

ТЕОРИЯ И ПРАКТИКА ПРОЕКТНОГО ОБРАЗОВАНИЯ

Ежеквартальный научно-теоретический и практический журнал

№ 1(17)/2021

Учредитель: ООО «ФАГОТ-ИНЖИНИРИНГ»,
ЦНИИ института русского жестового языка

E-mail: info@journaltpo.ru

Сайт: <http://journaltpo.ru>

ISSN: 2587-5922

Почтовый адрес: 107241, г. Москва,
Черницынский проезд, д. 3

Шеф-редактор: Олейник Андрей Владимирович

Председатель редакционного совета журнала:
Харламенков Алексей Евгеньевич

Главный редактор: Бритвина Валентина Валентиновна

Технический редактор и корректор:
Муханова Анна Александровна

Верстка: Логачёв Максим Сергеевич



Журнал в РИНЦ



Сайт журнала

Ответственность за содержание статей и качество перевода информации на английский язык несут авторы публикаций.

© Теория и практика проектного образования, 2021

© Коллектив акторов, 2021

РЕДАКЦИОННЫЙ СОВЕТ ЖУРНАЛА

ПРЕДСЕДАТЕЛЬ

Харламенков Алексей Евгеньевич

Директор центрального научно-исследовательского института русского жестового языка, эксперт НИУ ВШЭ, эксперт по информационным технологиям в области электронных документов, Doctor Honoris Causa

CHAIRPERSON

Harlamenkov Aleksej Evgen'evich

Director of the Central Research Institute of Russian Sign Language, HSE expert, information technology expert in the field of electronic documents, Doctor Honoris Causa

ЗАМЕСТИТЕЛЬ ПРЕДСЕДАТЕЛЯ

Лapidус Лариса Владимировна

Доктор экономических наук, профессор экономического факультета МГУ имени М.В. Ломоносова, директор Центра социально-экономических инноваций экономического факультета МГУ имени М.В. Ломоносова, директор Центра компетенций цифровой экономики Международной Ассоциации корпоративного образования

VICE-CHAIRMAN

Lapidus Larisa Vladimirovna

Doctor of Economics, Professor of the Faculty of Economics of Moscow State University named after M.V. Lomonosov, Director of the Center for Socio-Economic Innovations of the Faculty of Economics, Moscow State University named after M.V. Lomonosov, Director of the Digital Economy Competence Center of the International Association for Corporate Education

ЧЛЕНЫ РЕДАКЦИОННОГО СОВЕТА

Бондарь Валентин Степанович

Доктор физико-математических наук, профессор, Заслуженный деятель науки Российской Федерации, Почётный работник высшего профессионального образования Российской Федерации, академик РАН, академик Российской академии космонавтики им. К.Э. Циолковского

MEMBERS OF THE EDITORIAL BOARD

Bondar' Valentin Stepanovich

Doctor of Physical and Mathematical Sciences, Professor, Honored Scientist of the Russian Federation, Honorary Worker of Higher Professional Education of the Russian Federation, Academician of the Russian Academy of Natural Sciences, Academician of the Russian Academy of Cosmonautics. K.E. Tsiolkovsky

Джапарова Гульжамал Алькеновна

Ректор Университета «Туран-Астана», кандидат экономических наук, профессор, г. Нур-Султан, Казахстан

Dzhaparova Gul'zhamal Al'kenovna

Rector of the University "Turan-Astana", candidate of economic sciences, professor, Nur-Sultan, Kazakhstan

Димитров Любомир Ванков

Проректор по учебной деятельности, аккредитации и международным связям Технического университета София, доктор, профессор, Заслуженный доктор НГТУ, София (Sofia), София, Болгария

Dimitrov Ljubomir Vankov

Vice-Rector for Academic Affairs, Accreditation and International Relations of the Technical University of Sofia, Doctor, Professor, Honored Doctor of NSTU, Sofia (Sofia), Sofia, Bulgaria

Дусенко Светлана Викторовна

Доктор социологических наук, профессор, Почетный работник сферы образования Российской Федерации, заведующий кафедрой «Туризм и гостиничное дело» Института туризма, рекреации, реабилитации и фитнеса ФГБОУ ВО «Российский государственный университет физической культуры, спорта, молодежи и туризма (ГЦОЛИФК)». Эксперт государственной системы классификации гостиниц и иных средств размещения

Dusenko Svetlana Viktorovna

Doctor of Sociological Sciences, Professor, Honorary Worker of Education of the Russian Federation, Head of the Department of Tourism and Hospitality at the Institute of Tourism, Recreation, Rehabilitation and Fitness of the Russian State University of Physical Culture, Sports, Youth and Tourism (SCOLIFK). Expert of the state classification system of hotels and other accommodation facilities

Еникеев Ильдар Хасанович

Доктор технических наук, профессор, профессор кафедры «Математика» Московского политехнического университета

Enikeev Il'dar Hasanovich

Doctor of Technical Sciences, Professor, Professor of the Department of Mathematics, Moscow Polytechnic University

Молчанова Наталья Петровна

Доктор экономических наук, профессор Департамента общественных финансов Финансового университета при Правительстве Российской Федерации

Molchanova Natal'ja Petrovna

Doctor of Economics, Professor of the Department of Public Finance of the Financial University under the Government of the Russian Federation

Нижников Александр Иванович

Доктор педагогических наук, кандидат физико-математических наук, профессор, Заслуженный работник высшей школы Российской Федерации, Почётный работник высшего профессионального образования Российской Федерации, заведующий кафедрой технологических и информационных систем МИГУ

Nizhnikov Aleksandr Ivanovich

Doctor of Pedagogy, Candidate of Physics and Mathematics, Professor, Honored Worker of Higher Education of the Russian Federation, Honorary Worker of Higher Professional Education of the Russian Federation, Head of the Department of Technological and Information Systems of Moscow State University

Олейник Андрей Владимирович

Доктор технических наук, профессор, лауреат премии Правительства Российской Федерации в области науки и техники, лауреат премии Правительства Российской Федерации в области образования, заведующий кафедрой «Управление и информатика в технических системах» Московского государственного технологического университета «СТАНКИН»

Olejnik Andrej Vladimirovich

Doctor of Technical Sciences, Professor, Laureate of the Prize of the Government of the Russian Federation in the field of science and technology, Laureate of the Prize of the Government of the Russian Federation in the field of education, Head of the Department of Management and Informatics in Technical Systems, Moscow State Technological University STANKIN

Разумова Татьяна Олеговна

Доктор экономических наук, профессор, заведующий кафедрой экономики труда и персонала Экономического факультета МГУ имени М.В. Ломоносова

Устинова Лилия Николаевна

Доктор экономических наук, профессор кафедры «Управление инновациями и коммерческое использование интеллектуальной собственности» Российской государственной академии интеллектуальной собственности

Червяков Леонид Михайлович

Доктор технических наук, профессор, лауреат премии Правительства в области образования, Лауреат премии Правительства в области науки и техники, почетный работник высшего профессионального образования Российской Федерации, академик Академии проблем качества

Фалалеев Андрей Павлович

Доктор технических наук, профессор, ректор Крымского федерального университета имени В.И. Вернадского

Филиппович Андрей Юрьевич

Декан факультета Информационных технологий, профессор кафедры «Инфо-когнитивные технологии» Московского политехнического университета, кандидат технических наук. Эксперт Минобрнауки России, АПКИТ, СПК-ИКТ, ФУМО в сфере ИТ, WorldSkills Россия

Щербак Евгений Николаевич

Доктор юридических наук, профессор кафедры финансового права юридического факультета Российского государственного гуманитарного университета (РГГУ), Полковник ВВС, военный летчик-истребитель 1-го класса, Почётный работник высшего профессионального образования Российской Федерации, Академик РАЕН

Razumova Tat'jana Olegovna

Doctor of Economics, Professor, Head of the Department of Labor Economics and Personnel, Faculty of Economics, Moscow State University named after M.V. Lomonosov

Ustinova Liliya Nikolaevna

Doctor of Economics, Professor of the Department of Innovation Management and Commercial Use of Intellectual Property, Russian State Academy of Intellectual Property

Chervjakov Leonid Mihajlovich

Doctor of Technical Sciences, Professor, Laureate of the Government Prize in Education, Laureate of the Government Prize in Science and Technology, Honorary Worker of Higher Professional Education of the Russian Federation, Academician of the Academy of Quality Problems

Falaleev Andrej Pavlovich

Doctor of Technical Sciences, Professor, Rector of the Crimean Federal University named after V.I. Vernadsky

Filippovich Andrej Jur'evich

Dean of the Faculty of Information Technologies, Professor of the Department of "Information Cognitive Technologies" of the Moscow Polytechnic University, Candidate of Technical Sciences. Expert of the Ministry of Education and Science of the Russian Federation, APKIT, SPK-ICT, FUMO in IT, WorldSkills Russia

Shherbak Evgenij Nikolaevich

Doctor of Law, Professor of the Department of Financial Law of the Law Faculty of the Russian State University for the Humanities (RGGU), Air Force Colonel, 1st class military fighter pilot, Honorary Worker of Higher Professional Education of the Russian Federation, Academician of the Russian Academy of Natural Sciences

РЕДАКЦИОННАЯ КОЛЛЕГИЯ**Олейник Андрей Владимирович**

Шеф-редактор

Бондарь Валентин Степанович

Научный редактор

Бритвина Валентина Валентиновна

Главный редактор

Чаттаев Азамат Русланович, Муханов Сергей Александрович

Заместители главного редактора

Бычкова Наталья Александровна

Ответственный редактор раздела «Естественно-научная проектно-исследовательская деятельность в учебном заведении»

Сушкова Ольга Викторовна

Ответственный редактор раздела «Правовое обеспечение в сфере науки, технологий и образования»

Будылина Евгения Александровна

Ответственный редактор раздела «Проектирование и прогнозирование в социально-экономической сфере»

Седенков Сергей Евгеньевич

Ответственный редактор раздела «Проектная деятельность в области культуры, спорта и туризма»

Конюхова Галина Павловна

Ответственный редактор раздела «Молодые ученые – поиск самоопределения»

Бобров Кирилл Романович

Руководитель интернет проектов

Муханова Анна Александровна

Технический редактор и корректор

Olejnik Andrej Vladimirovich

Chief editor

Bondar' Valentin Stepanovich

Scientific editor

Britvina Valentina Valentinovna

Chief Editor

Chattaev Azamat Ruslanovich, Muhanov Sergej Aleksandrovich

Deputy editors-in-chief

Bychkova Natal'ja Aleksandrovna

Executive editor of the section "Natural scientific design and research activities in an educational institution"

Sushkova Ol'ga Viktorovna

Executive editor of the section "Legal support in the field of science, technology and education"

Budylna Evgenija Aleksandrovna

Executive editor of the section "Design and forecasting in the socio-economic sphere"

Sedenkov Sergej Evgen'evich

Executive editor of the section "Project activities in the field of culture, sports and tourism"

Konjuhova Galina Pavlovna

Executive editor of the section "Young Scientists - Search for Self-Determination"

Bobrov Kirill Romanovich

Internet project manager

Muhanova Anna Aleksandrovna

Technical editor and proofreader

Baier Tatiana

Редактор английского текста, PhD, MUSC Wellness Centre, Charleston, South Carolina, USA

Боброва Екатерина Олеговна

Секретарь редакционного совета журнала

Baier Tatiana

English text editor, PhD, MUSC Wellness Centre, Charleston, South Carolina, USA

Bobrova Ekaterina Olegovna

Secretary of the editorial board of the journal

ЧЛЕНЫ РЕДАКЦИОННОЙ КОЛЛЕГИИ**Артамонова Марина Вадимовна**

Кандидат экономических наук, доцент кафедры экономики труда и персонала экономического факультета МГУ имени М.В. Ломоносова

Архангельская Мария Владимировна

Кандидат педагогических наук, доцент кафедры социально-гуманитарных, экономических и естественнонаучных дисциплин ИП и НБ РАНХиГС при Президенте Российской Федерации

Архангельский Александр Игоревич

Почетный работник высшего профессионального образования Российской Федерации кандидат педагогических наук, доцент, доцент кафедры «Математика» Московского политехнического университета

Берков Николай Андреевич

Почетный работник высшего профессионального образования Российской Федерации, кандидат технических наук, доцент, доцент кафедры «Высшая математика 2» Физико-технологического института Московского технологического университета (МИРЭА)

Воронцова Софья Викторовна

Кандидат юридических наук, доцент, доцент ГТУ МАДИ, РУТ (МИИТ)

Диева Нина Николаевна

Кандидат технических наук, доцент кафедры нефтегазовой и подземной гидромеханики РГУ нефти и газа (НИУ) имени И.М. Губкина

Елисеева Наталья Владимировна

Кандидат технических наук, доцент кафедры «Управление и информатика в технических системах» Московского государственного технологического университета «СТАНКИН»

Еникеева Светлана Дмитриевна

Кандидат экономических наук, доцент, доцент экономического факультета Московского государственного университета им. М.В. Ломоносова

Жукова Ольга Владиславовна

Кандидат экономических наук, заведующий кафедрой Менеджмента и экономики спорта имени В. В. Кузина Российского государственного университета физической культуры, спорта, молодежи и туризма «ГЦОЛИФК»

Змазнева Олеся Анатольевна

Кандидат философских наук доцент кафедры «Инфокогнитивные технологии» Московского политехнического университета

Зуева Анна Сергеевна

Кандидат экономических наук, доцент, доцент кафедры компьютерного права и информационной безопасности Высшей школы государственного аудита Московского государственного университета имени М.В. Ломоносова, доцент кафедры правового обеспечения публичных финансов Института законодательства и сравнительного правоведения при Правительстве Российской Федерации, доцент кафедры «Государственный финансовый контроль и казначейское дело» Финансового университета при Правительстве РФ

Каширина Мария Михайловна

Кандидат филологических наук, кафедра межъязыковых коммуникаций и журналистики ФГАОУ ВО Крымский федеральный университет имени В.И. Вернадского

Логачёв Максим Сергеевич

Кандидат технических наук, доцент кафедры «Инфокогнитивные технологии» и руководитель образовательной программы «Корпоративные информационные системы» Московского политехнического университета, преподаватель

MEMBERS OF THE EDITORIAL BOARD**Artamonova Marina Vadimovna**

PhD in Economic Sciences, Associate Professor of the Department of Labor Economics and Personnel of the Faculty of Economics, Lomonosov Moscow State University

Arhangel'skaja Marija Vladimirovna

Candidate of Pedagogy, Associate Professor of the Department of Social, Humanitarian, Economic and Natural Sciences of the IP and NB RANEPА under the President of the Russian Federation

Arhangel'skij Aleksandr Igorevich

Honorary Worker of Higher Professional Education of the Russian Federation, Candidate of Pedagogical Sciences, Associate Professor, Associate Professor of the Department of Mathematics of the Moscow Polytechnic University

Berkov Nikolaj Andreevich

Honorary Worker of Higher Professional Education of the Russian Federation, Candidate of Technical Sciences, Associate Professor, Associate Professor of the Department of Higher Mathematics 2 of the Physico-Technological Institute of the Moscow Technological University (MIREA)

Voroncova Sof'ja Viktorovna

Candidate of Legal Sciences, Associate Professor, Associate Professor MADI, RUT (MIIT)

Dieva Nina Nikolaevna

PhD in of Technical Sciences, Associate Professor of the Department of Oil and Gas and Underground Hydromechanics of the National University of Oil and Gas «Gubkin University»

Eliseeva Natal'ja Vladimirovna

Candidate of Technical Sciences, Associate Professor of the Department of Management and Informatics in Technical Systems, Moscow State Technological University "STANKIN"

Enikeeva Svetlana Dmitrievna

Candidate of Economic Sciences, Associate Professor, Associate Professor of the Faculty of Economics, Moscow State University. M.V. Lomonosov

Zhukova Ol'ga Vladislavovna

Candidate of Economic Sciences, Head of the Department of Management and Economics of Sports named after V.V. Kuzin, Russian State University of Physical Culture, Sports, Youth and Tourism "GZOLIFK"

Zmazneva Olesja Anatol'evna

Candidate of Philosophy, Associate Professor of the Department of Information Cognitive Technologies, Moscow Polytechnic University

Zueva Anna Sergeevna

Candidate of Economic Sciences, Associate Professor, Associate Professor of the Department of Computer Law and Information Security of the Graduate School of State Audit, Moscow State University named after M.V. Lomonosov, Associate Professor of the Department of Legal Support of Public Finance at the Institute of Legislation and Comparative Law under the Government of the Russian Federation, Associate Professor of the Department "State Financial Control and Treasury" of the Financial University under the Government of the Russian Federation

Kashirina Marija Mihajlovna

PhD in Philology, Department of Interlanguage Communications and Journalism, V.I. Vernadsky Crimean Federal University

Logachev Maksim Sergeevich

Candidate of Technical Sciences, Associate Professor of the Department of "Information Cognitive Technologies" and Head of the educational program "Corporate Information Systems" of the Moscow Polytechnic University,

высшей квалификационной категории, эксперт демонстрационного экзамена по стандартам WorldSkills

Лхагвасурэн Гундэгмаа

PhD, проректор Национального Института Физической культуры Монголии

Микола Седак

Преподаватель права, доцент Университета Коменского в Братиславе, Словакия

Муханова Анна Александровна

Кандидат педагогических наук, зав. каф. «Природообустройство и водопользование» Российского государственного аграрного заочного университета

Нудьга Александр Александрович

Кандидат технических наук, заместитель директора Физико-технического института (СП) ФГАУ ВО Крымского федерального университета имени В.И. Вернадского

Нургазина Гульмира Есимбаевна

Кандидат экономических наук, доцент кафедры «Международные экономические и финансовые отношения» Российской государственной академии интеллектуальной собственности (РГАИС)

Петров Валерий Евгеньевич

Кандидат технических наук, доцент кафедры «Управление и информатика в технических системах» Московского государственного технологического университета «СТАНКИН», заместитель генерального конструктора по научной работе компании «СОЛВЕР»

Филиппович Юрий Николаевич

Кандидат технических наук, профессор кафедры «Инфокогнитивные технологии» Московского политехнического университета

Хмыз Алексей Иванович

Полковник полиции, кандидат юридических наук, заместитель начальника кафедры оружейведения и трасологии учебно-научного комплекса судебной экспертизы, Московского университета МВД России имени В.Я. Кикотя

Таукенова Лязат Жумабаевна

Доктор по профилю, кафедры «Информационные технологии» университета «Туран-Астана» г. Нур-Султан, Республика Казахстан

Чаттаева Виолетта Раисовна

Кандидат юридических наук, старший преподаватель кафедры «Управления и гражданское право» Института Деловой Карьеры

Щербак Анна

Кандидат юридических наук, сотрудник Bureau van Dijk, a Moody's Analytics Company, Женева, Швейцария

teacher of the highest qualification category, expert of the demonstration exam according to WorldSkills standards

Lhagvasurjen Gundjegmaa

PhD, Vice-rector of the National Institute of Physical Culture of Mongolia

Mikola Sedak

Lecturer in Law, Associate Professor at Comenius University in Bratislava, Slovakia

Muhanova Anna Aleksandrovna

Candidate of Pedagogical Sciences, Head. department "Environmental Engineering and Water Use" of the Russian State Agrarian Correspondence University

Nud'ga Aleksandr Aleksandrovich

Candidate of Technical Sciences, Deputy Director of the Physico-Technical Institute (JV) of the V.I. Vernadsky

Nurgazina Gul'mira Esimbaevna

Candidate of Economic Sciences, Associate Professor of the Department of International Economic and Financial Relations of the Russian State Academy of Intellectual Property (RGAIS)

Petrov Valerij Evgen'evich

Candidate of Technical Sciences, Associate Professor of the Department of "Management and Informatics in Technical Systems" of the Moscow State Technological University "STANKIN", Deputy General Designer for Scientific Work of the "SOLVER" company

Filippovich Jurij Nikolaevich

Candidate of Technical Sciences, Professor of the Department of Information Cognitive Technologies, Moscow Polytechnic University

Hmyz Aleksej Ivanovich

Police Colonel, Candidate of Legal Sciences, Deputy Head of the Department of Weapons Science and Traceology of the Educational and Scientific Complex of Forensic Expertise, Moscow University of the Ministry of Internal Affairs of Russia named after V.Ya. Kikotya

Taukenova Ljzat Zhumabaevna

Doctor in profile, Department of Information Technologies, University of Turan-Astana, Nur-Sultan, Republic of Kazakhstan

Chattaeva Violetta Raisovna

Candidate of Legal Sciences, Senior Lecturer of the Department of Management and Civil Law of the Institute of Business Career

Shherbak Anna

PhD in Law, Officer, Bureau van Dijk, a Moody's Analytics Company, Geneva, Switzerland

УЧРЕДИТЕЛИ

Бритвина Валентина Валентиновна

Кандидат педагогических наук, доцент кафедры «Управление и информатика в технических системах» Московского государственного технологического университета «СТАНКИН», доцент кафедры «Инфокогнитивные технологии» Московского политехнического университета

Седенков Сергей Евгеньевич

Тренер Школы Кёкусинкай Каратэ «Гамбару Додзё»

Харламенков Алексей Евгеньевич

Директор центрального научно-исследовательского института русского жестового языка. Эксперт НИУ ВШЭ, эксперт по информационным технологиям в области электронных документов, старший преподаватель кафедры «Инфокогнитивные технологии» Московского политехнического университета

Britvina Valentina Valentinovna

Candidate of Pedagogy, Associate Professor of the Department of "Management and Informatics in Technical Systems" of the Moscow State Technological University "STANKIN", Associate Professor of the Department of "Information Cognitive Technologies" of the Moscow Polytechnic University

Sedenkov Sergej Evgen'evich

Trainer of the Kyokushin Karate School "Gambaru Dojo"

Harlamenkov Aleksej Evgen'evich

Director of the Central Research Institute of Russian Sign Language. Expert of the Higher School of Economics, an expert on information technology in the field of electronic documents, senior lecturer of the Department of Information Cognitive Technologies, Moscow Polytechnic University

СОДЕРЖАНИЕ

Естественно-научная проектно-исследовательская деятельность в учебном заведении	8
Архангельская М.В., Архангельский А.И., Берков Н.А. Цифровизация образования и преподавание математики в ВУЗе.....	8
Самохвалова Е.И. Место креативности в таксономии Б. Блума	10
Ярных Ю.А. Microsoft Teams как средство организации кейс-стади при дистанционном обучении.....	12
Правовое обеспечение в сфере науки, технологий и образования.....	16
Таукенова Л.Ж., Исакаева А.Ж., Жумабаев Е.Н. Исследование и анализ IT-технологий, применяемых в инфраструктуре электронного правительства	16
Бритвина В.В. Вероятностный анализ безопасности в информационных системах.....	20
Проектирование и прогнозирование в социально-экономической сфере	23
Зубарев М.О., Конюхова Г.П. Проблемы при создании нейронной сети для сентимент анализа.....	23
Таукенова Л.Ж., Каиржанова А.К., Жумабаев Е.Н. IT-решения в автоматизации процесса подбора и управления кадрами	25
Федотов Н.О. Разработка веб-сервиса по анализу ошибок в поисковой оптимизации	29
Нуспеков Е.Л., Таукенова Л.Ж., Жумабаев Е.Н. Уравнения электромеханических переходных процессов в синхронном электроприводе насосного агрегата	31
Проектная деятельность в области культуры, спорта и туризма	34
Косарева Н.В. Использование разных каналов коммуникации для продвижения имиджа региона на примере мурманской области.....	34
Молодые ученые – поиск самоопределения	37
Зуева А.С., Василихина Ю.В. Правовое регулирование защиты персональных данных в социальных сетях.....	37
Дадашов И.О., Гужва Д.В. Определение условий применимости алгоритма шифрования RSA для ключей шифрования длиной менее 256 БИТ	39
Архипова А.С. Вопросы определения правовой природы Биткоина	42
Жандармова Е.А., Сорокин А.Ю. Приложение «ПО ТУ СТОРОНУ»	46
Яковлев Р.И., Сушкова О.В. NFT как цифровая инновация в авторском праве.....	49
Костюк М.Ф., Василихина Ю.В. Мошенничество в инновационной среде	51
Александрова А.В., Широков А.А., Соболев Д.В., Бритвина В.В. Концепции подхода к унификации критически важных систем и процесса обеспечения безопасности	54
Бычкова Е.С., Воронин И.В. Некоторые аспекты технических и психологических проблем при переходе на дистанционную форму обучения у подростков и педагогов	60
Перевесенский С.А., Сорокин А.Ю. Моделирование последствий взрывных нагрузок на конструктивные элементы объектов инфраструктуры любого типа	68
Зуева А.С., Басырова З.Р. Роль росфинмониторинга в противодействии легализации преступных доходов в условиях цифровой трансформации.....	71

Клейменов А.Р., Дубровина О.В. Создание электронного учебного пособия по дисциплине «Устройство и функционирование информационных систем» для студентов специальности 09.02.04 «Информационные системы (по отраслям)»	74
Строкова П.С. Понятие и правовое регулирование «Больших данных» в условиях становления законодательства в сфере информационного права	77
Бабаева С.Ш. Особенности проектного образования в юридическом вузе.....	80

ЕСТЕСТВЕННО-НАУЧНАЯ ПРОЕКТНО-ИССЛЕДОВАТЕЛЬСКАЯ ДЕЯТЕЛЬНОСТЬ В УЧЕБНОМ ЗАВЕДЕНИИ

ЦИФРОВИЗАЦИЯ ОБРАЗОВАНИЯ И ПРЕПОДАВАНИЕ МАТЕМАТИКИ В ВУЗЕ

DIGITALIZATION OF EDUCATION AND TEACHING MATHEMATICS AT THE UNIVERSITY

Архангельская Мария Владимировна

Кандидат педагогических наук, доцент кафедры социально-гуманитарных, экономических и естественно-научных дисциплин ИПНБ РАНХиГС



Arkhangel'skaya Mariya Vladimirovna

Candidate of Pedagogical Sciences, Associate Professor of the Department of Social, Humanitarian, Economic and Natural Science Disciplines of the Institute for the National Library of Science, RANEPА

Архангельский Александр Игоревич

Кандидат педагогических наук, доцент кафедры математики Московского политехнического университета



Arkhangel'skiy Aleksandr Igorevich

Candidate of Pedagogy, Associate Professor of the Department of Mathematics, Moscow Polytechnic University

Берков Николай Андреевич

Кандидат технических наук, доцент кафедры VM-2 Российского технологического университета МИРЭА



Berkov Nikolay Andreevich

Candidate of Technical Sciences, Associate Professor of the VM-2 Department of the Russian Technological University MIREA

Аннотация. Цифровизация образования выступает в настоящее время основной тенденцией его развития во всем мире. В статье рассматриваются проблемы встраивания математического контента в образовательное пространство высшего образования.

Ключевые слова: цифровизация, высшее образование, математика, современные технологии.

Abstract. Digitalization of education is currently the main trend of its development all over the world. The article deals with the problems of embedding mathematical content in the educational space of higher education.

Keywords: digitalization, higher education, mathematics, modern technology.

Цифровизация изменила все области деятельности человека, не обойдя стороной образования, особенно высшего, создав благоприятные условия для формирования собственной траектории образования, что дает возможности для творческого научного подхода к изучаемому предмету. И это (цифровизация образования) происходит практически в каждой стране мира и является основной тенденцией развития. Наблюдается

тенденция к заметному росту численности желающих дистанционно осваивать разнообразные образовательные программы.

В связи с бурными развитиями технологий система высшего образования не всегда успевает предоставить нужные в данный конкретный момент определенные образовательные услуги по некоторым направлениям. Цифровизация высшего образования позволяет за

сравнительно короткие сроки наращивать образовательный контент практически по всем направлениям траекторий обучения. Массовое создание разнообразных онлайн-курсов, да и онлайн-образования в целом позволяет проводить образовательный процесс в разнообразных форматах. Современное техническое оснащение высших учебных заведений и программное обеспечение позволяет преподавателям проводить дистанционно на высоком уровне занятия по различным предметам. То, что происходило во всем мире за последние годы подтвердило правильность выбранного направления развития высшего образования, заточенное на его цифровизации. Все большее внимание уделяется возможности предоставить студентам выбор своей образовательной траектории, то есть наблюдается крен в сторону индивидуализации образования и повышение его инклюзивности. При этом меняется и роль преподавателя в сторону наставничества и координации по изучаемым предметам. Преподаватель тратит гораздо меньше времени непосредственно на обучение, возрастает доля самостоятельной работы студента. По некоторым дисциплинам происходит укорочение образовательных траекторий за счет объединения материалов нескольких различных дисциплин в один междисциплинарный образовательный ресурс. Для этого необходимо развитие междисциплинарного сотрудничества при разработке и реализации соответствующих образовательных программ.

В настоящее время в образовании крен делается на развитие способностей к самообразованию, саморазвитию и самоорганизации

Цифровизация постепенно, поэлементно, внедряется в традиционную систему образования. При этом возрастают требования к техническому оснащению образовательной организации. Он-лайн обучение невозможно без стабильной и бесперебойной работы образовательных порталов вуза. Все обучающиеся должны иметь доступ к электронным образовательным ресурсам университета. В настоящий момент оптимальной представляется модель смешанного обучения, предусматривающую лишь частичную замену аудиторных занятий электронными образовательными ресурсами. Самое главное, чтобы современные образовательные технологии, применяемые в образовательном процессе, не заглушали мотивацию учащегося в освоении новых знаний.

Применительно к преподаванию математики в вузах важной составляющей является роль преподавателя. Зачастую, математический контент достаточно сложный и разобраться в нем самостоятельно обучающемуся бывает проблематично. Не каждый тьютор сможет отослать студента в правильном направлении при возникающих трудностях в понимании изучаемого материала. Часто требуется вмешательство высококвалифицированного специалиста, который сможет понятным языком объяснить наиболее сложные моменты. В таких случаях наиболее продуктивным является очное общение преподавателя со студентом.

Также важной частью изучения математики в современных условиях является применение компьютерных технологий и пакетов компьютерной алгебры. При изучении многих разделов математики необходимо применять основы программирования, так как помимо теоретических знаний студенты должны быть готовы решать и практические задачи.

Например, рассмотрим решение задачи о вычислении определенного интеграла от непрерывной функции $y = f(x)$ на ограниченном отрезке $[a, b]$. Если для подынтегральной функции $f(x)$ можно найти ее первообразную $F(x)$, то интеграл находится по формуле Ньютона-Лейбница:

$$\int_a^b f(x)dx = F(b) - F(a)$$

Если же для функции $f(x)$ не удастся найти ее первообразную $F(x)$, то для вычисления интеграла применяются методы численного интегрирования. При этом, в зависимости от применяемого метода численного интегрирования, необходимо написать соответствующую программу. Для более широкого кругозора обучающихся полезно разбирать такого типа задания используя разные программные продукты, что уже подразумевает высокую квалификацию и широкий кругозор преподавателя и тесную связь преподаватель-студент.

В заключении хотелось бы сказать, что цифровизация образования призвана облегчить работу преподавателям, а также помочь мотивированным студентам пройти свою образовательную траекторию. Но все в разумных пределах.

Список литературы

1. **Архангельский А.И.** Обучение высшей математике как основа формирования знаний и умений будущего специалиста с высшим профессиональным образованием / А.И. Архангельский // Актуальные проблемы гуманитарных, социальных и экономических наук: Межвузов. сб. науч. и науч.-метод. тр. — М., 2002. — С. 121–127.
2. **Берков Н.А.** Применение пакета Maxima: практикум / Н.А. Берков. — М.: МГИУ, 2009.
3. **Архангельский А.И.** Математический практикум с применением пакета Matlab. Теория вероятностей. Математическая статистика / А.И. Архангельский, Н.А. Берков, М.В. Архангельская. — М.: Институт системных технологий, 2018. — 70 с.
4. **Щенникова Е.И.** Практические аспекты применения дистанционных образовательных технологий. Интерактивные подходы к обеспечению образовательной деятельности в учреждениях высшего и среднего образования: сб. ст. / Е.И. Щенникова, В.Н. Щенникова, М.В. Архангельская; Российский экономический университет имени Г.В. Плеханова. Учебно-научный центр по переподготовке и повышению квалификации работников высшей школы. — 2017. — С. 107–110.

МЕСТО КРЕАТИВНОСТИ В ТАКСОНОМИИ Б. БЛУМА PLACE OF CREATIVITY IN B. BLOOM'S TAXONOMY

**Самохвалова
Екатерина Игоревна**

*Кафедра семиотики и общей теории искусства
МГУ имени М.В. Ломоносова*



**Samokhvalova
Ekaterina Igorevna**

*Department of Semiotics and General Theory of Art,
Moscow State University M.V. Lomonosov*

Аннотация. В данной статье автор акцентирует внимание на том, что вынужденные меры по переводу учебного процесса в цифровую среду породили трудности для педагогов в части дефицита необходимых компетенций. В то же время открылись новые возможности по использованию инновационных методов развития креативности. Для решения данной задачи в дистанционном формате потребовались новые подходы, работающие в онлайн-пространстве. Повысить качество такого перехода позволяет применение таксономии Б. Блума.

Ключевые слова: цифровая среда, креативность, креативная среда, дистанционное обучение, электронные сервисы, таксономия Б. Блума.

Abstract. In this article, the author focuses on the fact that the forced measures to transfer the educational process to a digital environment have created difficulties for teachers in terms of the lack of necessary competencies. At the same time, new opportunities have opened up for the use of innovative methods of developing creativity. To solve this problem in a remote format, new approaches were required that work in the online space. The quality of such a transition can be improved by using B. Bloom's taxonomy.

Keywords: digital environment, creativity, creative environment, distance learning, electronic services, B. Bloom's taxonomy.

Анализ научной литературы подтверждает высокий интерес ученых к пониманию креативности, ее структуры, особенностей креативного процесса и работы головного мозга в креативном процессе. Учеными Т. Амабайл, К. Робинсон, Р. Стенбергом, К. Урбаном было выявлено, что способность к творчеству

и креативности существует у каждого индивида и главной задачей является развитие данных способностей [2, 7, 8] (см. табл. 1).

Опираясь на научные труды ученых XX–XIX вв., можно сказать, что креативность — это широкое понятие, совмещающее в себе совокупность разных на-

Таблица 1

Научные подходы к изучению креативности

Подход	Авторы научного подхода	Описание подхода
Мистический	А. Ротенберг, К. Хаусман	Креативность рассматривается, как божественное
Психо-динамический	Р. Вайсберг	Креативность рассматривается как «напряжение между осознанной реальностью и бессознательными движущими силами»
Психометрический	Д. Гилфорд, Э. Торренс	Изучение творчества и креативности в ходе испытаний контрольной группой людей с помощью психометрических тестов, которые используются для измерения уровня креативности
Когнитивный	Д. Гилфорд, Г. Уоллес	Когнитивные процессы лежат в основе творческих способностей. Креативность рассматривается как понятие в мыслительном процессе
Социально-личностный	Т. Амабайл, Ф. Бэррон, А. Маслоу, Т. Любарт	Исследования включали личностные характеристики, влияние мотивации на креативность и социальный климат, стимулирующие факторы креативного процесса
Интегративный	М. Чиксент-михайи, Г. Гарднер, М. Мамфорд, Р. Стернберг	Креативность включает в себя: особенности личных черт человека, когнитивные аспекты. Особое внимание уделяется вопросам креативной среды и ее влияния на индивида

Источник: Морозов В.В. [13]

учных подходов. Российскими и зарубежными психологами было определено, что креативность является совокупностью мыслительных и личностных качеств индивида. Современные компьютерные девайсы и использование сети Интернет позволяют создавать единое образовательное пространство, совмещающее в себе интеллектуальные, мотивационные и эмоционально-волевые аспекты деятельности индивида. Наряду с этим, внедрение дистанционного обучения в образовательный процесс привело к снижению креативности в учебном процессе, что было сопряжено с неготовностью преподавательского состава к резким изменениям в формах учебного процесса.

Дистанционное обучение — это форма обучения, основанная на информационных и телекоммуникационных технологиях, таких как заочное и очное обучение, которое включает в себя лучшие традиционные и инновационные методы, средства и формы обучения [5, 6]. В то же время, дистанционное преподавание можно определить как систему методов обучения, при которой преподавание осуществляется отдельно от учебной деятельности учащегося, однако, тем не менее, включая такую учебную деятельность, которая в аналогичной ситуации осуществлялась бы в присутствии учащихся. Таким образом, общение между преподавателем и учащимся должно обеспечиваться с помощью печатных, механических, электронных или других устройств [4].

Введение дистанционного обучения поставило серьезный вопрос по обеспечению высокого качества проверки знаний студентов и получения обратной связи. Онлайн-ресурсы Google forms, Survey Monkey, Socrative и другие позволяют оперативно обрабатывать ответы студентов. Опираясь на научную модель — таксономию целей Б. Блума, обучение должно включать в себя не только запоминание фактов, но и их анализ, оценку. Таксономия Б. Блума — это педагогическая методика, позволяющая систематизировать цели и задачи обучения, а также улучшать результаты запоминания и усвоения знаний в образовательном процессе.

Педагогическая методика Б. Блума включает три сферы, которые так или иначе соприкасаются друг с другом: когнитивную (знания) психомоторную (установки) и эмоциональную (навыки). Таксономия целей Б. Блума позволяет спланировать программу обучения, спрогнозировать эффективность составленной программы обучения в разных формах: лекции, семинары, тренинги, в которых особое место занимают креативные, творческие задания.

В основании пирамиды лежит получение знаний, повторение или распознавание информации. В верхушке пирамиды — оценка, которая проводится в рамках установленных критериев [1]. Каждый последующий уровень пирамиды Б. Блума базируется на предыдущем. На рис. 1 показано место креативных заданий в таксономии Б. Блума.

Для развития креативности, выполнения креативных, творческих заданий, на уровнях таксономии Б. Блума «анализ», «синтез», «оценка» как в очном, так

и в дистанционном обучении целесообразно использовать инновационные цифровые платформы и онлайн-сервисы. Например, широкий функционал сервисов досок совместного использования Conceptboard, Miro, GroupBoard позволяют оставлять комментарии с отметкой конкретных учеников, использовать стрелки соединения объектов во время работы над проектом (см. табл. 2).



Рис. 1. Место креативных заданий в таксономии Б. Блума

Источник: составлено автором на основе таксономии Б. Блума

Таблица 2

Доски совместного пользования для развития креативности обучающихся при групповой и индивидуальной работе

Название ресурса	Возможности ресурса	Ссылка на ресурс
Доски совместного использования Miro	Шаблоны для рисования, составление интеллект-карт, ведение групповых проектов, планирование по технологиям agile, онлайн-чат с участниками группы, бесконечное рабочее пространство	https://miro.com
Conceptboard	Ведение проектов, назначение задач для участников проектов	https://conceptboard.com
GroupBoard	Совместное использование доски с возможностью встраивания на сайт, управления доступом к изменениям на доске	https://www.groupboard.com/products

Источник: составлено втором

Возможна загрузка файлов с компьютера, по ссылке, из открытых библиотек и т.д. Уже сформированные проект на доске совместного использования могут быть запущены в режиме презентации без необходимости компьютерной верстки в других программах. Коммуникация членов команды возможна

через встроенный чат на платформе. Выполнение любого задания благодаря внутреннему таймеру может быть ограничено по времени по желанию преподавателя. На подобных платформах также может быть организована и индивидуальная работа студентов как во время аудиторной работы, так и внеаудиторного времени. Также они эффективны для проверки промежуточных знаний по учебным дисциплинам.

Наряду с досками совместного пользования среди онлайн-инструментов, легко встраиваемые в учебный процесс, и способствующие развитию креативности у обучающихся, можно выделить: онлайн-сервисы на основе использования VR-технологий (Thinglink, Artefact); сервисы создания интерактивных видео-квестов и видеоскрайбинга (рисованного видео) (Adventr, Sparkol); подкастинг (SoundCloud, Google Podcasts, Яндекс музыка); сервисы для создания таймлайнов (Timeline JS, myHistro); кроссвордов (Cross, Фабрика кроссвордов); викторин, интерактивных заданий (Kahoot, Factile, Flippity) и др.

Список литературы

1. Абдуллаев С.Г. Оценка эффективности системы дистанционного обучения. Телекоммуникации и информация образования / С.Г. Абдуллаев. — С. 85.
2. Лун А.Н. Мышление и творчество / А.Н. Лун. — М.: Политиздат, 1976.
3. Морозов В.В. Обзор зарубежных теорий креативности / В.В. Морозов // Вестник Оренбургского государственного университета. — 2016. — №12(200). — С. 35–41.
4. Небылицын В.Д. Основные свойства нервной системы / В.Д. Небылицын. — М.: Медгиз, 1966. — 363 с.
5. Туник Е.Е. Тест Торренса / Е.Е. Туник // Лучшие тесты на креативность. Диагностика творческого мышления. — СПб.: Питер, 2013. — С. 152–312.
6. Эшонкулов Х.И. О преимуществах дистанционного образования / Х.И. Эшонкулов.
7. Keegan, D. Foundations of Distance Education. 2013. — 240 p.
8. James C. Kaufman, Ronald A. Beghetto. Beyond Big and Little: the Four C Model of Creativity. Review of General Psychology 2009, Vol. 13, No. 1, 1–12.

MICROSOFT TEAMS КАК СРЕДСТВО ОРГАНИЗАЦИИ КЕЙС-СТАДИ ПРИ ДИСТАНЦИОННОМ ОБУЧЕНИИ

MICROSOFT TEAMS AS A TOOL FOR ORGANIZING CASE STUDIES IN DISTANCE LEARNING

**Ярных
Юлия Анатольевна**

Кандидат технических наук, доцент кафедры социально-гуманитарных, экономических и естественно-научных дисциплин ИПНБ РАНХиГС



**Yarnykh
Yuliya Anatol'evna**

Candidate of Technical Sciences, Associate Professor of the Department of Social, Humanitarian, Economic and natural sciences IPNB RANEPА

Аннотация. В статье анализируется программный продукт Microsoft Teams. Выделяются достоинства и недостатки данного программного продукта. Приводится пример проведения занятия по дисциплине «Статистика» с применением Microsoft Teams.

Ключевые слова: дистанционное обучение, Microsoft Teams, кейс-стади, статистика, методика преподавания.

Annotation. This article analyzes the Microsoft Teams software product. The advantages and disadvantages of this software product are highlighted. An example of conducting a lesson in the discipline "Statistics" using Microsoft Teams is given.

Keywords: distance learning, Microsoft Teams, case studies, statistics, teaching methods.

В настоящий момент мировое сообщество переживает настоящий цифровой бум. Толчком к всемирной цифровизации стала пандемия COVID-19, которая коснулась всех сфер профессиональной деятельности и жизнедеятельности в целом. Необходимость работать удаленно, обучаться удаленно, получать официальную информацию и государственные услуги удаленно, пользоваться развлекательными и жизнеобеспечивающими сервисами удаленно — все

это вызвало резкую трансформацию подходов и методов работы всех предприятий, бизнеса и органов управления.

Во многих госструктурах, начавшаяся и влотекущая трансформация к информатизации и цифровизации, началась с новой силой. Произошло ускорение внедрения новых государственных сервисов и государственных услуг. Конечно, такой резкий переход вызвал и негативную реакцию в обществе, связанную

в первую очередь с усилением цифрового контроля за гражданами, а во вторую с непониманием, неготовностью переходить на цифровую платформу, отказаться от привычных средств получения государственных услуг. Однако, уже сейчас, по прошествии года от начала пандемии, можно утверждать, что сервисы предоставления услуг становятся все удобнее и, самое главное, все доступнее для граждан. Цифровизация коснулась всех сфер жизнедеятельности и привела к оптимизации устаревших процессов, к развитию настоящего цифрового государства.

Не в стороне осталась и такая сфера, как образование. И если еще два года назад мы говорили о том, что средства дистанционного обучения — это хороший инструмент для организации принципа *Life Long Learning*, как концепции «пожизненного обучения» с целью повышения своих профессиональных компетенций, то сейчас дистанционное обучение — это уже часть базового обучения и школьников и студентов [6].

В предыдущих статьях мы анализировали и сравнивали различные образовательные платформы, которые позволяют организовать обучение в дистанционном режиме, предоставляя доступ к контенту из различных областей знаний, а также к полноценным обучающим курсам и модулям [6].

В данной статье мы остановимся на таком программном модуле, как *Microsoft Teams (MS Teams)*, который активно используется для организации занятий в дистанционном режиме. Попробуем выделить преимущества и недостатки данного программного продукта, а также рассмотрим использование средств *MS Teams* на примере одного из занятий по статистике.

Итак, если говорить о контенте многочисленных образовательных платформ, то раньше преобладали записанные видеолекции, теоретические материалы, документальные фильмы и исследования. Но, потеря возможности использовать очное обучение в период карантина, невозможность обсуждать, делать выводы, спорить и прогнозировать развитие ситуации в реальном режиме времени, все это породило огромный интерес к сервисам, позволяющим смоделировать очное присутствие на занятии.

Одним из таких сервисов является программный продукт компании *Microsoft* — *Microsoft Teams*. *Microsoft Teams* является частью пакета программ *Office 365* и доступен по корпоративной подписке. Программный продукт работает на операционных системах *Windows*, *Mac OS* и *Linux*, а также мобильных платформах *Android* и *iOS* [2].

Microsoft Teams — современный удобный инструмент для организации удаленной работы с информацией, для организации совместной работы в команде и осуществления коммуникации.

Поработав с данным программным продуктом почти год, можно попытаться объективно выделить преимущества и недостатки данного инструмента.

Из главных преимуществ хочется выделить в первую очередь доступность программы. В эпоху со-

циального неравенства, каждый пользователь, желающий обучаться, общаться и развиваться может с легкостью воспользоваться on-line версией программного обеспечения, не устанавливая на свой ПК версию корпоративную — по подписке. При этом основные возможности сохраняются в on-line версии, и выбор такого варианта не влияет на качество работы в сети. Отметим, что *MS Teams* поставляется в рамках бесплатного предложения для школ по всему миру в составе пакета *Microsoft Office 365 A1* для образования.

Второй очевидный плюс — это возможность использования различных форм обучения и представления знаний и информации. Имеется ввиду, интеграция *MS Teams* с более чем 140 сторонними приложениями и собственными продуктами *Microsoft*. При этом программные продукты *Microsoft* встроены сразу в платформу *MS Teams*. А это значит, что преподаватель может создавать документы разного формата непосредственно в *Microsoft Teams* и использовать их для организации совместной работы с обучающимися.

Очень удобно и быстро загружаются любые приложения, необходимые в работе. Рассказывая новый материал, докладчик может использовать видео и аудио контент, загрузить презентацию и поделиться своим экраном со слушателями, использовать экран как интерактивную доску. При работе, например, со статистическими данными можно загрузить *MS Excel* или компьютерную программу для статистической обработки данных — *SPSS Statistics*. При работе с формулами можно загрузить профессиональный инструмент для набора формул и математических выражений — *MathType* или воспользоваться встроенным редактором формул в *MS Word*. Для создания заметок можно использовать виртуальные блокноты *OneNote* и *Class Notebooks*, которые позволяют обмениваться материалами, заметками и данными. А можно для создания небольших записей или тех же математических формул воспользоваться встроенной виртуальной доской, доступ к которой можно сделать совместным и организовать работу так, что будет полное ощущение работы с привычной классной интерактивной доской. Все это открывает широкие возможности для преподавателя, докладчика, модератора при планировании и проведении занятий.

Третье преимущество *MS Teams* это возможность хранения больших объемов информации. Корпоративный пакет включает в себя доступ к облачному хранилищу объемом 10 ГБ плюс дополнительные 2 ГБ на каждого зарегистрированного пользователя. Вы можете хранить свои лекции, видеоматериалы, задания и наглядные пособия в облачном сервисе, а значит иметь к ним доступ в любое время и в любом месте.

Четвертое преимущество *MS Teams* разнообразие форм работы в виртуальном классе. Это может быть совместная работа всех присутствующих, где есть возможность обмениваться сообщениями, файлами и мнениями. Это может быть работа в группах. В этом случае преподаватель выступает в роли модератора

и настраивает доступ пользователей в группы, перемещение между группами, работу отдельных групп и совместную работу групп с преподавателем и групп между собой. Это сложная, но очень увлекательная работа, позволяющая организовать такие формы обучения, как кейс-стади, брейншторм, проектная работа, выполнение лабораторных работ и т.д. Все это способствует совместному поиску продуктивных способов решения задач, повышает чувство ответственности и социально-личной значимости при выработке решения, создает возможности и благоприятные условия для диалога [1, 3].

Пятым преимуществом назовем возможность добавлять сторонних спикеров, консультантов, наблюдателей. По причинам безопасности, учебные группы в MS Teams рекомендуется создавать закрытыми. Однако, при необходимости пригласить спикера для разового выступления, в программном модуле реализована и такая возможность.

Шестым, седьмым и восьмым преимуществом выделим соответственно возможность организовать внеурочную совместную деятельность, возможность составлять расписания с уведомлениями и записывать учебные занятия для последующего использования.

Все основные преимущества, выделенные в данной статье представлены на рис. 1.

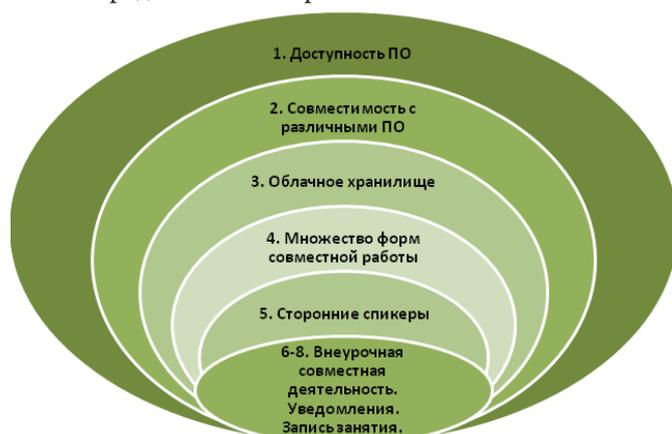


Рис. 1. Преимущества работы с программным модулем Microsoft Teams



Рис. 2. Недостатки при работе с программным модулем Microsoft Teams

Теперь поговорим о недостатках, неудобствах, которые возникли при работе с Microsoft Teams.

На основе проведенных исследований (опроса студентов 1–3 курсов факультета «Таможенного дела» РАНХиГС при Президенте РФ) выделим следующие, наиболее часто встречающиеся недостатки при работе с MS Teams (рис. 2).

1. Неустойчивая работа приложения. Возникали случаи, когда программа зависала, закрывалась или переставала выполнять ряд функций. В таких ситуациях приходилось перезапускать программное обеспечение и начинать работать заново. Следует отметить, что такие ошибки встречались чаще всего в on-line версии программы. Установленная на компьютере программа MS Teams работала более стабильно.

2. Не поддерживает некоторые форматы файлов. Так, не работает с файлами DOC, XLS и PPT. Для отображения данных документов, таблиц и презентаций их предварительно следует перевести в формат docx, xlsx, pptx соответственно.

3. Ограниченные возможности. Например, нельзя послать одновременно более 10 файлов, что вызывает неудобства и необходимость повторной отправки. Нет возможности поделиться звуком из ПК: при включении видеоролика со звуком — аудио будет транслироваться через микрофон, что, значительно ухудшает качество транслируемого звука.

4. Сложный функционал и непростой интерфейс. Для настроек некоторых возможностей, например, таких как виртуальные комнаты, следует потратить время и, возможно, воспользоваться инструкцией. Не совсем интуитивно понятный интерфейс, неподготовленный человек легко запутается.

Подводя итог сравнительной характеристике плюсов и минусов программного модуля MS Teams, отметим, что исследуемый программный продукт качественный, полезный и интересный для его использования в обучающих целях в ВУЗах.

Ранее мы описывали широкие возможности ситуационных центров для организации кейс-стади на примере УАЗ «Анализ и прогнозирование социально-экономической напряженности в регионе» [5], в данной статье рассмотрим пример организации и проведения кейс-стади по дисциплине «Статистика» у студентов 2 курса, обучающихся по специальности «Таможенное дело» РАНХиГС с использованием средств MS Teams. Кейс-стади проводится на занятии продолжительностью 4 академических часа.

Целью кейс-стади является освоение информационных технологий групповой работы в дистанционном режиме с использованием различных программных продуктов.

Теория статистики — теоретическая основа построения кейс-стади.

В ходе проведения кейс-стади студенты делятся на микрогруппы. При этом деление происходит по собственной инициативе и в соответствии с поставленными целями, возникшими интересами участников команд.

Каждая микрогруппа выбирает регион Российской Федерации для анализа демографической ситуации в

Этапы кейс-стадий

№ п/п	Этапы (участники)	Виды работ	Программное обеспечение
1	Формулировка цели, постановка задач. (Преподаватель)	Формулировка общей цели занятия. Постановка общей задачи. Постановка задач для каждой микрогруппы	MS Teams, MS Power Point
2	Работа в микрогруппах. (Участники микрогрупп, преподаватель)	Выбор региона исследования. Импортирование статистических данных в программу обработки [4]. Расчет основных статистических показателей: динамики роста рождаемости и смертности по региону за последние 10 лет. Построение аналитического графика с прогнозом на ближайшие 5 лет. Подготовка отчета в виде мини-презентации с основными данными, расчетами и выводами	MS Teams, Microsoft Power Point, Microsoft Excel, SPSS Statistics, Microsoft Word, Internet ресурсы (Портал Федеральной службы государственной статистики)
3	Представление результатов исследования и прогнозирования. (Участники микрогрупп)	Обоснование выборки данных. Выводы и прогнозы	MS Teams, Microsoft Power Point
4	Вопросы и обсуждение. (Преподаватель, эксперты, участники микрогрупп)	Вопросы по результатам прогнозирования для каждой микрогруппы. Оценка прогноза. Обсуждение и корректировка ошибок прогноза. Сбор оценочной информации в виде заготовленной формы	MS Teams, Microsoft Power Point, Microsoft Forms
5	Выводы, (Преподаватель)	Подведение итогов кейс-стади	MS Teams

нем за последние 10 лет. По результатам выполнения задания группа создает отчет в виде презентации и защищает его перед всеми участниками кейс-стади.

Основные этапы кейс-стади «Исследование и прогнозирование демографической ситуации в регионах Российской Федерации», участники и виды работ изложены в табл. 1.

Проводимое занятие в форме кейс-стади, позволяет не только обучить и познакомить студентов с методикой работы в группах в режиме дистанционного обучения с применением программного модуля MS Teams, но и отработать навыки поиска статистической информации, ее обработки и анализа.

Данное занятие позволяет полноценно участвовать в обучении всем студентам, без потери качества обучения.

Программный модуль Microsoft Teams является удобным инструментом, помощником и средством для подготовки, проведения и записи подобных занятий.

Список литературы

1. Быкова Н.И. Исследование «кейс-метода»: теорет. аспекты / Н.И. Быкова. — СПб.: Изд-во С.-Петербур. гос. ун-та экономики и финансов, 2002. — 16 с.

2. Официальный интернет-портал компании Microsoft. [Электрон. ресурс]. — Режим доступа: <https://www.microsoft.com/ru-ru>. (дата обращения 12.02.2021).
3. Развитие профессионализма преподавателя высшей школы: учеб.- метод. пособие / В.С. Агапов [и др.]; под науч. ред. А.А. Деркача; Рос. акад. гос. службы при Президенте Рос. Федерации. — изд. 2-е, стер. — М.: РАГС, 2009. — 383 с.
4. Федеральная служба государственной статистики [Электрон. ресурс]. — Режим доступа: <https://rosstat.gov.ru>. (дата обращения 12.02.2021).
5. Ярных Ю.А. Аналитический доклад, как результат УАЗ «Анализ и прогнозирование социально-экономической напряженности в регионе», реализованный средствами Ситуационного центра / Ю.А. Ярных // Электронный научный журнал. — 2019. — С. 102–110.
6. Ярных Ю.А. Концепция «Life Long Learning» как глобальная стратегия развития современного общества. Государственное управление и развитие России: национальные цели и институты / Ю.А. Ярных, Н.В. Свертилова — Т. 2. — М.: Научная библиотека, 2019. — 1432 с.

ПРАВОВОЕ ОБЕСПЕЧЕНИЕ В СФЕРЕ НАУКИ, ТЕХНОЛОГИЙ И ОБРАЗОВАНИЯ

ИССЛЕДОВАНИЕ И АНАЛИЗ IT-ТЕХНОЛОГИЙ, ПРИМЕНЯЕМЫХ В ИНФРАСТРУКТУРЕ ЭЛЕКТРОННОГО ПРАВИТЕЛЬСТВА

RESEARCH AND ANALYSIS OF IT-TECHNOLOGIES USED IN THE INFRASTRUCTURE OF ELECTRONIC GOVERNMENT

**Таукенова
Лязат Жумабаевна**

*Доктор по профилю, университет «Туран-Астана»,
Нур-Султан, Казахстан*



**Taukenova
Lyazat Zhumabaevna**

*Doctor in profile, University "Turan-Astana",
Nur-Sultan, Kazakhstan*

**Исакаева
Анара Жанатовна**

*Консультант департамента цифровизации
и планирования бюджета АО «Центр электронных
финансов», Нур-Султан, Казахстан*

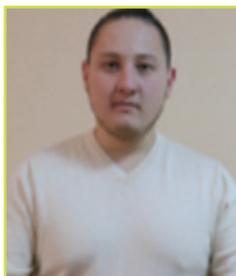


**Isakaeva
Anara Zhanatovna**

*Consultant of the Department of Digitalization
and Budget Planning, JSC "Center for Electronic Finance",
Nur-Sultan, Kazakhstan*

**Жумабаев
Ержан Ныгметжанович**

*Специалист по сопровождению и эксплуатации ИС,
«Академия Имиджологии», Нур-Султан, Казахстан*



**Zhumabaev
Erzhan Nygmetzhanovich**

*IS Maintenance and Operation Specialist,
"Imageology Academy", Nur-Sultan, Kazakhstan*

Аннотация. Глобализация и развитие «информационного общества» стремительно меняют облик современного мира. Одним из неотъемлемых фрагментов «информационного общества» является «электронное правительство», работающее на базе информационной инфраструктуры органов государственной власти, обеспечивающее эффективную реализацию большинства функций государственного управления и в первую очередь, ориентированную на взаимодействие государственного аппарата с гражданами и бизнес-структурами на основе новых информационных технологий. В данной статье рассматривается, построение архитектуры и инфраструктуры электронного правительства.

Ключевые слова: электронное правительство, единая архитектура, информационно-телекоммуникационная инфраструктура, электронно-цифровая подпись.

Abstract. Globalization and the development of the "information society" are rapidly changing the face of the modern world. One of the integral parts of the "information society" is the "electronic government", which operates on the basis of the information infrastructure of public authorities, ensuring the effective implementation of most functions of public administration and, first of all, focused on the interaction of the state apparatus with citizens and business structures based on new information technologies. This article discusses the construction of the architecture and infrastructure of e-government.

Keywords: e-government, unified architecture, information and telecommunications infrastructure, electronic digital signature.

Процесс совершенствования государственного управления посредством применения информационно-коммуникационных технологий принято называть созданием «электронного правительства».

«Электронное правительство» — это механизм функционирования государственных органов, основанный на широком применении информационных технологий и максимально ориентированный на предоставление услуг гражданам и организациям, в том числе посредством сети Интернет. Основным средством коммуникации во взаимодействии государственных органов с населением и организациями является Интернет, как наиболее доступное для людей средство электронного взаимодействия. Внедрение технологий «электронного правительства» в государственном управлении позволит ускорить рост экономики страны, уменьшит затраты на бюрократические процедуры, повысит эффективность работы и производительность труда государственных учреждений, расширит возможности участия населения в формировании гражданского общества за счет свободного доступа к различного рода информации, создания более прозрачной работы государственных органов, ослабления бюрократических барьеров, снижение коррупции. Электронное правительство базируется на распределенной информационно-телекоммуникационной инфраструктуре (инфраструктура электронного правительства), развернутой в масштабах государства. Ядром которой является система электронного документооборота, система автоматизации государственного управления, основанная на автоматизации всей совокупности управленческих процессов в масштабах страны и служащая цели существенного повышения эффективности государственного управления и снижения издержек социальных коммуникаций для каждого члена общества. Национальные программы по созданию электронного правительства предполагают поэтапное построение общегосударственной распределенной системы общественного управления, реализующей решение полного спектра задач, связанных с управлением документами и процессами их обработки. Суммируем их в следующем определении: электронное правительство — это новые возможности управления государством, созданные посредством применения информационно-коммуникационных технологий (ИКТ) в работе государственных органов на благо юридических и физических лиц, так же, как и для собственных нужд. Электронное правительство состоит из двух частей: первая — взаимоотношения власти и общества и вторая — внутреннее взаимодействие разных уровней (центрального, регионального, местного) и разных ветвей власти (исполнительной, законодательной, судебной) [1].

К стратегическим целям перехода к ЭП следует отнести:

- повышение открытости и прозрачности деятельности правительства, снижение уровня бюрократии при обращении граждан и бизнес-структур к правительственным услугам;

- реализацию прав граждан на доступ ко всем видам открытой государственной информации, имеющей индивидуальную и общественную значимость;
- увеличение уровня прогнозируемости общественных процессов и степени управляемости и самоуправляемости общества;
- обеспечение единства общенационального информационного пространства, а также эффективного использования государственной информационно-коммуникационной инфраструктуры;
- обеспечение необходимого уровня общественного контроля над деятельностью государственных органов и организаций, становление демократии и институтов гражданского общества, обеспечение гражданских свобод;
- поддержку процессов информатизации общества, достижение качественно новых состояний в сфере образования, информационной культуры [2].

Реализация инициатив ЭП будет обеспечена благодаря использованию структурированных, систематических подходов к планированию и реализации этих инициатив, основанных на разработке и реализации единой архитектуры ЭП.

Единая архитектура ЭП (далее — ЕА) представляет собой структуру, отображающую взаимосвязи между всеми элементами ЭП и должна позволить идентифицировать и систематизировать существующие у различных министерств и ведомств потребности по использованию ИКТ, возможности по сокращению имеющейся избыточности, а также определить направления, по которым у них имеются однородные запросы на инвестиции в ИКТ.

ЕА электронного правительства, являясь эталонной моделью процессов и структур государственного управления, представляет методологическую основу реализуемых ИКТ-проектов и мероприятий. В этом качестве ЕА предназначена обеспечивать:

- поддержку корректности целей отдельных проектов;
- координацию проектов между собой;
- оценку эффективности отдельных проектов;
- оптимизации использования средств за счет устранения дублирования работ;
- инвестирования в перспективные технологии и совместимые системы.

Ключевая роль ЕА четко проявляется на примере межведомственных проектов, где ЕА выступает в качестве единого «каркаса», который используется и как набор критериев оценки проектов и как один из обязательных нормативных и методических инструментов по выбору, выполнению и контролю эффективности проектов.

ЕА является целостным взглядом на то, что государство и отдельные ведомства делают, как они работают, и как ИКТ обеспечивают необходимую для этого поддержку. Без такого системного подхода реализация инициативы электронного правительства неизбежно будет сопряжена с большим количеством проблем и неэффективных затрат.

Общая структура ЕА состоит из трех архитектурных слоев, связанных требованиями реализации потребностей:

- архитектура деятельности;
- системная архитектура;
- техническая архитектура, а также двух «сквозных» архитектурных компонент, имеющими свои отражения в каждом из трех предыдущих слоев:
- архитектура непрерывности деятельности и безопасности;
- архитектура производительности (эффективности) [3].

В основе архитектуры деятельности должна лежать модель описания деятельности государственных и местных органов власти с точки зрения функций и процессов реализации этих функций. Эта модель должна описывать взаимные обязательства органов государственной власти, а также их обязательства по отношению к гражданам и бизнес-структурам.

Системная архитектура отражает главные связи предлагаемых государственными и местными органами власти услуг с прикладными архитектурными компонентами поддержки этих услуг средствами ИКТ прикладного уровня. Она содержит стандарты и рекомендации развития информационных систем государственных и местных органов власти, обеспечивающих реализацию государственных функций, а также базовых компонент и элементов ЭП, которые должны использоваться централизованно или многократно многими ведомствами: портал ЭП, удостоверяющий центр, национальная идентификационная система.

Техническая архитектура отражает возможности базовых информационно-коммуникационных технологий в качестве средств организации взаимодействия прикладных компонент системной архитектуры между собой, с источниками данных и с пользователями информационных систем. Данная архитектура включает в себя стандарты и рекомендации на используемые в государстве аппаратное и программное обеспечение, коммуникации, технологические стандарты и протоколы, а также методологию описания и стандартизации данных государственных информационных систем и стандарт на метаданные.

Архитектура непрерывности деятельности и безопасности предназначена для планирования, поддержки реализации и контроля на архитектурном уровне комплексов действий и средств, предназначенных для обеспечения непрерывности деятельности органов власти и систем ЭП с заданными значениями параметров и обеспечения информационной безопасности.

Архитектура производительности (эффективности) ЭП и его компонентов представляет собой систему сбалансированных показателей и общих метрик для оценки значений производительности, результативности и эффективности компонентов ЭП по всей вертикали — от отдельных информационных систем и деловых процессов до главных результатов деятельности и их стратегических влияний (последствий) [4].

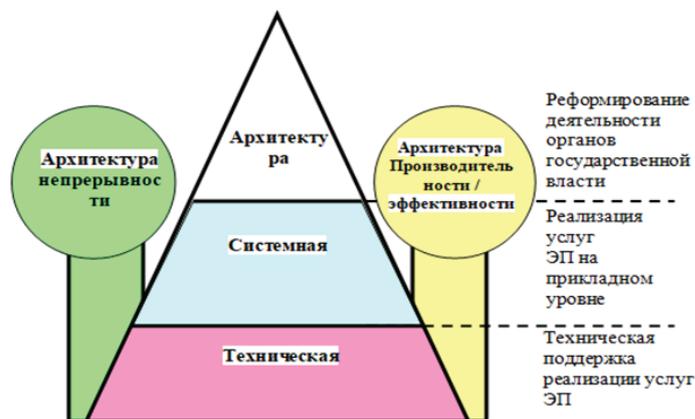


Рис. 1. Единая архитектура ЭП

Отношение субъектов электронного правительства. Инфраструктура электронного правительства состоит из двух взаимосвязанных, но функционально самостоятельных контуров:

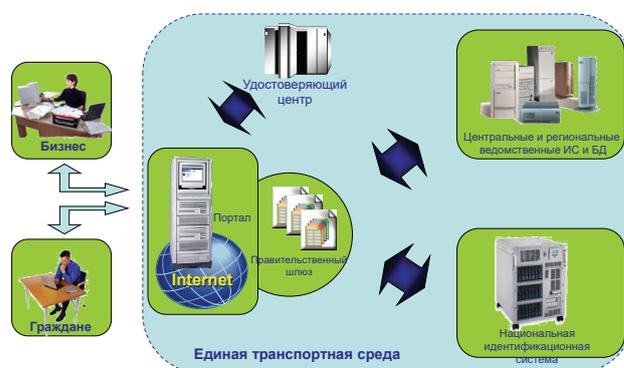


Рис. 2. Общая схема инфраструктуры ЭП

Внутренний контур. Данный контур охватывает информационные системы, обслуживающие внутри правительственные (ведомственные и межведомственные) бизнес-процессы, включая функционально-целевые ИС. Эти бизнес-процессы осуществляются как в центре, так и на региональном уровне.

Здесь идет речь о взаимоотношениях типа «правительство-правительство». Также в данном контуре выделяется такой сектор как «правительство-служащий», учитывая, что эти операции носят внутриведомственный характер, они могут рассматриваться как подгруппа сектора «правительство-правительство».

Внутренний контур содержит в себе виды деятельности, которые используют государственные структуры во взаимосвязи между собой для реализации государственных корпоративных задач.

Внешний контур. Данный контур охватывает публичную информационную инфраструктуру, обеспечивающую взаимодействие государства с гражданами и организациями и охватывающую информационные системы, обслуживающие бизнес-процессы взаимодействия населения и бизнес-структур с правительством через единый шлюз. Внешний контур содержит в себе два других сектора ЭП, таких как «правительство – граждане» и «правительство – организации».

К основным компонентам инфраструктуры ЭП относятся:

1. Портал ЭП, обеспечивающий реализацию единой точки входа к ведомственным информационным системам, ориентированным на предоставление интерактивных услуг гражданам и бизнес-структурам.

2. Удостоверяющий центр, являющийся компонентом инфраструктуры открытых ключей, являющийся основой для обеспечения защищенного информационного обмена, санкционированного доступа к услугам, предоставляемым ведомственными информационными системами, а также подтверждение авторства электронных документов.

3. Национальная ИС, позволяющая идентифицировать субъекты взаимодействия.

4. Единая защищенная транспортная среда, обеспечивающая функционирование и взаимодействие внутренних ИС, и защищенный выход в телекоммуникации общего пользования.

5. ИС ведомств и местных органов власти — поставщики электронных услуг.

В настоящее время ведомственные ИС, в основном предназначены для решения внутренних задач, и только некоторые ведомства предоставляют простые электронные услуги без достаточной гарантии конфиденциальности и целостности. Особое значение также принимает решение проблем совместимости корпоративных сетей и ведомственных ИС.

В связи с этим, нужно отметить, что создание инфраструктуры ЭП, должно отвечать описанным ниже требованиям.

Основная сложность реализации проектов в области электронного правительства, в частности, реализации межведомственных проектов, когда требуются существенные усилия по интеграции информационных систем, заключается не в применении конкретных технологий, а в организации процесса принятия соответствующих стандартов и согласования архитектур ИТ различных организаций и ведомств.

Для реализации инфраструктуры e-government необходимо предусмотреть такие стандарты, как:

- стандарты представления данных;
- стандарты межведомственного обмена информацией;
- стандарты метаданных (и поиска информации);
- стандарты информационной безопасности.

Необходимо уделить большое внимание стандартам и протоколам, которые должны гарантировать совместимость государственных систем и технологий. Ключевые стандарты обеспечения совместимости и единства государственных систем задают основные требования для предоставления интегрированных онлайн-услуг государственных услуг. Следование этим стандартам является обязательным для всех государственных систем.

Должны поддерживаться следующие стандарты:

- все государственные информационные системы должны использовать универсальные Интернет-совместимые общие спецификации (HTML, IP, SMTP и др.);

- в качестве основного стандарта при интеграции ведомственных информационных систем и представления данных в Интернете должен применяться язык XML или производные от него;
- все государственные информационные ресурсы должны быть доступны с помощью Интернет технологий, то есть предоставлять пользователям веб-интерфейс в качестве основного. В качестве дополнения могут использоваться другие интерфейсы, основанные на WAP технологиях;
- все государственные информационные ресурсы, представленные в Интернете должны быть снабжены метаданными, облегчающими публикацию и поиск информации[5].

В концепции «электронного государства» вся система органов исполнительной власти, функционирует как единая сервисная организация, предназначенная для оказания услуг населению. Деятельность «e-government» должна быть достаточно открытой, информационно прозрачной и доступной для граждан. Особое внимание уделяется принципу обратной связи, скорости и качеству предоставления услуг, посредством широко использования централизованных систем Интернета. Все это призвано повысить как качество оказания государством услуг населению, так и эффективность функционирования самого правительства.

Практическая реализация электронного правительства в России и Казахстане идет в одном русле, и его структура схематично представлена на рис. 3–4.

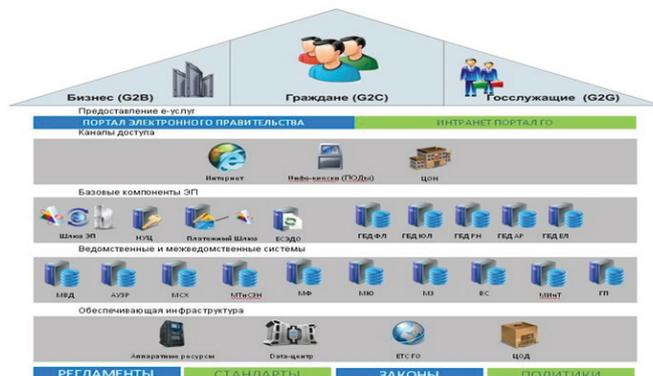


Рис. 3. Практическая реализация электронного правительства в Казахстане

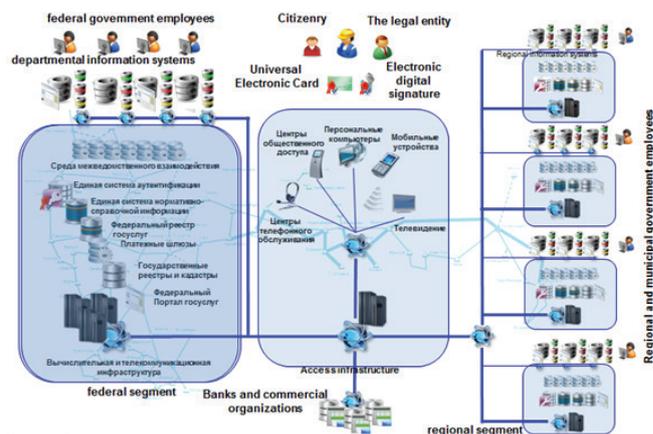


Рис. 4. Практическое внедрение электронного правительства в России

Электронное правительство базируется на распределенной информационно-телекоммуникационной инфраструктуре (инфраструктура электронного правительства), развернутой в масштабах государства. Ядром которой является система электронного документооборота, система автоматизации государственного управления, основанная на автоматизации всей совокупности управленческих процессов в масштабах страны и служащая цели существенного повышения эффективности государственного управления и снижения издержек социальных коммуникаций для каждого члена общества. Национальные программы по созданию электронного правительства предполагают поэтапное построение общегосударственной распределенной системы общественного управления, реализующей решение полного спектра задач, связанных с управлением документами и процессами их обработки. В глобальном рейтинге развития электронного правительства, который формирует ООН, Казахстан поднялся на 29 место, следуя за Канадой. Данный рейтинг составляется каждые 2 года и в нем оценивается 193 страны-члена ООН. При составлении текущего рейтинга (2020) оценивалась работа, проведенная государствами в 2018-2019 годах. Согласно данным ООН, в первую тройку лидеров по развитию электронного правительства вошли Дания, Южная Корея и Эстония, которые расположились на 1, 2 и 3 позициях соответственно. Среди стран СНГ Казахстан занял 1 место. Далее расположились Россия (36), Беларусь (40), Молдова (79), Украина (69), Узбекистан (87) и др. В рейтинге 2020 года Португалия располо-

жилась на 35 месте, Италия на 37, Бельгия на 41, Китай на 45, Малайзия на 47 месте. Отметим, самую высокую позицию в данном рейтинге, 28 место, Казахстан занимал в 2014 году. В 2016 страна расположилась на 33 месте, а в 2018 году на 39 позиции. Таким образом, за последние 2 года Казахстан поднялся на 10 позиций. Глобальный рейтинг ООН по развитию электронного правительства (EGDI) рассчитывается на основе трех составляющих: развитие электронных услуг (OSI), развитие человеческого капитала (HCI) и телекоммуникационной инфраструктуры (ТИ).

Список литературы

1. Реализация концепции электронного правительства: новый этап [Электрон. ресурс]. — Режим доступа: <http://emag.iis.ru/arc/infosoc/emag.nsf/BPAEng/890b2440d66b70fcc32571780046f577>.
2. Создание электронного правительства с учетом международного опыта [Электрон. ресурс]. — Режим доступа: <https://elib.bsu.by/bits/tream/123456789/57198/1/49803.pdf>.
3. Формирование региональных сегментов инфраструктуры электронного правительства на базе Единого национального оператора [Электрон. ресурс]. — Режим доступа: <https://en.ppt-online.org/13940>.
4. Электронное правительство в РФ [Электрон. ресурс]. — Режим доступа: <https://digital.gov.ru/ru/activity/statistic/rating/elektronnnoe-pravitelstvo-v-rf/>.
5. E-GOV: Портал «Электронного правительства» [Электрон. ресурс]. — Режим доступа: <https://www.nitec.kz/>.

ВЕРОЯТНОСТНЫЙ АНАЛИЗ БЕЗОПАСНОСТИ В ИНФОРМАЦИОННЫХ СИСТЕМАХ

PROBABILISTIC ANALYSIS OF SECURITY IN INFORMATION SYSTEMS

Бритвина Валентина Валентиновна

Кандидат педагогических наук, доцент кафедры «Инфокогнитивные технологии» Московского политехнического университета, доцент кафедры «Управление и информатика в технических системах» Московского государственного технологического университета «СТАНКИН»



Britvina Valentina Valentinovna

Candidate of Pedagogy, Associate Professor of the Department of Information Cognitive Technologies of the Moscow Polytechnic University, Associate Professor of the Department of Management and Informatics in Technical Systems, Moscow State Technological University STANKIN

Аннотация. В статье проанализировали вероятностный анализ безопасности в информационных системах. Определили его значимость при обеспечении ИБ в ИС.

Ключевые слова. Вероятностный анализ, информационная безопасность, информационные системы, Значимость.

Abstract. The article analyzes the probabilistic analysis of security in information systems. Determined its importance in providing information security in IP.

Keywords: Probabilistic analysis, information security, information systems, Significance.

Введение

Безопасность информации в информационных системах является очень важным вопросом. Так как, информация, находящаяся на электронных носителях играет большую роль в жизни современного общества. На сегодняшний день проблемам информационной безопасности (ИБ) как в масштабах государства, так и в масштабах отдельного предприятия уделяется достаточное внимание, несмотря на это, количество потенциальных угроз не становится меньше [1, 5].

Цель исследования

Выявить необходимость вероятностного анализа безопасности в информационных системах.

Задачи исследования:

Определить сферы и значимость использования вероятностного анализа в сфере ИБ

Результат исследования

В качестве основного показателя в вероятностных моделях обнаружения компьютерных атак используется:

- вероятность появления новой формы пакета передачи данных отличной от эталонной;
- математическое ожидание и дисперсия случайных величин, характеризующих изменение IP-адресов источника и потребителя информации, номеров портов АРМ источников и потребителей информации.

Статистические методы дают хорошие результаты на малом подмножестве компьютерных атак из всего множества возможных атак. Недостаток статистических моделей обнаружения аномальных отклонений состоит в том, что они не позволяют оценить объем передаваемых данных и не способны обнаружить вторжения атак с искаженными данными. Узким местом методов является возможность переполнения буфера пороговых проверок «спамом» ложных сообщений.

Для эффективного использования статистических моделей в методе обнаружения аномальных отклонений необходимы строго заданные решающие правила и проверка ключевых слов (порогов срабатывания) на различных уровнях протоколов передачи данных. В противном случае доля ложных срабатываний, по некоторым оценкам, составляет около 40 % от общего числа обнаруженных атак.

Существуют два основных подхода в анализе безопасности в ИС: обеспечение базового уровня защиты и подход, основанный на оценке и управлении рисками [5]. Для первого подхода обязательно проверяется соответствие компонентов ИС всем стандартам и требованиям [2, 3, 4].

В ходе реализации второго подхода оцениваются факторы риска, актуальность угроз и снижается уровень риска до приемлемого. Для определения актуальных мер защиты информации более рационально использовать второй подход. Поэтому далее будут рассмотрены методы реализации второго подхода.

В цикле работы ИС встречаются такие понятия, как риск, ущерб и угроза, которые представлены на рис. 1.



Рис. 1. Цикл работы ИС

Рис — это сочетание вероятности осуществления определенного события и негативных последствий (то есть нанесение потенциального или реального ущерба активу или группе активов), связанных с этим событием.

Ущерб — выраженные негативные последствия.

Угроза — возможность реализации риска.

Рациональным является использование подхода, завязанного на оценивании факторов риска, актуальности угроз и снижении уровня риска до приемлемого.

Выделяется два способа оценки рисков — двухфакторный (1) и трехфакторный (2) [6,7].

$$R(t) = \text{Poss}(T) \text{Impact}(t) \quad (1),$$

$$R(V, T) = \text{Poss}(V) \text{Poss}(T) \text{Impact}(T) \quad (2),$$

$\text{Poss}(V)$ — вероятность использования уязвимости V ;

$\text{Poss}(T)$ — вероятность реализации угрозы T через заданную уязвимость V ,

$\text{Impact}(T)$ — ущерб от реализации угрозы T .

Возможна качественная и количественная оценка рисков ИБ. В первом случае оценка производится на качественных шкалах, а во втором на непрерывных числовых интервалах.

Методы качественной оценки рисков ИБ представлены на рис. 2.

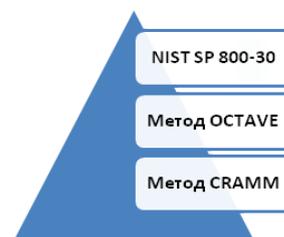


Рис. 2. Методы качественной оценки рисков ИБ

NIST SP 800-30 можно разделить на 9 основных этапов:

1. Определение характеристик системы.
2. Определения уязвимостей.
3. Определения угроз.
4. Анализ мер безопасности.
5. Определение вероятности.
6. Анализ влияния.
7. Определение риска.
8. Выработка рекомендаций.

9. Документирование результатов.

Метод OOSTAVE также предполагает несколько фаз: построение профиля угрозы на основе активов; идентификация уязвимостей инфраструктуры; разработка стратегии защиты и планов по снижению рисков ИБ.

Метод CRAMM был разработан Агентством по компьютерам и телекоммуникациям Великобритании, на сегодняшний день он используется в качестве государственного стандарта. Данный метод так же можно разделить на этапы:

1. Построение модели активов, определение их ценности.

2. Трехфакторная оценка рисков (без учета реализованных контрмер).

3. Определение набора мер безопасности.

Методы количественной оценки рисков ИБ показаны на рис. 3.

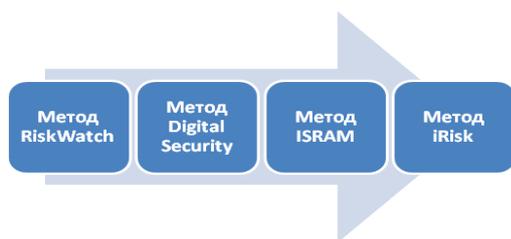


Рис. 3. Методы количественной оценки рисков ИБ

Метод RiskWatch один из самых мощных методов количественной оценки рисков. Он так же реализуется в несколько этапов:

1. Определение состава автоматизированной системы и требований по ее защите.

2. Описание активов, возможных потерь и инцидентов рассматриваемой системы.

3. Определение количественного значения рисков и выбор обеспечения мер безопасности.

4. Составление отчетности.

Метод Digital Security рассматривает две основных модели оценки рисков: модель информационных потоков и модель анализа угроз и уязвимостей (анализ угроз для активов и уязвимостей).

Метод ISRAM использует опросные листы для оценки факторов риска. Он находится в диапазоне от 1 до 25 и вычисляется по формуле, где i показывает номер вопроса, используемого для оценки вероятности реализации угрозы; j — номер вопроса, используемого для оценки последствий от реализации угрозы; m и n — количество экспертов, участвующих в опросе; w_i и w_j — веса вопросов (%); p_i и p_j — количественные значения выбранных ответов на вопросы с номерами i и j ; T_1 и T_2 — порядковые шкалы для оценки вероятности реализации угроз и последствий.

В методе iRisk оценка рисков осуществляется по формуле $iRisk = (Vulnerability \cdot Threat) - Control$, где Vulnerability — оценка уязвимости; Threat — оценка угрозы; Control — оценка мер безопасности.

Благодаря вероятностному анализу рисков можно более компетентно распределить ресурсы ИС, что позволит создать подготовленную ИБ.

Заключение

Использование вероятностного анализа на этапе оценки рисков в ИБ позволяет обеспечить максимальную защиту критических элементов ИС. Так как подсчет вероятности риска способствует определению важности конкретного элемента для владельца ИС. Вероятностный анализ является главным при построении ИБ ИС, так как он позволяет обеспечить максимальную защиту критических элементов и оберегает от лишней затраты ресурсов самой ИС. Происходит грамотное определение значимости элементов, что помогает в экономичном распределении возможностей владельцев ИС. В конечном итоге получаем систему высокого качества, в которой учтены все риски, и каждый критический элемент имеет квалифицированную защиту.

Для решения проблемы обеспечения ИБ необходимо применение законодательных, организационных и программно-технических мер. Пренебрежение хотя бы одним из аспектов этой проблемы может привести к утрате или утечке информации, стоимость и роль которой в жизни современного общества приобретает все более важное значение.

Список литературы

1. Аудит информационной безопасности — основа эффективной защиты предприятия [Электрон. ресурс]. — Режим доступа: <http://www.dialognauka.ru/press-center/article/4753/>.
2. Менеджмент риска. Анализ риска технологических систем [Электрон. ресурс]: ГОСТ Р 51901.1-2002. — Режим доступа: <http://vsegost.com/Catalog/62/6283.shtml>.
3. Информационная технология. Методы и средства обеспечения безопасности. Часть 1. Концепция и модели менеджмента безопасности информационных и телекоммуникационных технологий [Электрон. ресурс]: ГОСТ Р ИСО/МЭК 13335-1-2006. — Режим доступа: <http://vsegost.com/Catalog/27/271.shtml>.
4. Менеджмент риска. Анализ дерева неисправностей [Электрон. ресурс]: ГОСТ Р 51901.13-2005 (МЭК 61025:1990). — Режим доступа: <http://docs.pravo.ru/document/view/20841595/19930857/>.
5. Аникин И.В. Управление внутренними рисками информационной безопасности корпоративных информационных сетей / И.В. Аникин // Научно-техническое ведомости Санкт-Петербургского государственного политехнического университета. Информатика. Телекоммуникации. Управление. — 2009. — Т. 3. №80. — С. 35–40.
6. Аникин И.В. Метод количественной оценки уровня ущерба от реализации угроз на корпоративную информационную сеть / И.В. Аникин // Информационные технологии. — 2010. — №1. — С. 2–6.
7. Остапенко Г.А. Риски распределенных систем: методики и алгоритмы оценки и управления / Г.А. Остапенко, Д.О. Карпеев, Д.Г. Плотников [и др.] // Информационная безопасность. — 2010. — №4. — С. 485–530.

ПРОЕКТИРОВАНИЕ И ПРОГНОЗИРОВАНИЕ В СОЦИАЛЬНО-ЭКОНОМИЧЕСКОЙ СФЕРЕ

ПРОБЛЕМЫ ПРИ СОЗДАНИИ НЕЙРОННОЙ СЕТИ ДЛЯ СЕНТИМЕНТ АНАЛИЗА

PROBLEMS IN CREATING A NEURAL NETWORK FOR SENTIMENT ANALYSIS

Зубарев Максим Олегович

Андроид-разработчик Gilraen Limited, Москва, Россия



Zubarev Maksim Olegovich

Android developer Gilraen Limited, Moscow, Russia

Конюхова Галина Павловна

Кандидат педагогических наук, доцент кафедры
«Управление и информатика в технических системах»
Московского государственного технологического
университета «СТАНКИН»



Konjuhova Galina Pavlovna

Candidate of Pedagogy, Associate Professor
of the Department of Management and Informatics
in Technical Systems, Moscow State Technological University
"STANKIN"

Аннотация. Подавляющее большинство работ по анализу настроений было посвящено разработке более точных классификаторов настроений, обычно включающих контролируемые алгоритмы машинного обучения и набор функций. В этой главе мы подробно остановимся на некоторых нерешенных проблемах, вопросах, которые еще недостаточно изучены, и новых проблемах, возникающих в результате решения новых проблем анализа настроений. Мы также обсуждаем предложения по решению этих проблем. Цель этой статьи состоит в том, чтобы снабдить исследователей и практиков указателями на последние достижения в области анализа настроений и стимулировать больше работы в разнообразной области проблем, особенно в тех областях, которые относительно менее изучены.

Ключевые слова: сентимент анализ, нейронная сеть, сверточные нейронные сети, обработка естественного языка.

Abstract. A vast majority of the work in Sentiment Analysis has been on developing more accurate sentiment classifiers, usually involving supervised machine learning algorithms and a battery of features. In this chapter, we flesh out some of the challenges that still remain, questions that have not been explored sufficiently, and new issues emerging from taking on new sentiment analysis problems. We also discuss proposals to deal with these challenges. The goal of this chapter is to equip researchers and practitioners with pointers to the latest developments in sentiment analysis and encourage more work in the diverse landscape of problems, especially those areas that are relatively less explored.

Keywords: sentiment analysis, neural networks, convolutional neural networks, natural language processing.

Анализ настроений является одним из наиболее успешных и распространенных приложений в обработке естественного языка. Однако, несмотря на всю шумиху, которую он вызвал с момента своего создания, с ним все еще связано много проблем.

Анализ настроений может быть очень простым и дешевым, так как для этого существует множество бесплатных библиотек. Вот некоторые примеры: Syuzhet (для R), NLTK (python), spacy (python). Однако анализ

настроений иногда может быть очень сложным и сложным, и именно об этом я хочу здесь поговорить.

В частности, анализ настроений страдает одним серьезным недостатком: он зависит от контекста и языка. В этой статье я говорю о некоторых потенциальных проблемах, которые могут возникнуть при попытке применить анализ настроений к некоторым контекстам.

Вопросы анализа настроений

Проблема 1: Слова имеют противоположное значение в вашем контексте. Быть «агрессивным» в большинстве ситуаций считается не очень приятной чертой характера. Однако быть агрессивным, когда ты нападающий в футболе, может быть очень хорошо. Контраст еще более заметен с такими словами, как «убийца». Нападающий в футболе, который является «убийцей» или обладает «инстинктом убийцы», вероятно, является хорошим спортсменом. Однако не многие люди подумают, что «убийца» в реальной жизни — это хорошо. В этом контексте механизмы анализа настроений общего назначения будут очень запутаны.

Проблема 2: Смайлики и их использование. Иногда люди могут быть очень креативными с использованием смайликов. Например, «□» может быть интерпретировано как отрицательное или положительное. Фактическое значение зависит от контекста. Если вы зайдете в emojiTracker, вы найдете огромное количество смайликов. Значение многих из них (например, рыбы) может быть сложным для изучения в модели машинного обучения. Это может быть очень важным вопросом для таких тем, как сарказм, который является следующей темой в нашем списке.

Проблема 3: Ирония и сарказм. В целом они относятся к числу святых граалей НЛП. Алгоритмы все еще пытаются понять сарказм и иронию. Это общеизвестно сложная проблема. В последнее время наблюдается некоторый прогресс в использовании глубоких нейронных сетей. В недавней статье был сделан вывод о том, что сарказм зависит от темы и контекста. Это означает, что алгоритм нуждается в дополнительной информации, чтобы правильно классифицировать сарказм.

Это делает его значительно более сложной проблемой, чем просто понимание того, передают ли некоторые слова положительное или отрицательное значение, и может потребовать предварительно подготовленных вложений слов и моделей личности. Решением, согласно этой статье, является использование сверточных нейронных сетей. Свертки — очень интересный метод в глубоком обучении. Если вас интересует эта тема, существуют статьи, которые хорошо объясняют, как их можно использовать в тексте.

Проблема 4: Реальные знания. Одним из наиболее сложных аспектов обработки естественного языка является понимание фактического контекста того, что говорится. В этой области проводится множество исследований. Сети памяти — это модель, которая может использовать контекстную информацию для ответа на вопросы. Сети внимания могут обрабатывать отдельные части предложения так же, как человек может обращать внимание на разные слова. Рекуррентные нейронные сети, такие как двунаправленные LSTM, могут использоваться для понимания более широкого контекста предложения. В последнее время исследования начали внедрять их в анализ настроений.

В этой статье, например, обсуждается использование сетей памяти в анализе настроений, а также в этой статье с вниманием обсуждается возможное использование двунаправленных LSTM. Оба варианта являются возможными решениями, но эти модели довольно сложны для среднего человека, плюс они требуют больших наборов данных.

Решение вопросов анализа настроений

Итак, что можно сделать для решения этих проблем? Есть несколько разных решений.

Вы можете попробовать обучить свою собственную модель для своей конкретной области, в идеале используя более продвинутый метод (например, глубокие нейронные сети). Это самое дорогое и трудоемкое решение. Однако, если у вас действительно есть ресурсы, чтобы осуществить это, вы можете обнаружить, что держите в своих руках очень ценную и уникальную интеллектуальную собственность.

Другое решение состоит в том, чтобы исследовать, насколько серьезна проблема в общей схеме вещей. Вполне вероятно, что проблема проявляется только в подмножестве данных. Возможно, вы сможете придумать несколько более сфокусированных моделей для этой части данных. Например, в приведенном выше примере, касающемся слова «агрессивный» в контексте спорта, возможное решение состоит в том, чтобы просто присвоить ему нейтральное значение. Таким образом, вы не рискуете сильно ошибиться в классификации. (например, позитивный пост помечается как негативный, или пост о ком-то, кто буквально агрессивен, помечается как позитивный). Наконец, еще одним решением является создание моделей машинного обучения для подмножеств данных.

Список литературы

1. Посевкин Р. Автоматизация sentiment-анализа естественно-языкового текста / Р. Посевкин. — LAP Lambert Academic Publishing, 2014.
2. Гудфеллоу Я. Глубокое обучение / Я. Гудфеллоу, И. Бенджио, А. Курвилль. — 2017.
3. Шолле Ф. Глубокое обучение на Python / Ф. Шолле. — 2018.
4. Жерон О. Прикладное машинное обучение с помощью Scikit-Learn и TensorFlow / О. Жерон. — 2018.
5. Саттон Р. Обучение с подкреплением / Р. Саттон, Э. Барто. — 2017.

IT-РЕШЕНИЯ В АВТОМАТИЗАЦИИ ПРОЦЕССА ПОДБОРА И УПРАВЛЕНИЯ КАДРАМИ

IT-SOLUTIONS IN THE AUTOMATION OF THE PROCESS OF SELECTION AND MANAGEMENT OF PERSONNEL

Таукенова Лязат Жумабаевна

*Доктор по профилю, университет «Туран-Астана»,
Нур-Султан, Казахстан*



Taukenova Ljazat Zhumabaevna

*Doctor in profile, University "Turan-Astana",
Nur-Sultan, Kazakhstan*

Каиржанова Айгерим Куатжановна

*И.о. руководителя управления проектирования
и разработки, РГП на ПХВ «Инженерно-технический
центр» Управления Делами Президента РК,
Нур-Султан, Казахстан*



Kairzhanova Ajgerim Kuatzhanovna

*Acting Head of the Design and Development Department,
RGP on REM "Engineering and Technical Center"
of the Administrative Department of the President
of the Republic of Kazakhstan, Nur-Sultan, Kazakhstan*

Жумабаев Ержан Ныгметжанович

*Специалист по сопровождению и эксплуатации ИС,
«Академия Имиджелогии», Нур-Султан, Казахстан*



Zhumabaev Erzhan Nygmetzhanovich

*IS Maintenance and Operation Specialist, "Academy
of Imageology", Nur-Sultan, Kazakhstan*

Аннотация: в данной статье будет рассматриваться правильное планирование и организация процесса подбора персонала, повышение его эффективности, выгодные решения автоматизации процесса поиска и привлечения кадров, современные технологии, программы, системы подбора персонала, которые помогут осуществить автоматизацию, выгода и преимущества автоматизации данного процесса в различных организациях и кадровой службе.

Ключевые слова: управление персоналом, процесс найма, HR-сервис, автоматизация HR, автоматизированная система управления кадрами

Abstract: this article will consider the correct planning and organization of the recruitment process, increasing its efficiency, profitable solutions to automate the process of recruiting and attracting personnel, modern technologies, programs, recruitment systems that will help to carry out automation, the benefits and advantages of automating this process in various organizations and personnel service.

Keywords: personnel management, recruitment process, HR service, HR automation, automated personnel management system

Сегодня на рынке информационных технологий (ИТ) представлено много компаний-разработчиков, предлагающих услуги по внедрению систем и программ управления персоналом. Но большинство из них помогает автоматизировать лишь часть описанных бизнес-процессов. Для качественного подбора кадров требуется системность и комплексность. Для реализации всех упомянутых задач нужна комплексная автоматизация работы с персоналом, комплексное автоматизированное решение, полноценная многофункциональная HRM-система.

Основные этапы подбора сотрудников на предприятии. Поиск и набор кадров — это первый и один из наиболее важных этапов в общем цикле движения персонала на предприятии (рис. 1).

В свою очередь, процесс подбора кадров делится на следующие основные этапы:

Планирование:

- Подготовка и согласование требований к кандидатам.
- Определение каналов поиска и привлечения соискателей.

- Определение критериев отбора.
Реализация:
- Самостоятельное размещение информации о вакансиях (рекламная активность).
- Привлечение кадровых агентств и компаний по подбору персонала.
- Прием и проработка обращений соискателей.
- Учет кандидатов, резюме и другой информации.
- Непосредственный подбор и оценка персонала, тестирование, собеседования.
- Заключение трудового договора [1].



Рис. 1. Цикл движения персонала на предприятии

Классификация подбора квалифицированных кадров, включают следующие основные разновидности. Существует точечный, индивидуальный, а бывает массовый подбор, когда нужно найти, подобрать и нанять большое количество сотрудников одновременно. Есть внешний (реализуемый благодаря кадровым агентствам, рекрутинговым компаниям), а есть внутренний подбор (осуществляется внутри фирмы с помощью отдела кадров, службы по работе с персоналом, HR-менеджеров). Встречается экспресс-подбор, который производится в сжатые сроки. Отметим и удаленный или дистанционный отбор (используются современные информационные технологии, различные каналы связи, интернет; при этом личной встречи с кандидатом не происходит). Кроме того, в зависимости от должности и специализации сотрудников, которые требуются предприятию, встречается (и имеет свою специфику): подбор руководящих, административных кадров и отбор персонала среднего звена; подбор строительного, банковского, медицинского и прочего персонала; рабочего, торгового, производственного, технического, обслуживающего, а также временного и постоянного, иностранного и казахстанского, элитного и обычного персонала. К основным проблемам, с которыми сталкиваются HR-службы в процессе подбора работников это:

- Сложности с массовым отбором кадров. Все чаще речь идет не о точечном, индивидуальном отборе, а о массовом рекрутинге, когда нужно за короткий срок подобрать множество кандидатов одновременно. И сделать это не только быстро, но и максимально эффективно (да еще и с минимальными затратами). Представьте, сколько трудностей необходимо преодолеть, чтобы реализовать такой большой проект. Речь об управлении огромным

объемом информации, множеством ресурсов и каналов. Не каждой компании, кадровой службе по плечу такая задача. И не каждая система, программное обеспечение по подбору персонала справится с этим. Зачастую у кадровиков просто нет необходимого инструментария, опыта и знаний для осуществления подобного рода проектов.

- Неэффективный внешний подбор кадров. В наше время большим спросом пользуются услуги рекрутинговых агентств и агентов. Использование такого метода поиска и подбора кандидатов значительно экономит время кадровиков компании. Но что вы получаете в результате? Зачастую специалисты компаний по подбору персонала не могут правильно понять кадровые потребности и грамотно оценить кандидата. Если сроки поджимают, а соискателей все нет и нет, рекрутинговые фирмы «упрощают», снижают требования к кандидатам, начинают подбирать некачественные кадры, лишь бы выполнить свои обязательства перед клиентом и уложиться в срок. Но нужны ли Вам такие «работники»? Агентства по подбору кадров дают гарантии на сотрудников, но всегда ли эта гарантия уместна? Вам никто не вернет деньги (а стоимость подобных услуг по подбору персонала достаточно высокая).

- Неэффективный внутренний подбор кадров. Бывают ситуации, когда сами клиенты рекрутинговых агентств не всегда могут правильно сформулировать свои требования, но ждут, что их заказ будет выполнен на высшем уровне. Естественно, такого не произойдет. Для правильного подбора персонала должно быть четкое понимание внутри самой фирмы: кто, когда, зачем и на каких условиях нужен. В кадровой службе, отделе по персоналу компании должны быть собственные сильные HR-менеджеры, которые должны хорошо знать специфику, внутреннюю «кухню» фирмы, слабые и сильные места коллектива. Они должны уметь вести правильную информационную и учетную политику, грамотно оценивать сотрудников, понимать специфику поиска и привлечения кандидатов, владеть современными HRM-технологиями. Все это дает возможность эффективно подбирать персонал, не прибегая к помощи специализированных агентств.

При реализации проекта по поиску и привлечению (набору) персонала возникает масса других проблем и вопросов: какие каналы поиска задействовать; обращаться ли в компании, подбирающие кадры; какую рекламную стратегию выбрать; сколько менеджеров по персоналу подключить; сколько времени этому уделить; как правильно рассчитать бюджет и другие ресурсы. А еще: какую базу для учета кандидатов и резюме использовать; где хранить и как обрабатывать огромный объем информации; как не потерять ни одно резюме и не упустить ни одного соискателя; как оценить эффективность подбора персонала. Наконец, как подобрать нужного специалиста — того, кто будет максимально

эффективен в работе, какие методики и технологии использовать, из каких критериев исходить.

Эффективно решить упомянутые проблемы и задачи можно с помощью автоматизации процессов поиска, привлечения, подбора и учета кадров (а также других бизнес-процессов, связанных с кадровой работой: оценкой, адаптацией, обучением персонала и т.д.).

Внедрение автоматизированного решения (системы, программы) позволит усовершенствовать (сделать проще, легче, быстрее и удобнее) работу с подбором кандидатов, с ведением базы вакансий, соискателей и резюме, поможет повысить управляемость и результативность всей работы с персоналом.

Выгоды и преимущества автоматизации подбора сотрудников:

- Сокращение трудозатрат, связанных с планированием и реализацией подбора кадров.
- Минимизация бюджета (расходов, затрат) на подбор кадров.
- Убыстрение поиска и привлечения кандидатов.
- Постоянный рост базы.
- Грамотный учет, исключение потери данных.
- Качественная, полноценная проработка всех обращений, каждого резюме.
- Рост конверсии потенциальных кандидатов, соискателей в трудоустроившихся сотрудников, работников.
- Увеличение эффективности рекламных и PR мероприятий, направленных на поиск и привлечение кандидатов.
- Общая оптимизация управления HR-направлением компании (отделом по работе с персоналом, кадровой службой, отделом кадров) [2].

Все компании разные. Именно поэтому создаются универсальные системы поиска и подбора персонала, способные подстраиваться под специфику любого бизнеса. Почти во всех разработках предусмотрены гибкие настройки, которые позволяют добавлять дополнительные поля, этапы интервью, различные виды отчетов и так далее.

Необходимо заметить, что автоматизированная система рекрутинга обеспечивает только один из важнейших HR-процессов. Наибольшая выгода достигается в том случае, когда компания использует комплексный подход: планирование персонала, учет компетенций, оценка кадрового резерва. Тем не менее, все виды специализированного программного обеспечения для рекрутмента, доступные сегодня на рынке, многократно упрощают рутинные операции и экономят драгоценное время.

Процесс поиска, подбора и найма сотрудников становится удобным и по-настоящему эффективным: все его участники совершают минимум действий, но при этом выделяется только самая важная и объективная информация. Наиболее автоматизированные HR-процессы показаны на рис. 2.

Следовательно, автоматизация жизненно необходима не только рекрутинговым агентствам, но и остальным компаниям, которые стремятся к созданию

сильных команд. Это возможность наработать собственную базу кандидатов — то есть фактически создать кадровый резерв и сократить не только расход времени, но и прямые затраты на подбор нового персонала.

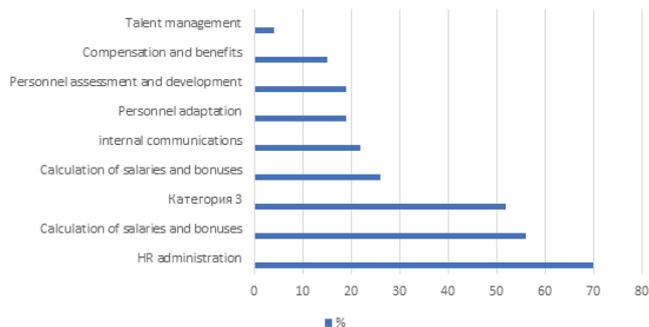


Рис. 2. Автоматизированные HR-процессы

Список ожиданий, которые оправдывает автоматизированная система рекрутинга:

- для каждой вакансии задаются чёткие параметры;
- для работы со всеми соискателями используются шаблоны (рассылка писем, предварительное анкетирование);
- анкеты с разных ресурсов хранятся в одном месте;
- формируется единая база кандидатов, с возможностью удобного добавления и перевода по статусам;
- предусмотрен быстрый поиск по заданным критериям и гибкая система фильтров;
- все важные пометки можно делать во время собеседования — непосредственно в профиле соискателя, который создается в системе;
- сохраняется вся история взаимодействия с кандидатами;
- каждый этап можно обсудить с коллегами;
- с любых устройств есть неограниченный доступ для всей HR-команды и нанимающих менеджеров ко всем данным системы;
- возможен массовый или региональный подбор персонала;
- вакансии размещаются на всех рабочих порталах (как бесплатных, так и платных) [3].

Речь о программном HRM-комплексе, который поможет formalизовать и отладить в единой информационной среде все бизнес-процессы, связанные с управлением кадрами, в том числе — с подбором. В состав решения должна входить настройка основных процессов структур, ответственных за работу с персоналом, выбор и внедрение подходящей информационной программы, услуги консультантов (консалтинг), комплексное сопровождение и техническая поддержка.

Особенности и преимущества автоматизированных HRM-систем:

- **Гибкость.** Описываемые решения могут легко и просто адаптироваться под любого пользователя, любую специализацию, любой масштаб предпринимательства (будь то предприятия малого, среднего или крупного бизнеса).

- **Интеграция с 1С.** Большинство HRM-комплексов, представленных на казахстанском рынке информационных технологий, разрабатываются и внедряются на платформе 1С:Предприятие (самой известной и популярной в нашей стране учетной системы). Поэтому данные системы легко интегрируются с такими конфигурациями 1С: например, с 1С:Зарплата и управление персоналом (ЗУП), 1С:Кадровое агентство, 1С:Оценка персонала, 1С:Комплексная автоматизация (КА), 1С:Управление производственным предприятием (УПП) и с любой версией платформы 1С (7.7, 8, 8.2 и 8.3). С 1С подбор персонала становится более качественным и результативным.
- **Быстрый поиск кандидатов на ту или иную должность.** Автоматизированная система для подбора персонала позволяет в считанные секунды получать перечень всех возможных кандидатов из сети интернет, которые соответствуют требованиям бизнеса. Не нужно заходить на каждый сайт отдельно и тратить время на настраивание критериев для поиска.
- **Исключение ручного ввода данных.** Информация о кандидатах, которых вы просматриваете, автоматически загружается в базу 1С. Вам не нужно вручную вводить имена, фамилии, телефоны и прочую информацию. Все поля автоматически распознаются, и на основе этой информации формируются карточки кандидатов и соискателей в базе 1С.
- **Мгновенное размещение вакансий.** Использование автоматизированных систем по поиску и отбору персонала дает возможность в считанные секунды размещать интересующие вакансии и получать на них отклики. Вы также можете загружать подобранные резюме кандидатов, расширяя при этом свою базу.
- **Возможность удаленного, дистанционного подбора.** Благодаря новому сервису для поиска, подбора и оценки персонала «EFSOL: HRM.Мой персонал», который разработан специалистами компании EFSOL, Вам не нужно тратить время на анкетирование и оценку кандидатов. Все это может проводиться удаленно (через интернет), за счет прохождения соискателями специальных онлайн-тестов. Вы получаете готовый результат с полной аналитической характеристикой подбранного кандидата (психологическое состояние, анализ компетенций, навыков, соответствия требуемой должности и многое другое). Такой сервис делает подбор персонала более быстрым, простым и удобным.
- **Новейшие методики и технологии отбора, реализованные в данной автоматической системе.** Вы получаете мощный функциональный инструмент, который способен быстро и эффективно подобрать Вам нужные кадры [5]. Автоматизация проходит в несколько этапов:
- Выбор необходимого программного обеспечения.

- Анализ, аудит подбора персонала; выявление проблем, ошибок, тонких мест.
- Разработка и согласование технического задания (ТЗ).
- Внедрение (установка) и запуск системы подбора персонала.
- Настройка и тестирование, при необходимости — доработка, корректировка.
- Консультации пользователей, обучение работе с системой.
- Абонентское сопровождение программы по подбору персонала, техническая поддержка [5].



Рис. 3. Функционал блока «Подбор кадров» в рамках системы управления персоналом

В зависимости от поставленных задач компания-разработчик закрепляет ведущего специалиста, который курирует взаимодействие с проектной командой (консультантами и программистами).

При создании автоматизированной системы важно провести анализ существующих программ и приложений применяемых в процессе подбора кадров. Все доступные на отечественном рынке программы для оптимизации рекрутмента можно разделить на две группы: онлайн-приложения и готовые прикладные решения «в коробках», которые устанавливаются на рабочие компьютеры. Среди них также выделяют профессиональные сервисы для кадровых агентств и более простые системы для остальных компаний.

Конечно, свои достоинства и недостатки есть у каждого софта. Специфика отдельных организаций требует создания проектов «под ключ»: к примеру, в готовых отечественных разработках не хватает некоторых важных функций, а в зарубежных продуктах не предусмотрена двуязычность.

Но в целом подбор оптимальной системы автоматизации сводится к трем ключевым вопросам: 1) какие у неё возможности; 2) что это даёт нашей компании; 3) сколько это стоит?

Подводя итог, приведем все, необходимые сервисы, которые должна содержать в себе современная автоматизированная система:

- Выполнять все рутинные операции: импортировать резюме любых форматов в единую базу, сортировать кандидатов по нужным параметрам, исключая повторные анкеты.
- Обеспечивать хранение большого массива данных с возможностью выбрать способ (облачное или на серверах компании).
- В считанные секунды находить нужных кандидатов по заданным параметрам.
- Координировать взаимные действия HR-команды, линейных менеджеров, и руководства.

- Собирать статистику: по источникам, по количеству кандидатов, по времени, по затратам — то есть анализировать воронку рекрутинга на каждом этапе и считать конверсию.
- Подстраиваться под конкретные запросы компании и уже действующие бизнес-процессы.

Кроме того, обязательно надо выяснить, возможна ли доработка сервиса под некоторые специфические задачи (самостоятельная или провайдером), интеграция с другими решениями, и гарантированная техническая поддержка.

И наконец, стоимость ПО должна быть настолько адекватной, чтобы сокращать затраты на поиск и подбор персонала, при этом многократно увеличивая его итоговую эффективность.

Как уже говорилось, задача-минимум любой рекрутинговой программы — упростить работу менеджеров и ускорить процесс найма сотрудников, задача-максимум — усовершенствовать HR-стратегию компании. Качественный сервис позволяет наглядно оценивать каждый этап отбора, формировать четкие ожидания от кандидатов и в результате привлекать лучших специалистов — квалифицированных и мотивированных на достижение целей компании. Осталось самое главное — продумать потребности бизнеса, подобрать программный продукт и начать пользоваться преимуществами автоматизации.

Осталось самое главное — продумать потребности бизнеса, подобрать программный продукт и начать пользоваться преимуществами автоматизации.

Список литературы

1. Автоматизация в HR: реальная ситуация и основные барьеры [Электрон. ресурс]. — Режим доступа: <https://topfactor.pro/blog/avtomatizatsiya-v-hr-realnaya-situatsiya-i-osnovnye-barery/>
2. Сиротенко В. Автоматизация рекрутинга. Практическое пособие по выбору, внедрению и применению ATS-систем / В. Сиротенко. — М., 2021.
3. Зинченко А.А. Моделирование процессов подбора и оценки персонала / А.А. Зинченко. — М., 2021.
4. HR System Express — система для автоматизации процесса подбора персонала [Электрон. ресурс]. — Режим доступа: <http://visol.ru/HRSystemExpress.aspx>.
5. HR-digital сегодня и завтра: решения по автоматизации управления персоналом [Электрон. ресурс]. — Режим доступа: <https://www.64159-hr-digital-segodnia-i-zavtra-populiarnye-resheniia-po-avtomatizatsii-upravleniia-personalom.pdf>.

РАЗРАБОТКА ВЕБ-СЕРВИСА ПО АНАЛИЗУ ОШИБОК В ПОИСКОВОЙ ОПТИМИЗАЦИИ

DEVELOPMENT OF A WEB SERVICE FOR ANALYZING ERRORS IN SEARCH ENGINE OPTIMIZATION

**Федотов
Никита Олегович**

Разработчик, Московский государственный технологический университет «Станкин»



**Fedotov
Nikita Olegovich**

Developer, Moscow State Technological University "Stankin"

Аннотация. В данной статье подробно рассматривается разработка веб-сервиса по анализу ошибок в поисковой оптимизации. Будет дано краткое описание технологий, которые необходимо использовать для разработки веб-сервиса.

Ключевые слова: Веб-сервис по анализу ошибок, поисковая оптимизация, SEO, разработка веб-сервиса.

Abstract. This article discusses in detail the development of a web service for analyzing errors in search engine optimization. A brief description of the technologies that need to be used to develop a web service will be given.

Keywords: Error analysis web service, search engine optimization, SEO, web service development.

Введение

Разработка веб-сервиса начинается с определения области и факторов, которые необходимо учитывать при проверке анализа. Необходимо выбрать и язык программирования, базу данных, а также библиотеки, которые необходимы для реализации данного проекта. Выбор данных технологий происходит при помощи сравнения и обоснования выбранных технологий.

Перед тем как начать разработку веб-сервиса необходимо произвести обзор параметров учитываемых

поисковыми система. В последствии при разработке сервиса учитывать данные параметры, а также реализовать новый алгоритм, который будет моделировать пользовательский фактор. [1]

Параметры используемые для контента страниц:

- Корректно настроенные мета-теги;
- корректные заголовки на странице;
- наличие ссылок на профиль в соц. сетях;
- параметры используемых изображений;

Параметры настройки серверной информации:

- наличие файлов и корректность их заполнения Robots.txt, Sitemap.xml;
- наличие счетчиков аналитики от Yandex и Google. Параметры ссылочной массы:
- Проверка на «битые ссылки»: подразумевается что необходимо проверять ссылки по которым контент сайта больше недействителен.

Важно отметить и пользовательские параметры, но здесь существует проблема в конфиденциальности этих данных, а именно о количестве отказов, времени, проведенном на сайте, которые играют значительную роль для поисковых роботов. [2]

Выбор языка программирования

Для решения данной задачи подходят два языка программирования это PHP и Python. Php является интерпретируемым языком с динамической типизацией, что в свою очередь позволяет ускорить написания кода, поскольку нигде явно не нужно указывать тип данных. В свою очередь интерпретатор подставляет тип данных автоматически но на данном языке программирования при большом количестве написанного кода выполнение написанного кода замедляется.

Python является также интерпретируемым языком программирования с динамической типизацией. Но в отличии от вышеописанного языка программирования PHP работает сравнительно быстрее за счет того, что скорость работы данного языка зависит от скорости работы компьютера. Чтобы не вызвать переполнения памяти в Python имеется специальная утилита, которая удаляет из памяти неиспользуемые переменные что позволяет избежать снижения скорости обработки данных.

В данное время оба языка активно используются в веб-разработке. Но поскольку Python имеет большое количество библиотек что позволяет ускорить разработку на данный момент он вытесняет язык PHP. Востребованность языков во временном промежутке указана на рис. 1.

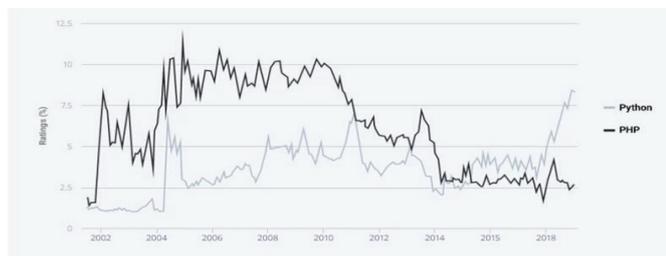


Рис. 1. Сравнение языков программирования

Для разработки необходимо выбрать Python поскольку данный язык программирования, дает доступ к различным библиотекам что помогает ускорить написания кода. Также данный язык разработки используется для создания искусственного интеллекта и нейронных сетей. Что в свою очередь необходимо для моделирования пользовательских факторов.

Для разработки пользовательского интерфейса был выбран фреймворк Django. При помощи которого будут соединяться и другие библиотеки.

Для разработки алгоритма получения данных с веб-сайтов в Python имеется две основные библиотеки: BeautifulSoup, Scrapy. BeautifulSoup предоставляет возможность получать данные с веб-страниц. Основным плюсом данной библиотеки является: простота настройки, удобная встраиваемость в проект. Недостатками данной библиотеки является то что для получения данных со всего сайта необходимо написать большое количество кода. Это в последствии не позволит масштабировать проект, и усложнит его поддержку. Scrapy также предоставляет возможность получать любые данные с веб-сайтов. Основным плюсом является написания качественного читабельного кода, возможность получать динамические данные с веб-сайта. Недостатком данной библиотеки является сложная настройка. Для создания алгоритма получения данных следует выбирать библиотеку Scrapy. Не смотря на сложную настройку она предоставляет большое количество возможностей.

Разработка веб-сервиса

Разработка веб-сервиса начинается с развертывания Django. После чего необходимо внутри корневого каталога проекта развернуть Scrapy. Далее необходимо сообщить Django, что библиотека Scrapy должна иметь доступ к базе данных для записи результатов анализа. После этого необходимо создать базу данных. Для создания выявляются те факторы, необходимые для анализа сайтов, описываются параметры, используемые поисковыми системами в виде полей и таблиц. Файл внутри каталога Scrapy и описать в нем те данные, необходимые для получения. После чего их необходимо записать в базу данных. Разработать алгоритм по модерированию пользовательского понимания сайта. Передать в него значение, которое было получено в результате анализа веб-сайта. Произвести вывод из базы данных и отобразить его в шаблоне, а также вывести результат работы алгоритма по модерированию пользовательского понимания сайта.

Заключение

Из всего вышеперечисленного можно сделать следующий вывод что для разработки веб-сервиса по анализу ошибок в поисковой оптимизации следует выбирать язык программирования Python, а также все вышеперечисленные библиотеки для быстрой и корректной работы веб-сервиса.

Список литературы

1. Горбунов А. Продвижение сайта без вложений: полное руководство для непрофессионалов / А. Горбунов. — М.: Издательские решения, 2018.
2. Северюхин О. Я создаю свой собственный персональный сайт / О. Северюхин. — М.: Издательские решения, 2016.
3. Головатый А. Django. Подробное руководство / А. Головатый, Дж. Каплан-Мосс. — М.: Символ плюс, 2010.
4. Dimitris Kouzis — Loukas, Learn Scrapy, Packt Publishing, 2016.

УРАВНЕНИЯ ЭЛЕКТРОМЕХАНИЧЕСКИХ ПЕРЕХОДНЫХ ПРОЦЕССОВ В СИНХРОННОМ ЭЛЕКТРОПРИВОДЕ НАСОСНОГО АГРЕГАТА

EQUATIONS OF ELECTROMECHANICAL TRANSITION PROCESSES IN A SYNCHRONOUS ELECTRIC DRIVE OF A PUMP UNIT

Нуспеков Ерболат Лязатович

Кандидат технических наук, университет «Туран-Астана», Нур-Султан, Казахстан



Nuspekov Erbolat Ljizatovich

Candidate of Technical Sciences, University "Turan-Astana", Nur-Sultan, Kazakhstan

Таукенова Лязат Жумабаевна

Доктор по профилю, университет «Туран-Астана», Нур-Султан, Казахстан



Taukenova Ljizat Zhumabaevna

Doctor in profile, University "Turan-Astana", Nur-Sultan, Kazakhstan

Жумабаев Ержан Ныгметжанович

Специалист по сопровождению и эксплуатации ИС, «Академия Имиджологии», Нур-Султан, Казахстан



Zhumabaev Erzhan Nygmetzhanovich

IS Maintenance and Operation Specialist, "Academy of Imageology", Nur-Sultan, Kazakhstan

Аннотация: в статье предложена математическая модель расчета переходных процессов для детального учета жидкости трубопровода в аномальных режимах системы электроснабжения. Методика расчета позволяет достаточно точно отражать момент сопротивления насосного агрегата в аномальных режимах системы электроснабжения.

Ключевые слова: ротор, двигатель, мощность, электрическая сеть, дифференциальные уравнения, трубопровод.

Abstract: The article proposes a mathematical model for calculating transients for detailed accounting of pipeline fluid in abnormal modes of the power supply system. The calculation method allows to accurately reflect the moment of resistance of the pumping unit in abnormal conditions of the power supply system.

Keywords: rotor, engine, power, electrical network, differential equations, pipeline.

Уравнения электромеханических переходных процессов отражают закон движения ротора двигателя под воздействием электромагнитного момента и момента сопротивления механизма.

Для нахождения положения ротора обычно используют синхронно вращающуюся систему координат. Относительное положение ротора в такой системе координат определяется углом δ между его поперечной осью и синхронно вращающейся осью, в качестве которой можно принять вектор напряжения питающей электрической сети [4]. В этом случае урав-

нение электромеханических переходных процессов в соответствии со вторым законом Ньютона представляются в виде [1]:

$$T_j \frac{d^2 \delta}{dt^2} = M_{\text{мех}} - M_{\text{э}} \quad (1)$$

где T_j — электромеханическая постоянная времени агрегата двигатель-механизм;

$M_{\text{мех}} - M_{\text{э}}$ — момент сопротивления механизма и электромагнитный момент.

Момент сопротивления различных механизмов [2, 3], приведенный к номинальной мощности, характеризуется обобщенной зависимостью:

$$M_{\text{мех}} = [M_0 + (k_3 - M_0) \omega^\gamma] \frac{P_{\text{ном}}}{S_{\text{ном}}} \quad (2)$$

Здесь M_0 — начальный момент (при $s = 1$ или $\omega = 0$); k_3 — коэффициент загрузки двигателя в синхронном режиме ($s = 0$); γ — показатель степени, характеризующий зависимость момента сопротивления механизма от частоты вращения.

При правильном выборе M_0 , k_3 и γ выражение (2) достаточно точно отражает моменты сопротивления типовых механизмов.

Электромагнитный момент, развиваемый синхронным двигателем (СД), определяется соотношением [2].

$$M_\vartheta = P / \omega_U \quad (3)$$

где P — активная мощность, потребляемая двигателем; ω_U — частота напряжения на статорной обмотке.

При питании двигателя от электрической сети $\omega_U = \omega_0$ и в относительных единицах $M_\vartheta = P$ (4).

Активную и реактивную мощности, потребляемые СД в переходных процессах, целесообразно выразить через составляющие E''_q и E''_d сверхпереходной ЭДС. Используя соотношения [4], получаем

$$P = \frac{E''_q U}{x'_d} \sin \delta - \frac{E''_d U}{x'_q} \cos \delta + \frac{U^2}{2} \left(\frac{1}{x'_q} - \frac{1}{x'_d} \right) \sin 2\delta \quad (5)$$

$$Q = \frac{E''_q U}{x'_d} \cos \delta - \frac{E''_d U}{x'_q} \sin \delta + \frac{U^2}{2} \left(\frac{\cos^2 \delta}{x'_q} + \frac{\sin^2 \delta}{x'_d} \right) \quad (6)$$

В качестве начальных условий для уравнений электромеханических переходных процессов (1) следует задать значение угла δ и его производной $d\delta / dt$ для момента времени $t = 0$. Поскольку параметры режима δ и $d\delta / dt = 2\pi f_0 s$ обладают свойством сохранять неизменным свое значение в первый момент времени при любых изменениях режима, то начальные условия можно вычислить из предшествующего режима.

Режим СД, подключенного к электрической сети с напряжением U , при напряжении на обмотке возбуждения U_f определяют следующие основные параметры: δ — угол, характеризующий положение ротора относительно синхронно вращающейся оси (вектора напряжения U электрической сети); s — скольжение ротора двигателя (или $\omega = 1 - s$ — частота вращения ротора); E''_d , E''_q — составляющие сверхпереходной ЭДС двигателя по осям d и q ; $E'_T = dE''_q / dt$ — производная от ЭДС E''_q . Эти параметры режима СД назовем основными. Через них относительно легко выражаются остальные параметры: P , Q — активная и реактивная мощности, потребляемые двигателем из сети; I — ток в статорной обмотке; I_p , I_{Id} , I_{Iq} — токи в обмотке возбуждения и демпферных обмотках по осям d и q ; E_q , E_d — составляющие синхронной ЭДС двигателя.

Основные параметры режима определяются следующей системой дифференциальных уравнений переходных процессов в СД:

$$\frac{d\delta}{dt} = 2\pi f_0 s \quad (7)$$

$$T_j \frac{ds}{dt} = M_{\text{мех}} - M_\vartheta \quad (8)$$

$$E'_T = \frac{dE''_q}{dt} \quad (9)$$

$$T'_d T''_d \frac{dE'_T}{dt} + (T'_d + T''_d) E'_T = -E'_q + (T'_d + T''_d) \frac{x'_d - x''_d}{dt} dU_q + U_q \frac{x'_d - x''_d}{x'_d} + \frac{x''_d}{x'_d} E_{q\text{ном}} \left(U_f + T_{\sigma 3d} \frac{dU_f}{dt} \right) \quad (10)$$

$$\frac{d\delta}{dt} = 2\pi f_0 s \quad (11)$$

которую необходимо дополнять соотношениями, выражающими через основные параметры режима момент сопротивления механизма (2) и электромагнитный момент (3), (4).

Начальными условиями системы дифференциальных уравнений (7)–(11) являются следующие:

$$\delta(0) = \delta(-0), \quad (12)$$

$$s(0) = s(-0), \quad (13)$$

$$E''_q(0) = E'_q(-0), \quad (14)$$

$$E'_T(0) = E'_T(-0) + \frac{T'_d + T''_d}{T'_d T''_d} \frac{x'_d + x''_d}{x'_d} \Delta U_q + \frac{x''_d}{x'_d} \frac{T_{\sigma 3d}}{T'_d T''_d} E_{q\text{ном}} \Delta U_f \quad (15)$$

$$E''_d(0) = E'_d(-0), \quad (16)$$

Здесь индексом (-0) отмечены параметры предшествующего режима СД. Если СД подключен к электрической сети конечной мощности, то напряжение на статорной обмотке U зависит от режима двигателя. Для определения напряжения в этом случае необходимо решить уравнение напряжения электрической сети. Пусть СД вместе с прочей нагрузкой подключен к шинам, удаленным от источника ЭДС с неизменной величиной E_c , за сопротивление $Z_c = R_c + jx_c$ (рис. 1). Активная и реактивная мощности прочей нагрузки учитывая по статическим характеристикам в зависимости от напряжения

$$\left. \begin{aligned} P_H &= P_0 U^{\gamma_1} \\ Q_H &= Q_0 U^{\gamma_2} \end{aligned} \right\} \quad (17)$$

где P_0 и Q_0 — активная и реактивная мощности прочей нагрузки при номинальном напряжении; γ_1 и γ_2 — показатели степени, характеризующие зависимость мощности прочей нагрузки от напряжения.

Суммарная мощность, потребляемая из электрической сети СД и прочей нагрузки, составит

$$\left. \begin{aligned} P_\Sigma &= P + P_0 U^{\gamma_1} \\ Q_\Sigma &= Q + Q_0 U^{\gamma_2} \end{aligned} \right\} \quad (18)$$

В соответствии с расчетной схемой (рис. 1) напряжение в электрической сети можно выразить нелинейным алгебраическим уравнением

$$U = -\frac{P_{\Sigma}R_c + Q_{\Sigma}X_c}{U} + \sqrt{E_c^2 - \left(\frac{P_{\Sigma}x_c + Q_{\Sigma}R_c}{U}\right)^2} \quad (19)$$

которое необходимо решать совместно с уравнениями мощности (5), (6) и (8). Для этого воспользуемся методом Гаусса — Зейделя, который применительно к выражению (19) обладает хорошей сходимостью. Решение с точностью $\varepsilon = 0,0001$ достигается за 5–10 шагов последовательных приближений.

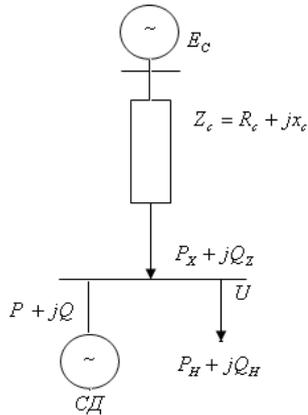


Рис. 1. Расчетная схема подключения СД

Напряжение на обмотке возбуждения СД, определяется типом возбудителя. Основные типы возбудительных устройств, применяемые СД, и соответствующие им законы изменения напряжения U_f , выраженные через основные параметры режима СД, подробно описаны в работе [4].

Система дифференциальных уравнений (7)–(11) при заданных начальных условиях (12)–(14) совместно с выражением (19) и уравнением напряжения на обмотке возбуждения U_f полностью определяет режим СД в переходных процессах.

Для детального учета переходных процессов жидкости трубопровода в аномальных режимах системы электроснабжения действительная величина γ , характеризующая зависимость момента сопротивления насоса от частоты вращения уточняется решением квазилинейных дифференциальных уравнений в частных производных гиперболического типа, описывающих нестационарное движение жидкости в трубопроводе. Правильный расчет γ в выражении (2) достаточно точно отражает момент сопротивления насосного агрегата в аномальных режимах системы электроснабжения.

Список литературы

1. Вишнеvский К.П. Переходные процессы в напорных системах водоподачи / К.П. Вишнеvский. — М.: Агропромиздат, 1986. — 135 с.
2. Спромятников И.А. Режимы работы асинхронных и синхронных электродвигателей / И.А. Спромятников. — М.: Госэнергоиздат, 1963. — 528 с.
3. Голоднов Ю.М. Самозапуск электродвигателей / Ю.М. Голоднов. — М.: Энергоатомиздат, 1985. — 136 с.
4. Гамазин С.И. Переходные процессы в системах электроснабжения с электродвигательной нагрузкой / С.И. Гамазин, Т.А. Садыбеков. — Алма-Ата: Гылым, 1991 — 302 с.

ПРОЕКТНАЯ ДЕЯТЕЛЬНОСТЬ В ОБЛАСТИ КУЛЬТУРЫ, СПОРТА И ТУРИЗМА

ИСПОЛЬЗОВАНИЕ РАЗНЫХ КАНАЛОВ КОММУНИКАЦИИ ДЛЯ ПРОДВИЖЕНИЯ ИМИДЖА РЕГИОНА НА ПРИМЕРЕ МУРМАНСКОЙ ОБЛАСТИ

USING DIFFERENT COMMUNICATION CHANNELS TO PROMOTE THE IMAGE OF THE REGION ON THE EXAMPLE OF THE MURMANSK REGION

**Косарева
Наталья Викторовна**

Кандидат географических наук, доцент кафедры геологии и геохимии ландшафта, заместитель декана по научно-исследовательской работе студентов географического факультета Московского педагогического государственного университета



**Kosareva
Natalija Viktorovna**

Candidate of Sciences in Geography, Associate Professor of the Department of Geology and Geochemistry of Landscape, Deputy Dean for Research Work of Students of the Geography Faculty of Moscow State Pedagogical University

Аннотация. В статье рассматриваются вопросы возможных каналов коммуникации с разными целевыми аудиториями туристов с целью продвижения имиджа Мурманской области.

Ключевые слова: имидж региона, Мурманская область, потенциальные туристы, целевая аудитория.

Abstract. The article deals with possible channels of communication with different target audiences of tourists in order to promote the image of the Murmansk region.

Keywords: image of the region, Murmansk region, potential tourists, target audience.

Важным моментом в процессе разработки бренда и брендинга территории становится дальнейший маркетинг имиджа. В нашей работе нам хотелось бы рассмотреть возможные каналы продвижения туристского имиджа Мурманской области на рынке внутреннего и въездного туризма с позиций разных целевых аудиторий: профессионалов турбизнеса, потенциальных туристов и метных жителей [1, 4].

Во-первых, самый простой способ продвижения бренда региона — это создание и дальнейшее продвижение регионального туристского продукта. Турпродукт Мурманской области с точки зрения реализации, будет интересен, прежде всего туристским компаниям Москвы, Санкт-Петербурга и Республики Карелии.

1. С этой целью можно рекомендовать администрации области использовать виртуальные возможности туристско-информационного центра Мурманской области. С его помощью столичные туроператоры могли бы осуществлять специальную рассылку о новых туристских программах, событиях и объектах в регион; о новых средствах размещения или новых услугах региональных средств размещения; о реконструкции/открытии новых подъездных путей к объектам туристского интереса; об изменении в авиарейсах; об акциях и специальных предложениях ре-

гиональных туроператоров. В рассылке будут уместны рекламные фотографии и видеоролики, отзывы туристов, легенды о регионе [3].

2. Участие в специализированных туристских выставках разного уровня как с точки зрения установления полезных бизнес-контактов, так и продвижения имиджа туристского региона: Интурмаркет, Отдых, INWETEX, Лыжный салон, МИТТ (Москва), МАТКА и выставка снегоходного оборудования SNOWMOBILE — MOOTTORIKELKKA MESSUT (Финляндия).

Важно расширять участие в выставках, которые напрямую не связаны с турбизнесом, но содержательно могут оказать неоценимую помощь в продвижении туристского имиджа Мурманской области. Это выставки, ориентированные не на профессионалов турбизнеса, а на потенциальных туристов: это очень популярная у конечного потребителя «Охота и рыбалка на Руси» (Москва, ВВЦ), и выставка специализированной техники «Вездеход» (Москва, «Крокус-Экспо»). Эти выставки согласуются с достаточно популярными турами рекреационного промысла (охота, рыбалка) и турами на снегоходной технике на территории Мурманской области.

3. Организация инфо- и рекламных туров. Несмотря на то, что это достаточно дорогостоящее пред-

приятие для туроператоров и турагентов, такие туры возможны не сполной, а частичной оплатой тура принимающей стороной с последующим возмещением участникам такого тура понесенных затрат при условии направления от 3 до 10 туристов в течение года.

4. Информационная поддержка как продвижения туристского имиджа Мурманской области, так и регионального турпродукта через ведущие издания о путешествиях (журналы «Вокруг света», «Гео», «National Geographic»), фильмы и передачи на телевидении (телеканалы Россия Культура, «Моя планета», Russia Today — с ориентацией на зарубежных потребителей). Несмотря на то, что это самый дорогой канал коммуникации, можно получить бесплатные для администрации области публикации, пригласим журналистов этих изданий и телевизионный канал поучаствовать в событийном мероприятии в регионе: Праздник Солнца, Праздник Севера, гонки на собачьих упряжках, День рыбака или Праздник Козули и др.

Во-вторых, в отношении потенциальных туристов нам видится перспективным, прежде всего, продвижение таких туров как:

1. Горнолыжные, снегоходные туры, туры на квадроциклах. Эти направления сейчас активно развиваются в Мурманской области.

2. Экскурсионные и этнические туры на Ловозеро и Терский берег — настоящая экзотика Севера. Пока такие туры мало востребованы как самостоятельные, чаще они являются сопутствующим продуктом к основным услугам. Кроме того, эти туры не пользуются широким спросом из-за высокой стоимости трансфера и нехваткой в этих районах средств размещения.

Активное продвижение данных видов активного отдыха на территории Мурманской области возможно с помощью наружной рекламы в ключевых туристических местах (на горнолыжных курортах, в крупнейших отелях, в музеях, на вокзале и в аэропортах); ссылок на страницах региональных туристских Интернет-ресурсов; презентаций на крупнейших этнофестивалях и народных праздниках соседних Архангельской, Вологодской областей и республики Карелии, где традиционно много событийных туристов.

В целом, активная и разнообразная реклама должна быть наиболее эффективным средством продвижения туристского имиджа Мурманской области, для чего мы порекомендовали бы включать региональные и федеральные музеи этнической направленности в разработку и реализацию рекламных акций и проектов по презентации культуры саамов и поморов.

Третий момент, касающийся местных жителей, также являющихся потенциальными потребителями регионального турпродукта.

Большая доля туристов из числа жителей Мурманской области (за исключением горнолыжного сегмента и рыбалки) выбирает путешествия по региону по принципу «слухов» (отзывов друзей, родственников, коллег и т.д.). Поэтому необходимо продвигать имидж родного региона и для местных

жителей с помощью организации на территориях муниципалитетов презентаций региональных турпродуктов. Особое внимание следует уделить турам выходного дня (на местной туристской выставке, с помощью наружной рекламы на улицах городов, в деловых и торговых центрах, на крупных предприятиях, кинотеатрах, предприятиях питания). Целесообразным представляется и проведение конкурсов среди местных жителей на лучшие фотографии, видеоролики о регионе с публичной презентацией победителей и наградой однодневной экскурсией/туром по региону [2].

На наш взгляд, важность и необходимость проведения таких конкурсов заключается и в том, что у целевых аудиторий кроме популяризации туристского региона заменяются стереотипы восприятия его имиджа.

Так, в сознании целевой группы потенциальных туристов конкурсные фото- и видеоматериалы помогут закрепить мысль о том, что Мурманская область — это:

- близко и быстро (2-2,5 часа перелета из Санкт-Петербурга или Москвы, поездом из Санкт-Петербурга одни сутки без смены часовых поясов); несложный пропускной режим на приграничных территориях;
- сила и красота северной природы с удивительными чудесами в любое время года: летом ночью светит солнце, а зимой — северное сияние, в июле цветет сирень, грибы бывают ростом с дерево, смешение трех климатических зон с цветущей тундрой, отсутствие лютых морозов и много снега без слякоти благодаря Гольфстриму;
- доступный по ценам и логистике горнолыжный отдых с полноценным снежным покровом и современным оборудованием трасс, с небольшим перепадом горных высот без неприятной акклиматизации; бескрайние дикие просторы для снегоходных сафари и экспедиций на квадроциклах; семужьей рыбалкой и катанием на оленях и собачьих упряжках, дайвингом в Баренцевом море (летом можно купаться даже детям);
- заповедные уголки подлинной жизни и традиционного уклада поморов и саамов (Лапландия);
- отдых от цивилизации «на краю света» в российской Арктике, где северная экзотика соединяется с транспортной доступностью и разнообразием активного отдыха.

Для местных жителей конкурсы помогут закрепить имидж Мурманской области как региона, где

- есть множество интересных мест, которые туристы едут за тысячи километров, и, живя поблизости, просто неприлично в них не побывать — нужно знать историю земли, на которой живешь и гордиться ею;
- есть много интересных мест, где можно отдыхать семьей в выходные или в отпуске, не затрачивая на отдых больших средств.

В целом привлечение не только потенциальных туристов, но и представителей СМИ разного уровня, фотографов и профессиональных национально-ориентированных блогеров к таким конкурсам будет способствовать формированию банка высококачественных и художественных фотографий и профессиональных видеосюжетов о регионе.

Список литературы

1. Геоинформационный портал Мурманской области [Электрон. ресурс]. — Режим доступа: <http://portal.kgilc.ru/private/turizm/>.
2. **Кирьянко А.В.** Теоретические подходы к понятию маркетинга имиджа города / А.В. Кирьянко // Бренддинг малых и средних городов России: опыт, проблемы перспективы: материалы Всерос. науч.-практ. конф. / отв. ред. А.М. Бритвин. — Екатеринбург: Изд-во Уральского гос. ун-та, 2012. — С. 90–95.
3. **Косарева Н.В.** Мурманская область: вопросы ребрендинга туристской территории / Н.В. Косарева // Актуальные проблемы развития туризма : Материалы IV Междунар. науч.-практ. конф. / под ред. С.В. Дусенко, Н.Л. Авиловой; РГУФКСМиТ. — М., 2020 — С. 269–278.
4. **Косарева Н.В.** Туристско-рекреационный потенциал Мурманской области как основа формирования имиджа туристской территории / Н.В. Косарева // Теория и практика проектного образования. Журнал научных публикаций. — 2019. — №4(12)/2019. — С. 52–55.

МОЛОДЫЕ УЧЕНЫЕ – ПОИСК САМООПРЕДЕЛЕНИЯ

ПРАВОВОЕ РЕГУЛИРОВАНИЕ ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ В СОЦИАЛЬНЫХ СЕТЯХ

LEGAL REGULATION OF THE PROTECTION OF PERSONAL DATA IN SOCIAL NETWORKS

Зуева

Анна Сергеевна

Кандидат экономических наук, доцент, доцент кафедры компьютерного права и информационной безопасности Высшей школы государственного аудита Московского государственного университета имени М.В. Ломоносова, доцент кафедры «Государственный финансовый контроль и казначейское дело» Финансового университета при Правительстве РФ, доцент кафедры правового обеспечения публичных финансов Института законодательства и сравнительного правоведения при Правительстве Российской Федерации



Zueva

Anna Sergeevna

Candidate of Economic Sciences, Associate Professor, Associate Professor of the Department of Computer Law and Information Security of the Graduate School of State Audit, Moscow State University named after M.V. Lomonosov, Associate Professor of the Department "State Financial Control and Treasury" of the Financial University under the Government of the Russian Federation, Associate Professor of the Department of Legal Support of Public Finance at the Institute of Legislation and Comparative Law under the Government of the Russian Federation

Василихина

Юлия Владимировна

Студент (бакалавр), Московский государственный университет имени М.В. Ломоносова, Высшая школа государственного аудита, Москва, Россия



Vasilihina

Julija Vladimirovna

Student (Bachelor), Moscow State University named after M.V. Lomonosov, Higher School of Government Audit, Moscow, Russia

Аннотация: в условиях цифровизации происходят все-сторонние изменения сфер жизнедеятельности общества. Прогресс в отдельных отраслях является подрывным фактором для других. Так, с развитием технологий возрастает риск злоупотребления персональными данными граждан, большинство из которых находятся в открытом доступе в социальных сетях. В силу того, что большинство социальных интернет площадок принадлежит иностранным компаниям, вопрос о способах защиты права граждан на защиту персональных данных как от внутренних, так и внешних посягательств стоит остро, что и предстоит рассмотреть в данной статье.

Ключевые слова: персональные данные, защита персональных данных, безопасность в социальных сетях.

Abstract: in the context of digitalization, there are comprehensive changes in the spheres of society. Progress in certain industries is disruptive to others. So, with the development of technology, the risk of abuse of personal data of citizens increases, most of which are in the public domain on social networks. Due to the fact that most social Internet sites belong to foreign companies, the question of how to protect the right of citizens to protect personal data from both internal and external encroachments is acute, which is to be considered in this article.

Keywords: personal data, personal data protection, safety in social networks.

В условиях цифровизации современного общества, существования большого числа социальных сетей, связывающих миллиарды людей различных государств, зарождается риск угрозы утечки персональным данным

пользователей, которые добровольно предоставляют злоумышленникам колоссальный массив информации о себе. В случае злоупотребления правом пользователя сети Интернет, нанесения ему материального или мо-

рального ущерба возникает сложность в государственном-правовом регулировании данных правоотношений, поскольку они в силу стремительного развития информационных технологий, в большей степени, законодательно не урегулированы. В связи с этим квалифицировать определенное действие как противоправное деяние представляется невозможным, в результате чего оно остается безнаказанным. Согласно статистике Министерства внутренних дел за 2020 год число преступлений, совершенных с использованием информационно — телекоммуникационных технологий, возросло на 73,4%, в том числе с использованием сети «Интернет» на 91,3% [1]. Данный вопрос сохраняет свою актуальность на протяжении долгого периода времени и его разрешение требует комплексного подхода к восполнению пробелов в регулировании правоотношений пользователей в социальных сетях.

Возрастающее число злоупотреблений конституционно-гарантированными правами граждан в информационном пространстве, в том числе в социальных сетях, породило необходимость в создании отдельного нормативного правового акта, который бы отчасти разрешил, а вернее сказать, создал основу для регулирования данных правоотношений, в особенности, мер правовой защиты от посягательств на прав и свобод человека в социальных сетях. Таковым стал сравнительно молодой, принятый 27 июля 2006 года, Федеральный закон «О персональных данных», в который в декабре 2020 года были внесены изменения. Согласно его положениям персональными данными является любая информация, которая прямо или косвенно относится к определенному или определяемому лицу, при этом сведения о субъекте персональных данных должны быть исключены в любое время из общедоступных источников персональных данных по его требованию или по решению суда или иных уполномоченных на то органов, в случае нарушения прав субъекта персональных данных виновное лицо понесет материальную ответственность. Также в данный закон были внесены изменения, которые вступят в силу 1 марта 2021 года. Согласно внесенным поправкам не допускается получение согласия на распространение персональных данных «по умолчанию», согласие на обработку персональных данных может даваться только оператору персональных данных. Молчание — актом согласия не является.

В области защиты персональных данных применяются также положения Федерального закона № 149 «Об информации, информационных технологиях и защите информации» от 27.07.2006 года. Так, статья 15.5 данного Закона учреждает реестр нарушителей прав субъектов персональных данных, основной задачей которого является ограничение доступа к информации в сети «Интернет», обрабатываемой с нарушением законодательства РФ в области персональных данных. За нарушение законодательства РФ в области персональных данных предусмотрена уголовная (ст. 137 УК РФ) и административная ответственность (ст. 13.11). Стоит отметить, что несмотря на важность

положений данных законодательных актов, предусмотренные ими механизмы регулирования защиты персональных данных являются незавершенным. В частности, остается не урегулированным способ определения места и времени совершения юридически значимых действий, пути правового воздействия на формирование инфраструктуры в социальных сетях, понятия база. Также существенными проблемами является установление связи между технической стороной обеспечения информационной безопасности и обеспечением экономическо-правовой и информационной безопасности личности в современных условиях, и то положение, что большинство социальных сетей принадлежат иностранным компаниям и, таким образом, правоотношения, возникающие в результате их использования, не могут регулироваться российским законодательством.

Свидетельством вышесказанного может послужить пример, связанный с крупнейшей в мире компанией Facebook, Inc и принадлежащим ей с 2014 года приложением для обмена сообщениями WhatsApp, который в феврале 2021 года создал новое пользовательское сообщения, правила которого подвергают опасности персональные данные граждан Российской Федерации и пользователей WhatsApp в целом. Так как WhatsApp принадлежит компании Facebook, Inc, все его пользователи в соответствии с новым пользовательским соглашением, за исключением граждан Великобритании и граждан стран Европейского союза, должны обязаться предоставить персональные данные данной компании, в числе которых контактные данные, личные транзакции и IP-адреса. Таким образом, компания сможет отследить местоположение пользователя, иметь доступ к его статусу, к фото их профайлов, что прямо подрывает конфиденциальности персональных данных. Важно учесть, что все полученные данные будут предоставлены всем компаниям, принадлежащим и сотрудничающим с Facebook. При этом, на пользователей отказавшихся принять новое пользовательское соглашение, WhatsApp планирует накладывать ограничения, в том числе и такую меру, как удаление из данной социальной сети. На данный момент введение этого соглашения отложено до 15 мая 2021 года, в связи со всеобщей его критикой. Несмотря на это, насущные вопросы о том, как обеспечить защиту персональных данных граждан Российской Федерации в пределах не только информационного пространства России, но и в пределах выходящих за ее границы, сохраняется, так как в рамках российского законодательства он не урегулирован. Разрешение данного вопроса имеет существенное значение как для отдельного гражданина, который является пользователем зарубежных социальных сетей, так и для национальной безопасности Российской Федерации в целом, так как вероятность утечки персональных данных как рядовых граждан, так и государственных служащих высока.

Таким образом, в ближайшем будущем российскому законодателю предстоит ликвидировать пробел

в праве для обеспечения суверенного интернет пространства. Ведь если мы зададимся вопросом о том является ли наш Интернет суверенным? Вероятно, последует ответ, нет. Поскольку на данный момент большинство российских компаний, среди которых Сбербанк, Госуслуги, Яндекс, используют сервисы американских Big Tech компаний (Google, Facebook, Amazon, Microsoft). И в том случае, если мы не имеем в настоящее время отечественных сервисов, готовых заменить зарубежные аналоги, то мы должны обеспечить безопасность персональных данных законодательным путем, защитив тем самым права и свободы граждан в данной области как от внутренних посягательств, так и внешних угроз.

Список литературы

1. Характеристика состояния преступности в Российской Федерации за январь — декабрь 2020 года [Электрон. ресурс]. — Режим доступа: <https://мвд.рф/reports/item/22678184/>.
2. Жуков А.З. Основные проблемы правового регулирования интернет-отношений в российской федерации / А.З. Жуков // Проблемы экономики и юридической практики. — 2018. — № 5.
3. Анисимова А.С. Правовое регулирование интернета: основные пробелы и направления деятельности государства / А.С. Анисимова // Юридический вестник ДГУ. — 2020. — Т. 33. — № 1.
4. Пономарев Д.В. Отдельные аспекты совершенствования законодательства в области противодействия незаконному использованию персональных данных пользователей социальных сетей / Д.В. Пономарев, Е.А. Гужов, В.А. Иноценко // Юрист-Правоведъ. — 2014. — № 6,2014(67).
5. Слесарев Ю.В. Проблемы правового регулирования размещения информации в социальных сетях / Ю.В. Слесарев, А.В. Лосяков // Балтийский гуманитарный журнал. — 2016. — Т. 5. № 2(15).
6. Исаев А.С. Правовые основы организации защиты персональных данных: учеб. пособие / А.С. Исаев, Е.А. Хлюпина. — СПб., 2014.
7. Состояние преступности в России за январь декабрь 2020 года.

ОПРЕДЕЛЕНИЕ УСЛОВИЙ ПРИМЕНИМОСТИ АЛГОРИТМА ШИФРОВАНИЯ RSA ДЛЯ КЛЮЧЕЙ ШИФРОВАНИЯ ДЛИНОЙ МЕНЕЕ 256 БИТ

DETERMINATION OF THE CONDITIONS OF APPLICABILITY OF THE RSA ENCRYPTION ALGORITHM FOR ENCRYPTION KEYS WITH A LENGTH OF LESS THAN 256 BIT

Дадашов Ильяс Октаевич

Студент 2-го курса ИАТЭ НИЯУ МИФИ отделения Ядерной физики и технологий, направление подготовки — ядерная физика и технологии



Dadashov Il'jas Oktaevich

2nd year student of IATE NRNU MEPHl of the Department of Nuclear Physics and Technology, direction of training — nuclear physics and technology

Гужва Дмитрий Вадимович

Студент 2-го курса МГТУ им. Н.Э. Баумана факультета Специального машиностроения, направления подготовки — робототехнические системы и мехатроника



Guzhva Dmitrij Vadimovich

2nd year student of M.V. N.E. Bauman Faculty of Special Mechanical Engineering, areas of training — robotic systems and mechatronics

Аннотация: В основе проекта лежит изучение проблемы работы алгоритма шифрования RSA с применением разработанной программой для шифрования информации. В рамках проекта была разработана методика получения открытых ключей шифрования в приложении Microsoft Excel.

Ключевые слова: Алгоритм, безопасность, методика, ключи шифрования.

Abstract: The project is based on the study of the problem of the RSA encryption algorithm using the developed program for encrypting information. Within the framework of the project, a method was developed for obtaining public encryption keys in Microsoft Excel.

Keywords: Algorithm, security, technique, encryption keys.

Введение

На сегодняшний день для защиты цифровой информации применяются симметричные и асимметричные системы шифрования. Работа симметричных криптосистем основана на использовании определённого ключа, который может шифровать и дешифровать информацию (рис. 1). Наиболее распространённым алгоритмом симметричных криптосистем является алгоритм шифрования AES, который получил широкое распространение во многих программных продуктах, таких как активаторы

WinZip, WinRAR, 7zip; системы бэкапа (Backup4all, Handy Backup, Acronis True Image и т.п.).

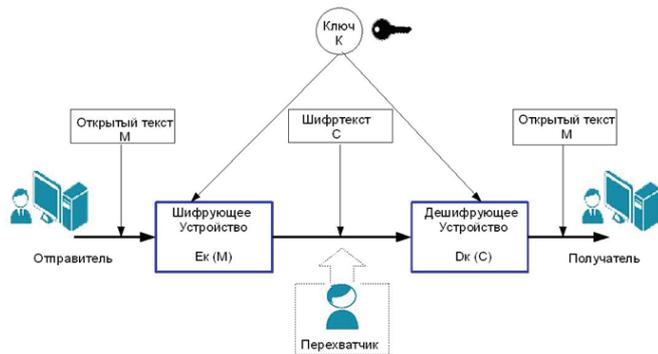


Рис. 1. Схема работы симметричных криптосистем

В асимметричных криптосистемах шифрования используются два типа ключей: открытый — для шифрования информации, который может передаваться по незащищённому каналу связи и закрытый — для дешифрования информации (рис. 2).



Рис. 2. Схема работы асимметричных криптосистем

Алгоритм RSA является самым распространённым алгоритмом шифрования с открытым ключом в мире и одним из самых копируемых программных продуктом в истории [5]. Он применяется для шифрования информации в операционных системах Windows, в программных продуктах компании Mozilla Firefox и т.д.

Работа алгоритма основана на действии факторизации. Для генерации ключа шифрования находят произведение двух чисел, следовательно, для того, чтобы взломать зашифрованное сообщение необходимо знать значения этих чисел, что можно сделать только путём факторизации. Однако при достаточно больших значениях чисел, даже самым мощным компьютером понадобится несколько лет, для выполнения факторизации числа (рис. 3), что делает алгоритм шифрования RSA более криптостойким по сравнению с AES.

С развитием технологий появляется всё больше различных приложений, созданных рядовыми поль-

зователями интернета. Как правило в таких приложениях либо применяют симметричные криптосистемы, что делает их не такими устойчивыми, как в случаях применения асимметричных криптосистем, либо вопросу безопасности информации вовсе не уделяется внимание.

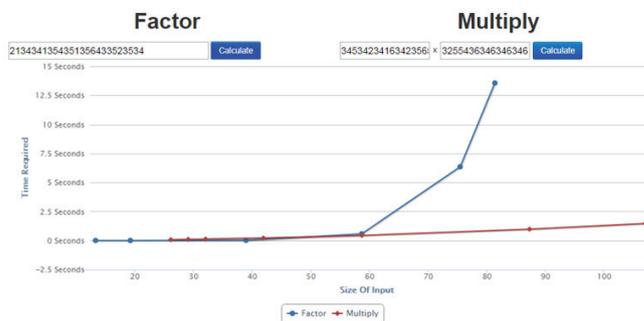


Рис. 3. График зависимости времени факторизации и умножения числа в зависимости от размера чисел

Основной проблемой применения асимметричных криптосистем в таких приложениях является сложность их структуры, а также использование длинных ключей шифрования, в результате чего, такие системы работают медленнее, чем симметричные. Для сравнения, длина ключей шифрования алгоритма RSA — 1024–2048 бит, а средняя скорость его работы — 1 Мбит/с, в то время, как у алгоритма AES длина ключа составляет 128–256 бит, средняя скорость работы — 150 Мбит/с.

Мы предполагаем, что можно увеличить скорость работы алгоритма шифрования RSA, сделав его применимым для рассматриваемых программных продуктов и тем самым увеличить защищённость информации в сравнении с использованием алгоритмов симметричных криптосистем таких как AES.

В таких приложениях нет необходимости использовать стандартную длину ключа 1024–2048 бит, так как, в большинстве случаев, они предназначены для локального пользования, что не требует настолько высокого уровня надёжности. Следовательно, можно использовать более короткие ключи шифрования, повышая скорость работы алгоритма. Конечно, можно увеличить и скорость работы алгоритмов симметричных криптосистем, уменьшив длину их ключа, но в таком случае они станут не криптостойкими.

Однако, при использовании коротких ключей, стандартных условий функционирования алгоритма RSA[6] — не достаточно, и алгоритм может работать некорректно, в результате чего возникает необходимость в установлении дополнительных условий для корректной работы алгоритма при коротких ключах шифрования (ключи длиной менее 256 бит).

Определение дополнительных условий для применения коротких ключей шифрования

Исследование проводилось в собственных программах, написанных на языке программирования C++, которые выполняли шифрование и дешифрование числового сообщения (сообщение, которое со-

держит в себе число) по алгоритму шифрования RSA. В ходе исследования было зашифровано и расшифровано более 500 тысяч числовых сообщений, при различных значениях взаимно простых чисел p и q [7], используемых для нахождения открытого ключа. Рассматривались такие числа p и q что $q > p$.

В результате нестабильной работы алгоритма при коротких ключах шифрования наблюдаются следующие ошибки:

1. Информация может быть неправильно зашифрована:

- Сообщение m шифруется само в себя ($c = m$), что не имеет смысла.
- Сообщение m шифруется в ноль ($c = 0$) что в дальнейшем приведёт к неправильному дешифрованию зашифрованного сообщения.

2. Информация может быть неправильно дешифрована:

- Зашифрованное сообщение c при расшифровке не принимает исходное значение шифруемого сообщения m , что может привести к потере информации.

В результате исследования определено и сформулировано дополнительное условие, которое позволяет корректно работать алгоритму RSA при использовании коротких ключей шифрования:

- $$m \in [2; q-1] \quad (1)$$
- $$m \neq a n, \quad (2)$$
- $$m \neq a n + 1 \quad (3)$$

где m — шифруемое числовое сообщение;

- $n = p q$;
- $a = 1, 2, 3, \dots$

Условия 1–3 также применимы при $q < p$: $m \in [2; p-1]$.

Таким образом, алгоритм шифрования RSA становится применим для ключей шифрования длиной менее 256 бит при одновременном соблюдении стандартных и дополнительных (1–3) условий, что позволяет увеличить скорость его работы.

Разработка алгоритмов для нахождения всех доступных значений открытого ключа

Дальнейшее исследование проводилось в программе для работы с электронными таблицами Microsoft Excel 2016 по методическому указанию «Основы кодирования и криптографии» [3] для разработки алгоритма, позволяющего получить все возможные значения открытой экспоненты e при фиксированных значениях чисел p и q . Что даёт возможность выбирать наиболее оптимальный вариант параметра надёжность — быстрое действие для определённых задач (чем больше длина ключа, тем больше криптостойкость, чем меньше длина ключа, тем выше скорость работы алгоритма). Были проведены расчёты для более 250 тысяч различных значений закрытой экспоненты d . На основе полученных результатов были разработаны два алгоритма генерации открытой экспоненты e .

Алгоритм 1. Формула = ОСТАТ(F4*\$F4;\$C\$2) протягивается на следующие значения графы «степень»

стоящих после значения e . Формула может протягиваться на неограниченное количество ячеек (количество возможных ячеек определяются вычислительной мощностью ПК). После чего с определённой периодичностью обнаруживаются столбцы, которые в своих ячейках будут содержать такие значения зашифрованного сообщения, как и в столбце под значением e . Следовательно, значения числа в графе «степень» над такими столбцами будут значениями открытой экспоненты (рис. 4).

Алгоритм 1 применим, если при переводе числа n в двоичную систему счисления, оно будет содержать в себе не более одного нуля.

Рис. 4. Пример Алгоритма 1

Алгоритм 2. Самостоятельно подбираются первые четыре значения открытой экспоненты e (значения экспоненты e начинаются с малых чисел (односоставные числа), поэтому подобрать эти числа не составит проблемы, которая требовала бы отдельного решения). Затем все действия повторяются так же, как и в алгоритме 1. Но уже с определённой периодичности будут обнаруживаться парные колонки, которые содержат в себе значения зашифрованного текста (рис. 5). Алгоритм 2 применим, если при переводе числа n в двоичную систему счисления, оно будет содержать в себе более одного нуля.

Рис. 5. Пример Алгоритма 2 — значения парных колонок J и L повторяются через 9 колонок в V и X (аналогично с парными колонками P и R)

Недостаток алгоритма 1 и алгоритма 2 заключается в том, необходимо выполнять всё «в ручную» путём построения таблиц с формулами.

Заключение

Нами было разработана методика применения алгоритма шифрования RSA с использованием ключей шифрования длиной менее 256 бит, что позволяет оптимизировать его для применения в программных продуктах, предназначенных для локального пользования.

Разработаны алгоритмы, вычисляющие все возможные значения открытой экспоненты e при фиксированных значениях взаимно простых чисел p и q . Таким образом, при разработке программных продуктов можно выбирать оптимальный размер открытого ключа под требуемые задачи, используя приведённые алгоритмы. Ведутся разработки по созданию программы, которая будет компенсировать текущие недостатки алгоритма 1 и алгоритма 2.

Ведётся разработка программы, которая будет выполнять шифрование информации по алгоритму AES для того, чтобы можно было провести полный сравнительный анализ между алгоритмами AES в котором будут использоваться ключи шифрования стандартной длины и алгоритма RSA с применением коротких ключей шифрования. Завершение разработки планируется по 15.03.2021.

Ведётся разработка тестового приложения на смартфоны в котором будет применяться созданная программа, шифрующая информацию по алгоритму RSA с использованием коротких ключей. После чего будут проведены окончательные тесты по применению алгоритма шифрования RSA в таких приложениях.

Список литературы

1. Системы шифрования с открытыми ключами. Основы криптографии / А.П. Алферов, А.Ю. Зубков,

А.С. Кузьмин [и др.]. — М.: Гелиос АРВ, 2002, — С. 310–322.

2. Diffie W., Hellman M.E. New Directions in Cryptography // IEEE Trans. Inf. Theory / F. Kschischang — IEEE, 1976. — Vol. 22, Iss. 6. — P. 644–654. — DOI:10.1109/TIT.1976.1055638
3. Основы кодирования та криптографії / В.В. Швигов. — Луганськ: ДЗ «ЛНУ імені Тараса Шевченка», 2014. — С. 58–64.
4. Дадашов И.О. Исследование применимости алгоритма шифрования RSA для ключей шифрования различной длины / И.О. Дадашов // Будущее атомной энергетики — AtomFuture 2019. — Обнинск, 2019. — С. 143–145.
5. Алгоритм шифрования RSA [Электрон. ресурс]. — Режим доступа: <http://www.e-nigma.ru/stat/rsa> (Дата обращения-10.11.2019).
6. Описание алгоритма шифрования RSA [Электрон. ресурс]. — Режим доступа: <http://teh-box.ru/informationsecurity/algorithm-shifrovaniya-rsa-na-palcah.html> (Дата обращения: 11.12.2017).
7. Алгоритм шифрования RSA [Электрон. ресурс]. — Режим доступа: <https://www.youtube.com/watch?v=vooHjWxmcIE&t=717s>.

ВОПРОСЫ ОПРЕДЕЛЕНИЯ ПРАВОВОЙ ПРИРОДЫ БИТКОИНА

QUESTIONS OF DETERMINING THE LEGAL NATURE OF BITCOIN

**Архипова
Арина Сергеевна**

*Студентка (магистрант)
Московского государственного юридического
университета имени О.Е. Кутафина (МГЮА)*



**Arhipova
Arina Sergeevna**

*Student (undergraduate)
of the Moscow State Law University named
after O.E. Kutafina (Moscow State Law Academy)*

Аннотация. Предполагается, что для правового анализа любого явления, прежде всего, стоит разобрататься с терминологией и природой появления этого явления, а также его свойствами и механизмами функционирования. В связи с этим, в первой части статьи будут предприняты попытки раскрыть основные понятия криптографической индустрии, причины возникновения и популярности такого явления, как Биткоин, его свойства и механизмы функционирования, а также способы его получения и использования. Во второй части статьи будет проведен правовой анализ Биткоина и возможностей его законодательного регулирования.

Ключевые слова: цифровая валюта, криптовалюта, биткоин, блокчейн, майнинг, государственное регулирование, правовое регулирование.

Abstract. It is assumed that for the legal analysis of any phenomenon, first of all, it is necessary to understand the terminology and the nature of the appearance of this phenomenon, as well as its properties and mechanisms of functioning. In this regard, the first part of the article will attempt to interpret reveal the basic concepts of the cryptographic industry, the reasons for the emergence and popularity of such a phenomenon as Bitcoin, its properties and mechanisms of functioning, as well as ways to obtain and use it. The second part of the article will attempt on legal analysis of Bitcoin and the possibilities of its legislative regulation.

Keywords: digital currency, cryptocurrency, bitcoin, blockchain, mining, government regulation, legal regulation.

Цифровая валюта: понятие и краткий исторический экскурс

Итак, в октябре 2012 года Европейский центральный банк распространил доклад «Схемы виртуальных валют», в котором раскрывал понятия и содержания цифровых валют и электронных денег, а также оценил риски в отношении стабильности цен, платежной системы и отсутствия регулирования. В соответствии с ним: «виртуальная валюта — это тип нерегулируемых, цифровых денег, которые выпускаются и обычно контролируются их разработчиками, и используются и принимаются среди участников определенного виртуального сообщества» [7, с. 68]. В свою очередь, криптовалюта — это разновидность цифровой валюты, создание и контроль за которой базируются на криптографических методах [6, с. 34–39].

Впервые криптовалюты были упомянуты уже в 1998 году, а идея приписывается японцу по имени Вей Дай, который описал идею создания «b-money». В это же время похожую идею предложил Ник Сабо для создания криптовалюты «bit-gold» [16, с. 336]. В 1999 году ученый экономист, лауреат Нобелевской премии Милтон Фридман в интервью, проведенном NTU / F, сказал, что: «...скоро будут разработаны надежные электронные наличные деньги» и оказался прав, так как позже была изобретена и введена в оборот новая цифровая валюта, отвечающая его требованиям, а именно Биткоин.

Преимущественные свойства Биткоина — причина его популярности

Биткоин остается наиболее популярной криптовалютой и по сей день, хотя на данный момент их огромное количество. И причины такого успеха именно этой криптовалюты содержатся в ее свойствах:

1. Биткоин не привязан к какой-либо валюте реального мира. Обменный курс определяется спросом и предложением на рынке.

2. Биткоин работает на глобальном уровне и может использоваться как валюта для всех типов операций (и для виртуальных, и для реальных товаров и услуг).

3. Операции анонимны, чтобы провести сделку в системе Биткоин, пользователю не нужно сообщать свои персональные данные ни другой стороне сделки, ни третьим лицам, так как счета не зарегистрированы и Биткойны отправляются напрямую из одного компьютера в другой. Также пользователи имеют возможность создавать несколько адресов Биткоин для дифференциации или отделения операций.

4. Операции в системе Биткоин осуществляются дешевле и быстрее по сравнению с традиционными платежными средствами.

5. При проведении сделки информацию о прохождении платежа можно проследить от начала до окончательного момента превращения электронной валюты в монеты. Следовательно, получатель может отследить всю цепочку транзакций в архивной базе

данных и убедиться, что оплата действительно была произведена [11, с. 142–154].

6. Система Биткоин абсолютно независима, так как не имеет ни единого владельца, ни администратора. Как упоминается в докладе Европейского центрального банка «Схемы виртуальных валют» в системе Биткоин отсутствует даже центральная точка доступа, то есть, нет сервера, который мог бы быть выключен, если бы органы власти сочли это необходимым [7, с. 68].

7. Отсутствие контролирующего центра, также означает то, что сделки всегда безвозвратны, поскольку нет возможности отменить платеж, «заморозить» счет или совсем заблокировать его.

8. Возможность не только обменивать и покупать, но и самостоятельно добывать деньги. Добывать Биткойны теоретически может каждый пользователь сети. Такая добыча называется «майнингом». Эмиссия Биткойнов совершается исключительно майнерами, причем ни один отдельный человек или корпорация не может контролировать этот процесс.

Понятие «майнинга» уже продолжительное время исследуется в научной юридической литературе [19]. И.В. Ершова, со ссылкой на текст проекта федерального закона №419059-7 «О цифровых финансовых активах» [17] справедливо определяет майнинг — предпринимательской деятельностью, которая признается таковой, в случае, когда лицо, которое его осуществляет, в течение трех месяцев подряд превышает лимиты энергопотребления, установленные Правительством РФ [18].

Таким образом, Биткоин — это децентрализованная электронная валютная система и в тоже время валюта, основанная на криптографии и имеющая ряд положительных качеств, обуславливающих ее популярность.

Система Блокчейн

Вся система Биткоин работает на основе технологии Блокчейн. Блокчейн — это многофункциональная и многоуровневая информационная технология, предназначенная для надежного учета различных активов. Технология надежного распределенного хранения записей обо всех когда-либо совершенных транзакциях [12, с. 49–55]. Блокчейн доступен публично и хранится локально множеством клиентов, его можно свободно загрузить из интернета [13, с. 91]. То есть вся история любых Биткойн-транзакций, сделанных кем угодно по всему миру с самого появления Биткойна публично доступна для просмотра любому человеку.

Все блоки в системе Блокчейн связаны между собой в непрерывную цепочку, причем внести изменения в уже записанные в базу блоки невозможно. Реестры базы данных хранятся не в одном месте, а на сотнях тысячах компьютеров пользователей — участников системы. Реестры постоянно автоматически обновляются и дополняются данными о новых добытых блоках Биткоин и о совершенных транзакциях.

Возникает вопрос, если вы будете использовать Биткойн, вся история когда-либо сделанных вами транзакций будет публично доступна? Это только частично так. Публичный аспект Блокчейн содержит только Биткойн-адреса и суммы транзакций. В нем нет какой-либо личной или опознаваемой информации [13, с. 91].

Другой момент, который необходимо понять, состоит в том, что количество Биткойн-адресов у одного пользователя не ограничено. Биткойн-программы не требуют индивидуального управления каждым балансом каждого адреса, они могут показать вам общий баланс всех адресов. Однако если вы получите одну транзакцию на большую сумму денег, например, тысяча долларов в Биткойнах, и если после этого вы захотите потратить один Биткойн с этого адреса, получатель сможет увидеть, что вы имеете в своем распоряжении тысячу долларов в Биткойнах, что, возможно, вам бы не хотелось раскрывать. На этот случай существуют программы, позволяющие скрыть информацию о имеющихся у вас денежных средствах, раскрывающие их по множеству адресов [13, с. 91].

Способы получения и использование Биткойна

Так как стать владельцем Биткойна и зачем он вообще нужен? Вопрос о полезности и востребованности очевиден: эту криптовалюту можно использовать и для оплаты товаров и услуг, и для инвестирования денег.

Получить же Биткойн можно 4 путями: купить, заработать, добыть или выиграть. Про добычу (майнинг) уже говорилось ранее. Заработать Биткойны можно на сайтах для заработка в сети, предлагающих данный способ оплаты. Выиграть виртуальные монеты можно в некоторых лотереях и играх. Приобрести Биткойны можно в онлайн-обменниках.

Учитывая вышесказанное Биткойн можно использовать в 3 направлениях: 1) хранить; 2) осуществлять международные платежи; оплачивать услуги.

Таким образом, можно сделать вывод о том, что простыми словами, Биткойн — это возможность тратить деньги быстро и анонимно.

Правовое регулирование

Несмотря на то, что криптовалюты на основе технологии блокчейн являются по сути саморегулируемыми, возникают вопросы, связанные с определением места среди объектов регулирования: требуется ли выделить новую категорию в современном гражданском праве или же возможно обратиться к уже существующим. В нашем случае, стоит обратиться к существующему законодательству и попытаться установить возможность регулирования в нынешних условиях [20]. Для этого стоит обратиться к наиболее близким по возможному регулированию объектам из статьи 128 Гражданского Кодекса Российской Федерации (далее ГК РФ) — бездокументарные ценные бумаги, безналичные денежные средства, а также дополнительно — электронные денежные средства.

Рассматривая категорию ценных бумаг, стоит отметить разницу между способом размещения ценных бумаг, то есть IPO, и размещением криптовалют — ICO. Поскольку ценные бумаги представляют собой обязательственные права, которые закреплены в решении о выпуске или ином акте лица, выпустившего ценные бумаги, то лицо, имеющее ценные бумаги имеет право требования. В случае с ICO отличие в том, что обязательственные права между организацией, выпустившей криптоединицу, и ее приобретателем не возникают. В этом видится различие между ценными бумагами и криптовалютой.

Относительно безналичных денег, с точки зрения гражданского права — это, прежде всего, право требования. Значит, эта категория также отпадает. Однако можно предположить, что понимание безналичных денежных средств несколько узко трактуется. В большинстве случаев, они используются не как само право требования, а выполняют функцию передачи определенной информации о платежах. Такое понимание безналичных денег уже гораздо ближе к сущности криптовалют, только транзакции отслеживаются и регулируются не эмитентом, а с помощью криптографии. Значит, некоторая схожесть присутствует.

Криптовалюта также не подпадает под определение электронных денежных средств, которое дано в п. 18 ст. 3 Федерального закона № 161-ФЗ «О национальной платежной системе». В данном пункте, под электронными денежными средствами в российском законодательстве понимаются только фиатные деньги, т. е. те, которые выражены в государственной денежной единице [2]. Соответственно, частная цифровая валюта не признается электронными денежными средствами в России. Единственная правовая категория, позволяющая отчасти охватить понятие «криптовалюты» — это понятие «иное имущество».

Стоит обратиться к глоссарию с определениями терминов новой экономики, сформированному Российской ассоциацией электронных коммуникаций. В частности, криптовалюта описана как «создаваемое и учитываемое посредством применения информационно-телекоммуникационных технологий имущество, не номинированное в валюте РФ или иностранных государств, которое может использоваться неопределенным кругом лиц для осуществления платежей и не является при этом электронным денежным средством» [5]. Вероятно, такое определение связано с тем, чтобы «подогнать» криптовалюту под определение «иного имущества».

Потенциальное создание закона о криптовалютах

Президент Владимир Путин на совещания по цифровым технологиям в финансовой сфере поручил Банку России и правительству разработать законодательное регулирование криптовалют, майнинга и ICO [3].

Основная задача закона — это определение правового статуса криптовалюты. На основании этого будет построена вся правовая база.

Однако уже сейчас нет единой точки зрения о том, какой же должен быть статус криптовалюты. Министерство финансов РФ предлагает приравнять криптовалюту к финансовому активу, а его использование будет доступно только для участников регулируемой биржи [10]. Это означает ограниченное хождение криптовалюты.

Руководитель рабочей группы Госдумы по оценкам риска оборота криптовалюты Элина Сидоренко не согласна с этой инициативой Министерства финансов. Ее предложение заключается в том, чтобы криптовалюте дать определение «цифрового актива» или «цифрового товара», что, однако, является достаточно размытым. В таком случае, криптовалюта будет близка по правовому статусу к ценным бумагам и облагаться налогами в соответствии с существующей практикой налогообложения ценных бумаг [4].

Стоит отметить, что Россия пока еще не пошла по пути легализации криптовалюты, так как до сих пор не решенным остается вопрос организации законодательной базы, которая будет эффективно регулировать новые цифровые технологии. Как отмечает, Минбалеев А.В. в процессе планирования и определения регуляторных механизмов развития цифровой экономики, в том числе и криптовалют, государство не определилось с ролью и возможностями тех или иных регуляторов, которые необходимы для развития цифровой экономики. Фактически происходит попытка законодательного регулирования на основе анализа зарубежного опыта, но без учета национальной системы и технологий правотворческого процесса [9, с. 31–36]. Также, Чубукова С.Г. отмечает необходимость принятия федерального закона, определяющего основные понятия и принципы правового регулирования цифровой экономики, особенности осуществления основных видов деятельности в цифровой экономике, права и обязанности ее участников, виды и объекты правоотношений, виды ответственности субъектов правоотношений в цифровой экономике и механизмы ее реализации, вопросы юридической значимости цифровых данных и другие [14, с. 67–72].

Биткоин — это очень противоречивое явление, одни видят в нем будущее, другие считают «злом». В любом случае, появление Биткоина очень важный этап в развитии денежной системы, поскольку это первый удачный пример криптовалюты, получивший широкое распространение в мире.

Есть ли у Биткоина будущее — вопрос спорный. Одно можно сказать точно — криптовалюты появились вследствие длительной эволюции денег, которая исключила неперспективные и оставила лучшие варианты. Криптовалюты на данный момент находятся на начальной стадии своего развития, и только история сможет показать, насколько перспективной является данная ветвь эволюции денежной системы.

Список литературы

1. Гражданский кодекс Российской Федерации (часть первая) от 30.11.1994 № 51-ФЗ (ред. от 09.03.2021) // Собрание законодательства РФ. — 1994. — № 32. — Ст. 3301.
2. Федеральный закон от 27.06.2011 № 161-ФЗ (с изм. и доп., вступ. в силу с 01.01.2021) «О национальной платежной системе» // Собрание законодательства РФ. — 2011. — № 27. — Ст. 3872.
3. Перечень поручений по итогам совещания по вопросу использования цифровых технологий в финансовой сфере (утв. Президентом РФ 21 октября 2017 г. № Пр-2132) // Правовая система «Гарант».
4. «Биткоин в законе»: как в России отрегулируют криптовалюты и ICO [Электрон. ресурс]. — Режим доступа: <https://www.rbc.ru/money/24/10/2017/59ef5de9a794713956b0b5d>.
5. Блокчейн поддержат на словах [Электрон. ресурс]. — Режим доступа: <https://www.kommersant.ru/doc/3475123?gr>.
6. Власов А.В. Криптовалюты как новый вид электронных денег / А.В. Власов // Гуманитарные и социальные науки. — 2012. — № 6 — С. 34–39.
7. Европейский Центральный Банк. Схемы виртуальных валют. — Франкфурт-на-Майне, 2012. — 68 с.
8. Манькова А.О. Криптовалюта: Биткоин и его развитие в современной экономике / А.О. Манькова // Молодежный научный вестник. — 2016. — С. 7.
9. Минбалеев А.В. Трансформация регулирования цифровых отношений / А.В. Минбалеев // Вестник Университета имени О.Е. Кутафина (МГЮА). — 2019. — №12. — С. 31–36.
10. Минфин предложил запретить «обычным людям» покупать криптовалюту [Электрон. ресурс]. — Режим доступа: <https://www.rbc.ru/business/28/08/2017/59a3cd869a7947835e1300d1>.
11. Николайчук О.А. Электронная валюта в свете современных правовых и экономических вызовов / О.А. Николайчук // JOURNAL OF ECONOMIC REGULATION (Вопросы регулирования экономики). — 2017. — Т.8. №1. — С. 142–154.
12. Пряников М.М. Блокчейн как коммуникационная основа формирования цифровой экономики: преимущества и проблемы / М.М. Пряников, А.В. Чугунов // INTERNATIONAL JOURNAL OF OPEN INFORMATION TECHNOLOGIES. — 2017. — Т.5 № 6. — С. 49–55.
13. Теллер А. Биткоин — деньги для всех / А. Теллер. — СПб.: Семиздат, 2016. — 91 с.
14. Чубукова С.Г. Стратегии развития информационного общества и направления развития законодательства / С.Г. Чубукова // Правовая информатика. — 2017. — №2. — С. 67–72.
15. Чубукова С.Г. Становление информационного общества и цифровой экономики в России: направления развития законодательства / С.Г. Чубукова // Инноватика и экспертиза. — 2019. — № 1. — С. 60–70.
16. Arvind Narayanan, Joseph Bonneau, Edward Felten, Andrew Miller, Steven Goldfeder. Bitcoin and Cryptocurrency Technologies. // Princeton: Princeton University Press, 2015. — С. 336.
17. В настоящее время указанный проект Федерального закона (с учетом внесенных изменений) принят как Федеральный закон от 31.07.2020 № 259-ФЗ «О цифровых финансовых активах, цифровой валюте и о

- внесении изменений в отдельные законодательные акты Российской Федерации» // Собрание законодательства РФ. — 2020. — № 31 (ч. I). — Ст. 5018.
18. **Ершова И.В.** Майнинг в цифровой экономике: проблемы правовой квалификации и регулирования / И.В. Ершова // Цифровая экономика: концептуальные основы правового регулирования бизнеса в России: моногр. / отв.ред. В.А. Лаптев, О.А. Тарасенко. — М.: Проспект, 2020. — С. 281–288.
19. **Михайлов А.В.** Проблемы становления цифровой экономики и вопросы развития предпринимательского права / А.В. Михайлов // Актуальные проблемы российского права. — 2018. — №11(96). — С. 68–70.
20. **Сушкова О.В.** Смарт-контракты как вид электронной сделки в коммерческом обороте / О.В. Сушкова // Современные проблемы коммерческого права России: сб. ст. XV Междунар. науч.-практ. конф. «Современные проблемы коммерческого права России» / под ред. Е.А. Абросимовой, Б.И. Пугинского. — М.: Юрист, 2019. — С. 76–83.

ПРИЛОЖЕНИЕ «ПО ТУ СТОРОНУ»

APPLICATION "ON THAT SIDE"

**Жандармова
Евгения Александровна**

*Магистрант 1-го курса юридического факультета
РГУ «Нефти и газа»*



**Zhandarmova
Evgenija Aleksandrovna**

*1st year master's student of the Faculty
of Law of the Russian State University "Oil and Gas"*

**Сорокин
Алексей Юрьевич**

*Преподаватель кафедры информатики
и вычислительной техники Академии гражданской
защиты МЧС России*



**Sorokin
Aleksej Jur'evich**

*Lecturer at the Department of Informatics and Computer
Engineering of the Academy of Civil Protection
of the Ministry of Emergency Situations of Russia*

Аннотация: работа посвящена научно-творческому проекту «по ту сторону». Проект представляет собой цифровую площадку обмена мнениями и опытом. Сам сервис выполняет две функции — удовлетворение потребности людей в упорядоченной информации, а также является источником статистических данных общественного мнения.

Ключевые слова: проект, информационные технологии, искусство.

Abstract: the work is devoted to the scientific and creative project "on the other side". The project is a digital platform for the exchange of views and experiences. The service itself performs two functions — meeting people's need for ordered information, and is also a source of statistical data on public opinion.

Keywords: project, information technology, art.

Введение

Одной из важнейших механизмов социально-демократического государства является учет и сбор общественного мнения. К сожалению, данный вид деятельности имеет свои проблемы, связанные с социально-политическими процессами во многих странах. О проблемах достоверности статистических исследований общественного мнения говорили в разные времена [1, 2]. Так же стоит отметить некоторое недоверие ВЦИОМ со стороны граждан РФ.

Второй не менее важной проблемой в настоящее время, является социальная разобщенность [3]. Демассификация информации в современном обществе не минуемо приводит к тому, что отдельные индивиды утрачивают объективное понимание общественных взглядов и норм [4].

С одной стороны, разнообразие социальных сетей и цифровых площадок социальной коммуникации должны были бы решить эту проблему, однако на деле, под действием товарно-рыночных и маркетинговых

интересов, данные ресурсы утрачивают свою целевую функцию. Данные площадки так же начинают делиться на группы и сообщества по «интересам».

Решением данных проблем может послужить цифровая площадка социальной коммуникации на принципиально новой концепции, которая с одной стороны позволит не допустить информационный «мусор», с другой сохранить финансовую независимость.

Идея приложения «по ту сторону»: описание для обычного пользователя

В детстве мы смотрели в эту темную бесконечную гладь, пытаясь понять ее суть и представить в ней себе нечто далекое, никому неведомое. Нас пугала ее таинственность и завораживала одновременно. Становясь старше наши фантазии становились более детальными: самолеты, космические корабли, неизведанные земли, далекие планеты, НЛО, инопланетяне, чужие галактики, теория Большого взрыва и постоянной энтропии... Мы возводим к нему руки в периоды грусти и печали, гордости и славы и великой радости и счастья... задаем ему вопросы, на которые никто не может ответить, посылаем ему эмоции гнева и всхлипы надежды... и ждем... что ответ придет... что внезапно упадет звезда, и мы загадаем желание, которое обязательно сбудется...

Ну а теперь немного поговорим. И не без доли самолюбия начну говорить сразу о себе. С самого введения. Когда меня спрашивают о том, чего я не знаю, каковы мои дальнейшие действия? Думаю, у Вас наверняка получилось отгадать. Да, я гуглю. В глобальной сети найдутся ответы на все вопросы. Используются те же механизмы, что и при живом общении, самое главное — грамотно задать вопрос. А неудовлетворяющий полученный ответ на него уже следствие твоего неправильно заданного вопроса. Но, согласитесь, не на все вопросы глобальная паутина поможет нам ясно дать ответ. И вот ты уже который час сидишь и ищешь что-то толковое по запросу как похудеть за один день, но ничего тебе не подходит. Ладно, можно уточнить вопрос, добавив свои основные показатели: рост и вес, тип внешности, свойства личности, особенности развития и тип мышления, относящийся к одному из известных психотипов... Как на такой длинный запрос отреагирует гугл? Скорее всего, даст ссылку на один из заброшенных форумов известной социальной сети, сайта субкультуры или санатория по борьбе с маниакальными зависимостями? Сколько придется потратить времени и сил, чтобы подобрать необходимую информацию и выстроить между отдельными ее элементами нейронные связи? А если цель вопроса, не была ее сутью? Может быть, просто, необходима была поддержка, взгляд со стороны на проблему, взгляд человека, не имеющего к твоей ситуации, к тебе, уже сформированного предвзятого мнения или назначенной жизнью социальной роли... Нам иногда нужен, просто, трезвый взгляд со стороны...

В какие бы сообщества и кружки по интересам мы не объединялись, мы разные. Со своей историей,

трудным детством, своими поисками пути... А нас здесь более 7 миллиардов. Даже, если предположить, что у двух близнецов случилась идентичная жизненная ситуация одновременно... их реакция на него, их эмоции и последующий усвоенный опыт будет различен... Ну, обобщив глобально: все мы учились когда-то ходить, всем нам было 10 лет, большинство из нас воспитывались в детских садах, закончили школу и поступили в институт, каждый думает, что создаст семью и у него будут дети... но даже имея совершенно одинаковый набор элементов, наши эмоции, наш опыт от ситуации будет уникален. Мы уникальны. Каждый из нас — это Вселенная. В которой существуют свои звездные системы и вращаются по заданным орбитам планеты. Какие-то из этих планет заселены, возможно, даже разумными существами... клетка нашего организма — это Вселенная и часть еще большей Вселенной — нашего тела. Так человек является частью общества Земли. А Земля частью Солнечной системы, а Солнечная система частью Млечного пути... микрокосмос, макрокосмос... Стойте, я начинаю уходить от сути...

Как клетка понимает (и то понимать, еще не значит осознавать, что творится внутри ее системы, так и человек знает только свои чувства и мысли... как гласит русская пословица: «Чужая душа — потемки»... Но суть не в том, чтобы познать «чужую душу», а в том, чтобы познать себя. Варясь в собственном котле страхов, переживаний и впечатлений, имея за плечами только усвоенный опыт, о котором периодически от перепадов атмосферного давления напоминают шишки на лбу, стараться объективно подойти к решению вопроса... объективно невозможно.

Как клетки связаны между собой являясь частью, например печени, также рука является частью тела, также и люди живущие на Земле тесно друг с другом связаны, так как являются частью единого живого организма. Еще К.Г. Юнг говорил об этом в своей теории Коллективного бессознательного К.Г. Юнга или Станислав Гроф в гипотезе единого информационного поля.

В процессе развития человечества, по каким типам нас только не разделяли: мы рационалы и иррационалы; правши и левши; кинестетики, визуалы, аудиалы; эндоморф, мезоморф и эктоморф; мыслители и художники; активные и пассивные; холерики, флегматики, меланхолики и сангвиники; интроверты и экстраверты... Мы живем в разных городах и странах, у нас разный цвет кожи, разные вкусовые предпочтения в музыке, одежде, еде... принадлежим разным социальным слоям и политическим партиям... Скажите, ведь иногда, просто, интересно, как бы на нашем месте поступил другой человек.

Поэтому «По ту сторону» — приложение, позволяющее расширить наше сознание на частичку чужого опыта. Позволит проследить эту простую закономерность причины и следствия, которую прожила другая личность. Позволит посмотреть на себя, на свою проблему задачу или, просто, на сегодня или погоду за окном глазами другого, соприкоснуться с другой Вселенной.

Приложение «По ту сторону»: функциональное описание

Тема приложения: космос. Вступительный экран заставки и авторизация — создание звезды. Перед созданием звезды на экране высвечивается сообщение наподобие пользовательского соглашения, в соответствии с которым:

«Создавая свою звезду, ты даешь свое согласие и принимаешь на себя всю ответственность за свои мысли и действия в развитии нашей общей звездной системы. Ты осознаешь причинно-следственную связь всего и понимаешь, что твои действия могут кардинальным образом изменить равновесия действующий в нашей системе сил и создание либо разрушение отдельный ее частей, таких же ярких звезд, как ты».

Человек авторизуется в приложении, создавая логин и пароль. Логин — является названием звезды. При регистрации анкету заполнять с данными не нужно. В дальнейшем при интересе к приложению к звезде пользователь может приписывать ряд характеристик, которые позволят выгружать статистические отчеты.

В итоге каждый пользователь делится при авторизации только своим номером телефона и фантазийным именованием себя — своей

Дальше на фоне космоса высвечивается кнопка: послать запрос в космос. Пользователь нажимает ее и вводит свой вопрос/описание ситуации. При необходимости прикладывает фотографию.

Его вопрос случайным образом приходит к 5 пользователям, авторизованным в системе (пуш-уведомление). Пользователь, к которому пришел запрос, для развития Вселенной и по кодексу «рыцаря», считает своим долгом выразить свое мнение и помочь союзной звезде в разрешении жизненной трудности.

За заданные вопросы и направленные ответы пользователи повышают рейтинг своих звезд. Пользователи также могут оценивать ответы и вопросы друг друга. В дальнейшем можно будет проработать вопрос кастомизации звезд за полученные пользователями баллы.

Механизм приложения довольно прост. Но, чем проще изложена информация, тем меньше у мозга ее обрабатывающего, воспринять ее с искажением.

Приложение «По ту сторону»: научная и экономическая сторона

С научной точки зрения, в вопросах психологии, социологии, политологии и экономики, существующий банк данных ответов и вопросов пользователей может представлять весьма большой интерес. Фактически, существующая потребность в таких банках данных может обеспечить данному приложению полную финансовую самодостаточность, при это не допустить влияния маркетологов, политиков и предпринимателей.

Приложение «По ту сторону»: визуальное оформление

Визуальное оформление приложения — космос. Некоторые дизайнерские решения представлены на рис. 1.

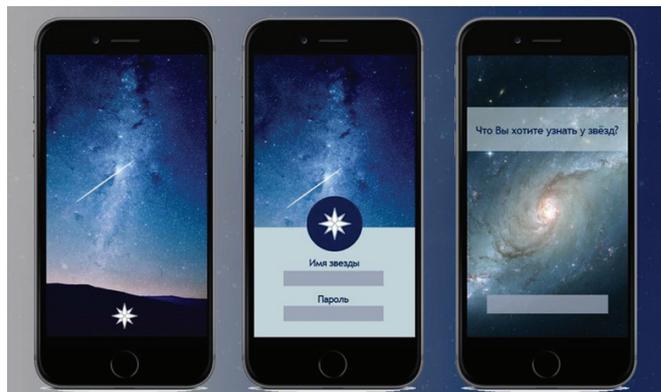


Рис. 1 Визуальная тема приложения

Заключение

Данное приложение при разработке и поддержке инфраструктуры не требует больших ресурсов, однако при правильной подаче, способно принести не мало плодов. Так для простого пользователя открываются следующие возможности, при полном отсутствии «не нужной», «мусорной» информации:

1. Получение независимого мнения со стороны по интересующему вопросу;
2. Удовлетворение потребности в желании «помочь», анонимное волонтерство. Своей оценкой ты помогаешь другому человеку;
3. Участие, ощущение сопричастности себя к общей системе, ощущение себя частью и счастья;
4. Самопознание через переживание чужого опыта. Рефлексия самосознания.

При этом для владельцев цифровой платформы открывается возможность ведения этичной деятельности приносящей приличных доход на торговле информацией.

Список литературы

1. Туманов С.В. К вопросу об изучении общественного мнения в России / С.В. Туманов, А.Т. Гаспаришвили // Социально-гуманитарные знания. — 2010. — №3.
2. Проблемы достоверности статистической информации в социологических исследованиях / В.Э. Шляпентох. — М.: Статистика, 1973. — 144 с.
3. Евенко С.Л., Бардаков Р.И. Механизмы профилактики социальной разобщенности в курсантских коллективах военных организаций высшего образования: управленческий дискус / С.Л. Евенко, Р.И. Бардаков // Медицина. Социология. Философия. Прикладные исследования. — 2020. — №6.
4. Тоффлер Э. Третья волна / Э. Тоффлер // Народное образование. — 2008. — №2. — С. 55–61.

NFT КАК ЦИФРОВАЯ ИННОВАЦИЯ В АВТОРСКОМ ПРАВЕ

NFT AS A DIGITAL INNOVATION IN COPYRIGHT

Яковлев Роман Игоревич

Студент 2-го курса магистратуры IT Law Московский государственный юридический университет имени О. Е. Кутафина (МГЮА)



Jakovlev Roman Igorevich

2nd year student of IT Law Moscow State Law University named after O. E. Kutafin (MSLA)

Сушкова Ольга Викторовна

Кандидат юридических наук, доцент, Московский государственный юридический университет имени О.Е. Кутафина (МГЮА)



Sushkova Ol'ga Viktorovna

Candidate of Legal Sciences, Associate Professor, Moscow State Law University named after O.E. Kutafina (Moscow State Law Academy)

Аннотация. NFT (аббревиатура с англ. Языка «non-fungible token») — это создаваемые на основе технологии блокчейн криптографические токены, каждый из которых является уникальным и не может быть заменён или замещён на другой аналогичный токен. На основании изучения практического опыта было выяснено, как NFT помогут развить авторское право.

Ключевые слова: NFT, блокчейн, обмен данными, авторское право, цифровое искусство.

Abstract. NFT (abbreviation from the English language "non-fungible token") are cryptographic tokens created on the basis of blockchain technology, each of which is unique and cannot be replaced or substituted for another similar token. Based on the study of practical experience, it was found out how NFTs will help develop copyright.

Keywords: NFT, blockchain, data exchange, copyright, digital art.

В данный момент в мире набирают популярность так называемые NFT. Какие же преимущества они имеют перед традиционными формами хранения и передачи данных и какое отражение находят в авторском праве? Актуальность данной темы определяется динамичным развитием цифровых технологий и законодательства, в том числе и авторского.

Целью представленной работы являлось изучение NFT как инновационной формы хранения и передачи данных и выявление степени полезности закрепления в авторском законодательстве. Необходимо было решить ряд задач: 1) ознакомиться с историей появления NFT 2) дать определение основным понятиям; 3) выявить основные достоинства и преимущества NFT; 4) раскрыть принципы работы системы; 5) привести примеры применения.

Говоря об NFT, нельзя обойти стороной тему блокчейна и криптовалют, ведь важное условие существования NFT — работа на блокчейне, то есть на представляющем собой цепочку блоков информации децентрализованном коллективном реестре цифровых транзакций, которые хранятся, одновременно соз-

даются и обновляются на всех носителях у всех участников реестра на основе заданных криптографических алгоритмов, обеспечивающих ее тождественность у всех пользователей реестра. На блокчейне одновременно могут сосуществовать множество различных токенов разного количества, однако в классическом понимании в открытом блокчейне эти токены равны друг другу, тождественны, взаимозаменяемы. Возьмем для примера всеми известный биткоин: каждый выпущенный отдельно взятый биткоин равен другому биткоину. Но технология non-fungible token (NFT) работает иначе. Каждый невзаимозаменяемый токен является уникальным, его нельзя подделать, разделить или незаметно заменить другим. Такая организация позволяет закрепить свои права на какой-либо уникальный объект, будь то произведение искусства в ограниченном тираже или вовсе в единственном экземпляре, предмет в цифровом мире или компьютерной игре и даже недвижимость. Стоит также отметить, что NFT — это не сам объект искусства, а лишь токен в системе блокчейн, который подтверждает право собственности на такой объект [Савельев 2017: 41].

Первые NFT связывают с появлением таким решений, как Colored coins (в 2013 году) и Counterparty (в 2014 году), сделавших возможным токенизацию активов на блокчейне. Позже в 2017 году начали появляться самостоятельные проекты, на которых пользователи могли приобретать и обмениваться различными пиксельными портретами, картинками и гифками. Такими проектами были Rare pepe Directory и CryptoPunks. Широкое распространение NFT получили благодаря проекту CryptoKitties, запущенному в ноябре 2017 года. Платформа давала возможность пользователям «разводить» виртуальных котиков, путем скрещивания двух других в форме NFT, что позволяло получить «потомство» в виде нового уникального цифрового объекта разной степени редкости, который можно было оставить себе или продать. На сегодняшний день индустрия NFT — это огромный рынок цифровой собственности с оборотом более 500 млн. долларов США и продолжает расти.

Большинство NFT выпускаются на основе Ethereum в нескольких основных стандартах. Стандартизация выпуска дает возможности блокчейнов взаимодействовать друг с другом, что позволяет передавать такие невзаимозаменяемые токены между различными децентрализованными приложениями.

ERC-721. Первая и самая простая реализация NFT на Ethereum, расширяющая возможности базового стандарта ERC-20. В ней каждый тип токенов требует отдельного смарт-контракта.

ERC-875. Доработанная версия стандарта ERC-721, дающая возможность отправлять несколько NFT одной транзакцией.

ERC-1155. Усовершенствованный стандарт, позволяющий работать сразу с несколькими типами токенов через один смарт-контракт. На таком контракте одновременно могут находиться и NFT, и обычные токены.

NFT создаются не только на Ethereum, они также существуют в сетях Neo, Tron, EOS, Flow, Wax, Cosmos и других платформах. Разные блокчейны являются друг другу не столько конкурентами, сколько партнерами, которые вместе развивают данную индустрию, создавая единые стандарты и кросс-чейн платформы. Более того, в этом также принимают участие непосредственно и деятели данного рынка, в лице компаний, занимающихся разработкой различных цифровых продуктов, такие как, например, Ubisoft. Это говорит о заинтересованности реального бизнеса в развитии и внедрении данной технологии.

Далее рассмотрим преимущества, которые предлагают NFT.

Прозрачность. Создавая эксклюзивный дефицитный набор данных в NFT, мы устраняем необходимость некой третьей стороны давать экспертизу тому или иному объекту, оценивая его подлинность, время создания и прочие параметры. Эту функцию берёт на себя блокчейн, благодаря надежной децентрализованной криптографии.

Удобство пользования. При приобретении и владении NFT нет необходимости в подписании и

хранении каких-либо правоустанавливающих документов [6]. Кроме того, сами документы можно обернуть в NFT, что упрощает процесс их предоставления. Так, например, протокол Bridge через NFT предоставляет доступ к единой цифровой идентичности для верификации, управления и передачи своих персональных данных.

Надежность. Благодаря технологии блокчейн, на которой базируются NFT, удаление или изменение информации о владении такими токенами не представляется возможным [Цихилов 2019: 23]. Множественное дублирование данных среди ее участников гарантирует сохранность и неизменность внесенной в реестр информации. Более того, из-за специфики устройства блокчейна данную информацию невозможно подменить, отредактировать или удалить. А применение алгоритмов консенсуса говорит о том, что все транзакции, включенные в блокчейн, являются подтвержденными.

Быстрота. Во многих странах мира, в том числе и в России существуют процедуры регистрации авторских прав. Эти процедуры как правило требуют немалых временных, бумажных и иных усилий. В случае с NFT время ожидания сокращается до нескольких кликов и одного платежа.

Таким образом, нельзя не признать, что цифровые технологии настолько прочно вошли в нашу повседневную жизнь, что постепенно происходит оцифровка большого количества информации, которая ранее передавалась через физические носители [7]. Электронные деньги и электронный документооборот оказались лишь только началом. Появление NFT вовсе не случайно. Человечество вступило в эпоху цифровых прав, а это означает появление и цифровых объектов, на которые распространяются эти права. Такими объектами сейчас являются различные произведения искусства (картины, музыка), предметы коллекционирования (карточки, фигурки, предметы), а также практически любые предметы виртуальной реальности и компьютерных игр. NFT за счет децентрализованной, прозрачной и надежной криптографии готово стать новой вехой в авторском праве, поскольку с каждым днем все больше и больше обрабатываемой нынешним поколением людей информации сосредотачивается в Сети.

Список литературы

1. Савельев А.И. Криптовалюта в системе объектов гражданских прав / А.И. Савельев // Закон. 2017. № 8. С. 136-153.
2. Цихилов А. Блокчейн. Принципы и основы / А. Цихилов. — М.: Альпина паблишер, 2019. — 180 с.
3. Шерстобитов С. Цифровизация экономики. БИТ. Бизнес&Информационные Технологии [Электрон. ресурс] / С. Шерстобитов. — Режим доступа: <http://bit.samag.ru/uart/more/67> (дата обращения 08.03.2021).
4. Словари и энциклопедии. Академик [Электрон. ресурс]. — Режим доступа: <https://dic.academic.ru/>.
5. Blockchain revolution: how the technology behind bitcoin is changing money, business, and the world [Электрон.

- ресурс]. — Режим доступа: <https://www.amazon.com/Blockchain-Revolution-Technology-Changing-Business/dp/1101980133> (дата обращения 08.03.2021).
6. Михайлов А.В. Проблемы становления цифровой экономики и вопросы развития предпринимательского права / А.В. Михайлов // Актуальные проблемы российского права. — 2018. — №11(96). — С. 68–70.
7. Сушкова О.В. Влияние интеллектуальных систем на развитие условий реализации экономических прав граждан в цифровой среде / О.В. Сушкова // Правовая защита интеллектуальной собственности: проблемы теории и практики: сб. материалов IX Международ. юридич. форума (IP Форума). — М.: ИЦ Ун-та им. О.Е. Кутафина (МГЮА), 2021. — С. 282–287.

МОШЕННИЧЕСТВО В ИННОВАЦИОННОЙ СРЕДЕ

FRAUD IN AN INNOVATIVE ENVIRONMENT

Костюк Михаил Федорович

Доктор юридических наук, профессор, профессор кафедры экономических и финансовых исследований ВШГА МГУ имени М. В. Ломоносова



Kostjuk Mihail Fedorovich

Doctor of Law, Professor, Professor of the Department of Economic and Financial Investigations of the Higher School of Economics, Lomonosov Moscow State University

Василихина Юлия Владимировна

Студентка 2-го курса Высшей школы государственного аудита Московский государственный университет имени М.В. Ломоносова



Vasilihina Julija Vladimirovna

2nd year student of the Graduate School of State Audit, Moscow State University named after M.V. Lomonosov

Аннотация: развитие компьютерных и информационно-телекоммуникационных технологий имеет положительные стороны, но в то же время порождает и негативные последствия, выраженные в возникновении новых видов мошенничества, посредством использования технологических достижений современности. В связи с чем возникает необходимость криминализации противоправных деяний, причиняющих вред объекту посягательства и внесения изменений в законодательные положения, которые позволят правоприменителю едино толковать существующие уголовно-правовые нормы, посвященные мошенничеству, что надлежит рассмотреть в данной статье.

Ключевые слова: мошенничество, информационные технологии, инновационное мошенничество.

Abstract: The development of computer and information and telecommunication technologies has positive aspects, but at the same time generates negative consequences, expressed in the emergence of new types of fraud, through the use of modern technological achievements. In this connection, it becomes necessary to criminalize unlawful acts that harm the object of encroachment and amend the legislative provisions that will allow the law enforcement officer to unify the interpretation of the existing criminal law norms on fraud, which should be considered in this article.

Keywords: fraud, information technology, innovative fraud.

Развитие инновационных технологий в современном обществе имеет значительную роль, поскольку позволяет улучшить качественные показатели жизнедеятельности человека. Однако, стоит отметить, что прогресс в той или иной сфере имеет и обратную сторону. Развитие инновационных, а в частности, компьютерных и информационно — телекоммуникационных технологий является основной для зарождения ранее не существовавших преступных посягательств. Важным является замечание и о том, что «высокие

технологии» — это не только лишь компьютеры, но и иные специальные технологии, предоставляющие возможность негласного получения информации, развитие и внедрение которых имеет значительные темпы, что расширяет возможности их использования в преступных целях [1]. Исключением тому не стало и мошенничество, что породило необходимость криминализации его квалифицированных видов в уголовном законодательстве Российской Федерации.

До 29 ноября 2012 года данная сфера правоотношений оставалась законодательно неурегулированной, в следствие чего мошенничество в сфере компьютерной информации квалифицировалось по статье 159 УК РФ как «хищение чужого имущества или приобретение права на чужое имущество путем обмана или злоупотребления доверием», что не соответствовало характеру и степени общественной опасности преступления и личности виновного, а то есть противоречило целям наказания, применяемого к лицу, совершившему преступления в соответствии с положениями ст. 43 УК РФ [2]. Однако Федеральным законом от 29.11.2012 № 207 «О внесении изменений в Уголовный кодекс Российской Федерации и отдельные законодательные акты Российской Федерации» [3] в уголовное законодательство были внесены изменения, направленные на дифференциацию различных видов мошенничества, в том числе в сфере экономической деятельности. В частности, уголовный закон был дополнен ст. 159¹ — 159⁶ УК РФ, которые предусмотрели ответственность за мошенничество, совершаемое в сфере кредитования, предпринимательской деятельности, страхования, компьютерной информации, а также при получении выплат или использования платежных карт [4], что позволило правоприменителю производить более точную уголовно-правовую оценку конкретного общественно-опасного деяния, но вместе с тем вызвало острую дискуссию в научном сообществе, в силу отсутствия устойчивой и однородной правоприменительной практики.

Особое значение для данного исследования имеет ст. 159⁶, посвященная мошенничеству в сфере компьютерной информации, а то есть «хищению чужого имущества или приобретению права на чужое имущество путем ввода, удаления, блокирования, модификации компьютерной информации или информационно-телекоммуникационных сетей», состав которого для полноты исследования следует рассмотреть далее.

Диспозиция ст. 159⁶ имеет бланкетный характер и требует привлечения дополнительной информации из сопутствующего законодательства РФ для установления признаков состава преступления. Основным непосредственным объектом рассматриваемого преступления выступают общественные отношения, связанные с отношениями собственности независимо от ее формы, дополнительным — правоотношения обеспечивающие информационную безопасность. Предметом данного преступления является чужое имущество, право на чужое имущество, а также компьютерная информация, используя которую виновное лицо достигает преступных целей. В свою очередь «компьютерной информацией» согласно примечанию к ст. 272 УК РФ являются «сведения (сообщения, данные), представленные в форме электрических сигналов, независимо от средств их хранения, обработки и передачи». Объективная сторона выражена общественно опасными деяниями в виде хищения чужого имущества или приобретения прав на него, общественно-опасным последствием в качестве при-

чинения имущественного ущерба собственнику и причинно-следственной связью между ними. Дополнительным признаком объективной стороны выступает способ совершения преступления, характеризующийся альтернативно как: ввод, удаление, блокирование, модификация компьютерной информации, а также вмешательство в функционирование средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей [5]. Следовательно, по конструкции объективной стороны состав является материальным. Согласно п. 5 Постановления Пленума Верховного суда РФ № 48 от 30.11.2017 «О судебной практике по делам о мошенничестве, присвоении и растрате» преступление считается оконченным с момента, «когда имущество поступило в незаконное владение виновного или других лиц и они получили реальную возможность пользоваться или распорядиться им по своему усмотрению». Субъективная сторона характеризуется прямым умыслом и корыстным мотивом, а то есть стремлением получить материальную выгоду. Субъектом преступления выступает вменяемое физическое лицо, достигшее возраста шестнадцати лет.

Важным является замечание о том, что данные преступные деяния являются наиболее распространенными в преступной среде, чему свидетельствуют статистические данные преступности, приведенные Министерством внутренних дел за январь-февраль 2021 года. Так, за данный отчетный период число преступлений, совершенных мошенническим путем в сфере компьютерной информации возросло на 51,9%, в том числе — на 48,3% с использованием сети «Интернет» и на 32,6% с использованием средств мобильной связи по сравнению с показателями предшествующего периода [6]. Актуальность данной нормы обусловлена и наличием проблем в квалификации преступлений, совершенных путем мошенничества в сфере компьютерной информации, а также отсутствием единообразного подхода в применении судами нормы, предусматривающей ответственность за данное преступление, что вызывает острые дискуссии в научной среде.

Так, М.В. Андрианов считает необоснованным необходимость выделения данного состава преступления, поскольку рассматриваемое деяние является лишь одним из способов совершения мошенничества [7]. Противоположного мнения придерживается В.М. Елина, которая считает необходимым криминализацию компьютерного мошенничества, поскольку это дает возможность Российской Федерации принимать участие в мировых интеграционных процессах в сфере борьбы с киберпреступностью. Ряд авторов придерживается мнения о том, что данная норма должна предусматривать ответственность за хищение вне зависимости от способа, если при этом используется несанкционированное вмешательство в функционирование средств хранения, обработки или передачи компьютерной информации или информационно-телекоммуникационных сетей [8]. Другие же

ученые, в частности И.А. Александрова считает, что данное деяние следует квалифицировать как кражу, поскольку компьютер — не физическое лицо, а фактически устройство, как и банкомат [9].

Не имеет единообразного подхода в применении данной нормы и правоприменитель, который сталкивается с определенными трудностями в квалификации хищения с использованием компьютерной информации, в следствие чего однородным преступным деяниям даются различные правовые оценки в виде кражи, общего мошенничества или мошенничества в сфере компьютерной информации, подтверждением чему судебная практика.

Так, согласно обвинительному приговору Октябрьского районного суда Ханты-мансийского автономного округа от 17 декабря 2013 года, лицо, используя забытый пассажиром в салоне мобильный телефон и содержащуюся в нем систему «Телекард», перечислило денежные средства, находящиеся на балансе счета потерпевшего, открытого в ОАО «Газпром», на баланс своего мобильного телефона и на свой электронный кошелек «Яндекс.Деньги», в следствие чего было признано судом виновным по ч.1 ст. 158 УК РФ [10].

В то же время, Железногорский городской суд Курской области, квалифицировал деяния лица, которое используя мобильный телефон, посредством услуги «Мобильный банк», подключенной предыдущим владельцем ФИО7 для доступа к банковскому счету ПАО «Сбербанк» и посредством отправления специального сообщения на номер «900», незаконно осуществило снятие со счета банковской карты, оформленной на ФИО7, денежных средств, которые посредством услуги «Мобильный банк» были автоматически зачислены на счет виновного по ч.2 ст.159.6 УК РФ [11].

Подводя итоги всему вышесказанному, становится очевидным, что рассматриваемая норма требует должного внимания со стороны законодателя, поскольку существует ряд проблем в ее применении, поскольку зачастую суды однородные преступные деяния квалифицирует различно, как общее мошенничество, кражу или мошенничество в сфере компьютерной информации. Также остается неразрешенным вопросом о том, что считать вмешательством в функционировании средств хранения, обработки или передачи компьютерной информации или информационно-телекоммуникационных сетей. Негативная тенденция в правоприменительной практике подлежит устранению, так как отсутствие единого подхода в применении нормы, предусматривающей ответственность за совершение мошенничества в сфере компьютерной информации, в том числе неблагоприятно влияет на авторитет судебной системы Российской Федерации. Вследствие чего, видится воз-

можным, разрешить данную ситуацию посредством более подробных разъяснений Верховного суда РФ о критериях отграничения данного состава от смежных составов преступления, а в частности, путем внесения их в Постановление Пленума Верховного суда РФ № 48 от 30.11.2017 «О судебной практике по делам о мошенничестве, присвоении и растрате».

Список литературы

1. Мазуров А.В. Преступность в сфере высоких технологий: понятие, общая характеристика, тенденции / А.В. Мазуров // Вестник Томского государственного университета. — 2007. — № 2. — С. 151–154.
2. Федосенко В. Цена высоких технологий. Гендиректор подозревается в присвоении двух миллионов евро / В. Федосенко // Российская газета. — 2008. — 22 апр.
3. Федеральный закон от 29.11.2012 № 207 «О внесении изменений в Уголовный кодекс Российской Федерации и отдельные законодательные акты Российской Федерации» // СПС «Консультант плюс».
4. Обзор судебной практики по применению ФЗ от 29.11.2012 № 207-ФЗ «О внесении изменений в Уголовный кодекс Российской Федерации и отдельные законодательные акты Российской Федерации» и постановления Государственной Думы Федерального Собрания РФ от 02.07.2013 № 2559 ГД «Об объявлении амнистии» // СПС «Консультант плюс».
5. Журавлева Г.В. Мошенничество в сфере компьютерной информации: спорные вопросы теории и практики / Г.В. Журавлева, Н.А. Карпова // Вестник москов. ун-та МВД России. 2017. С. 153–158.
6. МВД РФ, ФКУ «Главный информационно-аналитический центр» Состояние преступности в России за январь-февраль 2021 года [Электрон. ресурс]. — Режим доступа: <https://мвд.рф/>.
7. Андрианов М.В. Новые способы мошенничества в УК РФ / М.В. Андрианов // Вестник ВлГУ. — 2013. — № 9. — С. 63.
8. Иванченко Р.Б. Проблемы квалификации мошенничества с использованием информационных технологий / Р.Б. Иванченко, А.Н. Малышев // Уголовное право. — 2015. — № 5. — С. 131–134.
9. Александрова И.А. Новое уголовное законодательство о мошенничестве / И.А. Александрова // Юридическая наука и практика. Вестник Нижегородской академии МВД России. — 2013. — № 21. — С. 54–62.
10. Обвинительный приговор Октябрьского районного суда Ханты-Мансийского автономного округа от 17.12.2013 [Электрон. ресурс]. — Режим доступа: <https://sudact.ru/>.
11. Обвинительный приговор Железногорского городского суда Курской области по делу № 1-243/2014 от 21.10.2014 г. [Электрон. ресурс]. — Режим доступа: <https://sudact.ru/>.

КОНЦЕПЦИИ ПОДХОДА К УНИФИКАЦИИ КРИТИЧЕСКИ ВАЖНЫХ СИСТЕМ И ПРОЦЕССА ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ

CONCEPTS FOR AN APPROACH TO UNIFICATION OF CRITICAL SYSTEMS AND THE SAFETY PROCESS

Александрова Алина Викторовна

Студент 5-го курса по направлению «Информационная безопасность автоматизированных систем» Московского политехнического университета



Aleksandrova Alina Viktorovna

5th year student in the direction "Information security of automated systems" of the Moscow Polytechnic University

Широков Анатолий Александрович

Студент 5-го курса по направлению «Информационная безопасность автоматизированных систем» Московского политехнического университета



Shirokov Anatolij Aleksandrovich

5th year student in the direction "Information security of automated systems" of the Moscow Polytechnic University

Соболь Дмитрий Викторович

Студент 5-го курса по направлению «Информационная безопасность автоматизированных систем» Московского политехнического университета



Sobol' Dmitrij Viktorovich

5th year student in the direction "Information security of automated systems" of the Moscow Polytechnic University

Бритвина Валентина Валентиновна

Кандидат педагогических наук, доцент кафедры «Инфокогнитивные технологии» Московского политехнического университета, доцент кафедры «Управление и информатика в технических системах» Московского государственного технологического университета «СТАНКИН»



Britvina Valentina Valentinovna

Candidate of Pedagogy, Associate Professor of the Department of "Infocognitive Technologies" of the Moscow Polytechnic University, Associate Professor of the Department of "Management and Informatics in Technical Systems" of the Moscow State Technological University "STANKIN"

Аннотация. Обеспечение безопасности компьютерных систем, которые полагаются на гарантии безопасности и защищенности, такие как согласованность, долговечность, эффективность и доступность, требуют или нуждаются в ресурсах. Это нацелено на проблемы системы систем (SoS), за исключением трудностей и проблем, которые аналогичным образом применимы к взаимодействиям подсистем в отдельной системе и взаимодействиям системы как компонентов в большой информационной системе. Это исследование направлено на обеспечение безопасности и информации для критически важных систем, где вопросы безопасности и защиты рассматриваются до перехода к этапу

Abstract. Securing computer systems that rely on security and safety guarantees such as consistency, durability, efficiency, and availability requires or needs resources. It targets the problems of a system of systems (SoS), except for difficulties and problems that are similarly applicable to interactions of subsystems in a single system and interactions of a system as components in a large information system. This research focuses on providing security and information for critical systems, where security and protection issues are considered prior to moving to the actual implementation / development phase of component systems. This will require a conceptual idea or strategy that addresses the security issues of the application logic. This could indicate a vulnerability in a single

фактического внедрения / разработки компонентных систем. Для этого потребуется концептуальная идея или стратегия, которая касается вопросов обеспечения безопасности логики приложения. Это может показать уязвимость в отдельном компоненте или повторное использование спецификации в существующей логике в компонентной системе. Принимая во внимание эту ситуацию, мы определили семь концепций обеспечения безопасности и стратегии проектирования обеспечения безопасности для критически важных систем.

Ключевые слова: безопасность системы, гарантия работы компонентов, программное обеспечение, критически важное для безопасности, Software Assurance, информационная безопасность.

component, or reuse of a BOM in existing logic in a component system. With this situation in mind, we have identified seven security concepts and security design strategies for mission-critical systems.

Keywords: System security, component assurance, security-critical software, Software Assurance, information security.

Введение

Интеграция компонентов в промышленные системы управления, такие как железнодорожные системы контроля и управления (CCS), продолжается в рамках коммерческого готового аппаратного и программного обеспечения (COTS). Однако использование компонентов COTS в бывшей в использовании инфраструктуре безопасности приводит к новым рискам безопасности. Взаимодействие безопасности — важная область исследования, в которой еще предстоит решить несколько вопросов. Обеспечение безопасности является важной частью процесса разработки критически важного для безопасности программного обеспечения. Недостатки в инфраструктуре также может привести к ошибкам программного обеспечения и злоупотреблениям со стороны хакеров и преступников, стремящихся манипулировать недостатками в технологической отрасли. Тестирование, аккредитация и оценка проводятся для обоснования безопасности логической функции в процессе межкоммуникационного взаимодействия. Эта стратегия применяется на стадии проектирования, что относится к стандартной процедуре для повышения доверия к программе в процессе ее проверки [1].

Внедрение безопасности программного обеспечения в процессе проектирования / разработки было неотъемлемым аспектом общих инноваций современных критически важных систем, начиная от оружия, автомобильных систем управления, промышленных систем управления и медицинского оборудования. Программное обеспечение используется для отслеживания и регулирования физических процессов в этих системах, увеличение количества сбоев или отказов может привести к гибели людей или другим катастрофическим последствиям. Таким образом, обеспечение безопасности программного обеспечения для критически важных систем является одной из основных целей в системе компонентов [2].

Все больше программного обеспечения, включая встроенные системы, больше не предназначено для использования в системах безопасности. Вместо этого

они используются (или повторно используются) для COTS, GOTS Government в готовом виде для программного и аппаратного обеспечения, приложений с открытым исходным кодом и других приложений, не связанных с разработкой, часто без изменений в настройке. Большая часть этого программного обеспечения, не предназначенного для разработки, особенно COTS и программного обеспечения с открытым исходным кодом, является компонентом автономных частей программного обеспечения, которые можно использовать в качестве строительных блоков для создания более крупных и сложных систем программного обеспечения. Наименьшая независимая единица разложения в программной системе может быть или не быть компонентом [3]. В некоторых случаях собираются компоненты с меньшими модулями. Чтобы можно было использовать в качестве компонента более широкой структуры, автономная программа должна предоставлять интерфейс(ы), обычно стандартизированный, чтобы позволить интегрировать или монтировать другие компоненты. В этом случае степень обеспечения безопасности компонентов и безопасности системы является главным приоритетом в обеспечении информации для критически важных для безопасности компонентных программных систем в организации [4].

Самым важным аспектом в обеспечении безопасности компьютерных систем является межкомпонентная спецификация. Взаимодействия между системами могут быть разделены потреблением одного компонента и другого [5].

В этом исследовании мы собираемся рассмотреть влияние безопасности и обеспечения информации на критически важные для безопасности компонентные программные системы, в котором обсуждаются вопросы безопасности и защиты в процессе внедрения и разработки систем.

Метод исследования

В своей исследовательской работе мы использовали прикладной метод исследования. У метода есть подкласс, называемый исследовательской оценкой. В этом

методе мы обращаемся к анализу, и оценочный анализ представляет собой своего рода аналитическое исследование, оценивающее текущие исследовательские знания, которые зависят от результатов эмпирических исследований или принятия обоснованных решений [7], например, научный метод исследования, поскольку он применяет существующие научные знания. Поэтому, имея в виду этот метод исследования, мы предложили семь концепций обеспечения информации для критически важного для безопасности программного обеспечения на основе компонентов.

Предпосылки исследования

Увеличение роста атак, а также очевидный сдвиг в сторону большей уязвимости, по-видимому, означают, что наша способность отражать атаки уменьшается, а разрыв между атаками и защитой информации увеличивается. Большая часть современной информационной безопасности основана на концепциях, определенных Зальцером и Шредером в статье ACM Communications 1974 года, озаглавленной «Безопасность информации в компьютерных системах». Защита была охарактеризована как «методы отслеживания того, кто может получить доступ или изменить устройство или информацию, хранящуюся в нем», и были описаны три ключевые категории проблем: конфиденциальность, целостность и доступность [8].

Мы обеспечиваем безопасность в области кибербезопасности и обеспечения информации для критически важных программных систем на основе компонентов следующим образом: «Программа Software Assurance, рассматриваемая как безопасность, представляет собой степень надежности защиты от программного обеспечения. Некоторые ошибки, преднамеренно или непреднамеренно разработанные, внедряются в программное обеспечение на любом этапе его жизненного цикла, поэтому программное обеспечение работает по назначению».

С распространением уязвимостей за счет программ-вымогателей, ошибок и инъекций структурированного языка запросов (SQL), межсайтовых сценариев и т.д. Эти проблемы изменили структуру и функциональность программы. Оказалось, что полагаться исключительно на защиту личных данных совершенно недостаточно. Кроме того, важность программного обеспечения в сетях возросла так, что теперь программное обеспечение управляет большей частью функциональных возможностей и усиливает эффект отказа системы безопасности [9].

Конвергенция и взаимодействие критически важных систем безопасности становится все более очевидной. Следовательно, имеет смысл создать общую концепцию обеспечения безопасности программного обеспечения, охватывающую безопасность и защиту. Различные методы, предлагаемые нынешними концепциями, возникают из угроз, связанных со сложными структурами [10].

Кроме того, принятие коммерческого готового (COTS) и программного обеспечения с открытым

исходным кодом в качестве модулей, создает дополнительные проблемы для успешной операционной защиты. В результате операционные системы объединяют приложения из самых разных источников и собирают каждую часть по-своему [11].

Системы не могут быть построены так, чтобы устранять риски безопасности, но обладают способностью распознавать атаки, противостоять им и восстанавливаться после них. Система должна быть подготовлена к внедрению и обслуживанию при первоначальном проектировании. Чтобы гарантировать успешную защиту организации с течением времени, доверие должно быть запланировано на весь жизненный цикл [12].

Теперь мы используем следующую концепцию обеспечения жизненного цикла программного обеспечения на основе компонентов, созданную для:

Технологии и процедуры внедрены для получения требуемой степени уверенности в том, что приложения и службы работают должным образом, не имеют непреднамеренных или преднамеренных недостатков и обладают безопасными для угроз функциями защиты, а также восстановления после вторжений и сбоев.

Обзор существующих исследований

В области процесса унификации обеспечения безопасности критически важных для безопасности компонентных программных систем проводится не так много исследований. Тем не менее, мы рассмотрели некоторые важные работы, чтобы процитировать исследовательские работы.

По словам Фейсала Наби 2017, предложенный процесс унификации гарантии безопасности, который определяет защиту.

Автор описывает архитектуру в два этапа абстракции информационной системы.

1) Уровень проектирования метода объясняет форму для уровней архитектурной формы, которые должны быть реализованы на высшем уровне абстракции.

2) Определение архитектуры логической части.

Для обеспечения безопасного развертывания защиту необходимо применять с использованием подхода к проектированию, а не реализации уровня в структуре, путем взаимодействия с вышеупомянутыми основными элементами процесса обеспечения безопасности. Таким образом, архитектура может быть извлечена путем защиты курса протокола доверия [1].

Тим Келли, 2019 объяснил, что альтернативное решение путем создания структуры обеспечения соответствия и обеспечения данных (SSAF) ориентировано на фундаментальный набор стандартов безопасности. Вместо популярного совместного заверения, которое выявляет серьезные недостатки, защита и безопасность должны быть обеспечены индивидуально. Это часто позволяет использовать разные процессы и навыки практиков в каждой области. При таком расположении внимание переключается с простой кон-

вергенции на интеграцию посредством правильного обмена знаниями с синхронизацией в нужное время [3].

По словам Марши Чечик (Б., Рик Салай, Торин Вигер, Сахар Кокали и Мона Рахими, 2019), адреса тестовых случаев, тестовые данные, человеческое решение или их сочетание предоставят данные для обеспечения безопасности программного обеспечения. Это означает, что эксперты стремятся строить (критичные для безопасности) конструкции с осторожностью и выражать это рассуждение в соответствии с хорошо обоснованной методологией в обосновании безопасности, которое в конечном итоге проверяется человеком. Тем не менее, технологии имеют более глубокие корни в неопределенности, наиболее сложные функции открытого мира (например, понимание состояния земли самоуправляемым транспортным средством) часто не совсем предсказуемы или не рентабельны; вычислительные приложения также попадают в опасные условия, и могут возникать несоответствия [2].

Предлагаемая концепция обеспечения безопасности систем, критически важных для безопасности

Компоненты предназначены в первую очередь для объединения в системы, и в конечном итоге они действительно требуют безопасности. Компоновка катионов безопасности в более широкие системы — это не только нетривиальная задача, но и одна из проблем информационной безопасности, на которую трудно ответить, чтобы решить эту проблему в бизнес-логике соединения (дизайн, ориентированный на логические компоненты и интерфейс) в приложении электронной коммерции. Для быстрого развития на основе логических компонентов и для все более расширяющейся логики бизнес-процессов в системах электронной коммерции нам нужна конвергенция ресурсов процессов безопасности, как показано на рис. 1.

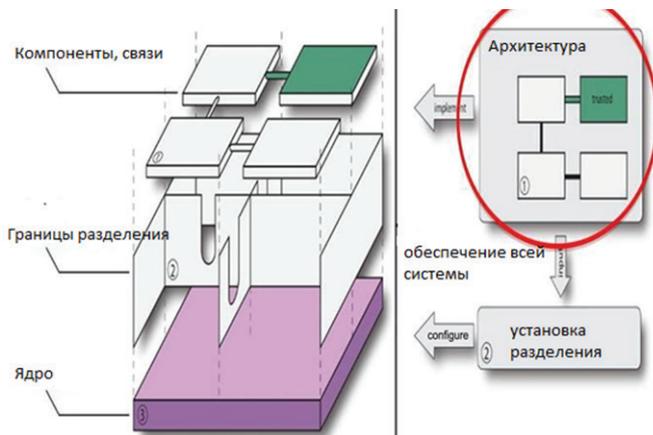


Рис. 1. Процесс обеспечения безопасности и свойства унификации

Чтобы достичь желаемой степени доверия к обеспечению безопасности программного обеспечения, мы рекомендуем семь концепций, направленных на решение проблем, связанных с обеспечением инфор-

мации для критически важных для безопасности программных систем на основе компонентов, построением, развертыванием и сохранением систем.

1) Принятие решений руководствуется восприятием риска. Организации, не получившие надежных гарантий безопасности, сталкиваются с опасностью эффективных атак на инфраструктуру и системы. Они могут использовать варианты гарантий в зависимости от их восприятия угрозы аналогичной атаки и ожидаемого эффекта, например, стратегии, процедуры, методы и ограничения, если эта угроза осознается. Из-за того, что организации изо всех сил пытаются понять свои проблемы и воздействия, они могут неверно интерпретировать риски. Эффективная безопасность позволяет предприятиям делиться информацией о рисках как с партнерами, так и с участниками проекта.

2) Вопросы риска должны быть связаны с заинтересованными сторонами, а стратегические аспекты должны быть взаимосвязаны. Сети с высокой степенью взаимосвязи, такие как Интернет, требуют координации рисков между всеми вовлеченными игроками и всеми техническими элементами, связанными с ними; в противном случае на различных этапах взаимоотношений важные риски упускаются из виду или игнорируются. Когда все тесно взаимосвязано, недостаточно рассматривать только очень важные элементы. Взаимодействие осуществляется на разных уровнях технологий (например, сеть, безопасность, инфраструктура и приложения) и поддерживается рядом функций. Безопасность на любом из этапов может быть применена и, если ее плохо спланировать, может возникнуть конфликт. Эффективное заверение требует четкой идентификации, реагирования на риски на всех уровнях и позиций, связанных с взаимодействием.

3) Из-за широкого использования цифровых цепочек поставок гарантия автоматизированного товара зависит от суждений этих лиц с точки зрения приверженности и степени доверия к ним. Все недостатки гарантии каждого компонента связи исходят от оптимизированных приложений. Кроме того, любая рабочая функция, включая утилиты, программное обеспечение безопасности и другие программы, подлежит гарантии любой другой функции, если только не действуют уникальные ограничения и меры контроля. Компания по-прежнему полагается на гарантийные решения других. Однако организации должны определить, насколько они уверены, что они полагаются на практическую оценку рисков, последствий и возможностей на основе разнообразного опыта. Зависимости не остаются неизменными, и предприятиям приходится ежедневно пересматривать доверительные связи, чтобы оценить корректировки, которые необходимо переосмыслить.

Следующие примеры определяют гарантированный ущерб от слабости: Централизованные технологические уязвимости (например, операционные системы, среды программирования, брандмауэры и маршрутизаторы) могут выступать в качестве общедоступных точек входа уязвимостей программного обеспечения. Использование нескольких общих инструментов разработки

технологий эффективно обеспечивает конечный цифровой продукт. Производители инструментов могут вносить уязвимости в программные продукты.

4) Конфиденциальность, целостность и доступность технических ресурсов приносятся в жертву широкой группе злоумышленников с растущими технологическими возможностями. Никакая защита от атак не является безупречной, и профиль злоумышленника продолжает развиваться. Некоторые угрозы используют технологии, а другие создают уникальные условия для использования средств защиты. Это то, как мы используем технологии.

5) Обеспечение того, чтобы соответствующая гарантия программного обеспечения нуждалась в хорошей командной работе. Организации должны обеспечить безопасность своих сотрудников, процедур и технологий, пока злоумышленники ищут все возможные точки доступа. Кроме того, организации должны конкретно определить на адекватном уровне политические полномочия и обязательства для обеспечения эффективного участия корпоративных участников в кибербезопасности. Эта теория предполагает, что все уверены в себе, но в целом это не так. Следовательно, организациям необходимо подготовить персонал для обслуживания технологий.

6) Гарантия может быть связующим звеном между программным обеспечением и сетевым администрированием, дизайном и обслуживанием и чрезвычайно подвержена улучшениям в любой из этих областей. Чтобы сохранить это равновесие, важно реагировать на частые смены, взаимосвязи, организационное использование и риски приложений. Это не разовый случай, потому что переход регулярный. После первоначального развертывания организации необходимо продолжить организационный мониторинг. Это должно быть включено в соответствующее обещание, требуемое компаниями. Это не будет добавлено позже. Каждый раз ни у кого нет денег на капитальный ремонт конструкций.

7) Должен быть реализован общий процесс оценки и оценки доверия. Организации не могут справиться с тем, что они не могут вычислить, а потребители технологий не будут нести ответственность за политику, пока они не возьмут на себя ответственность за нее. Если результаты отслеживаются и рассчитываются, уверенность не может эффективно конкурировать с другими конкурентными потребностями. Чтобы определить гарантии организации, все социально-технические элементы, такие как политики, процессы и процедуры, должны быть связаны вместе. Более эффективный процесс обеспечения уверенности реагирует и восстанавливается быстрее. Им будет выгодна их реакция и реакция других, а также они будут более тщательно предсказывать и выявлять угрозы.

Разработанная защитная стратегия как решение проблем на уровне бизнес-логики

Эта часть стратегии обеспечит строгий план контроля управления рисками, сосредоточенный на обе-

спечении строгой гарантии качества компонентов для быстрой разработки логики бизнес-приложений CBSD для критически важных для безопасности компонентных программных систем и их приложений в области электронной коммерции.

Ключевые элементы решения проблемы: 1) хороший план управления рисками; 2) Артефакты решения; 3) Характеристики безопасности компонентных компонентов.

1) Хороший план управления рисками: убедитесь, что каждый аспект дизайна приложения должен быть четко и достаточно подробным, чтобы проектировщик мог понять каждое предположение и логику спроектированной функции в приложении.

Обязать четко комментировать все CBSD и включать следующую информацию.

а) Цель и предполагаемое использование каждого компонента (если в коде компонента доступна информация о коде, если нет, его функциональная бизнес-логика в компоненте через описание контракта на использование).

б) Предположения и логика, сделанные каждым компонентом в отношении всего, что находится вне его прямого контроля.

с) Ссылка на все клиентские компоненты, в которых используется четкая документация по компонентам, которая могла бы предотвратить логическую ошибку в функциональности онлайн-регистрации.

2) Артефакты решения: поскольку нет уникальной сигнатуры, по которой можно было бы идентифицировать логические недостатки в веб-приложении, разработанном на основе компонентов Rapid, потому что до сих пор не разработано панацеи, которая могла бы защитить.

3) Характеристики безопасности компонентов программного обеспечения: поскольку программный компонент можно рассматривать как продукт или систему ИТ, естественно использовать общие критерии для оценки его свойств безопасности. Общие критерии обеспечивают основу для оценки ИТ-систем и перечисляют конкретные требования безопасности для таких систем. Требования безопасности делятся на две категории:

- Функциональные требования безопасности
- Требования к обеспечению безопасности

Функциональные требования безопасности:

Опишите желаемое поведение или функции безопасности, ожидаемые от ИТ-системы для противодействия угрозам в операционной среде системы. Эти требования классифицируются в соответствии с проблемами безопасности, которые они решают, и с различными уровнями безопасности. Они включают требования следующих классов: аудит безопасности, коммуникация, криптографическая поддержка, защита данных пользователя, идентификация и аутентификация, управление безопасностью, конфиденциальность, защита функций безопасности системы (метаданные безопасности), использование ресурсов, доступ к системе и надежный путь/каналы.

Требования к обеспечению безопасности:

Функциональные требования безопасности в основном касаются процесса разработки и эксплуатации ИТ-системы с учетом того, что более определенный и строгий процесс обеспечивает большую уверенность в поведении и работе системы в области безопасности. Эти требования классифицируются в соответствии с проблемами процесса, которые они решают, и с различными уровнями безопасности. Вопросы процесса включают поддержку жизненного цикла, управление конфигурацией, разработку, тесты, оценку уязвимостей, руководящие документы, доставку и эксплуатацию, а также гарантийное обслуживание.

На рис. 2 представлена идея процесса обеспечения безопасности, основанная на уровне обеспечения безопасности логики компонентного программного приложения для систем электронной коммерции. Этот процесс также полезен для разработчиков систем программного обеспечения на основе компонентов, критичных к безопасности, при повторном использовании спецификации существующей логики для текущей системы.

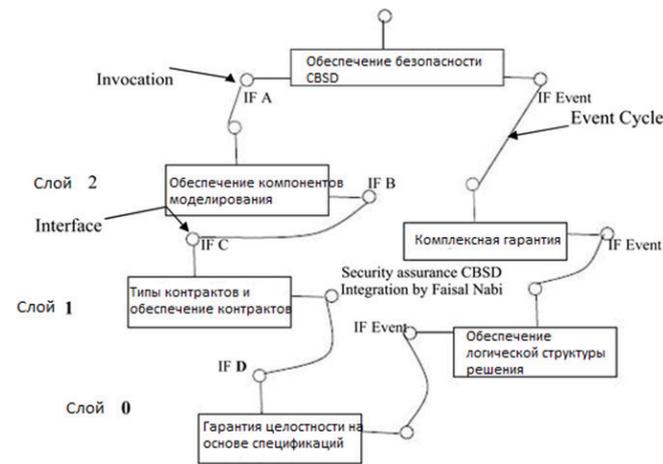


Рис. 2. Процесс разработки стратегии для логики бизнес-приложения обеспечения безопасности

Следовательно, важно, чтобы критически важные для безопасности системы, которые почти ежедневно используются при взаимодействии с людьми, и от простых систем до сложных систем на основе компонентов требовали гарантии перед прохождением стадии разработки, которая гарантирует безопасность системы в различных средах.

Заключение

В этом документе рассматриваются некоторые ключевые проблемы и информационные пробелы в защите больших и сложных системах. Эти недостатки связаны с пробелами между системами защиты и безопасности, тем, как угрозы изображаются и разъясняются, и как утверждения следует рассматривать как шаблоны. Эти семь концепций были описаны как механизм обеспечения безопасности и разработки стратегии обеспечения безопасности для независимой системы или компонента, устраняющий трудности

разработки механизма, который синхронизирует отдельные гарантии безопасности и обеспечивает более сложную форму оценки воздействий. Семь концепций представляют собой предварительный план, способный изменить взаимосвязь секторов разведки и безопасности, а процесс моделирования стратегии проектирования безопасности помогает разработчикам убедиться в обеспечении безопасности системы на этапе SDLC, который, как было доказано, служит ориентиром для критически важного для безопасности компонента.

Список литературы

1. Наби, Ф. и Наби, М. (2017) Процесс унификации свойств обеспечения безопасности для логики приложений. *Международный журнал электроники и информационной инженерии*, 6, 40–48.
2. Чечик, М., Салай, Р., Вигер, Т., Кокали, С. и Рахими, М. (2019) *Software Assurance в неопределённом мире*.
3. Келли, Т. (2019) Структура независимого обеспечения безопасности и защищенности. *Издательство Нью-Йоркского университета, Нью-Йорк*.
4. Чарнецки К. и Салай Р. (2018) К концепции управления неопределённостью восприятия для безопасного автоматизированного вождения. В: Галлина Б., Скавхауг А., Шойч Э. и Битч Ф., ред., *SAFECOMP 2018, LNCS, Vol. 11094*, Спрингер, Чам, 439–445.
5. Карлан, К., Галлина, Б., Касьянка, С. и Бреу, Р. (2017) Споры о целесообразности методов проверки на уровне программного обеспечения. В: Тонетта, С., Шойч, Э. и Битч, Ф.
6. Карлан К., Ратиу Д. и Шетц Б. (2016) Об использовании результатов проверки моделей с ограничениями на уровне кода в случаях уверенности.
7. Kriaa, S., Pietre-Cambacedes, L., Bouissou, M. и Halgand, Y. (2015) Обзор подходов, сочетающих безопасность и защищенность для промышленных систем управления. *Надежность и безопасность систем*, 139, 156–178.
8. Symantec (2018, март) Отчет об угрозах безопасности 2018. Отчет ISTR об угрозах безопасности в Интернете.
9. Берд Дж. (2017, октябрь) 2017 Состояние безопасности приложений: баланс скорости и риска.
10. Ульрих Дж. (2016 г., апрель) Состояние безопасности приложений, 2016 г.: навыки, конфигурации и компоненты. *Обзор института SANS*.
11. Закашевская, А. (2016) Модель пропорционального подхода для применения ASEMS
12. Финнеган, А. и Маккафферы, Ф. (2014) На пути к концепции международной безопасности для сетевых медицинских устройств. *Международная конференция по компьютерной безопасности, надежности и безопасности*, сентябрь 2014 г., Springer, Cham, 197–209.
13. Гер Т., Мильман М., Драхслер-Коэн Д., Цанков П., Чаудхури С. и Вечев М. (2018) AI2: Сертификация безопасности и устойчивости нейронных сетей с абстрактной интерпретацией.

НЕКОТОРЫЕ АСПЕКТЫ ТЕХНИЧЕСКИХ И ПСИХОЛОГИЧЕСКИХ ПРОБЛЕМ ПРИ ПЕРЕХОДЕ НА ДИСТАНЦИОННУЮ ФОРМУ ОБУЧЕНИЯ У ПОДРОСТКОВ И ПЕДАГОГОВ

SOME ASPECTS OF TECHNICAL AND PSYCHOLOGICAL PROBLEMS IN THE TRANSITION TO DISTANCE LEARNING FOR ADOLESCENTS AND TEACHERS

**Бычкова
Елена Сергеевна**

Магистрант ФГАОУ ВО «Российского государственного профессионально-педагогического университета», преподаватель ГАПОУ Свердловской области «Режевского политехникума»

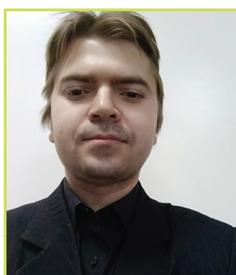


Bychkova Elena Sergeevna

Master student Federal State Autonomous Educational Institution of Higher Education "Russian State Vocational Pedagogical University", Teacher State autonomous professional educational institution of the Sverdlovsk region "Rezhevskaya Polytechnic"

**Воронин
Иван Владимирович**

Магистрант Московского государственного психолого-педагогического университета, преподаватель ГБПОУ города Москвы «Колледж связи № 54 имени П.М. Вострухина»



Voronin Ivan Vladimirovich

Master student Moscow State University of Psychology and Education, Teacher State budgetary professional educational institution of the city of Moscow "College of Communications No. 54" named after P.M. Vostrukhina

Аннотация. Дистанционное обучение в мире давно развивается. Есть успешные проекты и не очень. Достаточно много проведено исследований по выявлению положительных и отрицательных сторон такой формы обучения. В данной статье авторы подводят итог годовичного исследования дистанционного обучения, который начали весной 2020 года. Делают предположения о том, что надо улучшить, чтобы дистанционная форма обучения проходила более комфортно, чем в 2020-2021 году.

Ключевые слова: дистанционное обучение, образование, менеджмент, качество образования.

Annotation. Distance learning has been developing in the world for a long time. There are successful projects and not so much. Quite a lot of research has been conducted to identify the positive and negative aspects of this form of education. In this article, the authors summarize the results of a year-long study of distance learning, which began in the spring of 2020. They make assumptions about what needs to be improved so that distance learning is more comfortable than in 2020–2021.

Keywords: distance learning, education, management, quality of education.

В 2020 году произошла революция в образовательных учебных заведениях: по указанию правительств, практически всех стран мира, из-за пандемии ввели дистанционное обучение, при котором учебный процесс осуществляется удаленно с использованием современных интерактивных интернет ресурсов.

В статье 16 федерального закона «Об образовании в Российской Федерации» говорится о том, что учебные заведения РФ, осуществляя образовательную деятельность вправе применять программы электронного обучения и дистанционных технологий:

«Организации, осуществляющие образовательную деятельность, вправе применять электронное обучение, дистанционные образовательные технологии при реализации образовательных программ в порядке, установленном федеральным органом исполнительной власти, осуществляющим функции по выработке и

реализации государственной политики и нормативно-правовому регулированию в сфере высшего образования, по согласованию с федеральным органом исполнительной власти, осуществляющим функции по выработке и реализации государственной политики и нормативно-правовому регулированию в сфере общего образования.

При реализации образовательных программ с применением исключительно электронного обучения, дистанционных образовательных технологий в организации, осуществляющей образовательную деятельность, должны быть созданы условия для функционирования электронной информационно-образовательной среды, включающей в себя электронные информационные ресурсы, электронные образовательные ресурсы, совокупность информационных технологий, телекоммуникационных тех-

нологий, соответствующих технологических средств и обеспечивающей освоение обучающимися образовательных программ в полном объеме независимо от места нахождения обучающихся. Перечень профессий и специальностей среднего профессионального образования, реализация образовательных программ по которым не допускается с применением исключительно электронного обучения, дистанционных образовательных технологий, утверждается федеральным органом исполнительной власти, осуществляющим функции по выработке и реализации государственной политики и нормативно-правовому регулированию в сфере общего образования. Перечень специальностей и направлений подготовки высшего образования, реализация образовательных программ по которым не допускается с применением исключительно электронного обучения, дистанционных образовательных технологий, утверждается федеральным органом исполнительной власти, осуществляющим функции по выработке и реализации государственной политики и нормативно-правовому регулированию в сфере высшего образования». [1]

И, хотя вначале декларировалось, что это — вынужденная, временная мера, но всем уже ясно, что такой формат преподавания вошел в нашу жизнь всерьез и надолго. Его применение вызвано даже не столько появившейся необходимостью ввода карантинных мер, сколько назревшими реалиями развития образования.

Реакция общества на такое нововведение была не однозначной — от шокового неприятия сложившейся ситуации преподавателями и учащимися, до стремления официальных властей, не достаточно хорошо подготовивших внедрение онлайн обучения, провалить своё решение. Авторы исследовали данную тему, проведя анкетирование общества сразу после весеннего дистанционного обучения, и опубликовали результаты в статье.

Летом 2020 года у работников образовательных учреждений появилась возможность для осмысления накопленного опыта проведения обучения в дистанционном формате. В результате анализа возникших проблем, администрациями и преподавательским составом учебных заведений были предприняты усилия по обновлению технических средств, изучению онлайн ресурсов, созданию учебных методических пособий. Правда это было сделано не во всех учебных заведениях в силу различных причин как объективных, так и субъективных.

К объективным факторам можно отнести недостаточное финансирование региональных учебных заведений для обновления технической базы учебных заведений, накопившуюся усталость после стрессового весеннего периода пандемии, плохую осведомленность о возможностях интернет ресурсов для проведения качественного онлайн обучения.

К субъективным причинам — отсутствие мотивации, нежелание изучать и внедрять новые технологии.

Мы продолжили мониторинг развития адаптации населения к введению дистанционного обучения осенью 2020 года нами было проведено повторное анкетирование преподавателей и студентов.

Всего было опрошено 28 преподавателей и 98 учащихся в различных учебных заведениях (школах, техникумах, колледжах, ВУЗах), расположенных как в столице, так и на периферии.

Место проживания преподавателей:



Рис. 1. Города проживания педагогов



Рис. 2. Наименования образовательных организаций

Место жительства опрошенных учащихся:

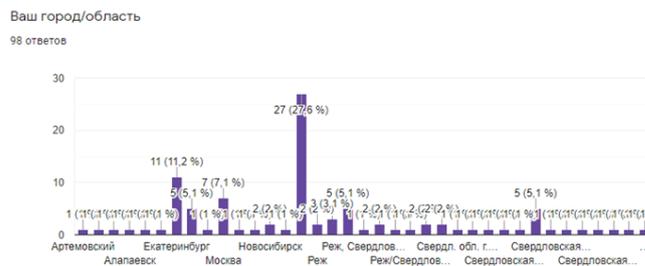


Рис. 3. Города проживания обучающихся

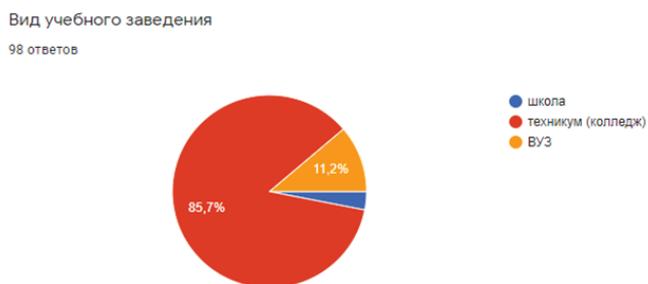


Рис. 4. Типы образовательных организаций

Адаптация к дистанционному формату обучения

Среди преподавателей ровно половина утверждает, что их отношение к дистанционному обучению с весны 2020 года не изменилось.

Среди студентов не поменяли своё отношение к дистанционному обучению 71,9%:

Изменилось ли Ваше отношение к дистанционному обучению с весны 2020 года?

96 ответов

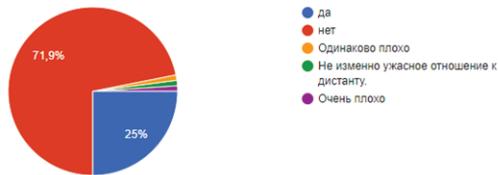


Рис. 5. Отношение студентов к дистанционному формату обучения

При этом почти каждый третий учащийся отметил, что он всё ещё не привык к подобному процессу обучения:

Быстрее ли прошла адаптация к дистанционному обучению по сравнению с весной 2020 года?

98 ответов



Рис. 6. Время, затраченное на адаптацию обучающихся к дистанционному формату обучения

40,8% опрошенных студентов считают, что они быстрее адаптировались, 31,6% не почувствовали разницу по сравнению с весенним периодом.

Среди педагогов лишь 3,6% опрошенных отметили, что такой процесс преподавания стал более привычным.

Таким образом, в результате опроса установлено, что учащиеся быстрее, чем педагоги, адаптируются к изменившимся условиям, это более молодая часть населения, в процессе обучения они должны усваивать тот материал, который подготовил преподаватель. Контакт с учебным заведением проходит с помощью мобильных и компьютерных устройств, в работе с которыми у молодёжи больше опыта. Для работы в новом формате педагогам пришлось осваивать современные технологии, но не у всех есть желание их изучать и применять на практике, в силу объективных и субъективных причин, либо они уже имеют необходимые навыки.

Организация учебного процесса.

Рассмотрим, какие меры по проведению дистанционного обучения были приняты учебными заведениями.

Осенью, в сравнении с весной 2020 года, по мнению 21,4% опрошенных преподавателей, улучшилась организация учебного процесса администрацией.

35,7% педагогов утверждают, что с весны 2020 года ничего не изменилось.

Этот результат указывает на то, что, возможно, не везде администрация учебного заведения адекватно отреагировала на вызов времени, либо преподавателям хотелось бы, чтобы начальство было более активно в этих вопросах. Также, вероятно, что есть проблема в оценке работы методического отдела:

Помогали ли Вам методисты в организации дистанционного учебного процесса?

27 ответов

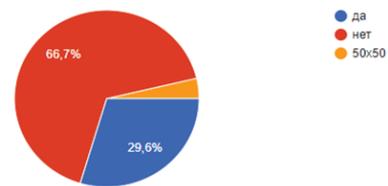


Рис. 7. Вовлеченность методистов в организацию дистанционного формата обучения

Если весной администрации учебных заведений были не готовы к новому типу обучения и инструктаж с преподавателями практически не проводился, то осенью ситуация немного улучшилась:

Проводился ли инструктаж по использованию систем дистанционного обучения?

28 ответов

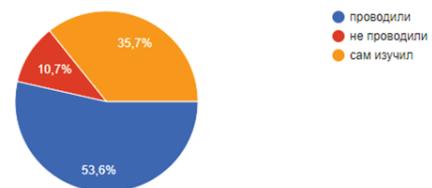


Рис. 8. Результат опроса преподавателей прошедших инструктаж по организации дистанционного формата обучения

Для изучения возможностей интернет ресурсов в настоящее время существует множество курсов, как платных, так и бесплатных. Возможность их прохождения летом была практически у всех.

60,7% педагогов, как самостоятельно, так и с помощью учебных заведений прошли учёбу по освоению новых навыков необходимых для дистанционного обучения.

39,3% не захотели изучать современные методы организации учебного процесса, часть их, хотелось бы предположить уже владеет образовательными методами работы в дистанционном формате, так как недавно закончила учебные заведения, но у другой части это вызвано, скорее всего, с психологическим неприятием дистанционного обучения. Качественное проведение обучения в дистанционном формате не возможно без освоения интерактивных и интернет технологий, элементы которого можно и нужно применять и при возвращении к традиционной модели преподавания:

Прошли ли Вы где либо обучение по освоению методов организации дистанционного учебного процесса с весны 2020 года?

28 ответов



Рис. 9. Результат опроса педагогов изучавших организацию дистанционного формата обучения

Одновременно с этим 60,7% педагогов считают, что нагрузка при обучении в дистанционном формате, по

сравнению с весной лишь увеличилась. 39,3% считают, что она уменьшилась.

Во время обучения в дистанционном формате возникли проблемы с организацией вне учебных мероприятий. Прежние способы проведения такой работы стали недоступны, новые приёмы — не разработаны. На возросшую нагрузку вне учебной деятельности указали 59,3% преподавателей, например, организацию различных онлайн мероприятий в виде Challenge — публикации в социальных сетях вида из окна. 37% это отрицают, 3,7% указали, что преподаватели перегружены психологически и физически.

Большая часть педагогов указывают на то, что много времени занимает работа за компьютером, что не может благотворно сказаться на здоровье:

Сколько времени в среднем каждый день Вы тратили на работу за компьютером?

28 ответов

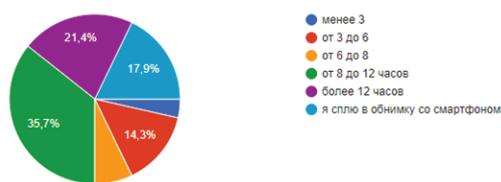


Рис. 10. Время, проведённое за компьютером педагогами

Временные затраты на учёбу у студентов достаточно различны:

Сколько времени в среднем каждый день Вы тратили на обучении за компьютером?

97 ответов

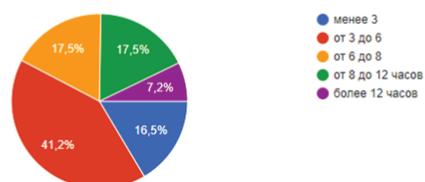


Рис. 11. Время, проведённое за компьютером обучающимися

48,5% учащихся не укладывались в отведенное для выполнения заданий время, хотя 51,5% студентов успевали выполнять поставленные задачи в установленный срок. Нехватка времени не обязательно связано с дистанционным форматом обучения и скорее говорит об отношении к учёбе, либо психологических особенностях учащихся, а не к способу преподавания.

Освоение современных технологий могло бы способствовать уменьшению нагрузки на преподавателей, но опрос показал, что это не везде применяется и не всеми. 14,8% преподавателей отмечают, что была внедрена автоматизация проверки заданий, что немного улучшает сложившуюся ситуацию, 33,3% отрицают применение такого нововведения, 51,9% отметили, что задания они проверяют привычным способом — вручную.

Опрос среди студентов об изменении формата заданий по сравнению с весной 2020 года дал следующие результаты:

34,7% указали, что формат заданий поменялся, а 65,3% отрицают такие изменения.

Нагрузка на педагогов могла бы уменьшиться при переводе ведения журналов в электронный формат, но это введено не во всех учебных заведениях.

32,1% преподавателей указали, что заполнение журналов происходит в электронном виде.

25% — в бумажном.

42,9% — журналы заполняются как в электронном, так и в бумажном формате, что никак не способствует ускорению работы.

База дистанционного обучения

Весной 2020 года было много проблем с отсутствием необходимого оборудования, виртуальных разработок. Осенью 78,6% педагогов указали на улучшение базы дистанционного образования по сравнению с весной 2020 года.

46,4% преподавателей считают, что этим изменениям они способствовали сами.

39,3% опрошенных педагогов, считают, что ничего не поменялось в базе для проведения дистанционного обучения.

Как изменилась база дистанционного обучения в вашем учебном заведении с весны 2020 года?

28 ответов



Рис. 12. Изменения в образовательной (контент) базе для проведения дистанционного обучения по мнению педагогов

Студенты, в отличие от педагогов более скептически отнеслись к изменению в образовательной (контенту) базе по сравнению с весной 2020 года. Результат показан на рис. 13.

Использовали ли педагоги интерактивные доски, интерактивные задания и иные образовательные технологии?

96 ответов

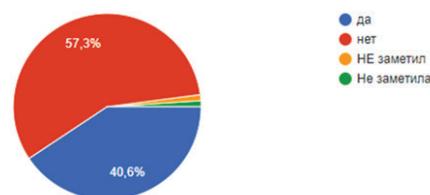


Рис. 13 Изменения в базе для проведения дистанционного обучения по мнению обучающихся

Анализируя данный рисунок можно сделать вывод, что 57,3% студентов не почувствовали улучшения образовательной базы:

Применяемые инструменты

89,3% педагогов указывают, что они освоили новые инструменты дистанционного обучения.

Преподаватели указали, что именно они стали использовать на практике (рис. 14).

Учащиеся также указали на разнообразие применяемых систем (рис. 15).

Какой инструмент дистанционного обучения Вы использовали?

28 ответов

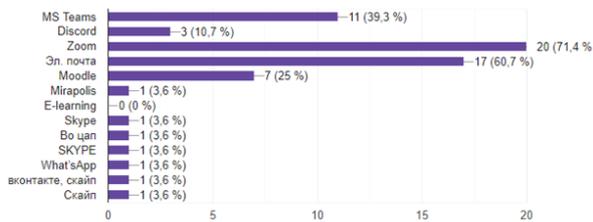


Рис. 14. Инструменты дистанционного обучения, используемые преподавателями

Какая система использовалась для взаимодействия с преподавателями?

96 ответов

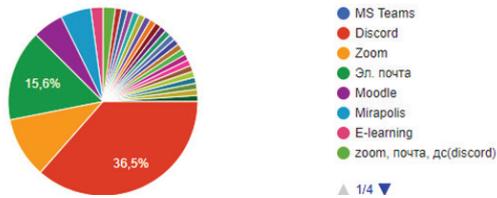


Рис. 15. Инструменты дистанционного обучения, используемые студентами

Полученная разница в использованных инструментах говорит скорее о предпочтениях опрошенных, чем о реально сложившейся ситуации. Кроме того существует множество разнообразных интернет платформ для проведения дистанционного обучения и единых требований по применению конкретных ресурсов не установлено.

42,9% респондентов, как преподавателей, так и студентов продолжают беспокоить проблемы с доступом к интернету и другие технические трудности.

Технические трудности

Ответы преподавателей:

Были ли технические проблемы с доступом в Интернет

28 ответов

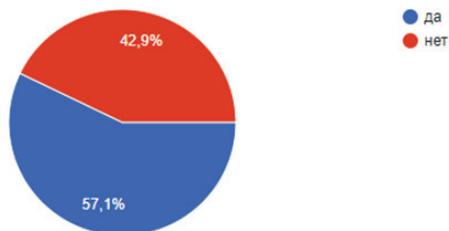


Рис. 16. Процент преподавателей испытывавших проблемы с доступом в сеть Интернет

Были ли проблемы во взаимодействии со студентами?

27 ответов

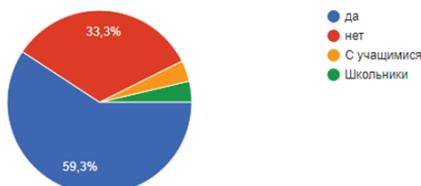


Рис. 17. Процент преподавателей испытывавших проблемы во взаимодействии со студентами

У студентов тоже были технические проблемы (рис. 18–19). 44,9% указали на проблемы с доступом к образовательным ресурсам (рис. 20).

Были ли технические проблемы с доступом в Интернет

98 ответов



Рис. 18. Процент обучающихся, испытывавших проблемы с доступом в сеть Интернет

Возникали ли технические трудности с подключением к иной конференц-связи?

98 ответов



Рис. 19. Процент студентов испытывавших проблемы во взаимодействии с преподавателями

Были ли проблемы с доступом к образовательным ресурсам, рекомендованным учебными заведениями?

98 ответов

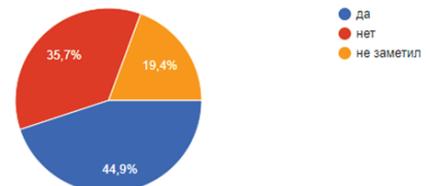


Рис. 20. Процент студентов, испытывавших проблемы с доступом к образовательным ресурсам

Различны и сетевые устройства, которые использовались студентами для учёбы (рис. 21). 60% учащихся считают, педагоги своевременно реагировали на возникающие вопросы (рис. 22).

Какой девайс Вы использовали при подключении к лекции?

97 ответов

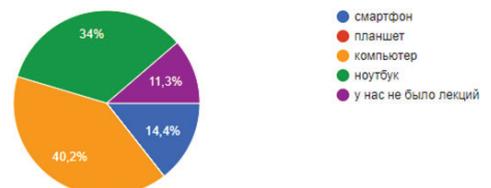


Рис. 21. Сетевые устройства студентов для учёбы

Оперативно ли реагировали преподаватели на возникающие вопросы в процессе выполнения задания?

95 ответов



Рис. 22. Оперативность отклика преподавателей

Экономические проблемы.

Если для преподавания в традиционном формате всё давно разработано, преподавателю достаточно было подготовиться и прийти в учебное заведение, где всё есть для работы, то для обучения в дистанционном формате требуется иметь собственное специальное оборудование и программы.

89,3% опрошенных преподавателей сообщили, что им пришлось обновить компьютеры и программное обучение (рис. 23–24). Компенсация затрат практически не предоставлялась (рис. 25). Также 40,7% педагогов указали на наличие проблем с доступом к компьютеру (рис. 26). Немного лучше дела обстоят у учащихся (рис. 27–28).

Пришлось ли Вам обновить Ваш компьютер?

28 ответов



Рис. 23. Процент преподавателей, обновивших свой компьютер

Покупали ли Вы программное обеспечение для проведения занятий?

28 ответов

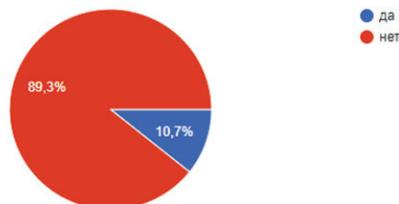


Рис. 24. Процент преподавателей, обновивших программное обеспечение на своём компьютере

Возместили ли Вам затраты на покупку программного и аппаратного обеспечения?

26 ответов

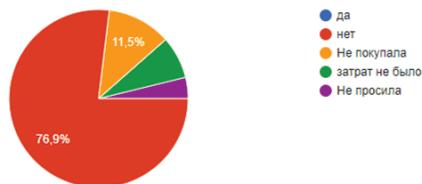


Рис. 25. Процент возмещений затрат на апгрейд

Были ли в семье проблемы с доступом к компьютеру (допустим, в семье 4 человека. Компьютеров всего 2 ед. Т.к. родители тоже перешли на дистанционную работу, то возможны проблемы детей с доступом к компьютеру и решению задач)?

27 ответов

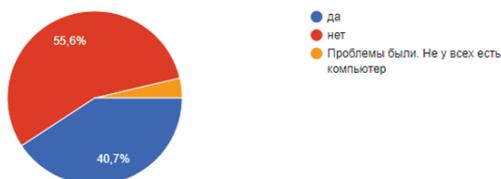


Рис. 26. Недостаток наличия компьютеров у педагогов

Предоставило ли учебное заведение компьютеры/ноутбуки, если у Вас их не было дома?

96 ответов



Рис. 27. Недостаток наличия компьютеров у обучающихся

За чей счет приобретались микрофон и веб-камера?

94 ответа

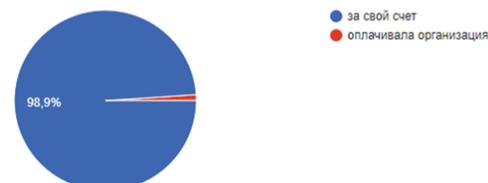


Рис. 28. Обеспеченность периферийными устройствами

Таким образом, с весны 2020 г. в организации материальной помощи населению ничего не изменилось: большая часть населения решала проблемы по приобретению компьютеров и программного обеспечения для проведения дистанционного обучения за свой счёт. Отсутствие компенсации понесённых материальных затрат во время экономического кризиса, не способствует заинтересованности в дистанционном обучении.

Плюсы и минусы дистанционного обучения

Во время анкетирования были рассмотрены положительные и проблемные моменты дистанционного обучения.

Среди преимуществ обучения в дистанционном формате педагогами были названы следующие:

- Не тратится время на проезд к учебному заведению (особенно актуально для крупных городов);
- Снижается опасность инфекционного заражения;
- Удобно для тех, кто заболел и для инклюзивного обучения;
- Учащиеся не отвлекаются на разговоры с однокурсниками (однокурсниками)
- Возможность автоматической проверки домашних заданий (правда это можно применять и при очном обучении)
- Учащихся привыкают к самостоятельной работе. К недостаткам были отнесены проблемы:
- Отсутствие личного контакта педагог — студент.
- Недостаточное оснащение техническими средствами.
- Отсутствие, либо затруднённая обратная связь с учениками.
- Отсутствие социального взаимодействия, возможности проверить знания ученика и проконтролировать выполнение домашнего задания (много списывают), возможности у некоторых ребят подключаться к урокам.
- Строится по урочному принципу, что отдельным педагогам представляется не правильным.

- Утомляемость, как детей, так и взрослых, не получены полноценные знания, Сильная нагрузка на зрение. Психологические и эмоциональные перегрузки. Недостаточная физическая активность. Постоянная привязка к рабочему месту 24/7 в телефоне и компьютере.
- В настоящее время наблюдается среди молодёжи рост интернет зависимости. Проблемой дистанционного обучения в онлайн формате является то, что к видеоиграм в интернете добавляются учебные часы, проводимые за компьютером.

Реальное взаимодействие с учителями и сверстниками заменяет виртуальное общение. Рвутся социальные связи. Это влияет на психическое здоровье подрастающего поколения негативно. Поэтому не стоит полностью переходить в дистанционный формат обучения, лучше совмещать традиционное обучение с элементами онлайн формата.

Недостаток времени из-за учёбы для встреч с друзьями приводит к общению с ними при помощи различных социальных сетей. Высокая социальная активность студенческого возраста выражается в поиске новых знакомств при помощи тех же услуг сети. [2]

Институт психологии Российской академии наук, в 2019 году, провели исследование интернет зависимости среди студентов и пришли к выводу что выраженная интернет-зависимость определилась у 11,9% человек, склонность к интернет-зависимости — у 52,3%, минимальный риск зависимого поведения — у 34,8% респондентов. [3] В целом, мотивация к обучению у большей части студентов на дистанционном обучении не понизилась (рис. 29). И, более половины студентов, так или иначе, не против дистанционной формы обучения (рис. 30).

Понизилась ли Ваша мотивация к обучению в целом?
97 ответов

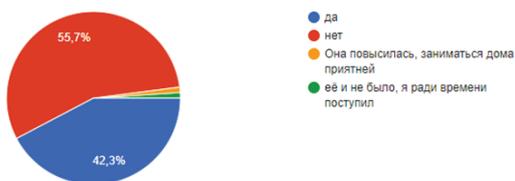


Рис. 29. Уровень мотивации к обучению у студентов

В каком формате Вы бы предпочли дальнейшее обучение?
98 ответов

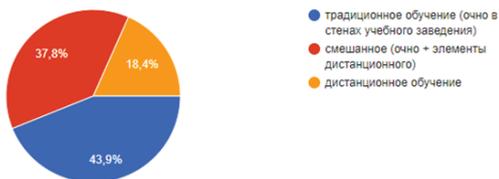


Рис. 30. Формат обучения, предпочитаемый студентами

Цифровизация образования.

Преподаватели также ответили на вопросы о информированности о проводимой цифровизации образования (рис. 31).

Вы знакомы с правительственными планами и проектами, направленными на цифровизацию образования.

28 ответов

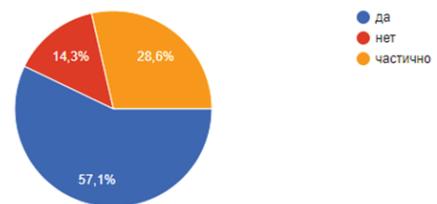


Рис. 31. Осведомлённость преподавателей о планах по цифровизации образования

Есть надежда, что с его осуществлением часть проблем дистанционной формы обучения будет снята. Так как при цифровизации образования планируется повысить доступность интернета на всей территории РФ, строительство дата-центров, дальнейшее развитие материальной инфраструктуры, внедрение цифровых программ, развитие онлайн-обучения, администрирования и контроля учебных курсов, разработка системы идентификации обучаемых, постепенный отказ от бумажных носителей, внедрение в образование геймификации и других современных наработок в области образования. Предполагается, что всё это будет способствовать обеспечению равного и свободного доступа к обучению, его разнообразию и соответствию требованиям, которые предъявляет к образованию современное общество. [4]

После изучения результатов анкетирования и на основании собственного опыта, можно сделать некоторые выводы. Например, то, что дистанционное обучение пришло в нашу жизнь не случайно — это требование времени. Те, кто говорит и пишет, что дистанционная форма обучения снижает качество образования, не совсем правы:

1. Они не правы в том плане, что своим высказыванием «гребут под одну гребенку» все специальности. Если при некоторых предметах проведение онлайн обучения затруднено (физкультура, трудовое обучение, лабораторные работы и т.п.), то другие вполне могут быть реализованы в дистанционном формате (лекции, проводимые в формате видеоконференции, с возможностью использования чата, презентаций и т.п.). Внедрение в образовательный процесс элементов VR-технологий способствует более наглядному показу уроков. Современные возможности электронного образования расширяют кругозор путем «кругосветных прогулок» на автомобиле, музейные экскурсии, посещение виртуальных городов.

2. Не все учебные заведения имеют специалистов по спецпредметам (особенно в деревенских школах и в региональных учебных заведениях) и такой формат позволит там найти возможность преподавания необходимых по программе предметов.

3. Уменьшение социальных связей у обучающихся по мнению многих характерно для дистанционного обучения. Хотя возможность непосредственной коммуникации между студентами снижается, существует возможность общения через социальные сети,

которые наоборот расширяют социальное взаимодействие, есть возможность подбора качественного контента и обратной связи от преподавателей-носителей языка и культуры другой страны

4. Во время вирусных инфекций и для инклюзивного обучения это наиболее оптимальный вариант организации учёбы. Есть возможность у заболевших учащихся продолжить обучение дома.

5. Во многих учебных заведениях материально-техническая база не соответствует по ФГОС для обучения, что на данный момент является реальностью. Это преодолимо, если будут отпущены на образование достаточные финансовые средства.

6. Многие учебные заведения пришли к смешанному формату обучения. Основная часть обучения проходит дистанционно, при необходимости часть занятий проходит очно в аудиториях

7. Дистанционное обучение повышает личную ответственность обучающихся, т.к. студент сам может регулировать время обучения. Это также благоприятно для тех, кто параллельно с учёбой работает.

К безусловным минусам такого формата обучения, на которых указали данные анкетирования можно отнести следующие проблемы:

1. Отсутствие постоянного контроля расслабляет студентов.

2. Гиподинамия — малоподвижный образ жизни плохо влияет на здоровье, как студентов, так и преподавателей.

3. Усугубление проблемы интернет — зависимости подрастающего поколения.

4. При недобросовестной работе преподавателя, либо его плохом владении современными средствами электронного обучения студент остается один на один с проблемами разбора новых тем и практических заданий.

5. Низкая скорость доступа в Интернет у многих пользователей.

6. Низкий уровень доходов у населения. Не у всех семей есть возможность приобрести необходимое оборудование для дистанционного обучения и это создает еще большее расслоение общества.

Заключение

Анализируя осенние данные анкетирования, можно сделать следующие выводы:

1. Тех, кто против введения дистанционного формата в обучение, по разным причинам, в том числе психологическим, примерно одна треть населения. Принципиальное неприятие такого формата обучения, должно уменьшиться с разработкой и освоением методов обучения, адаптированных для дистанционного формата.

2. Осталось достаточно много задач, которые объективно нуждаются в решении. Самыми главными из них являются плохое материальное обеспечение, недостаточное финансирование учебных заведений для введения дистанционного обучения правительством (на сегодня в перспективе есть вероятность ре-

шения этих проблем, либо уменьшения их остроты). Согласно Федерального закона от 26.07.2019 № 232-ФЗ «при реализации образовательных программ с применением исключительно электронного обучения, дистанционных образовательных технологий в организации, осуществляющей образовательную деятельность, должны быть созданы условия для функционирования электронной информационно-образовательной среды, включающей в себя электронные информационные ресурсы, электронные образовательные ресурсы, совокупность информационных технологий, телекоммуникационных технологий, соответствующих технологических средств и обеспечивающей освоение обучающимися образовательных программ в полном объеме независимо от места нахождения обучающихся».

3. Образование попадает в зависимость от качества предоставляемых услуг интернет провайдерами и в случае повышения нагрузки на сеть Интернет, возникают ситуации когда проведение дистанционного обучения становится не возможным.

4. Необходимо решить вопросы социализации учащихся при введении дистанционного обучения, для снижения риска повышения интернет зависимости студентов.

Список литературы

1. Федеральный закон от 29.12.2012 N 273-ФЗ (ред. от 30.04.2021) «Об образовании в Российской Федерации» (с изм. и доп., вступ. в силу с 01.06.2021) / Ст. 16. Реализация образовательных программ с применением электронного обучения и дистанционных образовательных технологий [Электрон. ресурс]. — Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_140174/9ab9b85e5291f25d6986b5301ab79c23f0055ca4/ (дата обращения: 20.02.2021).
2. Гуреева А.Ю. Интернет-зависимость: современное состояние проблемы [Электрон. ресурс] / А.Ю. Гуреева, С.В. Сизов. Режим доступа: <https://medconfer.com/node/5248> (дата обращения: 20.02.2021).
3. Бычкова Е.С. Форсированный переход на дистанционное обучение: проблемы и пути решения / Е.С. Бычкова, И.В. Воронин // Инновационные аспекты развития науки и техники: сб. ст. III Междунар. науч.-практ. конф. — Саратов: Цифровая наука, 2020. — С. 172–185.
4. Левина Т.В. Межличностные отношения у людей с разным уровнем интернет-зависимости [Электрон. ресурс] / Т.В. Левина // Социальная и экономическая психология. — 2019. — Т. 4. № 3(15). — Режим доступа: <http://soc-econom-psychology.ru/engine/documents/document721.pdf>. (дата обращения: 20.02.2021).
5. Бортников М.Е. Автоматизация оценки показателей работы профессорско-преподавательского состава / М.Е. Бортников, М.С. Логачёв // Стандарты и мониторинг в образовании. — 2020. — Т.8, №5. — С. 26–33. — DOI: 10.12737/1998-1740-2020-26-33.
6. Логачёв М.С. Мониторинг качества образовательных программ как средство повышения уровня подготовки выпускников колледжа / М.С. Логачёв // Про-

- фессиональное образование и общество. — 2015. — №2(14). — С. 102–104.
7. **Логачёв М.С.** Проблемы мониторинга качества образования / М.С. Логачёв // Автоматизированные системы управления качеством образовательного процесса: моногр. // М.С. Логачёв, Ю.Н. Самарин, М.С. Тигина. — М.: МГУП имени Ивана Федорова, 2016. — С. 71–101.
8. Семь задач цифровизации российского образования [Электрон. ресурс]. — Режим доступа: <https://trends.rbc.ru/trends/education/5d9ccba49a7947d5591e93ee> (дата обращения: 20.02.2021).

МОДЕЛИРОВАНИЕ ПОСЛЕДСТВИЙ ВЗРЫВНЫХ НАГРУЗОК НА КОНСТРУКТИВНЫЕ ЭЛЕМЕНТЫ ОБЪЕКТОВ ИНФРАСТРУКТУРЫ ЛЮБОГО ТИПА

MODELING THE CONSEQUENCES OF EXPLOSIVE LOADS ON STRUCTURAL ELEMENTS OF INFRASTRUCTURE OBJECTS OF ANY TYPE

Перевесенский Сергей Александрович

*Курсант 4-го курса
Академии гражданской защиты МЧС России*



Perevesenskij Sergej Aleksandrovich

*4th year cadet of the Civil Protection Academy
of the Ministry of Emergency Situations of Russia*

Сорокин Алексей Юрьевич

*Преподаватель кафедры информатики
и вычислительной техники Академии гражданской
защиты МЧС России*



Sorokin Aleksej Jur'evich

*Lecturer at the Department of Informatics and Computer
Engineering of the Academy of Civil Protection of the Ministry
of Emergency Situations of Russia*

Аннотация. Настоящая работа посвящена разработке программного обеспечения, реализующего методику определения последствий взрывных нагрузок на основе распределения механической энергии. Приведено общее описание программы и принцип работы, а также продемонстрированы основные функциональные элементы, промежуточная отрисовка, входные и выходные данные.

Ключевые слова: модели, безопасность, информационные технологии, методика.

Abstract. This work is devoted to the development of software that implements the method for determining the consequences of explosive loads based on the distribution of mechanical energy. The general description of the program and the principle of operation are given, as well as the main functional elements, intermediate rendering, input and output data are demonstrated.

Keywords: Models, security, information technology, methodology.

Введение

В настоящее время существуют определенные потребности в научно-методическом аппарате, позволяющем определять характеристики конструкции сооружения, обеспечивающие устойчивость объекта инфраструктуры к воздействию поражающих факторов взрыва. Актуализация данной проблемы с нормативной точки зрения инициируется следующими законодательными требованиями:

Законодательством Российской Федерации определено, что защита критически важных объектов инфраструктуры от различных ЧС должно осуществляться по средствам повышения уровня их защищенности [1].

Законы от транспортной безопасности и противодействию терроризму требуют обеспечивать работу на предупреждение и минимизацию последствий [2].

Исходя из анализа статистики реализации вышеописанных угроз, наиболее распространенная форма проявления диверсионных или террористических актов, заключается в подрывной деятельности [3].

В целях решения данной проблемы, был разработан научно-методический аппарат, основанный на распределении в конструкции механической энергии взрыва [4]. В целях упрощения использования приведенной методики, ведется работа по ее цифровизации. На данный момент разработан прототип, функцио-

нальным и техническим особенностям которого и посвящается настоящая работа.

Описание цифровой интерпретации методики

Благодаря тому, что на данной стадии развития технологий мы можем использовать мощности ЭВМ, а также создавать 3-D модель требуемых объектов. Мы можем создать симуляцию воздействия избыточного давления на объект.

С функциональной точки зрения, цифровая версия приведенной методики основана на принципе декомпозиции конечного объекта на составляющие элементы по аналогии с молекулярно-кристаллической решеткой. Так как известно, что воздушная ударная волна представляет собой область сжатия молекул воздуха, которая двигается в заданном направлении, принцип декомпозиции можно применить и к ней.

Таким образом, представляет конечный объект в виде взаимосвязанных частиц, размер которых может быть масштабирован в зависимости от потребностей и мощностей ЭВМ. Понятие взаимосвязанности, в данном случае подразумевает то, что для отрыва частиц друг от друга, к ним необходимо приложить энергию, которая будет превышать энергию их связи. При этом целостность связи с физической точки зрения обуславливает упругость деформации, нарушение целостности приводит к деформации не упругой.

Декомпозиция воздушной ударной волны так же производится на частицы. Каждая частица имеет свой вектор и характеристику энергетического состояния. Графическая интерпретация декомпозиции приведена на рис. 1.

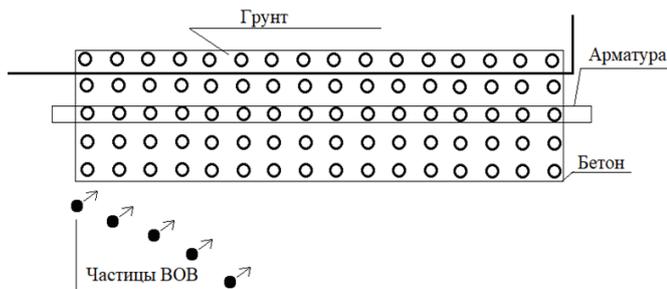


Рис. 1. Графическая интерпретация принципа декомпозиции

В ходе такого моделирования, с математической точки зрения будут фигурировать следующие величины:

- p_0 — давление частицы воздушной ударной волны;
- v — вектор движения частицы воздушной ударной волны;
- z — обратная реакция материала конструкции на нагрузку с учетом распределения напряжения;
- y — напряжение создаваемое внутри материала конструкции;
- v_y — скорость распределения напряжения внутри материала конструкции.
- G_T — предел текучести;
- E — модуль упругости;

На базе рис. 1 и приведенных величин, процесс моделирования можно описать следующим образом. Частицы эмитирующие ударную волну с рассчитанной по методике скоростью соударяются с элементом конструкции. При этом определяется время реакции конструкции, а следовательно, и величина, определяющая время действия нагрузки от одной частицы ВОВ.

Частица ударной волны при соударении, оказывает на конструкцию давление p_0 , вызывая в ней напряжение и упругую обратную реакцию, при этом за время взаимодействия, часть энергии частицы ударной волны, распределяется по конструкции увеличивая общее напряжение.

Материал конструкции в свою очередь, будет стремиться распределить собственное напряжение на любые элементы, с которыми соприкасается по оси нагрузки.

Напряжение первого материала конструкции, передаваемое второму, воспринимается им как нагрузка, которую он так же стремится распределить.

Для каждого материала, существует порог напряжения, который может в нем возникать. Данный порог, численно равен пределу текучести для соответствующей площади сечения. Для подземных сооружений, условно возможно принять, что грунт обладает бесконечным пределом текучести, так как его деформации, нас не интересуют.

Таким образом, для взаимодействия частиц ударной волны с декомпозированной структурой объекта строительной конструкции, задаются следующие условия:

$$P_0 < G_T, \begin{cases} z = E - y, z \leq G_T \\ \bar{v} = 0, z < G_T \\ \bar{v} = z - G_T, z \geq G_T \end{cases}$$

$$P_0 > G_T, \begin{cases} \bar{v} = \frac{P_0 + G_T}{2} \\ z = 0, \text{разрушено} \end{cases}$$

$$P_0 = G_T, z, P_0 = const \text{ (идеальное упругое соударение)}$$

На базе данных условий программа высчитывает общий объем повреждений, а также минимальные и максимальные энергетические нагрузки на элемент. При этом показывает квадратичное отклонение нагрузки и графически показывает места возможных дефектов внутри структуры материального объекта.

Пример моделирования на базе прототипа цифрового исполнения приведенной методики

Входными данными являются:

- 3D конструкции в формате .obj (рис. 2);
- N — количество векторов ударной волны;
- E_0 — энергия одного вектора ударной волны;
- p_0 — давление вектора ударной;
- I — размер кубика для разбиения конструкции
- v — скорость распределения напряжения внутри материала конструкции (по координатам сектора);
- G_T — пределе текучести материала (по координатам сектора);
- E — модуль упругости материала (по координатам сектора).

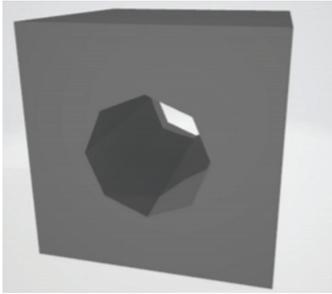


Рис. 2. 3D объект конструктивного элемента

После ввода входных данных, программа перерабатывает 3D модель в физическую 3D модель объекта с учетом декомпозиции и заданными характеристиками (рис. 3–4).

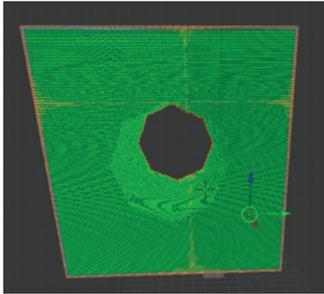


Рис. 3. Декомпозированная 3D модель с заданными характеристиками

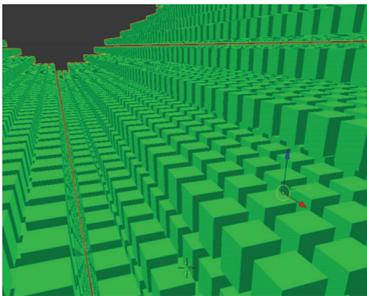


Рис. 4. Декомпозиция 3D модели

После переработки 3D модели, запускается процесс симуляции. На данный момент из-за тестирования программы на слабом ЭВМ, отрисовка воздействия происходит в плоскостном срезе. Срез отрисовки настраивается (рис. 5).

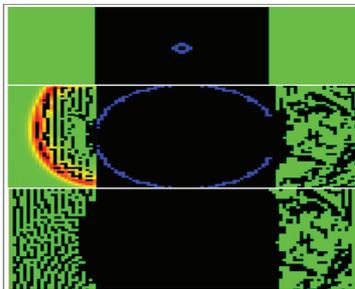


Рис. 5. Моделирование воздействия ударной волны

После моделирования, программа выдает результаты (рис. 6).

```
Destroyed 307450 of 863600
E min 261900
E max 1.70368e+12
E quadratic mean 3.3532e+10
```

Рис. 6. Результат моделирования

Заключение

В настоящее время все больше процессов подвергаются автоматизации. Разрабатываются различные ПО для решения целевых задач. Моделирование последствий взрывных нагрузок на конструктивные элементы объектов инфраструктуры также не является исключением, и в будущем будет автоматизирована.

Исследование показало, что данная концепция достаточно жизнеспособна и требует сравнительно низких затрат для внедрения. Главное достоинство такого подхода заключается в скорости и точности анализа, а самое главное экономит время для принятия решений и разработки соответствующих защитных мероприятий.

Список литературы

1. Основы государственной политики в области защиты населения и территорий от чрезвычайных ситуаций на период до 2030 года.
2. Федеральный закон от 06.03.2006 N 35-ФЗ (ред. от 18.03.2020) «О противодействии терроризму».
3. Распоряжение Правительства РФ от 30.07.2010 № 1285-р (ред. от 04.07.2019) «Об утверждении Комплексной программы обеспечения безопасности населения на транспорте».
4. Сорокин А.Ю. Универсальный подход к моделированию взрывных нагрузок на объекты инфраструктуры любого типа / А.Ю. Сорокин // Безопасность и охрана труда — 2019: тр. Междунар. молодеж. конф. (Москва, 10–13 декабря 2019 г.). — М.: МЭИ, 2019. — С. 166–169.

РОЛЬ РОСФИНМОНИТОРИНГА В ПРОТИВОДЕЙСТВИИ ЛЕГАЛИЗАЦИИ ПРЕСТУПНЫХ ДОХОДОВ В УСЛОВИЯХ ЦИФРОВОЙ ТРАНСФОРМАЦИИ

THE ROLE OF ROSFINMONITORING IN COMBATING MONEY LAUNDERING IN THE CONTEXT OF DIGITAL TRANSFORMATION

Зуева Анна Сергеевна

Кандидат экономических наук, доцент, доцент кафедры компьютерного права и информационной безопасности Высшей школы государственного аудита Московского государственного университета имени М.В. Ломоносова, доцент кафедры правового обеспечения публичных финансов Института законодательства и сравнительного правоведения при Правительстве Российской Федерации, доцент кафедры «Государственный финансовый контроль и казначейское дело» Финансового университета при Правительстве РФ



Zueva Anna Sergeevna

Candidate of Economic Sciences, Associate Professor, Associate Professor of the Department of Computer Law and Information Security of the Graduate School of State Audit, Moscow State University named after M.V. Lomonosov, Associate Professor of the Department of Legal Support of Public Finance at the Institute of Legislation and Comparative Law under the Government of the Russian Federation, Associate Professor of the Department "State Financial Control and Treasury" of the Financial University under the Government of the Russian Federation

Басырова Зарина Рудиковна

Студентка 3-го курса Высшей школы государственного аудита Московского государственного университета имени М.В. Ломоносова



Basyrova Zarina Rudikovna

3rd year student of the Graduate School of State Audit of the Moscow State University named after M.V. Lomonosov

Аннотация. В данной статье проанализирована международная нормативная правовая база по противодействию легализации доходов, полученных преступным путем, а также законодательство Российской Федерации в данной сфере. Определены роль и место Росфинмониторинга в противодействии отмыванию преступных доходов в условиях цифровизации, разработаны меры по улучшению деятельности Росфинмониторинга и повышению его эффективности.

Ключевые слова: легализация преступных доходов, цифровая трансформация, транзакция, Росфинмониторинг, цифровая идентификация, мониторинг.

Abstract. This article analyzes the international legal framework for countering money laundering from crime, as well as the legislation of the Russian Federation in this area. The role and place of the Federal Financial Monitoring Service in countering money laundering in the context of digitalization were determined, and measures were developed to improve the Service's activities and increase its effectiveness.

Keywords: money laundering, digital transformation, transaction, Federal Financial Monitoring Service, digital identification, monitoring.

Особое внимание международного сообщества вызывает легализация преступных доходов и финансирование терроризма. Для Российской Федерации легализация доходов, полученных преступным путем, — серьезное экономическое преступление. В ст. 3 Федерального закона от 07.08.2001 № 115-ФЗ «О противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма» закреплено, что легализация — это придание правомерного вида владению, пользованию или распоряжению денежными средствами или иным

имуществом, полученными в результате совершения преступления [1].

Правовой основой противодействия легализации преступных доходов называют Конвенцию ООН о борьбе против незаконного оборота наркотических и психотропных веществ (Венская конвенция) 1988 года, которая была ратифицирована СССР в 1990 году. В этом документе впервые попытались дать определение преступных доходов: «доходы» означают любую собственность, полученную или приобретенную прямо, или косвенно в результате совершения правонару-

шения, признанного таковым в соответствии с п. 1 ст. 3 [2, с. 479–516]. Немаловажную роль в сфере противодействия легализации (отмыванию) доходов, приобретенных преступным путем, сыграли Конвенция ООН против транснациональной организованной преступности [3, с. 3–33], Конвенция ООН против коррупции [4, с. 7–54].

Для российской законодательной базы большую роль сыграла Страсбургская конвенция 1990 года «Об отмывании, выявлении, изъятии и конфискации доходов от преступной деятельности» [5, с. 14–46]. Благодаря этой конвенции в 2001 году в Уголовном кодексе Российской Федерации появился уголовно-правовой запрет отмывания преступных доходов. В Страсбургской конвенции действия, связанные с отмыванием доходов, расширяются, по сравнению с Венской Конвенцией 1988 года. Признается, что преступные доходы могут быть получены от любого вида преступной деятельности, а не только от деятельности, связанной с незаконным оборотом наркотиков.

Также Российской Федерацией были заключены соглашения с другими государствами, которые связаны с противодействием легализации преступных доходов (Армения, Беларусь, Болгария, Венесуэла, Грузия, Италия, Мексика, Македония, Нигерия, Хорватия, ЮАР и др.).

Для обеспечения экономической безопасности мирового пространства и каждого отдельного государства, разрабатываются стандарты противодействия этим преступным явлениям и методические рекомендации по их пресечению, раскрытию, расследованию и предупреждению. Такая деятельность на международном уровне проводится Группой разработки финансовых мер по борьбе с отмыванием денег — ФАТФ (Financial Action Task Force — FATF). В Российской Федерации функции по противодействию легализации (отмыванию) доходов, полученных преступным путем, финансированию терроризма (далее — ПОД/ФТ), по выработке государственной политики и нормативно-правовому регулированию в этой сфере занимается Федеральная служба по финансовому мониторингу — Росфинмониторинг [6]. Этот федеральный орган исполнительной власти по классификации Рекомендаций ФАТФ — национальное подразделение финансовой разведки (ПФР). Оно было создано в 2001 году как самостоятельное ведомство в структуре органов исполнительной власти. До 2004 года было подотчетно Министерству финансов Российской Федерации, с 2004 года — Правительству Российской Федерации, с 2012 года отчетывается напрямую перед Президентом Российской Федерации.

Роль Росфинмониторинга во многом зависит от ее статуса, как государственного органа. Сущность государственных органов в том, что они выражают и защищают публичные интересы, то есть интересы всего общества в целом. Росфинмониторинг защищает интересы не только бизнеса и банков, их клиентов, не какой-то группы людей, а интересы всего населения Российской Федерации. Противодействию легализации

преступных доходов, Росфинмониторинг создает уникальные условия, которые невозможно создать в ходе работы каких-то других учреждений. Эти условия имеют целью сократить в обществе предикатные преступления, например, торговля оружием, наркотиками, мошенничество, хищение вкладов, денежных средств со счетов граждан, хищение и растрата бюджетных средств, коррупция и другие преступления, доходы от которых чаще всего пытаются легализовать.

Своей миссией Росфинмониторинг называет защиту финансовой системы и экономики государства от угроз отмывания денег, финансирования терроризма и финансирования распространения оружия массового уничтожения [7]. В рамках реализации этой миссии федеральная служба определила ряд стратегических целей на 2021–2023 годы:

- снизить риски легализации (отмывания) денежных средств и иного имущества, полученного преступным путем, финансирования терроризма и финансирования распространения оружия массового уничтожения;
- добиться соблюдения законодательства о ПОД/ФТ организациями, осуществляющими операции с денежными средствами или иным имуществом, и специалистами, входящими в национальную систему;
- повысить уровень прозрачности экономики, в том числе за счет применения механизма установления бенефициарных владельцев хозяйствующих субъектов;
- предупреждать нецелевое расходование бюджетных средств и обеспечивать повышения эффективности их использования;
- снижать уровень террористической угрозы и экстремистских проявлений в обществе, обеспечивать законность и прозрачность деятельности некоммерческих организаций;
- продолжать укреплять роль Российской Федерации в международной системе ПОД/ФТ;
- повышать уровень финансовой грамотности граждан в сфере борьбы с незаконными финансовыми операциями.

Цифровая трансформация и цифровизация предоставляют Росфинмониторингу больше возможностей для эффективного достижения поставленных целей. Проще и быстрее координировать деятельность в сфере ПОД/ФТ федеральных органов исполнительной власти, взаимодействовать с Банком России, саморегулируемыми организациями, реализующими контрольные функции в сфере ПОД/ФТ. Так, например, в 2019 году Росфинмониторингом был введен в промышленную эксплуатацию Личный кабинет надзорного органа для межведомственного обмена информацией. Через этот сервис осуществляется оперативное информирование о рисках в секторах и в деятельности конкретных организаций.

Постоянное информационное взаимодействие поддерживается с Федеральной налоговой службой Российской Федерации и ее территориальными ор-

ганами. Через систему электронного взаимодействия «запрос-ответ» — СМЭВ, Росфинмониторинг может оперативно получить актуальные сведения об организациях и индивидуальных предпринимателях из ЕГРЮЛ и ЕГРИП. И наоборот, если в ход проверки выявлено, что организация отсутствует по месту нахождения, заявленному при государственной регистрации, Росфинмониторинг в обязательном порядке информирует об этом налоговые органы.

Совместно с Министерством цифрового развития, связи и массовых коммуникаций Российской Федерации, Росфинмониторингом разработан сервис по отслеживанию транзакций с криптовалютой с помощью искусственного интеллекта. Сервис «Прозрачный блокчейн» был анонсирован главой Росфинмониторинга Юрием Чиханчиным на встрече с Президентом Российской Федерации. Новый сервис проводит анализ транзакции криптовалюты, оценивает ее законность или незаконность и затем определяет конечного бенефициара. Операции с криптовалютой сами по себе прозрачны, видны адреса покупателей и продавцов. Однако есть программные продукты, которые способны скрывать эти сведения. Одно из назначений «Прозрачного блокчейна» — раскрытие зашифрованных данных, если операция вызывает подозрения проверяющих. Официальной презентации сервиса еще не было.

В марте 2020 года ФАТФ опубликовала Руководство по цифровому удостоверению личности. ФАТФ напомнила, что количество цифровых транзакций растет примерно на 12,7% в год, к 2022 году, по некоторым оценкам, 60% мирового ВВП будет оцифровано [8]. Знание своего клиента в любой финансовой операции необходимо для обеспечения гарантии того, что привлеченные денежные средства не связаны с преступной деятельностью.

Надежное цифровое удостоверение личности может облегчить и обезопасить идентификацию физических лиц в финансовом секторе, будет способствовать облегчению мониторинга за переводами и минимизировать слабые места в ручных методах контроля. При этом, если снизить риски в финансовой сфере, это может повлечь за собой повышение рисков в другой. В частности, могут возникнуть такие риски, как:

- искажение персональных данных, мошенничество с использованием персональных данных клиентов;
- неэффективное управление данными;
- кража цифровой идентичности;
- и некоторые другие.

Кроме того, рассматриваемые в Руководстве вопросы включают в себя конкретные риски, которые цифровая идентификация может представлять для обеспечения соблюдения законов, каким образом технология может способствовать расширению доступа к финансовым услугам, как может помочь в мониторинге транзакций. В частности, Руководство содержит технологии распределенного реестра в качестве инструмента, который способен помочь росту сетей цифровой идентификации, также организация

призвала государства четко определить руководящие принципы, которые позволят надлежащим образом использовать независимые системы цифровой идентификации. ФАТФ предлагает регулируемым учреждениям, «использовать информированный подход с учетом оценки рисков в случае развертывания систем цифровой идентификации для надлежащей проверки клиентов». Организация также подчеркнула важность цифровой идентификации в платежных системах, и возможность использования технологии для выявления заинтересованных сторон в транзакциях.

В марте 2021 года ФАТФ опубликовала Руководство о применении риск-ориентированного надзора в сфере ПОД/ФТ. В нем содержатся рекомендации по применению риск-ориентированного надзора в соответствии со стандартами ФАТФ, организации процесса оценки рисков и принятию мер по их снижению, пониманию секторальных рисков поднадзорных субъектов и эффективному распределению надзорных ресурсов; стратегии по урегулированию наиболее распространенных проблем применения; а также примеры применения надзора в различных юрисдикциях в отношении финансовых учреждений и использования инновационных технологий при осуществлении надзора за деятельностью участников финансового рынка [9].

ФАТФ высоко оценила работу Росфинмониторинга. В Отчете о взаимной оценке Российской Федерации, завершившейся в 2019 году, оценщики из международной миссии ФАТФ подтвердили, что Росфинмониторинг обрабатывает огромный объем данных, включая большое количество сообщений о подозрительных операциях. Так, в среднем за год таких сообщений поступает около 20 млн. Проверяющие отметили, что российское подразделение финансовой разведки использует современные технологии и высокий уровень автоматизации процессов для определения приоритетности, инициирования и содействия в расследованиях дел, осуществляемых правоохранительными органами [10, с. 41].

Подводя итог, следует отметить, что в современный период деятельность Росфинмониторинга находится на высоком уровне, что выражается в достаточно слаженном функционировании ее внутренних механизмов и признании на международном уровне. Кроме того, Росфинмониторинг обладает внушительным ресурсным и информационным обеспечением, компетентными кадрами. Однако развитие информационных технологий с каждым днем набирает все большие обороты. Использование новых технологий в преступных целях оказывается более быстрым процессом, чем внедрение этих технологий в систему ПОД/ФТ. В первую очередь применение цифровых технологий зависит от того, насколько система ПОД/ФТ готова к использованию этих самых технологий. Использование финансовых продуктов — криптовалюты, смарт-контрактов, технологии блокчейн возможно, только если определить их правовой статус в Российской Федерации. Также нужно постоянно ак-

туализировать список организаций, которые осуществляют операции с денежными средствами или иным имуществом.

Список литературы

1. Федеральный закон от 07.08.2001 № 115-ФЗ «О противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма» // Российская газета. — № 151–152. — 09.08.2001.
2. Сборник важнейших документов по международному праву. Часть II особенная. — М.: Институт Международного права и экономики; Триада, лтд, 1997. — 544 с.
3. Бюллетень международных договоров. — 2005. — № 2. — С. 3–33.
4. Бюллетень международных договоров. — 2006. — № 10, октябрь. — С. 7–54.
5. Бюллетень международных договоров. — 2003. — № 3. — С. 14–46.
6. Указ Президента РФ от 13.06.2012 № 808 «Вопросы Федеральной службы по финансовому мониторингу» (вместе с «Положением о Федеральной службе по финансовому мониторингу») // Собрание законодательства РФ. — 18.06.2012, № 25. — Ст. 3314.
7. Стратегические цели Росфинмониторинга на 2021–2023 годы [Электрон. ресурс] // Росфинмониторинг. — Режим доступа: <http://www.fedsfm.ru/about/declaration>.
8. FATF (2020), Guidance on Digital Identity, FATF, Paris [Электрон. ресурс]. — Режим доступа: www.fatf-gafi.org/publications/documents/digital-identity-guidance.html.
9. Обзор событий в сфере противодействия отмыванию доходов, полученных преступным путем, и финансированию терроризма [Электрон. ресурс] / Официальный сайт Банка России. — Режим доступа: https://cbr.ru/Collection/Collection/File/32245/March_2021.pdf.
10. Anti-money laundering and counter-terrorist financing measures — Russian Federation // Fourth Round Mutual Evaluation Report, FATF, Paris. URL: <http://www.fatf-gafi.org/publications/mutualevaluations/documents/mer-russian-federation-2019.html>.

СОЗДАНИЕ ЭЛЕКТРОННОГО УЧЕБНОГО ПОСОБИЯ ПО ДИСЦИПЛИНЕ «УСТРОЙСТВО И ФУНКЦИОНИРОВАНИЕ ИНФОРМАЦИОННЫХ СИСТЕМ» ДЛЯ СТУДЕНТОВ СПЕЦИАЛЬНОСТИ 09.02.04 «ИНФОРМАЦИОННЫЕ СИСТЕМЫ (ПО ОТРАСЛЯМ)»

CREATION OF AN ELECTRONIC TEXTBOOK ON THE DISCIPLINE "STRUCTURE AND FUNCTIONING OF INFORMATION SYSTEMS" FOR STUDENTS OF THE SPECIALTY 09.02.04 "INFORMATION SYSTEMS (BY INDUSTRY)"

**Клейменов
Анатолий Романович**

Студент 4-го курса Технического колледжа ТГТУ



**Klejmenov
Anatolij Romanovich**

4th year student of the Technical College of TSTU

**Дубровина
Оксана Васильевна**

Преподаватель специальных дисциплин Технического колледжа ТГТУ



**Dubrovina
Oksana Vasil'evna**

Teacher of special disciplines at the Technical College of TSTU

Аннотация. На современном этапе развития образования очень большое распространение получила информатизация различных направлений. Внедряются электронные учебники и электронные курсы обучения по дисциплинам, применяются мультимедийные ма-

Abstract: At the present stage of the development of education, informatization of various directions has become very widespread. Electronic textbooks and e-learning courses on disciplines are being introduced, multimedia materials, testing systems and all possible options for network learning

На основе этой разбивки будет сделано меню учебного пособия. Общие вид меню представлен на рис. 2.



Рис. 2. Меню ЭУП

Электронное учебное пособие начинается с первой темы, расположенной на главной странице.



Рис. 3. Главная страница ЭУП

Каждая тема в разделе имеет карточки — вкладки, переходящие на страницы с учебным материалом.



Рис. 4. Тема «Типы организационных структур»

Все виды материалов разбиваются на лекционный материал и практические работы. Структура всех тем аналогична, изменяется количество подтем и состав.



Рис. 5. Фрагмент лекции по теме

Практические задания содержат материал для выполнения с пояснениями.

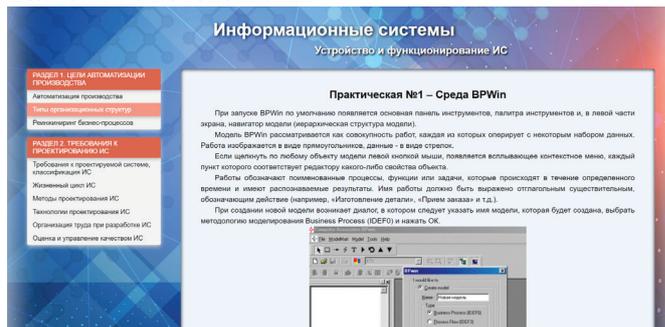


Рис. 6. Фрагмент практической работы

Основной формой контроля по курсу являются тесты на основе облачных технологий Google Form.

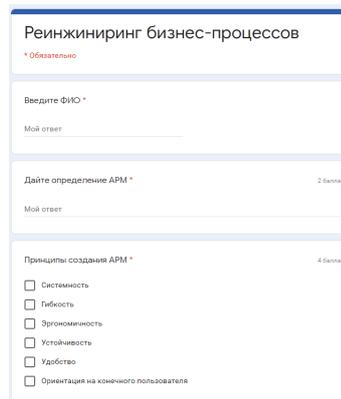


Рис. 7. Фрагмент теста по теме «Реинжиниринг бизнес-процессов»

Итогом изучения дисциплины является сдача экзамена, вопросы к которому также есть в электронном учебном пособии. Перед сдачей экзамена студенты должны успешно пройти итоговый тест.

Использование электронных учебных пособий в образовательном процессе позволяет глубже изучить материал, познакомиться с интересующими или плохо усвоенными темами. Различные графические и видео материалы предоставляют наглядную демонстрацию информации. При работе с электронными учебными пособиями происходит не только репродуктивная деятельность студентов, но и абстрактно-логическая, помогая лучше осознать и усвоить материал.

Список литературы

1. Андреев А.А. Дистанционное обучение и дистанционные образовательные технологии / А.А. Андреев, В.И. Солдаткин // Cloud of science. — 2013. — №1. — С. 14–20.
2. Бурцева Л.П. Методика профессионального обучения: учеб. пособие / Л.П. Бурцева. — М.: ФЛИНТА: Наука, 2015. — 157 с.
3. Майстренко А.В. Информационные технологии поддержки инженерной и научно-образовательной деятельности / А.В. Майстренко, Н.В. Майстренко, И.В. Дидрих. — Тамбов, 2014. — 81 с.
4. Основы разработки электронных учебных изданий / Г.В. Алексеев, И.И. Бриденко, Е.И. Верболюз [и др.]. — СПб.: Лань, 2016. — 144 с.

ПОНЯТИЕ И ПРАВОВОЕ РЕГУЛИРОВАНИЕ «БОЛЬШИХ ДАННЫХ» В УСЛОВИЯХ СТАНОВЛЕНИЯ ЗАКОНОДАТЕЛЬСТВА В СФЕРЕ ИНФОРМАЦИОННОГО ПРАВА

THE CONCEPT AND LEGAL REGULATION OF "BIG DATA" IN THE CONTEXT OF THE FORMATION OF LEGISLATION IN THE FIELD OF INFORMATION LAW

**Строкова
Полина Сергеевна**

Магистрант ФГБОУ ВО «Московская государственная юридическая академия имени О.Е. Кутафина (МГЮА)», юрист ООО «Акира Ойл», Москва



**Strokova
Polina Sergeevna**

Master student of the Federal State Budgetary Educational Institution of Higher Education "Moscow State Law Academy named after O.E. Kutafina (Moscow State Law Academy)", lawyer, LLC "Akira Oil", Moscow

Аннотация. В настоящей работе исследуются тенденции и особенности развития российского законодательства в сфере правового регулирования обработки Больших данных, приводится сравнительный анализ российского и зарубежного законодательства с целью выяснения оптимального подхода к определению термина «Большие данные» в условиях развивающегося законодательства в области информационного права.

Ключевые слова: правовое регулирование, информационное право, понятийный аппарат, большие данные, цифровые технологии, персональные данные.

Abstract. The research examines the trends and features of the development of Russian legislation in the field of legal regulation of big data processing, provides a comparative analysis of Russian and foreign legislation in order to determine the optimal approach to the definition of the term "Big Data" in the context of developing legislation in the field of information law.

Keywords: legal regulation, information law, conceptual apparatus, big data, digital technologies, personal data.

Построение информационного общества в Российской Федерации, получившее наиболее авторитетное формальное закрепление на нормативно-правовом уровне в октябре 2018 года с принятием Национальной программы «Цифровая экономика», идет по пути не только технологического и технического развития государства, но и по пути изменения нормативного правового регулирования в обновленных или вновь созданных сферах общественных отношений. Как закреплено в Стратегии развития информационного общества в Российской Федерации на 2017-2030 годы (утв. Указом Президента РФ от 9 мая 2017 г. №203), данные в цифровом виде признаны основой хозяйственной деятельности в условиях цифровой экономики [1], что породило ряд вопросов, не имеющих на данный момент однозначного пути решения.

Первоочередным вопросом, требующим разрешения, является разработка понятийно-категориального аппарата. Одной из проблем законодательства является тождественность понятий «информация» и «данные» [2]. В соответствии с Федеральным законом «Об информации, информационных технологиях и о защите информации» от 27.07.2006 №149-ФЗ «информацией» признаются любые сведения, сообщения, данные, а «данные», в соответствии с Федеральным законом «О персональных данных» от 27.07.2006 №152-ФЗ, понимаются как информация в любой форме. Таким

образом, очевидно, что законодатель ставит знак равенства между этими двумя категориями и не раскрывает их соотношение, что тоже выступает в качестве фактора, затрудняющего формирование концептуальных подходов. Вместе с тем, Международная организация по стандартизации (далее — ИСО) в Словаре «Информационные технологии» (в ред. 2015 года) устанавливает такое соотношение «данных» и «информации», при котором «данные» признаются предоставлением информации в формализованном виде, подходящем для коммуникации, интерпретации или обработки [3], а «информация» толкуется как результат интерпретации данных [4]. Учитывая, что интерес представляют не только сами данные как элементы информации, но и их качественные и количественные характеристики, в правовых целях можно рассматривать явление Больших данных как совокупность средств и методов обработки больших объемов структурированных и неструктурированных данных, как создаваемых человеком, так и предоставленных техническими источниками, с целью извлечения имеющей ценность информации. Вышеописанный подход полностью соответствует взгляду законодателя, выраженному в Стратегии развития информационного общества в Российской Федерации на 2017–2030 гг., однако в тексте используемого Стратегией определения наблюдается неточность, касаю-

сящая способов обработки информации, поскольку речь идет уже не просто о невозможности ручной обработки информации, но и невозможности обработки посредством типичных алгоритмов, что само по себе вынуждает обращаться к развитию и урегулированию обработки данных при помощи интеллектуальных систем, включение которых в правовое поле и является конечной целью разрабатываемого нормативного регулирования сферы информационного права. В этом свете особую критику вызывает определение, предложенное Министерством цифрового развития, связи и массовых коммуникаций Российской Федерации в проекте Федерального закона «О внесении изменений в Федеральный закон «Об информации, информационных технологиях и о защите информации» (ID проекта 04/13/02-20/00099581), опубликованное 14 февраля 2020 г., где Большие данные рассматриваются именно как собственно данные. [5]. Анализируя используемое в Проекте определение, можно отметить, что акцент на том факте, что данные могут правомерно обрабатываться исключительно при условии невозможности персонификации конкретного лица, является одной из «ниточек», подводящей нас к вопросу о разграничении персональных данных в понимании Федерального закона «О персональных данных» от 27.07.2006 №152-ФЗ и данных, подлежащих обработке как категория Больших данных и их вывода из сферы действия ФЗ «О персональных данных». Среди негативных аспектов анализируемого определения следует отметить: нецелесообразность перечисления конкретных видов данных, рассматриваемых в качестве Больших данных, что обосновано прогрессирующим технологическим развитием; классификация данных по группам не является признаком, характерным для Больших данных.

В Соединенных Штатах Америки не происходит нормативного регулирования Больших данных как самостоятельного объекта, а их обработка рассматривается только в рамках гарантированного Конституцией США права на неприкосновенность частной жизни. Использование такого подхода привело к тому, что нормы, регулирующие обработку данных, закреплены в отдельных отраслевых актах, где перечисляются виды данных, которые признаются персональной информацией в целях конкретного нормативного акта. Негативным последствием использования такого подхода на данный момент стала неспособность законодательства адаптироваться под появление на рынке новых видов данных, таких как геолокационные, телематические данные, [6] и невозможность урегулирования правил сбора и обработки таких данных на законодательном уровне. Таким образом, применение подхода, подразумевающего установление перечня данных, являющихся ограниченными в обороте по смыслу конкретного нормативного акта, позволяет соблюсти тонкую грань между информационной безопасностью субъектов данных и предпринимателями, заинтересованными в получении и обработке данных, однако не всегда могут

преодолеть состояние правовой неопределенности по отношению к вновь возникающим видам данных.

Развитая нормативная база в области обработки данных представлена в Канаде, где выстроена система трёхуровневого регулирования. Первый уровень представлен Федеральными законами: Законом о конфиденциальности (Privacy Act), и Законом о защите личной информации и электронных документов) [7]. Оба закона содержат перечень информации, рассматриваемой в качестве персональных данных, и, соответственно, запрещенной к сбору без получения согласия субъекта персональных данных. Отграничив круг персональной информации, Канадское законодательство перешло к регулированию оборота данных в условиях цифровой экономики, что ознаменовалось разработкой Цифровой Хартии Канады, установившей основные принципы обработки Больших данных. В 2016 году Правительство Канады обратило внимание на возрастающее для экономического развития значение данных, резкое увеличение их объема создания и в связи с этим инициировало «диалог» с гражданами и представителями бизнеса о путях и возможностях регулирования сбора и обработки данных, создаваемых в том числе в результате межмашинного взаимодействия [8]. В ходе обсуждения совершенствования законодательства были приняты изменения, касающиеся сбора данных, не признанных персональными по смыслу Закона о конфиденциальности, а также в законодательные акты, регулирующие порядок получения согласия пользователей на сбор данных, составлен перечень данных, в отношении которых оператор освобождается от обязанности получения предварительного согласия субъекта данных [9]. Как следует из материалов проведенных общественных обсуждений, такой подход не позволяет найти баланс между сохранением конфиденциальности личной информации и потребностью бизнеса в сборе и обработке данных, поскольку при существовании закрытого перечня, законодательство оказывается не способным адаптироваться под появление новых видов данных.

Кардинально иную позицию представляет собой законодательство Сингапура, построенное на открытости данных и широком их использовании не только в предпринимательских целях [11], но и в государственном секторе. Обращаясь к анализу законодательства в сфере обработки данных Сингапура, следует отметить основной акт, призванный обеспечить защиту персональных данных в условиях интенсивного развития ИТ-инфраструктуры – Закон о защите личных данных №26 от 7 декабря 2012 г. В статье, посвящённой целям Закона, прямо указано на необходимость не только регулирования сбора и обработки данных, но и на тот факт, что организации испытывают необходимость в сборе и обработке данных [10]. Либеральными представляются положения, предусматривающие так называемое «предполагаемое согласие», применяемое в тех случаях, когда субъект лично предоставляет данные организации и его согласие явствует из обстановки. Такое построение ос-

нового закона о данных свидетельствует о том, что Правительство Сингапура не только не применяет жесткого регулирования сбора и обработки данных, но и в значительной степени возлагает ответственность за сохранение режима конфиденциальности данных на самих субъектов, что и даёт возможность для эффективного развития технологического бизнеса [12] и развития государственного сектора в части скорости и качества предоставления услуг населению, построенному на принципах открытости данных. Нельзя, однако, не отметить, что злоупотребления, которых, впрочем, нельзя избежать ни при одном из существующих правовых режимов, приводят к созданию открытых баз, содержащих большие массивы разнородных, систематизированных и проанализированных данных, которые стали предметом предпринимательской деятельности и продаются как информационный продукт, что является предметом развития законодательства в сфере киберпреступлений.

Проанализировав подходы, используемые различными зарубежными странами, следует сделать вывод о том, что рассмотрение Больших данных в контексте их соотношения с персональными данными субъектов допустимо при условии соблюдения определенной степени свободы их регулирования. Приведение в законодательстве ограничительных перечней, как видно на примере Канады, не способствует ни технологическому развитию государства, ни экономическому в секторе информационных технологий и, более того, создают преграды для функционирования уже существующего бизнеса, подводя его под риск применения серьезных штрафных санкций. Следовательно, при разработке законодательства, регулирующего обработку, анализ и оборот данных в Российской Федерации, не следует применять жесткое регулирование, вводить в законодательство однозначные дефиниции тех объектов, которые подвержены постоянному развитию, как в случае с Большими данными.

Список литературы

1. Указ Президента Российской Федерации от 09.05.2017 г. № 203 «О Стратегии развития информационного общества в Российской Федерации на 2017–2030 годы» [Электрон. ресурс]. — Режим доступа: <http://kremlin.ru/acts/bank/41919> (дата обращения: 09.02.2021).
2. Савельев А.И. На пути к концепции регулирования данных в условиях цифровой экономики / А.И. Савельев // Закон. — 2019. — № 4. — С. 174–195.
3. Информационные технологии: словарь ИСО [Электрон. ресурс]. — Режим доступа: <https://www.iso.org/obp/ui/#iso:std:iso-iec:2382:ed-1:v1:en> (дата обращения: 09.04.2021 г.).
4. Системная и программная инженерия: словарь ИСО [Электрон. ресурс]. — Режим доступа: <https://www.iso.org/standard/50518.html> (дата обращения: 09.02.2021).
5. Доклад ОСЭР (2015). Инновации, основанные на данных, для роста и благополучия/ (OECD (2015). Data-driven Innovation for Growth and Well-being, OECD Publishing, Paris) [Электрон. ресурс]. — Режим доступа: <http://dx.doi.org/10.1787/9789264229358-en> (дата обращения: 09.02.2021).
6. Доклад Счетной палаты США. Компании, предоставляющие услуги на основе определения местоположения в автомобиле, предпринимают шаги для защиты конфиденциальности, но некоторые риски могут быть неясны потребителям. Декабрь 2013 г. [Электрон. ресурс]. — Режим доступа: <https://www.gao.gov/assets/660/659509.pdf> (дата обращения: 09.02.2021).
7. Закон О защите персональных данных и электронных документов (PIPEDA). Информационный портал Комиссара по защите персональных данных [Электрон. ресурс]. — Режим доступа: <https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-ripeda/> (дата обращения: 09.02.2021).
8. Цифровая Хартия Канады в действии: план канадцев, для канадцев [Электрон. ресурс]. — Режим доступа: <https://www.ourcommons.ca/DocumentViewer/en/42-1/ETNI/report-12/page-57#12> (дата обращения: 09.02.2021).
9. Предложения по модернизации закона О защите персональных данных и электронных документов [Электрон. ресурс]. — Режим доступа: https://www.ic.gc.ca/eic/site/062.nsf/eng/h_00107.html (дата обращения: 09.02.2021).
10. Закон О защите личных данных (Республика Сингапур) от 15 октября 2012 г. №26 [Электрон. ресурс]. — Режим доступа: <https://sso.agc.gov.sg/Act/PDPA2012> (дата обращения: 09.02.2021).
11. Михайлов А.В. Общие вопросы эффективности правового регулирования предпринимательских отношений / А.В. Михайлов // Современные проблемы юридической науки и правоприменительной практики: сб. науч. тр. / под общ. ред. О.А. Заячковского. — Калининград: Изд-во БФУ им. И. Канта, 2018. — С. 75–80.
12. Сушкова О.В. Особенности влияния института защиты коммерческой информации и персональных данных на разрабатываемые стартапами инновации / О.В. Сушкова // Цифровая трансформация: вызовы праву и векторы научных исследований: моногр. / под общ. ред. А.Н. Савенкова; отв. ред. Т.А. Полякова, А.В. Минбалева. — М.: Институт государства и права РАН, 2020. — С. 159–170.

ОСОБЕННОСТИ ПРОЕКТНОГО ОБРАЗОВАНИЯ В ЮРИДИЧЕСКОМ ВУЗЕ

FEATURES OF PROJECT EDUCATION IN A LAW SCHOOL

**Бабаева
Сабина Шамильевна**

*Магистрант 2 курса магистерской программы
«Магистр IT-LAW» Московского государственного
юридического университета
имени О.Е. Кутафина (МГЮА)*



**Babaeva
Sabina Shamil'evna**

*Master's student of the 2nd year of the Master's program
"IT-LAW Master" of the Moscow State Law University
named after O.E. Kutafina (Moscow State Law Academy)*

Аннотация. Актуальная проблема современного образования — разработка эффективной формы профессионального образования, которая подразумевает направленность на практическую ориентированность студентов. Проектное обучение отличается от традиционного, оно позволяет расширять знания в разных областях и развивать критическое мышление. Наиболее существенными особенностями проектного обучения являются его диалогичность, проблемность, интегративность и контекстность. На сегодняшний день метод проектов является одним из самых востребованных в мире, так как позволяет сочетать теоретические знания и их практическое применение. Следовательно, можно сделать вывод, что проектная деятельность в условиях совершенствования высшего образования должна выступить в качестве средства адаптации к будущей профессиональной деятельности и более взвешенного выбора юридического профиля.

Ключевые слова: образование, модели профессионального образования, проект, проектная деятельность, практико-ориентированная деятельность, проектная документация.

Abstract. The actual problem of modern education is the development of an effective form of professional education, which implies a focus on the practical orientation of students. Project-based learning is different from traditional learning, it allows you to expand your knowledge in different areas and develop critical thinking. The most significant features of project-based learning are its dialogic, problematic, integrative, and contextual nature. To date, the project method is one of the most popular in the world, as it allows you to combine theoretical knowledge and their practical application. Therefore, it can be concluded that project activities in the context of improving higher education should act as a means of adaptation to future professional activities and a more balanced choice of legal profile.

Keywords: education, models of professional education, project, project activity, practice-oriented activity, project documentation.

На сегодняшний день одной из актуальных проблем современного образования в юридических вузах является проблема разработки эффективной модели профессионального образования, включающей в себя практическую ориентированность студентов на реальную юридическую деятельность под руководством преподавателей, которые посредством контроля студентов будут учить их, указывать на ошибки и помогать в их устранении. Вся эта деятельность как раз и предполагает проектное образование (обучение).

Проектное обучение является такой моделью обучения, которая выходит за рамки традиционного, привычного образования. Знания, полученные в ходе данного обучения, являются долгосрочными, так как в процессе студент обращается к разным дисциплинам и сферам. Проекты направлены на работу студентов с большим уклоном на практику. Суть проектов заключается в расширении знаний в разных областях, взаимодействии друг с другом, а также в развитии критического мышления.

Целями проектного обучения являются:

1. Способствование повышению личной уверенности у каждого обучающегося, его самореализации и рефлексии.
2. Развитие у обучающихся осознания значимости коллективной работы для получения результата, роли сотрудничества, совместной деятельности в процессе выполнения различных проектов.
3. Развитие исследовательских умений (анализ проблемных ситуаций, выявление проблем, отбор необходимой информации из литературы, наблюдение и анализ практических ситуаций, сравнение, обобщение, выводы) [1].

Использование проектов, как одной из частей обучения, не является новой идеей, но теория проектного обучения представляет собой нечто другое. Проектное обучение не рассматривается как что-то дополнительное, оно является неотъемлемым компонентом обучения. История проектного метода в педагогике берет начало с конца XVI в. с внедрения проектной

работы в школах по обучению архитектуре в Европе. Изначально при помощи проектов педагоги пытались решить двуединую задачу: обеспечить прикладной характер процесса обучения и развить творческие способности будущих архитекторов. Однако проекты, выполняемые обучающимися, носили, в основном, гипотетический характер, развивающий преимущественно воображение, поскольку не имели реального «продукта» (выстроенного здания, памятника и т.д.), созданного в результате процесса проектирования.

Уходя своими корнями в конструктивизм, проектное обучение обосновывается работами таких психологов и воспитателей, как Лев Выготский, Джером Брунер, Жан Пиаже и Джон Дьюи [2]. Учение конструктивизма основано на активном участии учеников в решении проблем и критическом мышлении. Основная задача, которая стояла перед учениками, — контролировать свое обучение и находить свои ответы, используя все изобилие источников из разных сфер.

В своих работах Дьюи особенно подчеркивает, что опыт важнее теории. Он считает, что для того, чтобы научиться думать и рассуждать, необходимо решать настоящие проблемы, которые возникают по мере приобретения опыта. Процесс такого обучения позволяет ученикам извлекать пользу в процессе выполнения заданий (проектов), а не от их результатов, в этом его главная суть — получение практического опыта.

В отечественной педагогике начала XX в. метод проектов рассматривался как средство:

- всестороннего упражнения ума и развития мышления (П.Ф. Каптерев [3]);
- формирования творческих способностей (Блонский П.П. [4]);
- подготовки воспитанников к профессиональной деятельности (А.С. Макаренко [5]);
- слияния теории и практики в обучении (Е.Г. Касаров, М.В. Кружкина, В.В. Игнатъев, В.Н. Шульгин [6]).

В работах отечественных авторов проектирование рассматривается:

- как процесс создания условий, обеспечивающих единство личностных и предметных целей, превращения потенциальных возможностей учащихся в актуальные (А.П. Тряпицина [7]);
- как интеллектуальная по своему характеру деятельность, призванная до «пробы в реальном материале» исследовать, предвидеть, спрогнозировать, оценить последствия тех или иных замыслов (В.Е. Радионов [8]);
- как средство становления системы ценностных ориентаций каждой личности, возможностей самореализации (И.С. Батракова [9]).

Наиболее существенными особенностями проектного обучения являются его диалогичность, проблемность, интегративность и контекстность.

Диалогичность позволяет в процессе выполнения проекта вступать в диалог как с собственным Я, так и с другими людьми. Именно в диалоге, как утверждалось М.М. Бахтиным, осуществляется «свободное самоот-

кровение личности». Диалог в проектной технологии выполняет функцию специфической социокультурной среды, которая создает условия для принятия нового опыта, вследствие чего полученная информация становится личностно значимой [10].

Проблемность возникает при разрешении сложной ситуации, которая обуславливает начало активной мыслительной деятельности у обучающихся. Решение проблемы нередко приводит их к оригинальным, нестандартным способам деятельности и результату.

Контекстность в проектной технологии позволяет создавать проекты, приближенные к естественной жизнедеятельности обучающихся.

Интегративность проектной технологии «означает оптимальный синтез сложившихся концепций усвоения знаний и теорий обучения студентов» [11].

Использование проектного обучения имеет ряд своих преимуществ. Когда обучающимся дается возможность самостоятельно руководить своим проектом, над которым они работают для получения практического опыта, у них появляется мотивация. Вследствие глубины исследования, студенты изучают гораздо больший объем информации одновременно в нескольких областях, не заикливаясь на какой-то конкретной науке.

В ходе различных исследований было выяснено, что у обучающихся, задействованных в проектное обучение, более высокий уровень мышления и развития навыков. Информация, которую они получают, имеет большую вероятность перейти в другие контексты [12].

Несмотря на то, что у проектного обучения существует множество плюсов, при его использовании могут возникнуть и определенные трудности. Первое — это большое количество времени, которое требуется, как на подготовку, так и на претворение проектной деятельности в жизнь. Другим препятствием является то, что, многие обучающиеся до поступления в вузы проводят годы в классах, где практикуется традиционное обучение, к тому времени, как они впервые сталкиваются с проектным. Вследствие чего у некоторых студентов и преподавателей возникает дискомфорт при переходе от старой модели обучения к более модернизированной.

Необходимость использования метода проектов в профессиональной подготовке юристов продиктована спецификой юридического образования. Как правило, при обучении на юридическом факультете существует профилизация, которая предусматривает выбор студентом определенной сферы своей будущей профессиональной деятельности в рамках гражданско-правовой, государственно-правовой или уголовно-правовой специализации. Данный выбор обусловлен тем, что студент должен определиться с дальнейшим направлением своей деятельности, которое ему наиболее близко. Зачастую студенты не всегда могут правильно определить сферу, которая им больше импонирует, вызывает интерес, так как у них не бывает практического опыта, который бы наглядно продемонстрировал им каждое направление. В данном

случае проектная деятельность являлась бы незаменимым помощником в решении вопроса. Неправильный выбор профиля может привести к тому, что учащийся юридического факультета будет вынужден после окончания обучения в рамках практической деятельности срочно менять профиль и тратить свое время и силы для восполнения пробелов в знаниях по новому профилю.

Проектный подход в обучении призван, с одной стороны, обеспечить развитие у студентов аналитического мышления и практических навыков решения юридических проблем по выбранному направлению, а с другой — включить их в научно-исследовательскую и экспертную работу. Это предусматривает создание проектных групп, где вместе с преподавателями и практиками обучающиеся работают над решением актуальных научных и практических задач. Традиционные формы курсовой и выпускной квалификационной работы должны органично сочетаться с проектной деятельностью студентов.

Эта работа требует принятия локальных документов вуза, утверждающих методику и порядок осуществления проектной деятельности обучающихся и устанавливающих: порядок выбора темы и её конкретизация; определение цели и формирование задач проекта; определение методологии проекта; порядок и условия формирования проектных групп; распределение обязанностей участников проектной группы; определение требований к результатам проекта и сроки его выполнения; установление процедур и критериев оценки проекта и формы его представления; определение видов и форм отчетной документации; порядок проведения публичной защиты и другие формы представления результата проекта.

Для активизации проектной работы также должны быть созданы механизмы материального стимулирования студентов, магистрантов и аспирантов, показывающих хорошие результаты в проектной деятельности.

На сегодня метод проектов является одним из самых востребованных в мире, так как позволяет сочетать теоретические знания и их практическое применение. Следовательно, можно сделать вывод, что проектная деятельность в условиях совершенствования высшего образования должна выступить в качестве средства адаптации к будущей профессиональной деятельности и более взвешенного выбора юридического профиля. Также она позволит студентам развивать

навыки самообучения и самостоятельного поиска необходимой информации для разработки и реализации своих дальнейших проектов.

Список литературы

1. Середенко П.В. Развитие исследовательских умений и навыков младших школьников в условиях перехода к образовательным стандартам нового поколения: моногр. / П.В. Середенко. — Южно-Сахалинск: СахГУ, 2014. — 208 с.
2. Гончаров В.С. Психология проектирования когнитивного развития: моногр. / В.С. Гончаров. — Курган: Изд-во Курганс. гос. ун-та, 2005. — 235 с.
3. Историко-педагогический журнал: Научное издание ФГБОУ ВПО «Нижегородская государственная социально-педагогическая академия». — 2014. — №3. — 220 с.
4. Блонский П.П. Избранные педагогические произведения / П.П. Блонский. — М.: Изд-во Акад. пед. наук РСФСР, 1961. — 696 с.
5. Петрова Н.П. Реализация метода проектов в подготовке педагога (на примере гуманитарных дисциплин): моногр. / Н.П. Петрова, С.Р. Халилов. — Ставрополь: СКФУ, 2015. — 196 с.
6. Ситаров В.А. Теория обучения. Теория и практика: учеб. для бакалавров / В.А. Ситаров. — М.: Юрайт, 2019. — 447 с.
7. Теория и практика педагогического проектирования индивидуальных образовательных программ: учеб. пособие / Т.И. Боровкова. — Владивосток: ДФУ, 2015. — 160 с.
8. Дюков В.М. Современные наукоемкие технологии / В.М. Дюков, Г.С. Пьянкова. — 2010. — № 9 — С. 80–83.
9. Теория и практика педагогического проектирования индивидуальных образовательных программ: учеб. пособие / Т.И. Боровкова. — Владивосток: ДФУ, 2015. — 160 с.
10. Богуславская С.М. Диалог в трудах М.М. Бахтина / С.М. Богуславский // Вестник ОГУ. 2011. — №7(126), июль. — 23 с.
11. Проективная дидактика [Электрон. ресурс]: моногр. / Э.Ф. Зеер, С.Н. Уткина. — Екатеринбург: Изд-во Рос. гос. проф.-пед. ун-та, 2017. — 131 с. — Режим доступа: <http://elar.rsvpu.ru/978-5-8050-0630-3>.
12. Сушкова О.В. Использование интерактивного метода проведения игр на практических занятиях: постановка проблемы / О.В. Сушкова // Московский юридический форум онлайн — 2020: сб. тез. докл. — В 4 ч. Ч. 2. — М.: РГ-Пресс, 2020. — С. 53–57.

ТЕОРИЯ И ПРАКТИКА ПРОЕКТНОГО ОБРАЗОВАНИЯ

№1(17)/2021

Подписано в печать 12.03.2021
Формат 60x90/8 Бумага офсетная. Гарнитура Gilroy.
Усл. печ. л. 10,4. Тираж 900 экз. Заказ 015 от 12.12.2020

Издательство
ООО «Фабрика галтовочного оборудования и технологий – инжиниринг»
(«ФАГОТ-ИНЖИНИРИНГ»),
107241, г. Москва, Черницынский проезд, д. 3.
Отпечатано в типографии
ООО «Белый ветер»
115054, Москва, ул. Щипок, д. 28.



2587-5922