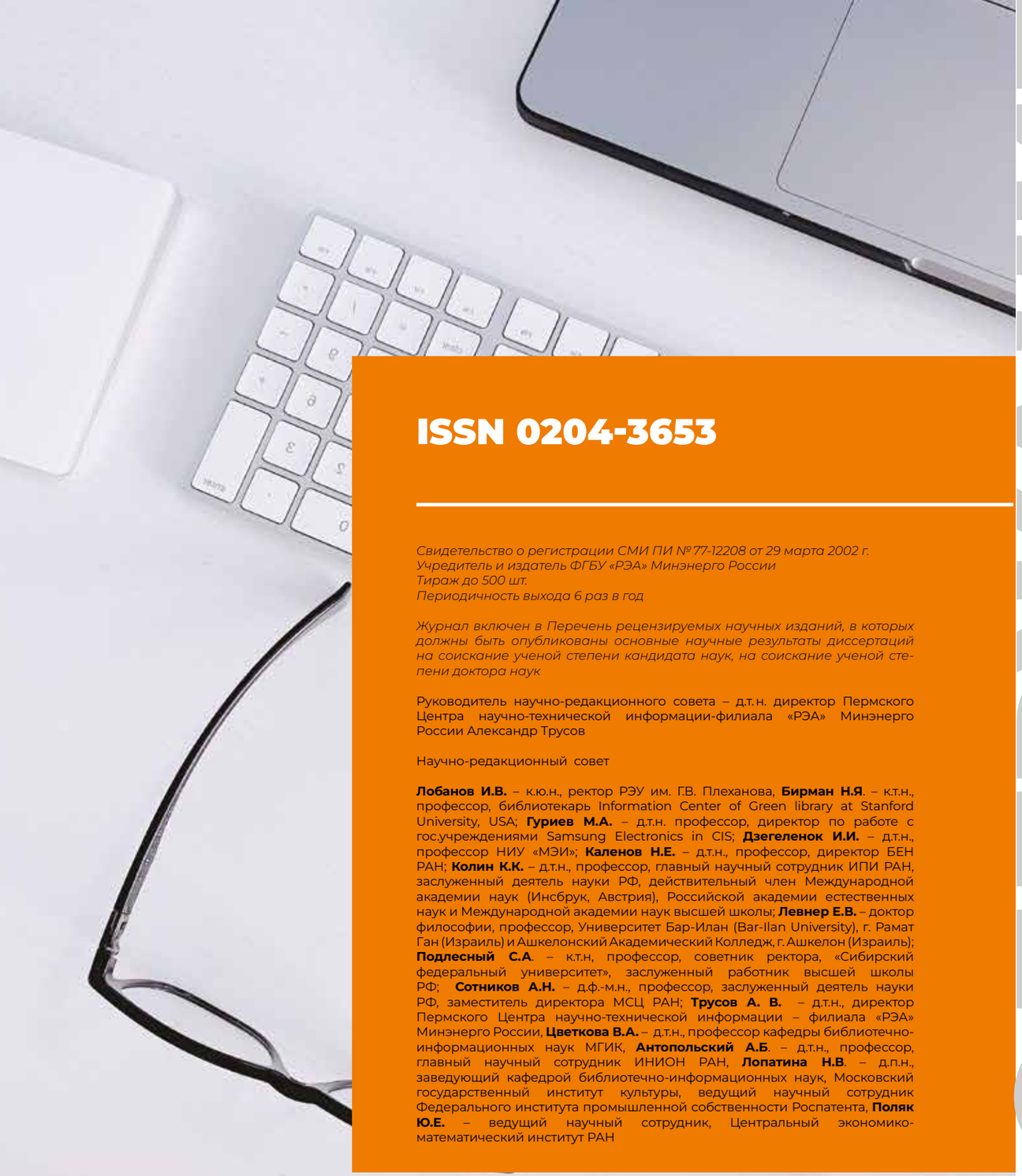
УЧРЕДИТЕЛЬ ЖУРНАЛА
РЭА МИНЭНЕРГО РОССИИ

ISSN 0204-3653

ИНФОРМАЦИОННЫЕ РЕСУРСЫ РОССИИ

03 [187] 2022

t.me/irr_rea /rosenergo.gov.ru irr@rosenergo.gov.ru



ISSN 0204-3653

Свидетельство о регистрации СМИ ПИ № 77-12208 от 29 марта 2002 г.
Учредитель и издатель ФГБУ «РЭА» Минэнерго России
Тираж до 500 шт.
Периодичность выхода 6 раз в год

Журнал включен в Перечень рецензируемых научных изданий, в которых должны быть опубликованы основные научные результаты диссертаций на соискание ученой степени кандидата наук, на соискание ученой степени доктора наук

СОДЕРЖАНИЕ

Содержание

ИНФОРМАЦИОННЫЕ РЕСУРСЫ РОССИИ

INFORMATION RESOURCES OF RUSSIA

Contents

ОТ РЕДАКЦИИ

Синергия индустриализации, цифровизации и информатизации

Сегодня перед нашей страной стоит задача повышения технологической независимости и конкурентоспособности на мировых рынках. Важное значение приобретает обеспечение инновационного развития и создание высокотехнологичного промышленного комплекса, базирующегося на передовых отечественных научных разработках.

Решение должно строиться на системном научном объединении разных направлений развития экономики: автоматизации, цифровизации, экологичности, информатизации и социальной ориентированности.

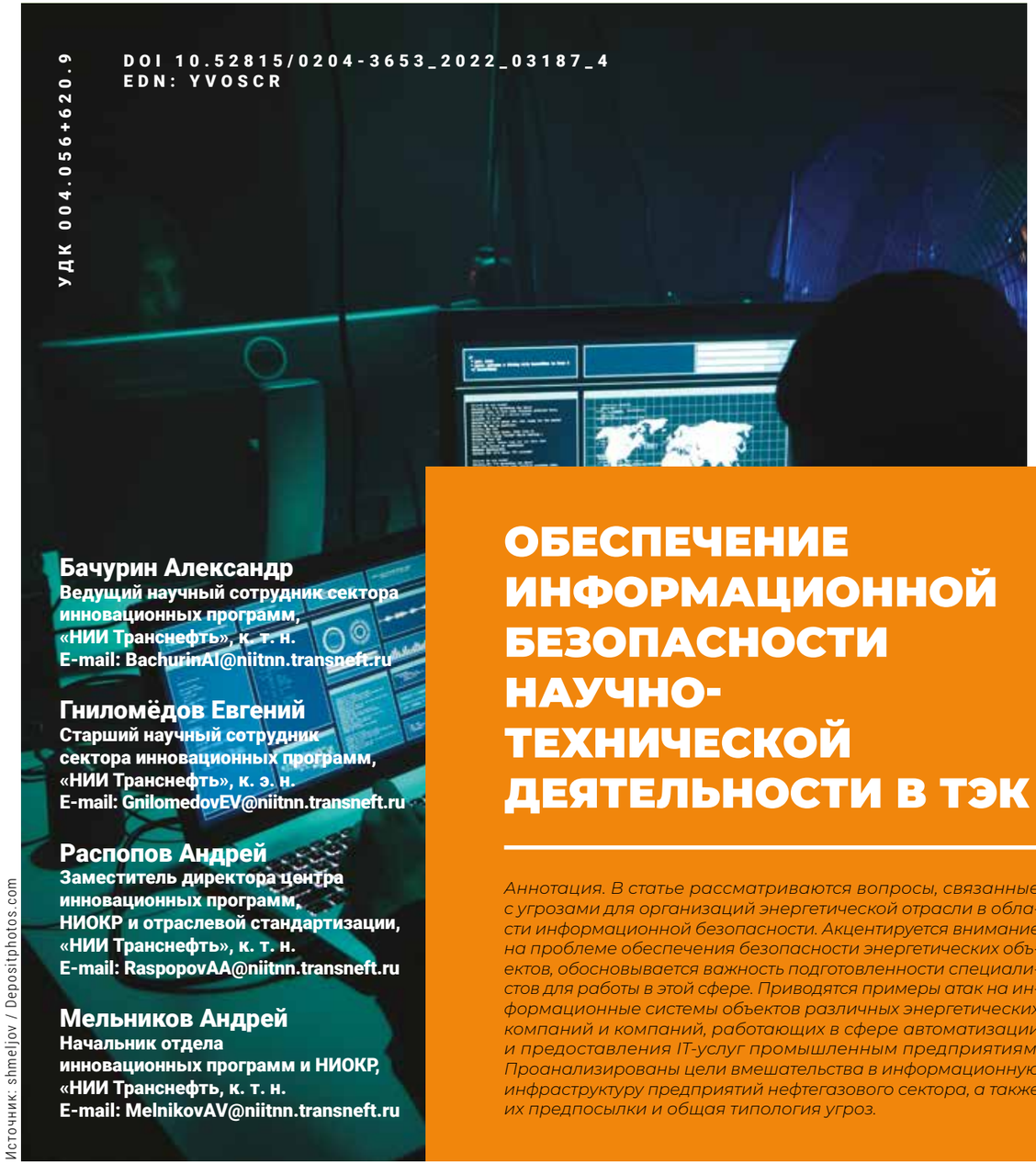
РЭА Минэнерго России занимается разработкой, анализом и систематизацией таких подходов, подготовкой программ поэтапного внедрения новых технологических платформ в отечественном производстве и развитием высокопрофессиональных кадров.

Данная работа требует концептуального видения технологической трансформации ключевых отраслей экономики и предоставления исчерпывающей информации о последних тенденциях в научно-производственных и цифровых сферах.

Журнал «ИРР», издаваемый РЭА Минэнерго России, призван стать флагманом этой трудоемкой работы. Он будет систематизировать опыт реализации научных, цифровых и индустриальных инноваций, содействовать формированию требований к внедряемым решениям и обеспечивать синергию в работе разных отраслей.

Генеральный директор
ФГБУ «РЭА» Минэнерго России,
Алексей Кулапин

УДК 004.056+620.9
DOI 10.52815/0204-3653_2022_03187_4
EDN: YVOSCR



Источник: shmeljov / Depositphotos.com

Бачурин Александр
Ведущий научный сотрудник сектора инновационных программ, «НИИ Транснефть», к. т. н.
E-mail: BachurinAI@niitnn.transneft.ru

Гниломёдов Евгений
Старший научный сотрудник сектора инновационных программ, «НИИ Транснефть», к. э. н.
E-mail: GnilomedovEV@niitnn.transneft.ru

Распопов Андрей
Заместитель директора центра инновационных программ, НИОКР и отраслевой стандартизации, «НИИ Транснефть», к. т. н.
E-mail: RaspopovAA@niitnn.transneft.ru

Мельников Андрей
Начальник отдела инновационных программ и НИОКР, «НИИ Транснефть, к. т. н.
E-mail: MelnikovAV@niitnn.transneft.ru

ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ НАУЧНО-ТЕХНИЧЕСКОЙ ДЕЯТЕЛЬНОСТИ В ТЭК

Аннотация. В статье рассматриваются вопросы, связанные с угрозами для организаций энергетической отрасли в области информационной безопасности. Акцентируется внимание на проблеме обеспечения безопасности энергетических объектов, обосновывается важность подготовленности специалистов для работы в этой сфере. Приводятся примеры атак на информационные системы объектов различных энергетических компаний и компаний, работающих в сфере автоматизации и предоставления IT-услуг промышленным предприятиям. Проанализированы цели вмешательства в информационную инфраструктуру предприятий нефтегазового сектора, а также их предпосылки и общая типология угроз.

Ключевые слова: *ТЭК, новые технологии, информационная безопасность, инновационное развитие, технологические риски, информационная система, риски, угрозы, программное обеспечение, киберугрозы, фишинг, кибербезопасность, корпоративная безопасность.*

Анализ показывает непрерывный рост противозаконных инцидентов, направленных на причинение ущерба корпоративным информационным системам и процессам

Прогресс в развитии науки и техники привел к созданию информационного пространства знаний, сформированного современными методами и средствами обеспечения их жизненного цикла. Он превратил информацию в ценный ресурс, который требует комплексной защиты.

В деятельности современных организаций значительно выросли объем используемой информации, а также ее техническая и экономическая ценность. По этой причине появилась острая необходимость управления данным активом. Обеспечение эффективности работы в условиях быстрого роста объемов информации потребовало формирования, поддержания и развития сложной телекоммуникационной и вычислительной инфраструктуры, предоставления пользователям выделенного доступа на любом физическом расстоянии к любым объемам знаний за максимально короткий период времени.

Фактически информация и соответствующая информационная инфраструктура приобрели роль главного ресурса интеллектуальной и инновационной деятельности, которой в числе прочих требуется обеспечение силами и средствами информационной безопасности.

Эффективное и стабильное развитие предприятий в подобных условиях во многом основывается на расширении необходимого потенциала автоматизации и цифровизации, а также на всесторонней поддержке совершенствования инфраструктуры и компетенций сотрудников в данной сфере. Недостаточный объем материальных вложений и трудовых затрат в указанной области может послужить фактором резкого снижения эффективности производственной и экономической деятельности предприятия и привести к полной потере конкурентоспособности.

В свою очередь, развитие энергетической отрасли полностью соответствует современным трендам, связанным с новыми технологиями. Крупные добывающие, транспортные и генерирующие компании следят за передовыми разработками и внедряют их в свою деятельность. В настоящее время деятельность компаний энергетического сектора характеризуется широким использованием информационных систем управления производственными процессами, предоставляющих ряд преимуществ, например:

- при поиске месторождений и добыче ресурсов: анализ данных в режиме онлайн из любых территориальных локаций с целью интеллектуального прогнозирования работ по диагностике и поддержанию технического состояния объектов;
- при транспортировке жидких углеводородов по трубопроводам и другими способами: анализ

Диспетчерская «Транснефть»
Источник: siberia.transneft.ru

данных от систем обнаружения утечек и контроля активности для парирования рисков аварий и несанкционированных действий на объектах;
– при переработке и сбыте жидких углеводородов: оптимизация периодов простоя специализированного оборудования, организация непрерывного доступа к информации о производственной деятельности на предприятиях [1].

Наравне с неоспоримыми преимуществами использования новых технологий их развитие связано с обеспечением защиты от вредоносных кибервоздействий, что в свою очередь, заставляет менеджмент организаций и компаний обратить пристальное внимание на обеспечение информационной безопасности.

В профильной литературе под информационной безопасностью часто фигурируют понятия, зависящие от ее контекста. Концептуальный подход к построению целостной модели информационной безопасности вызывает необходимость задания ключевых понятий в составе информационных отношений, требует определения субъектов таких отношений, их возможностей и интересов, оценки угроз, установления способов и задач защиты информации. В настоящей статье под информационной безопасностью понимается совокупность условий, сил и средств обеспечения защищенности выделенного объема данных, а также сопутствующей им инфраструктуры. Под объектами понимаются информационные системы, посредством которых осуществляются техническими способами процессы жизненного цикла информации. Субъекты – специалисты и профильные подразделения, которые обеспечивают информационную безопасность. Непосредственно информационная безопасность обеспечивается соответствующими силами и средствами, реализующими защиту информации и инфраструктуры от несанкционированных действий.

В контексте рассматриваемой проблемы можно выделить два вида опасных воздействий на информационные ресурсы: неправомерное внедрение недостоверной информации и потеря ценной информации из-за различных внешних и внутренних факторов. Оба вида воздействий создают комплекс угроз основной деятельности и снижают ее эффективность.

Таким образом, под информационной безопасностью понимается целостная система, которая одновременно позволяет обеспечить устойчивость и эффективность полноценной производственной деятельности, защищая от внешних и внутренних угроз [2], соблюдение требований к работе с конфиденциальной информацией и надежную работу информационных систем.

Возвращаясь к основной теме, следует отметить, что предприятия энергетического сектора в силу специфики деятельности относятся к объектам критически важной инфраструктуры. От их бесперебойной, стабильной работы зависят снабжение необходимыми услугами граждан, организаций и предприятий, обеспечение ресурсами производственных процессов в промышленности, строительстве и других отраслях экономики, а также стабильность и безопасность государства в целом.

Компании энергетической сферы осознают преимущества использования идей и подходов цифровизации, предоставляющей возможность вывести активно развивающийся процесс информационно-технического перевооружения на новый уровень, и обеспечить доступность результатов обработки и анализа данных.

Существенные технологические риски энергетических предприятий связаны с возможными авариями, которые могут привести к серьезным экологическим проблемам, изменить ситуацию на мировых сырьевых рынках, а также повлиять на социальные процессы в обществе. В этой связи вопросы информационной безопасности организаций топливно-энергетической сферы привлекают серьезное внимание специалистов, руководителей компаний и организаций. Особенно актуальной данная проблема становится в условиях роста количества атак на информационные системы объектов различных энергетических компаний и компаний, работающих в сфере автоматизации и предоставления IT-услуг промышленным предприятиям, в том числе нефтегазовым. Приведем несколько фактов:

1. Трубопровод «Баку – Тбилиси – Джейхан» в Турции. Отключена система сигнализации и связи, результатом чего стал разлив более 30 000 баррелей нефти. Злоумышленники отключили все аварийные системы на трубопроводе, а также автоматический клапан, который должен был предотвратить разлив нефти из трубопровода в случае его неисправности или подрыва [3].
2. Саудовская национальная нефтегазовая компания Saudi Aramco. Кибератака, в результате которой повреждены 30 000 компьютеров. Инцидент произошёл 15 августа 2012 г., злоумышленники использовали компьютерный вирус, известный как Shamoon. Целью атаки было остановить добычу нефти и нарушить поставки углеводородов на местный и международные рынки. В Saudi Aramco сообщили, что вирус поразил офисные компьютеры, с жестких дисков которых оказалась стерта информация, но системное программное обеспечение, отвечающее за производство, не пострадало [4].
3. Компания Telvent. Нарушение в 2012 г. внутренней системы защиты производителя специализированного технического обеспечения удаленного управления и контроля процессов в сфере энергетики. Произошло хищение данных проекта Oasys Supervisory Control and Data Acquisition (SCADA) посредством инструментов удаленного управления. Эксперты высказали мнение, что задачей данных действий злоумышленников стало получение доступа к исходному коду проекта для поиска и изучения уязвимостей в нем, что могло позволить в дальнейшем получить возможности хакерам проводить информационные атаки на предприятия топливно-энергетического комплекса [5].

Офис Saudi Aramco
Источник: neftianka.ru

4. Colonial Pipeline (США). Атака вредоносного ПО на американскую трубопроводную систему Colonial Pipeline 7 мая 2021 г. Вмешательство остановило работу всех трубопроводов системы на пять дней. Атака была совершена хакерской группой DarkSide. За день до атаки та же группа похитила 100 гигабайт данных с серверов компании. При этом работа трубопровода была полностью компьютеризирована, а техническая система управления соединена с административной, что упростило злоумышленникам проникновение через электронную почту. Пароль к этому аккаунту, как заявили в Mandiant, был обнаружен среди слитых в «даркнет» паролей и мог подходить также и к другим принадлежащим компании аккаунтам, которые могли быть взломаны ранее [6].
5. Вирус STUXNET применялся с целью получения контроля над производственными системами управления (ICS) в различных странах, в том числе в организациях топливно-энергетического комплекса в 2010 г. Важно подчеркнуть, что до данного вируса в области средств автоматизации на предприятиях не уделяли должного внимания средствам активной безопасности, так как физическое разделение оборудования от интернета считалось безопасным фактором. Но STUXNET смог проникнуть в локальные компьютеры, что создало новое направление в сфере кибербезопасности [7].
6. Вирус FLAME. Заражение компьютерных систем крупнейшего катарского экспортера СПГ Rasgas в 2012 г. Распространяемая вредоносная программа использовалась для целей шпионажа [8].

Анализ хакерских атак на инфраструктуру предприятий нефтегазового сектора показал, что в большинстве случаев они преследовали следующие цели:

1. Политические. Использование внешнего вмешательства в политических целях. Например, перехват управления средствами контроля трубопровода может привести к остановке передачи сырья или аварии, что способно спровоцировать конфликтные ситуации международного масштаба, внутригосударственную социальную нестабильность.
2. Экономические. Вмешательство в системы крупных добывающих или транспортных компаний может снизить или прекратить поставки большого количества

Рис. 1. Результаты технических аудитов в части оценки уязвимостей информационных систем

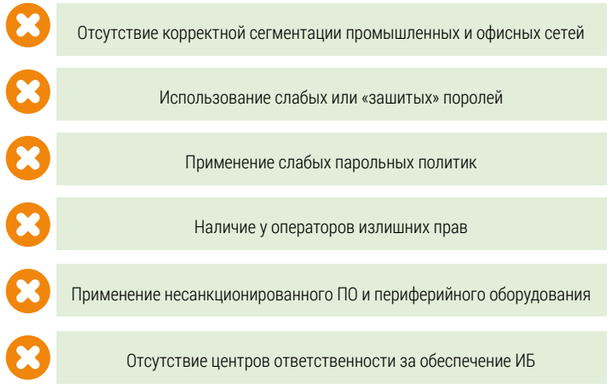


Рис. 2. Информационная модель угроз и защиты

энергоносителей на мировой рынок, что в свою очередь отразится на стоимости сырья и производных продуктов для потребителей.

3. Террористические. Террористические организации для реализации своих целей атакуют объекты нефтегазового сектора, рассчитывая на широкий социальный резонанс и большое количество потерпевших.

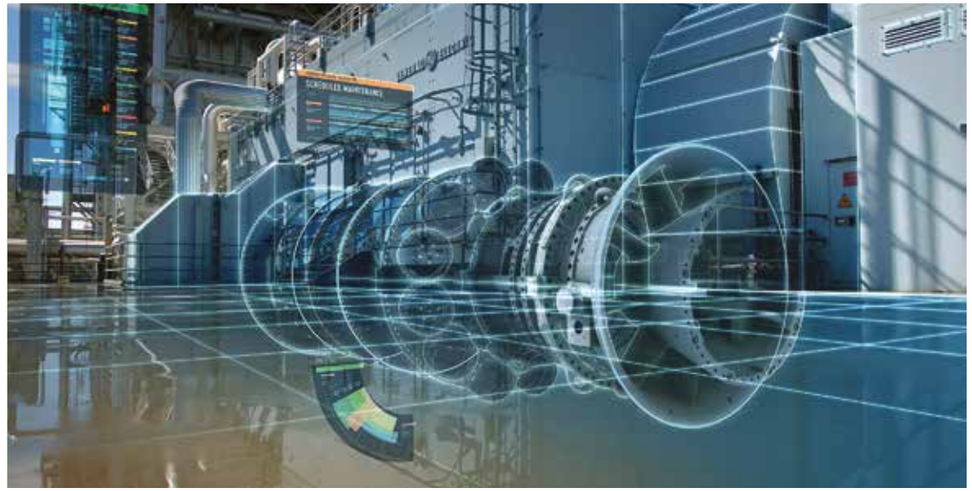
В качестве наиболее часто встречаемых инструментов в арсенале злоумышленников можно выделить [9]: фишинговые и шпионские программы; спам; DDos-атаки; вирусы (шифровальщики, трояны, программы для взлома и нарушения функционирования систем).

Увеличивающееся количество хакерских атак и попыток вмешательства в производственные процессы посредством воздействий на объекты информационной инфраструктуры продемонстрировали уязвимость систем, широко применяемых на предприятиях энергетического сектора. Среди предпосылок уязвимости информационной защиты объектов топливно-энергетического комплекса можно выделить следующие:

– несоответствие технологического уровня организаций топливно-энергетического комплекса современным мировым требованиям безопасности в данной сфере;
– зависимость от поставок оборудования, технологий, материалов и услуг, программного обеспечения монопольных производителей;
– недостаточность специалистов, имеющих соответствующие образование, опыт и квалификацию;
– неподготовленность персонала к атакам, а также недостаток знаний сотрудников в области предотвращения и снижения эффективности вмешательства в процесс функционирования информационной инфраструктуры.

Несовершенство защиты информационной инфраструктуры подтверждают результаты многочисленных технических аудитов, которые показывают следующие основные распространенные проблемы защиты информационных систем (рис. 1) [10].

Принципы работы системы информационной безопасности [11, 12] можно представить следующим образом (рис. 2):



Digital Twin цифровой двойник NX 1915 Siemens
Источник: akspic.ru

– объективная обоснованность уровня защиты и предъявляемых требований к системам, комплексная оценка рисков преодоления защиты;
– обеспечение бесперебойной работы и дублирования средств защиты, готовность к потенциальной возможности блокировки работы систем в случае преодоления защиты;
– регламентация информационной деятельности посредством корпоративных документов;
– достаточный объем сил и средств информационной безопасности в соответствии с заданным уровнем защиты.

Стоит обратить внимание, что при формировании концептуальной модели информационной безопасности целесообразно учитывать в первую очередь следующие элементы [13]: угрозы, риски, ущерб, уровень безопасности, субъекты нарушений, средства безопасности.

Под риском понимается негативный инцидент вследствие внутренней или внешней угрозы, который обладает вероятностью появления и нанесения какого-либо ущерба.

Рассматривая термин «риск», следует понимать, что он является одним из базовых в сфере безопасности в целом, и в информационной безопасности в частности. В информационной безопасности снижение рисков включает в себя задачи по решению проблем вероятности возникновения угроз информации, определения их причин, первоисточников, слабых мест в периметрах защиты, установления методов защиты, вероятностную оценку следствий наступления угроз. Также вопросы рисков связаны с задачами управления, экономики и технологий в части формирования физической архитектуры систем информационной безопасности [14].

Стоит отметить, что помимо технологических, экономических, политических появляются новые риски, которые ранее широко не фиксировались. Среди них необходимо выделить такой риск, как введение различных санкционных мер в отношении компаний, отдельных секторов экономики, а также целых государств. Санкции, лишая игроков выходов на прибыльные рынки доступа к современным разработкам и финансовым инструментам, становятся инструментом недобросовестной конкуренции. Наиболее эффективным средством борьбы в этом случае становится политика, направленная на импортозамещение, позволяющая создавать собственную инфраструктуру для независимой, бесперебойной работы, и поиск новых рынков сбыта.

Типологию угроз в сфере информационной безопасности, в том числе в энергетическом секторе, исходя из направлений их потенциального влияния, можно представить следующим образом [15]:
– элементы информационных ресурсов (пользователи информации, непосредственно информация, программное и аппаратное обеспечение);
– аспекты информационной безопасности (целостность, доступность, конфиденциальность);
– территориальное размещение объектов и субъектов, формирующих угрозы (внешнее, внутреннее относительно организации и географии региона расположения);
– характерные особенности причин возникновения угроз (целенаправленные, форс-мажор, человеческий и технический фактор).

В сложившейся ситуации среди основных задач информационной безопасности ТЭК можно выделить следующие:
– защита персональных вычислительных машин;
– защита корпоративных и персональных данных;
– обеспечение требований профильных регуляторов;
– исключение утечек информации.

В целом, рассмотренная модель информационной безопасности позволяет формировать подходы к реализации целостных систем комплексной защиты посредством необходимых и достаточных сил и средств безопасности, определять субъекты и объекты информационных процессов [16].

Учитывая вышесказанное, необходимо учитывать, что вопросы информационной безопасности зависят от особенностей ин-

БЕЗОПАСНОСТЬ

Единая система диспетчерского управления нефтепроводами
Источник: vostok.transneft.ru

формационных ресурсов и отраслей их использования, а также от размеров и функциональной сложности организации. В рамках систем, ограниченных одной организацией на одной территории, средства информационной безопасности являются технически и административно менее сложными, чем в распределенных ресурсах крупных компаний. Распределенные системы предполагают значительное число пользователей, обладающих различными ролями, размещение на удаленных территориях элементов информационных ресурсов, протяженные каналы коммуникации, а также различные программно-аппаратные комплексы.

Информационная безопасность распределенных систем основывается на выявлении уровней уязвимости элементов систем, прогнозирования и анализа потенциальных угроз, классификации субъектов информационной деятельности (авторы информации, пользователи, персонал поддержки информационной инфраструктуры и т. п.).

Информационные ресурсы с точки зрения их целостности, доступности и конфиденциальности определяют базовые основы информационной безопасности.

Доступность реализуется посредством доступа к информации в рамках заданного времени авторизованным субъектам согласно выделенным правам по функциональным ролям в системах и регламентированным требованиям.

Целостность реализуется посредством процедур защиты информации от модификации ее содержания и структуры любыми несанкционированными способами, также обеспечением логичности и полноты.

Конфиденциальность реализуется посредством защиты информации на всем ее жизненном цикле со строгим соблюдением выделенного доступа к ней.

Уровни защиты информационных ресурсов, их уязвимости [17]:

- организационно-управленческий, включающий в себя административные, организационные работы, определяющие нормативные требования к информационным процедурам и системам в части формирования и реализации политики информационной безопасности, систем управления;
- физический включает силы и средства технической защиты программного и аппаратного обеспечения, в том числе обоснованность выбора конкретных типов и производителей с учетом долгосрочной надежности соответствующих поставщиков, что особенно актуально в текущих условиях международных ограничений;
- профессиональный определяется уровнем квалификации профильных сотрудников подразделений информационных технологий и информационной безопасности;
- логический определяет целостность концептуального базиса методов информационной безопасности, интеллектуального шифрования и дешифрования информации.

Подводя итоги, можно констатировать, что энергетический сектор во всем мире консервативен и достаточно медленно обновляет инфраструктуру, включая технические средства и программное обеспечение. Данный факт в совокупности с тем, что энергетические объекты представляют собой критическую инфраструктуру, повышает риски и делает ТЭК одной из главных целей атак. Последствия атак на ИТ-инфраструктуру энергетических компаний непредсказуемы, поэтому постоянное отслеживание рисков, касающихся киберугроз, может стать залогом получения организациями дополнительной важной информации о характере потенциальных атак, а также об их источниках и разработчиках, анализ которой даст возможность своевременно разработать ответные меры для их предотвращения или снижения негативных последствий.

Проведенный анализ литературы и опыта российских и иностранных компаний, подвергшихся атакам, позволяют сделать следующие выводы:

1. Выявление векторов атак, наиболее часто влияющих на отрасль, становится основой построения эффективной системы защиты.

Нефтяные резервуары The Colonial Pipeline
Источник: EPA / the-sun.com

2. Применение операционных систем и программного обеспечения, входящих в реестр российского ПО, и использование различных средств защиты информации от компрометации сети.
3. Составление цифровых портретов сотрудников, облегчающее соответствующим структурам, отвечающих за безопасность, процесс выявления нежелательной активности и позволяющее своевременно остановить атаку, либо снизить ее негативное влияние.
4. Эффективное и своевременное обучение сотрудников в области противодействия киберугрозам, снижающее риск взлома и внешнего вмешательства в производственные процессы.

Немаловажную роль в борьбе с киберпреступностью и внешними вмешательствами играет менеджмент компаний и организаций. Именно от действий руководителей по выстраиванию современной и эффективной системы безопасности зависит благополучие не только отдельных игроков, но и всей энергетической отрасли [1].

В целом, стоит отметить, что анализ роста угроз организациям и объектам ТЭК показывает непрерывный рост инцидентов, связанных с противозаконными действиями, направленными на причинение ущерба корпоративным информационным системам и процессам. Следовательно, в условиях недружественной политики стран и компаний в сфере информационных технологий обретает еще большее значение обеспечение эффективной, комплексной и современной информационной безопасности ТЭК.

Получая данные о современных и актуальных угрозах безопасности, внедряя эффективные средства защиты информации, а также поддерживая проактивную безопасность и распространяя культуру осведомленности о рисках информационной безопасности среди сотрудников, компании топливно-энергетического сектора получают возможность предотвращать возможные атаки на свои ресурсы и в целом влиять на повышение устойчивости к внешним воздействиям всей отрасли.

ENSURING INFORMATION SECURITY FOR THE DEVELOPMENT OF SCIENTIFIC AND TECHNICAL ACTIVITIES IN ORGANIZATIONS OF THE FUEL AND ENERGY COMPLEX

Bachurin Alexander, Ph.D. in Engineering Science, Leading Researcher of the Innovation Programs Sector, Transneft Research Institute. E-mail: BachurinAI@niitnn.transneft.ru

Raspopov Andrey, Ph.D. in Engineering Science, Deputy Director of the Center for Innovative Programs, R&D and Industry Standardization, Transneft Research Institute. E-mail: RaspopovAA@niitnn.transneft.ru

Gnilomedov Evgeny, Ph.D. in Economics, Senior Researcher of the Innovation Programs Sector, Transneft Research Institute. E-mail: GnilomedovEV@niitnn.transneft.ru

Melnikov Andrey, Ph.D. in Engineering Science, Head of the Department of Innovative Programs and R&D, Transneft Research Institute.
E-mail: MelnikovAV@niitnn.transneft.ru

Abstract. The article discusses issues related to threats to energy industry organizations in the field of information security. Attention is focused on the problem of ensuring the safety of energy facilities, the importance of training specialists to work in this field is substantiated. Examples of attacks on information systems of facilities of various energy companies and companies working in the field of automation and provision of IT services to industrial enterprises are given. The objectives of interference in the information infrastructure of oil and gas sector enterprises, as well as their prerequisites and the general typology of threats are analyzed.
Keywords: fuel and energy complex, new technologies, information security, innovative development, technological risks, information system, risks, threats, software, cyber threats, phishing, cybersecurity, corporate security.

Библиографический список:

1. Корпоративная безопасность в нефтегазовом секторе // Neftegaz.RU – 2019. – URL: https://magazine.neftegaz.ru/articles/tsifrovizatsiya/443337-korporativnaya-bezopasnost-v-neftegazovom-sektore-protsess-obespecheniya-korporativnoy-bezopasnosti-/?ysclid=l6680f8nbg953000236
2. Жук Е.И. Концептуальные основы информационной безопасности // Наука и образование: научное издание МГТУ им. Н.Э. Баумана. № 4, 2010. С. 2.
3. Mysterious '08 Turkey Pipeline Blast Opened New Cyberwar // ИА «Bloomberg» – 2014. – URL: https://www.bloomberg.com/news/articles/2014-12-10/mysterious-08-turkey-pipeline-blast-opened-new-cyberwar
4. Саудовская Аравия рассказала о попытке хакеров сорвать экспорт нефти // ИА «Lenta.ru» – 2012. – URL: https://lenta.ru/news/2012/12/10/aramco/?ysclid=l6ujbqb8ox 496308071
5. Sequential Detection and Isolation of Cyber-physical Attacks on SCADA Systems // University of Technology of Troyes (UTT) – 2015. – URL: https://hal.archives-ouvertes.fr/tel-01352625/document
6. Эксперт предположил, что помогло хакерам атаковать Colonial Pipeline // РИА Новости – 2021. – URL: https://ria.ru/20210605/khaker-1735746582.html?ysclid =l6ukdrn0op406765144
7. Stuxnet: начало // Kaspersky Daily – 2014. – URL: https://www.kaspersky.ru / blog/stuxnet-victims-zero/6119/
8. Руководство по передовой практике защиты важнейших объектов неядерной энергетической инфраструктуры от террористических актов в связи с угрозами, исходящими от киберпространства // ОБСЕ – 2013. – URL: https://www.osce.org /files/f/documents/5/2/110472.pdf
9. Шабуня В.В. Организационно-правовые аспекты обеспечения корпоративной информационной безопасности в организациях ТЭК // Правовой энергетический форум. №1, 2022. С. 36–40.
10. Околот Д.Я. Аспекты подготовки специалистов по обеспечению информационной безопасности в сфере энергетики // Вестник молодежной науки Калининградского государственного технического университета. №3 (15), 2018. С. 7.
11. Балановская А.В. Концептуальный подход к построению системы информационной безопасности промышленного предприятия // Вестник Самарского государственного университета. Серия: Экономика и управление. №5 (127), 2015. С. 14–20.
12. Бойченко О.В., Иванюта Д.В. Модели информационной безопасности // Экономика строительства и природопользования. №3 (80). 2021. С. 33–39.
13. Медведев А.А., Созинова Е.Н. Разработка концептуальной модели информационной безопасности организации // Научно-технический вестник Поволжья. № 3, 2015. С. 175–177.
14. Аносов Р.С., Аносов С.С., Шахалов И.Ю. Концептуальная модель анализа риска безопасности информационных технологий // Вопросы кибербезопасности. № 2 (36). 2020. С. 2–10.
15. Информационная безопасность: конспект лекций / Р.Ш. Закиров. – Челябинск: издательский центр ЮУРГУ, 2014. – 73 с.
16. Родичев Ю.А., Родичев А.Ю. Системная модель защиты информации и информационных систем распределенного типа // Вестник Самарского государственного университета. Естественно-научная серия. № 2, 2003. С. 15–20.
17. Невский А.Ю. Анализ проблем обеспечения информационной безопасности объектов энергетики России // В сборнике: Актуальные вопросы современных научных исследований. Материалы Международной (заочной) научно-практической конференции. 2017. С. 108–118.

Bibliography:

1. Corporate security in the oil and gas sector // Neftegaz.RU - 2019. - URL: https://magazine.neftegaz.ru/articles/tsifrovizatsiya/443337-korporativnaya-bezopasnost-v-neftegazovom-sektore-protsess-obespecheniya-korporativnoy-bezopasnosti-/?ysclid=l6680f8nbg953000236
2. Zhuk E.I. Conceptual foundations of information security Science and Education: scientific publication of the Bauman Moscow State Technical University. 2010. No. 4. p. 2.
3. Mysterious '08 Turkey Pipeline Blast Opened New Cyberwar // IA «Bloomberg» - 2014. - URL: https://www.bloomberg.com/news/articles/2014-12-10/mysterious-08-turkey-pipeline-blast-opened-new-cyberwar
4. Saudi Arabia told about hackers' attempt to disrupt oil exports // IA «Lenta.ru» - 2012. - URL: https://lenta.ru/news/2012/12/10/aramco /?ysclid=l6ujbqb8ox 496308071
5. Sequential Detection and Isolation of Cyber-physical Attacks on SCADA Systems // University of Technology of Troyes (UTT) - 2015. - URL: https://hal.archives-ouvertes.fr/tel-01352625/document
6. The expert suggested that it helped hackers to attack the Colonial Pipeline // RIA Novosti - 2021. - URL: https://ria.ru/20210605/khaker-1735746582.html ?ysclid =l6ukdrn0op406765144
7. Stuxnet: the beginning // Kaspersky Daily – 2014. - URL: https://www.kaspersky.ru /blog/stuxnet-victims-zero/6119/
8. Guidelines on best practices for protecting the most important objects of non-nuclear energy infrastructure from terrorist acts in connection with threats emanating from cyberspace // OSCE - 2013. - URL: https://www.osce.org /files/f/documents/5/2/110472 .pdf
9. Shabunya V.V. Organizational and legal aspects of corporate information security in fuel and energy sector organizations Legal Energy Forum. 2022. No. 1. pp. 36-40.
10. Okolot D.Ya. Aspects of training specialists in ensuring information security in the field of energy Bulletin of Youth Science of the Kaliningrad State Technical University. 2018. No. 3 (15). p. 7.
11. Balanovskaya A.V. Conceptual approach to building an information security system of an industrial enterprise Bulletin of Samara State University. Series: Economics and Management. 2015. No. 5 (127). pp. 14-20.
12. Boychenko O.V., Ivanyuta D.V. Models of information security Economics of construction and environmental management. 2021. No. 3 (80). pp. 33-39.
13. Medvedev A.A., Sozinova E.N. Development of a conceptual model of information security of the organization Scientific and Technical Bulletin of the Volga region. 2015. No. 3. pp. 175-177.
14. Anosov R.S., Anosov S.S., Shakhalov I.Y. Conceptual model of information technology security risk analysis Cybersecurity issues. 2020. No. 2 (36). pp. 2-10.
15. Information security: lecture notes / R.Sh. Zakirov. – Chelyabinsk: SUSU Publishing Center, 2014. – 73 p.
16. Rodichev Yu.A., Rodichev A.Yu. System model of information protection of information systems of distributed type Bulletin of Samara State University. Natural Science series. 2003. No. S2. pp. 15-20.
17. Nevsky A.Yu. Analysis of the problems of ensuring information security of Russian energy facilities in the collection: Topical issues of modern scientific research. Materials of the International (correspondence) scientific and practical conference. 2017. pp. 108-118.

УДК 004.056
DOI 10.52815/0204-3653_2022_03187_16
EDN: OPUDSG

Источник: boggy22 / Depositphotos.com

РАЗРАБОТКА СИСТЕМЫ ЗАЩИТЫ ВЕБ-ПРИЛОЖЕНИЙ ОТ КОМПЬЮТЕРНЫХ АТАК НА ПРОИЗВОДСТВЕННЫХ ОБЪЕКТАХ

Козьминых Сергей
Профессор департамента информационной безопасности Финансового университета при Правительстве РФ, д. т. н., доцент
E-mail: SIKozminykh@fa.ru

Кулиев Рамиг
Аспирант департамента информационной безопасности Финансового университета при Правительстве РФ
E-mail: ramig.kuliev@mail.ru

Аннотация. В данной статье представлен комплексный подход к разработке системы защиты веб-приложений от компьютерных атак на производственных объектах. Проведен анализ существующих угроз веб-приложений, реализация которых может привести к существенным последствиям для организации. Проведен анализ возможных последствий от реализации угрозы веб-приложений, от нарушения в бесперебойном функционировании веб-приложения до регуляторных санкций. Предложен комплексный подход к реализации системы защиты веб-приложений от компьютерных атак, включающий применение как организационных, так и технических мер для митигации существующих рисков информационной безопасности (финансовых, репутационных, регуляторных и т. д.) и обоснована необходимость комплексного подхода

Ключевые слова: *web-приложение, система защиты, комплексный подход, SQL-инъекции, злоумышленник, компьютерные атаки, риски информационной безопасности, технические меры, организационные меры, контроль доступа, межсетевой экран, DDOS-атака, журналирование.*

Веб-приложения подвержены угрозам атак, поэтому необходимо разрабатывать способы противодействия, которые можно поделить на технические и организационные

ВВЕДЕНИЕ

В соответствии с речью П. Кинлана, которую он произнес на саммите Chrome dev summit 2019, можно с уверенностью утверждать, что в самом ближайшем будущем классические версии программных продуктов для персональных компьютеров (ПК) будут заменены на их аналоги, представленные в виде web-приложений. Уже сейчас одна половина программных продуктов реализуется в виде web-приложений, а другая – в виде стандартных консольных программ. Предприятиям сегодня экономически невыгодно иметь в своем штате программистов и разработчиков программного обеспечения (ПО), поскольку проще получить доступ к web-приложению и заключить договор на его обслуживание со сторонней компанией. Сегодняшний рост популярности web-приложений обусловлен не только стоимостью разработки, использования и обслуживания такого продукта, но и кроссплатформенностью, понятным и удобным интерфейсом, невысокими требованиями к технической оснащенности ПК и иного оборудования для использования таких приложений, широкими возможностями их интеграции в существующие корпоративные системы. При этом рост популярности web-приложений на производственных объектах неминуемо приводит к тому, что пользователи и администраторы таких приложений начинают обмениваться большими объемами информации, в том числе по незащищенным сегментам сети интернет. В результате многократно увеличиваются риски утечки или утраты конфиденциальной информации и персональных данных из-за атак хакеров. Для сокращения рисков, связанных с реализациями компьютерных атак, необходимо выстроить комплексную систему защиты веб-приложения.

На федеральном уровне в России была принята Доктрина информационной безопасности [1], в которой указывается на необходимость повышения потенциала России в области информационной безопасности, что позволит защитить интересы государства, общества и каждого человека, проживающего на территории российского государства. Сегодня в связи с развитием глобальной сети интернет и проникновением ее практически во все сферы жизни общества и государства необходимо уделять повышенное внимание уровню защиты при работе именно с интернетом и приложениями, работа которых реализована через данную сеть.

Так как веб-приложения по большей части имеют определённые уязвимости, организации, использующие их, ставят под большой риск свои бизнес-процессы. Это становится возможным вследствие того, что организации не принимают никаких

мер обеспечения информационной безопасности как технических, так и организационных для обеспечения защиты веб-приложений. Таким образом, можно сделать вывод, что на производстве для снижения риска нарушения бизнес-процессов необходимо разрабатывать системы защиты веб-приложений, чтобы предотвращать угрозы информационной безопасности, обеспечивать бесперебойное функционирование веб-приложения, повышать свой имидж.

Концепция построения системы защиты веб-приложения

В качестве основного метода, используемого для достижения результата используется системный анализ, позволяющий в качестве решаемой проблемы выделить обеспечение комплексной безопасности веб-приложений. Выделить задачи и методы их решения с использованием современных подходов и технологий, применяемых в настоящее время.

Глобальные сети интернета являются агрессивной средой, из которой происходят постоянные злоумышленные действия на веб-ресурсы различными методами, начиная с использования автоматизированных систем сбора конфиденциальной информации и заканчивая атаками, приводящими к отказу в обслуживании ПК. В таблице 1 представлены самые распространённые уязвимости веб-приложений. [5]

Как уже было отмечено, веб-приложения имеют уязвимости и подвержены угрозам атак, поэтому необходимо в отношении каждой угрозы разрабатывать способы противодействия, которые можно поделить на технические и организационные.

Требования к системе защиты веб-приложения

На производственных объектах для предотвращения атак типа SQL-инъекции используют разные технические методы. Данные методы направлены на исходный код веб-приложения и самого сервера. Необходимо изолировать базы данных от команд и запросов, чтобы злоумышленнику не удалось совершить несанкционированный доступ к данным с помощью вредоносного кода. Также следует применять функционал безопасного API, который не позволяет использовать интерпретатор и предоставляет собой параметризованный пользовательский интерфейс. На сервере, который обеспечивает поддержку веб-приложению, также возможно реализовывать белые списки для проверки входных данных, чтобы запросы и команды анализировались на этапе авторизированного доступа к информации. Необходимо обеспечить экранирование спецсимволов, используя соответствующий интерпретатор синтаксис и применять в запросах технологию LIMIT, а для других элементов компьютерного взаимодействия – SQL, чтобы предотвратить утечку данных. [4]

Чтобы предотвратить компрометацию системы аутентификации и авторизации возможны как технические методы, так и организационные. Одним из существующих методов является реализация многофакторной аутентификации, которая позволяет предотвратить реализацию автоматических хакерских атак, DDoS атак, а также блокировку скомпрометированной учетной записи пользователя. Не стоит использовать создаваемые по умолчанию учетные данные, особенно для администраторов, так как это позволит с легкостью скомпрометировать систему. Необходимо периодически проводить проверку надежности паролей и замену паролей через установленный срок. Необходимо в системе вести журнал неудачных попыток входа, а после каждой неудачной попытки устанавливать интервал для повторного введения данных, например, от 1 до 5 минут, кроме того, при превышении максимального количества неправильного ввода пароля (как правило, от 3 до 5) действие учетной записи должно быть временно приостановлено [2].

На производственных объектах также следует уделить особое внимания для предотвращения утечки конфиденциальных и персональных данных. Для их защиты следует, в первую очередь, провести группировку всех используемых в приложении данных на данные, которые имеют персональную и личную информацию и которые находятся под защитой закона о персональных данных; данные, которые составляют коммерческую тайну, и свободно распространяемые данные.

Таблица 1. Распространённые уязвимости веб-приложений

Уязвимость	Процентное соотношение наличия данной уязвимости в различных организациях	Уровень риска
Некорректная настройка параметров безопасности	84%	Средний
Межсайтовое выполнение сценариев (XSS)	53%	Средний
Недостатки аутентификации	45%	Высокий
Недостатки контроля доступа	37%	Средний
Внедрение SQL-инъекций	29%	Высокий
Использование компонентов с известными уязвимостями	13%	Низкий
Разглашение конфиденциальных данных	13%	Высокий
Внешние сущности XML (XXE)	5%	Высокий

Системы информбезопасности необходимы на всех объектах ТЭК
Источник: Chris LeBoutillier / Pixabay.com

Стоит обеспечить шифрование всей хранимой конфиденциальной информации, а также шифровать все передаваемые данные с помощью надежного протокола TLS с совершенной прямой секретностью (PFS). Возможно и отключение кэширования ответов, содержащих конфиденциальную информацию [8].

Избежать внедрение внешнего XML возможно несколькими способами. Конечно, для данного вида угроз лучшим средством является обучение разработчиков XML, которое имеет большое значение для выявления и противодействия злоумышленным действиям. Кроме того, для нейтрализации рассматриваемой угрозы нужно внедрить следующие организационные мероприятия:

- использовать простейшие разрозненные формы данных, что позволит потенциальному злоумышленнику, даже при получении доступа к одному информационному ресурсу, не получить доступ ко всей информационно-аналитической системе;
- своевременно устанавливать все обновления, которые предлагаются разработчиками прикладного и системного программного обеспечения;
- реализовать процесс проверки зависимостей различных данных;
- отключить обработку внешних сущностей XML и DTD для XML- обработчиков прикладного ПО;
- фильтровать поступающие сообщения на сервер от пользователей путем установки «белых списков» на разрешенные символы, слова и иные символьные конструкции;
- проверять и контролировать тот факт, что загрузочная функция XML или XSL выполняет проверку входящего потока информации с применением XSD или иного подобного метода;
- проводить аналитику программного кода для широкомасштабных приложений или приложений, затрагивающих внутреннюю инфраструктуру организации, не только в автоматическом, но и в ручном режиме.

Диспетчерское управление завода
Источник: veloliza / Depositphotos.com

На производственных объектах недочеты в системе контроля доступа могут привести к несанкционированному доступу к критическим данным. Для того чтобы предотвратить данную угрозу, существуют следующие способы:

- полный запрет свободного доступа к информации, кроме той, которая имеет свободное распространение;
- организация качественного контроля доступа, который подразумевает определенные правила выбора пароля (невозможно установить простой пароль), минимизация возможности сквозной авторизации, применение различных блокировок к скомпрометировавшим себя учетным записям пользователей;
- разделение всех пользователей на группы, например, владелец, администратор, пользователь, при этом каждый участник группы должен быть наделен определенными правами на доступ и изменение информации в системе;

- реализация доменной модели с целью установки специализированных ограничений для безопасной работы приложений;
- отключение возможности просматривать каталог веб-сервера через web-приложение, а также запрет на размещение резервных копий в корневых папках сервера;
- мониторинг доступности авторизации в приложении и при появлении сбоя информирование администратора сервера;
- ограничение периодичности доступа к API и web-контроллерам приложения;
- удаление с сервера токенов JWT незамедлительно после разлогинивания пользователя [9].

Неправильная настройка компонентов безопасности приложения является уязвимостью, которую злоумышленники могут эксплуатировать для компрометации системы. Для того чтобы предотвратить угрозу компрометации, необходимо реализовать процесс безопасной установки, которая включает в себя:

- оперативная воспроизводимость ранее запущенных процессов на сервере для развертывания необходимых виртуальных частных сред для изолированного и безопасного доступа. Все интегрированные среды конфигурируют однообразно с взаимосвязанными процессами, при этом для каждой среды должен быть предусмотрен свой пароль доступа. Максимальный объем информации в данных средах должен обрабатываться в автоматическом режиме, что позволит сократить трудозатраты администраторов;
- применение платформенных решений, в которых содержатся только все самое необходимое для работы программного обеспечения;
- удаление лишних компонентов или фреймворков;
- соответствие параметров антивирусного программного обеспечения, межсетевого экрана, брандмауэра актуальным параметрам настройки и актуальной версии как самой программы, так и антивирусных баз;

Промышленная лаборатория
Источник: AndreyBezuglov / Depositphotos.com

- разделение всех пользователей на несколько групп, в которых пользователи разделяются в соответствии с имеющимися у них правами на доступ и изменение тех или иных данных;
- выделение директив безопасности для пользователей;
- автоматизация корректности работы и выполненных настроек автоматизированных сред и программных конфигураций на сервере.

Такое явление, как межсайтовый скриптинг также является угрозой веб-приложения. Это происходит при попытке внедрения кода в HTTP-ответ, получаемый клиентом и выполняющимся на стороне клиента. Для того чтобы предотвратить данную уязвимость, необходимо при помощи программных средств, таких как сканеры уязвимостей, анализировать исходный код на предмет наличия «дыр», которыми злоумышленник может воспользоваться. [14]

Специалисты, занимающиеся информационной безопасностью, также практикуют отделение непроверенных данных от активного контента браузера. Этого можно добиться следующими способами:

- кодирование управляющих HTML-символов, JavaScript, CSS и URL перед отображением в браузере;
- проверка и кодирование входных данных;
- обеспечение безопасности cookies, которая может быть реализована путём ограничения домена и пути для принимаемых cookies.

Данные методы позволяют не допустить внедрение скрипта в страницу, выдаваемую веб-приложением и не допустить выполнение в браузере клиента [15].

Для того, чтобы защитить взаимодействие компонентов веб-приложения, необходимо отклонить объекты, имеющие аналогичные серийные свойства и поступившие из не доверительных источников, или запретить применение сред реализации, основанных на самых простейших типах данных. Данное мероприятие обязательно к реализации, так как, чем проще программный код, тем проще хакерам взломать имеющуюся защиту и подменить стандартный код на код вредоносного программного обеспечения.

Однако для некоторых оболочек и программных продуктов, реализованных на примитивном уровне, не существует аналогов, поэтому в таких ситуациях необходимо выполнить:

- непрерывный мониторинг целостности объектов одинаковой серийной структуры, к примеру, с использованием цифровых ключей, которые минимизируют возможность получения несанкционированного доступа к данным;
- использование жестких типовых ограничений в процессе десериализации перед созданием объекта, так как в данном случае в качестве ожидаемого будет выступать набор классов, который поддается формализации и определению;
- изолированный от системных процессов и других прикладных программ запуск кода, который производит десериализацию, в минимальной по привилегиям доступа среде;
- ведение журнала для фиксирования и оперативного устранения всех возникающих ошибок;
- анализ всех подключений и проведение обмена информацией между сервером баз данных и пользовательским устройством доступа с целью выявления фактов несанкционированного доступа и блокировки таких пользователей;
- отслеживание каждого факта перевода байтовой информации в информацию, понятную каждому пользователю, при этом основной акцент должен быть сделан на процессах, которые имеют длительный срок реализации.

Применение в производстве программных продуктов с известными уязвимостями – это достаточно популярная угроза информационной безопасности объекта, так как злоумышленники с помощью сканеров уязвимостей могут проанализировать версии компонентов веб-приложения и выявить наиболее чувствительные для системы [17].

Для того чтобы обезопасить веб-приложение от компрометации, необходимо реализовать процесс управления обновлениями:

- удаление неиспользуемых зависимостей, а также лишних функций, компонентов, файлов и сведений из документации;
- регулярная проверка актуальности версий клиентских и серверных компонентов (например, фреймворков и библиотек), а также их зависимостей;
- использование инструментов анализа состава ПО для автоматизации процесса;
- загрузка компонентов из официальных источников по безопасным ссылкам;
- контроль библиотек и компонентов, которые не поддерживаются или не получают обновлений безопасности.

Для безопасной работы каждого веб-приложения на сервере объекта необходимо в автоматизированном режиме вести текстовый журнал, в котором должно фиксироваться время и характер сбойной ситуации, попытки авторизации пользователей, попытки подбора пароля к системе, время и характер проводимых изменений баз данных на сервере и др. Некачественное ведение журналов входа в систему и внесенных изменений приводят к тому, что не происходит своевременное реагирование на инциденты, так как мониторинг либо настроен не правильно, либо полностью отсутствует, в следствии чего, злоумышленник при проведении атак полагается на отсутствие контроля и без своевременных предотвращающих действий может продолжать попытки компрометации системы.

Для ликвидации данной уязвимости применяют различные методы защиты, предназначенные обеспечить неприкосновенность конфиденциальной информации или персональных данных. К этим методам можно отнести:

- регистрирование каждой ошибки доступа с записью в системном журнале с целью последующего анализа этого события силами системного администратора;
- регистрирование каждого подозрительного события в таком формате, чтобы он был понятен любому аналитику, который проводит свою работу в серверном сегменте;
- использование контроля внесения изменений в системный журнал с целью недопущения подмены корректной информации на недостоверную;
- использование высококачественных систем мониторинга и обнаружения подозрительных действий с целью уменьшения времени реакции на такие события, причем реакция может выполняться как в автоматизированном, так и в ручном режиме;
- установка межсетевых экранов веб-приложений.

Для того, чтобы система защиты веб-приложений была комплексной, необходимо применять также организационные меры, которые позволят ограничить реализации атак на веб-приложение:

- необходимо внедрение многофакторной аутентификации (двухфакторная аутентификация);
- уничтожение учетных данных, созданных по умолчанию;

Работа веб-приложений
на производственных объектах
Источник: gzorgz / Depositphotos.com

– проведение проверок надежности паролей;
– увеличение интервала между неудачными попытками входа;
– запрет свободного доступа к информации, кроме той, которая размещена в открытом доступе (инструкция, правила использования, лицензионное соглашение и др.);
– внедрение алгоритмов контроля доступа к информационным ресурсам, получаемого посредством web-приложений, в том числе путем минимизации междоменного доступа к ресурсам;
– привлечение специалистов для работы с SIEM-системой и на другие классы-решений;
– тренинг персонала (курсы по фишингу и спам-атакам).

ЗАКЛЮЧЕНИЕ

В данной статье представлен комплексный подход к разработке системы защиты веб-приложений от компьютерных атак на производственных объектах. Отмечено, что для обеспечения эффективного противодействия компьютерным атакам, перечисленным источникам угроз и возможным последствиям от их реализации, необходимо использование как технических, так и организационных мер.

В качестве вывода к данной статье следует отметить, что представленный комплексный подход к разработке системы защиты веб-приложений от компьютерных атак является достаточно универсальным и применим к различным типам веб-приложений. Внедрение данного подхода позволяет не только повысить уровень безопасности техническими средствами, но и организационными.

Следует отметить, что на производственных объектах необходимо придерживаться комплексного подхода к разработке системы защиты веб-приложений организации от компьютерных атак, поскольку не применение каких-либо мер может привести к реализации угрозы и существующих рисков в информационной безопасности и защите web-приложения.

Загрузка приложений по техническому обслуживанию объекта
Источник: guruxox / Depositphotos.com

DEVELOPMENT OF A WEB APPLICATION PROTECTION SYSTEM AGAINST COMPUTER ATTACKS AT FUEL AND ENERGY COMPLEX

Kozminykh Sergey, professor of the Department of Information Security, Financial University under the Government of Russia, Doctor of Technical Sciences, Associate Professor.
E-mail: SIKozminykh@fa.ru

Kuliev Ramig, graduate student of the Department of Information Security of the Financial University under the Government of Russia.
E-mail: ramig.kuliev@mail.ru

Abstract. This article presents a comprehensive approach to the development of a system for protecting web applications from computer attacks at the facilities of the fuel and energy complex. The analysis of existing threats to web applications, the implementation of which can lead to significant consequences for the organization, is carried out. The analysis of possible consequences from the implementation of the threat of web applications for the objects of the fuel and energy complex from disruption in the smooth functioning of the web application to regulatory sanctions is carried out. A comprehensive approach to the implementation of a web application protection system against computer attacks is proposed, including the use of both organizational and technical measures to mitigate existing information security risks (financial, reputational, regulatory, etc.) and the need for an integrated approach is justified.
Keywords: web application, security system, integrated approach, SQL injection, attacker, computer attacks, information security risks, technical measures, organizational measures, access control, firewall, DDOS attack, logging.

Библиографический список:

1. Указ Президента РФ от 5 декабря 2016 г. № 646 "Об утверждении Доктрины информационной безопасности Российской Федерации".
2. OWASP, «OWASP Top 10 Application Security Risks – 2019», https://www.owasp.org/index.php/Top_10-2017_Top_10, 27 марта 2019 г.
3. Сэмми Пьюривал, «Основы разработки веб-приложений», 2019 г.
4. SQL инъекция. – URL: http://insafety.org/sql.php
5. Positive Research, «Статистика атак на веб-приложения: II квартал 2019 года», 14 сентября 2019 г.
6. Косинов А.А. Системы обнаружения атак: Учебный курс. Москва, 2017 г.
7. Бил Джей. Snort 2.1 обнаружение вторжений. 2018 г.
8. Лукацкий А.В. Система обнаружения атак. 2017 г.
9. Синица И.Н. Вопросы безопасности и пути их решения в современных компьютерных сетях. 2021 г.
10. Лапонина О.Р. Основы сетевой безопасности: криптографические алгоритмы и протоколы взаимодействия // Интернет-университет информационных технологий – ИНТУИТ.ру, 2020.
11. Robert Auger, Ryan Barnett, Yuval Ben-Itzhak, Erik Caso и др. - Web Application Security Consortium (перевод: Классификация ВЕБ угроз). Издательство webappsec, США, 2020.
12. Корпорация МАЙКРОСОФТ – Fundamentals of Network Security (перевод: основы сетевой безопасности) // Издательство МАЙКРОСОФТ, США, 2019.
13. Федеральный закон от 27.07.2006 г. № 152-ФЗ (ред. от 29.07.2017 г.) «О персональных данных».
14. Michael Sutton, Adam Greene, and Pedram Amini. Fuzzing : brute force vulnerabilty discovery. Upper Saddle River, NJ: Addison-Wesley, 2018.
15. Takanen, Ari, Jared D. Demott, and Charles Miller. Fuzzing for software security testing and quality assurance. Boston: Artech House, 2020.
16. Mark Dowd, John McDonald, and Justin Schuh. The art of software security assessment: identifying and preventing software vulnerabilities. Indianapolis, Ind: Addison-Wesley, 2019.
17. ГОСТ 50922-96. Защита информации. Основные термины и определения.
18. Зима В.М., Котухов М.М., Ломако А.Г., Марков А.С., Молдовян А. А. Разработка систем информационно-компьютерной безопасности: Учебное пособие. СП6, 2017. – 304 с.
19. Мельников В.В. Безопасность информации в автоматизированных системах. Москва, 2018. – 367 с.
20. Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных (утв. Заместителем директора ФСТЭК 14 февраля 2008 г.)
21. ГОСТ Р 50. 1. 056-2005. Техническая защита информации. Основные термины и определения.
22. Доценко С.П. Подход к построению модели систем менеджмента информационной безопасности // Научный журнал КубГАУ. №53, 2017. С. 1-4.

Bibliography:

1. Decree of the President of the Russian Federation No. 646 dated December 5, 2016 "On the approval of the Information Security Doctrine of the Russian Federation".
2. OWASP, «OWASP Top 10 Application Security Risks – 2019», https://www.owasp.org/index.php/Top_10-2017_Top_10 , March 27, 2019
3. Sammy Purival, «Fundamentals of Web Application Development», 2019
4. SQL injection. – URL: http://insafety.org/sql.php
5. Positive Research, «Statistics of attacks on web applications: The second quarter of 2019», September 14, 2019
6. Kosinov A.A. Attack detection systems: A training course. Moscow, 2017
7. Bill Jay. Snort 2.1 intrusion detection. twothousandeighteen
8. Lukatsky A.V. Attack detection system. twothousandseventeen
9. Sinitsa I.N. Security issues and ways to solve them in modern computer networks. twothousandtwentyone
10. Laponina O.R. Fundamentals of network security: Cryptographic algorithms and interaction protocols // Internet University of Information Technologies – INTUIT.<url>, 2020.
11. Robert Auger, Ryan Barnett, Yuval Ben-Itzhak, Erik Caso, etc. - Web Application Security Consortium (translation: Classification of WEB threats). webappsec Publishing House, USA, 2020.
12. MICROSOFT Corporation – Fundamentals of Network Security (translation: Fundamentals of network security) // MICROSOFT Publishing House, USA, 2019.
13. Federal Law No. 152-FZ of 27.07.2006 (as amended on 29.07.2017) «On Personal Data».
14. Michael Sutton, Adam Greene, and Pedram Amini. Fuzzing : brute force vulnerabilty discovery. Upper Saddle River, NJ: Addison-Wesley, 2018.
15. Takanen, Ari, Jared D. Demott, and Charles Miller. Fuzzing for software security testing and quality assurance. Boston: Artech House, 2020.
16. Mark Dowd, John McDonald, and Justin Schuh. The art of software security assessment: identifying and preventing software vulnerabilities. Indianapolis, Ind: Addison-Wesley, 2019.
17. GOST 50922-96. Information protection. Basic terms and definitions.
18. Winter V.M., Kotukhov M.M., Lomako A.G., Markov A.S., Moldovyan A. A. Development of information and computer security systems: A textbook. St. Petersburg, 2017. – 304 p.
19. Melnikov V.V. Information security in automated systems. Moscow, 2018. – 367 p.
20. Methodology for determining the actual threats to the security of personal data when they are processed in personal data information systems (approved by the Deputy Director of the FSTEC on February 14, 2008)
21. GOST R 50. 1. 056-2005. Technical protection of information. Basic terms and definitions.
22. Dotsenko S.P. Approach to building a model of information security management systems // Scientific Journal of KubGAU. No. 53, 2017. pp. 1-4.

УДК 69.05
DOI 10.52815/0204-3653_2022_03187_26
EDN: VCOXRO

Источник: Martin Widenka / unsplash.com

НАУЧНО-ТЕХНИЧЕСКОЕ СОПРОВОЖДЕНИЕ КАК НЕОБХОДИМОЕ УСЛОВИЕ ЭФФЕКТИВНОГО СТРОИТЕЛЬСТВА ВЫСОТНЫХ ЗДАНИЙ

Кангезова Марьянна
Преподаватель кафедры ИСТАС НИУ МГСУ.
E-mail: kangezovamh@mgsu.ru

Хубулов Георгий
Аспирант кафедры ТОСП НИУ МГСУ, Национальный исследовательский Московский государственный строительный университет.
E-mail: geo.khubulov@mail.ru

Аннотация. На сегодняшний день в практике проектирования уникальных зданий одним из наиболее значимых вопросов является повышение производительности объектов строительства. В статье рассматриваются комплекс мероприятий для повышения эффективности проектирования уникальных зданий. При выявлении наиболее значимых критериев, влияющих на качество работ, можно значительно улучшить параметры производительности и безопасности объекта строительства.

Ключевые слова: *производительность строительного процесса, эффективность, нормативное обеспечение, технические условия, организационно-технологические аспекты, систематизация.*

Времени на принятия решений при выявлении дефектов больше там, где НТС начал свою работу своевременно

ВВЕДЕНИЕ

Анализ факторов влияния процесса бетонирования на производительность возведения объекта является на данный момент одной из самых актуальных задач в современном строительстве уникальных зданий. Для решения данного вопроса в этой статье мы рассмотрим научно-техническое сопровождение строительства объектов, которое включает в себя следующие этапы:

1. Подготовительные работы.
2. Основные работы.
3. Составление промежуточных и итоговых заключений по объекту.

Для анализа мы декомпозировали процесс строительства по этапам выполнения работ. На каждом этапе необходимо провести детальное исследование и выбрать, какие виды работ необходимы при проведении научно-технического сопровождения строительства.

В данной статье научно техническое сопровождение будет рассматриваться на следующих этапах:

1. НТС строительства фундаментов.
2. НТС строительства несущих конструкций.

Необходимость обработки большого массива данных и наличия компетенции и практики проектирования уникальных зданий делает данную задачу непростой. В связи с чем, в качестве метода исследования был выбран метод экспертной оценки.

Для определения необходимого количества экспертов воспользуемся таблицей, позволяющей вычислить искомую величину в зависимости от вероятности и ошибки среднего, которая была сформирована на основе анализа математического аппарата метода экспертного оценивания [12].

Приняв ошибку среднего 10% и значение вероятности 1-а = 0,95, получим, что для проведения исследования с известной ошибкой репрезентативности, не превышающей 5%, необходимо участие 96 экспертов, обладающих необходимыми компетенциями по предмету исследования. Для этого следует обратиться к специалистам, состоящим в Национальном реестре строителей. Общее число экспертов представлено 11 группами.

Экспертам необходимо проранжировать представленные виды бригад на каждом этапе возведения многоэтажного жилого дома по принципу максимальной эффективности использования. Он заключается в том, что выбранный вид работы должен способствовать оптимальному сокращению сроков строительства в пределах этапа без отрицательного влияния на качество произведенных работ, а также без увеличения фактической стоимости строительства и увеличения трудовых затрат. Фактическое изменение показателей возведения здания будет

установлено в третьей главе работы после проведения экспериментального внедрения результатов исследования. Ранжировать типы бригад следует от 1 до n (n – колво работ в разделе).

После проведения опроса имеем 11 заполненных опросных анкет. В таблице 1 приведен пример заполненной опросной анкеты экспертной группы № 1.

После сбора экспертных данных была проведена проверка на их корректность критерием однородности дисперсий Бартлетта, то есть, была установлена достаточно высокая степень согласованности мнений экспертов для признания выборки данных репрезентативной.

После того, как данные, полученные в результате экспертного опроса, были проанализированы при помощи инструментов математической статистики, производится их моделирование, т. е. выборка тех видов работ, которые необходимо включить в программу НТСС [10].

Результаты проведенного исследования представлены в виде диаграммы (рис. 1, 2).

Таблица 1. Данные опросной анкеты в электронном виде

№	Вид работ	Наименование работ	ЭГ1	ЭГ2	ЭГ3	ЭГ4	ЭГ5	ЭГ6	ЭГ7	ЭГ8
1	НТС строительства фундаментов (от 1 до 7 баллов)	Анализ материалов инженерно-геологических изысканий	5	4	6	4	5	4	7	6
		Анализ проектной и рабочей документации	6	7	5	7	6	7	5	5
		Оценка необходимости усиления грунтов основания при превышении предельных величин осадок	3	5	3	5	3	5	3	3
		Оценка полноты разработанных мероприятий по усилению грунтов основания	2	1	2	2	2	1	2	3
		Разработка соответствующих рекомендаций	4	3	4	3	4	2	3	4
		Анализ расчетов на стадии проектной и рабочей документации, в том числе на возможность прогрессирующего обрушения и разработка соответствующих рекомендаций	7	6	7	6	7	6	6	7
		Анализ ППР	1	2	1	1	1	3	1	1

Таблица 1. Данные опросной анкеты в электронном виде (продолжение)

№	Вид работ	Наименование работ	ЭГ1	ЭГ2	ЭГ3	ЭГ4	ЭГ5	ЭГ6	ЭГ7	ЭГ8
2	НТС строительства несущих конструкции (от 1 до 9 баллов)	Оценка влияния выявленных дефектов и повреждений на объект	8	7	9	8	7	9	8	8
		Поверочные расчеты дефектных конструкций	4	3	4	4	3	4	3	4
		Разработка рекомендаций по устранению выявленных дефектов и повреждений конструкций	5	8	5	5	4	5	8	5
		Определение фактической прочности бетона	9	6	7	9	6	7	6	9
		Выборочный неразрушающий контроль прочности плит перекрытия	1	4	2	1	8	2	4	1
		Выборочный неразрушающий контроль прочности вертикальных конструкции	2	1	3	2	1	3	2	2
		Испытание арматурных стержней на растяжение	6	5	6	6	5	6	5	6
		Входной контроль поступающих материалов	7	9	8	7	9	8	9	7
		Выборочное визуально-инструментальное обследование конструкции	3	2	1	3	2	1	1	3

По результатам проведенной экспертной оценки и математической обработки данных была получена организационно-технологическая система, применение которой должно дать рассчитанную эффективность, равную 3,9 %. Для получения конкретных результатов оптимизации продолжительности строительства в результате применения данной системы необходимые расчеты динамических моделей строительства были проведены.

Результаты исследования показывают, что при идентичных дефектах и на разных корпусах времени на принятия решений при выявлении дефектов оказалось меньше, чем на корпусах, где НТС начал свою работу своевременно и учел наиболее значимые виды работ.

Таблица 2. Выборка основных видов работ

№	Вид работ	Наименование работ	Вес	Сред. Знач.	Отклоне-ние
1	НТС строительства фундаментов (от 1 до 7 баллов)	Анализ материалов инженерно-геологических изысканий	0,71	5,019842	0,57
		Анализ проектной и рабочей документации	0,86	5,936949	0,57
		Оценка необходимости усиления грунтов основания при превышении предельных величин осадок	0,43	3,633411	0,57
		Оценка полноты разработанных мероприятий по усилению грунтов основания	0,29	1,769228	0,57
		Разработка соответствующих рекомендаций	0,57	3,292905	0,57
		Анализ расчетов на стадии проектной и рабочей документации, в том числе на возможность прогрессирующего обрушения и разработка соответствующих рекомендаций	1	6,480741	0,57
		Анализ ППР	0,14	1,251033	0,57
2	НТС строительства несущих конструкции (от 1 до 9 баллов)	Оценка влияния выявленных дефектов и повреждений на объект	0,89	7,968565	0,57
		Поверочные расчеты дефектных конструкций	0,44	3,590938	0,57
		Разработка рекомендаций по устранению выявленных дефектов и повреждений конструкций	0,56	5,468727	0,57
		Определение фактической прочности бетона	1	7,259758	0,57
		Выборочный неразрушающий контроль прочности плит перекрытия	0,11	2,181015	0,57
		Выборочный неразрушающий контроль прочности вертикальных конструкций	0,22	1,86121	0,57
		Испытание арматурных стержней на растяжение	0,67	5,603486	0,57
		Входной контроль поступающих материалов	0,78	7,952894	0,57
		Выборочное визуально-инструментальное обследование конструкций	0,33	1,795469	0,57

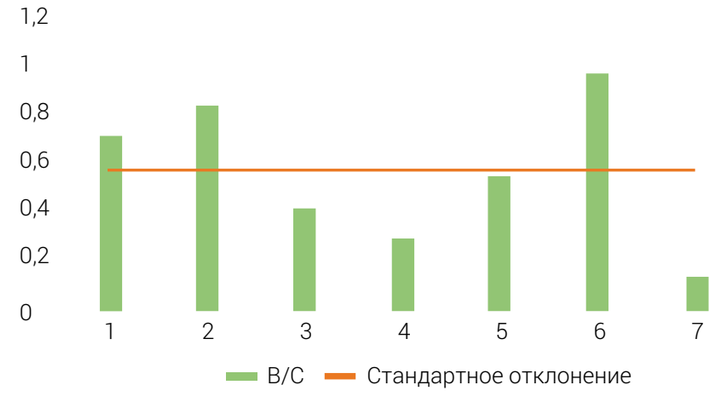


Рис. 1 Раздел 1. НТС строительства фундаментов

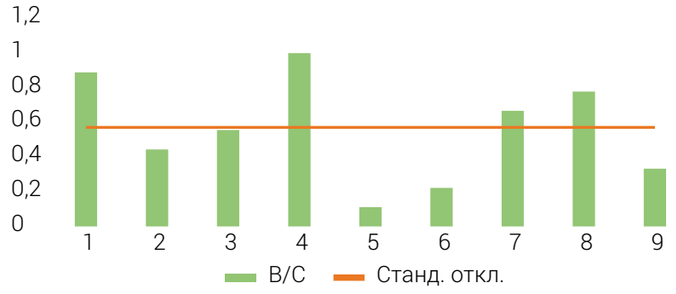


Рис. 2. Раздел 2. НТС несущих конструкций

SCIENTIFIC AND TECHNICAL SUPPORT AS A NECESSARY CONDITION FOR THE EFFECTIVE CONSTRUCTION OF HIGH-RISE BUILDINGS

Kangezova Maryanna, Lecturer, Department of ISTAS, Moscow State University of Civil Engineering.
E-mail: kangezovamh@mgsu.ru

Khubulov Georgiy, PhD student, Department of TOSP, National Research Moscow State University of Civil Engineering.
E-mail: geo.khubulov@mail.ru

Abstract. To date, one of the most significant issues in the practice of designing unique buildings is to increase the performance of construction projects. The article deals with a set of measures for increasing the efficiency of designing unique buildings. By identifying the most significant criteria affecting the quality of work, you can significantly improve the performance and safety parameters of the object of construction.
Keywords: productivity of the construction process, efficiency, regulatory support, technical conditions, organizational and technological aspects, systematization.

Библиографический список:

1. Градостроительный кодекс Российской Федерации. Статья 1 от 29.12.2004 г. № 190-ФЗ (ред. от 25.12.2018 г.).
2. Градостроительный кодекс Российской Федерации от 29.12.2004 г. № 190ФЗ (ред. от 21.10.2013 г.) (с изм. и доп. от 07.06.2013 г. № 113-ФЗ, вступившими в силу с 05.12.2013 г.).
3. СП 253.1325800.2016 г. Инженерные системы высотных зданий.
4. Гусаков А. А. Системотехника строительства. Москва: Стройиздат, 1993.
5. Олейник П. П., Бродский В. И. Особенности организации строительного производства при реконструкции зданий и сооружений // Технология и организация строительного производства. № 4 (5), 2013.
6. Федеральная служба государственной статистики // Срочная информация и справки по актуальным вопросам. Жилищное строительство. 2018.
7. Каган П. Б., Гинзбург А. В. Автоматизация организационно-технологического проектирования в строительстве // Автоматизация проектирования. № 4, 1997. С. 36–45.
8. Повзик Я. С. Справочник руководителя для тушения пожара. 2014 г. – 256 с.
9. Распоряжение от 15 июня 2007 г. № 70 «О разработке положения о технических условиях на проектирование и строительство уникальных, высотных и других экспериментальных объектов капитального строительства в городе Москве». – URL: http://docs.cntd.ru/document/3685951
10. Федеральный закон «О техническом регулировании» от 27.12.2002 г. № 184-ФЗ.
11. Межгосударственным стандартом ГОСТ 27751–2014 «Надежность строительных конструкций и оснований».
12. СП 20.13330.2016 «Нагрузки и воздействия».
13. СП 22.13330.2016 «Основания зданий и сооружений».
14. МГСН 4.19–2005 «Временные нормы и правила проектирования многофункциональных высотных зданий и зданий-комплексов в городе Москве».
15. МГСН 1.04–2005 «Временные нормы и правила проектирования планировки и застройки участков территории высотных зданий-комплексов, высотных градостроительных комплексов в городе Москве».
16. СП 267.1325800.2016 «Здания и комплексы высотные».
17. Лапидус А. А. Потенциал эффективности организационно-технологических решений строительного объекта // Вестник МГСУ. № 1, 2014. С. 175–180.
18. Лапидус А. А., Фельдман А. О. Оценка организационно-технологического потенциала строительного проекта, формируемого на основе информационных потоков // Вестник МГСУ. № 11, 2015. С. 193–201.
19. Системы автоматизации проектирования в строительстве: учебное пособие / Гинзбург А. В., Баранова О. М., Блохина Н. С., Волков А. А., Гаряев Н. А., Гинзбург В. М., Игнатов В. П., Игнатова Е. В., Истомин Б. С., Каган П. Б., Китайцева Е. Х., Куликов В. Г, Синенко С. А. Москва: Московский государственный строительный университет. ЭБС АСВ, 2014. – 664 с.

Bibliography:

1. . «Town-planning Code of the Russian Federation» art.1 of 29.12.2004 N 190-FZ (as amended on 25.12.2018)
2. «Town-planning Code of the Russian Federation» of 29.12.2004 N 190FZ (as amended on 21.10.2013) (with amendments and additions. dated 07.06.2013 N 113-FZ, effective from 05.12.2013).
3. SP 253.1325800.2016 Engineering systems of high-rise buildings
4. Gusakov A. A. System engineering of construction.– M.: Stroyizdat, 1993.
5. Oleinik P. P., Brodsky V. I. Features of the organization of construction production in the reconstruction of buildings and structures // Technology and organization of construction production, 2013, № 4 (5)
6. Federal State Statistics Service // Urgent information and information on current issues. Housing construction, 2018.
7. Kagan P. B., Ginzburg A. V. Automation of organizational and technological design in construction. / Automation of design, 1997 No. 4 – pp. 36–45.
8. Povzik Ya. S. Handbook of the head for fire extinguishing, 2014–256s.
9. ORDER No. 70 of June 15, 2007 On the Development of Regulations on Technical Conditions for the Design and Construction of Unique, High-rise and Other Experimental Capital Construction Facilities in the City of Moscow. http://docs.cntd.ru/document/3685951
10. Federal Law «On Technical Regulation» dated 27.12.2002 N 184-FZ.
11. Interstate standard GOST 27751–2014 «Reliability of building structures and foundations».
12. SP 20.13330.2016 «Loads and impacts».
13. SP 22.13330.2016 «Foundations of buildings and structures».
14. MGSN 4.19–2005 «Temporary norms and rules for the design of multifunctional high-rise buildings and building complexes in the city of Moscow».
15. MGSN 1.04–2005 «Temporary norms and rules for the design of the layout and development of sections of the territory of high-rise buildings-complexes, high-rise urban complexes in the city of Moscow».
16. SP 267.1325800.2016 «High-rise buildings and complexes».
17. Lapidus A. A. Efficiency potential of organizational and technological solutions of a construction object // Bulletin of MGSU. 2014. No. 1. pp. 175–180.
18. Lapidus A. A., Feldman A. O. Assessment of the organizational and technological potential of a construction project formed on the basis of information flows. Vestnik MGSU. 2015. No. 11. pp. 193–201.
19. Design automation systems in construction: textbook / Ginzburg A. V., Baranova O. M., Blokhina N. S., Volkov A. A., Garyaev N. A., Ginzburg V. M., Ignatov V. P., Ignatova E. V., Istomin B. S., Kagan P. B., Kitaytseva E. H., Kulikov V. G., Sinenko S. A.– M.: Moscow State University of Civil Engineering, EBS DIA, 2014.– 664 p.

УДК 004.89
DOI 10.52815/0204-3653_2022_03187_33
EDN: RIIZMN

Источник: photollurg2 / Depositphotos.com

РАЗРАБОТКА ГЛОБАЛЬНОГО ОГРАНИЧЕНИЯ BLOCK SEQUENCING ПРИ ПЛАНИРОВАНИИ ОТКРЫТЫХ ГОРНЫХ РАБОТ

Олейник Юрий
Младший научный сотрудник, Институт информатики и математического моделирования – обособленное подразделение ФИЦ «Кольский научный центр Российской академии наук».
E-mail: yoleynik@iimm.ru

Зуенко Александр
Ведущий научный сотрудник, к. т. н., Институт информатики и математического моделирования – обособленное подразделение ФИЦ «Кольский научный центр Российской академии наук»
E-mail: zuenko@iimm.ru

Аннотация. Статья посвящена созданию высокоэффективных средств программирования в ограничениях для решения задач планирования открытых горных работ. Разработано глобальное ограничение Block sequencing, обработчик которого совместно анализирует условия на последовательность извлечения блоков, а также некоторые дополнительные требования, что позволяет существенно повысить эффективность вычислений.

Ключевые слова: *задача удовлетворения ограничений, программирование в ограничениях, планирование открытых горных работ, глобальные ограничения, исследование операций.*

ВВЕДЕНИЕ

Одной из важных задач теории расписаний является задача планирования открытых горных работ [1–4]. Суть данной задачи заключается в том, что требуется разработать карьер заданной конфигурации за определенное количество одинаковых временных промежутков (периодов) наиболее эффективным способом. Карьер моделируется в виде набора блоков с известным содержанием полезного компонента и известной ценностью блока в каждый период. Ценность блока описывает предполагаемую прибыль от его извлечения с учетом стоимости его добычи и переработки. Таким образом, часть блоков, где достаточно полезного компонента, будет иметь положительную ценность, а другие – отрицательную. Кроме того, ценность блока может меняться согласно заданным закономерностям в зависимости от периода, когда блок извлекается. Решением рассматриваемой задачи будет являться присвоение каждому блоку номера периода, в который его следует извлечь из карьера. Предполагается, что модель карьера содержит только необходимые для извлечения блоки, то есть каждому блоку модели должен быть присвоен номер одного из периодов. Критерием эффективности при решении является сумма ценностей блоков, целью оптимизации – максимизация этого критерия.

Для решения поставленной задачи широко применяются методы смешанного целочисленного линейного программирования [1–3], принципиальным недостатком которых является необходимость представления всех ограничений в явном виде с помощью линейных уравнений и неравенств. Применение подобного подхода на практике предъявляет серьезные требования к объемам оперативной памяти, необходимым для хранения модели и реализации вычислений, что особенно важно для задач планирования открытых горных работ, где количество блоков в карьере составляет десятки и сотни тысяч. Кроме того, линеаризации некоторых типов ограничений могут вызывать существенные затруднения.

В работе излагаются результаты, которые развивают исследования авторов, представленные в [5, 6], где предлагается решать задачу планирования открытых горных работ как задачу удовлетворения ограничений (CSP – *constraint satisfaction problem*). В рамках парадигмы программирования в ограничениях, сами ограничения (отношения), как правило, задаются не прямо, а путем указания соответствующей процедуры, которая возвращает истину, если кортеж значений удовлетворяет ограничению. Подобные процедуры называются распространителями, поскольку позволяют при не полном задании входного вектора значений переменных делать выводы о множестве допустимых значений недоопределенных компонент данного вектора. Как правило, совокупность простых ограничений эффективнее обрабатывать совместно, объединяя в одно, так называемое, глобальное ограничение. В [5, 6] описаны основные типы глобальных ограничений, которые предлагается использовать для моделирования условий рассматриваемой задачи, в частности, условия на последовательность извлечения блоков было предложено представлять и обрабатывать с помощью набора глобальных ограничений *max* для каждого блока в отдельности.

В настоящей статье представлено разработанное авторами глобальное ограничение *Block sequencing*, распространитель (обработчик) которого анализирует условия на последовательность извлечения блоков, а также некоторые дополнительные требования, за один вызов для всех блоков, находящихся в очереди распространителя, что позволяет существенно повысить эффективность вычислений.

Парадигма программирования в ограничениях

Для решения сложных задач комбинаторного поиска все чаще применяется технология программирования в ограничениях (CP – *constraint programming*), реализующая декларативный подход к представлению знаний [7]. Понятие “переменная”, используемое в CP, ближе к математической трактовке понятия переменной, чем той, что принята в языках программирования. Для решения любой задачи в рамках парадигмы программирования в ограничениях она должна быть представлена как задача удовлетворения ограничений. Для описания задачи CSP необходимо задать множество переменных, множество возможных значений этих переменных (домены) и множество ограничений, описывающих допустимые или недопустимые сочетания значений. Для получения решения задачи CSP необходимо каждой переменной присвоить значение из ее домена таким образом, чтобы не нарушалось ни одно из заданных ограничений (удовлетворялись все ограничения) [7]. Любой метод решения задач CSP состоит из двух основных компонент: 1) компоненты, реализующей информированный поиск с применением специализированных эвристик выбора переменной и её значения (значений); 2) компоненты, осуществляющей логических вывод путем сокращения доменов одних переменных на основе конкретизированных доменов других переменных. Для каждого типа ограничений подобный логический вывод осуществляется специализированной процедурой, которая называется пропогатором или распространителем ограничений данного типа.

Итак, для каждого типа ограничений задачи CSP должен иметься свой распространитель, согласно которому сокращаются домены участвующих в ограничении переменных. Результат работы распространителей называется распространением ограничений. Процесс распространения ограничения может завершиться с тремя исходами:

1. Всем переменным ограничения присвоены непротиворечивые значения из их доменов – ограничение удовлетворено.
2. Домен какой-либо переменной ограничения сокращен до пустого множества – получено противоречие, задача CSP не имеет решения.
3. Не всем переменным ограничения присвоены значения и нет переменных с пустыми доменами, но распространитель

Карьер кимберлитовых алмазов, Якутия
Источник: tatisol / Depositphotos.com

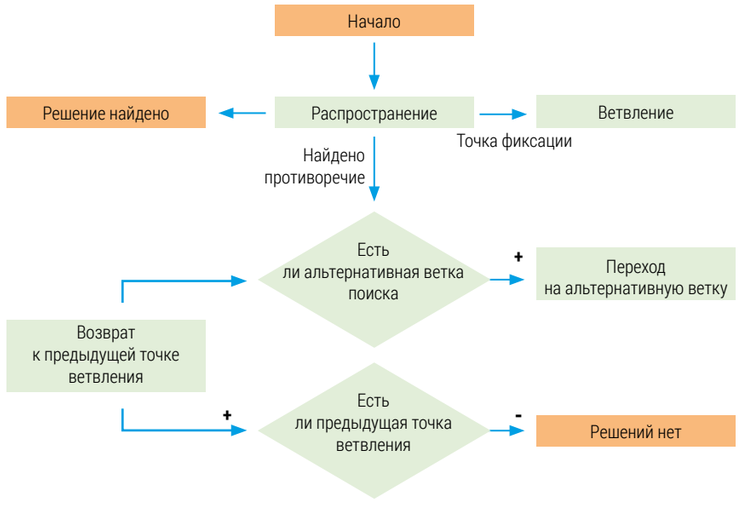
не в состоянии больше исключить ни одного значения из доменов оставшихся недоопределенными переменных, то есть процесс распространения достиг неподвижной точки (*fix point*).

В процессе решения задачи CSP последовательно запускаются распространители всех ограничений, причем, изменение домена какой-либо переменной в рамках одного распространителя приведет к повторному запуску распространителей всех ограничений, где участвует эта переменная. Таким образом, распространители постоянно запускают друг друга, пока каждый из них не придет к одному из вышеописанных результатов. При этом, выявление противоречия любым из распространителей делает задачу CSP неразрешимой.

В случае, если задача CSP имеет решение, то его не всегда удается отыскать только распространением ограничений, т. к. распространители могут прекратить свою работу, достигнув неподвижной точки. Для выхода из этой ситуации применяют различные стратегии информированного поиска [7] – к имеющимся ограничениям по определенным правилам (эвристикам) добавляется одно или несколько дополнительных ограничений на области определения некоторых переменных, а некоторые из имеющихся ограничений могут быть исключены из рассмотрения. Затем снова запускаются процедуры распространения ограничений, в которых задействованы данные переменных. К стратегиям информированного поиска, используемых при решении задач удовлетворения ограничений относят, прежде всего, методы поиска в глубину с возвратами, методы локального поиска и их гибриды. По какому принципу (согласно каким эвристикам) выбираются переменные и их значения (подмножества значений), а также то, как следует действовать, когда при данном выборе решения не существует, зависит от конкретной стратегии поиска.

При решении задач CSP часто используется комбинация стратегий поиска в глубину с возвратами и методов распространения ограничений [8–10]. Данный тип поиска называется систематическим, поскольку позволяет проверить все пространство поиска. Его обобщенная схема представлена на рис. 1.

Рис. 1. Обобщенная схема систематического поиска



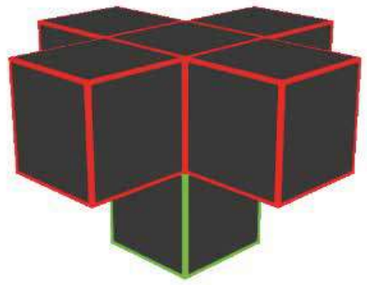


Рис. 2. Пример шаблона добычи

В работе [6] подробно изложены эвристики и другие особенности стратегии информированного поиска, предложенной авторами для реализации эффективных вычислений и организации процедуры ветвления при решении задачи планирования открытых горных работ.

Задача планирования открытых горных работ как задача удовлетворения ограничений

Для постановки задачи планирования открытых горных работ, карьер представляется в виде блочной модели, разделенный на блоки одинакового размера. Каждый блок модели обладает рядом свойств, зависящим от породы, содержащейся в нем, и каждому блоку в процессе решения должен быть сопоставлен номер периода разработки, в который этот блок должен быть извлечен из карьера.

Переменными задачи удовлетворения ограничений являются блоки модели, доменом переменных – множество периодов разработки карьера, а решением данной задачи будет присваивание каждой переменной определенного номера периода.

При построении решения задачи планирования открытых горных работ необходимо учитывать ряд условий, часть из которых отображают базовые ограничения на процесс разработки карьера, а некоторые описывают дополнительные требования к данному процессу.

К базовым ограничениям на процесс разработки карьера относятся ограничения технического и нормативного характера: допустимые углы уклона бортов карьера, минимальные размер площадок для расположения техники и т. д. В рамках блочной модели карьера эти ограничения обычно удается учесть путем задания шаблона извлечения блоков. Шаблон извлечение блоков применяется ко всем блокам модели и описывает, какие блоки карьера должны быть извлечены раньше или одновременно (в один период) с рассматриваемым блоком. Пример такого шаблона представлен на рис. 2, где ключевым является нижний блок.

К дополнительным можно отнести требования по равномерности работ, т. е. в каждый период необходимо извлекать примерно одинаковое количество блоков, а также ограничение на максимальную величину заглубления за один период выработки. Первое ограничение позволяет сформировать парк добывающей техники и равномерно его нагружать, второе – снизить сложность работ, поскольку излишнее заглубление осложнит перемещение техники по карьеру. Оба эти ограничения оптимизируют совокупные затраты на эксплуатацию добывающей техники, однако, эти затраты не учитываются в критерии эффективности решения задачи.

Важным аспектом эффективности вычислений в рамках парадигмы программирования в ограничениях является выбор способа представления задачи с помощью того или

Инженерные работы на объектах
Источник: agnormark.gmail.com / Depositphotos.com

иного набора ограничений, то есть моделирование задачи в терминах ограничений.

Для описания упомянутых выше ограничений задачи планирования открытых горных работ можно использовать ограничения базовых типов, которые встроены в среду программирования. Помимо арифметических и логических выражений, программные библиотеки программирования в ограничениях предоставляют ряд так называемых глобальных ограничений, которые представляют собой совокупности более простых ограничений. Распространители глобальных ограничений за счет совместного анализа простых ограничений позволяют исключать больше “лишних” значений из доменов переменных. Так, ограничение на то, что объемы добычи должны быть одинаковы с некоторой погрешностью для всех периодов разработки карьера, можно задать как линейное ограничение на количество блоков, которым присвоен номер определенного периода. В рамках задачи ограничения подобного типа задаются как для всех блоков, что позволяет равномерно загружать добывающую технику, так и отдельно для рудных блоков, поскольку рудные блоки дальше отправляются на обогащение, а мощности обогатительных предприятий также требуется загружать равномерно. Однако распространители линейных ограничений обладают низкой эффективностью, особенно в случае большого количества слагаемых.

В работах [5, 6] авторами был осуществлен выбор готовых глобальных ограничений для моделирования задачи планирования открытых горных работ.

Так, упомянутые ограничения на объемы добычи было предложено описывать с помощью глобального ограничения ***bin-packing***, которое легко масштабируется в зависимости от размерности задачи и эффективно обрабатывается решателем [5]. Ранее авторами условия на последовательность извлечения блоков было предложено представлять и обрабатывать с помощью набора глобальных ограничений ***max*** для каждого блока. При существенных размерностях блочной модели такое представление занимает значительные объемы памяти и недостаточно эффективно обрабатывается в связи с каскадным вызовом множества ограничений ***max*** при незначительных изменениях доменов переменных. Для более эффективного представления ограничений на порядок выработки блоков было разработано собственное ограничение.

В настоящей статье описывается разработанное авторами глобальное ограничение ***Block sequencing***, предназначенное для эффективной совместной обработки совокупности ограничений на последовательность извлечения блоков. Кроме того, глобальное ограничение ***Block sequencing*** позволяет учитывать требование на максимальную величину заглубления за один период разработки карьера.

Процедура-распространитель глобального ограничения Block sequencing

На листинге ниже представлен псевдокод, описывающий алгоритм работы распространителя для глобального ограничения ***Block sequencing***.

Block sequencing *(all, cubes)*

```
1   Q.init(all);
2   while Q not empty
3      k ← Q.first
4      Q.delete(Q.first)
5      maxlb←0
6      foreach value i ∈ cubes[k].above
7                lb←all[i].lb
8                if lb>maxlb then maxlb←lb
9                if all[i].ub←all[k].ub not failed
                 and changes all[i] domain then
                 Q.add(i)
10     if all[k].lb← maxlb not failed and
       changes all[k] domain then Q.add(k)
11     foreach value i ∈ cubes[k].below
12               if all[i].lb←all[k].lb not failed
                 and changes all[i] domain
                 then Q.add(i)
13     if all[cubes[k].bl].lb← all[k].lb+1 not
       failed and changes all[cubes[k].bl]
       domain then Q.add(cubes[k].bl)
14     if all[cubes[k].ab].ub← all[k].ub-1 not
       failed and changes all[cubes[k].ab]
       domain then Q.add(cubes[k].ab)
```

Поясним некоторые обозначения, приведенные на листинге.

Q – множество индексов распространяемых переменных.

all – массив распространяемых переменных (индексы этого массива хранятся в *Q*).

all[*k*].lb и *all*[*k*].ub – нижняя и верхняя границы домена переменной CSP *all*[*k*].

cubes – массив блоков, блоку *cubes*[*k*] соответствует переменная CSP *all*[*k*].

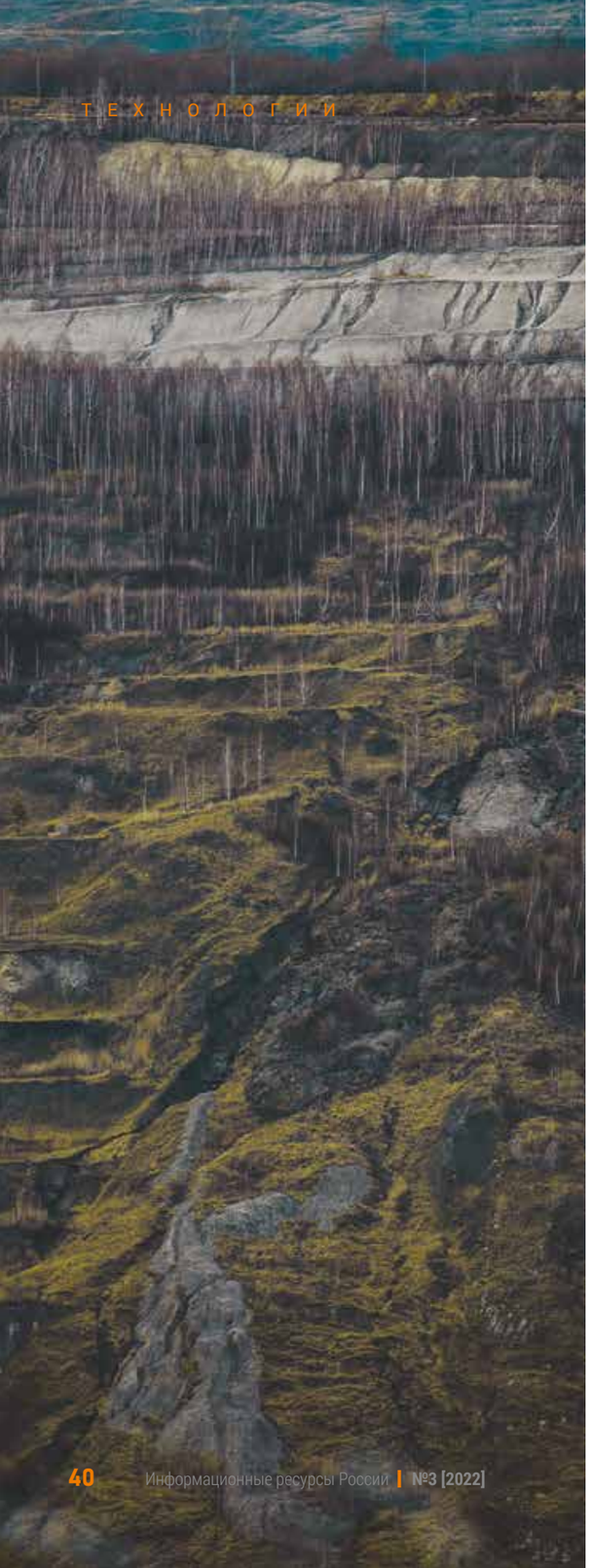
cubes[*k*].above – список индексов блоков (и соответствующих им переменных), которые необходимо вытащить вместе или раньше блока *k* согласно шаблону выработки.

cubes[*k*].below – список индексов блоков (и соответствующих им переменных), которые необходимо вытащить вместе или после блока *k* согласно шаблону выработки.

cubes[*k*].*ab* – индекс блока, находящегося выше блока *k* на величину нормы заглубления.

cubes[*k*].*bl* – индекс блока, находящегося ниже блока *k* на величину нормы заглубления.

Информатизация
производственных процессов
Источник: NATHAN MULLET / unsplash.com



Старый угольный карьер
Источник: Ilya Mirnyy / unsplash.com

В распространителе хранится очередь индексов переменных (*Q*), для которых надо выполнить распространение. На первом шаге производится инициализация данной очереди (строка 1). При первоначальном распространении в очередь попадают индексы всех блоков, при последующих распространениях – только индексы переменных, чей домен изменился.

Распространение продолжается, пока очередь не опустеет (строка 2). В процессе распространения из этой очереди извлекается индекс *k* (строки 3–4) и производятся следующие шаги алгоритма:

Шаг 1. Для всех блоков, находящихся согласно шаблону выше блока *k*, то есть для блоков, которые должны быть извлечены до блока *k*, урезаются домены соотнесенных с ними переменных, таким образом, чтобы все значения доменов были не больше максимального значения переменной *k*. Также при этом вычисляется максимальное из минимальных значений (*maxlb*) в упомянутых доменах переменных (строки 6–9).

Шаг 2. У переменной, соответствующей блоку *k*, урезается домен таким образом, чтобы его значения были не меньше *maxlb* (строка 10).

Шаг 3. Для всех блоков, находящихся согласно шаблону ниже блока *k*, урезаются домены таким образом, чтобы их значения были не меньше минимального значения домена переменной блока *k* (строки 11–12).

Шаг 4. Для блока *cubes*[*k*].*bl*, находящегося ниже блока *k* на величину нормы заглубления, урезается домен таким образом, чтобы его значения были больше минимального значения переменной *k* (строка 13).

Шаг 5. Для блока *cubes*[*k*].*ab*, находящегося выше блока *k* на величину нормы заглубления, урезается домен таким образом, чтобы его значения были меньше максимального значения переменной блока *k* (строка 14).

При попытке изменения домена любой переменной могут возникнуть следующие ситуации:

– домен переменной не поменялся. В этом случае никаких дополнительных действий не требуется;
– домен переменной поменялся, но не стал пустым. В этом случае индекс переменной добавляется в очередь распространения;
– домен переменной стал пустым. В таком случае сообщается о противоречии и распространитель завершает работу.

Если распространение завершилось без противоречий, производится проверка значений переменных. Если встречена хотя бы одна переменная с неопределенным значением (в домене осталось больше 1 значения), то считается, что ограничение достигло неподвижной точки. Если значения всех переменных определены, то ограничение считается удовлетворенным.

Далее в примере будут использованы следующие правила (эвристики) для выбора наиболее перспективной ветви дерева поиска:

Э1. Выбирается самый верхний рудный блок с еще не присвоенным значением, ему присваивается наименьшее значение из домена.

Э2. Если таких рудных блоков нет, то выбирается самый нижний вскрышной блок (блок с пустой породой), ему присваивается наибольшее значение из домена.

При наличии двух блоков на одной высоте, предпочтение будет отдано блоку с меньшим значением остальных координат.

В качестве примера рассмотрим построение плана разработки простейшего карьера. Пусть разработки ведутся в три периода. Сам карьер для наглядности будем считать двумерным, как и шаблон выработки для него (рис. 3).

В ячейках, представляющих блоки карьера, указаны домены соответствующих блокам переменных, цветом выделены рудные блоки (блоки с положительной ценностью). В качестве дополнительных ограничений укажем, что за период должно быть извлечено ровно 2 рудных блока и от 5 до 6 блоков в целом, а также что величина заглубления за период не должна превышать 2 блока. В примере будет демонстрироваться работа описанного распространителя. Детали работы стандартных распространителей (распространителей других глобальных ограничений, в частности *bin-packing*) будут опущены, а указаны лишь внесенные ими изменений. Также для решения будут использоваться эвристики для выбора текущей ветви дерева поиска, которые описаны выше.

Распространитель проверяет все блоки, начиная снизу. На основе анализа блоков D_4, C_3, D_3, E_3 на шаге 5 работы распространителя изменяются домены переменных для блоков D_2, C_1, D_1, E_1. На рис. 4 и далее редуцированные домены переменных выделены жирным шрифтом.

Далее на основе анализа блоков D_2, C_1, D_1, E_1 на шаге 4 работы распространителя изменяются домены переменных для блоков D_4, C_3, D_3, E_3 как показано на рис. 5, а сами переменные помещаются в очередь *Q*. Провер-

	A	B	C	D	E	F	G
1	[1..3]	[1..3]	[1..3]	[1..3]	[1..3]	[1..3]	[1..3]
2		[1..3]	[1..3]	[1..3]	[1..3]	[1..3]	
3			[1..3]	[1..3]	[1..3]		
4				[1..3]			

Рис. 3. Двумерная блочная модель карьера и шаблон извлечения

	A	B	C	D	E	F	G
1	[1..3]	[1..3]	**[1..2]**	**[1..2]**	**[1..2]**	[1..3]	[1..3]
2		[1..3]	[1..3]	**[1..2]**	[1..3]	[1..3]	
3			[1..3]	[1..3]	[1..3]		
4				[1..3]			

Рис. 4. Редукция доменов переменных для блоков, лежащих выше заданного более чем на норму заглубления

	A	B	C	D	E	F	G
1	[1..3]	[1..3]	[1..2]	[1..2]	[1..2]	[1..3]	[1..3]
2		[1..3]	[1..3]	[1..2]	[1..3]	[1..3]	
3			**[2..3]**	**[2..3]**	**[2..3]**		
4				**[2..3]**			

Рис. 5. Редукция доменов переменных для блоков, лежащих ниже заданного более чем на норму заглубления

	A	B	C	D	E	F	G
1	**1**	**1**	**1**	[1..2]	[1..2]	[1..3]	[1..3]
2		**1**	[1..3]	[1..2]	[1..3]	[1..3]	
3			[2..3]	[2..3]	[2..3]		
4				[2..3]			

Рис. 6. Редукция доменов переменных для блоков, лежащих выше заданного согласно шаблону выемки

	A	B	C	D	E	F	G
1	1	1	1	**1**	[1..2]	[1..3]	[1..3]
2		1	**1**	[1..2]	[1..3]	[1..3]	
3			[2..3]	[2..3]	[2..3]		
4				[2..3]			

Рис. 7. Состояние задачи CSP к моменту запуска ограничения bin-packing

	A	B	C	D	E	F	G
1	1	1	1	1	**2**	**[2..3]**	**[2..3]**
2		1	1	**2**	**[2..3]**	**[2..3]**	
3			[2..3]	[2..3]	[2..3]		
4				[2..3]			

Рис. 8. Состояние задачи CSP после работы ограничения bin-packing

	A	B	C	D	E	F	G
1	1	1	1	1	2	[2..3]	[2..3]
2		1	1	2	[2..3]	[2..3]	
3			[2..3]	[2..3]	**3**		
4				**3**			

Рис. 9. Состояние задачи CSP после очередной итерации

	A	B	C	D	E	F	G
1	1	1	1	1	2	[2..3]	[2..3]
2		1	1	2	[2..3]	[2..3]	
3			**2**	**3**	3		
4				3			

Рис. 10. Состояние задачи CSP после конкретизации значений для всех переменных, соответствующих рудным блокам

	A	B	C	D	E	F	G
1	1	1	1	1	2	**3**	[2..3]
2		1	1	2	3	3	
3			2	3	3		
4				3			

Рис. 11. Обнаружение тупиковой вершины дерева поиска

	A	B	C	D	E	F	G
1	1	1	1	1	2	2	2
2		1	1	2	3	3	
3			2	3	3		
4				3			

Рис. 12. Решение задачи CSP

ка оставшихся в очереди элементов ничего не дает. Процесс распространения ограничений достигает неподвижной точки.

Для выхода из этой ситуации необходимо выполнить ветвление процесса поиска решений. Для этого согласно первой эвристике (**Э1**) блоку B_2 присваивается значение 1, что влечет за собой запуск распространителя. При анализе блока B_2, на шаге 1 работы распространителя изменяются домены переменных, соответствующих блокам A_1, B_1, C_1 (рис. 6).

После этого процесс распространения снова достигает неподвижной точки. Выход из нее снова производится согласно **Э1** путем присваивания блоку C_2 значения 1, что на шаге 1 алгоритма вызовет изменение домена переменной для блока D_1 (рис. 7).

В результате получается, что максимальному количеству блоков (как рудных, так и в целом) присвоено значение 1, поэтому распространители ограничений на норму выработки руды и пустой породы (глобальное ограничение *bin-packing*) исключают значение 1 из доменов всех оставшихся переменных (рис. 8).

Затем снова активируется распространитель глобального ограничения *Block sequencing*. На основе анализа блоков E_1 и D_2, на шаге 4 работы распространителя домены переменных для блоков E_3 и D_4 сужаются до значения 3, то есть полностью конкретизируются, после чего достигается очередная неподвижная точка (рис. 9).

Для выхода из нее переменной блока C_3, согласно эвристике **Э1**, будет присвоено значение 2, после чего, в результате распространения ограничения на норму рудных блоков, блоку D_3 присваивается значение 3 (рис. 10).

Дальнейший процесс решения заключается в ветвлении дерева поиска с применением эвристики **Э2**. Согласно **Э2**, переменным E_2, F_2, в соответствующей очередности, присваивается значение 3. Далее эта же эвристика применяется и к блоку F_1, и переменной F_1 присваивается значение 3, однако, при дальнейшем распространении с помощью глобального ограничения bin-packing выясняется, что последнее присваивание приводит к противоречию, т. к. в этом случае останется всего 4 блока со значением 2 (рис. 11).

Большой алмазный карьер
Источник: ccat82 / Depositphotos.com

Программный код
Источник: Jake Walker / unsplash.com

Продолжение процесса решения заключается в осуществлении возврата в последний пройденный узел дерева поиска и выборе значения переменной F_1 отличного от того значения, которое привело к появлению конфликта (противоречия), то есть выбирается последнее из еще неисследованных значений переменной F_1, а именно значение 2. Аналогичным образом значение 2 присваивается и переменной G_1, что приводит к решению рассматриваемой задачи CSP, представленному на рис. 12.

ЗАКЛЮЧЕНИЕ

По сравнению с ранее использованным авторами способом представления ограничений на последовательность извлечения блоков, применение глобального ограничения *Block sequencing* при решении рассматриваемой задачи планирования открытых горных работ позволяет существенно увеличить скорость получения решения, поскольку избавляет от затратных процедур многократного вызова небольших распространителей. За один вызов разработанный распространитель глобального ограничения *Block sequencing* анализирует и редуцирует домены всех переменных, которые итеративно изменяются при выполнении шагов 1–5. Глобальное ограничение *Block sequencing* позволяет реализовать более глубокую редукцию доменов переменных, то есть в процессе распространения (вывода) из рассмотрения исключается больше “лишних” значений, которые не входят ни в одно решение задачи CSP. Подобный эффект достигается не только благодаря совместному анализу набора ограничений на последовательность извлечения блоков, но и учету в основном цикле распространителя дополнительного ограничения на допустимый уровень заглубления за период. По сравнению с методами целочисленного линейного программирования использование парадигмы программирования в ограничениях позволяет существенно снизить требования к оперативной памяти за счет имплицитного представления ограничений, что, в конечном счете, приводит к возможности решать задачи с требуемым уровнем дискретизации модели карьера.

Работа выполнена при финансовой поддержке РФФИ, грант №20-07-00708а.

DEVELOPMENT OF A GLOBAL BLOCK SEQUENCING CONSTRAINT TO EFFECTIVELY SOLVE THE OPEN PIT MINE SCHEDULING PROBLEM AS A CONSTRAINT SATISFACTION PROBLEM

Oleynik Yurii, Junior Researcher, Institute for Informatics and Mathematical Modeling – a separate Subdivision of the Federal Research Centre «Kola Science Centre of the Russian Academy of Sciences».
E-mail: yoleynik@iimm.ru

Zuenko Alexander, PhD in Technical Sciences, Leading Researcher, Institute for Informatics and Mathematical Modeling – a separate Subdivision of the Federal Research Centre «Kola Science Centre of the Russian Academy of Sciences».
E-mail: zuenko@iimm.ru

Abstract. The article is dedicated to the creation of highly efficient constrained programming tools for solving the problems of open pit mine scheduling. A global Block sequencing constraint has been developed, the propagator of which jointly analyzes the conditions for the block extraction sequence, as well as some additional requirements, which can significantly increase the efficiency of calculations.
Keywords: constraint satisfaction problem, constraint programming, open pit mine scheduling, global constraint, operation research.

Библиографический список:

1. Fathollahzadeh K. A mathematical model for open pit mine production scheduling with Grade Engineering and stockpiling / K. Fathollahzadeh, E. Mardaneh, M. Cigla, M. Waqar Ali Asad // International Journal of Mining Science and Technology. 2021. Vol. 31(4). P. 717–728.
2. Alipour A. An integrated approach to open-pit mines production scheduling / A. Alipour, A. A. Khodaiari, A. Jafari, R. Tavakkoli-Moghaddam // Resources Policy. 2022. Vol. 75. 102459.
3. Tolouei K. An optimisation approach for uncertainty-based long-term production scheduling in open-pit mines using meta-heuristic algorithms / K. Tolouei, E. Moosavi, A. Bangian, P. Afzal, A. Aghajani Bazzazi // International Journal of Mining Reclamation and Environment. 2021. Vol. 35. P. 1–26.
4. Alipour A. Production scheduling of open-pit mines using genetic algorithm: a case study / A. Alipour, A. A. Khodaiari, A. Jafari, R. Tavakkoli-Moghaddam // International Journal of Management Science and Engineering Management. 2019. Vol. 15. P. 1–8.
5. Zuenko A. A. Method for solving the open-pit mine production scheduling problem using the constraint programming paradigm / A. A. Zuenko, Y. A. Oleynik, R. A. Makedonov // Journal of Physics: Conference Series. 2021. Vol. 2060. P. 12–21.
6. Зуенко А. А. Интеллектуальный поиск точных решений задачи планирования открытых горных работ / А. А. Зуенко, Ю. А. Олейник, Р. А. Македонов // Системы анализа и обработки данных. № 3 (83). 2021. С. 99–114.
7. Russel S., Norvig P. Artificial Intelligence: A Modern Approach. 3rd edition. / Prentice Hall, 2010. 1132 p.
8. Narváez D. Constraint Satisfaction Techniques for Combinatorial Problems / D. Narváez // Proceedings of the AAAI Conference on Artificial Intelligence. 2018. Vol. 32(1). pp. 8028–8029.
9. Barto L. Polymorphisms, and how to use them. / L. Barto, A. A. Krokhin, R. Willard // The Constraint Satisfaction Problem: Complexity and Approximability. 2017. Vol. 7. P. 1–44.
10. Kozik M. Solving CSPs using weak local consistency / M. Kozik // SIAM Journal on Computing. 2021. Vol. 50(4). P. 1263–1286.

Bibliography:

1. Fathollahzadeh K. A mathematical model for open pit mine production scheduling with Grade Engineering and stockpiling / K. Fathollahzadeh, E. Mardaneh, M. Cigla, M. Waqar Ali Asad // International Journal of Mining Science and Technology. 2021. Vol. 31(4). P. 717–728.
2. Alipour A. An integrated approach to open-pit mines production scheduling / A. Alipour, A. A. Khodaiari, A. Jafari, R. Tavakkoli-Moghaddam // Resources Policy. 2022. Vol. 75. 102459.
3. Tolouei K. An optimisation approach for uncertainty-based long-term production scheduling in open-pit mines using meta-heuristic algorithms / K. Tolouei, E. Moosavi, A. Bangian, P. Afzal, A. Aghajani Bazzazi // International Journal of Mining Reclamation and Environment. 2021. Vol. 35. P. 1–26.
4. Alipour A. Production scheduling of open-pit mines using genetic algorithm: a case study / A. Alipour, A. A. Khodaiari, A. Jafari, R. Tavakkoli-Moghaddam // International Journal of Management Science and Engineering Management. 2019. Vol. 15. P. 1–8.
5. Zuenko A. A. Method for solving the open-pit mine production scheduling problem using the constraint programming paradigm / A. A. Zuenko, Y. A. Oleynik, R. A. Makedonov // Journal of Physics: Conference Series. 2021. Vol. 2060. P. 12–21.
6. Zuenko A. A. Intellectual search for exact solutions to the problem of planning open pit mining / A. A. Zuenko, Yu. A. Oleinik, R. A. Makedonov // Systems of data analysis and processing. 2021. Issue. 3(83). pp. 99–114.Russel S., Norvig P. Artificial Intelligence: A Modern Approach. 3rd edition. / Prentice Hall, 2010. 1132 p.
7. Russel S., Norvig P. Artificial Intelligence: A Modern Approach. 3rd edition. / Prentice Hall, 2010. 1132 p.
8. Narváez D. Constraint Satisfaction Techniques for Combinatorial Problems / D. Narváez // Proceedings of the AAAI Conference on Artificial Intelligence. 2018. Vol. 32(1). pp. 8028–8029.
9. Barto L. Polymorphisms, and how to use them. / L. Barto, A. A. Krokhin, R. Willard // The Constraint Satisfaction Problem: Complexity and Approximability. 2017. Vol. 7. P. 1–44.
10. Kozik M. Solving CSPs using weak local consistency / M. Kozik // SIAM Journal on Computing. 2021. Vol. 50(4). P. 1263–1286.

УДК 621.311
DOI 10.52815/0204-3653_2022_03187_46
EDN: GYJDGG

Источник: 4pmphoto@gmail.com / Depositphotos.com

ПОВЫШЕНИЕ КВАЛИФИКАЦИИ ПЕРСОНАЛА ПУТЕМ ВНЕДРЕНИЯ ЦИФРОВЫХ ТРЕНАЖЕРОВ

Орлов Константин
Доцент, к.т.н., заведующий кафедрой теоретических основ теплотехники им. М.П. Вукаловича ФГБОУ ВО «НИУ «МЭИ».
E-mail: OrlovKA@mpei.ru

Охлопков Андрей
Начальник службы экспертизы и технического развития (СЭТР) ПАО «Мосэнерго».
E-mail: OkhlopkovAV @mosenergo.ru

Битней Владислав
Главный специалист по управлению проектами.
E-mail: BitneyVD@mosenergo.ru

Аннотация. Развитие цифровизации актуализирует вопросы профессионализации и подготовки кадров, способных принимать оперативные решения в нештатных ситуациях. Использование компьютерных средств обучения и мониторинга на базе цифровых двойников технологических объектов обеспечивает повышение психологической устойчивости оперативного персонала при действиях в аварийных ситуациях, сокращение числа технологических нарушений, а также повышение уровня надежности и безотказности работы оборудования, сохранности имущества, безопасности и здоровья персонала объектов электроэнергетики. Профессиональная подготовка оперативного персонала с использованием программно-технических комплексов реализуется в «Мосэнерго» с 2011 г., в связи с чем в статье рассмотрены следующие области:

- *анализ существующих нормативно-технических документов, регламентирующих требования к тренажерам оперативного персонала;*
- *прототип тренажера – математическая модель турбогенератора ТЗФГ-160–2МУЗ позволяющего выполнять расчеты магнитного поля турбогенератора в полной трехмерной постановке и представлять информацию о режимах работы, магнитном состоянии элементов конструкции, силовых взаимодействий.*

Ключевые слова: *повышение квалификации персонала, автоматизированный обучающий комплекс, тренажер, ТЭС, математическая модель, турбоустановка.*

При аварийных ситуациях главной проблемой является взаимодействие специалистов. Проведение совместных тренировок всех цехов для отработки навыков совместных действий становится крайне актуальным

ВВЕДЕНИЕ

Повышение квалификации персонала – одна из наиболее значимых задач в энергетике, что подтверждается соответствующим приказом Минэнерго России от 22.09.2020 г. № 796 «Об утверждении правил работы с персоналом в организациях электроэнергетики Российской Федерации» [1]. На данный момент, на каждом объекте электроэнергетики имеются опытные специалисты, но не все из них способны передать свои знания новым сотрудникам. Молодые специалисты, приходящие в компанию, не только не обладают опытом и знаниями, но и зачастую должной мотивацией к обучению, что негативно сказывается как на собственной безопасности, так и на надежности и безопасности энергосистемы в целом.

В каждой организации электроэнергетики вопросам безопасности и снижения травматизма уделяется большое внимание. Для этих целей зачастую создаются отдельные службы, основными задачами которых являются: контроль соблюдения работниками организации требований в области охраны труда, проведение мероприятий по минимизации травматизма на производстве и организация инструктажей для работников предприятия по охране труда. К сожалению, полностью исключить травматизм невозможно, однако за счет применения современных методов подготовки и обучения персонала, можно значительно снизить количество несчастных случаев. Министерство энергетики России в своих отчетах регулярно публикует отраслевую статистику производственного травматизма. В отчете по итогам второго полугодия 2020 г. отмечены основные факторы несчастных случаев [2]:

- в генерирующих компаниях на первом плане нарушения требований и норм охраны труда (45,3% случаев), которая усугублялась неудовлетворительной организацией производства работ (26,6% случаев), личной неосторожностью пострадавших (15,6% случаев);
- в электросетевых предприятиях на первом плане нарушения требований и норм охраны труда (41,3% случаев), к которым добавились личная неосторожность пострадавших (26,9% случаев), неудовлетворительная организация работ (15,9% случаев).

В применении к любой категории оперативного персонала объем выполняемых работ, в том числе оперативных переключений, а, следовательно, и количество технологических нарушений, приводящих к авариям и несчастным случаям, зависят от ряда факторов, таких как состав оборудования, схема первичных соединений, ре-

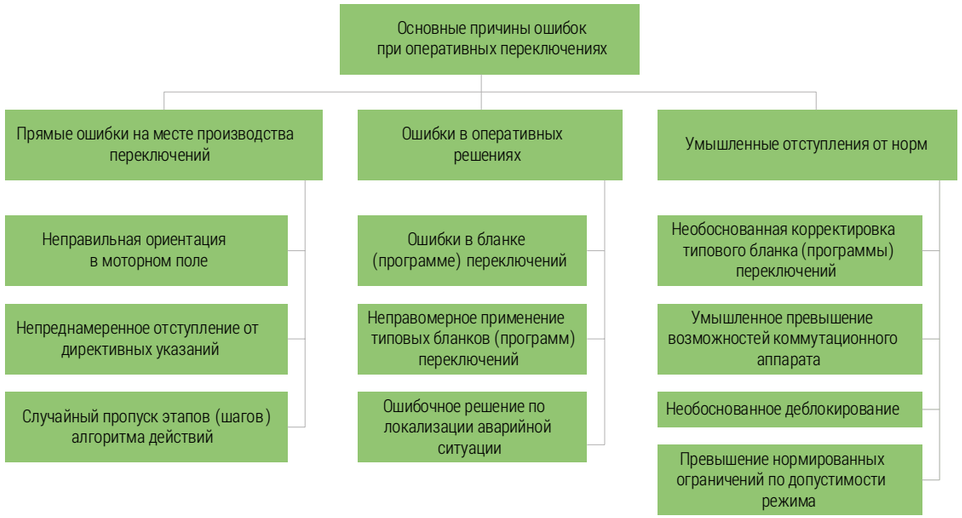


Рис. 1. Классификация причин ошибок при оперативных переключениях

жим работы и организация обслуживания энергообъекта.

По данным анализа ошибочных действий оперативного персонала ОАО «Федеральная сетевая компания единой энергетической системы» количество технологических нарушений, связанных с ошибочными действиями оперативного персонала от общего числа ошибочных действий составило в период с 2015 по 2021 гг. соответственно 58 %, 40 %, 74 %, 41,7 %, 30,9 %, 28,1 %, 39 % [3]. Классификация причин ошибок при оперативных переключениях приведена на рис. 1.

Нормативно-технические документы и регламентация требований к тренажерам оперативного персонала

Требования к тренажерам и программным средствам подготовки персонала энергетических предприятий регламентируются двумя нормативными документами, которые действуют в России и странах СНГ [4]: «Технические условия для сертификации прикладных программных средств тренажеров для тепловых электростанций и сетей» СТУ 115.015–2003 [5] и «Нормы годности программных средств подготовки персонала энергетики» – СО 153–34.0–12.305–99 [6].

Рассмотрим каждый из них:

1. Технические условия для сертификации прикладных программных средств тренажеров для ТЭС и сетей СТУ 115.015–2003 были введены 5 июня 2003 г. Министерством РФ по связи и информатизации. Данный документ, разработанный ФГУП «ВНИИПВТИ» совместно с ЗАО «ТЭСТ» и согласованный с РАО «ЕЭС России», регламентирует состав и возможные границы значений параметров для ПО тренажеров в соответствии с требованиями стандартов [7]. Особо значимым является описание основных требований к функциям обработки данных, методам оценки характеристик и информационной безопасности.
2. Нормы годности программных средств подготовки персонала энергетики были разработаны и введены в 1999 году департаментом генеральной инспекции по эксплуатации и финансового аудита РАО «ЕЭС России» и акционерным обществом «Главный вычислительный центр энергетики» при участии Московского энергетического института, Московского государственного университета, Новочеркасского государственного технического университета, Южного центра подготовки кадров предприятия «Южэнерготехнадзор». Данный документ устанавливает требования к программным средствам подготовки, используемым для персонала предприятий энергетики России на различных этапах производственной подготовки, которые состоят из программно-технических и функциональных норм годности.

Особенно важно отметить регламентированные требования к моделям объектов управления тренажеров:

- все допущения, которые принимаются при построении моделей, не должны искажать физическую картину происходящих в объекте процессов, при любых режимах работы объекта в тренажере;
- математическое описание физических процессов, которые происходят в реальном объекте, в виде систем дифференциальных, алгебраических и логических уравнений, должны лежать в основе построения модели. Определение параметров должно производиться на основе технологических характеристик оборудования и экспериментальных данных о работе объекта;
- модель должна иметь достаточную точность – отклонение моделируемых параметров от реальных настолько мало, что допускается экспертами при приемке тренажера;
- необходимо сохранение реального (ускоренного) масштаба времени при воспроизведении процессов на тренажере;
- должна обеспечиваться необходимая полнота моделирования, определяемая конкретной стадией подготовки: должны моделироваться все необходимые для

Цифровой тренажер 3D
Источник: annas.stills.gmail.com / Depositphotos.com

Пермская ГРЭС
Источник: «Интер РАО»

этой стадии режимы работы, контролируемые параметры и органы управления объекта моделирования при наличии требуемого набора воспроизводимых аварий и отказов в работе технологического оборудования и устройств автоматики.

Компьютерный тренажер для персонала энергоблока мощностью 800 МВт Пермской ГРЭС

Особой подготовки требует не только эксплуатационный персонал котлотурбинного цеха, действия которого определяют состояние водного режима энергоблока, но и персонал химического цеха, обеспечивающего работу установок по организации водного режима. Высокая квалификация персонала лежит в основе надежности и экономичности работы оборудования при эксплуатации мощных энергоблоков сверхкритического давления [8].

На данный момент на ТЭС применяются тренажеры, которые готовят и тренируют персонал отдельных цехов. Это позволяет осуществлять специализированную индивидуальную подготовку сотрудников, обслуживающих конкретное оборудование электростанций.

Однако в нештатных и аварийных ситуациях самой главной проблемой является взаимодействие групп специалистов. Поэтому проведение совместных (комплексных) тренировок оперативного персонала всех цехов и служб, направленных на совершенствование навыков взаимодействия при решении той или иной задачи, становится все более актуальным. Создание программ-тренажеров, моделирующих работу всего теплоэнергетического оборудования и процессов, протекающих в нем, является одним из путей решения этой проблемы.

Попытка разработки единого тренажера для сотрудников котлотурбинного и химического цехов была предпринята на Пермской ГРЭС. Основной программный комплекс тренажера энергоблока был создан специалистами ЗАО «Пик Прогресс». В результате их сотрудничества с кафедрой ТВТ (сейчас кафедра называется ТОТ) МЭИ тренажер был дополнен программами, моделирующими рабочие места аппаратчика блочной обессоливающей установки и лаборанта химической лаборатории.

Тренажер для подготовки персонала тепловых сетей

В соответствии с корпоративным стандартом «Стандарт организации профессиональной подготовки, переподготовки, повышения квалификации персонала» РАО «ЕЭС России» раз в три года проводятся соревнования по профмастерству сотрудников. В последнее время для оценки уровня квалификации персонала используются тренажеры и программно-технические средства, позволяющие смоделировать основные процессы, применяемые в энергетике. Для проведения соревнований по работе диспетчера по управлению оборудованием тепловых сетей при аварийных режимах и нормальной эксплуатации НИУ «МЭИ» и ООО «Триеру» разработали тренажер на базе оболочки TBT Shell [9].

Задачей тренажера была разработка программного продукта, который позволит проводить обучение и проверку знаний диспетчера тепловой сети, его умений по эксплуатации оборудования и локализации аварий. Оперативная технологическая схема с актуальными параметрами арматуры и приборов являлась основным вспомогательным инструментом диспетчера для принятия решений.

Тренажер КТЦ нового поколения для тепловой генерации «Русгидро» на базе открытой цифровой модели

НИУ «МЭИ» совместно с АО «ХЭТК» инициировало создание тренажера в сентябре 2021 г. для ПАО «Русгидро». На данный момент большинство существующих программ для повышения квалификации персонала имеют следующий набор проблем:

- созданы под устаревшее ПО (MS-DOS, Windows NT, Unix и т. д.);
- значительно ограничены (или полная невозможность) изменения пользователем;
- сложность или закрытость в изменении модели (нет компетенций у пользователя и требуется участие разработчика);
- невозможность или значительное неудобство использования для решения других задач, в том числе тиражирования и развития.

НИУ «МЭИ» осуществляет разработку научных основ и пилотного тренажера для персонала котлотурбинного цеха нового поколения на базе открытой цифровой модели с возможностью комплексных тренировок с участием сотрудников химического и тепловой автоматики и измерений цехов.

Открытая цифровая модель программно-технического комплекса будет иметь следующие преимущества:

- возможность изменения модели пользователем;
- возможность расчета модели в базовом ПО с возможностью получения всех данных по работе модели;
- первоначальная оптимизация модели для применения в тренажере КТЦ с возможностью развития модели для других применений;
- возможность подключения к внешней АСУ ТП и другим тренажерным комплексам;
- возможность расчета переходных теплогидравлических (с учетом сжимаемости), электрических и физико-химических процессов.

Тренажер-анализатор главной электрической схемы станции

ЗАО «Тренажеры для электростанций» разработало компьютерный тренажер-анализатор главной электрической схемы электростанции для оперативного персонала электроцеха.

Основная особенность тренажера: наличие высокоточной полной всережимной математической модели электрической части станции. Теоретические основы построения модели и основные уравнения изложены

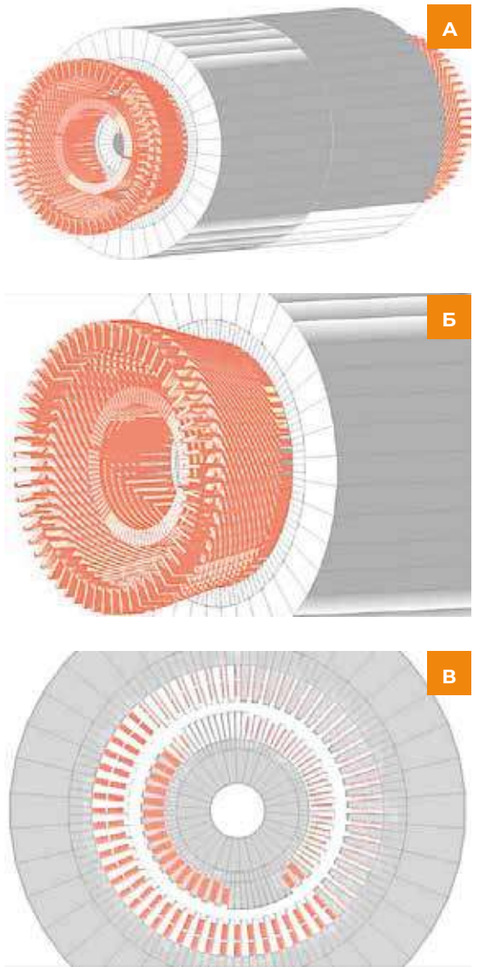
Работник инструментальной мастерской
Источник: kalinovsky / Depositphotos.com

в статье «Комплексные анализаторы процессов функционирования электрооборудования электростанций» [10].

Высокоточная модель в составе тренажера-анализатора позволяет предсказывать электрический режим работы станции (или подстанции) и производить анализ произошедших аварийных ситуаций, для чего в тренажер-анализатор включена функция построения осциллограмм «быстрых» переходных процессов.

В состав тренажера-анализатора включена подсистема поддержки обучения персонала, включающая:

- дополнительные защиты и блокировки, которых нет на реальной станции, или подстанции, но которые предупреждают обучаемого о сделанной ошибке, или о приближении к аварийной ситуации (за несколько шагов до нее);
- традиционными сервисными функциями обучающих систем, такими как:
  - загрузка исходного состояния;
  - сохранение текущего состояния;
  - режимы реальное/ускоренное время;
  - режимы работа/заморозка;
  - возможность повторения ранее выполненных действий.
- возможность работы в локальной сети одновременно на нескольких компьютерах.
- Назначение тренажера-анализатора:
- анализ электрических режимов станции (подстанции), возникающих в результате переключений в главной электрической схеме и изменений генерируемых и выдаваемых в систему (потребителям) активных и реактивных мощностей;
- проверку профессиональной квалификации оперативного персонала при управлении электрическим оборудованием в сложных режимах;
- проведение соревнований и конкурсов оперативного персонала по профессиональному мастерству;



а – общий вид модели турбогенератора;
б – лобовая часть турбогенератора;
в – поперечное сечение в средней части генератора

Рис. 2. Модель конструкции магнитной системы турбогенератора ТЗФГ-160-2МУЗ в программном комплексе Easymag3D

- проведение противоаварийных тренировок.

Разработка тренажера-анализатора применительно к главной электрической схеме ТЭЦ-26 «Мосэнерго» завершена в апреле 2004 г. Тогда же тренажер поставлен на ТЭЦ-26 «Мосэнерго» в двух модификациях: как анализатор (на одном компьютере – установлен на ЦЩУ) и как тренажер в центре подготовки персонала ТЭЦ-26 (на сети из трех компьютеров). В ноябре 2004 г. указанный тренажер использовался на системных соревнованиях оперативного персонала ОАО «Мосэнерго».

Разработка математической модели турбогенератора ТЗФГ-160–2МУЗ

В рамках проведения НИОКР «Разработка методики выбора оптимальных режимов по реактивной мощности для турбогенераторов с оценкой влияния режимов работы на надежность работы генерирующего оборудования» ФГБОУ ВО НИУ «МЭИ» разработало математическую модель турбогенератора ТЗФГ-160–2МУЗ для ПАО «Мосэнерго», которую в дальнейшем планируется перевести в цифровой тренажер, позволяющий исследовать поведение ТГ в маневренных режимах работы и обучить персонал базовому набору инструкций при его поломке.

Для расчетов электромагнитного поля турбогенератора использован программный комплекс EasyMag3D, разработанный в НИУ «МЭИ». Он базируется на методе пространственных интегральных уравнений и обеспечивает высокопроизводительные расчеты трехмерных магнитных систем в параллельных процессах.

На рис. 2 показана модель конструкции магнитной системы турбогенератора ТЗФГ-160–2МУЗ. Принято допущение о наличии полной зеркальной симметрии по длине генератора, т. е. расчетная область была ограничена половиной длины генератора. В азимутальном направлении расчетная область полная и охватывает 360°.

В результате расчетов будут получены данные о процессах, происходящих в режимах работы с регулированием реактивной мощности, которые позволят оценить их влияние на элементы конструкции турбогенератора. На рис. 4 представлена 3D-модель, используемая для расчета. Современные вычислительные средства позволяют воспроизвести геометрию магнитной системы и учесть ее особенности при анализе электромагнитного поля. Особое внимание уделяется торцевой части статора.

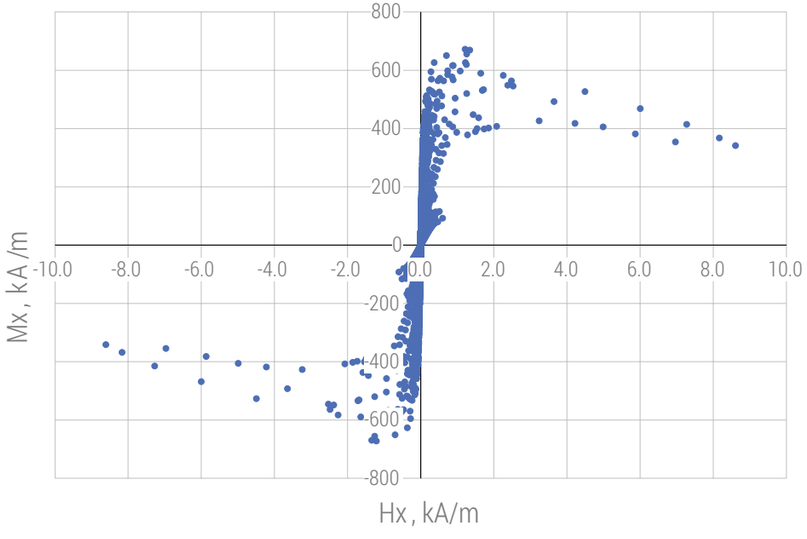
В результате моделирования могут быть получены различные типы данных, которые в дальнейшем анализируются и сопоставляются с режимами работы турбогенераторов. На рис. 3 представлены данные по осевой компоненте намагниченности в стали, на основе которых оценивается насыщение различных участков статора. Такие расчеты проводятся с целью проверки известного предположения об увеличении осевого магнитного поля в турбогенераторах в режиме потребления реактивной мощности, которое может вызывать увеличение потерь в торцевых зонах. На рис. 4 показано распределение вектора удельной силы, действующей на один стержень обмотки статора в зоне выхода из паза. Эти расчеты позволяют исследовать усилия, действующие в торцевых зонах, которые могут приводить к повышенным вибрациям обмотки и ее повреждению.

Разработанное программное обеспечение и модели позволяют выполнять расчеты магнитного поля турбогенератора в полной трехмерной постановке и представляют информацию о режимах работы, магнитном состоянии элементов конструкции, силовых взаимодействий и др.

ВЫВОДЫ

1. Всестороннее применение программно-технических комплексов по подготовке оперативного персонала позволит значительно снизить аварийность по вине персонала. Соответственно повышение капитальных затрат на реорганизацию процесса обучения сотрудников позволит получить значительный экономический эффект.
2. Приобретение персоналом навыков оперативной деятельности в нормальных и экстренных ситуациях, которые позволят обеспечить наилучшие показатели работы оборудования, особенно его сохранность, является основной задачей обучения персонала. При этом полученные знания должны служить только задаче принятия наилучших решений при управлении оборудованием.
3. Главной составляющей получаемых знаний является формирование навыка принятия оперативных решений.
4. Совместное использование программных средств подготовки персонала и обучающих вычислительных систем позволит получить наиболее качественное формирование навыков оперативной деятельности.
5. Тренажеры должны стать центральным, системообразующим фактором системы подготовки и повышения квалификации персонала, а также гарантом обеспечения надежной, безопасной и экономичной эксплуатации оборудования электроэнергетики России.

Рис. 3. Зависимость осевой компоненты намагниченности от осевой компоненты напряженности магнитного поля в статоре



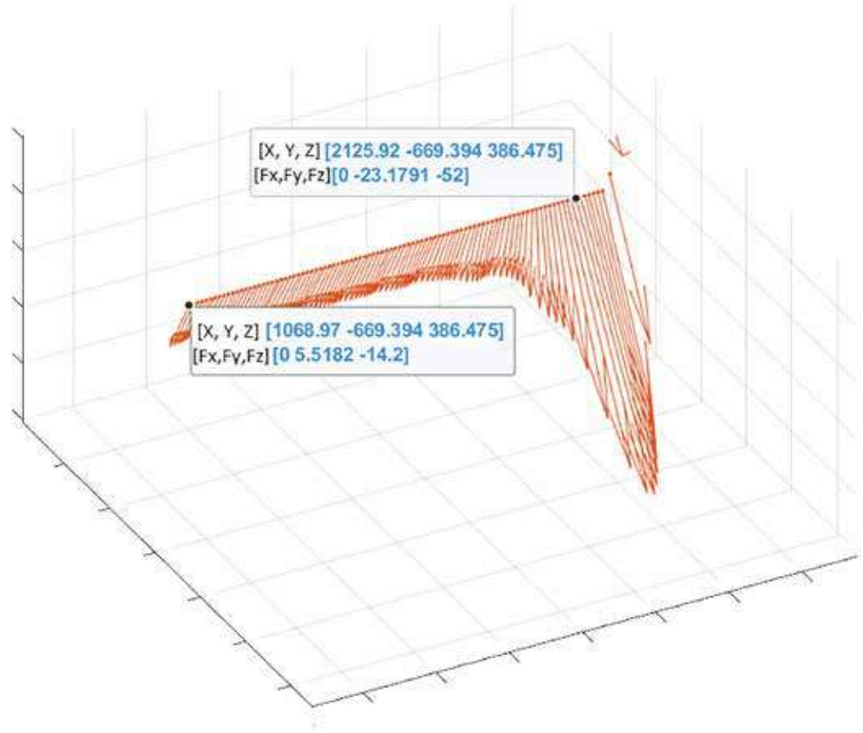


Рис. 4. Вектор удельной силы, действующий на стержень обмотки статора

STAFF DEVELOPMENT THROUGH THE INTRODUCTION OF DIGITAL SIMULATORS

Orlov Konstantin, Candidate of Technical Sciences, Associate Professor, Head of the Department of Theoretical Foundations of Thermal Engineering named after M.P. Vukalovich National Research University «Moscow Power Engineering Institute».
E-mail: OrlovKA@mpei.ru

Okhlopkov Andrey, Head of the Expertise and Technical Development Service PJSC Mosenergo.
E-mail: OkhlopkovAV@mosenergo.ru

Bitney Vladislav, Chief Project Management Specialist of the Expertise and Technical Development Service PJSC Mosenergo.
E-mail: BitneyVD@mosenergo.ru

Abstract. The development of digitalization with its dynamism and speed of innovative transformations actualize the issues of professionalization and training of personnel capable of making operational decisions in emergency situations. The use of computer-based training and monitoring tools based on digital twins of technological facilities ensures an increase in the psychological stability of operating personnel in emergency situations, a reduction in the number of technological failures, and an increase in the reliability and fail-safety of equipment operation, property safety, safety and health of electric power facilities personnel. Professional training of operating personnel via software and hardware complexes has been implemented in Mosenergo since 2011. The following areas are considered in the article in this regard:
- analysis of existing regulatory and technical documents governing the requirements for operating personnel simulators;
- simulator prototype - a mathematical model of T3FG-160-2MU3 turbogenerator, offering full three-dimensional calculations of turbine generator magnetic field and providing information about the modes of operation, the magnetic state of structural elements, force interactions.

Keywords: staff development, automated training complex, simulator, TPP, mathematical model, turbine unit.

Библиографический список:

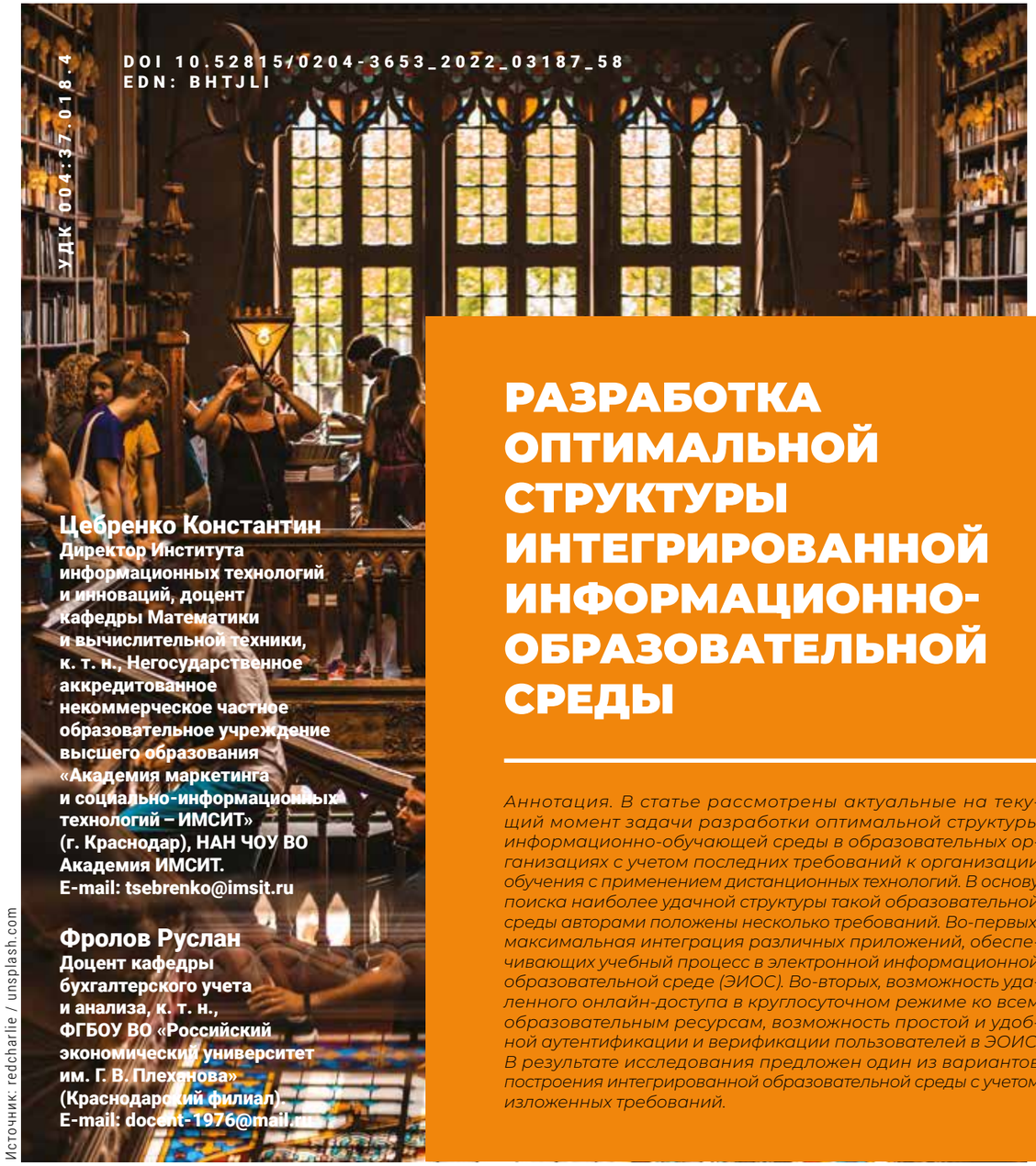
1. Приказ Министерства энергетики Российской Федерации от 22.09.2020 г. № 796 «Об утверждении правил работы с персоналом в организациях электроэнергетики Российской Федерации» – Текст: электронный // Официальный интернет-портал правовой информации: [сайт].– 2021 г.– URL: https://normativ.kontur.ru/document?moduleId=1&documentId=381455 (дата обращения: 10.11.2021).
2. Информационно-аналитическая справка по травматизму за 2-е полугодие 2020 г. Текст: электронный // Официальный сайт Министерства энергетики Российской Федерации: [сайт].– URL: https://minenergo.gov.ru/node/272 (дата обращения: 10.11.2021).
3. Детина С. А. Надежность оперативного персонала при осуществлении оперативных переключений: специальность 05.26.01 «Охрана труда (по отраслям)»: автореферат диссертации на соискание ученой степени кандидата технических наук / Детина Светлана Александровна.– Челябинск, 2021.– 22 с.
4. Магид С. И., Загретдинов И. Ш., Мищеряков С. В., Архипова Е. Н., Самойлов В. Л. Нормирование цифровых технологий тренажерных систем как способ обеспечения надежности условий обслуживания объектов электроэнергетики (часть 1). Надежность и безопасность энергетики. 2019;12(3):177–189. https://doi.org/10.24223/1999-5555-2019-12-3-177-189
5. Технические условия для сертификации прикладных программных средств тренажеров для тепловых электростанций и сетей» СТУ 115.015-2003.
6. «Нормы годности программных средств подготовки персонала энергетики» – СО 153-34.0-12.305-99.
7. ГОСТ Р ИСО 9127-94. Системы обработки информации. Документация пользователя и информация на упаковке для потребительских программных пакетов.
8. Певнева Н. Ю. Комплексный компьютерный тренажер для оперативного персонала энергоблока мощностью 800 МВт Пермской ГРЭС / Н. Ю. Певнева, В. Н. Писков, А. Н. Зенков // Теплоэнергетика. № 7, 2007. С. 31–35.
9. Тренажер для подготовки персонала тепловых сетей / В. Ф. Очков, С. В. Мищеряков, К. А. Орлов [и др.] // Энергосбережение и водоподготовка. № 1(45), 2007. С. 51–53.
10. Комплексные анализаторы процессов функционирования электрооборудования электростанций / В. А. Старшинов, А. И. Пойдо, А. С. Рубашкин, В. А. Рубашкин // Электрические станции. № 4, 2005. С. 66–73.
11. Александров А. А. Система уравнений IAPWS-IF97 для вычисления термодинамических свойств воды и водяного пара в промышленных расчетах. Ч. 1. Основные уравнения // Теплоэнергетика. № 9, 1998. С. 69–77.
12. Александров А. А. Система уравнений IAPWS-IF97 для вычисления термодинамических свойств воды и водяного пара в промышленных расчетах. Ч. 2. Дополнительные уравнения // Теплоэнергетика. № 10, 1998. С. 64–72.
13. Александров А. А. Система уравнений IAPWS-IF97 для вычисления термодинамических свойств воды и водяного пара в промышленных расчетах. Ч. 3. Оценка точности величин. Сравнение с IFC-67 // Теплоэнергетика. № 1, 1999. С. 67–70.
14. Левинштейн М. Л. Операционное исчисление в задачах.– 2-е изд., доп.– Л.: Энергия, 1972.

ОБРАЗОВАНИЕ

Bibliography:

1. Order of the Ministry of Energy of the Russian Federation No. 796 dated 22.09.2020 «On approval of the Rules of work with personnel in organizations of the electric power industry of the Russian Federation» – Text: electronic // Official Internet portal of legal information: [website].– 2021 – URL: https://normativ.kontur.ru/document?moduleId=1&documentId=381455 (date of application: 10.11.2021)
2. Information and analytical information on injuries for the 2nd half of 2020. Text: electronic // Official website of the Ministry of Energy of the Russian Federation.: [website]. URL: https://minenergo.gov.ru/node/272 (date of application: 10.11.2021).
3. Detina, S. A. Reliability of operational personnel in the implementation of operational switches: specialty 05.26.01 «Occupational safety (by industry)»: abstract of the dissertation for the degree of Candidate of Technical Sciences / Detina Svetlana Aleksandrovna.– Chelyabinsk, 2021.– 22 p.
4. Magid S. I., Zagretdinov I. Sh., Mishcheryakov S. V., Arkhipova E. N., Samoilov V. L. Rationing of digital technologies of simulator systems as a way to ensure the reliability of service conditions for electric power facilities (part 1). Reliability and safety of energy. 2019;12(3):177–189. https://doi.org/10.24223/1999-5555-2019-12-3-177-189
5. Technical conditions for certification of application software simulators for thermal power plants and networks» STU 115.015-2003.
6. «Shelf life of software for training energy personnel» – FROM 153-34.0-12.305-99.
7. GOST R ISO 9127-94. Information processing systems. User documentation and packaging information for consumer software packages.
8. Pevneva, N. Y. Complex computer simulator for the operational personnel of the 800 MW Perm GRES power unit / N. Y. Pevneva, V. N. Piskov, A. N. Zenkov // Thermal power engineering.– 2007.– No. 7.– pp. 31–35.
9. Simulator for the training of personnel of heating networks / V. F. Glasses, S. V. Mishcheryakov, K. A. Orlov [et al.] // Energy saving and water treatment.– 2007.– № 1(45).– Pp. 51–53.
10. Complex analyzers of processes of functioning of electrical equipment of power plants / V. A. Starshinov, A. I. Poido, A. S. Rubashkin, V. A. Rubashkin // Electric stations.– 2005.– No. 4.– pp. 66–73.
11. Alexandrov A. A. System of equations IAPWS-IF97 for calculating thermodynamic properties of water and water vapor in industrial calculations. Part 1. Basic equations // Thermal power engineering. 1998. No. 9. pp. 69–77.
12. Alexandrov A. A. System of equations IAPWS-IF97 for calculating the thermodynamic properties of water and water vapor in industrial calculations. Part 2. Additional equations // Thermal power engineering. 1998. No. 10. pp. 64–72.
13. Alexandrov A. A. The system of equations IAPWS-IF97 for calculating the thermodynamic properties of water and water vapor in industrial calculations. Part 3. Estimation of the accuracy of quantities. Comparison with IFC-67 // Thermal power engineering. 1999. No. 1. pp.67–70.
14. Levinstein M. L. Operational calculus in problems.– 2nd ed., supplement – L.: Energiya, 1972.

УДК 004:37.018.4
DOI 10.52815/0204-3653_2022_03187_58
EDN: BHTJLI



Источник: redcharlie / unsplash.com

Цебренко Константин
Директор Института информационных технологий и инноваций, доцент кафедры Математики и вычислительной техники, к. т. н., Негосударственное аккредитованное некоммерческое частное образовательное учреждение высшего образования «Академия маркетинга и социально-информационных технологий – ИМСИТ» (г. Краснодар), НАН ЧОУ ВО Академия ИМСИТ.
E-mail: tsebrenko@imsit.ru

Фролов Руслан
Доцент кафедры бухгалтерского учета и анализа, к. т. н., ФГБОУ ВО «Российский экономический университет им. Г. В. Плеханова» (Краснодарский филиал)
E-mail: docent-1976@mail.ru

РАЗРАБОТКА ОПТИМАЛЬНОЙ СТРУКТУРЫ ИНТЕГРИРОВАННОЙ ИНФОРМАЦИОННО-ОБРАЗОВАТЕЛЬНОЙ СРЕДЫ

Аннотация. В статье рассмотрены актуальные на текущий момент задачи разработки оптимальной структуры информационно-обучающей среды в образовательных организациях с учетом последних требований к организации обучения с применением дистанционных технологий. В основу поиска наиболее удачной структуры такой образовательной среды авторами положены несколько требований. Во-первых, максимальная интеграция различных приложений, обеспечивающих учебный процесс в электронной информационной образовательной среде (ЭИОС). Во-вторых, возможность удаленного онлайн-доступа в круглосуточном режиме ко всем образовательным ресурсам, возможность простой и удобной аутентификации и верификации пользователей в ЭОИС. В результате исследования предложен один из вариантов построения интегрированной образовательной среды с учетом изложенных требований.

Ключевые слова: *информационные технологии, информационная среда, образование, проектирование информационных систем.*

В настоящее время система образования в России качественно и организационно трансформируется на разных уровнях в силу ускоренной цифровизации всех сторон жизни современного общества [1]. Переход на цифровые платформы в образовательном процессе заявлен как один из приоритетов федеральной программы «Цифровая экономика Российской Федерации» [2], реализуемой до 2024 г. Вследствие этого идет интенсивное развитие как online образовательных проектов, так и массовое внедрение локальных информационно-образовательных систем в образовательных организациях. Данные тенденции затрагивают практически все уровни и сферы образовательной деятельности: среднюю школу, среднее профессиональное образование, высшую школу и дополнительное профобразование.

Можно утверждать, что в настоящее время в России в целом сформировался рынок дистанционных online образовательных платформ. Практически на всех уровнях образования созданы сетевые образовательные порталы для организации контролируемого дистанционного обучения. Среди наиболее популярных для уровня средней школы можно отметить ресурс uchi.ru – детский образовательный портал для интерактивного обучения при помощи игровых заданий и задач [3]. Данный ресурс охватывает большую часть предметов школьной программы, легко интегрируется с текущими учебными программами средней школы и позволяет отслеживать статистику успеваемости, как отдельных учеников, так и классов, параллелей и т. д. В период ограничительных мер 2020 г., вызванных распространением коронавирусной инфекции, этот портал стал поистине «спасительной соломинкой» для системы начального и среднего образования, предотвратив полную остановку учебного процесса, переведя его в режим онлайн. Разработчики подтверждают полное соответствие содержания заданий требованиям ФГОС. При этом ресурс не заменяет, а дополняет текущую образовательную программу, так как не предполагается его дальнейшая интеграция в школьные локальные образовательные среды, например, в систему «электронный дневник». Также заслуживает внимания ресурс, направленный на уровень высшего образования – Интернет-университет intuit.ru [4]. Данная платформа предлагает организацию профессиональной переподготовки и повышение квалификации в области computer science с использованием дистанционных форматов обучения. При этом для слушателей создан удобный интерактивный формат работы с курсами.

При всех достоинствах дистанционных онлайн-платформ, они обладают и серьезными недостатками, сдерживающими процессы замены ими традиционных форм образования

При всех достоинствах дистанционных онлайн-платформ, особенно ярко проявившихся во время

карантинных мер, они обладают рядом серьезных недостатков, сдерживающих их дальнейшее распространение в направлении замены традиционных образовательных форматов. Среди них особо следует отметить сложность верификации человека, реально выполняющего задания [5]. Данная проблема в случае отсутствия видеоконтроля при выполнении заданий и доступе в систему только по логину и паролю, может привести к подлогу при выполнении заданий, когда слушатель онлайн-курса привлекает для выполнения заданий более квалифицированного помощника. Таким образом, использование дистанционных форматов возможно только при грамотном их сочетании с традиционными методами обучения.

На текущий момент нет конкретных предложений по выработке оптимальной структуры такой информационно-образовательной среды вуза, которая бы обеспечивала интеграцию системы управления учебным процессом с системой online-обучения и работы в ЭИОС вуза, включая возможность текущего контроля успеваемости и итоговой аттестации. Помимо требований образовательных стандартов [6], необходимо учесть разнообразные задачи, решаемые информационной системой в образовательной организации. В первую очередь, задачи организации и управления учебным процессом: составление расписаний, учет нагрузки преподавателей, формирование ведомостей и ряд других задач. Во вторую очередь непосредственно электронно-образовательная среда, которая включает в себя информационные ресурсы в виде учебных заданий, методические материалы, систему текущего контроля усвоения учебного материала и итоговой аттестации. Все это разнообразие задач требует инновационных подходов к проектированию структуры информационно-образовательной среды, отвечающей конкретной специфике отдельно взятой образовательной организации. Таким образом, задача разработки оптимальной структуры подобной информационно-образовательной среды представляется достаточно актуальной.

В ряде работ [7], [8] отмечено, что «в ходе проектирования информационной системы

Студенты на занятиях
Источник: Dom Fou / unsplash.com

информационно-образовательной среды целесообразно использовать модельно-ориентированный подход». Предполагается, что «электронная информационно-образовательная среда организации высшего образования (ЭИОС) должна предоставить доступ к учебно-методическим материалам дисциплин (модулей), практик, электронным информационным ресурсам и учебным изданиям, обеспечить формирование электронного портфолио обучающегося, в том числе сохранение работ и оценок за эти работы, а также фиксацию хода образовательного процесса». Очевидно, что для решения этого спектра задач, стоящих перед ЭОИС, необходимо наличие четкой структуры, оптимизируемой по ряду параметров. В этом случае на первый план выходят задачи интеграции системы по нескольким структурным направлениям:

1. Оценка преподавателем в ЭИОС текущей и итоговой успеваемости и фиксация результата обучения в модуле деканата с ведением электронных журналов и ведомостей.
2. Консолидация результатов обучения студента и его внеаудиторной деятельности (участие в конференциях, олимпиадах, спортивных соревнованиях) в единое электронное портфолио студента с возможным последующим выходом на потенциального работодателя.
3. Увязка в единый модуль нагрузки преподавателей, расписания занятий с возможностью онлайн-запроса текущего состояния расписания, графиков учебного процесса со стороны всех заинтересованных лиц.
4. Наличие круглосуточно работающего онлайн-модуля для дистанционного выполнения и контроля текущих заданий.

Такие задачи частично решаются на данный момент в Краснодарском филиале ФГБОУ ВО «РЭУ им. Г. В. Плеханова» путем интеграции ЭОИС на базе системы Moodle с системой управления образовательным процессом «Магеллан» (рис. 1).

При поступлении студент получает персональный логин и пароль для входа в данную систему, который является единым для всех модулей, подключенных к личному кабинету. Такие же личные кабинеты создают преподаватели, сотрудники деканата, лица, отвечающие за организацию учебного процесса и т. д. В этом случае дистанционное взаимодействие становится многоканальным: студент заходит на официальный сайт университета и, выполнив вход, может выйти на контакт с преподавателем в процессе обучения по e-mail, во внутреннем чате системы, по видеосвязи. Такая связь является двусторонней, т. е. студент может быть также оперативно проинформирован преподавателем, деканатом и сотрудниками кафедр. Данные подходы особенно актуальны для студентов заочной формы обучения на современном этапе борьбы с распространением коронавирусной инфекции.

Рис. 1. Окно входа в информационно-образовательную среду онлайн, интегрированную с системой управления учебным процессом «Магеллан»

Похожая система используется в образовательной организации НАН ЧОУ ВО «Академия ИМСИТ». Электронное обучение и дистанционные образовательные технологии реализуются в электронной образовательной среде на базе eLMS Moodle в связке с кор-

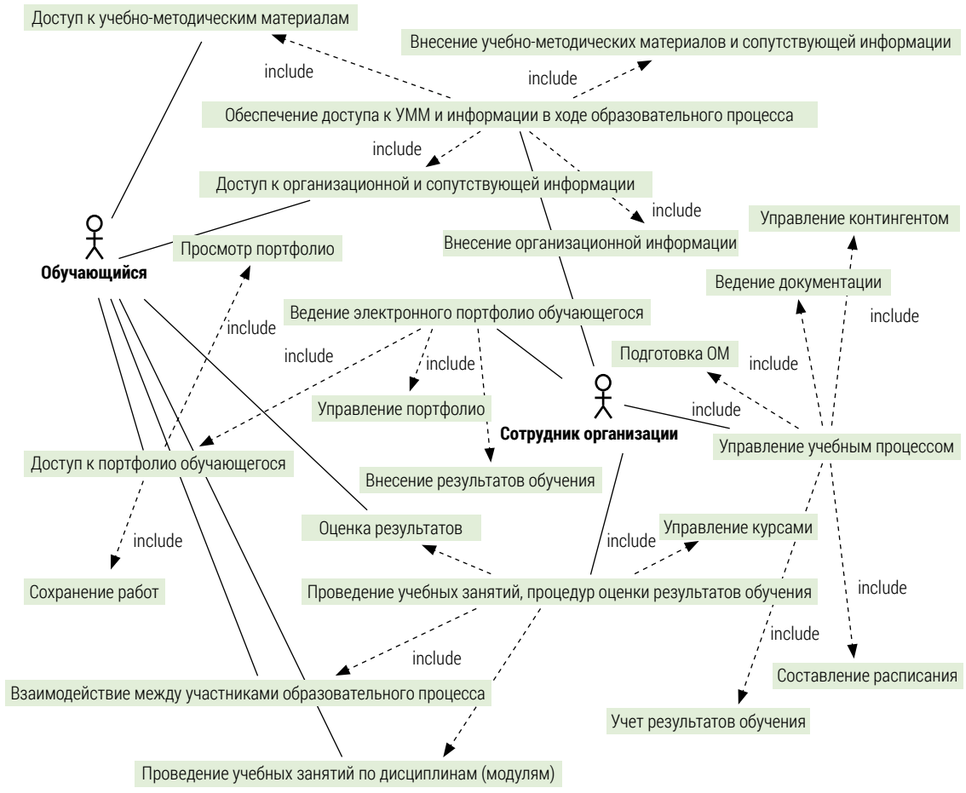


Рис. 2. Обобщенная диаграмма вариантов использования существующей ЭИОС

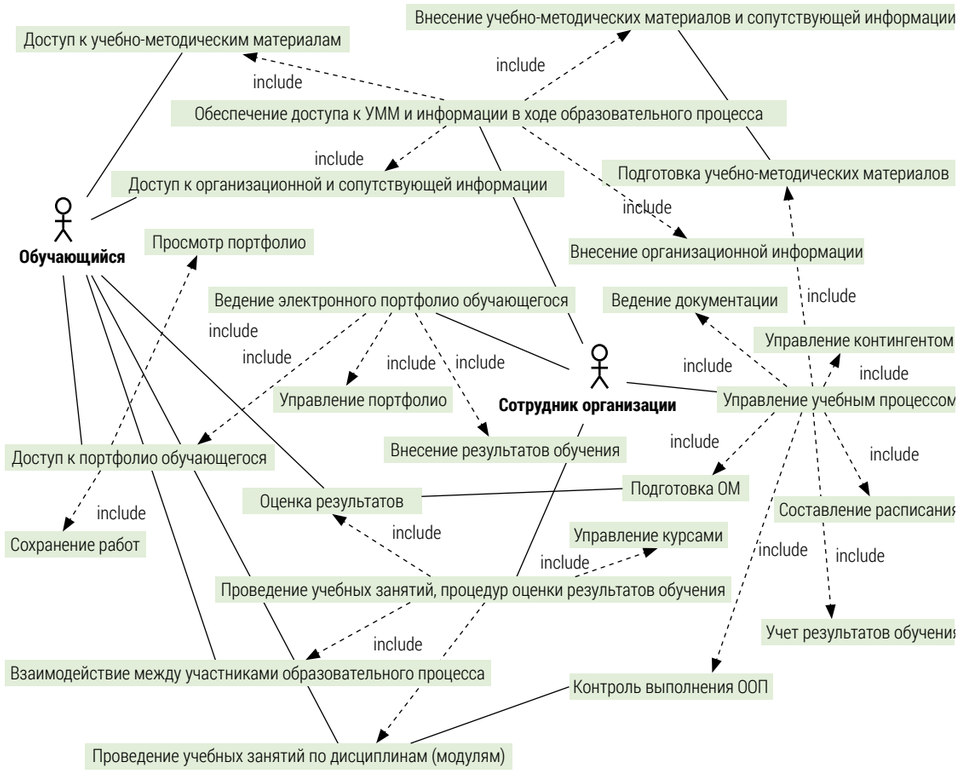
поративной платформой Microsoft Teams. Доступ к учебно-методическим материалам дисциплин (модулей), практик, электронным информационным ресурсам и учебным изданиям, а также формирование электронного портфолио обучающегося, в том числе сохранение работ и оценок за эти работы, фиксация хода образовательного процесса осуществляются средствами электронной образовательной среды Moodle, электронных библиотечных систем и официального сайта академии. Автоматизированная система управления образовательной организацией построена на платформе «Парус-ВУЗ». В связи с отсутствием интеграции «Парус-ВУЗ» с eLMS moodle данные в электронную информационно-образовательную среду (ЭИОС) приходится переносить в ручном режиме. Это создает дополнительную нагрузку на учебные подразделения и управленческий аппарат.

Многие образовательные организации сталкиваются с подобной проблемой. Существующие продукты либо не обеспечивают комплексных решений, охватывающих все области деятельности организации, либо требуют значительных ресурсов для внедрения и эксплуатации. Исходя из этого, необходимо разработать такую модель оптимальной структуры взаимодействия внутри подобных систем, которая бы полностью отражала элементы и связи для дальнейшего развития внедряемых в различных учебных заведениях информационно-образовательных сред.

Воспользуемся диаграммой Use Case для описания типичной структуры взаимодействия в электронной образовательной среде организаций (рис. 2). Как видно из модели, контроль выполнения основной образовательной программы не удалось автоматизировать средствами ЭИОС, так как планирование учебного процесса находится в одной среде, а реализация учебного процесса и оценка результатов в другой. По той же причине не удалось реализовать контроль предоставления и утверждения учебно-методических материалов (УММ).

Решить данную проблему можно путем внедрения модуля обмена данными между eLMS и автоматизированной системой управления образовательной организацией. В этом случае можно организовать только

Рис. 3. Диаграмма вариантов использования ЭИОС



периодический перенос данных, так как информация хранится в разных базах данных. Некоторые разработчики предлагают расширения для своих разработок, но как правило они либо имеют ограниченный функционал, либо требуют значительных затрат на внедрение при невысокой степени интеграции.

Для реализации предложенного решения необходимо реализовать информационную систему с единым информационным пространством. Для варианта реализации системы «с нуля» более предпочтительным является использование web-технологий при разработке среды.

На рис. 3 показана Use Case модель ЭИОС, лишенная указанных выше недостатков. Здесь среда интегрирована с системой автоматизированного управления образовательной организацией и нет необходимости многократно вводить одни и те же данные, либо осуществлять периодическую синхронизацию информации. Предусмотрена цифровизация процесса подготовки УММ по образовательным программам, что позволит исключить ошибки при заполнении документов и обеспечить четкое выполнение планов дисциплин (модулей) и практик. Автоматизирован контроль выполнения программы в том числе за счет анализа «цифрового следа» обучающихся в ЭИОС.

В ходе моделирования разработаны диаграммы последовательностей для показанных вариантов использования, построены диаграммы классов. Дальнейшее развитие модели предполагает использование результатов обследования конкретной организации. Предложенная модель позволяет максимально автоматизировать процессы управления обучением и сопровождения учебного процесса, причем независимо от характеристик программ обучения, что актуально для организаций, совмещающих процесс подготовки обучающихся по направлениям и специальностям высшего образования с другими уровнями подготовки. Адаптация модели под нужды образовательной организации позволит снизить риски проекта и положить основу формирования единого цифрового пространства.

Онлайн-обучение
Источник: Lisha Riabinina / unsplash.com

THE PROBLEMS OF DESIGNING THE OPTIMAL STRUCTURE OF THE INTEGRATED INFORMATION EDUCATIONAL ENVIROMENT

Tsebrenko Konstantin, PhD in Technical Sciences, director of the Institute of Information Technology and Innovation, Associate Professor of the Department of Mathematics and Computer Science, Nonstate Accredited Noncommercial Private Educational Establishment of Higher Education «The Academy of Marketing and Social information Technologies - IMSIT» (Krasnodar), (NAN PEE HE The Academy IMSIT).
E-mail: tsebrenko@imsit.ru

Frolov Ruslan, PhD in Technical Sciences
Krasnodar branch of G.V. Plekhanov Russian University of Economics
Associate Professor, Department of Accounting and Analysis.
E-mail: docent-1976@mail.ru

Abstract. The article discusses the current tasks of developing the optimal structure of the information and training environment in educational organizations, taking into account the latest requirements for the organization of training using distance technologies. The search for the most successful structure of such an educational environment is based on several requirements: the maximum integration of various applications that ensure the educational process in the electronic information educational environment, the possibility of remote online access around the clock to all educational resources, the possibility of simple and convenient verification and user authentication in information educational environment. As a result of the research, one of the options for constructing an integrated educational environment was proposed, taking into account the stated requirements.
Keywords: information technology, information environment, education, information systems design.

Библиографический список:

1. Фролов Р. Н., Цебренко К. Н., Салий В. В. Информатизация современного российского общества: социально-экономические и правовые аспекты // Информационные ресурсы России. № 4 (176), 2020. С. 26–29.
2. Программа «Цифровая экономика Российской Федерации». [Электронный ресурс]. – Режим доступа: URL: static.government.ru/media/files/ 9gFM4FHj4PsB79I5v7yLVuPgu4bvR7M0.pdf
3. Интерактивная образовательная онлайн-платформа. Режим доступа: URL: https://uchi.ru/
4. Национальный открытый университет ИНТУИТ. Режим доступа: URL: intuit.ru
5. Фролов Р. Н., Дудченко А. В., Колкарева И. Н. Актуальные проблемы стандартизации требований к верификации личности пользователя в сети при организации дистанционного обучения // Информационно-экономические аспекты стандартизации и технического регулирования. № 2 (54), 2020. С. 65–71.
6. Цебренко К. Н. Моделирование электронной среды образовательной организации в соответствии с требованиями федеральных стандартов // Информационные ресурсы России. № 4 (164), 2018. С. 38–44.
7. Абросимов А. Г., Печерская Э. П., Погорелова Е. В. Методология и инструментарий проектирования электронной информационно-образовательной среды в системе профессионального экономического образования // Вопросы современной науки и практики. Университет им. В. И. Вернадского. № 2, 2008. С. 51–58.
8. Саакян И. А. Моделирование электронной информационно-образовательной среды образовательной организации // Информационные ресурсы России. № 5 (171), 2019. С. 25–29.

Bibliography:

1. Frolov R.N., Tsebrenko K.N., Saliy V.V. Informatization of modern Russian society: socio-economic and legal aspects // Information resources of Russia. – 2020. №4 (176). – Pp. 26-29.
2. The program «Digital Economy of the Russian Federation». [electronic resource]. – Access mode: static.government.ru/media/files / 9gFM4FHj4PsB79I5v7yLVuPgu4bvR7M0.pdf
3. Interactive online educational platform. Access mode: URL: https://uchi.ru/
4. National Open University INTUIT. Access mode: URL: intuit.ru
5. Frolov R.N., Dudchenko A.V., Kolkareva I.N. Actual problems of standardization of requirements for verification of the user's identity in the network when organizing distance learning // Information and economic aspects of standardization and technical regulation. – 2020. № 2 (54). – Pp. 65-71.
6. Tsebrenko, K. N. Modeling of the electronic environment of an educational organization in accordance with the requirements of federal standards // Information resources of Russia. – 2018. – № 4(164). – Pp. 38-44.
7. Abrosimov A.G., Pecherskaya E.P., Pogorelova E.V. Methodology and tools for designing electronic information and educational environment in the system of professional economic education // Issues of modern science and practice. V.I. Vernadsky University. – 2008. No. 2. – pp. 51-58.
8. Sahakyan, I.A. Modeling of the electronic information and educational environment of an educational organization// Information Resources of Russia. – 2019. №5 (171). – Pp. 25-29.

УДК 37.018.43
DOI 10.52815/0204-3653_2022_03187_66
EDN: EENKXM

Источник: neyron1566 / Depositphotos.com

ЦИФРОВИЗАЦИЯ ВЗАИМООТНОШЕНИЙ УЧАСТНИКОВ ОБРАЗОВАТЕЛЬНОГО ПРОЦЕССА ВУЗА

Грибков Дмитрий
Доцент, к. п. н., заведующий кафедрой информатики и документоведения, ФГБОУ ВО «Орловский государственный институт культуры».
E-mail: bibliotekar2005@mail.ru

Манько Светлана
Старший преподаватель кафедры информатики и документоведения, ФГБОУ ВО «Орловский государственный институт культуры».
E-mail: svetik_comp@mail.ru

Аннотация. Целью данной статьи является определение проблем для участников образовательного процесса в режиме удаленной работы. Перечислены некоторые online-технологии и сервисы, которые позволяют организовать процесс работы в период самоизоляции и ограничений. Обозначен ряд основных причин, которые сдерживают процесс внедрения информационных технологий в реализации дистанционного обучения в Орловском государственном институте культуры.

Ключевые слова: *образовательное пространство, вузовские библиотеки, удаленная работа, дистанционный формат, цифровизация.*

Многие вузы испытывают трудности с внедрением новых технологий

Цифровые сервисы сегодня являются неотъемлемой частью человека, а дистанционное образование идет наравне с традиционным. Все это – благодаря реализации национального проекта «Цифровая экономика» [11].

В сфере образования совершенствуются и развиваются дистанционные технологии различного назначения: ClassDojo, Edmodo, Zoom, Microsoft Teams, Google Classroom, Schoology, Skooler, Funzi, KaiOS, Kolibri, Canvas Network и т. д. [10]. Эти дистанционные образовательные технологии (далее ДОТ) применяются для проведения аудиторных занятий и различных видов практик, смешанного и перевёрнутого обучения, контроля и систематизации знаний.

Удовлетворяя меняющимся требованиям системы образования, поставщики IT-решений обеспечивают:

- новые конструкции, основанные на простоте использования средств управления хостом быстрого подключения к совещаниям и интеграции с системами конференц-залов;
- параметры безопасности, которые исключают возможность участия незваных гостей в собрании или обмене нежелательным контентом;
- смешанная асинхронная (обмен сообщениями, содержимым, планирование, задачи, записи) и синхронная (голос, аудио, совместное использование экрана) совместная работа в постоянных комнатах или рабочих пространствах;
- равные возможности для различных типов конечных точек доступа, от кодеков групповой видеосистемы до настольных компьютеров, ноутбуков (через браузеры или клиенты), смартфонов, планшетов и т. д.;
- транскрипция и языковой перевод для проведения вебинаров, общих собраний и конференций;
- искусственный интеллект – технологии, улучшающие возможности конференц-зала благодаря автоматизации процессов присоединения к собранию и обмена контентом;
- оптимизация доставки в корпоративные сети – например, посредством поддержки безопасности через виртуальную частную сеть (VPN) или широковещательной передачи через сеть доставки контента (CDN) [2].

Очевидно, что одним из приоритетных направлений государственной политики Российской Федерации является переход к цифровой экономике [9], формированию информационного общества [6], в реализации которых повышается значимость процесса цифровизации всех сфер жизнедеятельности человека, в том числе образования и библиотечно-информационная деятельность.

Студенты в аудитории
Источник: DragonImages / Depositphotos.com

Таким образом, развитие электронного обучения – это не только вынужденная ответная мера международных организаций, Министерства науки и высшего образования РФ. E-learning и дистанционные формы обучения потенциально способны оказать существенную помощь в повышении качества образования, сетевого профессионального взаимодействия, реализации методологических изменений. Дистанционные технологии в инициативах ЮНЕСКО и концепции «мира без границ» должны стать основой создания инклюзивных обществ, опираться на самые современные программные средства.

В то же время, очевидно, что многие вузы испытывали и испытывают трудности с внедрением новых технологий в образовательную среду. В этих условиях необходимо обеспечить распространение дидактических принципов и стандартов, которые будут приняты не только на административном уровне, но и самими педагогами, студентами вуза. Важным фактором, способствующим принятию e-learning и организации образовательного процесса обучающихся средствами ДОТ, является их восприятие как относительного преимущества. Другими словами, и студенты, и преподаватели должны понимать, что применяемая инновация лучше, чем тот инструмент или практика, которым она пришла на смену. Поэтому важно проводить исследования и оценки, помогающие фиксировать результаты аудиторной/внеаудиторной работы с ДОТ, организации профессионального сетевого взаимодействия, различных видов контактной работы и практик (проектной, учебной, научной, преддипломной и т. д.).

В сфере образования информационные технологии, по мнению авторов [3], открывают пути для новых педагогических подходов, в рамках которых обучающиеся, как ожидается, будут играть более активную роль, чем раньше, тем самым концентрируя внимание на важнейших вопросах образовательного процесса в электронной среде.

Для участия и максимального использования возможностей и преимуществ, предлагаемых этими технологиями, необходима цифровая компетентность, которая является результатом электронной трансформации [1]. В данном документе достаточно детально рассмотрены необходимые компетенции (грамотность в области информации и данных, коммуникация и сотрудничество, создание цифрового контента, безопасность, решение задач), которые сегодня необходимы как студентам, так и преподавателям в рамках процесса глобализации и трансформации высшего образования.

В связи с беспрецедентным ростом интернета и последующими преобразованиями в образовательной среде необходимо понять, как участники учебного процесса принимают и используют цифровые технологии. Для решения данной задачи было проведено анкетирование среди студентов Орловского государственного института культуры. Основные результаты эксперимента представлены в статье «Основные проблемы студентов в процессе перехода на дистанционное обучение: на примере Орловского государственного института культуры [5].

Проведенный анализ позволяет выделить ряд основных причин, которые сдерживают процесс внедрения информационных технологий в реализации дистанционного обучения:

– высокая стоимость разработки, внедрения и поддержки систем дистанционного обучения;
– отсутствие необходимой технической поддержки для внедрения дистанционного обучения в образовательный процесс;
– отсутствие квалифицированных преподавателей, специально обученных для удаленной работы;
– отсутствие полноценных электронных дистанционных курсов в вузах;
– низкое качество дистанционного обучения.

Дистанционный формат организации работы вузов продолжает совершенствоваться. Поэтому важно уделять внимание повышению квалификации сотрудников для реализации федерального закона «Об образовании в Российской Федерации» [8], образовательных стандартов и реалиям времени. При этом подавляющее большинство интернет-решений ориентируются не на переосмысление процесса обучения и взаимодействия его участников, а на создание просто удобных инструментов для использования в рамках существующей системы образования.

Другими немаловажными участниками образовательного процесса выступают библиотекари. Их роль в данном взаимодействии достаточно велика, так как основные информационные образовательные ресурсы аккумулируются в фондах и электронном пространстве вуза. Последние годы сотрудники вузовских библиотек посвятили тому, чтобы, сохраняя традиционные формы общения с читателем, органично ввести новые. Развитие современной библиотеки вуза характеризуется возрастанием темпов изменений, происходящих в информационном пространстве, системе образования и научной коммуникации.

В связи с этим каждая образовательная организация формирует собственную электронную информационно-образовательную среду для создания перспективной системы образования и обеспечивает подготовку конкурентоспособных специалистов в новых условиях. Функционирование электронной

Студенты
Источник: DragonImages / Depositphotos.com

Городская библиотека Перта
Источник: Harry Cunningham / unsplash.com

информационно-образовательной среды обеспечивается соответствующими средствами информационно-коммуникационных технологий и квалификацией работников, ее использующих и поддерживающих [7].

Ответственность за формирование электронной информационно-образовательной среды возлагается в значительной степени на вузовскую библиотеку как основного держателя документных фондов, поэтому уровень электронной среды и рейтинг вуза определяется качеством ресурсной составляющей библиотеки.

Цифровая эпоха и новые информационные технологии, определяющие индивидуальный подход в образовательной деятельности для каждого обучающегося в вузе, существенно изменяют роль вузовских библиотек.

Дистанционный формат организации работы вузовских библиотек продолжает совершенствоваться. Поэтому важно уделять внимание повышению квалификации сотрудников для реализации образовательных стандартов 3++ поколения и реалиям времени. Один из способов продвинуться в этом направлении – кооперироваться с другими библиотеками (областными) и прочими учреждениями культуры – музеями, архивами и др.

В качестве решения проблемы интеграции электронного образовательного контента может стать проект межвузовской электронной библиотеки вузов культуры [4]. Библиотека такого уровня, позволит участникам образовательного процесса повысить оперативность взаимодействия и качество образовательных ресурсов. При этом, затраты на оплату электронных библиотечных систем значительно сократятся. Результатом реализации данного проекта может стать 100 % книгообеспеченность всех направлений и уровней подготовки институтов культуры. Профессорско-преподавательский состав получит актуальные электронные учебные материалы своих коллег из вузов-партнеров, вступивших в корпорацию, а студенты – возможность работать с научными, учебно-методическими и практическими изданиями в online-режиме.

Российская государственная
библиотека им. Ленина
Источник: KKulikov / Depositphotos.com

В настоящий момент в электронной информационно-образовательной среде Орловского государственного института культуры реализуются алгоритмы и процедуры, которые направлены на то, чтобы поддерживать:

- возможность доступа к учебным планам, рабочим программам дисциплин (модулей), практик, к изданиям ЭБС и электронным образовательным ресурсам;
- возможность проведения всех видов занятий, процедур оценки результатов обучения, реализация которых предусмотрена с применением ДОТ;
- возможность формирования электронного портфолио обучающегося;
- возможность взаимодействия между участниками образовательного процесса, в том числе, синхронное и (или) асинхронное взаимодействие посредством сети Интернет.

В качестве трудностей, которые осложняют применение ДОТ, можно выделить следующее: зависимость от разработок зарубежных компаний, высокая стоимость мобильных платформ и приложений, технические сбои оборудования в труднодоступных районах России, удаленных местах; координация деятельности сотрудников вуза, привыкших работать по традиционным методикам, и самих студентов.

Итак, описанная система действий по применению ДОТ в обучении студентов Орловского государственного института культуры позволяет:

- сформировать востребованные цифровые навыки (составление автоматических запросов, поиск данных, анализ информации и оценка её качества, организация и хранение библиотечных фондов, соблюдение этических норм при виртуальном взаимодействии и т. п.);
- получить опыт проектной научно-исследовательской и учебно-познавательной деятельности;
- смоделировать выполнение трудовых функций;
- применить теоретическую информацию из библиотечного дела при организации культурных мероприятий, развлекательных событий.

DIGITALIZATION OF RELATIONSHIPS BETWEEN PARTICIPANTS IN THE EDUCATIONAL PROCESS OF THE UNIVERSITY

Gribkov Dmitry, candidate of pedagogical sciences, associate professor, head of the department of informatics and documentary science, Oryol State Institute of Culture.
E-mail: bibliotekar2005@mail.ru

Manko Svetlana, senior lecturer at the Department of Informatics and Documentary Science, Oryol State Institute of Culture.
E-mail: svetik_comp@mail.ru

Abstract. The purpose of this article is to identify problems for participants in the educational process in remote operation mode. Listed are some on-line technologies and services that allow you to organize the work process during a period of self-isolation and restrictions. A number of main reasons are identified that hinder the process of introducing information technologies in the implementation of distance learning at the Oryol State Institute of Culture.
Keywords: educational space, university libraries, remote work, remote format, digitalization.

Библиографический список:

1. DigComp 2.0: The Digital Competence Framework for Citizens. Update Phase 1: the Conceptual Reference Model: [Electronic text]. – URL: https://ec.europa.eu/jrc/en/publication/eur-scientific-and-technical-research-reports/digcomp-20-digital-competence-framework-citizens-update-phase-1-conceptual-reference-model – (accessed 19.10.2021.) – Text: direct.
2. Magic Quadrant for Meeting Solutions: [Electronic text] – URL: https://www.gartner.com/doc/reprints?id=1-2468658S&ct=200917&st=sb – (accessed 29.11.2021.) – Text: electronic.
3. Tulinayo F. Digital technologies in resource constrained higher institutions of learning: a study on students' acceptance and usability / Tulinayo.F., Ssentume, P. & Najjuma, R.: [Electronic text] – Int J Educ Technol High Educ 15, 36 (2018).– URL: https://doi.org/10.1186/s41239-018-0117-y.– (accessed 19.11.2021.) – Text: direct.
4. Грибков Д. Н. Межвузовская электронная библиотека как механизм управления процессом книгообеспеченности для институтов культуры // Вестник Московского государственного университета культуры и искусств. № 1 (69), 2016. С. 206–210.
5. Грибков Д. Н. Основные проблемы студентов в процессе перехода на дистанционное обучение: на примере Орловского государственного института культуры / Грибков Д. Н., Махонин Е. В. // Ученые записки Орловского государственного университета. № 4 (89), 2020. С. 161–164.– Текст: непосредственный.
6. О стратегии развития информационного общества в РФ на 2017–2030 годы. Указ Президента РФ от 09.05.2017 г. № 203.– URL: https://www.garant.ru/products/ipo/prime/doc/71570570/ (дата обращения: 15.10.2021).– Текст: электронный.
7. О федеральных государственных образовательных стандартах: Письмо Министерства образования и науки РФ от 20 августа 2014 г. № АК-2612/05 [Электронный ресурс]. – URL: http://www.garant.ru/products/ipo/prime/doc/70631470/#review (дата обращения: 01.09.2021).– Текст: электронный.
8. Об образовании в Российской Федерации: Федеральный закон от 29.12.2012 г. № 273-ФЗ (ред. от 31.07.2020): [Электронный ресурс].– URL: http://base.consultant.ru/cons/cgi/online.cgi?req=doc; base=LAW; n=173432; fld=134; from=148547-9; rnd=0.7614195423666388 (дата обращения: 19.11.2021).– Текст: электронный.
9. Паспорт национальной программы «Цифровая экономика Российской Федерации». Утвержден президиумом совета при президенте РФ по стратегическому развитию и приоритетным проектам (протокол от 24.12.2018 г. № 16).– URL: http://static.government.ru/media/files/urKHm0gTPPnzJlaKw3M5cNLo6gczMkPF.pdf (дата обращения: 15.08.2021).– Текст: электронный.
10. Соболева Е. В. Формирование навыков вычислительного мышления при разработке компьютерных игр образовательного назначения / Соболева Е. В., Кириллова Е. П., Ломакин Д. Е., Грибков Д. Н. // Перспективы науки и образования. № 1 (49), 2021. С. 464–477.– Текст: непосредственный.
11. Цифровая экономика РФ: [Текст электронный] – URL: https://digital.gov.ru/ru/activity/directions/858/ (дата обращения 12.12.2021.) – Текст: электронный.

Bibliography:

1. DigComp 2.0: The Digital Competence Framework for Citizens. Update Phase 1: the Conceptual Reference Model: [Electronic text]. – URL: https://ec.europa.eu/jrc/en/publication/eur-scientific-and-technical-research-reports/digcomp-20-digital-competence-framework-citizens-update-phase-1-conceptual-reference-model (accessed 10/19/2021.) – Text: direct.
2. Magic Quadrant for Meeting Solutions: [Electronic text] – URL: https://www.gartner.com/doc/reprints?id=1-2468658S&ct=200917&st=sb (accessed 11/29/2021.) – Text: electronic.
3. Tulinayo F. Digital technologies in resource constrained higher institutions of learning: a study on students' acceptance and usability / Tulinayo.F., Ssentume, P. & Najjuma, R.: [electronic Text] – Int J Educ Technol High Educ 15, 36 (2018).– URL: https://doi.org/10.1186/s41239-018-0117-y.– (accessed 11/19/2021.) – Text: direct.
4. Gribkov D. N. Interuniversity electronic library as a mechanism for managing the process of book supply for cultural institutions / D. N. Gribkov // Bulletin of the Moscow State University of Culture and Arts. 2016. No. 1 (69). P. 206–210.
5. Gribkov D. N. The main problems of students in the process of transition to distance learning: on the example of the Oryol State Institute of Culture / Gribkov D. N., Makhonin E. V. // Scientific notes of the Oryol State University. 2020. No. 4 (89). FROM. 161–164.– Text: direct.
6. On the Strategy for the Development of the Information Society in the Russian Federation for 2017–2030. Decree of the President of the Russian Federation of May 9, 2017 No. 203.– URL: https://www.garant.ru/products/ipo/prime/doc/71570570/ (date of access: 10/15/2021).– Text: electronic.
7. On federal state educational standards: Letter of the Ministry of Education and Science of the Russian Federation dated August 20, 2014. No. AK-2612/05 [Electronic resource]. – URL: http://www.garant.ru/products/ipo/prime/doc/70631470/#review (date of access: 09/01/2021).– Text: electronic.
8. On education in the Russian Federation: Federal Law of December 29, 2012 No. 273-FZ (as amended on July 31, 2020): [Electronic resource].– URL: http://base.consultant.ru/cons/cgi/online.cgi?req=doc; base=LAW; n=173432; fld=134; from=148547-9; rnd=0.7614195423666388 (date accessed: 11/19/2021).– Text: electronic.
9. Passport of the national program «Digital Economy of the Russian Federation». Approved by the Presidium of the Council under the President of the Russian Federation for Strategic Development and Priority Projects (Minutes No. 16 dated December 24, 2018).– URL: http://static.government.ru/media/files/urKHm0gTPPnzJlaKw3M5cNLo6gczMkPF.pdf (date of access: 08/15/2021).– Text: electronic.
10. Soboleva E. V. Formation of computational thinking skills in the development of educational computer games / Soboleva E. V., Kirillova E. P., Lomakin D. E., Gribkov D. N. // Prospects of science and education. 2021. No. 1 (49). P. 464–477.– Text: immediate.
11. Digital Economy of the Russian Federation: [Electronic text] – URL: https://digital.gov.ru/ru/activity/directions/858/ – (accessed 12.12.2021.) – Text: electronic.

УДК 004.031.4 + 651.83
DOI 10.52815/0204-3653_2022_03187_73
EDN: FMNFIR

Источник: commons.wikimedia.org / Depositphotos.com

СОВЕРШЕНСТВОВАНИЕ РАБОТЫ ЕДИНОГО ПОРТАЛА ГОСУДАРСТВЕННЫХ И МУНИЦИПАЛЬНЫХ АРХИВОВ РФ В ИНТЕРНЕТЕ

Санашкина Мария
Инженер-программист, ФГБОУ ВПО «Военно-космическая академия имени А.Ф. Можайского».
E-mail: 19.masha.63@mail.ru

Свеколкин Николай
Начальник лаборатории ФГБОУ ВПО «Военно-космическая академия имени А.Ф. Можайского».
E-mail: Ins_61@mail.ru

Аннотация. На протяжении столетий поиск и систематизация данных при проведении различных исследований, часто сталкивались с необходимостью удаленной работы с информацией, хранящейся в муниципальных, региональных или столичных архивах. Подобная ситуация была общемировой практикой, начиная с середины XVII века. Для ее решения были предусмотрены возможность работы в читальном зале и процедура оформления платных тематических запросов. Необходимость оформления отдельных запросов в каждый архив, при имеющихся начальных ограничениях, выражающихся в неполноте исходных данных, делали качество такой работы неудовлетворительным. Кроме того, проблемы были обусловлены ограниченными возможностями самих архивов: малое число посадочных мест в читальных залах, необходимость заблаговременной записи для посещения и работы, сезонный характер приема. В Российской Федерации ситуация усугублялась неразвитостью информационно-телекоммуникационных технологий и наступившей после распада СССР сложной экономической обстановкой. Наблюдаемые в Российской Федерации положительные изменения связаны с развитием экономики, высоким уровнем компьютеризации и появлением глобальной сети Интернет. В статье сформулированы предложения по работе единого информационного портала «Архивы России», разработанные по результатам проведения простейшего тестирования.

Ключевые слова: *интернет-ресурс, портал, web-ресурс, каталог, архив, фонд, информационный ресурс.*

ВВЕДЕНИЕ

Перемены в жизни любого общества сопровождаются противоречивостью ощущений – энтузиазмом ожидания от внедрения чего-то нового и эйфорией от сопричастности к этому, а также настороженностью в отношении ожидаемых к получению результатов.

Взятый в России курс на создание информационного общества и экономики готовит нас к главенствованию различных компьютерных, интерактивных и виртуальных технологий в жизни общества. В этой связи актуальными становятся вопросы организации взаимодействия и использования информационных ресурсов в различных сферах деятельности.

Доверие к информационным ресурсам и технологиям современных пользователей определяется многочисленными параметрами их работы: надежностью, трудоемкостью, достоверностью и др.

Возникновение разного рода сбоев в работе информационных ресурсов является чувствительным для любого информационного общества. Появление сбоев и некорректность работы связано в первую очередь с допущенными при проектировании просчетами в логике функционирования, т. е. организационными мероприятиями.

На примере работы с единым информационным интернет-порталом «Архивы России» покажем некорректность его функционирования как источника информации, выявленную при простейшем тестировании. Обозначив, таким образом, направления дальнейшего совершенствования его работы.

Из истории создания интернет-ресурсов отечественных архивов

Создание и функционирование первых отечественных архивов в глобальной сети Интернет широко обсуждались на различных конференциях и круглых столах. Изучался и анализировался иностранный опыт, экономическая целесообразность создания web-ресурсов и возможные перспективы от их внедрения и последующего использования. Разработанные предложения послужили фундаментом сформулированных рекомендаций по вступлению отечественных архивов в сеть Интернет и план работ по предоставлению материалов архивных конференций, исторических источников, исполнению интернет-запросов пользователей.

Первые сайты архивов РФ стали создаваться в начале 2000-х гг. Первым информационно-представительским отечественным архивным порталом стал сайт «Архивы России». Открывшийся в мае 2001 г. под эгидой Федерального архивного агентства России (далее – Росархива) при поддержке Института «Открытое общество» (Фонд Сороса) и Министерства РФ по делам печати, радиовещания и средств массовых коммуникаций. Материалы размещались на серверах Российского государственного архива научно-технической документации (далее – РГАНТД). Первоначально информационный контент размещался в 16 разделах: Архивная отрасль, Архивное законодательство, Федеральные архивы, Региональные архивы, Летопись событий, Архивные справочники, Базы данных, Архивные проекты, Издания и публикации и др. Ресурс содержал данные обо всех федеральных и региональных архивах РФ, информировал об основных событиях в архивном мире, предоставлял возможность изучения нормативно-правовых документов и методических пособий по архивоведению и многое другое [1].

Уже к концу 2014 г. web-ресурсы в сети Интернет имели все федеральные архивы страны [2]. Но услуги по их техническому сопровождению (поддержке) в большинстве случаев были отданы сторонним организациям, при этом информационное наполнение контентом с тех времен и по сей день возложено на штатных сотрудников архивов. Первоначально создание сайта архива регулировалось Федеральным законом от 27.07.2006 г. № 149 «Об информации, информационных технологиях и о защите информации», в котором были прописаны основные определения информации и информационных технологий. Не все его положения были бесспорны. К достоинствам указанного нормативного акта следует отнести системное регулирование отношений, касающихся статуса информационных систем, а также комплекса прав и обязанностей участников (операторов) таких систем. В Федеральном законе от 21.01.2009 г. № 8 «Об обеспечении доступа к информации о деятельности государственных органов и органов местного самоуправления», было дано определение понятия «Официальный сайт государственного органа или органа местного самоуправления», под которое и подпадают сайты всех архивов.

Большое значение в сфере виртуального развития архивного дела оказали Рекомендации по созданию архивного сайта в интернете, разработанные Росархивом в далеком 2001 г. Необходимо отметить, что рекомендации касались проблем информационного контента сайта, организации его создания и поддержки, размещения и продвижения в интернете, разработки концепции и дизайна. При этом совершенно не рассматривали узкоспециализированный пласт технических вопросов, связанных с установкой, подключением и обеспечением защиты информации и собственного серверного оборудования. Кроме того, положения упомянутого норматива приветствовали творческий подход и самостоятельность, подчеркивая, что структура конкретного сайта не обязательно должна была совпадать с представленной в рекомендациях градации информационного наполнения сайта по разделам [3].

Вопросы, связанные с технической составляющей на этапе своего возникновения, при отсутствии достаточного опыта и квалификации, коллективам архивов приходилось решать самостоятельно, что воплощалось в виде не отвечающих страниц, избыточной и не до конца продуманной структуре ресурсов.

Архив
Источник: Ula Kuźma / unsplash.com

Архивы СПБ
Источник: piter-news.net

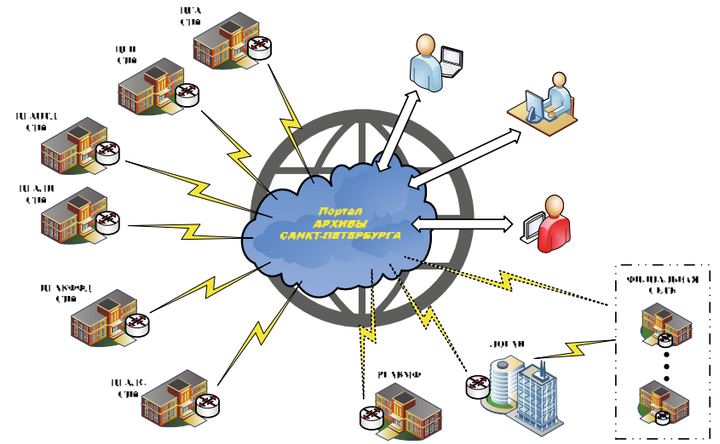
Основные направления развития для информационных ресурсов отечественных архивов [4–8] с тех пор остались прежними:

1) актуализация нормативно-правовой базы по созданию архивных сайтов в сети Интернет, с учетом постоянно меняющейся современной конъюнктуры;
2) продвижение за счет широкого внедрения возможностей социальных сетей и медиа, в виде размещения ссылок на официальном сайте архива и наоборот. Данный шаг ориентирован на привлечение новой аудитории посетителей в архивы и популяризацию архивного дела;
3) активное внедрение и применение современных технологий работы баз данных, по предоставлению и поиску архивных документов на сайте, для ускорения поиска необходимой информации;
4) изучение и внедрение передового опыта зарубежных архивных сайтов в сфере взаимодействия с образовательными учреждениями и учащимися в рамках интернет среды;
5) создание мультиязычных версий сайтов отечественных архивов, для привлечения зарубежной аудитории и международного партнерства;
6) увеличение доходов за счет оплаты пользователями доступа к оцифрованным материалам.

Пример рационального подхода и воплощения

В любом субъекте РФ существует не менее одного архива, занимающегося хранением информации по определенному критерию (период или вид). В качестве примера можно привести опыт реализации регионального масштаба – интернет-портал «Архивы Санкт-Петербурга» [9], предоставляющего возможность поиска информации исключительно по архивным фондам

Рис. 1. Схема взаимодействия ресурсов на портале «Архивы Санкт-Петербурга»



Условные обозначения:

– действующая сеть;

– перспективные подключения;

– информационный обмен;

ЦГА СПб	– Центральный государственный архив Санкт-Петербурга;
ЦГИА СПб	– Центральный государственный исторический архив Санкт-Петербурга;
ЦГАИПД СПб	– Центральный государственный архив историко-политических документов Санкт-Петербурга;
ЦГАНТД СПб	– Центральный государственный архив научно-технической документации Санкт-Петербурга;
ЦГАЛИ СПб	– Центральный государственный архив литературы и искусства Санкт-Петербурга;
ЦГАКФФД СПб	– Центральный государственный архив кинофотофонодокументов Санкт-Петербурга;
ЦГАЛС СПб	– Центральный государственный архив документов по личному составу ликвидированных государственных предприятий, учреждений, организаций Санкт-Петербурга;
РГАВМФ	– Российский государственный архив Военно-Морского Флота;
ЛОГАВ	– Ленинградский областной государственный архив (г. Выборг);
Филиальная сеть	– Архивные отделы администраций муниципальных районов Ленинградской области.

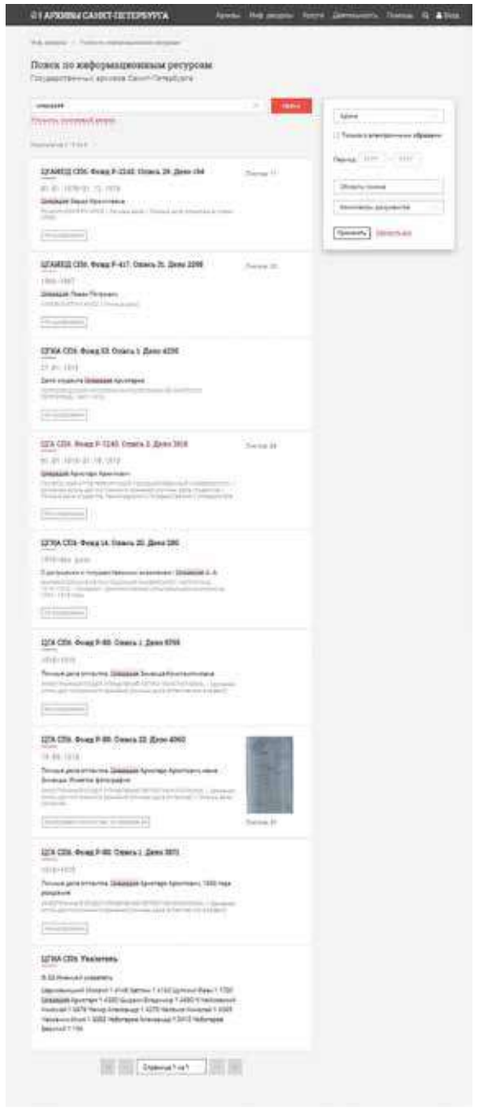


Рис. 2. Пример вывода результатов поиска на «Архивы Санкт-Петербурга»

Санкт-Петербурга. И если пользователю повезет, то интересующие материалы могут быть даже оцифрованы.

Кроме того, на обозначенном ресурсе предусмотрена возможность перехода в социальные сети Вконтакте, Телеграм и др. Визуально взаимодействие на интернет-сервисе показано на рис. 1.

После обработки введенных исходных данных поиска с необходимыми уточнениями, на экране отображаются все найденные материалы: с указанием названия мест хранения, номеров фондов, описей и дел, а также информация о типе обнаруженных данных (оцифрован, графический или текстовой) (рис. 2).

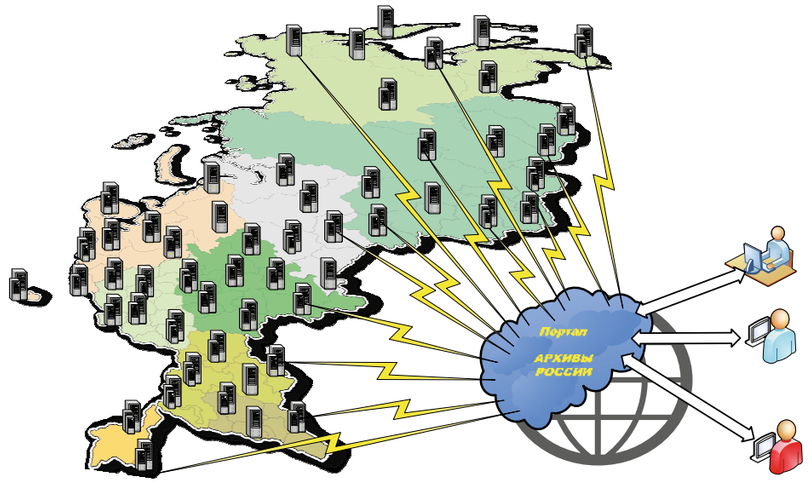
Кроме того, есть возможность уточнения поиска согласно данным Единого классификатора документной информации Архивного фонда.

К неудобству в работе с порталом относится отсутствие возможности самостоятельной регулировки количества отображаемых на странице результатов поиска (найденных дел).

Данное решение могло бы стать еще более эффективным и востребованным, если подключить к этому порталу другие близлежащие архивные учреждения.

Для Санкт-Петербурга, например, речь может идти о Российском государственном архиве Военно-Морского Флота (далее – РГАВМФ) [10], так как он содержит информацию о работниках и служащих, являвшихся, в том числе жителями города и его пригородов.

Кроме того, несмотря на близость расположения, исторически тесные экономические и другие виды связей между Санкт-Петербургом и Ленинградской областью, возможность одновременной работы с архивами этих двух субъектов на одном интернет-ресурсе не предусмотрена, не приводится даже ссылка на соответствующие ресурсы. Необходимость предоставления этой возможности объясняется тем, что за прошедшие десятилетия наблюдалось несколько интенсивных волн миграции людей между этими регионами (Гражданская война, НЭП,



Условные обозначения:

– сеть;

– информационный обмен;

– регион с большим количеством архивов (свыше 10);

– регион со средним количеством архивов (свыше 5);

– регион с малым количеством архивов (менее 5);

Рис. 3. Схема взаимодействия информационного портала «Архивы России»

Великая Отечественная война и послевоенное время, перестройка и распад СССР, многое другое).

На момент написания статьи на портале «Архивы Санкт-Петербурга» возможность сопряжения и последующего отображения найденной информации о делах из РГАВМФ и архивов Ленинградской области не предусмотрена. Даже с помощью персонального кабинета Единой системы идентификации и аутентификации, такой возможности нет.

Пути совершенствования работы единого портала государственных и муниципальных архивов

Полученный отечественный опыт, наработанный при создании, эксплуатации и обслуживании порталов и систем хранения данных, был применен при реализации ряда проектов федерального уровня, таких как: Памяти героев Великой войны 1914–1918 гг.,

Память народа 1941–1945 гг., Государственная автоматизированная система РФ «Правосудие», Георгиевские кавалеры Великой войны 1914–1918 гг., Единая государственная автоматизированная информационная система и др. [11–16].

К сожалению, дальнейшие работы по развитию информационного портала «Архивы России» [17] со времени создания если не остановились совсем, то сильно замедлились (не считая представительство в социальной сети Вконтакте). Речь идет о предоставлении возможности гражданам РФ работать с каталогами и фондами всех архивов любого субъекта РФ (включая работу с муниципальными и многочисленными филиалами) на едином интернет-ресурсе (портале), без перенаправлений и переходов на персональные сайты. Наглядно это представлено на рис. 3.

Предполагалось, что при осуществлении поиска интересующих данных пользователь, зайдя на единый интернет-ресурс, вводит в поисковую строку разыскиваемую информацию, выставляет ограничительные пометки [ключевое слово (слова), дата (рождения, смерти или иная), территория (регион), название населенного пункта, область поиска и так далее]. Система, обработав запрос, выводит на экран монитора полученный результат. Если он не устраивает пользователя ни качественно и ни количественно, то последний может добавить или уменьшить количество ограничений по изменению условий поиска.

Проведение простейшего тестирования функции поиска в Центральном фондовом каталоге[1] (далее – ЦФК) [18] портала «Архивы России» по состоянию на сентябрь 2021 г. показало следующие результаты (таблица 1):

- отсутствие возможности задания временных ограничений по установлению исследуемого периода (верхней и нижней границ поиска);
- отсутствие возможности добавления поиска по уточняющим (дополнительным) словам;
- неполнота результатов поиска (например, только лишь по фамилии Цхададзе было найдено всего 4 единицы хранения [2 в Санкт-Петербурге и 2 в Удмуртии], при этом не выводились результаты поиска на [12]. При воспроизведении условий поиска на портале «Архивы Санкт-Петербурга» там будет обнаружено 8 дел, а на портале «Памяти героев Великой войны 1914–1918 гг.» их нашлось еще больше);
- недостоверность поиска [так при поиске по фамилии Иванов, с одновременным указанием в качестве субъекта РФ Санкт-Петербург, выдало ее отсутствие среди имеющихся записей. Ситуация повторилась при проверке по отдельности фамилий Петров и Попов. После смены региона на Ленинградскую область и поочередной проверке названных выше фамилий, было указано об отсутствии записей в ЦФК]. Хотя, например, в фондах РГАВМФ обнаружено свыше 1500 упоминаний при поиске «Попов». Поиски по фамилии Иванов в РГАВМФ указали о наличии более 4500 записей.

В ходе тестирования были выявлены хронологические некорректности. Например, на посвященном Первой мировой войне ресурсе [11], не подключенном к ЦФК портала «Архивы России», можно найти людей, призванных из Ленинградской области или г. Ленинграда (названных так в 1924 г.). На основе результатов тестирования можно утверждать об отсутствии синхронизации работы ЦФК портала «Архивы России» с каталогами

[1] Центральный фондовый каталог (ЦФК) – федеральная государственная информационная система, представляющая сведения о составе Архивного фонда РФ и предназначенная для информационного обеспечения пользователей архивными документами, хранящихся во всех федеральных архивах, государственных и муниципальных архивах субъектов РФ [18]. Архивный фонд РФ – это исторически сложившаяся и постоянно пополняющаяся совокупность архивных документов, отражающих материальную и духовную жизнь общества, имеющих историческое, научное, социальное, экономическое, политическое, культурное значение, являющихся неотъемлемой частью историко-культурного наследия народов РФ, относящихся к информационным ресурсам, подлежащих постоянному хранению в соответствии с российским законодательством [18].

Таблица 1. Результаты тестирования поиска по ключевым словам

№ п/п	Ключевые слова поиска (уточнения)		Сайт (количество найденных дел, упоминаний и т. п.)				
			Архивы России	РГАВМФ	Архивы Санкт-Петербурга	Памяти героев Великой войны 1914–1918 гг.	Память народа 1941–1945 гг.
1	Цхададзе		4	0	9	>10	>500
2	Ручимский Константин		4	2	3	8	5
3	1880		>500 000	595	27 313	45 985	1 937
4	Иванов	Общее	>700 000	>4 500	>53 000	>97 000	>50 000
		СПб / Птрг	0 / --	-- / --	3 357 / 26 717	25 / 226	54 / 4
		СпбГ/ПтргГ	-- / --	-- / --	13 / 344	21 / 2 384	5 / 0
		Лнгр / ЛО	-- / 0	-- / --	30 006 / 3 285	25 / 25	29 408 / 60 228
5	Петров	Общее	>70 000	>17 500	>155 000	>51 000	>368 000
		СПб / Птрг	0 / --	-- / --	15 870 / 92 453	6 / 56	19 / 13
		СпбГ/ПтргГ	-- / --	-- / --	17 / 1156	5 / 1029	4 / 0
		Лнгр / ЛО	-- / 0	-- / --	64 949 / 5 289	0 / 0	13 313 / 27 405
6	Попов	Общее	>76 000	>1 500	>8 000	>59 000	>370 000
		СПб / Птрг	0 / --	-- / --	756 / 3 342	3 / 8	6 / 4
		СпбГ/ПтргГ	-- / --	-- / --	0 / 9	2 / 56	1 / 1
		Лнгр / ЛО	-- / 0	-- / --	4 582 / 478	2 / 2	1 579 / 5 216

СПб – Санкт-Петербург;

СпбГ – Санкт-Петербургская губерния;

Птрг – Петроград;

ПтргГ – Петроградская губерния;

Лнгр – Ленинград;

ЛО – Ленинградская область;

-- – отсутствие возможности задать интересующий регион.

государственных и муниципальных архивов как единого информационного ресурса.

Также нужно отметить выборочный характер подключения ресурсов архивов к исследуемому порталу. Так на нем не удалось обнаружить записей из, например, РГАВМФ, Военно-исторического и Центрального архива Министерства обороны РФ. Некоторые дела или фонды военных архивов могут иметь ограничительные пометки, но это касается лишь части хранящейся информации, в основном относящейся к XX веку.

Необходимо указать, что по состоянию на дату исследования (сентябрь 2021 г.), название ресурса «Архивы России» не в полной мере соответствует смысловому содержанию и возможностям предоставляемого функционала. В защиту портала нужно отметить, что предусмотрена возможность сбора замечаний и предложений по его работе.

ЗАКЛЮЧЕНИЕ

Авторы согласны с отсутствием необходимости полной оцифровки всех имеющихся в государственных архивах РФ фондов, понимая нескончаемость данного процесса и масштабность требуемых усилий. При этом, необходимо создание единого архивного каталога, заполняемого информацией (сведениями) по единым стандартам и принципам. Что не требует значительных финансовых вливаний при учете имеющихся наработок и опыта. Предсказуемо ожидаемые проблемные вопросы будут связаны с:

- распределением и настройкой полномочий пользователей;
- определением и фиксацией доверительных IP-адресов и протоколов;
- обеспечением информационной безопасности;
- бесперебойностью функционирования 24/7;
- разработкой алгоритма действий должностных лиц на случай возникновения чрезвычайных ситуаций;
- выработкой единых организационных мер: унификация и стандартизация понятийного аппарата, сроков и правил размещения (описания параметров), классификации (отношения) элементов фондов, требований к размещаемым изображениям.

Заявления об отсутствии в этом надобности являются деструктивными. Концепция реализации единого информационного портала должна строиться по принципу «Единого окна», реализуемого на подобии многофункциональных центров обслуживания населения, когда большинство индивидуальных запросов граждан можно решить в одном месте.

В случае практической реализации этого подхода, такое решение способно дать следующие результаты:

1) стать источником уточнений для четкости планируемых к подаче запросов от граждан РФ, а также пользователей из других стран;
2) ускорить проведение исследований (не только исторических, но и экономических, в том числе в области государственного управления);
3) повысить эффективность использования ранее закупленного (приобретенного) серверного и других видов оборудования;
4) уменьшить избыточную трудоемкость сотрудников архивов;
5) повысить скорость служебной переписки и документооборота;
6) снизить эксплуатационные издержки, связанные с поддержанием работоспособности центров хранения и обработки данных;
7) увеличить число пользователей за счет привлечения зарубежной аудитории, расширив международное партнерство;
8) повысить доходность от исполнения запросов зарубежных пользователей.

Необходимо отметить отсутствие рисков, связанных с распределением доходов от выполнения платных тематических запросов, по причине того, что их получает хранящий информацию архив. Пользователь самостоятельно определяет, что ему больше подходит и куда обращаться после изучения размещенной в ЦФК информации.

IMPROVING THE WORK OF THE UNIFIED PORTAL OF STATE AND MUNICIPAL ARCHIVES OF THE RUSSIA ON THE INTERNET

Sanachkina Maria, software engineer, Mozhaisky Military Space Academy.
E-mail: 19.masha.63@mail.ru

Svekolkin Nikolay, head of laboratory, Mozhaisky Military Space Academy.
E-mail: Ins_61@mail.ru

Abstract. For centuries, the search and systematization of data during various studies have often faced the need to work remotely with information stored in municipal, regional or metropolitan archives. Such a situation has been a worldwide practice since the middle of the XVII century. To solve it, the possibility of working in the reading room and the procedure for processing paid thematic requests were provided. The need to make separate requests to each archive, with the existing initial limitations, expressed in the incompleteness of the source data, made the quality of such work unsatisfactory. In addition, the problems were caused by the limited capabilities of the archives themselves: a small number of seats in the reading rooms, the need for early registration for visits and work, the seasonal nature of the reception. In the Russian Federation, the situation was aggravated by the underdevelopment of information and telecommunication technologies and the difficult economic situation that came after the collapse of the USSR. The positive changes observed in the Russian Federation are associated with the development of the economy, a high level of computerization and the emergence of the global Internet. The article formulates proposals for the work of the unified information portal "Archives of Russia", developed based on the results of the simplest testing.
Keywords: internet resource, portal, web-resource, catalog, archive, fund, information resource.

Библиографический список:

1. Петриченко М. Б. Архивы и компьютерная генеалогия: взаимосвязь и развитие. Российский и зарубежный опыт // Вестник архивиста. № 2, 2003. С. 164.
2. Юмашева Ю. Ю. Информатизация архивного дела в Российской федерации (1991–2016 гг.) Научные исследования в области применения информационных технологий / Юмашева Ю. Ю. Москва, 2016. С. 175–181.
3. Приложение к письму Росархива от 17.05.2001 г. № 6/513-К «Рекомендации по созданию архивного сайта в сети Интернет» [Электронный ресурс] / Официальный веб-сайт Росархива России.– URL: http://www.rusarchives.ru/methodics/sait.shtml (дата обращения: 20.07.2021).
4. Копырина С. Н. Зарубежный опыт популяризации архивного дела с использованием официального веб-сайта архива // Общественные практики: уроки истории и современные вызовы: тезисы докладов Всероссийской научной конференции студентов –стипендиатов Оксфордского Российского Фонда. Екатеринбург: УрФУ, 2016. С. 214–216.
5. Копырина С. Н. Использование социальных медиа в работе архивных сайтов России и США // Документ в современном обществе: парадигмы прошлого и реалии настоящего: материалы IX Всероссийской студенческой научно-практической конференции. Екатеринбург: РГППУ, 2016. С. 104–106.
6. Копырина С. Н. Мониторинг архивных сайтов Российской Федерации // Документ в современном обществе: от теории к практике: тезисы VIII Международной студенческой научно-практической конференции. Екатеринбург: УрФУ, 2015. С. 147–150.
7. Копырина С. Н. Образовательные программы на официальном сайте Национального архива и управление документацией США // Документ. Архив. История. Современность: материалы VI межд. научно-практ. конференции / гл. ред. Л. Н. Мазур. Екатеринбург: Изд-во Урал. ун., 2016. С. 157–160.
8. Копырина С. Н. Официальные веб-сайты федеральных архивов России: сравнительный анализ: сб. научн. тр. / Урал. федер. ун-т, [под ред. Л. Н. Мазур]. Екатеринбург: Изд-во Урал. ун., 2016. Вып.16. С. 32.
9. Архивы Санкт-Петербурга. [Электронный ресурс].– Режим доступа: URL: https://spbarchives.ru/archives (дата обращения: 15.09.2021).
10. Российский государственный архив Военно-Морского Флота. [Электронный ресурс].– Режим доступа: URL: https://rgavmf.ru/ (дата обращения: 23.08.2021).
11. Памяти героев Великой войны 1914–1918 гг. [Электронный ресурс].– Режим доступа: URL: https://gwar.mil.ru/ (дата обращения: 19.09.2021).
12. Память народа 1941–1945 гг. [Электронный ресурс].– Режим доступа: URL: https://pamyat-naroda.ru/?static_hash=4bc4c85963eb9e8a24a7bc030f094315v1 (дата обращения: 13.09.2021).
13. Государственная автоматизированная система Российской Федерации «Правосудие». [Электронный ресурс].– Режим доступа: URL: https://sudrf.ru/ (дата обращения: 23.05.2021).
14. Георгиевские кавалеры Великой войны 1914–1918 гг. [Электронный ресурс].– Режим доступа: URL: http://cavalier.rusarchives.ru/ (дата обращения: 18.08.2021).
15. Единая государственная автоматизированная информационная система по регулированию алкогольного рынка. [Электронный ресурс].– Режим доступа: URL: https://egais.ru/ (дата обращения: 27.06.2021).
16. Единая государственная автоматизированная информационная система учёта древесины и сделок с ней. [Электронный ресурс].– Режим доступа: URL: https://lesegais.ru/ (дата обращения: 15.07.2021).
17. Официальный сайт Федерального архивного агентства (Росархива). [Электронный ресурс].– Режим доступа: URL: https://archives.gov.ru/ (дата обращения: 26.09.2021).
18. Архивный фонд Российской Федерации. Центральный фондовый каталог [Электронный ресурс].– Режим доступа: URL: https://cfc.rusarchives.ru/CFC-search/ (дата обращения: 26.09.2021).

Bibliography:

1. Petrichenko M. B. Archives and computer genealogy: interrelation and development. Russian and foreign experience // Archivist's Bulletin. No. 2, 2003. p. 164.
2. Yumasheva Yu. Yu. Informatization of archival business in Russian Federation (1991–2016) Scientific research in the field of information technology application / Yumasheva Yu. Yu. Moscow, 2016. pp. 175–181.
3. Appendix to the letter of the Rosarchiv dated 17.05.2001 No. 6/513-K «Recommendations for creating an archive site on the Internet» [Electronic resource] / Official website of the Rosarchiv of Russia.– URL: http://www.rusarchives.ru/methodics/sait.shtml (accessed: 07/20/2021).
4. Kopyrina S. N. Foreign experience in popularizing archival work using the official archive website // Public practices: History lessons and modern challenges: abstracts of the All-Russian Scientific Conference of Scholarship Students of the Oxford Russian Foundation. Yekaterinburg: UrFU, 2016. pp. 214–216.
5. Kopyrina S. N. The use of social media in the work of archival sites in Russia and the USA // Document in modern society: paradigms of the past and realities of the present: materials IX All-Russian Student Scientific and Practical Conference. Yekaterinburg: RGPPU, 2016. pp. 104–106.
6. Kopyrina S. N. Monitoring of archival sites of the Russian Federation // Document in modern society: from theory to practice: theses VIII International Student Scientific and Practical Conference. Yekaterinburg: UrFU, 2015. pp. 147–150.
7. Kopyrina S. N. Educational programs on the official website of the National Archive and Documentation Management of the USA // Document. Archive. History. Modernity: materials of the VI International Scientific and Practical Conference / ch. ed. L. N. Mazur. Yekaterinburg: Publishing House Ural. un., 2016. pp. 157–160.
8. Kopyrina S. N. Official websites of the Federal Archives of Russia: comparative analysis: collection of scientific tr. / Ural. feder. un-t, [edited by L. N. Mazur]. Yekaterinburg: Publishing House Ural. un., 2016. Issue 16. p. 32.
9. Archives of St. Petersburg. [electronic resource].– Access mode: URL: https://spbarchives.ru/archives (accessed: 09/15/2021).
10. The Russian State Archive of the Navy. [electronic resource].– Access mode: URL: https://rgavmf.ru / (accessed: 08/23/2021).
11. In memory of the heroes of the Great War of 1914–1918. [electronic resource].– Access mode: URL: https://gwar.mil.ru / (date of address: 09/19/2021).
12. Memory of the people 1941–1945. [electronic resource].– Access mode: URL: https://pamyat-naroda.ru/?static_hash=4bc4c85963eb9e8a24a7bc030f094315v1 (date of application: 13.09.2021).
13. The State automated system of the Russian Federation «Justice». [electronic resource].– Access mode: URL: https://sudrf.ru / (accessed: 05/23/2021).
14. St. George 's Cavaliers of the Great War of 1914–1918. [electronic resource].– Access mode: URL: http://cavalier.rusarchives.ru / (accessed: 08/18/2021).
15. Unified State automated information system for alcohol market regulation. [electronic resource].– Access mode: URL: https://egais.ru / (accessed: 06/27/2021).
16. Unified state automated information system for timber accounting and transactions with it. [electronic resource].– Access mode: URL: https://lesegais.ru / (accessed: 07/15/2021).
17. Official website of the Federal Archival Agency (Rosarchiv). [electronic resource].– Access mode: URL: https://archives.gov.ru / (accessed: 26.09.2021).
18. Archive Fund of the Russian Federation. Central Stock Catalog [Electronic resource].– Access mode: URL: https://cfc.rusarchives.ru/CFC-search / (accessed: 09/26/2021).

ИНФОРМАЦИОННЫЕ РЕСУРСЫ РОССИИ

12+

УЧРЕДИТЕЛЬ ЖУРНАЛА
РЭА МИНЭНЕРГО РОССИИ

irr@rosenergo.gov.ru

Специальности ВАК:
0204-3653
05.13.01 – Системный анализ, управление и обработка информации (по отраслям) (физико-математические науки),
05.13.17 – Теоретические основы информатики (технические науки),
05.25.05 – Информационные системы и процессы (технические науки)

Адрес и контакты:
129085, г. Москва, проспект Мира, д. 105, стр. 1
Главный редактор журнала ИРР
Анна Горшкова
Телефон: +7 910 463-53-57
E-mail: anna.gorshik@yandex.ru,
gorshkova@rosenergo.gov.ru

Заместитель главного редактора по подписке, распространению и продвижению журнала «ИРР»
Виолетта Локтева
Телефон: +7 903 733-72-57
E-mail: Lokteva@rosenergo.gov.ru

Главный редактор журнала «Информационные ресурсы России» – **Анна Горшкова**
Руководитель научно-редакционного совета – д. т. н., доцент **Александр Трусов**
Заместитель главного редактора по распространению и продвижению – **Виолетта Локтева**
Корректор – **Роман Павловский**
Фотограф – **Иван Федоренко**
Вёрстка – **Роман Павловский**

Сайт журнала
https://rosenergo.gov.ru/information_and_analytical_support/informatsionnie_resursi_rossii

Подписка
Подписку на журнал можно приобрести в офисах «Урал-Пресс», «Ивис», ФГБУ «РЭА» Минэнерго России
По вопросам подписки:
Виолетта Локтева
+7 903 733-72-57

Стоимость подписки:
550 рублей за один номер
Отпечатано в Печатном бюро «Модуль»,
115162, г. Москва, ул. Мытная, д. 48
E-mail: pbmodul@bk.ru

Подписано в печать: 24.10.2022