатель, электронная библиотека, качество, параметр.
Annotation
The key concepts, structural features and basic components of modern data transmission networks and electronic libraries are considered. The analysis of the types and features of their structure that determine the suitability of these objects for their intended use is carried out. A hypothesis has been put forward about the possibility of constructing an intelligent algorithm that, when assessing the quality of objects of this class, would make a selection of those elements, and therefore those indicators of the quality of the structure and components that make the greatest contribution to the quality of data transmission networks and electronic libraries in general.
Keywords: structure, data transmission network, component, indicator, electronic library, quality, parameter.

Современные сети передачи данных (СПД) и электронные библиотеки (ЭБ), использующие СПД в качестве транспортной составляющей, являются, по сути, сложными техническими информационно-телекоммуникационными системами, причем смена их физического состояния под воздействием окружающей среды характеризует поведение таких систем и описывается процессами функционирования их элементов. Активное развитие информационных технологий и сложность современных

условий эксплуатации подобных систем повышает актуальность проблемы обоснования и разработки новых методов оценки качества функционирования как самих СПД и ЭБ, так и качества реализуемых ими процессов передачи данных и предоставления контента. Анализ факторов, влияющих на качество функционирования таких сложных информационно-телекоммуникационных систем, как СПД и ЭБ, говорит о том, что важное место в качестве подобных объектов занимают факторы, обуславливающие и характеризующие их структуру [1-3].

При этом различают физическую, логическую, программную, функциональную и топологическую структуры. Физическая структура СПД и ЭБ – схема связей физических элементов данных систем, таких как технические средства, аппаратура, вычислительная техника и др. Логическая структура СПД и ЭБ – множество типов информационных процессов, реализуемых данными системами, функциональными возможностями этих процессов по обработке и объему информации, по правилам обмена и обработки информации, форматами ее представления. Программная структура СПД и ЭБ – взаимосвязанные программные модули в рамках данных систем. Функциональная структура – обеспечивает выполнение целей и реализацию задач (целевых функций, назначений) СПД и ЭБ. Топологическая структура СПД и ЭБ – обобщенная геометрическая модель физической структуры этих систем.

Рассмотрим влияние структурных параметров на оценку качества сетей передачи данных и электронных библиотек на примере физической и функциональной структуры ЭБ. Физическая и функциональная структура, как организация взаимосвязанных компонентов, например, компонентов ЭБ, может быть описана в виде упорядоченного набора взаимосвязанных подсистем и сервисов. При этом необходимо различать понятия «структура» и «архитектура». Под «структурой» СПД и ЭБ понимается состав элементов систем такого класса, каждому из которых соответствует определенная функция, организация связей и отношений между элементами СПД и ЭБ. Понятие «архитектура» СПД и ЭБ включает организацию таких систем, воплощенную в ее элементах, их внутренних и внешних связях, на основе общей политики создания и функционирования объектов такого класса [4].

Ключевыми компонентами (элементами функциональной структуры) структуры, например, современной ЭБ, являются подсистема сервиса и подсистема поддержки. Каждая их подсистем ЭБ обладает своими свойствами, показателями качества, которые должны учитываться при оценке качества ЭБ в целом. Таким образом, можно отметить, что элементами функциональной структуры ЭБ являются фонд ЭБ и все виды ее обеспечения. При этом существенный вклад в общее качество

ЭБ вносят качественные показатели фонда ЭБ в целом, а также качество контента и метаданных, в частности [4].

Анализ особенностей структуры и функциональных возможностей современных СПД и ЭБ показал, что ключевым вопросом теории и практики управления и текущего контроля качества систем такого класса, является математическое моделирование их функционирования, разработка алгоритмов и методов расчета, анализа и прогнозирования их качества.

Иногда о качестве СПД и ЭБ, говорят, как о качестве политики создания и функционирования объектов такого класса. При этом качественная оценка принятой политики создания и функционирования СПД и ЭБ проводится в виде сравнительного статистического анализа их работы, мониторинга показателей их качества, экспертной оценки и, зачастую, введения весовых коэффициентов, определяемых для каждой конкретной СПД и ЭБ. Качественная оценка является основанием для изменения политики создания и функционирования СПД и ЭБ [4].

Таким образом, рассмотрены и систематизированы ключевые понятия и особенности структур современных СПД и ЭБ, их базовые компоненты, которые вносят свой существенный вклад в качество таких сложных технических информационно-телекоммуникационных систем. Анализ общей организации компонентов позволил провести предварительный анализ возможного влияния структурных параметров современных СПД и ЭБ на итоговую оценку их качества. При этом отмечено, что состав и взаимосвязь компонентов обуславливают функциональные возможности СПД и ЭБ, а их структурные параметры численно характеризуют качество систем такого класса. В свою очередь, особенности структуры современных СПД и ЭБ определяют их пригодность к применению в конкретной ситуации.

Учет всех особенностей структуры с точки зрения оценки качества СПД и ЭБ является, безусловно, важной задачей, но использование того или иного показателя качества структуры систем такого класса зависит от многих условий, в том числе от целей, стоящих перед исследователем и от имеющихся исходных данных. Поэтому актуальной остается задача построения интеллектуального алгоритма, который бы при автоматизированной оценке качества СПД и ЭБ производил выборку тех элементов, а значит и тех показателей качества структуры таких сложных объектов, которые вносят наибольший вклад в их качество в целом.

Библиографический список

1. Таненбаум Э., Уэзеролл Д. Компьютерные сети. 5-е изд. – СПб.: Питер, 2012. – 960 с.

2. Зуйкина К. Л., Соколова Д. В., Скалабан А. В. Электронные библиотеки в России. Текущий статус и перспективы развития. – М.: Ваш формат, 2017. – 120 с.
3. ГОСТ Р 7.0.96-2016. Электронные библиотеки. Основные виды. Структура. Технология формирования. – М.: Стандартинформ, 2018. – 11 с.
4. Крюкова Е. С., Паращук И. Б., Ясинский С. А. Общая организация компонентов и анализ влияния структурных параметров современных электронных библиотек на оценку их качества // Труды ЦНИИС. Санкт-Петербургский филиал. Научно-технический сборник статей. Т. 2. №12. 2021. С. 20–26.

ИНФОРМАЦИОННАЯ СРЕДА И ТЕЛЕКОММУНИКАЦИОННАЯ ИНФРАСТРУКТУРА

УДК 004.89

А. В. Митько[1], вице-президент, доц., канд. техн. наук, В. К. Сидоров[2]
[1]Арктическая общественная академия наук
Искровский пр-т 22 офис 175, г. Санкт-Петербург, Россия, 193168
[1]Всероссийский научно-исследовательской институт метрологии имени Д.И. Менделеева
Московский пр-т 19, г. Санкт-Петербург, Россия, 190005
e-mail: arseny73@yandex.ru
[2]Санкт-Петербургский университет ГПС МЧС России
Московский пр-т 149, г. Санкт-Петербург, Россия, 196105
e-mail: hamradio-spb@yandex.ru

ОСНОВНЫЕ ТЕНДЕНЦИИ РАЗВИТИЯ ИНТЕЛЛЕКТУАЛЬНЫХ СИСТЕМ В АРКТИЧЕСКОЙ ЗОНЕ РОССИЙСКОЙ ФЕДЕРАЦИИ

Аннотация
В статье рассматриваются проблемы и перспективы развития искусственного интеллекта. Отмечены актуальность и востребованность использования искусственного интеллекта в Арктической зоне Российской Федерации, как одной из экстремальных территорий деятельности человека. Основные результаты получены в совместных разработках Арктической общественной академии наук и Санкт-Петербургского университета ГПС МЧС России.
Ключевые слова: искусственный интеллект, цифровизация, мониторинг, Арктика, пространственное планирование, информационные технологии, связь.

A. Mitko[1], V. Sidorov[2]
[1]Arctic Public Academy of Sciences
Iskrovskij pr., 22, office 175, Saint-Petersburg, Russia, 193168
[1]D. I. Mendeleev All-Russian research institute of metrology
Moskovskij pr., 19, Saint-Petersburg, Russia, 190005
e-mail: arseny73@yandex.ru
[2]Saint-Petersburg university of State fire service of EMERCOM of Russia
Moskovskij pr., 149, Saint-Petersburg, Russia, 196105
e-mail: hamradio-spb@yandex.ru

MAIN TRENDS IN THE DEVELOPMENT OF INTELLIGENT SYSTEMS IN THE ARCTIC ZONE OF THE RUSSIAN FEDERATION

Abstract
The article deals with the problems and prospects for the development of artificial intelligence. The relevance and demand for the use of artificial intelligence in the Arctic zone of the Russian Federation, as one of the extreme areas of human activity, is noted. The main results were obtained in the joint developments of the Arctic Public Academy of Sciences and St. Petersburg University of the State Fire Service of the Ministry of Emergency Situations of Russia.
Keywords: artificial intelligence, digitalization, monitoring, Arctic, spatial planning, information technology, communications.

Современное развитие экономики и политики в последние годы неоднократно указывало о необходимости создания и локализации ключевых технологий и решений, в том числе для освоения Арктики и разработки морского шельфа. В создавшихся условиях, единственно правильным решением является понимание того, что в стране в самые кратчайшие сроки необходимо сформировать передовую законодательную базу, снять все барьеры для разработки и широкого применения робототехники, искусственного интеллекта, беспилотного транспорта, электронной торговли, технологий обработки больших данных. Это означает, что оба этих направления – Арктика и передовые технологии искусственного интеллекта – находятся в тренде у органов федеральной власти и будут являться наиболее актуальными и приоритетными для внедрения в период до 2025–2030 гг [1].

Исследования в сфере искусственного интеллекта вошли в число приоритетов государственной политики, и именно поэтому в центре внимания оказались отечественные или совместные с зарубежными учёными или практиками разработки интеллектуальных систем и систем искусственного интеллекта. Со страниц средств массовой информации можно узнать о самых передовых зарубежных достижениях, однако и в России существует достаточное количество проектов и уже готовых решений по внедрению искусственного интеллекта в практическое хозяйствование.

За последние тридцать лет на территории российского арктического шельфа открыты более двух десятков месторождений. По предварительным оценкам Института нефтегазовой геологии и геофизики Российской академии наук запасы составляют около 10 млрд тонн нефти. Ресурсы российского шельфа в целом оцениваются отечественными специалистами примерно в 100 млрд тонн условного топлива, из которых более 80% приходится на газ, 20% на нефть [2]. Именно разработка

полезных ископаемых является отправной точкой нового витка освоения Арктики. Поэтому Президент России также считает, что цифровизация топливно-энергетического комплекса и искусственный интеллект приведут к уменьшению стоимости энергоресурсов [3]. Об этом он заявил, выступая в октябре 2017 г. на Международном форуме по энергоэффективности и развитию энергетики «Российская энергетическая неделя». Президент отметил, что одной из ключевых тенденций развития топливно-энергетического комплекса станет быстрая обработка колоссальных объёмов информации и искусственный интеллект, а внедрение умных энергосетей позволит системно анализировать выработку и потребление энергии и в перспективе существенно уменьшить себестоимость энергоресурсов, повысить эффективность их использования и снизить потери.

Количество определений того, что же такое искусственный интеллект, приближается к нескольким десяткам. В данной работе предлагается считать, что искусственный интеллект – это научная дисциплина, занимающаяся моделированием разумного поведения [4].

Необходимо отметить, что в России, равно как и в мировой практике, применение искусственного интеллекта за Полярным кругом до настоящего времени весьма ограничено. Это относится в полной мере к США, Канаде, Норвегии. Также практически отсутствуют системные аналитические работы по возможностям разработки и применения систем искусственного интеллекта для потребностей в Арктике с учётом особых климатических условий и ведения хозяйственной деятельности.

Международные эксперты сходятся во мнении, что к 2030 г. масштабные системы искусственного интеллекта, начиная от умных машин, беспилотного транспорта и роботизированных заводов до умных городских систем и устойчивых производственных комплексов, станут массовым явлением в мировой практике [5].

Несмотря на это, в России ситуация складывается несколько иначе. Последние десять лет с самых высоких трибун звучат обещания о переходе к инновационной экономике знаний и высоких технологий.

При этом российская экономика и хозяйство, в основном, направлены на ресурсные отрасли. Существующее федеральное законодательство является одной из нерешенных проблем, препятствующих массовому внедрению и распространению инновационных технологий. Отечественными законодателями не ведётся системной работы по включению искусственного интеллекта в законодательные акты. В России до сих пор не созданы комитеты, комиссии, крупные инвестиционные группы и консорциумы, которые бы занимались вопросами разработок

и практического внедрения искусственного интеллекта в отрасли хозяйства. Кроме этого, не существует единой базы или реестра проектов внедрения искусственного интеллекта, а имеющиеся публичные работы носят разрозненный и в основном краткий обзорный характер. Большинство проектов в области искусственного интеллекта и робототехники - это краткие по времени стартапы, не переходящие в стадию массового производства, не представляющие собой готовые продукты для внедрения.

Условно хронологию появления и развития форм искусственного интеллекта можно разделить на три этапа. Первый этап относится примерно к середине 1960-х гг., когда впервые были написаны программные коды; специалисты программировали первые правила на основе кибернетических азов. Тогда программное обеспечение и алгоритмы начали решать первые практические задачи. Эти действия привели к созданию автоматизированных процессов, например, появилось планирование маршрутов транспорта или действий промышленных станков. Они стали основой многих современных технологий. В основу второго этапа в 1980-1990-е гг. легло контролируемое машинное обучение. Это попытки распознавания речи и изображений, машинный перевод, интеллектуальный анализ данных и иные сферы применения искусственного интеллекта для облегчения человеку решения ряда задач. С начала 2000-х гг. начался третий этап развития искусственного интеллекта, когда он становится автономным или близким к автономности. Технологии третьего этапа ещё не используются в современных массовых продуктах, но исследователи и практики уже демонстрируют рабочие прототипы и готовые решения.

Необходимо отметить, что современное состояние искусственного интеллекта и связанные с этим вызовы и угрозы, имеют свои особенности использования его в условиях Арктики. Систематизируя накопленный опыт можно сделать следующие выводы:

1. Искусственный интеллект, в случае рассмотрения его как предмета изучения одного из разделов компьютерной науки, уже сегодня способен выполнять достаточно сложные задачи, будучи обученным и натренированным своими создателями.

2. Технологии искусственного интеллекта являются универсальными и не зависят от территорий применения. Не существует арктических особенностей применения методов математического анализа или технологий баз данных, но при этом отмечается ряд задач, специфичных для условий Арктики, и решать их способны интеллектуальные робототехнические комплексы в сфере транспорта, охраны и патрулиро-

вания, разведки и спасения, энергетики и строительства. Таким образом, условия Арктики не накладывают особых требований к зрелости технологий искусственного интеллекта, отличаясь лишь специфическим набором прикладных интеллектуальных задач, решение которых требует его применения.

3. Следует отметить, что все же существует ряд технологических решений, непосредственно применимых только для решения задач, связанных с особенностями условий Арктики, а их необходимость в иных условиях не так актуальна. Это в основном касается добычи полезных ископаемых, строительства и жилищно-коммунального комплекса.

4. Искусственный интеллект не может быть полной заменой человека. Он может снизить нагрузку на человека, существенно упростить процессы, на порядки расширить возможности человека-оператора при решении большого количества рутинных задач. Искусственный интеллект в Арктике может взять на себя решение вопросов во всех сферах, связанных с рутинными технологическими процессами: в добыче или использовании природных ресурсов, логистике, системах жизнеобеспечения, телекоммуникациях и управлении информацией, наблюдении и анализе обстановки.

5. Ограничений по сферам применения искусственного интеллекта в Арктике нет. В каждой из сфер человеческой деятельности найдётся то, что такая система сможет делать гораздо лучше и эффективнее человека.

Подводя итог, можно выделить следующие сферы применения систем искусственного интеллекта в Арктике:

– применение технологий искусственного интеллекта, обработки больших массивов данных, создание интеллектуальных транспортных систем для глобальной транспортной отрасли в Арктике и развития Северного морского пути;

– управление движением беспилотных транспортных средств при решении задач мониторинга Арктики, доставки грузов, проведении спасательных операций;

– высокий потенциал внедрения искусственного интеллекта в отраслях непрерывного производства: нефтяной, газовой и химической промышленности, металлургии. Искусственный интеллект становится основой интегрированного нефтяного и газового инжиниринга;

– электросетевая и генерирующая инфраструктуры. В энергетике новые решения будут базироваться на технологиях предиктивного управления производственными активами, математического моделирования производства, искусственного интеллекта и нейронных сетей;

– медицина. Применение систем мобильной телемедицины в труднодоступных и удалённых поселениях, а также для нужд коренных и малочисленных народов Севера крайне актуально;

– строительство, ЖКХ и промышленность, где искусственный интеллект способен изучать особую для Арктики проектную документацию, находить расхождения на ранних стадиях, помогает снижать расходы на проект и дальнейшее строительство объектов. Искусственный интеллект в ближайшее время станет базисом «умных домов» и «умных городов»;

– автономная робототехника. Управление антропоморфными манипуляторами при полной замене человека в предельно экстремальных условиях, исключающих безопасное пребывание людей;

– информационная поддержка работ, выполняемых людьми, в автономных условиях, при отсутствии связи с материковой частью страны. Системы поддержки принятия решений, экспертные и советующие системы – обслуживание техники и систем жизнеобеспечения, поддержка принятия медицинских решений, поддержка научных исследований и др.;

– автоматизированная обработка информации, поступающей от средств охранного и технологического видеонаблюдения;

– телекоммуникации и связь, энергетика и энергосбережение, спасение;

– применение искусственного интеллекта в военных целях.

Библиографический список

1. «Вертолеты России»: Активное применение БПЛА в Арктике может начаться в течение двух лет [Электронный ресурс] // Aviation Explorer. – 05.12.2017. – URL: https://www.aex.ru/news/2017/12/5/178623/. (дата обращения 08.08.2022).

2. AVIST: универсальная платформа интеллектуального месторождения [Электронный ресурс] // Нефтегазовая вертикаль. – № 6. – 2016. – URL: http://www.ngv.ru/magazines/article/avist-universalnaya-platforma-intellektualnogo-mestorozhdeniya/news/rfikitaybudu (дата обращения 08.08.2022).

3. Pyrkov, T.V., Slipensky, K., Barg, M., Kondrashin, A., Zhurov, B., Zenin, A., Pyatnitskiy, M., Menshikov, L., Markov, S., Fedichev, P. O. Extracting biological age from biomedical data via deep learning: too much of a good thing? [Электронный ресурс] // Scientific Reports. – Vol. 8. – Article number: 5210.- 2018. – URL: https://www.nature.com/articles/s41598-018-23534-9 (дата обращения 08.08.2022).

4. Академик: запасы нефти в Арктике сравнимы с запасами Западной Сибири [Электронный ресурс] // МИА «Россия сегодня». – 12.10.2015.- URL: https://ria.ru/economy/20151012/1300499673.html (дата обращения 08.08.2022).
5. Алексеев, А., Удалова, Т. Искусственный интеллект для решения логистических задач: опыт «Газпром нефть» [Электронный ресурс] // Сибирская нефть (Управление производством). – 06.02.2018. – URL: http://www.up-pro.ru/library/logistics/transport/multiagentnye-tehnologii.html (дата обращения 08.08.2022).

УДК 681.3
Д.В.Моисеев, доктор технических наук, профессор, А.Г.Шокин, доцент, Е. В. Татурина
Севастопольский государственный университет
ул. Университетская 33, г. Севастополь, Россия, 299053

ОЦЕНКА ВРЕМЕНИ ВОССТАНОВЛЕНИЯ ПРЕОБРАЗУЕМОЙ ВЕЛИЧИНЫ ИЗ ВЕРОЯТНОСТНОГО ОТОБРАЖЕНИЯ

Аннотация
Рассматривается быстродействие вероятностного отображения в сравнении с кодом Рида-Соломона.
Ключевые слова: вероятность, код Рида-Соломона вероятностно представленные данные.
Annotation
The speed of the probabilistic mapping is considered in comparison with the Reed-Solomon code.
Key words: probability, Reed-Solomon code, probabilistically presented data.

В ходе исследования было произведено сравнение времени декодирования (восстановления преобразуемой величины) из кода Рида-Соломона [1] и из вероятностного отображения [2].

Разработана имитационная модель на языке C++, включающая функцию генерации псевдослучайных вспомогательных последовательностей с равномерным законам распределения и вероятностного преобразования с последующим восстановлением [3].

Таблица 1 – Время декодирования из кода Рида-Соломона (мкс)

Кол-во ош	t декод	Кол-во ош	t декод	Кол-во ош	t декод	Кол-во ош	t декод
1	540	33	19859	65	38185	97	56793
2	1048	34	20325	66	38902	98	57205
3	1553	35	21000	67	39398	99	57663
4	2070	36	21477	68	40092	100	58136
5	2604	37	22152	69	40611	101	58609
6	3146	38	22747	70	41267	102	59433
7	3716	39	23277	71	41740	103	60150
8	4332	40	23979	72	42145	104	60349
9	4900	41	24429	73	42633	105	61325
10	5438	42	25047	74	43282	106	61752
11	6067	43	25604	75	44029	107	62164
12	6582	44	25955	76	44685	108	62698

13	7479	45	26817	77	45166	109	63705
14	8778	46	27351	78	45746	110	64285
15	9352	47	27954	79	46234	111	64789
16	9993	48	28320	80	46539	112	65384
17	10521	49	29182	81	47333	113	66010
18	11219	50	29648	82	48096	114	66238
19	11806	51	30159	83	48233	115	67169
20	12341	52	30907	84	49179	116	67612
21	12932	53	31441	85	49896	117	67978
22	13588	54	31944	86	50400	118	68451
23	14095	55	32654	87	50919	119	69443
24	14622	56	33157	88	51636	120	69382
25	15320	57	33760	89	51773	121	70053
26	15846	58	34378	90	52567	122	70969
27	16350	59	34874	91	53436	123	71335
28	17033	60	35408	92	53726	124	72266
29	17570	61	35995	93	54306	125	72083
30	18097	62	36499	94	54825	126	73181
31	18723	63	37064	95	55237	127	73166
32	19260	64	37842	96	56274		

Среднее время декодирования 37530 мкс.

Имитация производилась на системе Intel(R) Core (TM i5-4460) CPU @ 3.20GHz.

Наблюдается линейная зависимость декодирования кода Рида-Сломона от количества ошибок, таблица 1.

При восстановлении из вероятностного отображения зависимости от количества ошибок не наблюдается таблица 2, время в основном зависит от конкретной сгенерированной псевдослучайной последовательности в данный момент. Т.е. одна и та же преобразуемая величина декодируется разное время при разных ПСП.

Таблица 2 – Время декодирования из вероятностного отображения (мкс)

Кол-во ош.	Время декод.	Кол-во ош.	t декод.	Кол-во ош.	t декод	Кол-во ош	t декод
1	9016	33	23722	65	24578	97	18196
2	15423	34	13611	66	14809	98	21875
3	14000	35	14446	67	17253	99	14229

4	15999	36	16625	68	20554	100	16321
5	21154	37	13859	69	14022	101	24194
6	10016	38	15803	70	16030	102	14271
7	17047	39	23642	71	21602	103	20165
8	20265	40	13499	72	10643	104	24630
9	19020	41	13484	73	17223	105	17370
10	23027	42	15277	74	20512	106	20718
11	9099	43	12269	75	12931	107	21529
12	9139	44	13576	76	14504	108	10541
13	16743	45	9155	77	22471	109	12693
14	19840	46	15616	78	11860	110	14170
15	23262	47	11467	79	15080	111	14417
16	12967	48	12454	80	17511	112	16583
17	17876	49	24328	81	13625	113	18697
18	21426	50	14459	82	15474	114	22576
19	19835	51	20327	83	9672	115	16561
20	24168	52	24858	84	9941	116	19585
21	12582	53	21315	85	13769	117	12929
22	14014	54	10240	86	15676	118	14501
23	14746	55	10783	87	16399	119	12306
24	17045	56	11496	88	19359	120	13628
25	15318	57	14902	89	13403	121	18004
26	17845	58	17262	90	15164	122	21605
27	24689	59	14341	91	14384	123	24268
28	14964	60	16478	92	16538	124	14375
29	22126	61	20500	93	23615	125	19294
30	11376	62	9099	94	13460	126	23412
31	14310	63	24649	95	19525	127	11403
32	16433	64	14908	96	23735		

Среднее время декодирования 16642.

Из приведенных результатов тестирования, полученные данные позволяют судить о минимум двукратном превосходстве при декодировании вероятностно представленной величины.

Библиографический список

1. Ничипорук Н. Е., Сай С.В. Оценка корректирующей способности кодов Рида - Соломона при передаче подводных изображений через зашумленный канал связи // Вестник ТОГУ, – Хабаровск, 2011, Вып. 3(22). – С. 29-36

2. Сапожников Н.Е. К вопросу о вероятностном преобразовании информации / Н.Е. Сапожников // Приборостроение., – Севастополь, 1983, Вып. 34, – С. 31-38.
3. Сапожников Н.Е., Моисеев Д.В., Шокин А.Г. Новые методы помехоустойчивого кодирования информации // Восточно-европейский журнал передовых технологий, Информационно-управляющие системы. - 2012 - 6/9 (60). – С. 26-30.

УДК 681.3
Д.В.Моисеев, доктор технических наук, профессор, А.Г.Шокин, доцент
Севастопольский государственный университет
ул. Университетская 33, г. Севастополь, Россия, 299053

ПРИМЕНЕНИЕ ВЕРОЯТНОСТНОГО ПОМЕХОУСТОЙЧИВОГО КОДИРОВАНИЯ В СИСТЕМАХ ПЕРЕДАЧИ ЦИФРОВОЙ ИНФОРМАЦИИ С ОБРАТНОЙ СВЯЗЬЮ

Аннотация
Рассматривается механизмы применения вероятностного помехоустойчивого кодирования в каналах связи с информационной обратной связью.
Ключевые слова: вероятность, вероятностно представленные данные, вероятностное помехоустойчивое кодирование.
Annotation
The mechanisms of application of probabilistic error-correcting coding in communication channels with information feedback are considered.
Key words: probability, probabilistically represented data, probabilistic error-correcting coding.

Использование помехоустойчивого вероятностно кодирования, основанного на вероятностно представленных данных [1], позволяет применять широкий спектр известных и зарекомендовавших себя методов помехоустойчивой передачи данных в существующих цифровых каналах связи.

Одним из вариантов применения стоят отметить системы передачи цифровой информации с решающей обратной связью. В них возможно применение и дифференцированный подход к параметрам передаваемой информации на основе аналитических моделей принятия решений.

Предлагается использовать несколько режимов обработки вероятностно представленного сигнала:

− без помех режим предполагает отсутствие помех в канале связи, направлен на увеличение пропускной способности канала связи

− с помехой предполагает использование корректирующих способностей вероятносто представленных данных, с применением мажоритарного принципа коррекции.

В первом случае увеличение пропускной способности будет достигнуто быстрым решением системы уравнения (1)

$$\begin{cases} \forall \max\{R_j \in (p_{ij} = 1)\} < \min\{R_j \in (p_{ij} = 0)\} \\ a_i = \max\{R_j \in (p_{ij} = 1)\} \end{cases} \quad (1)$$

Принцип, заложенный в системе (1) легко представить в виде графика представленного на рисунке 1. Процесс выборки $max\{\boldsymbol{R_j} \in (\boldsymbol{p_{ij}} = \boldsymbol{1})\}$ (на графике R1max) и $min\{R_j \in (p_{ij} = 0)\}$ (на графике R1min) устанавливает значение восстановленной величины равной 6 и количество статистических испытаний потребовавшихся для восстановления равно 11. Так же понятно, что в случае отсутствия помех целесообразно по каналу обратной связи передать запрос нового значения, это как раз и позволит сократить время обработки передаваемого вероятностно представленного сигнала эмпирическим путем получены показатели, которые позволяют судить об эффективности данного решения, так в ходе испытаний был достигнут прирост эффективности от 5 до 40 раз.

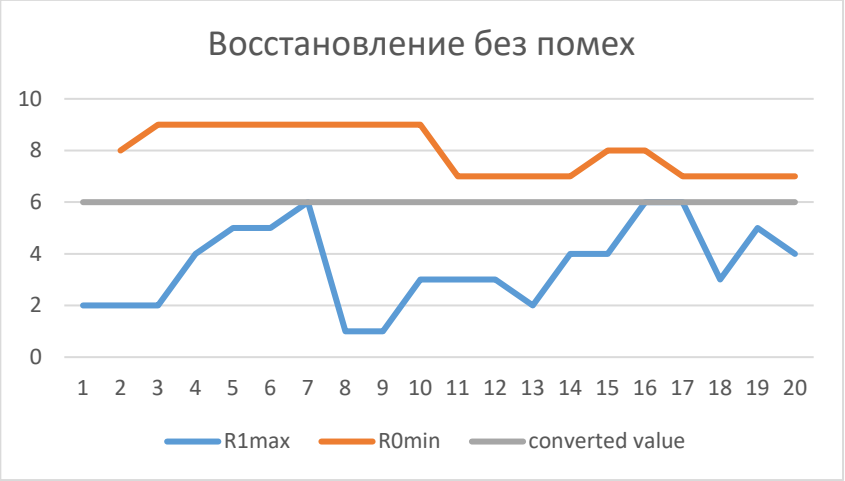


Рисунок 1 – Принцип восстановления преобразуемой величины

Во втором режиме работы наличие ошибки в канале связи будет так же определятся по нарушению первого выражения системы (1), представление данного процесса графически будет выражено пересечением кривых R1max и R1min. Применение данного принципа с мажоритарным принятием решения, когда происходит решение не четного количества блоков поиска решения системы (1) в рамках сеанса передачи,

без дополнительных алгоритмов, позволит на минимальной аппаратной базе решить данную техническую задачу.

В заключении необходимо отметить, что вероятностно представленные данные на ряду с применением помехоустойчивых механизмов позволяют получить качественно новые показатели, как для самого вероятностного представления в части снижения избыточности, так и для классических систем в части использования энергоэффективных платформ.

Библиографический список

1. Моисеев Д.В., Шокин А.Г., Серяк Е.С. Вероятностное кодирование с множественным исправлением ошибок // Автоматизация и измерения в машино- приборостроении. 2021. № 2 (14). С. 51-58.
2. Сапожников Н.Е., Моисеев Д.В., Шокин А.Г. Новые методы помехоустойчивого кодирования информации // Восточно-европейский журнал передовых технологий, Информационно-управляющие системы. - 2012 - 6/9 (60). – С. 26-30.

УДК 519.674
А.А. Поляков[1], кандидат технических наук, заместитель начальника кафедры, Е. В. Татурина, Д.В. Моисеев[2], доктор технических наук, доцент, профессор кафедры
[1] *Черноморское высшее военно-морское училище имени П.С. Нахимова*
[2] *Севастопольский государственный университет*
ул. Университетская 33, г. Севастополь, Россия, 299053

СПОСОБ ПОСТРОЕНИЯ ГАМИЛЬТОНОВОГО ЦИКЛА ПУТЕМ ОБЪЕДИНЕНИЯ ВЕРШИН В ПОДМНОЖЕСТВО В НЕОРИЕНТИРОВАННОМ ПОЛНОСВЯЗАННОМ СИММЕТРИЧНОМ ВЗВЕШЕННОМ ГРАФЕ

Аннотация
В статье поднимается вопрос о способе построения гамильтонового цикла путем объединения подмножеств и вершин в неориентированном полносвязанном симметричном взвешенном графе.
Ключевые слова: задача коммивояжёра, алгоритм Прима, алгоритмизация, неориентированные графы, поиск наикратчайшего пути в графе, поиск остова минимального веса.
Annotation
The article raises the question of how to construct a Hamiltonian cycle by combining subsets and vertices in an undirected fully connected symmetric weighted graph.
Keywords: traveling salesman problem, Prim algorithm, algorithmization, undirected graphs, shortest path search in a graph, minimum weight skeleton search.

Задача коммивояжера относится к классу NP-трудных задач, ее точное решение может быть получено за экспоненциальное время, решать задачу коммивояжера при большом числе вершин алгоритмом полного перебора не эффективно. В связи с этим, проводились и будут проводится исследования в поиске способа, который бы удовлетворял исследователя по времени и точности вычисления.

Предлагаемый способ относится к классу «жадных» алгоритмов и может быть применён для построения минимального гамильтонового цикла в неориентированном полносвязанном взвешенном конечном графе при включении его в специализированные программные продукты или программно-аппаратные комплексы. Наиболее близким к предлагаемому способу является способ, известный как «Алгоритм Прима».

Технический результат достигается за счёт того, что проводится неполная неубывающая сортировка взвешенных рёбер, с целью определения вершин, которые связаны минимальным весом, выбирается одно парасочетание и объединяется в одно подмножество. Подмножество имеет левую и правую границу, соединенную с другими вершинами по весу исходящих рёбер присоединенных вершин. Исходящие рёбра с наибольшими весами, расположенные на правой и левой границе подмножества и инцидентные другим вершинам графа, поочередно поглощаются исходящими ребрами с наименьшими весами, которые так же инцидентны этим же вершинам графа. Осуществляется присоединение вершин в подмножество по инцидентным ребрам с минимальным весом. Инцидентные ребра вершин, расположенные между левой и правой границей подмножества, исключаются. Объединение вершин в подмножество продолжается пока все вершины графа не будут включены в одно подмножество. Закольцовывается правая и левая граница подмножества между собой.

Построение взвешенного минимального гамильтонового цикла осуществляется с построения неориентированного полносвязанного симметричного взвешенного конечного графа $G = (V, E)$, матрицы весов $M[V][V]$, где V - это число вершин в графе G, а E - число неориентированных взвешенных симметричных ребер в графе G, Рис. 2 а. Для каждого ребра (V_i, V_j) графа задан вес $w(V_i, V_j)$, вес симметричен $w(V_j, V_i)$. Промежуточным этапом при построении гамильтонового цикла является построение минимального полугамильтоного пути, который состоит в нахождении подмножества $T \subset E$, связующего все вершины, для которых суммарный вес минимальный, при условии, что каждая вершина посещается один раз.

$$w(T) = \min \sum_{(i,j) \in T} w(V_i, V_j).$$

На основании графической части графа строиться матрица весов $M[V][V]$ Рис. 2 б, задается одномерный массив $S[E]$ Рис. 3 а, в $S[E]$ проводится неполная сортировка ребер E.

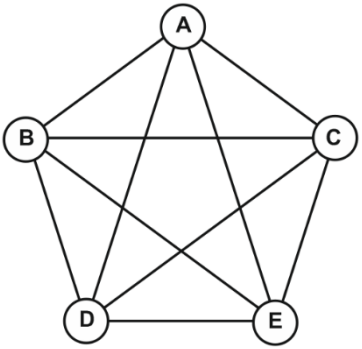


Рисунок 2 а

	A	B	C	D	E
A		1	1	2	2
B			2	1	2
C				2	1
D					1
E					

Рисунок 2 б

Пусть E_i ребро минимального веса в графе G, вершины связанные между собой минимальным весом перемещаются в начало массива $S[E]$, сортировка прекращается Рис. 3 б.

A-B	A-C	A-D	A-E	B-C	B-D	B-E	C-D	C-E	D-E
B-A	C-A	D-A	E-A	C-B	D-B	E-B	D-C	E-C	E-D
1	1	2	2	2	1	1	2	1	1

Рисунок 3 а

A-B	A-C	B-D	B-E	C-E	D-E	A-D	A-E	B-C	C-D
B-A	C-A	D-B	E-B	E-C	E-D	D-A	E-A	C-B	D-C
1	1	1	1	1	1	2	2	2	2

Рисунок 3 б

Осуществляется обход матрицы весов ребер $M[V][V]$, проводится объединение вершин в подмножество по минимальному весу инцидентного ребра, Рис. 4 а - Рис. 4 б.

	A	B	C	D	E
A		1	1	2	2
B			2	1	2
C				2	1
D					1
E					

Рисунок 4 а

	A	B	C	D	E
A	L(AB)=1		1	2	2
B			2	1	2
C				2	1
D					1
E					

Рисунок 4 б

Проводится проверка построен ли полугамильтонов путь, если нет, то продолжается объединение вершин в подмножество. Пусть существует подмножество $V_i, V_f, \cdots, V_z, V_j$ на основании проведенной процедуры, где V_i - является левой l границей подмножества, V_j - является правой r границей подмножества, проводится попарное поглощение на границах r и l подмножеств инцидентных рёбер с наибольшим весом, Рис. 5 а. - Рис. 5 б.

	A	B	C	D	E
A	L(AB)=1		1	2	2
B			2	1	2
C				2	1
D					1
E					

Рисунок 5 а

	A	B	C	D	E
A	L(AB)=1		1		2
B				1	2
C				2	1
D					1
E					

Рисунок 5 б

Далее проводится исключение инцидентных рёбер вершин, расположенных между левой l и r правой границей подмножества, Рис. 6 а., данная операция позволяет исключить дальнейшее появление циклов при соединении вершин к подмножеству. Объединение вершин продолжается, пока все вершины графа не будут включены в одно подмножество - полугамильтонов путь Рис. 6 а. - Рис. 6 г. Для построения минимального гамильтонового цикла проводится закольцовывание правой r и l левой граница подмножества между собой, гамильтонов цикл

построен. Закольцовывание проводится по инцидентной связи между вершинами правой r и l левой границы подмножества представленной в массиве $S[E]$.

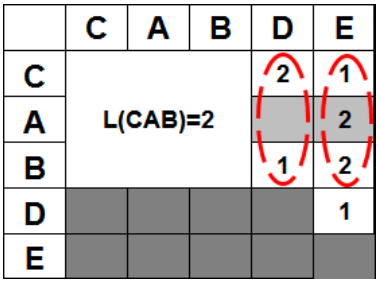


Рисунок 6 а

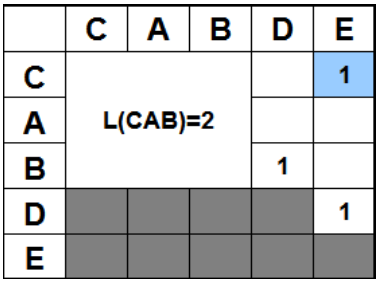


Рисунок 6 б

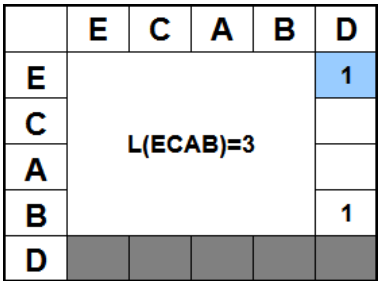


Рисунок 6 в

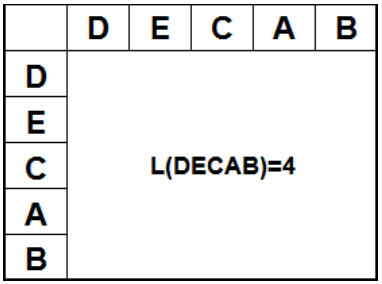


Рисунок 6 г

Время работы предлагаемого способа построения минимального взвешенного гамильтонового цикла путём объединения вершин в подмножество в неориентированном полносвязанном симметричном взвешенном графе составляет:

$$O(E \lg V).$$

Таким образом, результатом работы способа является построенный минимальный гамильтонов цикл на основе неориентированного полносвязанного симметричного взвешенного конечного графа.

Технико-экономическая эффективность предлагаемого способа заключается в повышении быстродействия при построении минимального взвешенного гамильтонового цикла путём объединения вершин в подмножество в неориентированном полносвязанном симметричном взвешенном конечном графе, с допустимой точностью свойственной «жадным» алгоритмам.

Библиографический список

1. Поляков А. А., Моисеев Д. В. Комплекс методик декомпозиции структурно-сложных систем различного назначения. //Wschodnioeuropejskie Czasopismo Naukowe (East European Scientific Journal) Warsaw, Poland.: «Jerozolimskie», № 7(47), 2019 г. – С. 66 – 70.

2. Поляков А. А., Моисеев Д. В. Методика полной декомпозиции структуры технической системы. //Сборник научных трудов «Национальная ассоциация ученых» Екатеринбург: 620144, № 45, 2019 г. – С. 28 – 31.

УДК. 004.89
А.В. Скатков, д-р техн. наук, профессор, Д.В. Моисеев, д-р техн. наук, доцент, А.А. Брюховецкий, к-т техн. наук, заведующий кафедрой
ФГАОУ ВО "Севастопольский государственный университет", г. Севастополь, Россиия

АДАПТАЦИЯ МЕХАНИЗМОВ ИСКУССТВЕННЫХ ИММУННЫХ СИСТЕМ ДЛЯ КОАЛИЦИОННОГО ПРОТИВОСТОЯНИЯ УГРОЗАМ ВТОРЖЕНИЯ НА БТС

Аннотация
В настоящей работе продолжены исследования авторов, посвящённые адаптации механизмов искусственных иммунных систем путём модификации классических математических моделей в соответствии со спецификой искусственных иммунных систем, что позволило значительно повысить их эффективность для противостояния угрозам вторжения на беспилотные транспортные средства. В работе предложены модели кооперативного взаимодействия нескольких автономных инфо-телекоммуникационных систем, защита которых, построены на базе искусственных иммунных систем.

Abstract
In this paper, the authors continue their research on the adaptation of the mechanisms of artificial immune systems by modifying classical mathematical models in accordance with the specifics of artificial immune systems, which significantly increased their effectiveness to counter the threats of invasion of bi-pilot vehicles. The paper proposes models of cooperative interaction of several autonomous infotelecommunication systems, the protection of which is built on the basis of artificial immune systems.

Введение. Обобщая и развивая существующие направления исследований биоинспирированных методов, нами предлагается их следующая классификация (см. рис. 1) [1].

Одним из актуальных классов биоинспирированных алгоритмов в современных исследованиях являются иммунные системы. Методы иммунных систем ориентированные на решение задачи глобальной оптимизации, основаны на некоторых аспектах поведения иммунной системы человека в процессе защиты ею организма. Защитные клетки иммунной системы (антитела) претерпевают при этом множество изменений, целью которых является создание клеток, обеспечивающих наилучшую защиту. искусственные иммунные системы (ИИС) обладает основными свойствами искусственного интеллекта: памятью, способностью к обучению и принятию решений в незнакомой ситуации [2-4].

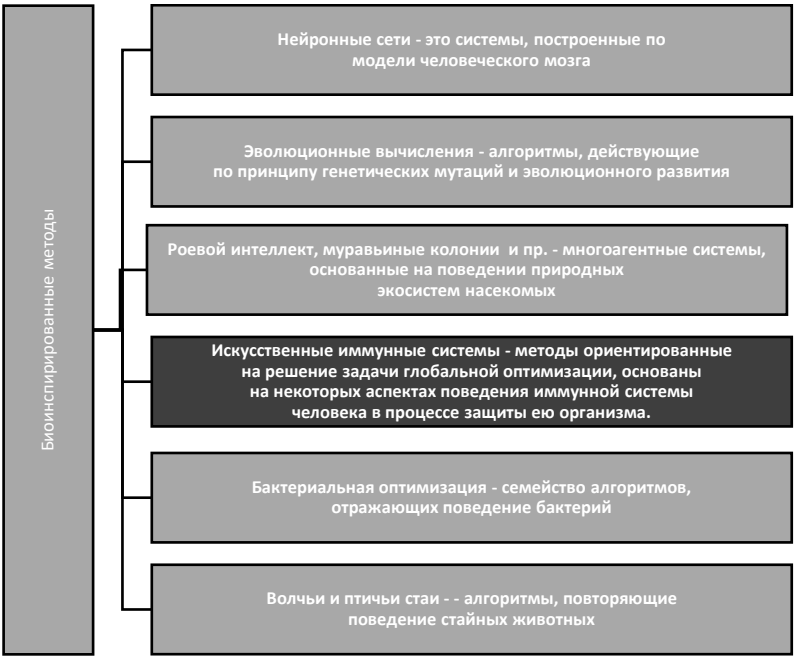


Рисунок 1 – Классификация биоинспирированных методов

Рассмотрим вопросы адаптации механизмов искусственный иммунных систем для противостояния угрозам вторжения на беспилотные транспортные средства (БТС).

Целью данной работы является адаптация механизмов искусственных иммунных систем для коалиционного противостояния угрозам вторжения на БТС.

Изложение основного материала. В соответствии с изложенными фактами и представлениями о динамике иммунного ответа выделим следующие переменные модели, которые являются непрерывными функциями [1-2]:

$V = V(t)$ – мощность деструктивного воздействия вирусов;

$C = C(t)$ – относительный размер антивирусной базы;

$F = F(t)$ – вычислительная сложность антивирусных алгоритмов;

$m = m(t)$ – доля поражённого вирусов ресурса.

Математическая модель адаптированной иммунной реакции на вторжение, в соответствии с [1-2, 5-8], строится на основе соотношений баланса для каждой из зависимых переменных в предположении, что

«организм» описывается однородным замкнутым объемом, в котором все компоненты процесса равномерно перемешаны:

$$\begin{gathered}\frac{dV}{dt} = \beta V - \gamma FV,\\ \frac{dF}{dt} = \rho C - \eta\gamma FV - \mu_f F,\\ \frac{dC}{dt} = \alpha F(t-\tau)V(t-\tau) - \mu_c(C - C"),\\ \frac{dm}{dt} = \sigma V - \mu_m m,\end{gathered} \quad (1)$$

с начальными условиями:

$$V(0) = V^0, F(0) = F^0,$$
$$C(0) = C^0, m(0) = m^0$$

и фазовыми ограничениями:

$$V(t) \geq 0.0, F(t) \geq 0.0,$$
$$C(t) \geq 0.0, m(t) \geq 0.0,$$

где

$\beta > 0$ – скорость размножения вирусов; $\gamma > 0$ – коэффициент, учитывающий вероятность определения вируса антивирусом; $\alpha > 0$ – коэффициент стимуляции иммунной системы; $\rho > 0$ – скорость антивирусного алгоритма; $\mu_c > 0$ – величина, обратная продолжительности жизни специфического алгоритма; $\mu_f > 0$ – величина, обратная продолжительности антивирусного алгоритма; $\eta > 0$ – количество операций, необходимое для нейтрализации одного вируса; $\sigma > 0$ – скорость (темп) поражения ресурса; $\mu_m > 0$ – скорость восстановления ресурса; $C" > 0$ – предсуществующий размер антивирусной базы; $\tau > 0$ – время, необходимое для формирования каскада специфических антивирусных алгоритмов.

В рассматриваемом иммунном ответе участвуют вирусы $V(t)$, антивирусные алгоритмы $F(t)$, антивирусная база $C(t)$ и атакуемый (повреждаемый) ресурс $m(t)$.

Проведено исследование поведения модели иммунного ответа ИИС при различных наборах начальных условий (результаты моделирования представлены на рис. 2).

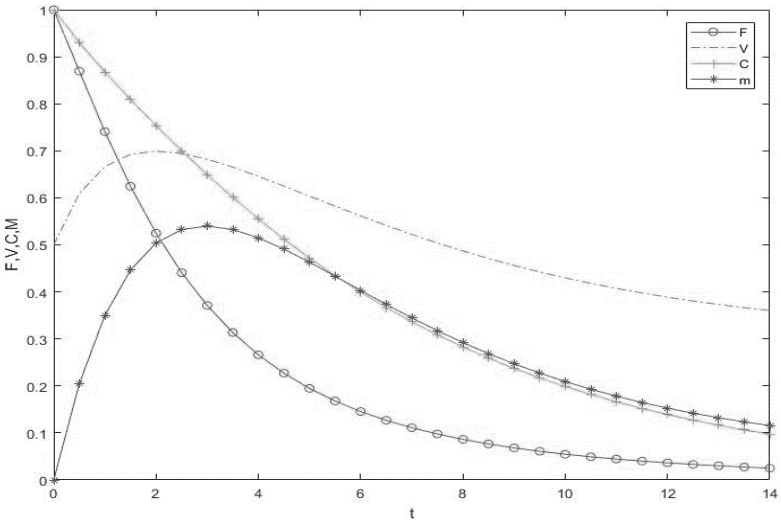


Рисунок 2 – Результаты моделирования иммунного ответа ИИС при начальных условиях $V(0) = 1.0, F(0) = 0.5, C(0) = 1.0, m(0) = 0.0$

Зависимости, приведённые на рис. 2, характеризуют иммунный ответ ИИС на воздействие вируса в соответствии с выражением (1) при начальных условиях: относительная концентрация вируса – 1.0, относительное количество антивирусных клеток – 0.5, относительный объём антиген-специфических клеток – 1.0, и поражаемый орган полностью здоров.

Следует отметить, что выражение (1) описывает идеализированное поведение заражаемого организма, в котором не учитывается невозможность при определённом уровне поражения органа (ресурса) выполнять иммунный ответ. Для моделирования ситуации работы иммунной системы вследствие значительного поражения органа (ресурса) введём следующую переменную:

ξ(m) — невозрастающая неотрицательная функция, учитывающая нарушение нормальной работы иммунной системы вследствие значительного поражения органа (ресурса):

$$(m) = \begin{cases} 1, 0 \le m \le m', \\ (1-m)k, m' \le m \le 1, \end{cases} \quad (2)$$

где $m' > 0$ — предельный уровень поражения, при котором ещё возможна нормальная работа иммунной системы

k — коэффициент предельного уровня поражения.

Тогда выражение (1) примет вид:

$$\begin{gathered}\frac{dV}{dt} = \beta V - \gamma FV,\\ \frac{dF}{dt} = \rho C - \eta\gamma FV - \mu_f F,\\ \frac{dC}{dt} = \xi(m)\alpha F(t-\tau)V(t-\tau) - \mu_c(C - C''),\\ \frac{dm}{dt} = \sigma V - \mu_m m,\end{gathered} \tag{3}$$

Таким образом, впервые для корректного описания механизмов ИИС для БТС авторами предлагается рассматривать поражения ресурсов БТС вирусами как мультипликативную функцию.

Следует отметить, что предложенная авторами [1 - 2] модификация математической модели циклического иммунного ответа ИИС на внешнее вторжение, с учётом накопления антивирусной базы с опережением $C^*(t)$ приносит положительный эффект в скорости уменьшения объёмов накопленных вирусов $V^*(t)$ и повышению эффективности антивирусных алгоритмов $F^*(t)$, соответственно появляется потенциальная возможность, в случае коалиционной работы нескольких ИИС, передать ресурсы одной ИИС, которая в настоящий момент не испытывает враждебных атак, другой ИИС, которая в настоящий момент противостоит атаке.

Авторы рассматривают три возможных сценария кооперативного взаимодействия двух ИИС, с учётом вышеописанного сценария:

1. ИИС, неподверженная атаке передаёт второй ИИС в распоряжение свою, превентивно наращённую $C_1^*(t)$.

2. ИИС, неподверженная атаке передаёт второй ИИС в распоряжение не только свою, превентивно наращённую C1*(t), но и целиком свои антивирусные базы

3. Возможно совместное использование антивирусными базами как первой, так и второй ИИС.

Выводы. Анализ полученных результатов позволяет сделать вывод: модификация классических математических моделей в соответствии со спецификой ИИС значительно повысила их эффективность, что позволяет использовать методы ИИС для обнаружения уязвимостей интерфейсов БТС. Также авторами предлагается коалиционное использование антивирусных базам несколькими ИИС, которое приводит к значительному повышению эффективности иммунного ответа. Модификации математических моделей иммунного ответа ИИС на внешнее вторжение, с учётом накопления антивирусной базы с опережением $C^*(t)$ приносит положительный эффект в скорости уменьшения объёмов накопленных вирусов $V^*(t)$ и повышению эффективности антивирусных алгоритмов $F^*(t)$.

Работа выполнена при частичной поддержке Российского фонда фундаментальных исследований (гранты № 19-29-06015/21 и № 19-29-06023/21)

Список использованных источников

1. Адаптивное обнаружение уязвимостей интерфейсов беспилотных транспортных средств / А. В. Скатков, А. А. Брюховецкий, Ю. В. Доронина [и др.]. – Симферополь: Общество с ограниченной ответственностью «Издательство Типография «Ариал», 2020. – 352 с. – ISBN 978-5-907310-87-2.

2. Скатков, А. В. Адаптация механизмов искусственных иммунных систем для контроля параметров окружающей среды / А. В. Скатков, А. А. Брюховецкий, Д. В. Моисеев // Системы контроля окружающей среды. – 2020. – № 2(40). – С. 127-133. – DOI 10.33075/2220-5861-2020-2-127-133.

3. Станкевич Л.А., Казанский А.Б. Иммунологическая система обеспечения безопасности гуманоидного робота // Актуальные проблемы защиты и безопасности: тр. 9-й Всерос. науч.-практич. конф. 2006. № 5. С. 145-152.

4. Garrett S.M. How do we evaluate artificial immune systems? How do we evaluate artificial immune systems? 2005, vol. 13, pp. 145-178.

5. Skatkov A V, Bryukhovetskiy A A and Moiseev D V 2020 Adaptive vulnerability detection model for unmanned vehicles drugs based on artificial immune systems IOP Conference Series: Materials Science and Engineering 734 012028 DOI: iopscience.iop.org/article/10.1088/1757-899X/734/1/012028

6. Model for vulnerabilities detection in unmanned vehicle interfaces based on artificial immune systems IOP Publishing Ltd Journal of Physics: Conference Series 1515 022043 DOI: https://doi.org/10.1088/1742-6596/1515/2/022043

7. Математические модели в иммунологии. Вычислительные методы и эксперименты / ред. Г.И. Марчук. М.: Наука, 1991. 299 с.

8. Математические модели в иммунологии и медицине / ред. Г.И. Марчук. М.: Мир, 1986. 150 с.

УДК 681.3

А.В. Скатков, д-р техн. наук, профессор, Д.В. Моисеев, д-р техн. наук, доцент, А.А. Брюховецкий, к-т техн. наук, заведующий кафедрой

ФГАОУ ВО "Севастопольский государственный университет", г. Севастополь, Россиия

ВЫБОР СТРАТЕГИИ КОЛЛАБОРАЦИИ ПРИ АНАЛИЗЕ СОСТОЯНИЙ ИНТЕРФЕЙСОВ РОЯ БТС В УСЛОВИЯХ СЕТЕЙ 5G

Аннотация

Характеристики высокой мобильности и быстрого изменения топологии интеллектуальных транспортных автомобильных сетей в условиях гетерогенных технологий связи 5G делают их уязвимыми для различных вредоносных внешних воздействий. Злоумышленник используя нестабильность линии связи, вызванную частыми изменениями структуры топологии, получает возможность для снижения надежности и своевременности автомобильной связи, что создает серьезные угрозы безопасности. В работе предлагается подход обнаружения уязвимостей интерфейсов БТС на основе динамической оценки поведения роя БТС, учитывая строгое ограничение задержки и высокие требования к надежности передачи информации между транспортными средствами.

Abstract

The characteristics of high mobility and rapid changes in the topology of intelligent transport automobile networks in the conditions of heterogeneous 5G communication technologies make them vulnerable to various harmful external influences. An attacker using the instability of the communication line caused by frequent changes in the topology structure gets the opportunity to reduce the reliability and timeliness of automobile communication, which creates serious security threats. The paper proposes an approach to detecting vehicular interfaces vulnerabilities based on a dynamic assessment of the behavior of a vehicular swarm, taking into account the strict limitation of latency and high requirements for the reliability of information transmission between vehicles.

Введение. 5G является ключевой технологией, способствующей достижению высокой скорости передачи данных / расширенной широкополосной мобильной связи (eMBB), сверхнадежной связи с низкой задержкой (URLLC) и массовой связи машинного типа (mMTC) для расширения устаревшей сети передачи данных. Гетерогенные сети с поддержкой 5G (HetNets) необходимы для современной связи для несколь-

ких одновременно работающих приложений, меняющих правила взаимодействия, таких как интернет вещей (IoT), связь между устройствами (D2D) и связь между машинами (M2M). Эти приложения обладают огромным потенциалом, способным оказать значительное влияние на социально-экономические слои современного мира. Тем не менее, неоднородность в нескольких областях технологий для развертывания таких систем на базе 5G рассматривается как возможность, сопряженная с проблемами. В частности, интеллектуальные транспортные автомобильные сети считаются основной системой для развертывания приложений на ее основе, которые способствуют повышению качества вождения, стремятся обеспечить безопасность движения на дорогах, информируют водителей об опасностях и выбора оптимального маршрута и т.д. [1]. При этом мобильная транспортная сеть обладает рядом специфических особенностей:

- неоднородность различных приложений и системной архитектуры (рис.1),
- высокодинамичная топология из-за высокой скорости движения транспортных средств,
- низкая доступность канала и ограниченный диапазон передачи приводят к частому отключению каналов связи.

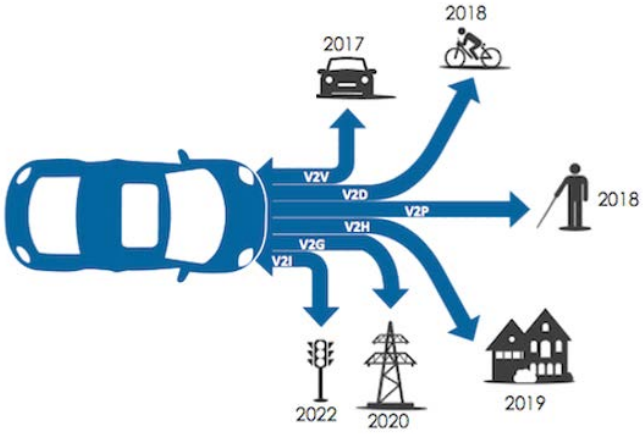


Рисунок – 1. Автомобиль через сеть взаимодействует с окружающей средой и объектами, поэтому в нем выделяют несколько систем: автомобиль-автомобиль (vehicle-to-vehicle, V2V), автомобиль - инфраструктура (vehicle-to-infrastructure, V2X) , автомобиль-пешеход (vehicle-to-pedestrian, V2P), автомобиль - электросеть (vehicle-to-grid, V2G) и автомобиль - устройство (vehicle-to-device, V2D).

Подключенные транспортные средства к интеллектуальной сети обмениваются информацией с другими транспортными средствами (V2V) и транспортной инфраструктурой (V2I) с помощью беспроводной связи, что повышает безопасность дорожного движения, обеспечивает эффективные услуги мобильности и снижает воздействие на окружающую среду [2]. Однако риск внешних воздействий возрастает по мере того, как транспортные средства становятся все более подключенными через интернет и беспроводные сети. Одним из шлюзов для кибератак на подключенные транспортные средства является V2I. Кибератаки на связь V2I могут иметь разрушительные последствия, если системы V2I не защищены должным образом. Приложения V2I содержат множество уязвимостей, которые создают привлекательную мишень для хакеров.

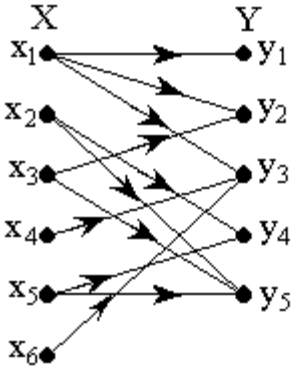
Известны решения обеспечивающие улучшения взаимодействия между транспортными средствами. Так, например, в [3] предложена структура системы обнаружения вторжений, основанная на теории игр. В [4] рассматриваются алгоритмы управления поведением роботов. В [5] предлагаются алгоритмы обнаружения вторжений, которые принимают входные данные в виде ряда характеристик движения транспортного средства. В других публикациях представлен обзор приложений, архитектур, протоколов и проблем, связанных с коммуникацией в транспортных интеллектуальных сетях [6,7,8]. Однако быстро меняющиеся модели поведения при атаках в сетях 5G являются многоструктурными, многопараметрическими и многодоменными, так что традиционные технологии обнаружения вторжений не могут эффективно идентифицировать их поведение.

Многие из рассматриваемых приложений связаны с безопасностью V2I (например, предупреждение о превышении скорости на повороте, указатели в автомобиле и система помощи при прохождении знака остановки) [9]. Все эти приложения имеют некоторые общие подприложения (например, предупреждения о превышении скорости, безопасность на перекрестках) и используют общие процессы (например, сбор данных о безопасности на дорогах и обработка собранных данных о безопасности транспортных средств) для поддержки этого прикладного уровня. По этой причине потоки данных могут представлять угрозу безопасности при совместном использовании между этими приложениями. Таким образом, если риск кибербезопасности присутствует в какомлибо из совместно используемых вложенных приложений или процессов, другие приложения могут быть подвержены риску.

Целью является разработка подхода обнаружения уязвимостей интерфейсов БТС на основе исследования динамических свойств коллабораций транспортных средств. В качестве реализации предлагается графовая модель, учитывающая заданные свойства транспортных средств.

Изложение основного материала. Транспортные средства (ТС) оснащены бортовыми устройствами, устройством беспроводной связи, системой глобального позиционирования, записью данных о событиях и различными датчиками. Транспортные средства взаимодействуют друг с другом, обмениваются контекстной информацией между собой и базовой станцией, которая отвечает за сбор и распространение информации о характеристках движения транспортных средств. Для определения состояний движения транспортных средств и повышения безопасности сетевого трафика требуется точная передача информации о потоке трафика в режиме реального времени. Тем не менее, высокая мобильность транспортных средств и частые изменения топологии сети увеличивают задержку и ненадежность передачи такой информации. Кроме того, из-за ограничений скорости движения на городских дорогах, сигналов светофоров транспортные средства обычно движутся группами. В связи с этим предлагается использовать обобщенные характеристик коллабораций транспортных средств, которые будут формироваться в соответствии с заданными характеристиками, такими, например, как: местоположение ТС, местоположение базовой станции, скорость ТС, время попадания ТС в зону действия базовой станции, время когда ТС покидает базовую станцию, количество ТС в пределах достижимости i-ого ТС, количество ТС в пределах диапазона связи базовой станции, скорость приема / передачи данных i-ым ТС, мощность принимаего сигнала i-ым ТС и другие.

Задача формирования коллабораций в терминах теории графов формулируется так. Задано множество ТС. Связь между вершинами в каждый временной интервал $\Delta t = t_i - t_{i-1}$ показана на рисунке 2 в виде матрицы смежности M(X,Y), в которой строкам соответствуют вершины типа Xi , столбцам – вершины типа Yj, i=1,m; j=1,k.



	y_1	y_2	y_3	y_4	y_5
x_1	**1**	1	1	0	0
x_2	0	0	0	**1**	1
x_3	0	**1**	0	0	1
x_4	0	0	**1**	0	0
x_5	0	0	0	**1**	**1**
x_6	0	0	**1**	0	0

f

a) b)

Рисунок – 2. a) Двудольный граф b) Матрица смежности

В свою очередь матрица представляется двудольным графом G = (V, E), где V – множество вершин, E – множество дуг. V содержит два типа вершин: индукторы – Xi и коллекторы – Yj. При этом $V = X \cup Y$, где $X \cap Y = \emptyset$, и никакая дуга не соединяет две вершины из одной доли. Каждой дуге графа приписан вес (стоимость) Ci,j.

Задано множество A = {a1,…ah,….ar} жадных алгоритмов построения минимального покрытия, которые отличаются целевой функцией Fh и критерием выбора очередного набора вершин на каждой итерации алгоритма, который максимизирует, например, отношение количества непокрытых элементов к их стоимости, пока все элементы не будут покрыты.

Первоначально алгоритм построения минимального покрытия выбирается случайным образом и формируется интегральная оценка стоимости множества наборов вершин, входящих в покрытие. На первом шаге каждому алгоритму присвается оценка ph=1/r , (h=1,r) – вероятность выбора алгоритма для построения очередного множества покрытия. На каждом очередном i-ом шаге алгоритм сравнивает текущую стоимость покрытия ci > ch, i<>h , h=1,r. Соответственно, если условие выполняется, то выбор i-ого алгоритма поощряется на величину $+\Delta p$, а остальных алгоритмов – уменьшается на величину $-\Delta p/(r-1)$. Время, которое отводится на принятие решения по выбору наилучшего покрытия ограничивается Δt, обеспечивающее безопасность движения транспортных средств.

Выводы. В работе предлагается подход обнаружения уязвимостей интерфейсов БТС на основе динамической оценки поведения роя БТС в условиях сетей 5G. Рассмотрена графовая модель, учитывающая заданные свойства транспортных средств и стохастический характер среды.

Исследование выполнено при финансовой поддержке РФФИ в рамках научных проектов № 19-29- 06015 , № 19-29-06023.

Список использованных источников

1. J. Hoebeke, I. Moerman, B. Dhoed , P. Demeester. An overview of mobile ad hoc networks: applications and challenges, J. Commun. Netw. 3 (1) (2004) 60-66 .

2. Jie Ji. ew Architecture, New Challenges: Service Security Issues in the 5G Core Network and How to Detect Them// URL: https://nsfocusglobal.com/new-architecture-new-challenges-service-security-issues-in-the-5g-core-network-and-how-to-detect-them/5g/ September 24, 2021.

3. B. Subba, S. Biswas, S. Karmakar A game theory based multi layered intrusion detection framework for VANET Future Generat. Comput. Syst., 82 (2018), pp. 12-28

4. Каляев И.А, Капустян С. Г., Гайдук А. Р. Самоорганизующиеся распределенные системы управления группами интеллектуальных роботов, построенные на основе сетевой модели // Управление большими системами, 30.1 (2010), с. 605–639.

5. M.Waniek, G.R.Raman. Traffic networks are vulnerable to disinformation attacks// Scientific Reports 11(1):5329 , March 2021.

6. Адаптивное обнаружение уязвимостей интерфейсов беспилотных транспортных средств. Скатков А.В., Брюховецкий А.А., Моисеев Д.В. и др. // Издательство «Ариал» (Симферополь), 2020. - 352 с.

7. Zhaojun, L., Gang, Q. & Liu, Z. A survey on recent advances in vehicular network security, trust, and privacy. *IEEE Trans. Intell.Transport. Syst.* **20**(2), 760–776 (2018).

8. Ahmed, A., A. Ahmed, and E. Ahmed. A Survey on Mobile Edge Computing A Survey on Mobile Edge Computing. No. January, 2016. https://doi.org/10.13140/RG.2.1.3254.7925.

9. Delgrossi, L., and T. Zhang. Connected vehicles and cybersecurity. *Usdot*, 2012, pp. 32–43.

ИТ В ОБРАЗОВАНИИ, ПОДГОТОВКА И ПЕРЕПОДГОТОВКА ИТ-СПЕЦИАЛИСТОВ

УДК 004.056.53
М.Х. Аль-Барри, И.Б. Саенко, д-р техн. наук, профессор
Военная академия связи
Тихорецкий пр. 3, г. Санкт-Петербург, Россия, 194064
e-mail: ibsaen@mail.ru

О ПОСТРОЕНИИ ПРИЗНАКОВОГО ПРОСТРАНСТВА ДЛЯ ОБНАРУЖЕНИЯ АНОМАЛЬНЫХ SQL-ЗАПРОСОВ МЕТОДАМИ МАШИННОГО ОБУЧЕНИЯ

Аннотация
Рассматривается модель признакового пространства, которое используется в задаче обнаружения аномальных SQL-запросов методами машинного обучения. Обсуждается структура признакового пространства и подход к его оптимизации. Приводятся результаты экспериментальной оценки эффективности обнаружения аномальных запросов с использованием оптимизированного признакового пространства.
Ключевые слова: признаковое пространство, база данных, запрос, аномалия, машинное обучение, метод.

M. Al-Barri, I. Saenko
Military Telecommunication Academy
Tikhoretsky av. 3, Saint-Petersburg, Russia, 194064
e-mail: ibsaen@mail.ru

ON THE CONSTRUCTION OF FEATURE SPACE FOR DETECTING ABNORMAL SQL-QUERIES BY MACHINE LEARNING METHODS

Abstract
The paper considers the model of feature space, which is used in the task of anomalous SQL-queries detection by machine learning methods. The structure of the feature space and the approach to its optimization are discussed. The results of experimental efficiency evaluation of abnormal queries detection using optimized feature space are given.
Keywords: feature space, database, query, anomaly, machine learning, method.

Проводимое исследование преследует две цели. Во-первых, оценивается возможность использования методов машинного обучения для

обнаружения аномальных SQL-запросов [1]. Во-вторых, исследуется возможность оптимизации признакового пространства, используемого в методах машинного обучения, в целях повышения эффективности обнаружения аномальных SQL-запросов [2].

Наборы данных были взяты из регистрационных журналов СУБД. Первоначальное признаковое пространство было сформировано из трех групп признаков. Первая группа была образована из количеств вхождения в SQL-запрос ключевых слов языка SQL. С помощью значений этих признаков можно определить уровень сложности SQL-запроса и его тип. Вторая группа признаков включала в себя количества вхождений в запрос специальных конструкций, свойственных SQL-инъекциям. Третья группа признаков была образована количествами вхождения различных имен таблиц данных в SQL-запросы. С помощью этой группы признаков можно обнаруживать аномальные SQL-запросы, в которых пользователи предпринимают попытки несанкционированного доступа.

Реализация моделей машинного обучения была сделана в системе Orange 3.32. Эксперименты на полном признаковом пространстве проводились для следующих моделей машинного обучения: SVM, DT, LR, KNN, RF, BN, ANN. Все классификаторы показали точность, превышающую 0,92.

Оптимизация признакового пространства проводилась на основе оценки информативности признаков. Использовались следующие метрики: Info.Gain, Gain ratio, ANOVA, а также нормированное среднее значение этих метрик. Была проведена серия экспериментов по оценке точности обнаружения аномальных запросов за счет сокращения количества признаков. Критерий сокращения был следующим: остаются те признаки, метрика которых превышает среднее значение этой метрики. Эксперименты подтвердили эффективность предложенного подхода. Точность обнаружения аномальных SQL-запросов возросла с 0,92 до 0,98.

Таким образом, полученные результаты подтверждают возможность успешного использования методов машинного обучения для обнаружения SQL-запросов и правомерность предложенного подхода к сокращению используемого этими методами признакового пространства. Программная реализация этого подхода и внедрение ее в систему защиты базы данных является дальнейшим направлением исследований.

Библиографический список

1. Mousa A. Database Security Threats and Challenges / A. Mousa, M. Karabatak, T. Mustafa // 2020 8th International Symposium on Digital Forensics and Security (ISDFS). – 2020. – Pp. 1-5.

2. Ageev S. Abnormal traffic detection in networks of the internet of things based on fuzzy logical inference / S. Ageev, Y. Kopchak, I. Kotenko, I. Saenko // 2015 XVIII International Conference on Soft Computing and Measurements (SCM). – 2015. – Pp. 5-8.

УДК 004.946
О.В. Батенькина, кандидат технических наук, доцент
Федеральное государственное автономное образовательное учреждение высшего образования «Омский государственный технический университет»

ВОПРОСЫ РАЗРАБОТКИ ОБУЧАЮЩИХ ВИРТУАЛЬНЫХ ТРЕНАЖЕРОВ ДЛЯ ПРОФЕССИОНАЛЬНОЙ ПОДГОТОВКИ СПЕЦИАЛИСТОВ

Аннотация
В данной статье рассмотрены вопросы эффективной разработки обучающих тренажеров с использованием технологий виртуальной реальности и их влияние на психофизиологические характеристики пользователя во время прохождения обучения. Представлены проблемы изучения влияния технологии виртуальной реальности на когнитивные процессы формирования профессиональных знаний и умений.
Ключевые слова: виртуальная реальность, когнитивные процессы, обучение, психофизиологические характеристики.
Abstract
This article discusses the issues of effective development of training simulators using virtual reality technologies and their impact on the user's psychophysiological characteristics during training. The problems of studying the influence of virtual reality technology on the cognitive processes of the formation of professional knowledge and skills are presented.
Keywords: virtual reality, cognitive processes, learning, psychophysiological characteristics.

Технологии виртуальной реальности на сегодняшний день активно используются в разработке приложений для подготовки специалистов в различных сферах деятельности, так как созданные обучающие VR-тренажеры являются идеальной обучающей средой. Тренажеры данного типа позволяют изучать предмет на качественно новом, более высоком уровне за счет большей наглядности по сравнению, например, с традиционными компьютерными тренажерами. В итоге обучающийся получает как минимум не меньший опыт, чем при реальном взаимодействии с объектами окружающего мира, а зачастую - гораздо больший.

Технология виртуальной реальности значительно отличается от классических методик обучения тем, что она позволяет осуществлять полный контроль за вниманием человека и достигается за счет реализации свойств виртуальной реальности таких как иммерсивность и интерактивность. Данные свойства формируют иллюзию «погружения», что характеризуется возникновением у пользователя глубоких впечатлений

пребывания в реалистичной ситуации, хотя на самом деле вся виртуальная среда искусственно смоделирована специальными программно-аппаратными средствами [1].

Однако технологии VR - это достижение не только кибернетики, но и психологии. Они изначально реализовывалась и задумывалась как способ эффективного моделирования человеческого восприятия [2]. При этом оценка влияния свойств виртуальной реальности на человека в настоящее время практически не ведется, поскольку сама технология представляет собой симбиоз различных научных направлений и отличается междисциплинарным подходом.

Ряд исследователей отмечают, что виртуальная реальность оказывает комплексное влияние на психику человека, активизируя его познавательную деятельность, способствует развитию творческих способностей и логического мышления [3].

Но при этом остаются не изучены вопросы влияния технологий виртуальной реальности на психологическое состояние человека, такие как:

1. взаимодействия между когнитивными процессами (восприятие, память, мышление) и поведенческими актами (действиями);
2. влияния степени и форм двигательно-когнитивной кооперации на успешность выполнения пользователем различных видов практической деятельности в рамках обучения новым навыкам с использованием технологий виртуальной реальности;
3. специфики активности мозга и вегетативной нервной системы в условиях реального целенаправленного поведения в виртуальной среде.

Поэтому процессы профессионального становления и управления профессиональной деятельностью персонала требуют специальных знаний и умений в области изучения когнитивных процессов для оптимального их формирования.

Установлено, что неэффективность профессиональной деятельности примерно на 80 % обусловлена физиологическими, психическими и социально-психологическими особенностями человека [4]. Для разработки эффективного обучающего VR-тренажера необходимо будет учитывать и психофизиологические особенности пользователя, которые изначально отличаются у каждого человека, но они также и меняются у человека с возрастом, так как активность когнитивных процессов и состояние вегетативной нервной системы начинает ухудшаться.

Для обеспечения эффективного процесса обучения в виртуальной среде также необходимо определить сколько по времени должен состав-

лять сеанс работы, так как после продолжительного нахождения в виртуальной среде начинается ухудшаться самочувствие человека, а после выхода «из погружения» наблюдаются различные эффекты – головокружение, потеря ориентации, тошнота, головная боль и др.

Таким образом, необходимо определить оптимальное время сеанса обучения, которое бы позволило более эффективно формировать необходимые знаний и умения без причинения ущерба здоровью человека.

Проведение междисциплинарных исследований влияния технологий виртуальной реальности на психофизиологическое состояние пользователя, находящегося в виртуальной среде, позволит одновременно создавать различные профессионально-подобные симулируемые ситуации и изучать модели поведения человека в экстремальных условиях, как в период освоения профессиональных навыков, так и в процессе профессиональной деятельности. Поскольку виртуальная среда программируется, то это делает ее гибкой и позволяет пластично менять параметры виртуальных объектов и процессы взаимодействия пользователя с ними.

В виртуальных средах появляется возможность моделировать разные ситуации и предъявлять множество разнообразных стимулов (как неподвижных, так и движущихся) с контролируемыми параметрами (яркость, цвет, форма и др.). Кроме того, в виртуальных средах программируется структура появления стимуляции и настройка этой структуры в зависимости от реакции человека.

Изучение данных вопросов позволит получить представление о том, как когнитивные процессы участвуют в формировании различных профессиональных знаний и умений человека с использованием технологий виртуальной реальности, полученные результаты позволят реализовывать разработку VR-приложений, показывающих высокую эффективность и безопасность обучения.

Библиографический список

1. Авербух, Н. В. Феномен присутствия и его влияние на эффективность решения интеллектуальных задач в средах виртуальной реальности / Н. В. Авербух, А. А. Щербинин // Психология. Журнал Высшей школы экономики. – 2011. – Т. 8, № 4. – С. 102–119.

2. Wilson, C. J. The Use of Virtual Reality in Psychology: A Case Study in Visual Perception / C. J. Wilson, A. Soranzo // Computational and Mathematical Methods in Medicine. – 2015. – Vol. 2015. – 7 P. – DOI: 10.1155/2015/151702.

3. Bartolome, N. A. Innovative system for cognitive brain enhancement and language disorders treatment using a virtual reality environment / N. A. Bartolome, B. G. Zapirain, A. Mendez // The 17th International Conference on Computer Games. – Louisville, 2012. – P. 120–124.
4. Technologies of virtual reality in the context of world-wide and Russian psychology: methodology, comparison with traditional methods, achievements and perspectives / Yu. P. Zinchenko, G. Ya. Menshikova, Yu. M. Bayakovsky [et al.] // Psychology in Russia: State of the Art. – M., 2010. – P. 11–45.

УДК 378.14
Ю.А. Бахмутский, заведующий кафедрой «Математические методы и информационные технологии в экономике»; Е.А. Калиберда, канд. тех. н., доцент; О.Г. Шевелева, старший преподаватель
Омский государственный технический университет (ОмГТУ)

ИНТЕГРАЦИЯ ПРОЕКТНО-ОБРАЗОВАТЕЛЬНЫХ ИНТЕНСИВОВ С УЧЕБНЫМ ПРОЦЕССОМ

Аннотация
Рассматриваются вопросы внедрения проектно-образовательных интенсивов (ПОИ) в учебный процесс высшего учебного заведения. С помощью функциональной модели анализируются области возникновения возможных проблем и предлагаются варианты их решений.
Ключевые слова: образование, проектно-образовательный интенсив, проектная деятельность, учебный процесс, функциональная модель.
Abstract
The issues of implementation of project-educational intensives (PEIs) in the educational process of a higher educational institution are considered. With the help of a functional model, areas of possible problems are analyzed and options for their solutions are proposed.
Keywords: education, project-educational intensity, project activities, educational process, functional model.

Проектно-образовательный интенсив (ПОИ) предполагает, что учащиеся образовательных организаций разрабатывают и создают практические решения проблем, предоставленных задач от внешних заказчиков. Образовательная ценность ПОИ заключается в том, что он направлен на развитие у учащихся, работающих в небольших группах, творческих способностей для решения сложных или плохо структурированных задач и формирование командных компетенций [1]. Как правило, ПОИ проводит учащихся через следующие этапы или шаги:

1. Выявление проблемы.
2. Согласование или разработка решения и потенциального пути минимизации проблемы.
3. Проектирование и разработка прототипа решения.
4. Доработка решения на основе отзывов экспертов, авторов разрабатываемого проекта, наставников и/или коллег.
5. В зависимости от целей автора проекта размер и объем проекта могут сильно различаться. Студенты могут проходить четыре перечисленных этапа в течение многих недель или даже несколько раз в течение одного учебного периода.

В ОмГТУ, чьей основной целью является непрерывное обеспечение образовательного процесса, проектно-образовательный интенсив включает в себя несколько ключевых видов деятельности:

1. Управление деятельностью по организации проведению проектно-образовательных интенсивов.
2. Инициация нового проектно-образовательного интенсива.
3. Подготовка нового проектно-образовательного интенсива.
4. Проведение проектно-образовательного интенсива.
5. Завершение проектно-образовательного интенсива.

Для проведения детального анализа каждого из выделенных видов деятельности и определения проблемных зон авторами статьи была построена функциональная модель деятельности образовательной организации в рамках ПОИ. Пример диаграммы верхнего уровня модели в нотации IDEF0 приведен на рисунке 1.

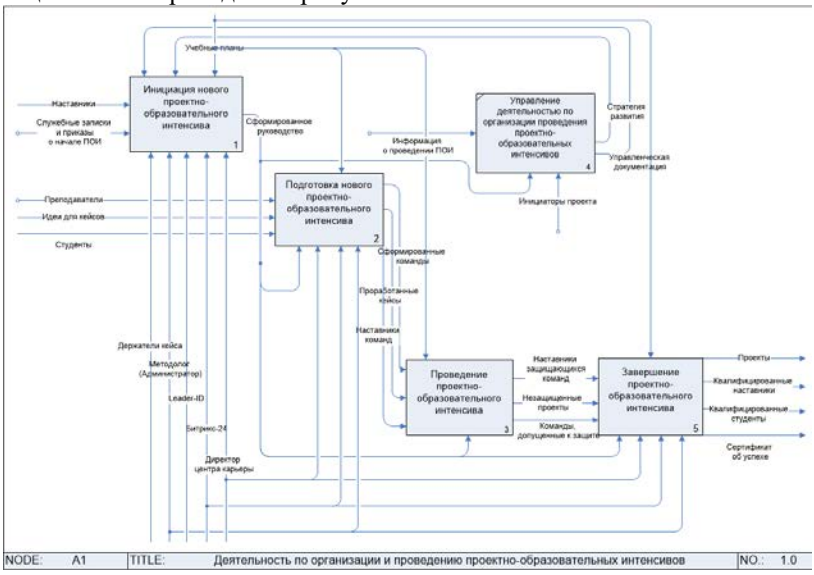


Рисунок 1 – Диаграмма деятельности по организации и проведению ПОИ

В силу того, что опыт проведения ПОИ в таком формате в ОмГТУ, на сегодняшний день, еще не велик, интенсивы проводятся здесь только второй год, в процессе проведения, возникает большое количество организационных, идеологических, методических и других вопросов.

Одним из таких вопросов является вопрос корреляции результатов прохождения студентами ПОИ с решением образовательных задач, поскольку в интенсивах участвуют студенты первого и второго курса разных направлений

Студенты участвуют в ПОИ в рамках освоения дисциплины "Проектная деятельность". Поэтому, помимо выполненного проекта, результатом интенсива является курсовая работа по дисциплине, с формированием всех необходимых компетенций, предусмотренных рабочей программой дисциплины.

Процесс интеграции двух видов деятельности, проектной и образовательной может выглядеть, например, так, как показано на рисунке 2.

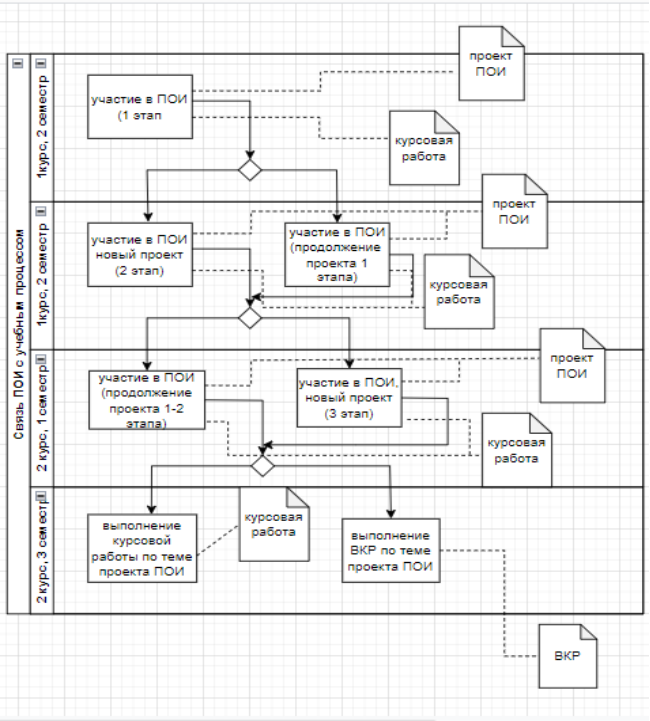


Рисунок 2 – Интеграция ПОИ с учебным процессом

Каждый этап выполнения ПОИ заканчивается представлением результатов в форме проекта и курсовой работой по дисциплине "Проект-

ная деятельность". Курсовая работа, в этом случае, выполняется на основе результатов, которых удалось достичь студентам при выполнении проекта в рамках ПОИ. Однако, по желанию студента, он может не участвовать в ПОИ, а выполнять только курсовую работу по отдельной теме.

На каждом следующем этапе можно начинать новый проект, выполняя его на более высоком уровне. Или можно продолжать проект, уже начатый на предыдущем этапе, совершенствуя свои компетенции и развивая их. Результатом развития проекта может стать выпускная квалификационная работа или стартап.

Однако, в предлагаемой схеме интеграции существует проблемная зона: в случае выполнения студентом и проекта, и курсовой работы по одной теме, необходимо обеспечить обязательное соответствие компетенций, формируемых в процессе прохождения ПОИ, компетенциям, закрепленным за учебной дисциплиной основной образовательной программой. Возможно, для достижения необходимого соответствия, потребуется доработка рабочих программ дисциплины "Проектная деятельность", тщательный отбор кейсов для проведения ПОИ для студентов конкретных направлений и для междисциплинарных команд.

Библиографический список

1. Смирнова И. Н. Проектная деятельность как способ формирования профессиональных компетенций обучающихся: барьеры и возможности / И. Н. Смирнова, П. В. Агафонова // Современное университетское образование: вызовы и проблемы, ценности и инновации, технологии и качество: сборник статей, Иваново, 24–25 ноября 2021 года. – Иваново: Ивановский государственный университет, 2021. – С. 407-414. – EDN BHHOPK.

УДК 004.032.26
В.Н. Бондарев, доц., канд. техн. наук
Севастопольский государственный университет
ул. Университетская 33, г. Севастополь, Россия, 299053
e-mail: bondarev@sevsu.ru

ОСОБЕННОСТИ РЕАЛИЗАЦИИ И ОБУЧЕНИЯ СВЕРТОЧНЫХ СПАЙКОВЫХ НЕЙРОСЕТЕЙ

Аннотация
Рассматривается архитектура спайковой нейросети для классификации изображений и различные подходы к реализации функций спайковой свёртки при прямом и обратном распространении сигналов.
Ключевые слова: спайковые нейронные сети, спайковая свёртка, обработка изображений.

V. Bondarev
Sevastopol State University
Universitetskaya Str. 33, Sevastopol, Russia, 299053
e-mail: bondarev@sevsu.ru

IMPLEMENTATION FEATURES AND TRAINING OF CONVOLUTIONAL SPIKING NEURAL NETWORKS

Abstract
We consider the architecture of spiking neural network for image classification and study various approaches to the implementation of spike convolution functions in forward and backward propagation of signals.

Спайковые нейронные сети (SNN - Spiking Neural Network). отличаются от традиционных нейросетей используемыми моделями нейронов, в которых информация представляется в виде последовательности импульсов (спайков), что обеспечивает их более высокую энергоэффективность [1].

Наибольшее распространение получили модели спайковых нейронов на основе порогового интегратора с утечкой (LIF – Leaky Integrate and Fire). Состояние LIF-нейрона определяется значением мембранного потенциала. Если его значение превышает некоторый порог, то нейрон формирует выходной спайк и мембранный потенциал устанавливается равным нулю. На вход интегратора подается сумма взвешенных входных спайков, поступающих от других нейронов сети.

Обучение глубоких спайковых нейросетей может осуществляться на основе алгоритма обратного распространения с использованием суррогатного градиента пороговой функции, используемой в составе LIF нейрона [1].

В докладе рассматривается сверточная спайковая нейросеть, осуществляющая классификацию изображений. Архитектура сети состоит из 2-х сверточных спайковых слоев (convLIF), за которыми следуют усредняющие спайковые пулинг слои (avepoolLIF), полносвязный слой (fc) и слой классификатора (softmax). Формально архитектура сети может быть описана строкой 12conv5x5-avepool-64conv5x5 - avepool- fc – softmax. Первый сверточный слой состоит из 12 фильтров размером 5x5, второй – из 64 фильтров размером 5x5.

В качестве примера на рисунке 1 показаны результаты обработки цветного изображения с помощью реализованной в составе сети 2D спайковой свертки. Исходное изображение было преобразовано в последовательсность спайков. Результирующие изображение восстанавливалось путем простого подсчета входных и выходных спайков. Обработка выполнялась тремя 2D фильтрами размером 3x3. Первый фильтр обеспечивал преобразование цветного изображения в полутоновое, а второй и третий осуществляли подчеркивание перепадов яркости (оператор Собела).

Рисунок 1 – Обработка изображения с помощью 2D спайковой свертки

Рассмотренная сверточная спайковая нейросеть позволяет получить точность классификации 99,2% для задачи классификации датасета MNIST, что соответствует точности традиционных сверточных нейросетей аналогичной архитектуры.

Библиографический список

1. Bondarev V. Training a digital model of a deep spiking neural network using backpropagation // E3S Web of Conferences "Topical Problems of Agriculture, Civil and Environmental Engineering, TPACEE 2020", Vol. 224, № 01026, 2020, 7 p.
https://doi.org/10.1051/e3sconf/202022401026

УДК 004.514
А.С. Голунова, к.т.н., доцент, А.В. Голунов, к.т.н., доцент
Омский государственный технический университет

КОГНИТИВНАЯ ДОСТУПНОСТЬ ЦИФРОВЫХ ПРОДУКТОВ

Аннотация
В статье рассматриваются вопросы когнитивной доступности цифровых продуктов, представлен анализ эргономических характеристик интерфейсов.
Ключевые слова: цифровой продукт, интерфейс, когнитивная доступность, эргономика.
Annotation
The article deals with the issues of cognitive accessibility of digital products, presents an analysis of the ergonomic characteristics of interfaces.
Key words: digital product, interface, cognitive accessibility, ergonomics.

В настоящее время когнитивной доступности и эргономическим характеристикам интерфейсов цифровых продуктов уделяется все большее внимание, что связано с непрерывным развитием отрасли.

Каким образом будут складываться взаимодействие пользователя с сайтом или приложением, чтобы каждое действие, которое совершает человек, давалось ему легко, и какой опыт он получит в результате, определяется когнитивной доступностью цифрового продукта.

При взаимодействии человека с графическим пользовательским интерфейсом в процессе обмена информацией в значительной степени задействован зрительный анализатор с характерной напряженностью труда [1]. При переутомлении зрения возникает риск развития «прогрессирующей близорукости от повышенного напряжения зрения» (по МКБ–10 код H52.1, код внешних причин X50.1–8).

Целью работы является анализ эргономических характеристик пользовательских интерфейсов и степень их влияния на когнитивную доступность цифровых продуктов.

При проектировании пользовательского интерфейса необходимо учитывать, что с интерфейсом должно быть удобно взаимодействовать при любых обстоятельствах и на любом устройстве, а также пользовательский опыт целевой аудитории.

Внедрение в системы и искусственную среду эффективных и удобных для всех функций может быть обеспечено средствами универсального дизайна.

Неограниченный доступ к информационным продуктам, способствует вовлечению людей с самым широким диапазоном когнитивных потребностей в широкий круг жизненных ситуаций.

Известен спектр когнитивных потребностей и данные о том, как можно изменить деятельность и факторы окружающей среды для расширения участия пользователей, которые необходимо применить на практике при разработке интерфейсов цифровых продуктов.

Таким образом, при разработке когнитивно доступных цифровых продуктов необходимо обеспечивать мотивацию и удерживать фокус пользователя, учитывать различия в способности пользователя к совладанию, обеспечить поддержку обратной связи системой и упрощения языка и структуры сообщения, обеспечивать ориентацию в пространстве и понимание значений и размеров.

Библиографический список:

1. ГОСТ Р ИСО 21801-1-2022. Когнитивная доступность. Общие руководящие указания. – // Библиотека нормативной документации: [сайт]. – URL: http://https://files.stroyinf.ru/Data/793/79309.pdf (дата обращения: 29.08.2022)

УДК 519.8
В.В. Захаров к.т.н., С.В. Микони д.т.н., профессор
ФГБУН «Санкт-Петербургский Федеральный исследовательский Центр Российской академии наук», Санкт-Петербургский институт информатики и автоматизации РАН
14 линия 39, г. 199178, Санкт-Петербург, Россия, 199178
e-mail: valeriov@yandex.ru
e-mail: smikoni@mail.ru

МОДЕЛЬ ПОДБОРА ИСПОЛНИТЕЛЯ РАБОТЫ

Аннотация
Исполнитель любой работы характеризуется профессионализмом и морально-волевыми качествами. Раскрытие и моделирование этих свойств позволяет более объективно оценить, насколько они удовлетворяют требованиям, предъявляемым к исполнителю работы. Рассматриваются показатели, отражающие профессионализм и личностные свойства исполнителя работы.
Ключевые слова: работа, исполнитель работы, модель оценивания, квалификация, личностные качества, психологический портрет.

SELECTION MODEL OF WORK CONTRACTOR

Abstract
The performer of any work is characterized by professionalism and moral-volitional qualities. The disclosure and modeling of these properties allows a more objective assessment of how they meet the requirements for the performer of the work. The indicators reflecting the professionalism and personal properties of the performer of the work are considered.
Key words: work, performer of work, assessment model, qualification, personal qualities, psychological portrait.

Качество любой работы зависит как от применяемой технологии её выполнения, так и от человека, использующего эту технологию. Наряду с профессионализмом человека на результаты работы влияют его личностные качества, характеризующие приспособленность к эффективному выполнению данной работы. Решению этой проблемы посвящена, в частности, работа [1]. В связи с этим актуальной является разработка формальной модели исполнителя работы с целью автоматизации подбора кадров с применением системы поддержки принятия решений (СППР).

Квалификация исполнителя определяется его знанием, умением и опытом работы в конкретной предметной области. Знание характеризуется набором закономерностей и принципов, которым исполнитель должен владеть для выполнения конкретной работы. Оно формализуется

перечнем нормативов. Степень соответствия им определяет пригодность исполнителя к заданной работе с точки зрения профессионального знания. В том случае, если нормативы упорядочены по степени их ужесточения, задача определения принадлежности специалиста одной из категорий квалификации может быть автоматизирована с применением модели многомерной классификации по упорядоченным классам (классификация по принадлежности классу).

Умение проверяется решением типовых задач соответствующей специальности и оценивается числом решённых задач за допустимое время. Опыт работы измеряется временем работы по специальности и её оценкой (благодарности, премии).

На профессиональную деятельность влияют личностные качества исполнителя. К ним относятся: нравственность, жизненные ценности, волевые качества, стрессоустойчивость, отношение к внешнему миру (к людям, животным и т.п.), приспособляемость к переменам, организаторские способности. Перечисленные качества подлежат дальнейшей конкретизации. Например, к волевым качествам относятся: настойчивость, трудолюбие, дисциплинированность, целеустремлённость и пр. Для успешного выполнения различных работ устанавливается различное соотношение перечисленных качеств, измеренных, например, в десятибалльной шкале.

Вектор балльных оценок, сформированный экспертами для конкретной работы, представляет собой цифровой психологический портрет (шаблон) нужного специалиста. Степень соответствия предлагаемой работе определяется вектором отклонений балльных оценок претендента от психологического портрета специалиста. По векторам отклонений определяется очерёдность претендентов на эту работу (упорядочение по *отклонениям* от портрета исполнителя работы) [2]. Качество оценивания зависит от системы принятых показателей, точности их измерения (самим претендентом или психологом) и от предложенного экспертом эталонного психологического портрета исполнителя работы.

Исследования, выполненные по данной тематике, проводились в рамках бюджетной темы FFZF–2022–0004.

Библиографический список

1. Фрумкин А.А. Психологический отбор в профессиональной и образовательной деятельности. – СПб.: Речь, 2004.
2. Микони С.В., Берестнёва О.Г., Сорокина М.И. Реализация экспертной системы по профессиональному отбору студентов в инструментальной системе СВИРЬ // Вестник Томского гос. унив-та (Приложение). №18. 2006. С. 237-242.

УДК 378.14:004

Т.А. Костылева, канд. филос. наук, доцент, О.В. Самарина, канд. ф.-м. наук, доцент
ФГБОУ ВО «Югорский государственный университет»

СОВРЕМЕННЫЕ ПОДХОДЫ К СИСТЕМЕ ПОДГОТОВКИ ИТ-СПЕЦИАЛИСТОВ В РЕГИОНАЛЬНОМ ВУЗЕ

Аннотация
В статье представлен подход к подготовке IT-специалистов, реализуемый в Югорском государственном университете. Описаны формы взаимодействия с представителями отрасли, организация практической подготовки студентов, процессы развития soft skills и hard skills студентов на базе лабораторий и центров университета.
Ключевые слова: IT-образование, высшее образование, подготовка IT-кадров, IT-среда университета.

Annotation
The article presents an approach to IT specialists training implemented at Yugra State University. The interactions forms with IT- industry, the practical training organization of students, the processes of developing students soft skills and hard skills in laboratories and centers university are described.
Key words: IT education, higher education, IT personnel training, IT environment of the university.

В современных реалиях масштабного перехода на импортозамещение, дефицита в квалифицированных ИТ-кадрах остро встает вопрос построения качественной системы региональной подготовки студентов по ИТ-специальностям [1, 2]. Учитывая критику к непоследовательности преподавания, оторванности от решения реальных (не учебных) задач, университет принял вызов и разработал новые программы подготовки ИТ-специалистов. Основными подходами подготовки специалистов в области информационных технологий стали:

Тесное партнерство с представителями отрасли. В университете функционируют базовые кафедры, что позволяет выстроить образовательный процесс в специализированных лабораториях и центрах. Специалисты ИТ-компаний привлекаются в качестве преподавателей профильных дисциплин (2022 год - 40%). Для формирования актуальных профессиональных компетенций, оценки качества программ сформирован экспертный совет, в состав которого вошли крупнейшие представители ИТ-отрасли региона.

Включение в деятельностные практики, расширение возможностей обучающихся для самореализации и саморазвития за счет формирования индивидуальных образовательных траекторий и выбора надпрофессиональных и профессиональных треков.

Привлечение студентов в группы разработки ИТ-продуктов. В лабораториях инженерной школы цифровых технологий студенты принимают активное участие в реализации реальных проектов в таких областях как автоматика и робототехника, технология 3D-моделирования, виртуальная и дополненная реальность, веб-разработка, а также анализ и обработка данных.

Развитие мягких компетенций. Большое внимание при подготовке ИТ-специалистов уделяется формированию таких компетенций, как работа в команде, навыки коммуникации, и планирования. Наработка данных навыков осуществляется в рамках дисциплин, проектной деятельности студентов, их практической подготовки на базе лабораторий и центров университета, площадках работодателей.

Цифровизация образовательного процесса. Важным элементом организации учебного процесса является IT-среда университета. В университете создана и успешно функционирует система цифровых сервисов, позволяющая студентам получать подробную информацию об учебном процессе, активно взаимодействовать с преподавателями и администрацией университета.

Библиографический список

1. Computing Curricula 2020: Paradigms for Global Computing Education https://dl.acm.org/doi/pdf/10.1145/3467967 (дата обращения 15.02.2023)
2. ИТ-кадры для цифровой экономики в России https://apkit.ru/files/it-personnel%20research_2024_APKIT.pdf?_ysclid=le6n2qu9sm543272923 (дата обращения 15.02.2023)

УДК 378.14:004

Т. В. Макарова, канд. пед. наук, доцент кафедры «Математические методы и информационные технологии в экономике»
ФГАОУ ВО «Омский государственный технический университет»

СТУДЕНЧЕСКОЕ КОНСТРУКТОРСКОЕ БЮРО КАК ПРОФЕССИОНАЛЬНЫЙ СИМБИОЗ ПРЕПОДАВАТЕЛЯ И СТУДЕНТОВ

Аннотация
Опыт проектной работы студенческого конструкторского бюро «Политех\Медиа» выявил существование профессионального симбиоза студентов и преподавателей, позволяющего первым реализовывать свой творческий потенциал и комфортно входить в профессию, а вторым – всегда оставаться в актуальной профессиональной форме, что в свою очередь, повышает качество подготовки студентов ИТ-направлений.
Ключевые слова: ИТ-образование, студенческое конструкторское бюро, научно-техническое творчество, профессиональный симбиоз.
Annotation
The experience of project work of the student design bureau "Polytech\Media" revealed the existence of professional symbiosis of students and teachers, which allows the first to realize their creative potential and comfortably enter the profession, and the second - to always remain in the current professional form, which in turn, improves the quality of training of IT students.
Key words: IT-education, student design bureau, scientific and technical creativity, professional symbiosis.

Одной из ведущих тенденций в развитии инженерного образования, способствующих эффективному преобразованию студентов ИТ-направлений в компетентных специалистов отрасли, является создание студенческих конструкторских бюро.

Являясь добровольным объединением, студенческое конструкторское бюро (СКБ) привлекает единомышленников, имеющих интерес и склонность к научно-техническому творчеству. Те же характеристики, как правило, присущи и руководителю СКБ – преподавателю тематической кафедры.

Пятилетний опыт проектной работы в СКБ «Политех\Медиа» (Омский государственный технический университет) со студентами профиля «Информационные технологии в медиаиндустрии», показал, что у студенческой молодежи есть стремление создавать нечто общественно-значимое, уникальное, современное и завершенное, а работу в СКБ они

рассматривают, как возможность реализовать свою потребность к когнитивному творчеству, а также пораньше и поглубже погрузиться в профессиональную среду.

Ранний вход в ИТ-профессию возможен и через свободный подряд на выполнение коммерческих заказов (фриланс). Однако, коммерческий заказ, содержащий четкое ТЗ и минимальный срок исполнения, для студента, не имеющего соответствующих знаний и опыта, часто оказывается неподъемным делом.

СКБ «Политех\Медиа» сотрудничает с мультимедийным историческим музейным парком «Россия – Моя история» (г. Омск), руководитель которого заинтересован в наполнении экспозиций современными интерактивными цифровыми продуктами. Когда сотрудники музея задумывают очередную выставку, у них существует концептуальное видение будущих инсталляций, но нет четко сформированного техническое задания. И это – идеальная ситуация для творческого поиска, сочетающаяся с научно-образовательными задачами СКБ.

Творческих ребят привлекает работа в команде, а наличие руководителя-наставника добавляет спокойствия и уверенности. При этом отсутствие требуемых умений не пугает и не останавливает ребят, а, напротив, мотивирует к освоению новых средств и технологий, разжигает азарт.

Перед участниками СКБ ставится открытая задача, к выполнению которой обе стороны продвигаются итерациями, и где студент может предлагать собственное, современное с его точки зрения, решение.

Симбиоз – форма взаимоотношений, когда элементы не просто взаимодействуют, а нуждаются друг в друге. Участие в проектах СКБ являет собой то сообщество – преподавателей и студентов – которое питает и обеспечивает профессиональное совершенствование друг друга.

Студенту этот симбиоз обеспечивает комфортный вариант входа в профессию – когда первые реальные продукты создаются под руководством наставника, который не просто выдает задание, но помогает спланировать этапы работы, организовывает на каждом этапе «приемку» и коррекцию, задает определенный когнитивный уровень проработки задачи, помогает определиться с референсами и технологиями.

Преподавателю руководство творческой, (с инновационным поиском), работой, исполняемой студентами по коммерческому договору с СКБ, во-первых, дает новые знания, которые актуализируют профессиональную информацию – будущее содержание лекционного материала, и, во-вторых, повышает качество самого педагога, как специалиста, поскольку хорошо выполненная командой работа отражает, в том числе,

способности, ум, вкус и педагогическое мастерство самого преподавателя. Эти факторы, в свою очередь, положительно отражаются на качестве подготовки всех студентов ИТ-направлений, охваченных деятельностью преподавателя, курирующего проекты тематического СКБ.

УДК 681.518

А.В. Алексеев[1], проф., д-р техн. наук, В.В. Касаткин[2], доц., канд. техн. наук, В.И. Салухов[2], доц., канд. техн. наук

[1]Санкт-Петербургский государственный морской технический университет

e-mail: iapbgks@bk.ru

[2]Санкт-Петербургский Федеральный исследовательский центр Российской академии наук

e-mail: spiiras@iias.spb.su

ТЕХНОЛОГИЯ АВТОМАТИЗИРОВАННОГО ОЦЕНИВАНИЯ КАЧЕСТВА РАБОТЫ НАУЧНЫХ РУКОВОДИТЕЛЕЙ АСПИРАНТОВ

Аннотация

В условиях возрастания требований к качеству подготовки научных и научно-педагогических кадров высшей квалификации немаловажное значение приобретает вопрос оценки и стимулирования труда научных руководителей аспирантов. Рассматривается технология квалиметрической оценки качества работы научных руководителей. Представлены результаты экспериментального внедрения Автоматизированной системы поддержки принятия решений «АСОР-2022.1_НР», которая может быть рекомендована к использованию в качестве инструмента цифровизации процедуры оценивания качества работы научных руководителей аспирантов на различных этапах обучения (подготовки диссертационных работ) с учетом специфики выбранной укрупненной группы научных специальностей, профиля научно-образовательной организации и других факторов.

Ключевые слова: кадры высшей квалификации, оценка качества работы научного руководителя аспиранта, измерение качества, квалиметрия, критерии и технология оценивания, автоматизированная система поддержки принятия решений.

Abstract

In the context of increasing requirements for the quality of training of scientific and scientific and pedagogical personnel of the highest qualification, the issue of assessing and stimulating the work of scientific leaders of graduate students becomes important. The technology of kvali-metric assessment of the quality of work of scientific supervisors is being considered. The results of the experimental introduction of the Automated Bathroom Decision Support System "ASOR-2022.1_NR", which can be recommended for use as an in-tool for digitalization of the procedure for assessing the quality of work of post-graduate students at various stages of training (preparing dissertation works), taking into account the specifics of the selected enlarged group of

scientific specialties, the profile of the scientific and educational organization and other factors, are presented.
Keywords: personnel of the highest qualification, assessment of the quality of the work of the scientific co-driver of the graduate student, quality measurement, qualimetry, criteria and assessment technology.

Стремительное развитие отечественных информационных технологий (ОИТ) в условиях цифровой трансформации отраслей экономики и социальной сферы, сопровождаемое неуклонным возрастанием сложности организационно-технических систем (ОТС), обуславливает необходимость рассматривать повышение эффективности управления ОТС на основе внедрения ОИТ в качестве одной из ключевых проблем [1-3], гарантирующих их устойчивое функционирование и развитие. Сведение множества требований, критериев и частных показателей качества к групповым, модельным и в конечном счете – агрегированному (интегральному) показателю качества позволяет осуществить переход к цифровизации и автоматизировать анализ системных характеристик ОТС за счет снижения уровня сложности решаемых задач. Применение квалиметрической парадигмы в сочетании с рядом соответствующих методов и технологий [4-12] наряду с уникальным свойством инвариантности к специфике решаемых задач обеспечивает возможность сопоставления сложных и разнородных ОТС по такому важному системному критерию как качество (мера соответствия объекта анализа своему предназначению). В наибольшей степени эта возможность проявляются при исследовании трудноформализуемых процессов, к числу которых следует отнести процессы управления ОТС, и, в частности, процесс руководства подготовкой научных и научно-педагогических кадров в аспирантуре, в рамках которого научный руководитель аспиранта осуществляет руководство научной (научно-исследовательской) деятельностью аспиранта с целью достижения конечного результата – подготовки и защиты диссертации на соискание ученой степени кандидата наук.

В условиях возрастания требований к качеству подготовки научных и научно-педагогических кадров высшей квалификации немаловажное значение приобретает задача оценки и стимулирования труда научных руководителей аспирантов, которая может быть решена на основе интенсивно развивающихся в последнее время методов квалиметрического анализа, синтеза и оптимизации [4-7].

При выборе критериев оценивания результатов работы научного руководителя аспиранта, учитывающих результативность, а также сте-

пень заинтересованности и личного участия научного руководителя аспиранта в реализации соответствующей программы подготовки научных и научно-педагогических кадров и подготовке аспирантом кандидатской диссертации, за основу приняты критерии, которым должны отвечать диссертации на соискание ученой степени кандидата наук, определенные постановлением Правительства Российской Федерации от 24 сентября 2013 г. № 842 (ред. от 11.09.2021) «О порядке присуждения ученых степеней» (вместе с «Положением о присуждении ученых степеней»). В частности, оценка результатов работы научного руководителя аспиранта в баллах может быть организована в процессе проведении аттестационных мероприятий (промежуточной и итоговой аттестации аспирантов) по критериям: выполнения аспирантом индивидуального плана научной деятельности; выполнения аспирантом индивидуального учебного плана; результативности работы аспирата над диссертацией; взаимодействия научного руководителя с аспирантом.

Особое значение задача оценки качества работы научных руководителей аспирантов в соответствии с Федеральным законом от 30.12.2020 № 517-ФЗ приобретает в связи с введением в действие с 01.03.2022 постановления Правительства РФ от 30.11.2022 № 2122 и приказа Минобрнауки России от 20.10.2021 № 951, согласно которым прием в аспирантуру, начиная с 2022/23 учебного года, осуществляется в соответствии с федеральными государственными требованиями к программам подготовки научных и научно-педагогических кадров в аспирантуре [1].

Ниже представлены результаты разработки и использования автоматизированной системы поддержки принятия решений (АСППР) РПК «АСОР-2022.1_НР», включающей пять модулей, предназначенных для выполнения следующих функций:

«1.Задача»: постановка задачи оценивания качества работы научного руководителя аспиранта;

«2.Требования»: формулировка основных требований Положения ВАК с описанием системы соответствующих критериев и показателей.

«3.Модель»: систематизация критериев и их агрегирование в три групповых показателя качества и основные свойства – ГПК «1.Результативность», ГПК «2.Учебно-методическое обеспечение», ГПК «3. Научно-организационное обеспечение» с последующим сведением в единый агрегированный показатель качества научного руководства АПК на основе гармонического алгоритма агрегирования 10 ЧПК в 3 ГПК, в 3 МПК (по числу лет подготовки диссертационной работы) и один АПК [7-9].

При этом матрица индексов критериальной значимости (ИКЗ, весовые коэффициенты) может быть расширена и обеспечивать возможность по заданным отношениям предпочтений учитывать не только год подготовки аспиранта, но и специфику научной специальности (укрупненной группы научных специальностей), профиль научно-образовательной организации, характер диссертационного исследования (теоретический или прикладной) и т.п.

«4.Оценка»: главная экранная форма, обеспечивающая ввод исходных данных, их регистрацию, обработку и вывод результатов оценивания, включая значения АПК, итоговый АПК по всем обучаемым, относительный уровень выполнения научным руководителем заданного показателя и относительный уровень его конкурентноспособности по отношению к лучшему значению АПК в данной организации (ее подразделении).

«5.Архив»: база данных, включающая в том числе скриншоты аттестационных листов (экранных форм модуля «4.Оценка») по каждому аспиранту и их научным руководителям.

На рисунке 1 представлен пример главной экранной формы АСППР «АСОР-22.1_НР» в режиме оценки качества научного руководства профессором Алешиным А.В. аспиранта Смирнова А.В. на третьем году обучения по 10+8+8=26 частным показателям качества (фрагмент требований и соответствующих ЧПК приведен на рис. 2), сведенным в три групповых показателя качества.

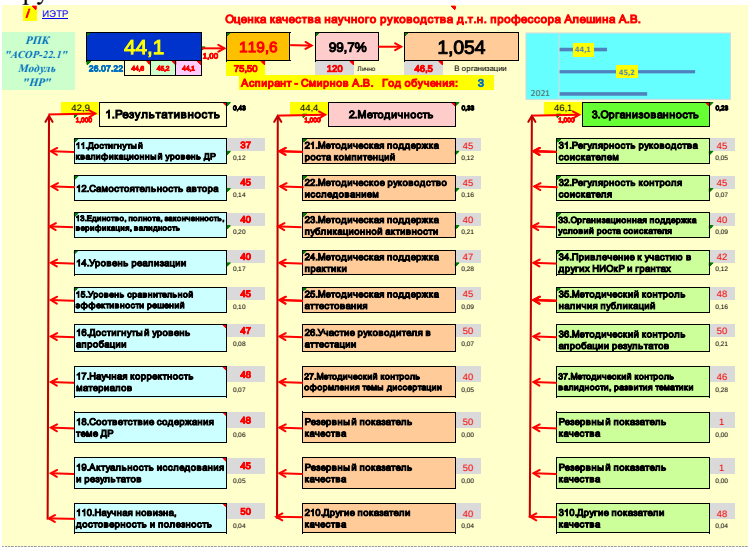


Рисунок 1 – Главная экранная форма АСППР (РПК) «АСОР-22.1_НР»

Результаты оценки качества научного руководства (левая верхняя часть рис. 1) составили: на первом году обучения – 44,6, на втором году – 45,2 (+1,4%), на третьем году – 44,1 (-1,1%). Причем, с целью анализа влияния специфических особенностей требований на разных годах обучения эти оценки выполнены при одинаковых исходных данных. Соответствующие отличия оценок приведены выше в скобках.

Также на рис. 1 приведены значение итогового АПК научного руководства по всем обучаемым аспирантам 119,6 (при введенном значение суммы АПК по двум другим аспирантам 75,5) и соответствующая степень 99,7% выполнения научным руководителем заданного показателя 120 по трем обучаемым, а также соответствующий индекс (конкурентная способность по качеству научного руководства) 1,054 в сравнении с лучшим значением АПК по организации 46,5.

Представленные результаты количественного оценивания позволяют руководителю организации принимать обоснованные решения в сфере управления подготовкой кадров высшей квалификации, направленные на повышение качества образовательного процесса и результативности диссертационных исследований, совершенствование системы подготовки аспирантов, стимулирование повышения качества научного руководства аспирантами.

1. Основные критерии оценивания результатов работы научного руководителя аспиранта

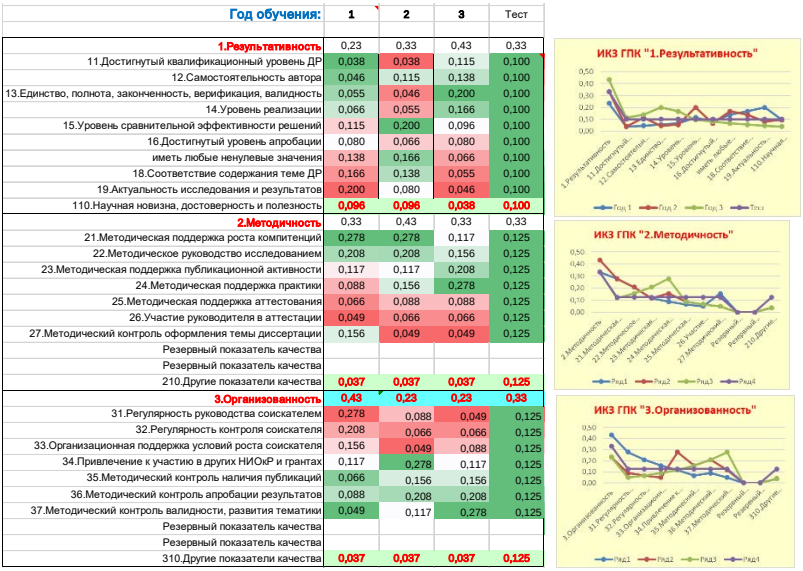
(согласно критериям, которым должны отвечать диссертации на соискание ученой степени кандидата наук, определенным «Положением о присуждении ученых степеней» (постановление Правительства РФ от 24.09.2013 № 842 (ред. от 11.09.2021) «О порядке присуждения ученых степеней»)

№	Основные критерии	Показатель
1	Является ли представленная диссертация научно-квалификационной работой, в которой содержится решение научной задачи, имеющей значение для развития соответствующей отрасли знаний, либо изложены новые научно обоснованные технические, технологические или иные решения и разработки, имеющие существенное значение для развития страны	11.Достигнутый квалификационный уровень ДР
2	Подготовлена ли диссертация автором самостоятельно, содержит ли диссертация новые научные результатыи положения, выдвигаемые для	12.Самостоятельность автора
3	Характеризуется ли представленная диссертация внутренним единством, полнотой и законченностью, достигаетли сформулированные цели проведения диссертационного исследования, решает ли поставленные задачи	13.Единство, полнота, законченность, верификация, валидность
4	Если диссертация носит прикладной характер, имеются ли сведения о практическом использовании полученных автором диссертации научных результатов, а в диссертации, имеющей теоретический характер, представленыли рекомендации по использованию основных научных выводов	14.Уровень реализации
5	Являются ли предложенные автором диссертации решения достаточно аргументированными и оцененными по сравнению с другими известными решениями	15.Уровень сравнительной эффективности решений
6	Опубликованы ли основные научные результаты диссертациив количестве, установленном требованиями Высшей аттестационной комиссии при Министерстве науки и высшего образования Российской Федерации, в рецензируемых научных изданиях, перечень которых установлен Министерством науки и высшего образования Российской Федерации, имеютсяли у автора приравненные к указанным публикациям патенты на изобретения, полезные модели, промышленные образцы, селекционные достижения, свидетельства о государственной регистрации программ для ЭВМ, баз данных, топологий интегральных микросхем	16.Достигнутый уровень апробации
7	Включены ли автором в диссертацию ссылки на авторов и (или) источники заимствования материалов или отдельных результатов диссертации; отмечено ли автором использование в диссертации результатов научных работ, выполненных соискателем ученой степени лично и (или) в соавторстве	17.Научная корректность материалов

Рисунок 2 – Фрагмент формирования системы критериев

Матрица индексов критериальной значимости (весовых коэффициентов) принятой системы критериев оценки качества работы научного руководителя, позволяющая учесть специфику соответствующих процессов подготовки кадров, формируемая учебно-методической комиссией и утверждаемая руководителем научно-образовательной организации, приведена на рис. 3 с соответствующими графиками.

Программная реализация данной задачи позволяет корректировать перечень и содержательное наполнение принятой системы критериев и соответствующих ИКЗ, что обеспечивает широкие возможности использования оболочки АСППР «АСОР-22.1» и ее адаптации к условиям учебного процесса с учетом специфики научно-образовательной организации, а также к принятой системе критериев оценки качества руководства без предъявления к пользователям требований к уровню их подготовки в среде открытого программирования.



Год обучения:	1	2	3	Тест
1.Результативность	0,23	0,33	0,43	0,33
11.Достигнутый квалификационный уровень ДР	0,038	0,038	0,115	0,100
12.Самостоятельность автора	0,046	0,115	0,138	0,100
13.Единство, полнота, законченность, верификация, валидность	0,055	0,046	0,200	0,100
14.Уровень реализации	0,066	0,055	0,166	0,100
15.Уровень сравнительной эффективности решений	0,115	0,200	0,096	0,100
16.Достигнутый уровень апробации	0,080	0,066	0,080	0,100
иметь любые ненулевые значения	0,138	0,166	0,066	0,100
18.Соответствие содержания теме ДР	0,166	0,138	0,055	0,100
19.Актуальность исследования и результатов	0,200	0,080	0,046	0,100
110.Научная новизна, достоверность и полезность	**0,096**	**0,096**	**0,038**	**0,100**
2.Методичность	0,33	0,43	0,33	0,33
21.Методическая поддержка роста компитенций	0,278	0,278	0,117	0,125
22.Методическое руководство исследованием	0,208	0,208	0,156	0,125
23.Методическая поддержка публикационной активности	0,117	0,117	0,208	0,125
24.Методическая поддержка практики	0,088	0,156	0,278	0,125
25.Методическая поддержка аттестования	0,066	0,088	0,088	0,125
26.Участие руководителя в аттестации	0,049	0,066	0,066	0,125
27.Методический контроль оформления темы диссертации	0,156	0,049	0,049	0,125
Резервный показатель качества				
Резервный показатель качества				
210.Другие показатели качества	**0,037**	**0,037**	**0,037**	**0,125**
3.Организованность	**0,43**	**0,23**	**0,23**	**0,33**
31.Регулярность руководства соискателем	0,278	0,088	0,049	0,125
32.Регулярность контроля соискателя	0,208	0,066	0,066	0,125
33.Организационная поддержка условий роста соискателя	0,156	0,049	0,088	0,125
34.Привлечение к участию в других НИОкР и грантах	0,117	0,278	0,117	0,125
35.Методический контроль наличия публикаций	0,066	0,156	0,156	0,125
36.Методический контроль апробации результатов	0,088	0,208	0,208	0,125
37.Методический контроль валидности, развития тематики	0,049	0,117	0,278	0,125
Резервный показатель качества				
Резервный показатель качества				
310.Другие показатели качества	**0,037**	**0,037**	**0,037**	**0,125**

Рисунок 3 – Фрагмент формирования матрицы ИКЗ

Как показал опыт экспертного оценивания сложных процессов, наиболее результативным следует считать метод «регулируемой самооценки», при котором научный руководитель представляет самоотчет в

соответствии с предложенной системой критериев, который корректируется по итогам проведения аттестации коллективным органом регулирования — аттестационной комиссией. Как показало тестирование, время, затрачиваемое научным руководителем на подготовку самоотчета о результатах работы в течение отчетного периода (семестра, учебного года) при наличии подготовленных шаблонов и дружественного интерфейса весьма незначительное, а наличие расширяемой базы данных способствует сокращению временных затрат.

При этом ключевую роль играют факторы коллегиальности, прозрачности и объективности оценивания, возможности систематизации и ранжирования требований, предъявляемых к результатам работы научного руководителя и опосредованно – аспиранта, а также мотивирование на достижение более высоких показателей, характеризующих творческую активность, ответственность и квалификационную зрелость, обеспечение взаимопонимания и межличностного взаимодействия с аспирантом и, в конечном счете, на достижение конечной цели – подготовки и успешной защиты диссертации на соискание ученой степени кандидата технических наук.

Результаты опытной эксплуатации разработанного в среде открытого программирования программного комплекса АСППР (РПК) «АСОР-22.1» позволяют рекомендовать его к использованию в качестве инструмента цифровизации процедуры оценивания качества работы научных руководителей аспирантов с учетом выбранной научной специальности (укрупненной группы научных специальностей), профиля научно-образовательной организации, специфики области научных исследований и других факторов. Приведенный пример междисциплинарного использования технологии квалиметрического анализа подтверждает возможность и целесообразность проведения анализа и автоматизированного оценивания объектов информатизации при принятии и обосновании соответствующих организационно-технических, инновационных и инвестиционных решений.

Библиографический список

1. Постановление Правительства Российской Федерации от 30 ноября 2021 г. № 2122 «Об утверждении Положения о подготовке научных и научно-педагогических кадров в аспирантуре (адъюнктуре)»
2. Приказ Минобрнауки России от 20 октября 2021 г. № 951 «Об утверждении Федеральных государственных требовании к структуре программ подготовки научных и научно-педагогических кадров в аспиран-

туре (адъюнктуре), условиям их реализации, срокам освоения этих программ с учетом различных форм обучения, образовательных технологий и особенностей отдельных категорий аспирантов (адъюнктов)».
3. Постановление Правительства РФ от 24.09.2013 N 842 (ред. от 11.09.2021) «О порядке присуждения ученых степеней» (вместе с «Положением о присуждении ученых степеней»).
4. Азгальдов Г.Г., Костин А.В. Квалиметрия и бизнес // Менеджмент инноваций, 2011. - №4(16). – С.284-296.
5. Микони С. В., Соколов Б. В. Юсупов Р. М. Квалиметрия моделей и полимодельных комплексов: монография. — М.: РАН, 2018. – 314 с.
6. Субетто А.И., Алексеев А.В. Теория практики квалиметрического обеспечения развития морских автоматизированных систем / Актуальные проблемы морской энергетики: материалы седьмой Всероссийской межотраслевой научно-технической конференции в рамках Второго Всероссийского научно-технического форума «Корабельная энергетика: из прошлого в будущее». – СПб.: Изд-во СПбГМТУ, 2018, с. 78 – 86.
7. Алексеев А.В. Модель и технология мониторинга и информационно-аналитической поддержки управления информатизацией и развитием информационного общества / Перспективные направления развития отечественных информационных технологий: материалы VI межрегиональной научно-практической конф. Севастополь, 22-26 сентября 2020 г. / Севастопольский государственный университет; науч.ред. Б.В.Соколов. – Севастополь: СевГУ, 2020, с. 16-18.
8. Алексеев А.В. Методика инвариантной оценки качества и эффективности объектов морской техники и морской инфраструктуры / Морские интеллектуальные технологии/Marine intellectual technologies, № 1 (51) том 2, 2021, с. 60-67.
9. Алексеев А.В. Примеры реализации полимодельного квалиметрического метода системной оптимизации объектов морской техники и морской инфраструктуры / Морские интеллектуальные технологии/Marine intellectual technologies, № 2 (52) том 3, 2021, с. 69-81.
10. Бобрович В.Ю., Алексеев А.В., Антипов В.В., Смольников А.В. Синтетическая квалиметрия: метод и технология поиска конкурентно способных решений в классе систем борьбы за живучесть корабля / Актуальные проблемы морской энергетики: материалы одиннадцатой международной научно технической конференции. – СПб.: Изд-во СПбГМТУ, 2022, с. 290-299.
11. Алексеев А.В., Михальчук А.В. Перспективные направления развития технологии полимодельного квалиметрического анализа, синтеза и

оптимизации организационных и технических решений / Перспективные направления развития отечественных информационных технологий: материалы VII межрегиональной научно-практической конф. Севастополь, 21-25 сентября 2021 г. / Севастопольский государственный университет; науч.ред. Б.В.Соколов. – Севастополь: СевГУ, 2021, с. 40-41.
12. Мусатенко Р.И., Алексеев А.В. Примеры полимодельной оценки компетенций обучающихся при подготовке морских кадров // Актуальные проблемы морской энергетики: материалы десятой международной научно-технической конференции в рамках Пятого Всероссийского научно-технического форума «Корабельная энергетика: из прошлого в будущее». – СПб.: Изд-во СПбГМТУ, 2021, с. 363 – 369.

УДК 337.004
М. В. Шматко, к. филос. н., доцент; Д. Д. Мухина, магистрант; А. А. Соседко, магистрант
ФГАОУ ВО Омский государственный технический университет, Россия

ПРОФЕССИОНАЛЬНОЕ ОБРАЗОВАНИЕ ПО ЦИФРОВЫМ СПЕЦИАЛЬНОСТЯМ В ОМСКОМ РЕГИОНЕ

Аннотация
Статья посвящена исследованию проблемы профессиональной подготовки кадров по цифровым специальностям в Омском регионе. В его контекст включены направления профессиональной подготовки высших учебных заведений, учреждений среднего профессионального образования, а также различные программы повышения квалификации и переподготовки. В статье приводятся результаты анализа и сопоставления потребностей государства в кадрах по цифровым специальностям, определенных в рамках Программы «Цифровая экономика Российской Федерации», с востребованностью различных ИТ-направлений у абитуриентов и количеством выпускников по ним в учебных заведениях Омского региона.
Ключевые слова: цифровые специальности, Омский регион, профессиональное обучение, цифровая экономика, ИТ-направления, цифровые технологии.
Abstract
The article is devoted to the study of the problem of professional training of personnel in digital specialties in the Omsk region. Its context includes areas of professional training of higher educational institutions, institutions of secondary vocational education, as well as various professional development and retraining programs. The article presents the results of the analysis and comparison of the needs of the state for personnel in digital specialties, defined within the framework of the Program «Digital Economy of the Russian Federation», with the demand for various IT-areas among applicants and the number of graduates in them in educational institutions of the Omsk region.
Keywords: digital specialties, Omsk region, vocational training, digital economy, IT-areas, digital technology.

Введение. В 2017 г. Правительство нашей страны утвердило Программу «Цифровая экономика Российской Федерации». Согласно ее положениям, основными сквозными цифровыми технологиями являются:

– большие данные;
– нейротехнологии и искусственный интеллект;
– системы распределенного реестра;

– квантовые технологии;
– новые производственные технологии;
– промышленный интернет;
– компоненты робототехники и сенсорика;
– технологии беспроводной связи;
– технологии виртуальной и дополненной реальностей [1].

При этом в Программе подчеркивается важность обеспечения цифровой экономики Российской Федерации высокопрофессиональными кадрами для проектирования и внедрения перечисленных цифровых технологий.

Особенно актуальным профессиональное образование по цифровым специальностям стало в 2022 г. Многие крупные зарубежные ИТ-компании, такие как «Microsoft», «Oracle», «SAP», «Autodesk», «Acronis», «EPAM Systems», «Cisco», «Intel», «AMD» и др., приостановили свою деятельность в нашей стране. Как следствие этого возникла потребность в разработке собственных цифровых технологий, а, значит, усилилась роль образования по различным ИТ-направлениям.

Так, например, в Омском регионе в 2022 г. для решения этой проблемы создано региональное Министерство цифрового развития и связи, которое под руководством Андрея Александровича Ключенко осуществляет разработку и реализацию государственных и ведомственных целевых программ, а также и приоритетных национальных проектов [2]. Примером такого проекта является национальный проект «Наука и университеты», а также программа цифровой трансформации Омской области [3].

Постановка задачи. Цель данного исследования – выявление приоритетных направлений подготовки кадров по цифровым специальностям в Омском регионе для обеспечения потребности региональной цифровой экономики.

В рамках исследования необходимо проанализировать открытые данные различных учебных заведений Омского региона – государственных и частных вузов, а также техникумов и колледжей, включая программы повышения квалификации и профессиональной переподготовки.

Теория. В Российской Федерации подготовка кадров по цифровым специальностям осуществляется как учреждениями среднего профессионального образования, так и высшими учебными заведениями.

Согласно действующим федеральным государственным образовательным стандартам, информационно-образовательная среда профессиональной подготовки ИТ-специалистов в условиях непрерывного обу-

чения должна опираться на новые подходы и технологии: широкое использование информационно-коммуникационных ресурсов, сочетание высокой экономической эффективности и гибкости учебного процесса, а также построение новых результативных форм освоения сквозных цифровых технологий. Для создания такой образовательной среды в качестве базового закладывается принцип модульности: модуль – это самостоятельный курс, предусматривающий освоение одной или нескольких цифровых компетенций [4]. Это позволяет обеспечивать конкретные области производства цифровыми кадрами, готовыми эффективно решать конкретные прикладные задачи.

Также можно выделить и другие принципы, которые должны использоваться при создании информационно-образовательной среды подготовки ИТ-кадров: технологичность, организованность, динамичность, целостность, открытость, многофункциональность [4]. Через контроль за реализацией этих принципов государство обеспечивает процесс профессиональной подготовки кадров по цифровым специальностям.

Что касается экспертов от ИТ-сообщества и представителей производств, нуждающихся в ИТ-специалистах, то они сходятся во мнениях, что ИТ-образование должно следовать международным тенденциям. Приведем некоторые из них.

Первая тенденция – это гибридный формат обучения, особенность которого состоит в сочетании оффлайн и онлайн обмена знаниями. Вторая – дополнение базового образования постоянным освоением программ микрообучения в онлайн-режиме. По мнению экспертов, использование микрообучения работником является важным показателем его прогрессивности и способности к профессиональному самосовершенствованию. Еще одна важная тенденция, которая, по мнению, экспертов должная распространиться в российском ИТ-образовании – непрерывное совмещение учебы с практикой. Особенно это касается студентов, которые получают базовую ИТ-подготовку. В свою очередь, эксперты отмечают, что на ее осуществление у учебных заведений в нашей стране пока недостаточно ресурсов, позволяющих в полной мере объединить государственные стандарты подготовки ИТ-специалистов с потребностями региональных предприятий.

Четвертая тенденция появилась благодаря молодым и мобильным сотрудникам, которые стремятся к автономному обучению. Она, по мнению экспертов, приобретает большое значение и станет «ключевой» в 2023 г., так как ИТ-специалисты должны сами формировать свою об-

разовательную траекторию, осваивая интересующие их, а не работодателей, цифровые компетенции и имея возможность смены отрасли производства [5].

Результаты экспериментов. Для достижения поставленной цели исследования нами были составлены базы данных по вузам, техникумам и колледжам Омского региона, государственным программам повышения квалификации и профессиональной переподготовки, а также по курсам от омских организаций, на которых слушатели могут обучиться цифровым направлениям на коммерческой основе.

В результате анализа данных было выявлено, что в Омском регионе в государственных и частных вузах, а также в учреждениях среднего профессионального образования (СПО) осуществляется подготовка по 20-ти различным цифровым направлениям, среди которых по 17-ти направлениям – в высших учебных заведениях, а по 3-м направлениям – в техникумах и коллежах.

В свою очередь, на программах повышения квалификации и переподготовки в Омской области, доступ к которым предоставляется бесплатно (за счет средств бюджета) или и на коммерческой основе, слушатели могут выбрать любое из 177 различных цифровых направлений.

Определим наиболее популярные направления подготовки по цифровым специальностям в Омском регионе. Сперва представим на рисунке 1 рейтинг, сформированный по количеству поданных заявлений в государственные и частные вузы.

Рисунок 1 – Рейтинг направлений подготовки студентов по различным цифровым специальностям в государственных и частных вузах Омского региона (на основе данных о количестве заявлений, поданных на очную форму обучения за счет бюджетных и коммерческих ассигнований)

Как видно из данных на рисунке 1, топ-5 самых популярных среди абитуриентов направлений подготовки по цифровым специальностям в вузах охватывает следующий перечень: 09.03.01 «Информатика и вычислительная техника» (государственные ВУЗы – 2 727 заявлений); 09.03.03 «Прикладная информатика» (государственные ВУЗы – 2 264 заявления, частные ВУЗы – 8 заявлений); 10.03.01 «Информационная безопасность» (государственные ВУЗы – 2 257 заявлений); 09.03.02 «Информационные системы и технологии» (государственные ВУЗы –1 345 заявлений); 02.03.02 «Фундаментальная информатика и информационные технологии» (государственные ВУЗы – 657 заявлений).

Что касается заведений среднего профессионального образования в Омском регионе, то по аналогичному параметру абитуриенты выбирают другие ИТ-направления подготовки (рис. 2).

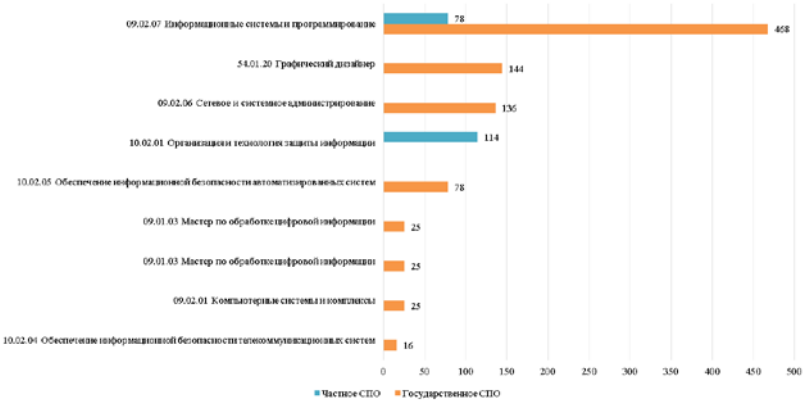


Рисунок 2 – Рейтинг направлений подготовки студентов по различным цифровым специальностям в государственных и частных учреждениях СПО Омского региона (на основе данных о количестве заявлений, поданных на очную форму обучения за счет бюджетных и коммерческих ассигнований)

Как показывают данные диаграммы на рисунке 2, топ-5 выбранных абитуриентами направлений подготовки по цифровым специальностям в Омских учреждениях СПО включает: 09.02.07 «Информационные системы и программирование» (468 заявлений, поданных в государственные учреждения СПО, 78 – в частные); 54.01.20 «Графический дизайнер» (144 заявления, поданных в государственные учреждения СПО);

09.02.06 «Сетевое и системное администрирование» (136 заявлений, поданных в государственные учреждения СПО); 10.02.01 «Организация и технология защиты информации» (114 заявлений, поданных в частные учреждения СПО); 10.02.05 «Обеспечение информационной безопасности автоматизированных систем» (78 заявлений, поданных в государственные учреждения СПО).

Также представим результаты анализа численности выпускников по различным направлениям в государственных и частных вузах, а также учреждениях СПО (рис.3).

Рисунок 3 – Рейтинг направлений подготовки студентов по различным цифровым специальностям в государственных и частных учреждениях СПО Омского региона (на основе данных о численности выпускников очной формы обучения за счет бюджетных и коммерческих ассигнований)

Согласно данным диаграммы на рисунке 3, топ-5 направлений подготовки по цифровым специальностям, которые в 2022 г. обеспечили вузам абитуриентов, уже имеющих базовую профессиональную подготовку, а также приток на рынок труда новых кадров (выпускников государственных и частных учреждений СПО) включает: 09.02.07 «Информационные системы и программирование» (332 выпускника в Омском регионе); 09.02.02 «Компьютерные сети» (76 выпускников в Омском регионе); 10.02.05 «Обеспечение информационной безопасности автоматизированных систем» (65 выпускников в Омском регионе); 09.01.03 «Мастер по обработке цифровой информации» (46 выпускников в Омском регионе); 09.02.03 «Программирование в компьютерных системах» (44 выпускника в Омском регионе).

Аналогичный анализ произведен на основе данных о выпускниках государственных и частных вузов Омского региона. Его результаты предоставлены на рисунке 4.

Рисунок 4 – Рейтинг направлений подготовки студентов по различным цифровым специальностям в государственных и частных вузах Омского региона (на основе данных о численности выпускников бакалавриата очной формы обучения за счет бюджетных и коммерческих ассигнований)

Согласно данным диаграммы на рисунке 4, топ-5 направлений подготовки по цифровым специальностям, которые в 2022 г. обеспечили приток на рынок труда новых профессиональных кадров (выпускников государственных и частных вузов) включает: 09.03.01 «Информатика и вычислительная техника» (116 выпускников в Омском регионе); 09.03.03 «Прикладная информатика» (111 выпускников в Омском регионе); 09.04.01 «Информатика и вычислительная техника» (88 выпускников в Омском регионе); 01.03.02 «Прикладная математика и информатика» (69 выпускников в Омском регионе); 09.03.02 «Информационные системы и технологии» (45 выпускников в Омском регионе).

Обсуждение результатов. Выявление приоритетных направлений подготовки по цифровым специальностям в Омском регионе одновременно с двух позиций – абитуриентов и государства – позволяет сопоставить, насколько потребности цифровой экономики (региональной и федеральной) могут быть обеспечены профессиональными кадрами.

Однако, наше исследование показало, что формально названия направлений профессиональной подготовки в учреждениях СПО и в вузах не соответствуют перечню основных сквозных цифровых технологий, утвержденных в рамках Программы «Цифровая экономика Россий-

ской Федерации». Следовательно, абитуриенты, выбирая для себя определенное направление, не могут сориентироваться, какие необходимые для государства и его цифрового суверенитета задачи они будут решать, когда пополнят рынок труда.

Выводы и заключение. Очевидно, что для эффективного выполнения Программы «Цифровая экономика Российской Федерации» требуется более глубокая специализация цифровых профессий. Кадры, необходимые для решения конкретных отраслевых задач, обеспечения нашей экономики сквозными цифровыми технологиями, должны проходить обучение на совместно создаваемых ресурсных базах учебных заведений и предприятий. В этом контексте, более тесное взаимодействие Министерства цифрового развития, связи массовых коммуникаций РФ с Министерством науки и высшего образования РФ может привести к оптимизации перечня направлений и профилей подготовки по цифровым специальностям, а также к повышению требований по интеграции профессионального образования с производственной деятельностью предприятий.

Библиографический список

1. Цифровая экономика Российской Федерации: программа: распоряжение Правительства Российской Федерации от 28 июля 2017 г. N 1632-р // Собрание законодательства Российской Федерации. 2017. № 32. Ст. 5138; Официальный интернетпортал правовой информации. URL: http://www.pravo.gov.ru (дата обращения: 03.08.2017).
2. Министерство цифрового развития и связи Омской области. URL: https://digital.omskportal.ru/oiv/digital (дата обращения: 11.12.2022).
3. Программа цифровой трансформации Омской области. URL: https://digital.omskportal.ru/magnoliaPublic/dam/jcr:15da8dd3-053e-428b-ad7b-f6fc83dc5868/PROGRAMMA%20CT%202021.pdf (дата обращения: 11.12.2022).
4. Балунова С. А. Информационно-образовательная среда подготовки IT-специалистов в системе среднего профессионального образования // Вестник ЧГПУ им. И.Я. Яковлева. 2012. №2-2. URL: https://cyberleninka.ru/article/n/informatsionno-obrazovatelnaya-sreda-podgotovki-it-spetsialistov-v-sisteme-srednego-professionalnogo-obrazovaniya (дата обращения: 11.12.2022).
5. Мировые тренды образования в российском контексте – 2023. URL: https://ioe.hse.ru/edu_global_trends/ (дата обращения: 11.12.2022).

УДК 337.004
М.И. Шубинский, к.т.н.,
НП ПРИОР Северо-Запад

МЕЖРЕГИОНАЛЬНЫЙ УЧЕБНО-МЕТОДИЧЕСКИЙ РЕСУРСНЫЙ ЦЕНТР ПО НАПРАВЛЕНИЮ «КИБЕРБЕЗОПАСНОСТЬ»

Аннотация
В настоящей работе рассмотрен принцип создания учебно-методического ресурсного центра по направлению «Кибербезопасность». Рассматриваются стоящие цели, задачи и краткое описание проекта.
Ключевые слова: кибербезопасность, учебно-методический центр, технические и кадровые риски, дистанционный курс по кибербезопасности.
Annotation
In this paper, the principle of creating an educational and methodological resource center in the direction of "Cybersecurity" is considered. The worthwhile goals, objectives and a brief description of the project are considered.
Key words: cybersecurity, educational and methodological center, technical and personnel risks, distance course on cybersecurity.

Введение.

Один из самых важных вопросов, стоящих сейчас перед любым государственным учреждением с точки зрения применения информационных технологий, – это вопрос информационной безопасности (кибербезопасности). Однако особенно остро этот вопрос стоит перед учреждениями среднего образования.

Риски, связанные с использованием сети Интернет, не ограничиваются опасностью заражения вирусами или хакерскими атаками. Проблема киберпреступности, защиты детей от информации, причиняющей вред здоровью и (или) развитию детей, а также не соответствующей задачам образования, особенно актуализирована в настоящее время. Проблемы, возникающие в связи с кибератаками и киберпреступностью, имеют далеко идущие последствия и должны решаться путем согласованной киберстратегии.

Школа должна выполнять все требования федерального законодательства по защите информации, например, 152–ФЗ «О персональных данных» и 149-ФЗ «Об информации, информационных технологиях и о защите информации». Однако, сотрудники школ (учителя, инженеры) не имеют должной квалификации в вопросах защиты информации.

Методические рекомендации по ограничению в образовательных организациях доступа обучающихся к видам информации, распространяемой посредством сети «Интернет», причиняющей вред здоровью и

(или) развитию детей, а также не соответствующей задачам образования, подготовленные Министерством образования и науки Российской Федерации в 2014 году, указывают, что в соответствии с Федеральным законом № 436-ФЗ (часть 1 статьи 14) должны проводиться организационно-административные мероприятия, направленные на защиту детей от информации, причиняющей вред их здоровью и (или) развитию. В том числе, мероприятия должны осуществляться по направлению «Повышение квалификации специалистов (руководителей) образовательных организаций и муниципальных органов управления образованием, ответственных за информатизацию по вопросам защиты детей от информации, причиняющей вред их здоровью и (или) развитию, распространяемой посредством сети «Интернет»»;

В качестве области практического использования и применения результатов выполнения проекта предлагается следующее.

Создание пилотного учебно-методического ресурсного центра по направлению кибербезопасность. Это позволит не только аккумулировать новейшие информационно-технологические и научно-методические ресурсы, предназначенные для повышения квалификации по направлению кибербезопасность, но и обеспечить условия устойчивой интеграции подобных межрегиональных центров в национальную систему образования России.

В рамках созданного пилотного учебно-методического ресурсного центра будет произведено объединение технических, технологических и кадровых ресурсов для дальнейшего роста Проекта, и, в том числе, будут разработаны новые и развиты имеющиеся подходы, технологии и методики дополнительного профессионального образования, в том числе, с использованием технологий дистанционного обучения, соответствующих международным стандартам. Будут сформированы материально-техническая и нормативная базы, необходимые для реализации проекта.

Цели и задачи, краткое описание проекта.

Цель проекта:

Повышение качества общего образования за счет повышения квалификации специалистов (руководителей) образовательных организаций и муниципальных органов управления образованием, ответственных за информатизацию по вопросам защиты детей от информации, причиняющей вред их здоровью и (или) развитию, распространяемой посредством сети «Интернет». Для реализации Проекта на первом этапе будет создан учебно-методический ресурсный центр по направлению кибербезопасность, с дальнейшим тиражированием опыта и результатов для увеличения зоны охвата регионов РФ. Созданный центр должен

быть оснащен необходимым программно-аппаратным обеспечением, и аккумулировать в себе научно-методические и информационно-технологические образовательные ресурсы по направлению кибербезопасность.

Задачи проекта:

Анализ современных тенденций и лучших образцов практики кибербезопасности;

SWOT – анализ массива имеющихся методических разработок по повышению квалификации специалистов по направлению информационная безопасность и кибербезопасность;

Разработка и адаптация учебных и информационных образовательных ресурсов по программам повышения квалификации для нужд специалистов (руководителей) образовательных организаций по направлению кибербезопасность;

Разработка дистанционных курсов повышения квалификации по направлению кибербезопасность, предназначенных для руководителей образовательной организации и специалистов органов управления образованием, для ответственных по информационной безопасности в образовательной организации, для педагогов, читающих курс кибербезопасность (или его аналог) учащимся образовательных организаций;

Разработка методических рекомендаций для тьютеров, которые будут организовывать повышение квалификации по направлению кибербезопасность на региональных площадках;

Создание единого образовательного Интернет-портала, предназначенного для дистанционного повышения квалификации по направлению кибербезопасность.

Создание библиотеки научных и методических материалов по вопросам кибербезопасности;

Содействие в диссеминации и тиражировании опыта, накопленного межрегиональным пилотным учебно-методическим ресурсным центром, в систему повышения квалификации в Российской Федерации и стран СНГ.

Краткое описание проекта

В настоящее время в регионах РФ практически нет ни положительного опыта адаптации курсов повышения квалификации по вопросам информационной безопасности для нужд образовательных организаций, ни опыта повышения квалификации специалистов (руководителей) образовательных организаций и муниципальных органов управления образованием, ответственных за информатизацию по вопросам защиты детей от информации, причиняющей вред их здоровью и (или) разви-

тию, распространяемой посредством сети «Интернет». Для создания подобных положительных практик, объединяемых термином кибербезопасность, предлагается создать пилотный межрегиональный учебно-методический ресурсный центр, который бы занялся адаптацией существующих программ, апробированием их на практике и внедрением этих программ в ряде регионов России.

В дальнейшем практику создания подобных ресурсных центров можно будет распространить и на остальные Федеральные округа.

Планируемые работы.

Анализ нормативно-правовой базы, регламентирующей вопросы информационной безопасности в образовательных организациях и защиту детей от информации, причиняющей вред их здоровью и (или) развитию.

Анализ современных тенденций и лучших образцов практики кибербезопасности;

SWOT – анализ массива имеющихся методических разработок по повышению квалификации специалистов по направлению информационная безопасность и кибербезопасность;

Анализ имеющихся методических разработок по повышению квалификации специалистов по направлению информационная безопасность и кибербезопасность и выделение успешных «практик».

Разработка и адаптация учебных и информационных образовательных ресурсов по программам повышения квалификации по направлению кибербезопасность, предназначенных для ответственных по информационной безопасности в образовательной организации.

Разработка учебного плана курсов дистанционного повышения квалификации по направлению кибербезопасность.

Разработка рабочих программ дистанционных курсов повышения квалификации по направлению «кибербезопасность».

Разработка методических рекомендаций для тьютеров, которые будут организовывать повышение квалификации по направлению кибербезопасность на региональных площадках.

Определение мест проведения апробации дистанционных курсов повышения квалификации по направлению «кибербезопасность».

Создание единого образовательного Интернет-портала, предназначенного для дистанционного повышения квалификации по направлению кибербезопасность.

Создание библиотеки научных и методических материалов по вопросам кибербезопасности.

Создание дистанционных курсов по разработанным программам повышения квалификации по направлению кибербезопасность

Проведение апробации дистанционных курсов на специалистах (руководителях) образовательных организаций, одного из регионов России (например, Северо-Запад).

Проведение обучения тьютеров, которые будут организовывать повышение квалификации по направлению кибербезопасность на региональных площадках.

Анализ и обобщение опыта создания межрегионального пилотного учебно-методического ресурсного центра по направлению кибербезопасность.

Подготовка отчета по результатам работы межрегионального пилотного учебно-методического ресурсного центра по направлению кибербезопасность.

В качестве индикаторов результативности проекта могут быть выбраны следующие показатели

- Доля специалистов преподавательского и управленческого корпуса системы дошкольного и общего образования, обеспечивающих распространение современных моделей доступного и качественного образования, а также моделей региональных и муниципальных образовательных систем, обеспечивающих государственно-общественный характер управления образованием, в общей численности специалистов преподавательского и управленческого корпуса системы дошкольного и общего образования
- Доля учителей, эффективно использующих современные образовательные технологии (в том числе информационные коммуникационные технологии) в профессиональной деятельности, в общей численности учителей.

Библиографический список

1. Распоряжение Правительства РФ от 02.12.2015 № 2471-р «Об утверждении Концепции информационной безопасности детей»
2. Федеральный закон Российской Федерации от 29 декабря 2010 г. N 436-ФЗ «О защите детей от информации, причиняющей вред их здоровью и развитию».
3. Чернобай Е.В. Современное понимание учебного процесса в информационно-образовательной среде// Справочник заместителя директора школы. 2013. №11. С. 69 -74.
4. Шубинский М.И. Информационная безопасность школы//Вестник ОГУ. 2013. №1 С. 108-112.

УДК 004.4
Д.В. Шиленков, ведущий инженер-программист
ФГБОУ ВО «Югорский государственный университет»

РАЗРАБОТКА ЛИЧНОГО КАБИНЕТА СТУДЕНТА ЮГОРСКОГО ГОСУДАРСТВЕННОГО УНИВЕРСИТЕТА

Аннотация
В статье дано описание процесса разработки и модернизации личного кабинета студента Югорского государственного университета.
Ключевые слова: личный кабинет студента, цифровые сервисы университета.
Annotation
The article describes the process of development and modernization of the personal account of Yugra State University's student.
Key words: student's personal account, university digital services.

Первый личный кабинет студента в Югорском государственном университете был введен в эксплуатацию в 2016 году. Сервис был написан на языках программирования PHP и JavaScript. У всех студентов под рукой оказались: персональная информация, расписание занятий, отметки за промежуточные аттестации, новости университета и даже ежедневное меню столовой. Кроме того, студенты могли видеть размеры стипендий, карту учебных корпусов, и список всех работающих на базе университета творческих коллективов. Опыт применения цифровых технологий для взаимодействия со студентами оказался очень успешным, но выбранная архитектура лишила сервис масштабируемости и гибкости.

В 2019 году началась разработка новой версии личного кабинета. В этот раз в качестве фреймворка был выбран Laravel. Клиентская часть разрабатывалась с использованием фреймворков Bootstrap и VueJs. Портал был организован на основе модульной архитектуры, по принципам SOLID, Dry, Kiss.

В начале 2020 года на портале начал работу сборщик Webpack, что позволило сократить объемы данных, загружаемых пользователями и реализовать систему ленивой загрузки. Также было принято решение разрабатывать микросервисы с использованием фреймворка Vuetify. С августа 2022 года, разработка сервисов осуществляется на фреймворке VueJs v3, некоторые микросервисы используют вебсокеты для обмена информацией.

За прошедшее время портал значительно вырос и взял на себя автоматизацию процессов не только учебной, но и административной, научной и финансово-экономической деятельности. Портал обзавелся

собственным API и теперь может выступать сервером авторизации для других информационных систем университета. На серверной стороне портала работают джобы, которые выполняют рутинную работу по обновлению и интеграции данных с другими системами. Также для серверных задач, которые слишком тяжело решить средствами PHP, рядом с Laravel развернута система на фреймворке Django. Интерфейс личного кабинета студента версии 2022 года представлен на рисунке 1.

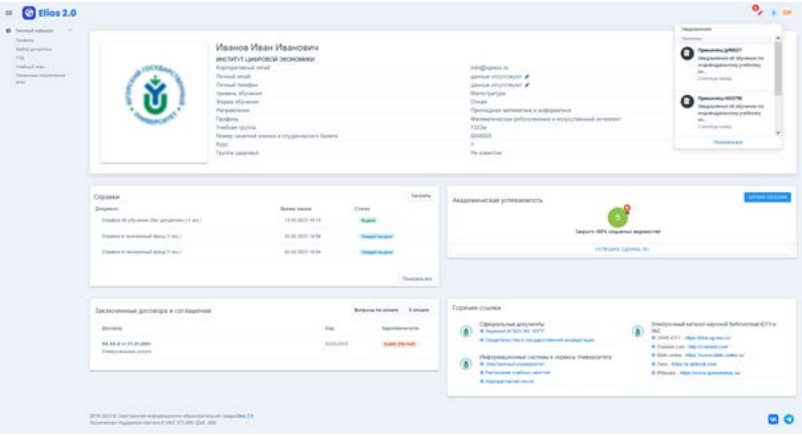


Рисунок 1 – Личный кабинет студента ЮГУ

В 2022 году личный кабинет мигрировал на компонентную верстку. Такой подход, сделал его в 14 раз легче, при этом увеличил его гибкость. Сейчас портал включает в себя немного более 100 микросервисов, при этом сохраняется его первоначальная гибкость, а проработанные в 2019 году системы модульности и ролевой политики не претерпевали изменений и удачно справляются со своими задачами. Посещаемость личного кабинета студентами с каждым годом увеличивается, а это означает, что портал развивается в правильном направлении.

ИСКУССТВЕННЫЙ ИНТЕЛЛЕКТ И ТЕХНОЛОГИИ «УМНОГО ГОРОДА»

УДК: 004

Ю.В.Аникин, к.х.н., доцент, В. И.Шилков, к.э.н., доцент
ФГАОУ ВО «Уральский федеральный университет имени первого Президента России Б.Н. Ельцина»
Мира, ул., 19, Екатеринбург, Россия, 620002
e-mail: anikin-urfu@yandex.ru

ИСКУССТВЕННЫЙ ИНТЕЛЛЕКТ И УПРАВЛЕНИЕ ВОДОСНАБЖЕНИЕМ В УМНОМ ГОРОДЕ

Аннотация
В статье обосновывается необходимость применения искусственного интеллекта в системах водоснабжения умных городов.
Ключевые слова: умный город, водоснабжение, интернет вещей искусственный интеллект.
Abstract
The article substantiates the need for the use of artificial intelligence in the water supply systems of smart cities.
Key words: smart city, water supply, internet of things, artificial intelligence.

К критическим жизненно важным системам городского хозяйства, наряду с системами электро-, газо- и теплоснабжения относится система водоснабжения и водоотведения. Глобальный водный кризис, уже затронувший многие страны мира, заставил обратиться не только к сбору дождевой воды, но и технологиям водной циркуляции, применяемым для обеспечения повторного и оборотного использования водных ресурсов. Проблема дефицита водных ресурсов обсуждается в научной печати и на международных конференциях и является актуальной и для Российской федерации, большая часть населения которой проживает в городах. Вместе с тем, многие существующие централизованные системы водоснабжения не соответствуют современным технологическим, экономическим и экологическим требованиям, необходимым для достижения целей устойчивого развития городов [1-2]. Адекватная политика управления водными ресурсами также предполагает разработку эффективных методик отраслевого промышленного мониторинга для отслеживания качества сточных вод.

Решение оперативных и стратегических задач эффективного распределения и управления водными ресурсами при условии обеспечения качества воды, а также при необходимости учета большого количества

различных параметров и факторов и соблюдения экономических, экологических социальных требований невозможно без внедрения информационно-коммуникационных систем и технологий. Решение актуальных проблем водного хозяйства городов требует применения технологий интернета вещей (IoT), обработки больших массивов данных (Big Data) и внедрения систем искусственного интеллекта. С помощью интеллектуальных систем и алгоритмов глубокого машинного обучения могут быть решены задачи определения и устранения утечек воды, мониторинг расходов, их чрезмерного значения, сброса загрязнений, превышающих установленные нормативы. Инфраструктура распределения воды, которая может быть смоделирована с помощью интеллектуальных алгоритмов, сможет поддерживать эффективное распределение безопасного и устойчивого водоснабжения среди населения и промышленных объектов, социальной инфраструктуры. В настоящей работе предлагается концептуальная многоступенчатая модель информатизации и автоматизации процессов управления водными ресурсами, используемыми для хозяйственно-питьевых нужд. На первой ступени располагаются датчики качества воды и сенсорные сети, которые используются для обнаружения утечек воды. Вторая ступень модели используется для сбора данных. Третья ступень хранит всю информацию: качество и количество потребляемой воды для различных точек потребления, утечки воды. Такая модель может быть использована для глубокого обучения искусственного интеллекта и стать частью более развитой системы управления водным хозяйством города.

Библиографический список

1. Schaffer, D., Vollmer, D., 2010. Pathways to urban sustainability: research and development on urban systems. In: Summary of a Workshop. National Academies Press, Washington D.C., United States. https://www.researchgate.net/publication/260312138_Pathways_to_urban_sustainability_Research_and_development_on_urban_systems

2. Burn, S., Maheepala, S., Sharma, A., 2012. Utilising integrated urban water management to assess the viability of decentralized water solutions. Water Sci. Technol. 66 (1), 113e121. https://www.researchgate.net/ publication/225283196_Utilising_integrated_urban_water_management_to_assess_the_viability_of_decentralised_water_solutions

УДК 656.072.6: 519.872
А.С. Свистунова, младший научный сотрудник
Санкт-Петербургский Федеральный исследовательский центр Российской академии наук,
Россия, Санкт-Петербург
e-mail: svistunova_alexandra@bk.ru

УПРАВЛЕНИЕ АГЕНТАМИ В ИМИТАЦИОННОМ МОДЕЛИРОВАНИЕ УМНЫХ ГОРОДОВ

Аннотация
Научные исследования в области технологий умных городов направлены на использование их ресурсов для улучшения качества жизни людей. Также можно использовать различные виды управляющих сигналов от массивных систем и устройств, например, системы светофоров в умных городах. Сложно собрать массивную базу данных сигналов управления, поскольку в реальных условиях это требует значительных усилий и времени. В этой работе предлагается генеративная модель, объединяющая модели долговременной памяти и состязательную сеть (LSTM-GAN) для генерации сигналов управления агентами.
Ключевые слова: логистика, имитационное моделирование, умный город, агенты, транспорт, управление сигналом.
Abstract
Scientific research on smart city technology is aimed at using its resources to improve the quality of life of people. Various kinds of control signals from massive systems and devices, such as traffic light systems in smart cities, can also be used. It is difficult to collect a massive database of control signals because it requires considerable effort and time in the real world. This paper proposes a generative model that combines long-term memory models and an adversarial network (LSTM-GAN) to generate agent control signals.
Keywords: logistics, simulation modeling, smart city, agents, transportation, signal management.

Введение

Информационные и коммуникационные технологии (ИКТ) играют важную роль в развитии умных и устойчивых городов, которые представляют собой всеобъемлющую структуру, включающую не только физическую инфраструктуру, но и человеческие и социальные факторы [1]. Умные города являются одной из основных тем исследований, основанных на технологии Интернета вещей (IoT) [2]. В частности, приложения умных городов требуют различных интегрированных алгоритмов [3]. Разнообразные ресурсы умных

городов анализируются и используются с помощью таких технологий, как IoT, большие данные, социальные сети и облачные вычисления, которые улучшают качество жизни горожан [4]. В настоящее время развитие умных городов включает в себя разработку и внедрение систем транспорта, энергетики, управления движением, безопасности и других областей [5]. Стоимость физической установки этих систем очень высока как с точки зрения денег, так и ресурсов.

Трудно оценить эффективность моделей и технологий, разработанных для умных городов [6]. Например, управление дорожным движением является одной из важных тем, рассматриваемых в исследованиях умных городов. Оценить различные модели и технологии сложно, когда в разных городах применяются различные интеллектуальные системы управления дорожным движением [7]. Поэтому для проверки моделей и технологий создаются имитационные среды [8]. В средах моделирования необходимо учитывать поведение и движения людей. Например, очень большие затраты потребуются при тестировании системы, используемой для обнаружения и отслеживания движения пешеходов. Методы симуляции помогают спроектировать такую систему, значительно снижая затраты; однако есть и недостаток, заключающийся в том, что для создания среды симуляции необходимо собрать управляющие сигналы от различных агентов. Хотя среда моделирования снижает затраты на сбор данных в эксперименте, для создания среды моделирования необходимы некоторые базовые данные для формулирования правил для агента.

Моделирование умного города

В нескольких предыдущих исследованиях по умным городам проводились междисциплинарные исследования по разработке виртуальных городов с транспортом, энергетикой [9, 10] и т.д. Тема "умных городов" все еще сталкивается с некоторыми проблемами при ее реализации, но было проведено больше исследовательских проектов по реализации "умных городов". Между тем, недавно был предложен фотореалистичный метод моделирования трехмерного города для обучения автономных транспортных средств в симуляции умного города. Методы глубокого обучения, такие как конволюционные нейронные сети (CNN), также широко применяются для моделирования поведения различных агентов и транспортных систем в реальном мире [11]

В будущих умных городах новые информационные и коммуникационные технологии будут лучше управлять городскими ресурсами. Инфраструктура интеллектуальной энергосистемы превращается в сложную систему. Такая система может контролировать

и управлять производством и потреблением энергии в энергосистеме для повышения энергоэффективности.

Для создания динамического поведения умных городов построен симулятор на основе программных агентов. Он также моделирует дискретные гетерогенные устройства, которые производят и потребляют энергию. Таким образом, "умные города используют множество технологий для улучшения реализации услуг транспортных, энергетических и дорожных систем, что приводит к повышению уровня комфорта для их жителей. При моделировании услуг умного города технология, имеющая значительный потенциал — это анализ больших данных. Важнейшей частью системы моделирования для обучения автономных агентов является генерация различных реальных ситуаций на основе данных, полученных из реального мира.

LSTM и GAN

Перечислим некоторые преимущества объединения моделей LSTM и GAN для автоматической генерации управляющих сигналов. Параллельно обсуждается производительность LSTM-GAN путем сравнения сигналов управления, генерируемых GAN, с сигналами управления, имеющимися в базах данных.

Очевидно, что GAN достигли значительного успеха в компьютерном зрении в отношении создания реалистичных изображений. Опираясь на этот успех, недавно GAN изображений были расширены на такие задачи, как увеличение объема данных. Когда генератор на основе LSTM используется в качестве генераторной сети в GAN, вектор скрытого шума представляет собой входное скрытое состояние LSTM, а выход генератора - выходная сентенция, выдаваемая LSTM. [1]

Управляющие сигналы, генерируемые LSTM-GAN, имеют формат, включающий выражения времени, действия и места в последовательном порядке. Они имеют хорошо упорядоченную структуру по сравнению с управляющими сигналами

Таким образом, управляющие сигналы агентов, созданные на основе этого метода, могут быть использованы в имитационном эксперименте, что значительно повысит эффективность обучения.

Заключение

Сигналы управления агентами, сгенерированные с помощью предложенного метода, должны быть применены для последующего имитационного эксперимента, чтобы они соответствовали анимации в имитационном эксперименте. Управляющие сигналы агентов, созданные на основе предложенного метода, использовались в

имитационном эксперименте, что повысило эффективность обучения [12].

Предлагаемые сигналы управления агентами представляют собой набор данных для моделирования пешеходов в реальном времени в неконкретных местах или местах без адресов, которые являются общими факторами в общем моделировании дорожного движения. Чтобы убедиться, что новые разработанные сигналы управления агентами способны справиться с моделированием пробок в умном городе, нам необходимо модифицировать предложенную структуру данных для моделирования потоков людей и транспортных средств в конкретных местах. Для этого необходимо более детально определить движение людей, а именно, интегрировать места с определенными адресами в существующие дорожные сети для моделирования пешеходов в реальном времени [13]. В будущем нам необходимо создать набор данных о дорожном движении, основанный на новых данных, для моделирования движения пешеходов, на основе более четко сформулированных эмпирических данных.

Библиографический список

1. Bibri S.E. A foundational framework for smart sustainable city developmrnt: theoretical, disciplinary and discursive dimensions and their synergies. Sustain Cities Soc 38:758-794 – 2018.
2. Искандеров, Ю. М. Мультиагентная модель управления беспилотной снегоходной транспортной платформой при решении практических задач / Ю. М. Искандеров, Д. Ю. Андрианов, Ю. С. Андрианов // Вестник Поволжского государственного технологического университета. Серия: Материалы. Конструкции. Технологии. – 2020. – № 3. – С. 35-42. – DOI 10.25686/2542-114X.2020.3.35.
3. Хасанов Д.С., Свистунова А.С. – Оценка эффективности обслуживания пассажиров в аэровокзальном комплексе. – Транспорт России: Проблемы и перспективы -2020. – 32 с.
4. Искандеров Ю.М., Свистунова А.С., Хасанов Д.С., Чумак А.С. - Интеллектуальная поддержка принятия решений в логистических системах. – Морские интеллектуальные технологии т.1 №2. 2021. – 145 с.
5. Svistunova, A. S. Using the AnyLogic software product in modeling the passenger traffic of a railway station / A. S. Svistunova // Computing, Telecommunications and Control. – 2020. – Vol. 13. – No 4. – P. 54-65. – DOI 10.18721/JCSTCS.13405.
6. Юсупов Р.М., Микони С.В., Соколов Б.В. Методология оценивания качества моделей и полимодельных комплексов. В сборнике: Перспективные направления развития отечественных информационных

технологий. Сборник научных трудов пятой межрегиональной научно-практической конференции. Севастополь, 2019. С. 13-14.
7. Свистунова, А. С. Возможности автоматических транспортеров-погрузчиков и их использование при создании имитационной модели развития контейнерного терминала / А. С. Свистунова, Д. С. Хасанов // Морские интеллектуальные технологии. – 2020. – № 4-1(50). – С. 169-174. – DOI 10.37220/MIT.2020.50.4.023.
8. Искандеров, Ю. М. Моделирование транспортно-технологических процессов в цепях поставок на основе мультиагентных технологий / Ю. М. Искандеров, М. Б. Ласкин // Перспективные направления развития отечественных информационных технологий: материалы V межрегиональной научно-практической конференции, Севастополь, 24–28 сентября 2019 года / Севастопольский государственный университет; Санкт-Петербургский институт информатики и автоматизации РАН. – Севастополь: Федеральное государственное автономное образовательное учреждение высшего образования "Севастопольский государственный университет", 2019. – С. 71-74.
9. Concept and Models of Information Application for Actions in Systems / A. Geyda, L. Fedorchenko, I. Lysenko [et al.] // Conference of Open Innovations Association, FRUCT. – 2022. – No 31. – P. 407-415.
10. Хасанов, Д. С. Технология сбора данных в логистике / Д. С. Хасанов, А. С. Свистунова // Системный анализ в проектировании и управлении: сборник научных трудов XXV Международной научной и учебно-практической конференции в 3 ч., Санкт-Петербург, 13–14 октября 2021 года. – Санкт-Петербург: Политех-Пресс, 2021. – С. 275-279. – DOI 10.18720/SPBPU/2/id21-377.
11. Iskanderov, Y. Comprehensive Intelligent Information Security Management System (CIISMS) for Supply Networks: The Actor-Network Perspective / Y. Iskanderov, M. Pautov // Advances in Intelligent Systems and Computing. – 2020. – Vol. 1294. – P. 130-142. – DOI 10.1007/978-3-030-63322-6_10. – EDN BCKIVY.
12. Svistunova, A. S. Improving the efficiency of traffic management in a metropolis based on computer simulation / A. S. Svistunova, D. S. Khasanov // Computing, Telecommunications and Control. – 2021. – Vol. 14. – No 3. – P. 33-42. – DOI 10.18721/JCSTCS.14303.
13. Хасанов, Д. С. Технология сбора данных в логистике / Д. С. Хасанов, А. С. Свистунова // Системный анализ в проектировании и управлении: сборник научных трудов XXV Международной научной и учебно-практической конференции: в 3 ч., Санкт-Петербург, 13–14 октября 2021 года. – Санкт-Петербург: Политех-Пресс, 2021. – С. 275-279. – DOI 10.18720/SPBPU/2/id21-377.

УДК: 004.78
В. И. Шилков, к.э.н., доцент, Б.П. Гуаман Вела, студент
ФГАОУ ВО Уральский федеральный университет имени первого Президента России Б.Н. Ельцина
Мира, ул., 19, Екатеринбург, Россия, 620002
e-mail: vi.shilkov@urfu.ru

ИСКУССТВЕННЫЙ ИНТЕЛЛЕКТ, ОБЛАЧНЫЕ И ТУМАННЫЕ ВЫЧИСЛЕНИЯ В УМНОМ ГОРОДЕ

Аннотация
В статье обосновывается необходимость разработки многоуровневых архитектур умных городов на основе облачных и туманных вычислений, интернета вещей и искусственного интеллекта. Обозначены основные функциональные направления и риски, связанные с применением искусственного интеллекта в умных городах.
Ключевые слова: умный город, облако, туман, искусственный интеллект, интернет вещей.
Abstract
The article substantiates the need to develop multi-level architectures of smart cities based on cloud and fog computing, the Internet of Things and artificial intelligence. The main functional areas and risks associated with the use of artificial intelligence in smart cities are outlined.
Key words: smart city, cloud, fog, artificial intelligence, Internet of things.

Согласно оценкам Gartner, Inc., ожидается, что в 2025 году, 51% расходов на ИТ в сферах услуг, бизнес-процессов, системной инфраструктуры, а также прикладного программного и инфраструктурного программного обеспечения переместится с традиционных решений на облачные технологии и на которые будут переориентированы, в том числе, почти две трети (65,9%) корпоративных расходов на прикладное программное обеспечение по сравнению с 57,7% в 2022 году. Экономическая целесообразность применения облачных технологий обусловлена, в первую очередь, снижением затрат на закупку программных средств, серверного и сетевого оборудования, возможностью быстрого увеличения вычислительных мощностей и оперативного синтеза новых технологий для расширения круга решаемых задач [1].

Применение облачных технологий следует считать целесообразным и для управления функциональными подсистемами умных городов (Smart City). Традиционная модель удаленного управления в умных городах предполагает облачную обработку данных полученных от большого количества датчиков являющихся неотъемлемой частью системы,

называемой интернетом вещей (IoT). Вместе с тем, на смену традиционной двухуровневой IT архитектуре (“IoT”- “Cloud”), должна прийти трехуровневая архитектура (“IoT”-“Fog”-“Cloud”), имеющая в своем составе уровень “туманных вычислений”, глобальный рынок которых, к 2025 году может превысить 700 миллионов USD [2].

Создание трехуровневой архитектуры, предполагающей уровень туманных вычислений, является целесообразным для важнейших подсистем умного города, к которым, относятся, например, подсистемы управления: городским транспортом; водоснабжением; вывозом твердых коммунальных отходов; энергопотреблением (Smart Energy), элементом которых является, применяемый в различных отраслях Интернет вещей (IoT). Именно трехуровневая архитектура умного города, позволяющая уменьшить нагрузку на облачный уровень управления, может стать основой для осуществления интеллектуального и эффективного управления. Вместе с тем, в связи с ожидаемым применением инструментов искусственного интеллекта для управления умными городами, необходимо разработать не только трехуровневые, но и многоуровневые варианты, как централизованных, так и децентрализованных IT архитектур умного города, важным элементом, которых может выступить еще и уровень интеллектуального принятия решений. Однако, следует принять во внимание, что новые архитектурные решения могут приводить к появлению новых рисков, связанных, например, с угрозами кибербезопасности, с уязвимостью и неконтролируемым развитием искусственного интеллекта, что может приводить к непредсказуемым управленческим последствиям.

Библиографический список

1. Кашаева В.А., Агафонова В.В. Характерные черты использования облачных технологий в различных сферах применения. Известия Института систем управления СГЭУ. 2021.№1(23). С. 130-133.
2.Бурый А.С. Облачные вычисления в цифровой трансформации информационных технологий. Правовая информатика. 2021.№ 2. С. 4-14

ФУНДАМЕНТАЛЬНЫЕ ПРОБЛЕМЫ РАЗВИТИЯ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ

УДК 517.98: 519.2.621.033

В.А. Острейковский, д-р техн. наук, профессор, А.В. Сорочкин
Сургутский Государственный Университет

О НОВОМ ПОДХОДЕ К УЧЁТУ АСИММЕТРИИ ВНУТРЕННЕГО ВРЕМЕНИ ПРИ ОЦЕНКЕ РЕСУРСА СТРУКТУРНО И ФУНКЦИОНАЛЬНО СЛОЖНЫХ СИСТЕМ С ДЛИТЕЛЬНЫМИ СРОКАМИ АКТИВНОГО СУЩЕСТВОВАНИЯ

Аннотация

В статье рассмотрены современные математические методы и модели в теории долговечности, повышающие достоверность оценок и анализа показателей срока службы макроскопических сложных критически важных систем.

Ключевые слова: долговечность; ресурс; срок службы или остаточные значения; неустойчивость; необратимые процессы; асимметрия времени.

Annotation

The article deals with modern mathematical methods and models in the theory of durability, that increase the reliability of estimates and analysis of lifetime indicators of macroscopic complex critical systems.

Key words: durability; resource; service life or residual values; instability; irreversible processes; asymmetry of time.

Введение

Существующие в настоящее время методы и модели оценки и анализа показателей долговечности ресурса, срока службы и их остаточных значений структурно и функционально сложных систем (СФСС) основаны на хорошо развитых теориях длительной прочности и не учитывают эффект асимметрии времени в модусах «прошлое – настоящее - будущее» сложных комплексов с длительными сроками активного существования. В первую очередь это относится к системам типа наземных, плавучих и подвижных ядерных энергетических установок, космических аппаратов, магистральных трубопроводов нефти и газа и других критически важных комплексов. Причем модели долговечности обязательно должны учитывать особенности неустойчивостей и необратимых процессов и весь комплекс природных и эксплуатационных факторов. [1-3]

Именно поэтому целью предлагаемой статьи является дальнейшее уточнение современных математических методов и моделей, повышающих достоверность оценок и анализа показателей долговечности макроскопических сложных критически важных систем.

1. Анализ современного состояния исследования теории долговечности СФСС

Подавляющее большинство работ в области теории долговечности сложных систем как в нашей стране, так и за рубежом, в настоящее время базируются на результатах исследований, выполненных во второй половине XX века и получивших дальнейшее развитие на идеях классической механики (В.В. Болотина «Ресурс машин и конструкций» / М.: Машиностроение, 1990. -448 с., В.В. Болотина «Прогнозирование ресурса машин и конструкций» / М.: Машиностроение, 1984. – 312 с., А.С. Проников «Надежность машин» / М.: Машиностроение, 1978. -592 с., Дж. Богданофф и Ф. Козин «Вероятностные модели накопления повреждений» / Пер. с англ. – М.: Мир, 1989. -344 с., Н.А. Махутов «Научные проблемы безопасности техногенной сферы» // Проблемы машиностроения и надежности машин – 1999. - №1 – С.109-116, А.Ф. Гетман «Ресурс эксплуатации сосудов и трубопроводов атомных станций» / М.: Энергоатомиздат, 2000, А.В. Антонов, В.А. Острейоквский «Ресурс и срок службы энергоблоков атомных станций» / Москва: Инновационное машиностроение, 2017. -553 с.).

Следует сказать, что в рассматриваемый период XX века в проблеме оценки и прогнозирования ресурса машин на основе методологии исследования длительной прочности были систематизированы огромное количество теоретического и экспериментального материала, что нашло отражение в нормативной документации по этой проблеме, как например, в «Нормах расчета на прочность оборудования и трубопроводов атомных энергетических установок». [4]

Многочисленные исследования в приведенных работах свидетельствуют, что неустойчивость и необратимые процессы имеют свои особенности на трех уровнях описания систем: субмикроскопическом, микроскопическом и макроскопическом. Установлено, что причина сложных деградационных процессов, приводящих в итоге к отказам, авариям и катастрофам СФСС, являются коррозия, эрозия, износ, усталость, деформации и другие макроскопические процессы. В указанных и других макропроцессах первопричиной служат необратимые процессы типа химических реакций, диффузии, распада твердых растворов, адсорбции и т.п. Причем необратимые процессы обычно развиваются и прогрессируют под действием комплекса внутренних и внешних эксплуатационных факторов внешней среды (температуры, влажности,

давления, динамических и статических механических нагрузок, термогидравлических ударов, облучения, воздействия электрических, магнитных и других полей, а также влияние человеческого фактора.

Необходимо обязательно подчеркнуть, что большим достижением теории прогнозирования ресурса, срока службы и их остаточных значений является получение в XX века аналитических выражений для математических моделей деградации конструкционных материалов оборудования СФСС. В качестве примеров некоторые их них приведены в таблицах 1-4.

Таблица 1 – Модели процессов старения конструкционных материалов сложных систем на субмикроскопическом и микроскопическом уровнях

№	**Физико-химический процесс**	**Модель процесса**
1	Диффузия	$\mathrm{D}(T^0) = D_0 exp\left(-\frac{E_a}{R_1 T^0}\right)$
2	Химические реакции	$C = C_0 e^{-k_p T^0}, \quad k_p = k_{p0} exp\left(-\frac{E_a}{R_1 T^0}\right)$
3	Рекристаллизация твердого тела	$\frac{dx}{dt} = k^*(1-x) exp\left(-\frac{E_a}{R_1 T^0}\right)$
4	Распад твердых растворов	$\frac{C_1 - C_2}{C_3 - C_2} = \exp(-at^b)$
5	Фазовые превращения в твердых телах	$n = a_1 e^{-\frac{E_a}{R_1 T^0}} e^{-\frac{a_2}{T^0} - \frac{\gamma^3}{(\Delta T^0)}}$
6	Распад мартенситной структуры в закаленных сталях	$V = a_3 V_0 \left[1 - exp\left(-te^{-\frac{E_a}{R_1 T^0}}\right)\right]$
7	Удельная электропроводность	$\sigma_э = \sigma_{э0} exp(-\alpha_T T^0)$
8	Удельная электропроводность диэлектриков	$\sigma_э = \sigma_{э0} exp(a_4 E)$

9	Диэлектрическая проницаемость	$\varepsilon_{\text{п}} = \varepsilon_{\text{п0}} exp(\alpha_{E\text{п}} T^0)$
10	Напряженность электрического поля при тепловом пробое	$E_{\text{кр}} = E_{\text{кр0}} exp(-\alpha_E T^0)$
11	Электрическая прочность	$E_{\text{пр}} = E_{\text{пр0}} - a_5 \sigma_{\text{м}}^{b_1}$

Примечание:

$t -$ время;
$D(T^0) -$ коэффициент диффузии;
$T^0 -$ абсолютная температура;
$D_0 -$ коэффициент диффузии при $T = 0\ °C$;
$E_a -$ энергия активации;
$R_1 -$ универсальная газовая постоянная;
$\text{C} -$ концентрация вещества;
$\text{C}_0 -$ начальная концентрация исходного вещества;
$k_p -$ константа скорости химической реакции;
$\frac{dx}{dt} -$ скорость рекристализации;
$k^* -$ коэффициент, зависящий от материала;
$\text{C}_1 -$ концентрация оставшихся в растворе частиц;
$\text{C}_2 -$ концентрация примесей на границе зародыша;
$\text{C}_3 -$ концентрация примесей на достаточно большом удалении от зародышей;
$a -$ коэффициент, характеризующий число и объем зародышей;
$n -$ число циклов кристаллизации;
$V -$ объем материала;
$\gamma -$ коэффициент поверхностного натяжения;
$\sigma_{\text{э0}} -$ удельная электрическая проводимость при $T = 0\ °C$;
$\alpha_T, \alpha_{E\text{п}}, \alpha_E -$ температурные коэффициенты;
$E -$ напряженность электрического поля;
$\varepsilon_{\text{п0}} -$ начальная диэлектрическая проводимость при $T = 0\ °C$;
$E_{\text{кр0}} -$ напряженность электрического поля при пробое для $T = 0\ °C$;
$\sigma_M -$ механическое напряжение;
$E_{\text{пр0}} -$ напряженность электрического поля при пробое для $\sigma_M = 0$;

$2l$ – длина трещины.

Таблица 2 – Модели процессов, приводящих в потере работоспособности элементов конструкций СФСС на макроскопическом уровне

№	Процесс	Модель процесса
1	Рост трещин в твердых телах	$\frac{dl}{dN} = A\Delta K_I^n, \ \frac{dl}{dN} = C\Delta K_I^n;$ $b(t) = exp\left[lnb_{\text{кр}} - \frac{t}{\alpha}\left(\frac{\sigma_{\text{ср}}}{R^T_{\rho 0,2}}\right)^2\right]$
	Деформация твердого тела под напряжением	$\dot{\varepsilon} = \dot{\varepsilon_0} exp\left(-\frac{\Delta G}{R_1 T^0}\right)$
3	Ползучесть	$\dot{\varepsilon} = \alpha exp\left(-\frac{E_a}{R_1 T^0}\right)$
4	Начальная стадия ползучести	$\dot{\varepsilon} = \dot{\beta} t^m$
5	Изменение относительного удлинения	$\dot{\varepsilon} = \frac{\sigma_m}{E_1} + \frac{\sigma_m}{E_2}\left(1 - e^{-t/\tau}\right) + \frac{\sigma_m}{\eta_r}$
6	Вязкость при запаздывающей упругой деформации	$\eta_1 = A_1 exp\left(\frac{\Delta E_a}{R_1 T^0}\right)$
7	Вязкость при течении материала	$\eta_2 = B exp\left(\frac{\Delta E_a}{R_1 T^0}\right)$
8	Старение полупроводниковых ферромагнетиков	$\Delta\mu(t) = \Delta\mu_{max} \frac{1 - e^{ut}}{1 - \omega e^{ut}}$

9	Старение конденсаторов	$I_{\text{ут}}(t) = I_{\text{ут}\,max}[1 - exp(-k_1 t^{n_1})]$
10	Старение терморезисторов	$\Delta R(t) = \Delta R_{max}[1 - exp(-k_1 t^{n_1})]$
11	Старение терморезисторов при одновременном протекании процессов диффузии примесей и химических реакций в рабочем материале	$\Delta R(t) = a + bexp(-ct);$ $\Delta R(t) = a_1 - \frac{b_1}{(t+d)^{n_1}}$
12	Скорость коррозии	$\frac{dy}{dt} = C_0 k_p exp(\alpha_1 T^0)$ $\frac{dy}{dt} = \gamma C_0 e^{\alpha_1 T} t^{\gamma-1}$
13	Скорость окисления циркониевых сплавов в водяном паре	$k_p = A_2 exp\left(-\frac{E_a}{R_1 T^0}\right)$
14	Износ	$x(t) = a_2(e^{k_2 t} - 1), \ k_2 > 0;$ $x(t) = a_2(1 - e^{k_2 t}), \ k_2 > 0$
15	Износ при вращении (подшипники)	$\frac{dx}{dt} = a_3 \varepsilon_э e^{a_3 t}, \ a_3 = k_3 m \omega^3$

Примечание:

$t -$ время;

$\text{C} -$ число циклов нагружения;

$\Delta K_1 -$ размах коэффициента интенсивности напряжений;

$b_{\text{кр}} -$ критическая глубина трещины;

$n -$ число центров кристаллизации;

$\sigma_{\text{ср}} -$ среднее напряжение;

$R^T_{\rho 0,2} -$ предел текучести;

$\varepsilon -$ деформация;

E_1 – модуль упругости;
E_2 – модуль упругости при запаздывающей упругой деформации;
τ – постоянная времени;
μ – магнитная проницаемость;
$I_{ут}$ – ток утечки;
ΔR – изменение сопротивления резистора;
m – масса;
ω – угловая скорость;
$\varepsilon_э$ – начальный эксцентриситет;
a_0 – радиус пятна касания;
q_1 – заряд электронавремя;
U – напряжение;
E_{a0} – начальная энергия активации процесса разрушения;
γ_1 – структурный коэффициент;
k_1 – постоянная Больцмана;
$a, b, c, d, \gamma, A, B, \alpha, \beta, k, n_1, u, \omega$ – константы.

Таблица 3 – Модели, описывающие процессы изменения выходных параметров реле во времени

№	Вид процесса выходного параметра объекта	Модель
1	Разборные электрические контакты. Изменение переходного сопротивления	$R_n(t) = \frac{R_{n0}}{1 - \frac{1}{a_0}\sqrt{2D_0 t\, exp\left(-\frac{E_a}{R_1 T^0}\right)}}$
2	Напряжение срабатывания электромагнитых реле	$V_{ср}(t) = V_{ср0}\exp(-at^b)$

Таблица 4 – Математические модели показателей долговечности

№	Показатель	Модель
1	Срок службы твердых тел	$\tau = \tau_0 exp\left(\frac{E_{a0} - \gamma_1 \sigma_M}{K_1 T^0}\right)$
2	Срок службы полимеров и неорганических диэлектриков	$\tau = \tau_0 exp\left(\frac{E_{a0} - \gamma_1 \sigma_M}{K_1 T^0}\right)$

3	Постоянная времени деградации туннельных диодов	$\tau_д = \tau_{д0} exp\left(\frac{a_1(\varphi - U)}{k_1 T^0}\right)$

Примечание:
τ_0 – постоянная времени;
E_{a0} – начальная энергия активации процесса разрушения;
E^m – энергия массы m;
K_1 – коэффициент интенсивности напряжений;
γ_1 – структурный коэффициент;
σ_M – механическое напряжение;
R_1 – универсальная газовая постоянная;
T^0 – абсолютная температура.

2. Новый этап развития теории долговечности с учётом асимметрии внутреннего времени оборудования СФСС

Середина и конец XX века характеризуются следующим важных этапом научно-технической революции, который, в частности, обогатил науку новым подходом в теории асимметрии времени. В центре идей были работы научных школ А.М. Ляпунова, В.И. Вернадского и И.Р. Пригожина. [5-7]

Физическая и математическая сущность нового подхода состоит в анализе уровней описания процессов старения конструктивных элементов СФСС с учётом достижений классической механики и термодинамики в следующем:

1) широкое применение языка теории операторов функционального анализа в классической механике, что означает замену описания систем на уровне изучения траекторий исследованиями их функций распределения;

2) введение в описание систем более простых уравнений, учитывающих специфику необратимых процессов и диссипативных структур;

3) обязательное применение теории случайных процессов и функций Ляпунова;

4) феномен времени не параметр, а оператор;

5) оператор эволюции с нарушенной временной симметрией;

6) применение макроскопической физики бифуркаций с нарушенной асимметрией времени.

3. Роль оператора внутреннего времени в повышение достоверности расчетов показателей долговечности сложных систем

В главе 4 на с. 96 – 108 [1] в соответствии с [7] приведено строгое математическое доказательство существования оператора внутреннего

времени, которое с помощью простых уравнений учитывает специфику неустойчивости и необратимости физико – химических процессов конструкционных материалов оборудования СФСС. В данной же статье автор избегает изложенного в [7] математического существа оператора внутреннего времени Т и ограничивается только формальным заключительным выражением:

$$\langle T\rangle_{\rho} = \frac{\langle \bar{\rho}, T\bar{\rho}\rangle}{\langle \bar{\rho}, \bar{\rho}\,\rangle}, \tag{1}$$

где

$\langle T\rangle_{\rho}$ – средний возраст (читай ресурс или срок службы)объекта;

ρ – функция распределения состояния анализируемого объекта;

$\bar{\rho}$ – избыток ρ по сравнению с равномерным распредлением.

$$\bar{\rho} = \rho - 1 = \sum_{n=-\infty}^{+\infty} C_n \varphi_n, \tag{2}$$

n – собственные значения оператора Т; а i – степень вырождения собственных значений n.

То есть каждая функция распределения состояния объекта ρ допускает разложение по собственным функциям $\{1, \varphi_n\}$.

При этом автором статьи так подробно изложил п.1, чтобы было понятно откуда берут данные для расчётов ресурса и срока службы значения ρ из таблиц типа 1-4 конкретных конструктивных элементов систем.

Таким образом появляется возможность сравнения результатов расчётов ресурса по принципиально различным методам: 1) по данным прогнозных методик теории длительной прочности, 2) с данными по методике с учётом асимметрии внутреннего времени объекта.

Выводы

1. Выполнен анализ состояния исследований расчётов ресурса оборудования СФСС с применением классических методов теорий длительной прочности.

2. Сделан обзор прогнозирования функций распределения ρ состояния конструкционных материалов объектов различного назначения, функций усталости и математических моделей ряда процессов, приводящих к отказам на субмикроскопическом и микроскопическом уровнях.

3. Рассмотрена физическая и математическая сущность нового подхода к определению показателей долговечности с учётом оператора внутреннего времени объектов, учитывающего влияние фактора асимметрии внутреннего времени в модусах «прошлое – настоящее – будущее».

4. Таким образом в статье фактически сформирован новый подход к развитию теории долговечности структурно и функционально сложных систем с учетом двух факторов: асимметрии внутреннего времени и длительных сроков активного существования критически важных систем.

Именно следуя идеям в этих источниках автором в последние годы были опубликованы монографии пока применительно только к одному из свойств надежности и безотказности – долговечности и риска [6].

Библиографический список

1. Острейковский В. А. Математическое моделирование эффекта асимметрии внутреннего времени в теории долговечности структурно и функционально сложных критически важных систем / В.А. Острейковский, Е.Н. Шевченко // В книге: Итоги науки. Выпуск 37. Избранные труды Международного симпозиума по фундаментальным и прикладным проблемам науки. – М.: РАН, 2018. – С. 69–1112.
2. Острейковский В. А. Старение и прогнозирование ресурса оборудования атомных станций. М.: Энергоатомиздат, 1994. -286с.
3. Острейковский, В.А. Асимметрия времени в теории прогнозирования состояния сложных динамических систем: монография. - / В.А. Острейковский, Т.Ю. Денисова, Е.Н. Шевченко. –Сургут: «Печатный мир», 2018. – 574 с.
4. Нормы расчета на прочность оборудования атомных энергетических установок (ПН Г – 7 – 002 – 86 – Правила и нормы в атомной энергетике). М.: Энергоатомиздат, 1989. – 525 с.
5. Ляпунов А.М. Собрание сочинений. Т.2. – М.-Л., 1956. – 263 с
6. Вернадский В. И. Размышления натуралиста / В. И. Вернадский. – М.: Живое слово, 1977, кн. 2. – 192 с.
7. Пригожин И.Р. От существующего к возникающему: Время и сложность в физических науках: Пер. с англ. / Под ред. Ю.Л. Климонтовича. – Изд. 2-е, доп. – М.: Едиториал УРСС, 2002. – 288 с.

УДК 004.056.53
В.В. Николаев, адъюнкт кафедры (автоматизированных систем специального назначения)
И.Б. Саенко, д.т.н., профессор кафедры (автоматизированных систем специального назначения)
Военная академия связи

ПОДХОД К ПОСТРОЕНИЮ МОДЕЛИ ЕДИНОГО ИНФОРМАЦИОННОГО ПРОСТРАНСТВА В ЦЕЛЯХ ОПТИМИЗАЦИИ РАСПРЕДЕЛЕНИЯ ЕГО РЕСУРСОВ

Аннотация
Рассматривается подход к построению модели единого информационного пространства для выбора наилучшего варианта распределения информационных ресурсов по узлам единого информационного пространства.
Ключевые слова: единое информационное пространство, информационный ресурс, оптимизация, распределение, модель
Annotation
An approach to the construction of a model of a single information space for choosing the best option for the distribution of information resources across the nodes of a single information space is considered.
Keywords: unified information space, information resource, optimization, distribution, model

Решение задачи оптимизации распределения информационных ресурсов (ИР) единого информационного пространства (ЕИП) априори подразумевает необходимость моделирования процесса функционирования ЕИП.

Основной задачей ЕИП является предоставление пользователям доступа к необходимым информационным ресурсам из любого узла ЕИП с учетом разграничения прав доступа к информации [1], что является одной из отличительных особенностей ЕИП в сравнении с обычными транзакционными системами. Второй особенностью предлагаемой модели является, то что ИР ЕИП имеют различный объем (от небольших текстовых документов до высокообъемного графического и видео контента).

Существующее ЕИП имеет сложную топологию связей между узлами, а интенсивность формирования запросов разными пользователями зачастую описывается различными законами распределения. В связи с этим для построения математической модели необходимо внести некоторые допущения: будем использовать диспетчеризацию FIFO, коллизии внутри каналов передачи данных учитывать не будем, поток

заявок на доступ к ИР будет Пуассоновским, максимальный объем запрашиваемого ИР будет ограничен 100 Мб, а очередь ожидающих заявок возьмем неограниченной длины.

Допущения, которые были введены, существенно упрощают исследование модели, но вместе с тем незначительно изменяют порядок предоставления (получения) доступа к ИР в ЕИП и цель конструирования модели, а именно определение времени реакции на запрос конкретного пользователя, а также времени реакции всей системы в целом, может быть успешно достигнута.

Библиографический список:

1. Саенко И.Б., Бирюков М.А., Ефимов В.В., Ясинский С.А. Модель администрирования схем разграничения доступа в облачных инфраструктурах // Информация и космос. 2017. № 1. С. 121-126.
2. Горобец В.В. Облачная модель транзакционной системы // Вестник компьютерных и информационных технологий. 2013. № 4. С. 19-24.

УДК 004
Д.С. Хасанов, младший научный сотрудник
Санкт-Петербургский Федеральный исследовательский центр Российской академии наук
Россия, Санкт-Петербург
e-mail: dkhasanovsuai@yandex.ru

МУЛЬТИАГЕНТНЫЕ СИСТЕМЫ В РАЗНЫХ ОБЛАСТЯХ ПРИМЕНЕНИЯ

Аннотация
В статье рассматривается возможности МАС в областях моделирования и «умном городе». Работа в области агент-ориентированной программной инженерии, мультиагентного обучения, агент-ориентированного моделирования и применения агентов в таких актуальных областях, как умные города и окружающий интеллект позволяют сильно продвинуть интеллектуализацию и прогрессию государственных систем для помощи гражданам.
Ключевые слова: агенты, логистика, транспорт, мультиагентные системы, Anylogic, моделирование
Abstract
This article examines the capabilities of MAS in the fields of modeling and the smart city. Work in agent-based software engineering, multi-agent learning, agent-based modeling, and agent-based applications in topical areas such as smart cities and ambient intelligence strongly advance the intelligence and progression of government systems to help citizens.
Keywords: agents, logistics, transportation, multi-agent systems, Anylogic, modeling.

Введение

Концепция интеллектуального агента - это концепция, которая родилась из области искусственного интеллекта; фактически, общепринятое определение связывает дисциплину искусственного интеллекта с анализом и проектированием автономных сущностей, способных демонстрировать разумное поведение. С этой точки зрения предполагается, что интеллектуальный агент должен быть способен воспринимать окружающую среду, рассуждать о том, как достичь своих целей, действовать для их достижения, применяя некоторый принцип рациональности, и взаимодействовать с другими интеллектуальными агентами, искусственными или человеческими [1].

Мультиагентные системы являются частным случаем распределенной системы, и их особенность заключается в том, что

компоненты системы автономны и эгоистичны, стремятся к достижению своих собственных целей. Кроме того, эти системы отличаются тем, что являются открытыми системами без централизованного дизайна [2]. Одна из основных причин большого интереса и внимания, которое уделяется мультиагентным системам, заключается в том, что они рассматриваются как технология, позволяющая создавать сложные приложения, требующие распределенной и параллельной обработки данных и действующие автономно в сложных и динамичных областях.

Исследования в области мультиагентных систем (MAC) основаны на результатах распределенных вычислений, задающих новые вопросы о том, как агенты должны взаимодействовать друг с другом, чтобы координировать свою деятельность и решать сложные проблемы. Большинство современных исследований сосредоточено на разработке соответствующих механизмов координации для управления коалициями или командами агентов. Программирование интеллектуальных агентов ставит перед инженерами сложные задачи, поскольку в дополнение к сложности проектирования параллельных и распределенных систем добавляется сложность, связанная с тем, что компоненты должны иметь архитектуру, включающую такие аспекты, как реактивность, проактивность и общительность. Эти свойства нелегко запрограммировать, когда среда динамична и сложна. Для того чтобы достичь реального программирования агентов, многими исследователями было сделано множество предложений по архитектуре агентов, языкам общения, механизмам принятия решений и координации. В последнем случае, возникает необходимость в том, что агенты должны уметь договариваться, чтобы иметь возможность работать в многоагентной системе. Здесь кроется важный аспект сложности программирования интеллектуальных агентов.

MAC и обучение

Обучение в MAS является парадигмой огромной важности, поскольку система, способная обучаться и динамически менять свой образ действий, предоставляет большой потенциал для решения многих проблем, для которых нам неизвестно поведение других агентов в окружающей среде. Это добавляет дополнительные уровни сложности в задачи консенсуса и координации между агентами, поскольку они могут постоянно обучаться и менять свое поведение.

Мультиагентное обучение (MAL) позволяет разработать определенные рекомендации, на основе которых агент сможет использовать динамику своей среды и приспосабливаться к ней. В многоагентной среде обучение является одновременно и более важным,

и более сложным, поскольку выбор действий должен осуществляться в присутствии других агентов, которые не обязательно должны следовать правилам среды и могут принимать недетерминированные решения. Эти агенты, в свою очередь, будут адаптировать свои действия к тем, которые ранее выполняли другие агенты. Проблемы, рассматриваемые в MAL, имеют тесную связь с теорией игр, в которой агент выбирает действия, чтобы максимизировать свое преимущество над остальными.

В области обучения MAC рассматривается проблема согласованного управления несколькими судами. Для решения этой проблемы необходимо разработать алгоритмы согласованного управления для нескольких агентов. Для одного транспортного средства они предложили использовать нейронные сети радиальных базисных функций для улучшения устойчивости контроллера. Для нескольких транспортных средств можно рассмотреть возможность использования направленной топологии, но с учетом того, что связь между транспортными средствами является непрерывной.

Так же можно разработать подход к изучению моделей поведения в виде деревьев поведения для автономных агентов. Основная цель предложения - облегчить моделирование поведения автономных агентов в симуляторах и компьютерных играх.

MAC и моделирование

Агентное моделирование - это подход к моделированию систем, который фокусируется на моделировании сложных технических систем, которые распределены и включают сложное взаимодействие между людьми и машинами. Его можно рассматривать как тип вычислительной модели, которая позволяет имитировать действия и взаимодействия автономных индивидуумов в среде и позволяет определить, какие эффекты они производят в системе в целом. Она сочетает в себе элементы теории игр, сложных систем, вычислительной социологии, многоагентных систем и эволюционного программирования. Модели имитируют одновременные действия множества субъектов (агентов) в попытке воссоздать и предсказать действия сложных явлений. Это процесс чрезвычайных ситуаций от самого элементарного уровня (микро) до самого высокого уровня (макро).

Таким образом, агентное моделирование можно рассматривать как мощный исследовательский метод, позволяющий в простой форме справиться со сложностью, чрезвычайностью и нелинейностью, характерными для многих социальных, политических и экономических явлений.

Мной была разработана модель цифрового двойника Западного Скоростного Диаметра Санкт-Петербурга на основе мультиагентного подхода и имитационного моделирования в программной среде Anylogic. Результатами разработки стало «построение цифрового двойника рассмотренной системы позволяет оценить проектные решения и наглядно продемонстрировать «узкие места», которые в будущем будут снижать пропускную способность. В целом, данная система требует незначительных доработок, например увеличение количества полос на съезд, что поможет увеличить поток автомобилей и, соответственно, увеличить путь из источника в сток. Данный путь развития бесспорно актуален и правилен для будущего развития Западного Скоростного Диаметра, вся система будет готова к постоянно растущему потоку автомобилей и сможет обрабатывать до 4000 автомобилей в час, что обеспечит устойчивое развитие транспортного комплекса мегаполиса.» [4]

МАС в умных городах

Концепция умного города возникла в связи с необходимостью найти решение проблемы быстрого роста населения и рисков, которые это влечет за собой для города, экономических рисков, таких как безработица, или физических рисков, таких как чрезмерное загрязнение окружающей среды. Для решения этих проблем были использованы различные технологии, в том числе и МАС.

Мультиагентные системы вместе с Интернетом вещей традиционно являются наиболее используемыми.

Как правило, эти концепции объединяются, проектируя взаимосвязанные сети, которые отвечают потребностям граждан, как по отдельности, так и в целом, а также отслеживая с помощью датчиков уровень загрязнения, трафика, шума и т.д. Умный город - это большой взаимосвязанный организм, который вместе с организациями стремится улучшить качество жизни своих граждан.

Поэтому умный город будет полон датчиков, постоянно собирающих информацию о действиях, происходящих в городе, датчиков влажности, температуры, шума, загрязнения и т.д. Все эти датчики являются частью системы сбора данных, которая будет отвечать за быструю и интеллектуальную обработку информации. Именно для этого момента имеет смысл использовать мультиагентные системы. Децентрализованное управление МАС дает возможность распределенно управлять всей доступной информацией, а также эффективно координировать возможные действия в масштабах города. Более того, процессы принятия решений, помимо координации, могут выполнять параллельные действия в разных точках города, без сильного

централизованного контроля, что обеспечивает большую гибкость и адаптацию всей системы.

Мною будет предложена мультиагентная система, которая предоставляет инструменты визуализации и прогнозирования для разрабатываемых систем улучшения городской инфраструктуры. Предложенная МАС включает агентов, который выполняет процессы сбора и очистки данных, а также способен создавать модели транспорта для каждой новой точки входа в систему. В предложенном решении собранная информация использовалась агентами, которые выполняли прогнозирование пробок и предложение альтернативного маршрута в случае проблем с дорожной сетью. Кроме того, в процессе прогнозирования будут использованы различные алгоритмы регрессии. Кроме того, был проведен статистический анализ, чтобы показать различия в их работе и определить релевантность результатов. Может быть реализована мультиагентная система для облегчения анализа различных возможных конфигураций размещения станций зарядки электромобилей в городе на основе спроса и местоположению регистрации электрических транспортных средств. МАС, предложенная в данной работе, объединяет информацию, извлеченную из разнородных источников данных, в качестве отправной точки для определения областей, где потенциально могут быть размещены будущие зарядные станции.

Выводы

Исследования в области МАС продолжают предлагать технологические решения в самых разных областях. Исследователи МАС разрабатывают новые достижения, которые позволяют создавать более мощные, гибкие и адаптированные системы, позволяющие прогнозировать необходимые данные.

Библиографический список

1. Искандеров, Ю. М. Мультиагентная модель управления беспилотной снегоходной транспортной платформой при решении практических задач / Ю. М. Искандеров, Д. Ю. Андрианов, Ю. С. Андрианов // Вестник Поволжского государственного технологического университета. Серия: Материалы. Конструкции. Технологии. – 2020. – № 3. – С. 35-42. – DOI 10.25686/2542-114X.2020.3.35.
2. Хасанов Д.С., Свистунова А.С. – Оценка эффективности обслуживания пассажиров в аэровокзальном комплексе. – Транспорт России: Проблемы и перспективы -2020. – 32 с.

3. Искандеров Ю.М., Свистунова А.С., Хасанов Д.С., Чумак А.С. - Интеллектуальная поддержка принятия решений в логистических системах. – Морские интеллектуальные технологии т.1 №2. 2021. – 145 с.
4. Свистунова, А. С. Построение цифрового двойника Западного скоростного диаметра Санкт-Петербурга на основе имитационного моделирования / А. С. Свистунова, Д. С. Хасанов, Д. М. Кравец // Десятая всероссийская научно-практическая конференция по имитационному моделированию и его применению в науке и промышленности «Имитационное моделирование. Теория и практика» (ИММОД-2021) : Труды конференции (электронное издание), Санкт-Петербург, 20–22 октября 2021 года / Редакторы Плотников А.М., Долматов М.А., Смирнова Е.П.. – Санкт-Петербург: АО «Центр технологии судостроения и судоремонта», 2021. – С. 382-388.
5. Юсупов Р.М., Микони С.В., Соколов Б.В. Методология оценивания качества моделей и полимодельных комплексов. В сборнике: Перспективные направления развития отечественных информационных технологий. Сборник научных трудов пятой межрегиональной научно-практической конференции. Севастополь, 2019. С. 13-14.
6. Свистунова, А. С. Возможности автоматических транспортеров-погрузчиков и их использование при создании имитационной модели развития контейнерного терминала / А. С. Свистунова, Д. С. Хасанов // Морские интеллектуальные технологии. – 2020. – № 4-1(50). – С. 169-174. – DOI 10.37220/MIT.2020.50.4.023.
7. Искандеров, Ю. М. Моделирование транспортно-технологических процессов в цепях поставок на основе мультиагентных технологий / Ю. М. Искандеров, М. Б. Ласкин // Перспективные направления развития отечественных информационных технологий : материалы V межрегиональной научно-практической конференции, Севастополь, 24–28 сентября 2019 года / Севастопольский государственный университет; Санкт-Петербургский институт информатики и автоматизации РАН. – Севастополь: Федеральное государственное автономное образовательное учреждение высшего образования "Севастопольский государственный университет", 2019. – С. 71-74.
8. Concept and Models of Information Application for Actions in Systems / A. Geyda, L. Fedorchenko, I. Lysenko [et al.] // Conference of Open Innovations Association, FRUCT. – 2022. – No 31. – P. 407-415.
9. Хасанов, Д. С. Технология сбора данных в логистике / Д. С. Хасанов, А. С. Свистунова // Системный анализ в проектировании и управлении : сборник научных трудов XXV Международной научной и

учебно-практической конференции : в 3 ч., Санкт-Петербург, 13–14 октября 2021 года. – Санкт-Петербург: Политех-Пресс, 2021. – С. 275-279. – DOI 10.18720/SPBPU/2/id21-377.
10. Iskanderov, Y. Comprehensive Intelligent Information Security Management System (CIISMS) for Supply Networks: The Actor-Network Perspective / Y. Iskanderov, M. Pautov // Advances in Intelligent Systems and Computing. – 2020. – Vol. 1294. – P. 130-142. – DOI 10.1007/978-3-030-63322-6_10. – EDN BCKIVY.
11. Svistunova, A. S. Improving the efficiency of traffic management in a metropolis based on computer simulation / A. S. Svistunova, D. S. Khasanov // Computing, Telecommunications and Control. – 2021. – Vol. 14. – No 3. – P. 33-42. – DOI 10.18721/JCSTCS.14303.

УДК 004.021
И.Д. Ничипоров[1], магистрант, Н.Г. Мустафин[2], канд. техн. наук, проф., С.В. Савосин[3], канд. техн. наук, доцент, Б.В. Соколов[4], д-р техн. наук, проф.
[1,2,3] Санкт-Петербургский государственный электротехнический университет им. В.И. Ульянова (Ленина) «ЛЭТИ»
ул. Профессора Попова, д 5, Санкт-Петербург, Россия, 197376
e-mail: id_nichiporov@mail.ru
e-mail: nikolay.mustafin@gmail.com
e-mail: svsavosin@yandex.ru
[4] Федеральное государственное бюджетное учреждение науки Санкт-Петербургский институт информатики и автоматизации Российской академии наук (СПИИРАН)
14 линия, д.39, Санкт-Петербург, Россия, 199178
e-mail: sokolov_boris@mail.ru

ПОДХОДЫ К ПОИСКУ КОМПРОМИССНЫХ РЕШЕНИЙ МНОГОКРИТЕРИАЛЬНЫХ ЗАДАЧ КОММИВОЯЖЁРА

Аннотация
Рассматриваются решения многокритериальных задач коммивояжера. Предлагаются подходы, основанные на методах уступок для поиска компромиссных решений.
Ключевые слова: задача коммивояжера, многокритериальная задача коммивояжёра, метод идеальной точки, методы уступок, квазиоптимальные траектории.

I.D. Nichiporov[1], N.G. Mustafin[2], S.V. Savosin[3], B.V. Sokolov[4]
[1,2,3] Saint Petersburg Electrotechnical University «LETI» Professor Popov St., 5, St. Petersburg, Russia, 197376
[4] Saint Petersburg Institute for Informatics and Automation of Russian Academy of Sciences 14th Line, 39, St. Petersburg, Russia, 199178

APPROACHES TO THE SEARCH OF COMPROMISE SOLUTIONS OF MULTICRITERIA TRAVELING SALESMAN PROBLEMS

Abstract
We consider solutions to multi-objective traveling salesman problems. The proposed approaches based on the methods of concessions to find compromise solutions.
Keywords: traveling salesman problem, multi-objective traveling salesman problem, ideal point method, concession method, quasi-optimal trajectories.

В практике разработки информационных систем различного назначения: информационно-аналитического, организационных, технологических, экономических, и др. часто встречаются логистические задачи

в различных постановках в том числе задачи коммивояжёра в скалярной и векторных (многокритериальных) постановках.

Методы решения скалярных задач коммивояжёра разработаны и применяются на практике. В векторных задачах коммивояжёра дуги связывающие узлы имеют несколько, зачастую, противоречивых оценок.

Стоит задача нахождения компромиссного решения обеспечивающего, в некотором смысле, наилучшее сочетание оценок траекторий, соответствующее конкретной постановке задачи.

Целесообразно при поиске компромиссов иметь оценки, соответствующие «идеальной точке»: для выбора уступок, для интегральной оценки компромиссных траекторий.

Предлагается в зависимости от содержательной постановки задачи иметь возможность назначения приоритетов локальных критериев.

Таким образом имея одинаковые входные данные можно получить различные решения, которые будут являться компромиссными при выбранных приоритетах локальных критериев и назначаемых уступках.

В работе предложены два возможных метода поиска решения задачи.

Рассмотрим применение предложенных методов для задачи коммивояжёра с тремя критериями.

Первый метод основан на методе последовательных уступок. Применяем метод последовательных уступок для оценок траекторий по первому (по важности) критерию оставляем только те траектории, которые по данному критерию имеют оценки не хуже, чем оценка в идеальной точке плюс уступка (при задаче минимизации). На следующем шаге для оставшегося множества траекторий находится наилучшая оценка по второму критерию и с учётом уступки получаем следующее множество траекторий для следующего шага. Операции продолжаются до последнего локального критерия. На последнем шаге выбираем траекторию с наилучшей оценкой по соответствующему критерию.

Следующий алгоритм связанных уступок во много основан на предыдущем. Он даёт большую вариативность при постановке задачи и большую возможность выбора для пользователя. Получив все возможные значения траекторий для исходных данных, мы можем определить оценки, соответствующие идеальной точке для каждого из имеющихся критериев и задать уступки по каждому из них. Получаем пересечение множеств траекторий, удовлетворяющих уступкам по всем критериям.

В случае если это пересечение множеств является пустым, то задача считается не решённой и требует коррекции уступок. Если данное множество содержит несколько траекторий, то траектория может быть

выбрана с учётом ранжирования критериев либо на основе другой схемы компромиссов.

Исследования, выполненные по данной тематике, проводились в рамках бюджетной темы FFZF-2022-0004.

Библиографический список

1. А.В.Степченко, Н.Г.Мустафин, С.В.Савосин, Б.В.Соколов. Оптимизация маршрута коммивояжера по векторному критерию // Перспективные направления развития отечественных информационных технологий: материалы VII межрегиональной научно-практической конф. Севастополь, 21-25 сентября 2021 г. / Севастопольский государственный университет; науч. ред.: Б.В. Соколов. – Севастополь: СевГУ, 2021. С. 138–140.
2. Hameed I. A. Multi-objective solution of traveling salesman problem with time // International Conference on Advanced Machine Learning Technologies and Applications. – Springer, Cham, 2019. – С. 121-132.

УДК 004.852
В. С. Авраменко, к-т техн. наук, доцент, А. А. Ренсков, к-т техн. наук, доцент, Канчалан С.Д.
Военная академия связи
пр-т Тихорецкий 3, г. Санкт-Петербург, Россия, 194064
e-mail: vsavr@yandex.ru

ПРОГНОЗНЫЙ КОНТРОЛЬ ТЕХНИЧЕСКОГО СОСТОЯНИЯ СРЕДСТВ АВТОМАТИЗАЦИИ НА ОСНОВЕ РЕКУРРЕНТНОЙ НЕЙРОННОЙ СЕТИ

Аннотация
Рассмотрен способ автоматического прогнозного контроля технического состояния средств автоматизации на основе системы рекуррентных нейронных сетей долгой краткосрочной памяти.
Ключевые слова: средства автоматизации, техническое состояние, прогноз, контроль, рекуррентная нейронная сеть.

V. Avramenko, A. Renskov, S. Kanchalan
Military Academy of Telecommunications
prospect Tikhoretsky 3, St. Petersburg, Russia, 194064
e-mail: vsavr@yandex.ru

PREDICTIVE CONTROL OF THE TECHNICAL CONDITION OF AUTOMATION TOOLS BASED ON A RECURRENT NEURAL NETWORK

Abstract
A method of automatic predictive control of the technical condition of automation equipment based on a system of recurrent neural networks of long short-term memory is considered.
Keywords: automation tools, technical condition, forecast, recurrent neural network.

В настоящее время к критически важным автоматизированным системам предъявляются повышенные требования по надежности [1]. Одним из направлений повышения надежности автоматизированных систем и входящих в их состав средств автоматизации является совершенствование и развитие систем контроля (мониторинга) технического состояния, так как существующие системы контроля не в полной мере удовлетворяют современным требованиям по оперативности обнаружения отказов (сбоев) [2].

Одним из путей решения данной проблемной ситуации является реализация автоматического прогнозного контроля технического состояния средств автоматизации, позволяющего администратору в близком

к реальному масштабу времени получать данные о возможном отказе (сбое) на прогнозируемом периоде.

Для прогнозирования значений параметров технических и программных средств автоматизации целесообразно использовать рекуррентные нейронные сети (НС) долгой краткосрочной памяти (LSTM (Long short-term memory)).

В качестве прогнозируемых параметров состояния средств автоматизации могут использоваться следующие: температура (центрального процессора, жесткого диска и др.), средняя загруженность оперативной памяти, жесткого диска, процессора и другие. Для прогнозирования параметров технического состояния средств автоматизации для каждого из этих параметров строится отдельная LSTM сеть. Для обучения НС используется набор данных о параметрах технического состояния элементов средств автоматизации, в периоды их функционирования.

В ходе контроля каждая НС периодически формирует на выходе прогнозное значение соответствующего параметра состояния средства автоматизации с заданным прогнозным периодом, далее определяется степень соответствия каждого из них допустимым значениям. Затем на основе полученных прогнозных значений технического состояния отдельных элементов в соответствии с выбранным критерием контроля определяется прогнозное техническое состояние средства автоматизации в целом (работоспособное, частично неработоспособное, неработоспособное).

Также для определения технического состояния средства автоматизации может использоваться одна рекуррентная НС, на вход которой подаются значения всех существенных параметров (температура отдельных элементов, загруженность ОП и т.д.).

Таким образом, реализация функции прогнозного контроля технического состояния средств автоматизации обеспечит администратору возможность проведения упреждающих мероприятий для предотвращения их отказов и сбоев.

Библиографический список

1. Паращук И.Б., Крюкова Е.С., Михайличенко А.В. Анализ зашумленных и неоднородных данных о значениях параметров надежности дата центров // VI Межвузовская научно-практическая конференция «Проблемы технического обеспечения войск в современных условиях». Сборник трудов. Санкт-Петербург: 2021. с. 164-172.

2. Ковалев А.А., Авраменко В.С., Иванов Р.М. Анализ проблемы автоматизированного контроля технического состояния комплексов средств автоматизации специального назначения // VI Межвузовская научно-

практическая конференция «Проблемы технического обеспечения войск в современных условиях». Сборник трудов. Выпуск 1 – СПб: ВАС, 2021. с. 55-59.

УДК 005.07:004.05.
С. В. Микони, д-р техн. наук, профессор
Санкт-Петербургский Федеральный исследовательский Центр РАН
Санкт-Петербургский институт информатики и автоматизации РАН
14 линия 39, г. 199178, Санкт-Петербург, Россия, 199178
e-mail: smikoni@mail.ru

ОБОСНОВАНИЕ ДВУХКОМПОНЕТНОЙ МОДЕЛИ МНОГОМЕРНОГО ОЦЕНИВАНИЯ ОБЪЕКТОВ

Аннотация
Обосновывается необходимость разделения модели многомерного оценивания на две части – модель предметной области и модель предпочтений ЛПР. Модель ПрО не зависит от решаемой задачи оценивания. Модель предпочтений ЛПР содержит информацию, предназначенную для решения конкретной задачи оценивания. Такое разделение моделей упрощает построение и отладку модели многомерного оценивания объекта для решения задач классификации и упорядочения конечного множества объектов.
Ключевые слова: модель, оценивание, предметная область, предпочтение ЛПР, классификация, упорядочение.

SUBSTANTIATION OF THE MODEL OF MULTIDIMENSIONAL ESTIMATION OF OBJECTS

Abstract
The necessity of dividing the multivariate estimation model into two parts is substantiated – the model of the subject area and the model of preferences of the decision maker. The SbA model does not depend on the estimation problem being solved. The decision maker's preference model contains information intended for solving a specific evaluation problem. This separation of models simplifies the construction and debugging of a multidimensional object estimation model for solving problems of classifying and ordering a finite set of objects.
Key words: model, estimation, subject area, decision maker's preference, classification, ordering.

В работах, посвящённых принятию решений на конечном множестве альтернатив, описание этапов принятия решения слабо увязывается с проектированием модели многомерного оценивания (ММО) [1]. Между тем, трудоёмкость проектирования модели ММО несоизмеримо больше трудоёмкости других этапов принятия решения. Её проектирование осуществляется в два этапа [2].

На первом из них изучаются свойства объекта оценивания и выбираются те из них, которые существенны для решения поставленной задачи. Эту работу выполняют специалисты-предметники.

На втором этапе ЛПР задаёт требования к показателям, отражающим выбранные свойства объекта. Оба этапа выполняются под руководством системного аналитика, отвечающего за качество модели ММО. Сообразно такой последовательности создания модель ММО делится на две части: модель предметной области (ПрО) и модель предпочтений ЛПР.

Модель ПрО представляет собой структуру показателей $R \subseteq J \times J$. В зависимости от числа показателей и их различия определяется число уровней этой структуры, отражающей дерево целей выбора. Узлам нижнего уровня этой структуры соответствуют таблицы «Объекты/ Показатели». Они имеют одинаковое количество строк, именуемых оцениваемыми объектами X, $|X| = N$ и в общем случае разное количество столбцов, именуемых показателями J. Суммарное количество столбцов в таблицах нижнего уровня иерархии равно $n = |J|$. На этом же этапе задаются границы шкалы $[y_{j,\min}, y_{j,\max}]$ j-го показателя, $j \in J$.

Модель предпочтений ЛПР в задаче упорядочения объектов характеризуется следующими параметрами:

5) *важность* (вес) w_j j-го показателя;
6) *целевое значение* c_j j-го показателя;
7) *оценочная функция* $u_j = f_н(y_j)$ полезности j-го показателя;
8) *вид* обобщающей функции.

В задаче определения принадлежности оцениваемого объекта одному из заданных классов параметром 2 являются границы между смежными классами, а параметром 3 – функции принадлежности этим классам. Предлагаемое деление модели ММО на две части позволяет создавать модели разнообразных задач классифицирования и упорядочения объектов на общей модели предметной области. Это создаёт предпосылки для экономичного решения разнообразных задач принятия решений и упрощения отладки их моделей.

Исследования, выполненные по данной тематике, проводились в рамках бюджетной темы FFZF–2022–0004.

Библиографический список

1. Рамеев О.А., Корнеенко В.П. Основы теории многокритерального оценивания объектов с многоуровневой структурой показателей эффективности. –М.: МаксПресс, 2018. –413 с.
2. Микони С.В. Теория принятия управленческих решений: – СПб.: Издательство «Лань», 2022. – 460 с. Издание 2-е: исправленное и дополненное (Учебники для вузов. Специальная литература).

УДК 681.3
А.В. Скатков, А.А. Брюховецкий, Д.В.Моисеев, Н.В.Сухарев
Севастопольский государственный университет,
РФ, г. Севастополь, ул. Университетская, 33,
e-mail: dmitriymoiseev.mail.ru

САМООБУЧАЮЩАЯСЯ АВТОМАТНАЯ МОДЕЛЬ ОБНАРУЖЕНИЯ УЯЗВИМОСТЕЙ ИНТЕРФЕЙСОВ БТС С УЧЕТОМ ТЕХНОЛОГИЙ 5G

Аннотация
Целью данной работы является разработка модели, которая предоставляет возможности исследования процессов обнаружения уязвимостей интерфейсов БТС в условиях динамически меняющейся внешней среды. Рассматривается алгоритмический подход, базирующийся на методах адаптивной интеллектуальной технологии контроля состояния ресурсов БТС. Представлена самообучающаяся модель с использованием вероятностного оценивания изменения состояний ресурсов и методов непараметрической статистики в сетях 5G.
Ключевые слова: вероятностный автомат, динамическое оценивание ресурсов, самообучающаяся модель, самонастройка, мобильные сети 5G
Annotation
The purpose of this work is to develop a model that provides opportunities to study the processes of detecting BTS interfaces in a dynamically changing external environment. An algorithmic approach based on the methods of adaptive intelligent technology for monitoring the state of BTS resources is considered. A self-learning model using probabilistic estimation of changes in the states of resources and methods of nonparametric statistics in 5G networks is presented.
Keywords: probabilistic automaton, dynamic resource estimation, self-learning model, self-tuning, 5G mobile networks

Введение. Предлагаемый в статье подход ориентирован на решение задач обнаружения моментов времени изменения состояния контролируемых ресурсов БТС: канал связи, процессор, память. При этом скорость и достоверность оценки ситуации может иметь решающее значение. Реализация таких задач в реальном времени не всегда возможна с помощью аналитического подхода, поскольку эти задачи характеризуются противоречивостью, нелинейностью, недифференцируемостью, многоэкстремальностью, сложной топологией области допустимых значений, высокой вычислительной сложностью оптимизируемых функций, высокой размерностью пространства поиска и т.п. В условиях дефицита априорной информации большая часть проблем анализа данных

связана с исследованиями стохастических систем [1]. Одним из наиболее эффективных инструментов моделирования сложных стохастических систем является методология вероятностно-автоматного моделирования [2]. Продуктивность указанной методологии обусловлена возможностью построения унифицированных моделей для широкого класса систем и использованием систем поддержки принятия решений при необходимости в точной оценке выбора различных альтернатив на основе вероятностных автоматов.

Настоящая работа посвящена применению модели обучаемых вероятностных автоматов для обнаружения уязвимостей интерфейсов объектов, которые функционируют в интеллектуальных мобильных транспортных сетях, обеспечивающхе межмашинное взаимодействие с использованием технологии интернет вещей и др. Разнородность приложений и беспроводных коммуникаций в сетях 5G существенно усложняет обеспечение безопасности объектов [3]. Методы предупреждения атак для безопасной эксплуатации транспортных средств должны быть динамичными и реагировать на возможные угрозы. Упреждающий подход к угрозам должен быть ключевым требованием, которое должно быть выполнено. Сети транспортных средств очень динамичны и не имеют централизованного управления. Как следствие, обмен информацией между средствами не всегда надежен, учитывая гетерогенный характер технологий, применяемых в сетях 5G. Поэтому важное значение приобретает разработка подходов, направленных на обеспечение безопасности интерфейсов при взаимодействии устройств в сети.

Постановка задачи. Целью работы является разработка модели с использованием вероятностного оценивания состояний ресурсов БТС. Модель базируется на основе вероятностного автомата с адаптивной самонастройкой. На основе предлагаемой модели решается задача оценки состояний ресурсов с целью повышения достоверности результатов классификации информационных ситуаций. Апостериорная информация о состоянии ресурсов в процессе функционирования БТС используется для адаптации к воздействиям внешней стохастической среды.

Транспортное средство в предлагаемой модели является интеллектуальным устройством, оснащенным коммуникационными возможностями, подключенным на основе интернет-протокола, мощной платформой с несколькими датчиками, вычислительными блоками, функционирующих с высокой производительностью и эффективностью в соответствии со спецификациями стандартов связи 3GPP. Подключенные средства могут взаимодействовать с внутренней, т.е. V2S (vehicle-to-

sensor) и внешней средами, такими как V2V и V2I, включая придорожные устройства-базовые станции (RSU), которые используют выделенную связь ближнего действия (DSRC). Бортовой блок (OBU), размещенный внутри транспортного средства, передает информацию в окружающую среду. RSU собирают данные с транспортных средств, а приложения, установленные в RSU, предоставляют запрошенную услугу. Вместе сеть датчиков обеспечивает мониторинг сети в режиме реального времени.

В рабочем режиме функционирования БТС подвержен влиянию внешних воздействий, которые приводят к изменению значений априорных вероятностей. С целью учета влияния внешних факторов предлагается на основе апостериорной информации, получаемой в процессе контроля состояния ресурсов БТС, использовать адаптивную модель, базирующуюся на оценке однородности распределений числа «поощрений» («штрафов») для каждого элемента формируемых матриц – $SP(T_{норм})$ на этапе обучения и $SP(T_{внеш})$ в процессе контроля. В каждом такте автомат формирует сигнал поощрения (штрафа) в зависимости от выполнения условия: $S_k(t+1) = S_k(t)$. Если условие выполняется, то соответствующий элемент матрицы поощрения (штрафа) $SP_k(T_{норм})$ на этапе обучения или в рабочем режиме $SP_k(T_{внеш})$ увеличивается на 1. При этом происходит перерасчет вероятностей матриц переходов по следующим формулам (модель Буша-Мостеллера [4]).

В зависимости от оценки величины неоднородности матриц $SP(T_{норм})$, $SP(T_{внеш})$ определяется принадлежность к одному из возможных классов. Величина неоднородности может быть получена при сравнении указанных матриц с применением методов непараметрической статистики [5]. Переход системы в состояния S_0, S_1, S_2 случайный, что имеет место, когда не осуществляется целенаправленного воздействия. Такое состояние ресурсов относится к нормальному состоянию БТС. Если матрицы (поощрений или штрафов) значительно отличаются друг от друга, то из этого можно сделать вывод, что состояние БТС подвержено внешнему воздействию – атаке.

В статье рассмотрен алгоритмический подход обнаружения уязвимостей интерфейсов БТС на основе самообучающихся вероятностных автоматов. Предлагаемый метод ориентирован на обнаружение изменения состояния контролируемых ресурсов БТС: канал связи, процессор, память. Предложенный адаптивный подход приведет к повышению достоверности и оперативности процессов поддержки принятия решений в задачах обеспечения безопасности объектов критической информационной инфраструктуры в условиях сетей 5G.

*Работа выполнена при частичной поддержке Российского фонда фундаментальных исследований (грант № 19-29-06015, 19-29-06023**).***

Библиографический список

1. Адаптивное обнаружение уязвимостей интерфейсов беспилотных транспортных средств. Скатков А.В., Брюховецкий А.А., Доронина Ю.В., Моисеев Д.В. и др.// Издательство «Ариал» (Симферополь), 2020. - 352 с.
2. Поспелов Д.А. Вероятностные автоматы. М.: Энергия, 1970. – 88 с.
3. Jie Ji. Service Security Issues in the 5G Core Network and How to Detect Them. https://nsfocusglobal.com/new-architecture-new-challenges-service-security-issues-in-the-5g-core-network-and-how-to-detect-them/((дата обращения: 03.08.2022)
4. Буш Р., Мостеллер Ф. Стохастические модели обучаемости. - М.: Гос. изд-во физ.-мат. лит., 1962. – 483 с.
5. Прикладная статистка. Основы эконометрики: Учебник для вузов: в 2 т. 2-е изд., испр. – Т. 1: Айвазян С.А., Мхитарян В.С. Теория вероятностей и прикладная статистика. – М.: ЮНИТИ-ДАНА,2001. – 656 с.

УДК. 681.3
Моисеев Д.В., доктор технических наук, профессор, Барановский Ю.А., Цофнас Д.А., Скрябина Е.В.
Севастопольский государственный университет
ул. Университетская 33, г. Севастополь, Россия, 299053

РАЗРАБОТКА ВЕРОЯТНОСТНОГО УСТРОЙСТВА ИЗМЕРЕНИЯ МАТЕМАТИЧЕСКОГО ОЖИДАНИЯ НА БАЗЕ FPGA CYCLONE IV

Аннотация
В работе приводится решение задачи разработки устройства для вычисления математического ожидания случайного сигнала при вероятностном представлении данных, обладающего малым аппаратным объёмом и способностью обрабатывать сигнал в масштабе реального времени, реализованного на базе FPGA CYCLONE IV.
Ключевые слова: вероятностная форма представления информации, точность, вычислительное устройство, быстродействие, аппаратный объём, математическое ожидание, FPGA, CYCLONE IV.
Abstrac
The paper provides a solution to the problem of developing a device for calculating the mathematical expectation of a random signal with a probabilistic representation of data, which has a small hardware volume and the ability to process a signal in real time, implemented on the basis of the CYCLONE IV FPGA.
*Keywords: probabilistic form of information representation, accuracy, computing device, performance, hard*ware volume, mathematical expectation, FPGA, CYCLONE IV.

Введение. Изделие «Экспериментальный, опытно-демонстрационный образец «Вероятностный измеритель математического ожидания случайного сигнала»» относится к области автоматики и вычислительной технике и может быть использовано для измерения характеристик случайных процессов в системах автоматического контроля и управления [1-5].

Задачей, на решение которой направлено заявляемое образец является разработка устройства для вычисления математического ожидания случайного сигнала при вероятностном представлении данных, обладающего малым аппаратным объёмом и способностью обрабатывать сигнал в масштабе реального времени [5-8].

Решение технической задачи достигается путём использования вероятностной формы представления данных, в связи с чем изменяется

аппаратная реализация основных математических операций [1-3].

Техническим результатом, обеспечиваемым приведенной совокупностью признаков является уменьшение аппаратного объёма устройства вычисления математического ожидания случайного сигнала и возможности обработки входного сигнала в масштабе реального времени, достигаемым путём замены в прототипе цифровых компараторов, делителей и сумматоров на накопительные двоичные счетчики.

Целью является показ основных этапов прототипирования и кодирования экспериментального, опытно-демонстрационного образца «Вероятностный измеритель математического ожидания случайного сигнала» на базе FPGA CYCLONE IV.

Изложение основного материала. При выборе схемы реализации измерителя учитывались следующие положения:

- стремление к улучшению энергетической эффективности и универсальности вычислительных устройств;
- уменьшение аппаратурных затрат;1
- повышения быстродействия; точности и отказоустойчивости;
- применения вероятностной формы представления информации.

Исходя из данных положений был определен состав изделия, внешний вид которого представлен на рис.1.

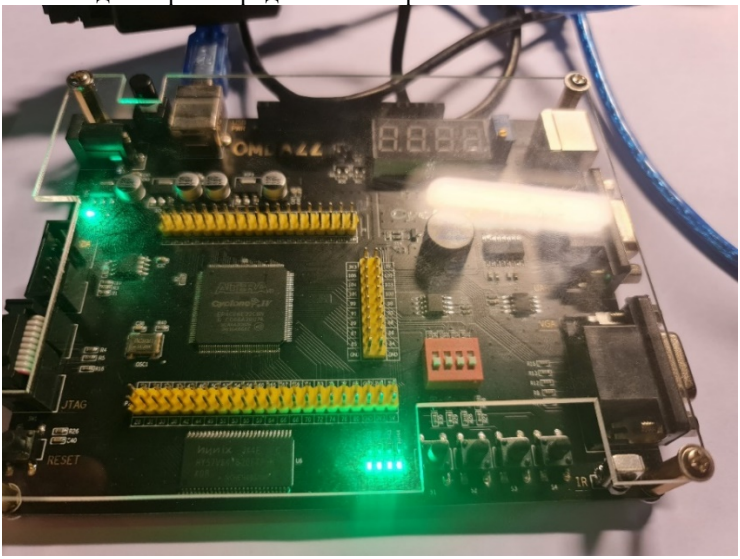


Рисунок 1 – Внешний вид печатной платы, на которой реализован экспериментальный, опытно-демонстрационный образец «Вероятностный измеритель математического ожидания случайного сигнала»

В состав образца входят следующие изделия:

1 – вероятностный преобразователь;

2 – двухвходовой конъюнктор;

3 – счетчик математического ожидания;

4 – генератор тактовых импульсов;

5 – счетчик произведения/

Сущность образца поясняется чертежом (рис. 2), на котором изображена функциональная схема вероятностного устройства вычисления математического ожидания.

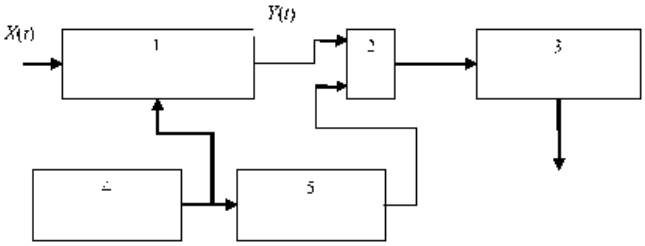


Рисунок 2 – Функциональная схема вероятностного устройства вычисления математического ожидания

Измеряемый сигнал X(t) поступает на тактируемый от генератора тактовых импульсов (4) вероятностный преобразователь (1), с выхода которого вероятностное отображение Y(t) через открытый вентиль (2) поступает в счетчик mx* (3), где суммируется. При переполнении счетчика N×K (5) вентиль (2) закрывается, и информация об оценке математического ожидания поступает на выход схемы [1-3].

Рассмотрим пример реализации вероятностного преобразователя. Принципиальная схема вероятностного преобразователя предназначен для преобразования входного позиционного кода в вероятностную форму представлена на рис.3.

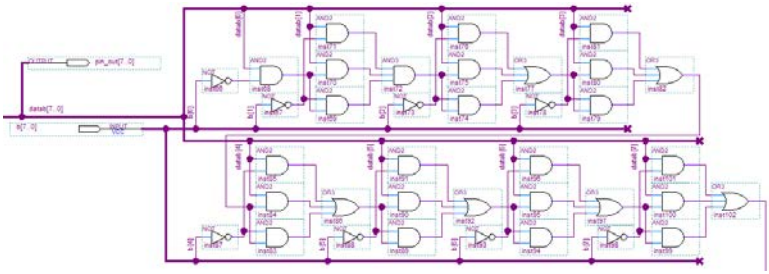


Рисунок 3 – Принципиальная схема вероятностного преобразователя

Общая принципиальная схема «Вероятностный измеритель математического ожидания случайного сигнала»» представлена на рис.4.

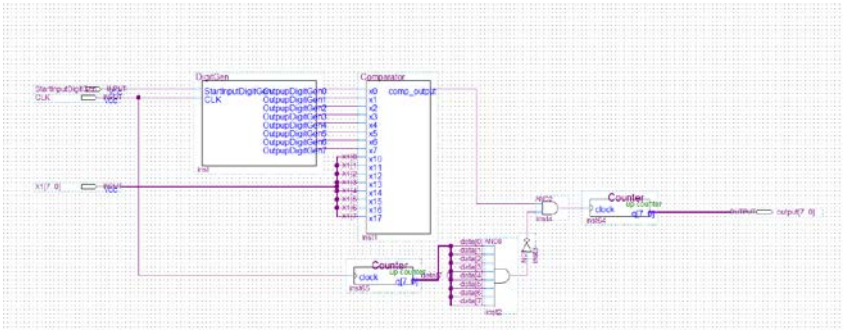


Рисунок 4 – Принципиальная схема экспериментального, опытно-демонстрационного образеца «Вероятностный измеритель математического ожидания случайного сигнала»»

Процессы в схеме предлагаемого устройства протекают в следующей последовательности. В начале работы значения счетчиков (3) и (5) сбрасываются, после чего начинается выполнение вычисления. На вход вероятностного преобразователя (1) подается измеряемый случайный сигнал $X(t)$. С выхода вероятностного преобразователя (1), тактуемого генератором тактовых импульсов (4), вероятностное отображение $Y(t)$ через открытый двухвходовой конъюнктор (2) поступает в счётчик математического ожидания (3), где подсчитывается количество единиц в вероятностном отображении $Y(t)$. Параллельно с вероятностным преобразователем (1), сигнал с генератора тактовых импульсов (4) тактует

счётчик произведения $N*K(5)$, при переполнении которого, двухвходовой конъюнктор (2) закрывается и информация об оценке математического ожидания в виде двоичного числа с параллельных выходов счётчика математического ожидания (3), поступает на выход всей схемы [1-3].

Выводы. На данном этапе построен прототип экспериментального, опытно-демонстрационного образца «Вероятностный измеритель математического ожидания случайного сигнала», который обладает малым аппаратным объёмом и способен обрабатывать сигнал в масштабе реального времени, реализованный на базе FPGA CYCLONE IV**.**

Работа выполнена при частичной поддержке Российского фонда фундаментальных исследований (грант № 19-29-06023/21), в рамках внутреннего гранта ФАОУ ВО СевГУ (грант № 31/06-31) и гранта Президента Российской Федерации МД-260.2022.1.6.

Список использованных источников

1. Патент № 2761500 C1 Российская Федерация, МПК G06F 17/18. Вероятностное устройство вычисления математического ожидания : № 2021101775 : заявл. 26.01.2021 : опубл. 08.12.2021 / Н. Е. Сапожников, Д. В. Моисеев, А. С. Захаров, А. Д. Костюков ; заявитель Федеральное государственное бюджетное военное образовательное учреждение высшего образования "Черноморское высшее военно-морское ордена Красной Звезды училище имени П.С. Нахимова" Министерства обороны Российской Федерации.

2. Моисеева, И. Н. Вероятностное устройство вычисления математического ожидания / И. Н. Моисеева, Д. В. Моисеев // Инновационные научные исследования. – 2021. – № 5-2(7). – С. 338-343. – DOI 10.5281/zenodo.5041221.

3. Моисеев, Д. В. Вероятностное устройство определения математического ожидания случайного процесса / Д. В. Моисеев // Перспективные направления развития отечественных информационных технологий : Материалы VI межрегиональной научно-практической конференции, Севастополь, 22–26 сентября 2020 года / Науч. ред. Б.В. Соколов. – Севастополь: Федеральное государственное автономное образовательное учреждение высшего образования "Севастопольский государственный университет", 2020. – С. 168-169.

4. Моисеев, Д. В. Вероятностное устройство вычисления спектральной плотности сигнала / Д. В. Моисеев, О. Д. Чужикова-Проскурнина // Автоматизация и приборостроение: проблемы, решения : Материалы Международной научно-технической конференции, Севастополь, 11–15 сентября 2017 года / Научный редактор В.Я. Копп. – Севастополь: Федеральное государственное автономное образовательное

учреждение высшего образования "Севастопольский государственный университет", 2017. – С. 151-152.

5. Skatkov, A. V. Adaptive vulnerability detection model for unmanned vehicles drugs based on artificial immune systems / A. V. Skatkov, A. A. Bryukhovetskiy, D. V. Moiseev // IOP Conference Series: Materials Science and Engineering, Krasnoyarsk, 18–21 ноября 2019 года / Krasnoyarsk Science and Technology City Hall of the Russian Union of Scientific and Engineering Associations. – Krasnoyarsk: Institute of Physics and IOP Publishing Limited, 2020. – P. 12028. – DOI 10.1088/1757-899X/734/1/012028.

6. Modeling of monitoring processes of structurally heterogeneous technological objects / A. Skatkov, V. Shevchenko, D. Voronin, D. Moiseev // MATEC Web of Conferences, Sevastopol, 11–15 сентября 2017 года. – Sevastopol: EDP Sciences, 2017. – P. 03022. – DOI 10.1051/matecconf/201712903022.

7. Оценка погрешностей выполнения вероятностных арифметических операций сложения и умножения / Н. Е. Сапожников, Д. В. Моисеев, П. С. Бейнер, Н. В. Бейнер // Восточно-Европейский журнал передовых технологий. – 2013. – Т. 3. – № 4(63). – С. 40-42.

8. Скатков, А. В. Методология организации мониторинговых процессов при решении крупномасштабных задач в облачных вычислительных средах / А. В. Скатков, А. А. Брюховецкий, Д. В. Моисеев // Информационные технологии и информационная безопасность в науке, технике и образовании "ИНФОТЕХ - 2017" : сборник статей Всероссийской научно-технической конференции, Севастополь, 18–20 сентября 2017 года / Севастопольский государственный университет, Институт «Информационные технологии и управление в технических системах». – Севастополь: Федеральное государственное автономное образовательное учреждение высшего образования "Севастопольский государственный университет", 2017. – С. 78-80.

УДК. 681.3
Моисеев Д.В., доктор технических наук, профессор, Цофнас Д.А., Бородин В.Д., Михайлова О.С.
Севастопольский государственный университет
ул. Университетская 33, г. Севастополь, Россия, 299053

РАЗРАБОТКА МОДУЛЯ ВЕРОЯТНОСТНОГО ПРЕОБРАЗОВАНИЯ И ВОССТАНОВЛЕНИЯ ИНФОРМАЦИИ

Аннотация
В работе приводится реализация программы предназначенной для моделирования работы вероятностного кодера/декодера информации, которая может применяться в различных предметных областях, где имеется необходимость выполнения преобразования информации в вероятностную форму представления и преобразования с последующей обработкой в виде вероятностных отображений с дальнейшим её обратным преобразованием. Инструментальным базисом разработки является язык С++. Программа обеспечивает выполнение следующих функций: генерацию псевдослучайных вспомогательных последовательностей с равномерным законом распределения; вероятностного преобразования информации; обратного преобразования информации из вероятностного представления.
Ключевые слова: вероятностная форма представления информации, точность, вычислительное устройство, быстродействие, аппаратный объём, математическое ожидание, FPGA, CYCLONE IV.
Abstract
The paper presents the implementation of a program designed to simulate the work of a probabilistic encoder / decoder of information, which can be used in various subject areas where there is a need to convert information into a probabilistic form of representation and transformation, followed by processing in the form of probabilistic mappings with its further reverse transformation. The instrumental basis of development is the C++ language. The program provides the following functions: generation of pseudorandom auxiliary sequences with a uniform distribution law; probabilistic transformation of information; inverse transformation of information from a probabilistic representation.
Keywords: probabilistic form of information representation, accuracy, computing device, performance, hardware volume, mathematical expectation, FPGA, CYCLONE IV.

Введение. Настоящий период развития теоретических положений, методов и алгоритмов синтеза устройств вычислительной техники

(ВТ), используемых при разработке перспективных и совершенствовании существующих информационных систем (ИС), характеризуется интенсивным поиском новых принципов обработки и хранения информации, построения вычислительных архитектур и систем с привлечением современных технологий, среди которых технология вероятностного представления и преобразования информации (ВППИ) является одной из наиболее перспективных. В общем виде суть стохастического или вероятностного преобразования информации в непозиционное вероятностное отображение (ВО) заключается в том, что любому значению преобразуемой величины можно привести в соответствие некоторую вероятность – вероятность того, что значение преобразуемой величины будет больше величины, сгенерированной случайным образом внутри диапазона изменения преобразуемой величины. Реализация вычислительных устройств (ВУ), выполняющих арифметические и логические операции над ВО, приводит к многократному уменьшению аппаратного объёма ВУ, а само ВППИ обеспечивает помехоустойчивость и криптографическую стойкость обрабатываемой и передаваемой информации. Развитие современных, а также создание перспективных информационных систем (ИС) требует создания единой архитектуры, с унифицированным аппаратным и программным обеспечением на базе комплексной интеграции не только на техническом, но и на функциональном уровне входящих в состав ИС компонент [1-7]. Реализация приведённой структуры приводит к многократному увеличению объемов вычислений над массивами данных большой разрядности, проводимых в реальном масштабе времени, усложнению вычислительных алгоритмов. Вследствие этого возникают острые противоречия между аппаратными затратами, быстродействием, точностью и отказоустойчивостью. Данная работа посвящена вопросу моделирования работы вероятностного преобразователя информации и оценки его эффективности.

Целью работы является реализация программы предназначенной для моделирования работы вероятностного кодера/декодера информации.

Изложение основного материала. В простейшем случае вероятностного представления информации – однолинейном однополярном представлении информации в виде ВО значение преобразуемой величины либо всегда положительно, либо всегда отрицательно, а сам процесс преобразования выполняется в соответствии с правилом (1):

$$y_{ij} = \begin{cases} 1 \ \text{при} \ x_i > R(t_{ij}) \\ 0 \ \text{при} \ x_i \le R(t_{ij}) \end{cases}, \qquad (1)$$

где

x_i - *i*-е значение преобразуемого сигнала $X(t)$;

$R(t_{ij})$ - *j-е* значение параметра вспомогательного случайного сигнала $R(t)$, изменяющегося в интервале изменения $X(t)$;

$i = \overline{1,N}$ - число циклов преобразования сигнала $X(t)$;

$j = \overline{1,K}$ - количество статистических испытаний каждого значения x_i внутри временного интервала $\Delta t_i = t_{i+1} - t_i$; y_{ij} - значение ВО параметра сигнала x_i из ряда:

$$Y_i(t) = \{y_{i1}; y_{i2}; ... y_{ij}; ... y_{iK}\}. \quad (2)$$

ВО обладает свойствами синхронности и независимости каждого члена отображения от любого другого. Использование этих свойств и применение представления информации в виде ВО позволяет упростить функциональные узлы для выполнения арифметических и логических операций, в частности, сложения, вычитания, умножения, возведения в целую степень, деления, компарации и т.д. и, тем самым, значительно уменьшить их аппаратный объём.

Поскольку для представления информации в виде ВО основным является вероятностный характер формирования последовательности из «1» и «0» и вероятностный характер количества «1» в последовательности, это и приводит к дополнительной погрешности вероятностного преобразования.

Для уменьшения, а в граничном случае устранения погрешности вероятностного преобразования, следует отказаться от второй характерной особенности ВО.

Для данного случая введено понятие «псевдовероятностное» представление информации, для которого изменяется сам алгоритм формирования ВО (1) и заранее задаётся в нём количество «1» в соответствии с выражением:

$$P(y_{ij} = 1) = x_i. \quad (3)$$

При этом, для сохранения свойств ВО, распределение единиц в псевдовероятностном отображении должно оставаться случайным.

Для однолинейного однополярного представления информации в виде псевдовероятностного отображения значение преобразуемой вели-

чины либо всегда положительно, либо всегда отрицательно, а само псевдовероятностное отображение, в соответствии с (2), будет иметь вид:

$$Y_i(t) = \{y_{i1}; y_{i2}; ...y_{ig}; ...y_{iG}\}, \quad (4)$$

где $g = \overline{1,G}$ – номер разряда в ВО, причём $G=2^L-1$, где L – количество разрядов, необходимое для позиционного представления преобразуемого значения X_i.

Структурная схема преобразователя цифровой информации в непозиционное псевдовероятностное отображение представлена на Рис. 1.

Для того, чтобы количество «единиц» в псевдовероятностном отображении было строго равно весу преобразуемого значения X_i, необходимо, чтобы вероятность появления одной «единицы» в псевдовероятностном отображении $Y_i(t)$ была равна:

$$P(y_{ij} = 1) = P_j(Z = Z_l) = \frac{x_i}{2^L - 1}. \quad (6)$$

Время преобразования $t_{пр}$ также пропорционально x_i, то есть:

$$t_{пр} = \frac{x_i}{f_{такт}}, \quad (7)$$

где $f_{такт}$ – тактовая частота работы ВП.

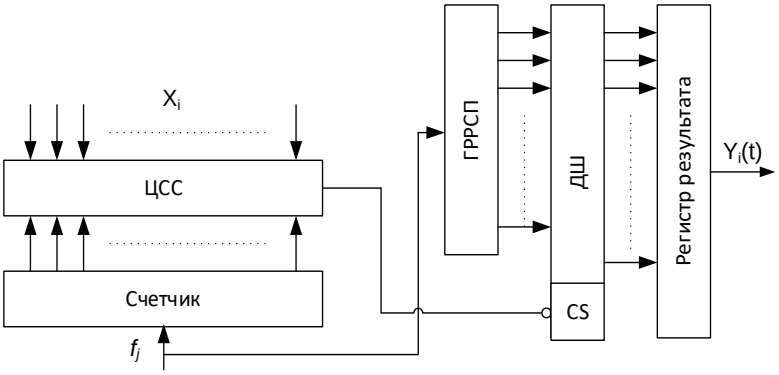


Рисунок 1 – Структурная схема преобразователя цифровой информации в непозиционное псевдовероятностное отображение

В состав данной схемы входят:

- ДШ – дешифратор.
- Счетчик.
- ЦСС – цифровая схема сравнения на «равенство».
- Регистр результата.
- ГРРСП – генератор равномерно распределенных случайных последовательностей.

На Рис. 2 представлен внешний вид модуля вероятностного преобразования и восстановления информации.

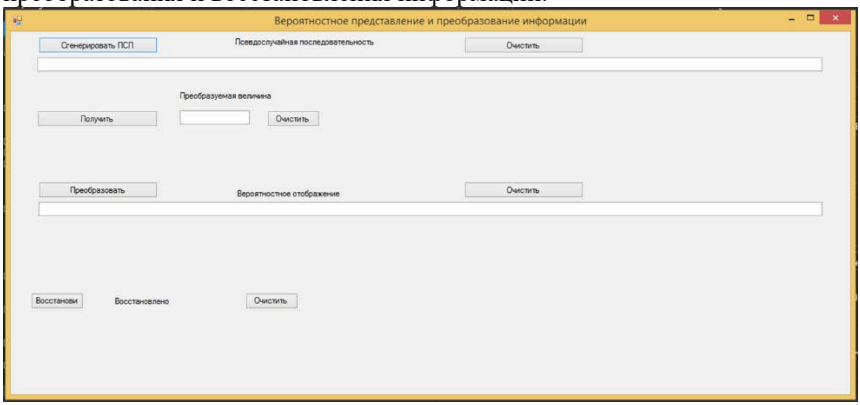


Рисунок 2 – Модуль вероятностного преобразования и восстановления информации.

Выводы. Реализована программа предназначеная для моделирования работы вероятностного кодера/декодера информации, которая может применяться в различных предметных областях, где имеется необходимость выполнения преобразования информации в вероятностную форму представления и преобразования с последующей обработкой в виде вероятностных отображений с дальнейшим её обратным преобразованием.

Работа выполнена при в рамках гранта Президента Российской Федерации МД-260.2022.1.6.

Список использованных источников

9. Свидетельство о государственной регистрации программы для ЭВМ № 2021665633 Российская Федерация. Модуль вероятностного преобразования и восстановления информации : № 2021664738 : заявл. 21.09.2021 : опубл. 30.09.2021 / Д. В. Моисеев, А. Г. Шокин, О. С. Михайлова, А. А. Пахомова ; заявитель Федеральное государственное автономное образовательное учреждение высшего образования «Севастопольский государственный университет».

10. Modelling performing calculations over the data presented in a probabilistic form / N. Sapozhnikov, A. Polyakov, A. Bryukhovetskiy, D. Moiseev // MATEC Web of Conferences : 2018 International Conference on Modern Trends in Manufacturing Technologies and Equipment, ICMTMTE 2018, Sevastopol, 10–14 сентября 2018 года. – Sevastopol: EDP Sciences, 2018. – P. 04019. – DOI 10.1051/matecconf/201822404019.
11. Выполнение параллельных вычислений при вероятностном представлении данных / Н. Е. Сапожников, Д. В. Моисеев, П. С. Бейнер, Н. В. Бейнер // Технологический аудит и резервы производства. – 2013. – Т. 3. – № 1(11). – С. 9-12.
12. Моисеев, Д. В. Выполнение арифметических операций сложения и умножения над вероятностно представленными параллельными данными / Д. В. Моисеев, Н. Е. Сапожников // Многоядерные процессоры, параллельное программирование, ПЛИС, системы обработки сигналов. – 2015. – Т. 1. – № 5. – С. 46-54.
13. Оценка погрешностей выполнения вероятностных арифметических операций сложения и умножения / Н. Е. Сапожников, Д. В. Моисеев, П. С. Бейнер, Н. В. Бейнер // Восточно-Европейский журнал передовых технологий. – 2013. – Т. 3. – № 4(63). – С. 40-42. – EDN QCJYOT.
14. Шокин, А. Г. Новые методы помехоустойчивого кодирования информации / А. Г. Шокин, Н. Е. Сапожников, Д. В. Моисеев // Восточно-Европейский журнал передовых технологий. – 2012. – Т. 6. – № 9(60). – С. 26-30. – EDN QBGNGR.
15. Моисеев, Д. В. Вероятностное представление информации в экологическом мониторинге / Д. В. Моисеев // Экологическая, промышленная и энергетическая безопасность - 2018 : сборник статей по материалам международной научно-практической конференции, Севастополь, 24–27 сентября 2018 года / под ред. Л. И. Лукиной, Н. А. Бежина, Н. В. Ляминой. – Севастополь: Федеральное государственное автономное образовательное учреждение высшего образования "Севастопольский государственный университет", 2018. – С. 821-823.

ИТ-ПРОДУКТЫ И УСЛУГИ. ИМПОРТОЗАМЕЩЕНИЕ И ТЕХНОЛОГИЧЕСКАЯ БЕЗОПАСНОСТЬ ИТ-СФЕРЫ

УДК 004.056.5

Е.С. Пуеров, ведущий специалист по защите информации
ФГБОУ ВО «Югорский государственный университет»

ОБЕСПЕЧЕНИЕ ИНФОРМАЦИННОЙ БЕЗОПАСНОСТИ В ЮГОРСКОМ ГОСУДАРСТВЕННОМ УНИВЕРСИТЕТЕ ПРИ ВЗАИМОДЕЙСТВИИИ С ГИС СЦОС

Аннотация
Данная статья посвящена вопросу подключения к государственным информационным системам органов государственной власти Российской Федерации и выполнению требований по информационной безопасности при таких подключениях.
Ключевые слова: государственная информационная система, технические условия, средства защиты информации.
Annotation
This article is devoted to the issue of connecting to state information systems of state authorities of the Russian Federation and the fulfillment of information security requirements for such connections.
Key words: state information system, specifications, information protection means.

В ходе образовательной деятельности Югорский государственный университет осуществляет взаимодействие с информационной системой «Современная цифровая образовательная среда» (далее – ГИС СЦОС), созданной постановлением Правительства Российской Федерации от 16 ноября 2020 года № 1836. Требования, предъявляемые к защите информации в ГИС, регламентируются нормативными правовыми актами Российской Федерации [1, 2].

Для подключения к ГИС СЦОС установлены и настроены следующие средства защиты информации и средство криптографической защиты информации:

1. Средство защиты информации Secret Net Studio с дополнительным модулем межсетевого экрана. Secret Net Studio представляет собой комплексное решение для защиты рабочих станций и серверов на уровне данных, приложений, сети, операционной системы и периферийного оборудования.

2. Антивирусное средство Kaspersky Endpoint Security для Windows - включает передовую многоуровневую защиту от угроз, проактивные технологии, такие как контроль программ, веб-контроль и контроль устройств, средства управления уязвимостями и установкой исправлений.

3. Средство криптографической защиты информации Континент TLS-Клиент – представляет собой локальный прозрачный прокси-сервис, который обеспечивает обоюдную аутентификацию с сервером ГИС СЦОС, установку защищенного соединения, обмен зашифрованными данными с сервером.

Схема подключения к ГИС СЦОС представлена на рисунке 1.

Рисунок 1 - Схема подключения к ГИС СЦОС

Установка и настройка всех средств защиты информации выполнена специалистами Университета самостоятельно с оформлением соответствующего акта. Выполненный комплекс мер организационного и технического характера направлен на сохранение и защиту информации, в том числе персональных данных студентов Университета, при передаче по открытым каналам связи в ГИС СЦОС.

Библиографический список

1. Федеральный закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации».
2. Приказ ФСТЭК России от 11.02.2013 №17 «Об утверждении требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах».

УДК 004.7, 644.129
А.В. Шицелов, старший преподаватель
Ю.А. Тукмачева, магистрант
ФГБОУ ВО «Югорский государственный университет»

ОПТИМИЗАЦИЯ ПОТРЕБЛЕНИЯ ТЕПЛОНОСИТЕЛЯ В СИСТЕМЕ ОТОПЛЕНИЯ В РАМКАХ ИНДИВИДУАЛЬНОГО ЖИЛОГО ПРОСТРАНСТВА

Аннотация
В данной статье предлагается способ создания системы оптимального использования ресурсов в рамках индивидуального жилого пространства отопления посредством использования системы умного дома и управляемых устройств контроля подачей теплоносителя в систему отопления квартиры. В ходе исследования получена архитектура системы, в которой имеется 2 контура контроля: локальный сервер умного дома и автономный контур из контроллеров климата. Оба контура имеют проводную связь по протоколу Modbus.
Ключевые слова: умный дом, автоматизация, оптимизация ресурсов, Modbus, проектирование.
Annotation
This article proposes a method for creating a system for the optimal use of resources within an individual living space for heating by using a smart home system and controlled devices for controlling the supply of coolant to the apartment heating system. In the course of the study, the architecture of the system was obtained, in which there are 2 control loops: a local smart home server and an autonomous loop of climate controllers. Both circuits are wired via the Modbus protocol.
Key words: smart home, automation, resource optimization, Modbus, design.

Местом для оптимизации потребления ресурсов была выбрана квартира, а не многоквартирный дом, так как это обеспечивает индивидуальный подход к решению проблемы оптимального использования ресурсов. В этом случае результаты работы будут представлены не виде общей статистики, а в качестве конкретной выгоды для жильцов отдельной квартиры. Исходя из этого в качестве средства для контроля потребления ресурсов будет выступать класс систем под названием «умный дом» [1, 2].

При выборе физической архитектуры системы следует обращать внимание на такие характеристики как доступность, автономность, отказоустойчивость, возможность интеграции и используемый канал связи для интеграции. В качестве канала связи между частями системы

была выбрана шина RS-485 с протоколом общения Modbus. Одним из немногих устройств, поддерживающих данную архитектуру сети, являются автономные климат контроллеры от компании Tuya. В данной архитектуре оптимизация будет производится за счет автоматизации контроля за работой системы отопления.

Архитектура системы должна состоять из 2-х частей: локальный сервер и автономный контур управления отоплением. Что позволит получить централизованное управление системой и сбор статистических данных, но при этом в случае нарушения связи между сервером и контроллерами даст возможность системе функционировать автономно. Данная архитектура представлена на рисунке 1.

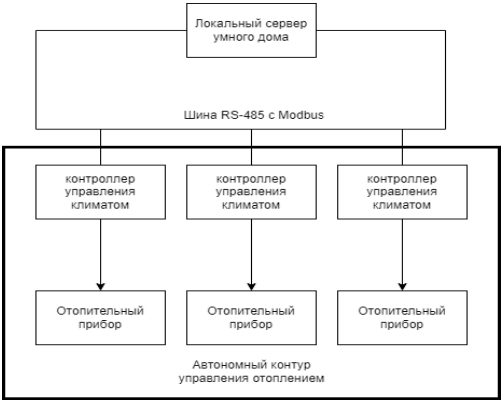


Рисунок 1 – Архитектура системы

Библиографический список:

1. Дмитриева, Н. Н. Использование энергосберегающих технологий на основе системы "умный дом" при строительстве многоквартирных домов / Н. Н. Дмитриева, О. И. Плотникова, М. А. Романов // Фотинские чтения. – 2017. – № 2(8). – С. 138-141.

2. Серебряник, И. А. Интеллектуальные системы в российских домах ("умный дом"): роскошь или возможность экономии / И. А. Серебряник, Т. Я. Дружинина // Актуальные проблемы гуманитарных и естественных наук. – 2010. – № 11. – С. 109-111**.**

ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ В МОРЕХОЗЯЙСТВЕННОЙ ДЕЯТЕЛЬНОСТИ

УДК 004.89

А. В. Митько[1], вице-президент, доц., канд. техн. наук, В. К. Сидоров[2]
[1]Арктическая общественная академия наук
Искровский пр-т 22 офис 175, г. Санкт-Петербург, Россия, 193168
[1]Всероссийский научно-исследовательской институт метрологии имени Д.И. Менделеева
Московский пр-т 19, г. Санкт-Петербург, Россия, 190005
e-mail: arseny73@yandex.ru
[2]Санкт-Петербургский университет ГПС МЧС России
Московский пр-т 149, г. Санкт-Петербург, Россия, 196105
e-mail: hamradio-spb@yandex.ru

РАЗВИТИЕ ЦИФРОВЫХ СИСТЕМ В АРКТИЧЕСКОМ РЕГИОНЕ

Аннотация
В статье рассматриваются проблемы и перспективы развития перспективных цифровых систем. Отмечены актуальность и востребованность цифровизации всех сфер деятельности человека в Арктической зоне Российской Федерации, как одной из экстремальных территорий. Основные результаты получены в совместных разработках Арктической общественной академии наук и Санкт-Петербургского университета ГПС МЧС России.

Ключевые слова: цифровые системы, цифровизация, мониторинг, Арктика, искусственный интеллект, информационные технологии, связь

A. Mitko[1], V. Sidorov[2]
[1]Arctic Public Academy of Sciences
Iskrovskij pr., 22, office 175, Saint-Petersburg, Russia, 193168
[1]D. I. Mendeleev All-Russian research institute of metrology
Moskovskij pr., 19, Saint-Petersburg, Russia, 190005
e-mail: arseny73@yandex.ru
[2]Saint-Petersburg university of State fire service of EMERCOM of Russia
Moskovskij pr., 149, Saint-Petersburg, Russia, 196105
e-mail: hamradio-spb@yandex.ru

DEVELOPMENT OF DIGITAL SYSTEMS IN THE ARCTIC REGION

Abstract
The article deals with the problems and prospects for the development of promising digital systems. The relevance and demand for digitalization of all spheres of human activity in the Arctic zone of the Russian Federation, as one

of the extreme territories, is noted. The main results were obtained in the joint developments of the Arctic Public Academy of Sciences and St. Petersburg University of the State Fire Service of the Ministry of Emergency Situations of Russia.
Keywords: digital systems, digitalization, monitoring, Arctic, artificial intelligence, information technology, communications

Искусственный интеллект способен решать практические задачи для нужд Крайнего Севера в самых различных сферах – от управления городами до регулирования тепла в квартирах северян.

Так, авторы проекта «SEVER / СЕВЕР» предлагают видение будущего городов Крайнего Севера под управлением искусственного интеллекта. Созданный автоматизированный промышленный комплекс устранит потребность в значительной части человеческого труда, который необходим сейчас. Вместо того, чтобы самостоятельно работать в суровых арктических условиях, люди могли бы, прежде всего, осуществлять функции надзора за работой машин [1].

Директор ООО «Технологии комфорта» из Якутска, человек, не понаслышке знающий, что такое экстремальные условия Севера, выпускник Физико-технического института Северо-Восточного федерального университета им. Аммосова (СВФУ) Айыысхан Алексеев разработал нейрокогнитивную машину, которая решает задачи в области нейросетевых технологий, сопряжённых с проблемой создания искусственного интеллекта. Он и другие молодые инженеры представили проект «умного» дома Robo-house. Его компания выиграла в конкурсе бизнес-проектов «Идея на миллион» и получила 1 млн руб. от венчурной компании «Якутия» [2].

Министерство промышленности и торговли РФ реализует проект по созданию Фабрик будущего – систем комплексных технологических решений (интегрированных технологических цепочек), обеспечивающих в кратчайшие сроки проектирование и производство глобально конкурентоспособной продукции нового поколения. В рамках создания дорожной карты «Технет», направленной на цифровизацию промышленности, опорные точки могут быть созданы и в арктических городах. Их основа – Big data и искусственный интеллект. Самый большой атомный ледокол «Арктика» на Балтийском заводе в Санкт-Петербурге строился также при помощи цифровых систем проектирования и сборки [3].

В программе развития Федерального исследовательского центра «Кольский научный центр РАН» (КНЦ РАН) основными ориентирами и точками развития в ближайшем будущем должны стать наноматериалы, нанотехнологии, а также и технологии искусственного интеллекта

[4]. В структуре КНЦ в городе Апатиты успешно работает Институт информатики и математического моделирования. Основные исследования, проводимые в Институте, сосредоточены на развитии перспективных и значимых для Арктической зоны РФ направлений в области решения задач формирования электронной (цифровой) экономики России, разработки и развития проблемно-ориентированных информационных технологий, методов и средств компьютерного моделирования, представления и обработки междисциплинарных знаний, человеко-машинного взаимодействия, информационно-аналитических систем поддержки принятия решений при осуществлении различных видов деятельности в Арктике.

В Институте разработаны и используются основанные на методах системного анализа и искусственного интеллекта технологии моделирования и прогнозирования устойчивого развития социальноэкономических систем Арктической зоны РФ, методы оценки системных рисков развития моногородов Севера России, средства информационной поддержки ситуационных центров для управления региональной безопасностью. Институт имеет богатый опыт по подготовке научных кадров и научно-образовательной деятельности. В Институте работает пять докторов наук, двенадцать кандидатов наук.

Рассмотрим подробнее применение искусственного интеллекта и цифровых систем в различных сферах хозяйственной деятельности человека в Арктике.

Закономерно, что наибольшую активность в сфере добычи и переработки полезных ископаемых проявляют компании, реализующие мегапроекты, и представители инновационных кластеров.

Известно, что добыча газа в условиях Заполярья сопряжена с необходимостью решения целого комплекса вопросов. В частности, серьёзной проблемой для газодобытчиков является предупреждение гидратообразования в газосборных шлейфах. Её решают подачей в трубопроводы ингибитора – метанола.

Для минимизации расхода метанола в ООО «Газпром добыча Ямбург» была разработана инновационная технология предупреждения гидратообразования, реализуемая интеллектуальной автоматизированной системой управления технологическими процессами. Суть в том, что метанол в необходимых объёмах подают в шлейф только тогда, когда начинается процесс гидратообразования. Для этого контролируют ход реальных процессов с параллельным их моделированием с использованием искусственного интеллекта управляющей системы. Поскольку в условиях Крайнего Севера автоматизированная система

управления работает нестабильно, специалистами компании решены задачи оперативного выявления отказов и определены необходимые алгоритмы оперативных действий. Это технологическое решение запатентовано. Результат применения в том, что только на снижении расхода метанола предприятию удаётся ежегодно экономить свыше 4 млн руб. Соответственно уменьшается и нагрузка на окружающую среду.

И это только одна из целого комплекса технологий, которые успешно применяются на месторождениях ООО «Газпром добыча Ямбург».

В компании постоянно решается ряд задач, вводятся элементы искусственного интеллекта для повышения надёжности ведения технологических процессов, используются возможности работы интеллектуальных управляющих систем при поступлении нечёткой информации, например, отказах измерительных каналов. Найденные решения патентуются как изобретения и внедряются в производство.

Специалистами компании выявлены специфические особенности построения интеллектуальных систем для нефтегазоконденсатных месторождений Крайнего Севера; описаны принципы функционирования технологических объектов автоматизации; приведено общее состояние автоматизации газопромысловых объектов Ямбургского нефтегазоконденсатного месторождения; выявлены особенности освоения нефтегазоконденсатных месторождений Крайнего Севера, связанные с проблемами автоматизации и моделирования технологических процессов газопромысловых объектов; разработаны и исследованы математические модели установок комплексной подготовки газа. В компании на повестке дня – решение 18 вопросов интеллектуализации системы управления газопромысловых объектов: построение гибридных интеллектуальных систем, систем управления на базе нечёткой логики и математики; общая методология построения распределенных интеллектуальных мультиагентных систем; применение теория принятия решений в условиях несовершенной информации [5].

Компании «Газпром» для обслуживания скважин на арктическом шельфе нужны автономные морские роботы, способные работать на глубине до 500 м, управляться с берега, запускаться со льда или из подледного состояния в любую погоду. Об этом заявил начальник службы перспективного развития «Газпром добыча шельф Южно-Сахалинск» Тамаз Барамидзе. По его словам, ни в России, ни за рубежом аппаратов, отвечающих этим запросам, пока нет [6]. Для работы по обслуживанию скважин на арктическом шельфе «Газпрому» требуются роботы, базирующиеся не на судах, а на берегу, спускаемые со льда, работающие автономно круглый год и в любую погоду на расстоянии до 300 км от

берега. В настоящее время компания вынуждена использовать телеуправляемые аппараты судового базирования. При этом экономика проекта такова, что 80% средств идёт на оплату работы судов, а на все выполняемые операции – 20%. В связи с тем, что большая часть шельфовых месторождений, разрабатываемых Россией, находится в Арктике или Субарктике, то времени для работ подводных необитаемых аппаратов крайне мало. Например, на Киринском газоконденсатном месторождении в Охотском море с ноября по июнь стоит лед, и в этот период оборудование, находящееся под водой, не доступно для обследования и ремонта. По словам Тамаза Барамидзе, в задачи подводных беспилотных аппаратов входят регламентные и ремонтно-восстановительные работы, обследование акватории и дна, уборка посторонних предметов, а также съемка, очистка оборудования от обрастания водорослями и илом, сварка и экологический мониторинг. Он отметил, что компания сама не может провести конкурс среди разработчиков морской робототехники на создание морских роботов по заявленным параметрам, поскольку не обладает нужным уровнем экспертизы и не может тратить деньги на инвестиционные проекты так же свободно, как раньше. По его мнению, конкурс могло бы провести Минобрнауки РФ с учетом того, что морские роботы с заданными параметрами пригодятся не только добывающим компаниям, но и при спасательных операциях и осуществлении экологического мониторинга [7].

В России ведется разработка прототипа подводной роботизированной буровой платформы. Её планируют использовать для разработки месторождений углеводородов на шельфе Северного ледовитого океана. Буровая платформа будет полностью автономной как в техническом обслуживании, так и в электропитании, поэтому ей не нужен постоянный обслуживающий персонал. Она сможет самостоятельно устранять нештатные ситуации, её работу будут контролировать дистанционно с берега. Проект выполнил Фонд перспективных исследований при участии органов исполнительной власти, производителей морской техники и нефтегазовых компаний. Следующим шагом станет создание прототипов и их испытание в реальных условиях. Особенность будущей платформы – компактные размеры: высота – 30 м, ширина – 25 м, возможность работать на дне Северного Ледовитого океана подо льдом. Она предназначена для бурения вертикальных, наклонных и горизонтальных разведочных нефтяных и газовых скважин. Разработчики рассчитывают, что создание прототипа позволит привлечь инвесторов и заказчиков. На первом этапе предполагают, что созданный демонстратор будет способен бурить на глубину нескольких сотен метров. В итоговом варианте она должна обеспечить создание скважин длиной до 3,5

км на морских глубинах от пятидесяти до четырехсот метров. После освоения месторождения платформу перевезут на новое место бурения [8].

Практически все специалисты указывают на большой потенциал искусственного интеллекта в поиске и спасении людей в Арктике и субарктических регионах. Отрадно, что в России полным ходом идет разработка таких уникальных по мировым стандартам систем.

К 2022 г. планируется, что спасательными работами в Арктике займутся группы роботов. Они смогут оказывать помощь отрезанным от внешнего мира и терпящим бедствие нефтяникам, газовикам и полярным экспедициям. Воздушные и наземные дроны, объединенные с помощью искусственного интеллекта, сумеют при минимальном вмешательстве операторов найти и эвакуировать пострадавших.

Такая необычная служба спасения, основанная на роботах, дронах и искусственном интеллекте, – совместная разработка МЧС России и Центрального научно-исследовательского и опытно – конструкторского института робототехники и технической кибернетики (ЦНИИ РТК) [9]. Предполагается использовать два типа роботов – воздушных и наземных. Группа небольших БПЛА должна определять координаты терпящих бедствие. Эти дроны будут вести навигационную разведку маршрута и в режиме реального времени создавать электронную карту местности. Наземный отряд в виде роботизированных платформ амфибийного типа займется поиском и транспортировкой терпящих бедствие. Планируется, что один дрон будет способен эвакуировать до двадцати человек. Сейчас разработчики определяют, какими должны быть эти аппараты: на гусеничном или шнекороторном ходу. На дальние расстояния дроны-спасатели будут перемещать самолетами, а поскольку на судне нет пилота, робот сможет выдержать даже «жесткое» десантирование с воздушного транспорта [10].

В настоящее время ученые создают сложный алгоритм, чтобы научить дроны действовать в группе.

При этом электроника сможет корректировать полученные задания.

Заместитель главного конструктора ЦНИИ РТК Сергей Половко поясняет, что именно так будет формироваться искусственный интеллект системы со строгой иерархией уровней управления. На самом верхнем из них находится человек-оператор, в исключительной ситуации управление на себя может взять один из роботов с большими вычислительными мощностями. Проект является уникальным и полезным с практической и с научной точки зрения. Он может послужить толчком для развития этой технологии по всему миру. Технология группового

управления дронами считается одной из самых перспективных в робототехнике.

АО «Вертолеты России» в середине 2020 г. начали летные испытания беспилотного вертолета VRT-300 Arctic Supervision с радаром бокового обзора для ведения ледовой разведки и эксплуатации в условиях Арктики. Директор программ компании «Вертолеты России» Андрей Панасюк сделал прогноз о том, что широкое использование беспилотных летательных аппаратов для ледовой разведки, поиска пропавших людей и других целей в Арктике может начаться уже в ближайшие два года.

Понимают необходимость внедрения интеллектуальных систем спасения и в самих северных регионах. Распространение беспилотников в Арктическом регионе при должном регулировании может помочь сотрудникам экстренных служб. Об этом заявила начальник службы робототехнических средств пожарной службы республики Карелия Ксения Чекуева. Она высказала идею, что частные беспилотники также могут в перспективе применяться для мониторинга объектов, представляющих потенциальную опасность.

Современные инновационные технологии помогут России сделать Арктику более комфортной и безопасной для жизни и ведения хозяйственной деятельности. Многие ученые считают, что в будущем искусственный интеллект способен освободить нас от выполнения рутинных задач во многих сферах, особенно в экстремальных условиях. Жесткие условия среды в Арктике, не всегда совместимые с нормальной человеческой жизнью, требуют максимального средоточия технического и интеллектуального потенциала общества и государства. Необходимо понимать, что статус ведущей мировой арктической державы в настоящее время уже не дается только по географическому положению, а требует постоянной и упорной работы по всем направлениям, в т.ч. и в инновациях.

Библиографический список

1. В Росатоме создают цифровую модель безэкипажного судна для Арктики [Электронный ресурс] // РИА Новости. – 05.04.2018. – URL: https://ria.ru/atomtec/20180405/1517956613.html (дата обращения 08.08.2022).
2. Власти РФ не отказались от строительства на Адмиралтейских верфях ледостойкой платформы Северный полюс взамен дрейфующим обсерваториям в Арктике [Электронный ресурс] // Neftegaz.RU. – 09.10.2017. – URL: https://neftegaz.ru/news/view/165640-Vlasti-RF-ne-otkazalis-otstroitelstva-na-Admiralteyskih-verfyah-ledostoykoy-platformy-

Severnyj-polyus-vzamen-dreyfuyuschim-observatoriyam-v-Arktike (дата обращения 08.08.2022).
3. Газпрому нужен искусственный интеллект [Электронный ресурс] // Рамблер. – 10.10.2017. – URL: https://news.rambler.ru/other/38118738-gazpromu-nuzhen-iskusstvennyy-intellekt/ (дата обращения 08.08.2022).
4. Газпрому нужен искусственный интеллект [Электронный ресурс] // ИА «Север-Пресс – Новости Ямала». – 10.10.2017. – URL: http://sever-press.ru/ekonomika/neft-i-gaz/item/33365-gazpromu-nuzhen-iskusstvennyj-intellekt (дата обращения 08.08.2022).
5. Головкин, К., Качалин, Ф. Ничья земля: Арктика в лучах лазерного радара [Электронный ресурс] // STRELKA. – 20.04.2017. – URL: https://beta.strelkamag.com/ru/article/arctic-fieldtrip (дата обращения 08.08.2022).
6. Губкинцы снова покоряют Арктику [Электронный ресурс] // РГУ нефти и газа. – 10.10.2016. – URL: https://gubkin.ru/news2/detail.php?ID=36813. (дата обращения 08.08.2022).
7. Газпрому нужен искусственный интеллект [Электронный ресурс]// Рамблер.- 10.10.2017. – URL: https://news.rambler.ru/other/38118738-gazpromu-nuzhen-iskusstvennyy-intellekt (дата обращения 08.08.2022).
8. Искусственный интеллект на арктическом шельфе. От людей – только контроль [Электронный ресурс]// ИА «Север-Пресс – Новости Ямала». – 15.10.2017. – URL: http://sever-press.ru/obshchestvo/nauka/item/33495-iskusstvennyj-intellekt-na-arkticheskom-shelfe-ot-lyudej-tolko-kontrol (дата обращения 08.08.2022).
9. Круглов, А., Рамм, А. Роботы займутся спасением в Арктике [Электронный ресурс]// МИЦ Известия. – 29.01.2018. – URL: https://iz.ru/699859/aleksandr-kruglov-aleksei-ramm/roboty-zaimutsia-spaseniem-v-arktike (дата обращения 08.08.2022).
10. Российские дроны займутся спасением людей в Арктике [Электронный ресурс]// Федеральное агентство новостей. – 29.01.2018. – URL: https://riafan.ru/1020194-rossiiskie-drony-zaimutsya-spaseniem-lyudei-v-arktike (дата обращения 08.08.2022).

УДК 681.518+378
А.В. Алексеев, д-р техн. наук, профессор, Д.О. Куприянов, Ю.М. Заведеев, Е.М. Гадаев, И.Д. Стефанович
Санкт-Петербургский государственный морской технический университет
ул. Лоцманская, д. 3., г. Санкт-Петербург, Россия, 190121,
e-mail: iapbgks@bk.ru

ПРАКТИЧЕСКИЕ ВОПРОСЫ ОПЕРЕЖАЮЩЕГО ОБУЧЕНИЯ ПРИ РЕАЛИЗАЦИИ ДОРОЖНОЙ КАРТЫ ЦЕНТРА ОСВОЕНИЯ ТЕХНОЛОГИЙ ИНФОРМАЦИОННОГО ПРОТИВОБОРСТВА САНКТ-ПЕТЕРБУРГСКОГО ГОСУДАРСТВЕННОГО МОРСКОГО ТЕХНИЧЕСКОГО УНИВЕРСИТЕТА

Аннотация
Систематизированы практические и проблемные вопросы реализации концепции опережающего обучения с учетом опыта реализации дорожной карты инновационного Центра Освоения Технологий Информационного Противоборства, созданного в 2016 г. в Санкт-Петербургском государственном морском техническом университете. Для обсуждения и развития в рамках научного сообщества показаны новые возможности и перспективы развития инновационных центров типа ЦОТИП, включая формирование технологии и организацию Межвузовского полигона освоения перспективных направлений развития отечественных информационных технологий.
Ключевые слова: систематизация практических вопросов, цифровизация учебных процессов, межвузовский полигон освоения технологий.

A.V. Alekseev, Doctor of Technical Sciences, Professor, D.O. Kupriyanov, Yu.M. Zavadeev, E.M. Gadaev, I.D. Stefanovich
Saint Petersburg State Maritime Technical University, 3, Lotsmanskaya str., Saint Petersburg, Russia, 190121,
e-mail: iapbgks@bk.ru

PRACTICAL ISSUES OF ADVANCED TRAINING IN THE IMPLEMENTATION OF THE ROADMAP OF THE CENTER FOR THE DEVELOPMENT OF INFORMATION WARFARE TECHNOLOGIES OF THE ST. PETERSBURG STATE UNIVERSITY MARITIME TECHNICAL UNIVERSITY

Annotation
The practical and problematic issues of implementing the concept of advanced training are systematized, taking into account the experience of implementing the roadmap of the Innovation Center for the Development of Information Warfare Technologies, established in 2016 at the St. Petersburg State Marine Technical University. For discussion and development within

the scientific community, new opportunities and prospects for the development of innovation centers such as TSOTIPB are shown, including the formation of technology and the organization of an Interuniversity training ground for the development of promising areas for the development of domestic information technologies.
Keywords: systematization of practical issues, digitalization of educational processes, interuniversity technology development training ground.

Актуальность. Бурное развитие информационных технологий и цифровая трансформация учебных процессов требуют модернизации и, даже, новых подходов к развитию учебной лабораторной базы (УЛБ). Предъявляются не только новые требования к составу лабораторного оборудования, его многопрофильности, модульности, учебной доступности и универсальности использования, но, прежде всего, к необходимости учета: сокращения сроков морального старения; ограниченных возможностей серийного производства и использования; резко возросших стоимостных показателей; ограниченных возможностей использования оборудования с израсходованными ресурсными показателями; ограничения возможностей приобретения запасного имущества и принадлежностей.

Важную роль сегодня для вхождения в состав лидирующих вузов в отрасли, в стране, в мире играет цифровая зрелость лабораторной базы, включая цифровую зрелость вузовской научно-исследовательской и опытно-конструкторской деятельности, которая также должна способствовать эффективной загрузке технологической базы УЛБ и ее развитию.

Не менее остро эти проблемы проявляются при оснащение учебных лабораторий даже программными и программно-аппаратными средствами (ПАС), а при сроке эксплуатации в 3…5 лет практически не оставляют возможности использования в составе УЛК «долгоиграющих» ПАС, поддержания лабораторной базы на должном уровне технологической зрелости.

В этих условиях представляется актуальным на межвузовском уровне в рамках конференции «ПНРОИТ-2022» обсудить ряд практических и проблемных вопросов реализации концепции опережающего обучения [1-5], в том числе в варианте, реализуемом Кафедрой судовой автоматики и измерений (КСАИ) Санкт-Петербургского государственного морского технического университета (СПбГМТУ) [6]. Среди этих вопросов:

1. Вопрос интеграции традиционных и используемых средств и УЛК с вновь вводимыми в состав УЛБ. Анализ источников [1-5] показал

тенденцию роста требований при одновременном использование «классических» подходов к формированию УЛБ большинством ВУЗов страны при наличии ряда весьма интересных и, даже, перспективных предложений по использованию мультимедийного оборудования, компьютерных классов и других вариантов УЛК.

2. Вопрос форсированного развития УЛБ. Материально-техническая база большинства ВУЗов находится сегодня в ненадлежащем состоянии и требует серьезного обновления [2, 3]. Укрепление и модернизация вузовской материально-технической базы сегодня рассматриваются как важнейшее стратегическое направление развития и одно из главных условий достижения нового, современного качества образовательного процесса в высшей школе, основанного на идее опережающего обучения [4, 5]. Однако, «убедительных» рекомендаций по реализации данной парадигмы в научном сообществе почти нет.

3. Вопрос нейтрализации рисков неэффективных решений выбора закупаемого оборудования с учетом специфики российского рынка предоставления продуктов и услуг, включая особенности маркетинга, недостаточный уровень сертификационного обеспечения (контроля соответствия требованиям и необходимым показателям качества), соответствующих конфликтов.

Методические аспекты. Задача опережающей подготовки давно получила отражение в литературе [1-5]. Сегодня она реализуется в форме взаимодействия персонала, включая, прежде всего, обучаемых, производства, технико-технологической базы на основе синтеза результатов прикладных, экспериментальных и научно-методических исследований. Одним из «слабых» звеньев данного подхода является несовершенство используемых методов автоматизации процессов УЛК. В этой связи в [6] предложена новая концепция реализации парадигмы опережающего обучения, ключевым принципом которой является организационно-техническая интеграция процессов:

- освоения комплекса современных технологий из состава осваиваемых программно-аппаратных средств (ПАС), включенных в Реестр ПАС УЛК;
- углубленному исследованию их сравнительных свойств с формированием и включением результатов в квалиметрическую базу данных и знаний QSWOT-анализа (КБДЗ УЛК) с автоматическим ранжированием ПАС по значению агрегированного показателя качества (АПК);
- исследования и обоснования стартап-предложений по наращиванию значения АПК (модернизации, проектирования конкурентно-

способных ПАС с синтезом нового качества и их характеристик) с соответствующим обоснованием направлений развития, в том числе в контексте цифровой трансформации объектов морской техники и морской инфраструктуры (ОМТИ).

С одной стороны, реализация данного подхода *позволяет*, как показывает практика освоения современных технологий в рамках созданного при КСАИ в 2016 г. инновационного Центра освоения технологий информационного противоборства (ЦОТИП), в значительной мере нейтрализовать у обучаемых факторы неуверенности и, даже, подавленности сложностью и информационной насыщенностью данными при ознакомлении и освоении новых технологий.

С другой стороны, *за счет* реализации возможностей группового и интерактивного «проникновения» в их «тайны», формирования и анализа свойств, ранжирования ПАС *на основе* технологий количественного QSWOT-анализа, а также анализа корневой чувствительности позволяет перейти к «активной фазе» освоения *путем* синтеза новых (модернизации) свойств и системных характеристик изучаемых ПАС, обоснования и формулирования соответствующих новых конкурентно-способных технологических, технических и организационных решений, и, тем самым, развивать у обучаемых творческую активность, компетентность, профессиональную уверенность и целеустремленность.

При этом следует отметить особую роль автоматизации процессов мониторинга и контроля качества процессов освоения новых технологий, квитирования результатов по контрольным точкам, в том числе в рамках учебной практики с самостоятельным освоением типовых пакетов программного обеспечения, выполнения учебных заданий по разработке конкурентно-способных технологических решений, личного участия обучаемых в актуализации БДЗ конкурентно-способных решений УЛК, разработки соответствующих лабораторных работ.

Практические аспекты. Как известно, основой управления является планирование. Поэтому в практике ЦОТИП активно используется технология сетевого дорожного картирования планируемых мероприятий с использованием программного комплекса «Прогноз», позволяющего, например, в отличие от MS Project, непрерывно контролировать ожидаемый уровень реализации всего комплекса стартап-проектов ЦОТИП. Это в определенной мере способствует формированию у студентов уровня коллективной ответственности и состязательности. Пример фрагмента Дорожной карты из [6] по освоению новых технологий из «технологического арсенала» ЦОТИП КСАиИ приведен на рис. 1 и показывает возможность решения самых амбициозных задач типа ран-

жирования качества высокотехнологичных решений по анализу и синтезу конкурентно способных решений с обеспечением защищенности и противодействия компьютерным атакам на основе только создаваемых сегодня технологий и решений классов «SGRC», «RSA», «IRP», «СПРУ», «ЭМБЧ», «Прогноз-21», «CRS» [7-10].

С другой стороны, планирование групповых работ позволяет студентам освоить практику ведения и использования подобных дорожных карт с прогнозированием и цифровым контролем ожидаемых результатов для «личного» планирования, что в современных условиях является весьма немало важным.

Личностное развитие участников стартап-проектов. Другим практическим аспектом реализации принципа опережающего обучения следует считать фактор личностного развития студентов в процессе выполнения стартап-проектов, в основе которого, прежде всего, лежат:

ПК "Прогноз 9"	План утвержден 08.09.2021.	Мониторинг выполнения Плана работы ЦОТИП-7 по состоянию на:					22.01.22 14:20
Цель	**Задачи**	**Исполнитель: Содержание, форма отчета**	**Значимость,%**	**Начало**	**Срок**	**Текущий результат**	**Прогноз на срок**	**Итог**
УГ: Куприянов Д.О., Заведеев Ю.М., Гадаев Е.М., Стефанович И..	Разработка Плана работы ЦОТИП-7	**ОрКомитет:** 1.Согласование целей и задач ЦОТИП-7.3.Разработка и согласование Плана работы ЦОТИП-7.	5,0%	02.09.21	08.09.21	100,0	100,0	100,0
Цель ЦОТИП 7: **Освоение технологий СПРУ, Прогноз, МСКР и других технологий информационного противоборства**	Представление Плана работы ЦОТИП-7 на утверждение с последующей рассылкой.	**УГ:** Уяснение исполнителями целей, задач и сроков выполнения Плана работы ЦОТИП-7. Представление и утверждение Плана УП - Куприянов Д.О.	5,0%	08.09.21	17.09.21	100,0	100,0	*Цель достигнута*
	1.Разработка алгоритма для студентов по настройке межсетевых экранов с презентацией в видеокурсом.	**Альфа:** Изучение МСЭ и их программной реализации. Разработка алгоритма настройки МСЭ для PC, локалкой (домашней сети) и сети университета. Руководитель - Заведеев Ю.М.	15,0%	17.09.21	20.02.22	83,9	100,0	
	2.Изучение ПК КИБ Searchinform для последующей интеграции с СПРУ	**Бета:** Изучение ПК, анализ его функций. Занесение сведений в КБДЗ. Руководитель - Гадаев Е.М.	15,0%	17.09.21	21.12.21	100,0	100,0	
	3.Освоение ПК СПРУ с последующей модернизацией в программной середе Python	**Гамма:** Изучение СПРУ с развертыванием на заранее созданном полигоне. Создание СПРУ 2.0. Руководители - Куприянов Д.О. и Стефанович И.Д.	15,0%	01.02.22	07.05.22	100,0	100,0	85
	4."ТГ БЧ-5"	**Дельта:** Разработка приложения в программной среде Python по оценке технической готовности электромеханической боевой части корабля к выходу в море. Руководитель - Стефанович И.Д.	15,0%	17.09.21	20.02.22	86,1	100,0	80
	5.Разработка ПК "Прогноз 9.3" в программной среде Python.	**Омега:** Освоение программного комплекса с последующей модернизацией в программной среде Python. Руководитель - Куприянов Д.О.	15,0%	17.09.21	20.02.22	84,0	100,0	50
	Приложение: П.1.Презентация результатов УП. П.2.Проект статей.	**Совещание УГ:** Итоги стартап-проектов (индивидуальные содоклады групп).	5,0%	20.02.22	20.02.22	100,0	100,0	
	Оформление и представление Отчета о стартап-проектах.	**ОрКомитет:** Отправка отчета о результатах стартап-проектов по электронной почте.	5,0%	20.02.22	21.02.22	100,0	100,0	Резерв времени: 0,5
	Резерв времени	Резерв времени	5,0%	21.02.22	21.02.22	100,0	100,0	

Рисунок 1 – Фрагмент перспективного плана развития ЦОТИП

- ускоренное приобретение практических навыков за счет участия в решение актуальных научно-технических задач в хорошо знакомой предметной области – развитие УЛБ кафедры;
- возможности внести свой личный социально значимый вклад в развитие учебной лабораторной базы Университета;
- широкие возможности по приобретению новых знаний и опыта за счет участия в коллективном решение стоящих задач, взаимном обмене знаниями и опытом и реализации тем самым синэргетического эффекта;
- приобретение навыков организации и руководства процессами

в процессе формирования и деятельности исследовательских групп по соответствующей тематике стартап-проектов;

- возможность ускоренного освоения под руководством преподавателей университета лучших практик и методических навыков участия в исследовательских процессах.

Цифровая трансформации учебных процессов. Наконец, главным практическим аспектом реализации принципа опережающего обучения следует считать расширение состава лабораторного оборудования в части ПАС, в том числе по опыту ЦОТИП с использованием их демоверсий, предлагаемых вендерами и дистрибьютерами, обеспечение многопрофильности осваиваемых ПАС, повышение учебной доступности новых ПАС и универсальности их использования [8-10].

При этом, по нашему мнению, существенно снизится на качестве подготовки обучаемых влияние сокращения сроков морального старения ПАС и их практического использования, роста ресурсных затраты на приобретение и освоение ПАС «традиционным путем» и их достаточного числа.

В целом, это безусловно будет способствовать повышению уровня цифровой зрелости учебных процессов и соответственно - уровня качества профессиональной подготовки.

Проблемные практические аспекты. Среди проблемных аспектов реализации данного подхода наряду с ростом сложности организации учебно-методических комплексов для преподавателей следует ожидать трудности согласования использования данных технологий обучения с учебно-методическими органами, в связи с чем можно их рассматривать в качестве дополняющих к технологиям, ранее установленным регламентами.

Перспективный вариант развития. Среди ряда возможных направлений развития концепции опережающего обучения, прежде всего, следует считать вариант формирования на основе интеграции центров, подобных ЦОТИПу, так называемого Межвузовского полигона освоения перспективных направлений развития отечественных информационных технологий (МПО ПНРОИТ) *с целью* практического освоения ПНРОИТ и обмена лучшими практиками, формирования студенческого научного сообщества и межвузовских коллективов исследователей с их участием в решении важных национальных задач на основе выполнения конкретных инновационных проектных задач.

Заключение. На основе опыта изучения новых программных средств в рамках инновационного Центра освоения технологий информационного противоборства КСАИ СПбГМТУ предложена концепция и технология, а также основные мероприятия дорожной карты создания

и развития учебно-лабораторных комплексов ВУЗов как для обсуждения и развития в рамках научно-педагогического сообщества, так и для формирования и организации Межвузовского полигона освоения перспективных направлений развития отечественных информационных технологий.

Реализация предложенного варианта опережающего обучения в сочетании с возможностями одновременного опережающего личностного развития (повышения самостоятельности, уверенности, целеустремленности при изучении новых технологий) в рамках цифровой трансформации учебных процессов нацелена на решение уже ставшей критической проблемы развития учебной лабораторной базы ряда ВУЗов в условиях роста стоимости закупки и сервисной поддержки программно-аппаратных средств, снижения сроков их морального старения при повышении многопрофильности использования, сложности оснащения ими учебно-лабораторных комплексов, их освоения.

Библиографический список

1. Учебно-лабораторная база, уровень ее оснащения URL: https://docs.yandex.ru/docs/view?tm=1642510431&tld=ru&lang (дата обращения: 2021.01.17).
2. Инновационный путь развития лабораторной базы. URL: https://cyberleninka.ru/article/n/inovatsionnyy-put-razvitiya-vuzovskoy-laboratornoy-bazy/viewer (дата обращения: 2021.01.17).
3. Конова Т.А., Нестеров В.Л. Оценка эффективности использования материально-технической базы вузов в системе показателей качества подготовки специалистов // Фундаментальные исследования. – 2014. – № 12-10, - с. 2103-2107; URL: http://fundamental-research.ru/ru/article/view?id=36533 (дата обращения: 15.12.2016).
4. Новиков П.М., Зуев В.М. Опережающее профессиональное образование: научно-практическое пособие. – М.: РГАТиЗ., -2000. – 266 с.
5. Минаев И., Вострухин А., Вахтина Е., Ушкур Д. Создание лабораторной базы опережающего обучения // Высшее образование в России. - 2008. №9. URL: http://cyberleninka.ru/article/n/sozdanie-laboratornoy-bazy-operezhayuschego-obucheniya (дата обращения: 15.12.2016).
6. Алексеев А.В., Куприянов Д.О., Заведеев Ю.М, Гадаев Е.М, Стефанович И.Д. Концепция, структура и дорожная карта учебно-лабораторного комплекса «ЦОТИП» / Актуальные проблемы морской энергетики: материалы одиннадцатой международной научно-технической конференции. – СПб.: Изд-во СПбГМТУ, 2022, с. 282-289.
7. D.O. Kupriyanov, I.D. Stefanowitsch, Ju.M. Zavedeev, Je.M. Gadaev, A.V. Alekseev. Analyse der intelligenten technologie der

datensicherhetssteuerung “A-SGRC + SPRU” / Д.О. Куприянов, И.Д. Стефанович, Ю.М. Заведеев, Е.М. Гадаев, А.В. Алексеев/ Анализ интеллектуальной технологии управления ИБ “a-SGRC + СПРУ” / Диалог поколений: материалы II региональной научно-практической конференции (23 апреля 2021 г.) / Минобрнауки РФ; ФГБОУ ВО «С.-Петерб. Гос. ун-т промышленных технологий и дизайна»; под общ. Ред. В.В. Кирилловой. – СПб.: ВШТЭ СПбГУПТД, 2021, с. 34-42.

8. Куприянов Д.О., Дедков А.В., Аносов А.В., Жуков О.А., Гагарин А.И., Алексеев А.В. Новая технология прогнозирования проектных результатов: ПК «Прогноз-21» / Неделя науки СПбГМТУ-2021: сборник докладов Всероссийского фестиваля науки «Nauka 0+»: в 2 т. – Т.1. – СПб.: Изд-во СПбГМТУ, 2021, с. 22-33.

9. Алексеев А.В., Москаленко В.А., Куприянов Д.О., Заведеев Ю. М., Стефанович И.Д., Гадаев Е.М. Программный комплекс поддержки принятия решений по оценке технической готовности корабля к выходу в море / Перспективные направления развития отечественных информационных технологий: материалы VII межрегиональной научно-практической конф. Севастополь, 21-25 сентября 2021 г. / Севастопольский государственный университет; науч.ред. Б.В. Соколов. – Севастополь: СевГУ, 2021, с. 184-188.

10. Заведеев Ю.М., Куприянов Д.О., Алексеев А.В. Анализ технологий интеграции программных комплексов CRS и СПРУ в интересах роботизации управления информационной безопасностью / Труды Крыловского государственного научного центра. Специальный выпуск, № 1. 2021. Материалы Десятой международной научно технической конференции «Актуальные проблемы морской энергетики» / СПб, 2021. Специальный выпуск, № 1, 2021, с. 204 – 206.

СОДЕРЖАНИЕ

Научное издание

Перспективные направления развития отечественных информационных технологий

Материалы VIII межрегиональной научно-практической конференции
(Севастополь 20–24 сентября 2022 года)

Advanced national information systems and technologies

Materials of VII interregional scientific-practical conference
(Sebastopol, September 20 – 24, 2022)

Ответственный за издание
Д.В. Моисеев, д-р. техн. наук, проф. кафедры
«Информационные технологии и компьютерные системы»
Севастопольского государственного университета

Научный редактор Б.В. Соколов
Технический редактор, компьютерная верстка: А.Е.Безуглая

ISBN 978-5-6049992-2-6

Издательство и типография ООО «Интерактивные технологии»
299038, г. Севастополь, ул. Колобова, 34/1, пом. XV.
тел. 7(978) 778 92 02
Подписано в печать 13.09.2022 г. Формат 60x84/16. Усл. печ.л. 11,74
Бумага офсетная. Тираж 300 экз. Зак. № 129.