Παράδειγμα

Парадигма

Paradigma

Електронно
научно
списание

№3, 2025

Часть 2. Технологии

Парадигма
Електронно
научно списание

БРОЙ 3/2025
Часть 2

Издател:
"ЦЕНТЪР ЗА НАУЧНИ ИЗСЛЕДВАНИЯ И ИНФОРМАЦИЯ "ПАРАДИГМА"" ЕООД
БЪЛГАРИЯ, гр. Варна 9002,
р-н Одесос, ул. Опълченска No 27
E-mail:
niiparadigma@gmail.com

www.paradigma.science

ISSN 2367-8658

Договоры на размещение:
eLIBRARY.RU
CYBERLENINKA

Публикационная политика:

Редакционен съвет

УДК 004.415.25

Буц А.Е.
РТУ МИРЭА, Москва, Россия

Оптимизация работы docker контейнеров

Аннотация. В статье рассматриваются методы оптимизации контейнеров Docker, включая управление слоями образов, минимизацию их размера и эффективное использование кэша. Анализируются выбор базового образа и преимущества многоступенчатой сборки для разделения этапов компиляции и выполнения приложений. Экспериментально подтверждено, что предложенные методы сокращают объем контейнеров, повышают их производительность и ускоряют сборку. Рекомендации будут полезны разработчикам и администраторам контейнерных систем.

Ключевые слова: Docker, оптимизация контейнеров, слои образов, минимизация размера, кэширование, базовый образ, многоступенчатая сборка, управление Dockerfile.

Вис А.Е

Optimizing docker containers

Abstract. In the article are considered methods for optimizing Docker containers to enhance their efficiency. It focuses on managing image layers, minimizing their size, and optimizing caching mechanisms. The importance of selecting a base image and the benefits of multi-stage builds for separating compilation and execution stages are analyzed. Experimental results confirm that the proposed methods significantly reduce container size, improve performance, and accelerate the build process. The presented recommendations will be useful for developers and administrators working with container technologies.

Keywords: Docker, container optimization, image layers, size minimization, caching, base image, multi-stage builds, Dockerfile management.

Введение. Docker широко применяется для контейнеризации приложений, обеспечивая изоляцию, переносимость и удобство развертывания. Однако неэффективное управление контейнерами может приводить к увеличению их размера, замедлению сборки и снижению производительности. Оптимизация контейнеров позволяет уменьшить потребление ресурсов, ускорить развертывание и повысить эффективность работы системы.

Актуальность темы обусловлена растущим использованием контейнерных технологий в разработке и эксплуатации программного обеспечения. Сокращение размера образов и ускорение их сборки особенно важно в условиях облачных вычислений, CI/CD-процессов и работы с ограниченными ресурсами.

Особенности описания слоев. При написании Dockerfile важно понимать, что каждая команда создает новый слой образа [1]. Сам слой, в свою очередь, тоже представляет из себя промежуточный образ, только

неименованный. Значит, итоговый образ – это не что иное, как коллекция других образов, которые наслаиваются друг на друга. Зная эти особенности, попробуем разобраться в правильном написании инструкций для Dockerfile.

Одной из ошибок написания Dockerfile является удаление неиспользуемых файлов в отдельной инструкции. Так как новый уровень уже не может изменить предыдущий, это приводит к тому, что создается новый слой, файловая система которого уже не содержит удаленный файл, а это не влияет на размер предыдущего образа.[8] Одним из решений этой проблемы является объединение команд в одну инструкцию. Рассмотрим вышесказанное на практике: загрузим исходник библиотеки libpcap в виде архива, распакуем его в отдельную директорию и удалим (листинг 1).

Листинг 1 - Содержимое Dockerfile

```
FROM alpine:latest


RUN wget -O ./tcpdump.tar https://www.tcpdump.org/release/libpcap-0.5.2.tar.gz
RUN mkdir tcpdump && tar -xf ./tcpdump.tar -C tcpdump

RUN rm ./tcpdump.tar
```

При разбиении команд таким способом, получим вывод команды *docker history <image_id>,* приведенный в листинге 2: сам архив добавил к базовому образу 132 килобайта, а распакованные файлы – еще 481 килобайт. Удаление архива не приводит к уменьшению размера образа, в чем и получилось убедиться на практике.

Листинг 2 - Вывод команды docker history

```
RUN /bin/sh -c rm ./tcpdump.tar # buildkit      0B        buildkit.dockerfile.v0

RUN /bin/sh -c mkdir tcpdump && tar -xf ./tc…   481kB

RUN /bin/sh -c wget -O ./tcpdump.tar https:/…   132kB

CMD ["/bin/sh"]                                 0B

ADD alpine-minirootfs-3.21.3-x86_64.tar.gz /…   7.83MB
```

Попробуем объединить команды так, чтобы скачивание и удаление выполнялось в одном слое. Dockerfile будет иметь вид, представленный в листинге 3.

Листинг 3. Содержимое Dockerfile

```
FROM alpine:latest


RUN wget -O ./tcpdump.tar https://www.tcpdump.org/release/libpcap-0.5.2.tar.gz && \
    mkdir tcpdump && tar -xf ./tcpdump.tar -C tcpdump && \
```

```
rm ./tcpdump.tar
```

Как показано в листинге 4, вывод docker history не содержит информации о дополнительном слое, размером 132 килобайта.

Листинг 4. Вывод команды docker history

```
RUN /bin/sh -c wget -O ./tcpdump.tar https:/…   481kB

CMD ["/bin/sh"]                                 0B

ADD alpine-minirootfs-3.21.3-x86_64.tar.gz /…   7.83MB
```

Использование утилиты export. Другим вариантом решения проблемы является использование утилит import и export. С помощью export (в отличие от save, которая применяется для образов и сохраняет всю историю преобразований) можно сохранить файловую систему контейнера в виде архива. [3] Для этого нужно запустить контейнер на основе любого из образов, описанных выше. Применив к нему export, а затем import можно получить образ, состоящий из одного слоя, который имеет необходимый размер.

Существенным минусом данного подхода является то, что метаданные и история образов не сохраняются. Это означает, что предыдущие слои уже не смогут использоваться повторно в других образах. Данные связанных с контейнером томов также не сохраняются. Убедимся в этом, выполнив команды и листинга 5. Размер полученного архива соответствует ожиданиям.

Листинг 5 - Запись файловой системы контейнера в архив

```
#docker run -d <image_id>

#docker export -o example1.tar <container_id>

#ls -lh example1.tar

-rw------- 1 root root 8.3M Feb 22 21:04 example1.tar
```

Эффективное использование кэша. При написании Dockerfile также важно иметь в виду наличие кэша сборки в Docker. Если оказывается, что образ для очередного слоя уже имеется в кэше – используется он, это ускоряет процесс сборки контейнерных решений. Иначе создается новый слой для текущей инструкции и для всех, последующих за ней (так как команды наслаиваются друг на друга) [4]. Из этого можно сделать вывод, что для того, чтобы эффективнее использовать данную опцию, ближе к концу файла стоит размещать инструкции, которые предполагаемо могут измениться. Также важно учитывать, что в отличие от других инструкций, которые просто сравниваются с теми, что уже есть в промежуточных образах, при выполнении команд ADD и COPY проверяется содержимое самих добавляемых файлов, поэтому часто

редактируемые файлы, добавляемые с помощью ADD и COPY стоит также размещать по возможности ближе к концу.

Выбор базового образа. Стоит обратить внимание и на выбор базового образа. Если проекту не нужны системные библиотеки или системные утилиты, лучше не использовать полнофункциональную ОС в качестве базового образа [5]. Например, существуют alpine-образы, основанные на дистрибутиве одноименного дистрибутива с корневой файловой системой весом 5 мегабайт. Также существуют slime-образы, они основаны на минимизации компонентов и пакетов таких дистрибутивов как Debian или Ubuntu. Рекомендуется использовать минимальный базовый образ, который содержит только код самого приложения и необходимое количество дополнительных пакетов. Однако минусом такой минимизации является то, что теперь требуется больше усилий для установки дополнительных пакетов.

В некоторых случаях такой подход может облегчить контейнер, но иногда это заставит разработчика потратить время на дополнительную настройку. [6]

Применение многоступенчатой сборки. Даже образ с минимальными пакетами для сборки можно сделать еще меньше. Ведь софт, который используется для сборки не всегда нужен для запуска готового файла. Частой практикой является разделение логики контейнеров на две составляющие: контейнер для сборки и продакшн контейнер. К примеру, в первом компилируется бинарный файл для программы на Go, а во втором контейнере он запускается. Исследуем такой подход.

Сначала соберем образ, который будет содержать Go-компилятор и прочие зависимости, в него поместим файл с программой, которая выводит “Hello world!” в консоль Содержимое Dockerfile для такого образа представлено в листинге 6.

Листинг 6 - Содержимое Dockerfile образа сборки

```
FROM golang:tip-alpine3.21

COPY ./main.go .

RUN go build ./main.go
```

Размер получившегося образа около 349 мегабайт (листинг 7), что очень много для программы, выводящей одну строку в консоль.

Листинг 7 - Размер образа сборки

```
#docker build -t hello-world-build .

#docker save hello-world-build -o hello-world-build.tar

#ls -lh hello-world*
```

```
-rw------- 1 root root 349M Feb 25 14:58 hello-world-build.tar
```

Запустим контейнер, основанный на этом образе, полученный после выполнения команды go build ./main.go бинарный файл переместим в новый контейнер, где он сможет запуститься уже без компилятора. Реализуем это с помощью команд, представленных в листинге 8.

Листинг 8 - Запуск в контейнере скомпилированного бинарного файла

```
#docker run --name container-builder hello-world-build

#docker cp container-builder:/go/main ./prod

/prod# docker build -t hello-world-prod .
```

Образ из prod/Dockerfile будет основываться на alpine3.21, как и предыдущий (листинг 9), поэтому сравнение можно считать объективным.

Листинг 9 - Содержимое Dockerfile продакшн образа

```
FROM alpine:3.21

COPY ./main .

RUN ./main
```

Размер получившегося контейнера около 10 мегабайт (листинг 10), что примерно в 35 раз меньше, чем размер образа hello-world-build. Это доказывает эффективность применения такого подхода.

Листинг 10 - Размер продакшн образа

```
# docker history hello-world-prod

CREATED BY                                      SIZE

RUN /bin/sh -c ./main # buildkit                0B

COPY ./main . # buildkit                        2.22MB

CMD ["/bin/sh"]                                 0B

ADD alpine-minirootfs-3.21.3-x86_64.tar.gz /…   7.83MB
```

В настоящее время делать столько ручной работы не приходится, потому что появился специальный инструмент – многоступенчатая сборка (multi-stage builds). Это позволяет объединить действия, описанные на предыдущем шаге в один Dockerfile (листинг 11). Повторим те же операции, используя многоступенчатую сборку.

Листинг 11 - Реализация многоступенчатой сборки в Dockerfile

```
FROM golang:tip-alpine3.21 AS build

COPY ./main.go .

RUN go build ./main.go

FROM alpine:3.21
```

```
COPY --from=build /go/main .

RUN ./main
```

Убедимся в том, что размер готового образа равен размеру образа, в котором присутствует конфигурация дистрибутива и бинарный файл. Результат продемонстрирован в листинге 12.

Листинг 12 - Размер итогового образа

```
# docker history multi-stage-hw

CREATED BY                                SIZE

RUN /bin/sh -c ./main # buildkit          0B

COPY /go/main . # buildkit                2.22MB

CMD ["/bin/sh"]                           0B

ADD alpine-minirootfs-3.21.3-x86_64.tar.gz /…  7.83MB
```

Выводы. Исследование подтвердило, что оптимизация слоев образов, минимизация их размера и эффективное кэширование повышают производительность контейнеров Docker. Объединение команд в одной инструкции уменьшает количество слоев, а использование минималистичных базовых образов снижает объем конечного контейнера.

Многоступенчатая сборка доказала свою эффективность, позволяя исключить лишние зависимости и сократить размер образов без потери функциональности. Представленные методы оптимизации рекомендованы для повышения эффективности контейнерных решений.

Список литературы

1. Слои, кеширование и оптимизации | Docker: Основы - Хекслет [Электронный ресурс]. URL: https://ru.hexlet.io/courses/docker-basics/lessons/image-layers/theory_unit (дата обращения: 26.02.2025).
2. 5 приемов оптимизации сборки Docker-образов [Электронный ресурс]. URL: https://1cloud.ru/help/docker/5_docker_tricks (дата обращения: 26.02.2025).
3. Методики уменьшения размеров образов Docker [Электронный ресурс]. URL: https://habr.com/ru/companies/ruvds/articles/485650 (дата обращения: 26.02.2025).
4. Изучаем Docker, часть 4: уменьшение размеров образов и оптимизация сборки [Электронный ресурс]. URL: https://habr.com/ru/companies/ruvds/articles/440658 (дата обращения: 26.02.2025).
5. Оптимизация Dockerfile для уменьшения размера и быстрой сборки образа [Электронный ресурс]. URL: https://habr.com/ru/companies/first/articles/702168 (дата обращения: 26.02.2025).
6. Оптимизация образов Docker для производства [Электронный ресурс]. URL: https://www.8host.com/blog/optimizaciya-obrazov-docker-dlya-proizvodstva (дата обращения: 26.02.2025).

УДК 004.42

Беглиева Д.[1], Бекмурадова Б. [1], Беллиева М. [1], Беглиев А. [2]
[1]Туркменский государственный институт культуры, Ашхабад, Туркменистан
[2]Туркменский национальный институт мировых языков им. Довлетмаммета Азади, Ашхабад, Туркменистан

Влияние цифровых технологий на языковое развитие

Аннотация. Цифровизация оказывает значительное влияние на языковое развитие, трансформируя как процессы обучения, так и повседневное использование языка. В статье рассмотрены основные аспекты влияния цифровых технологий на развитие речи, письменности, а также на использование языка в различных социальных и образовательных контекстах. Акцент сделан на преимуществах и рисках, связанных с использованием современных технологий в обучении и коммуникации. Представлены данные о влиянии цифровых средств на фонетическое, лексическое и грамматическое развитие, а также на формирование новых форм общения в цифровой среде.

Ключевые слова: цифровые технологии, языковое развитие, обучение, коммуникация, речь, письменность, лексика, грамматика.

Beglıeva D., Bekmýradova B., Beláeva M., Beglıev A.

The Impact of Digital Technologies on Language Development

Abstract. Digitalization has a significant impact on language development, transforming both learning processes and everyday language use. This article examines the main aspects of how digital technologies influence the development of speech, writing, and language usage in various social and educational contexts. Emphasis is placed on the advantages and risks associated with the use of modern technologies in education and communication. Data is presented on the impact of digital tools on phonetic, lexical, and grammatical development, as well as on the formation of new forms of communication in the digital environment.

Keywords: digital technologies, language development, education, communication, speech, writing, lexicon, grammar.

Введение. Цифровые технологии, охватывающие широкий спектр средств — от мобильных приложений и платформ для обучения до искусственного интеллекта и нейросетей, становятся важной частью современного образовательного и культурного пространства. Особенно заметно их влияние на языковое развитие, которое традиционно зависело от школьных методов преподавания, общения в социальной среде и письменных источников. Однако с развитием технологий, таких как интернет, искусственный интеллект, цифровая грамотность, происходят значительные изменения как в способах обучения, так и в практике повседневной коммуникации [1] .

Цифровизация образования в последние десятилетия значительно преобразила процесс обучения, в том числе и в области изучения иностранных и родных языков. Интеграция новых технологий открывает перед учащимися широкие возможности, позволяя учить и совершенствовать языковые навыки в удобной и гибкой форме [2].

Важную роль в этом процессе играют разнообразные онлайн-платформы, интерактивные приложения и инструменты, которые делают обучение доступным, персонализированным и эффективным [3].

Одним из ярких примеров таких платформ являются Duolingo и Memrise, которые предоставляют пользователям удобный формат для освоения новых языков. Эти сервисы предлагают различные упражнения для тренировки грамматики, лексики, произношения, а также позволяют настроить индивидуальный темп обучения. Важным аспектом их работы является элемент геймификации, который делает процесс изучения языка увлекательным и мотивирующим, побуждая пользователя к регулярным занятиям.

Современные образовательные технологии также включают доступ к онлайн-курсам с носителями языка, чат-ботам для практики общения, а также интерактивным упражнениям, которые дают возможность развивать не только теоретические знания, но и практические навыки. Например, с помощью специализированных приложений учащиеся могут не только изучать новые слова, но и сразу же применить их в контексте, тренируя речевые и аудитивные навыки. Кроме того, видеоуроки и вебинары позволяют организовать обучение в гибком формате, давая учащимся возможность работать с материалами в любое время. Это особенно важно в условиях загруженности студентов и необходимости адаптировать образовательный процесс под их личные потребности.

Цифровые инструменты, такие как автоматические переводчики (например, Google Translate), играют не менее значимую роль в облегчении процесса обучения языкам. Они позволяют быстро переводить слова и фразы, что особенно полезно при изучении незнакомых слов и выражений. В условиях глобализации, когда межкультурное общение и знание иностранных языков становятся всё более важными, такие инструменты становятся незаменимыми помощниками в повседневной жизни.

Тем не менее, использование цифровых технологий в обучении языкам вызывает и определенные опасения. Одной из основных проблем является искажение смысла перевода, особенно при использовании автоматических систем. В некоторых случаях переводчики могут неправильно интерпретировать контекст, что может привести к ошибкам в коммуникации. Также существует риск утраты навыков самостоятельного перевода, так как студенты могут слишком полагаться на эти технологии и не развивать критическое мышление и языковую интуицию.

Таким образом, роль цифровых технологий в обучении языкам многогранна. Они делают процесс обучения более доступным и эффективным, обеспечивая широкий спектр инструментов для практики и взаимодействия с языком. В то же время важно, чтобы студенты использовали эти технологии осознанно, не забывая о необходимости

развивать свои собственные языковые навыки и способности к самостоятельному переводу.

Цифровая среда оказывает значительное влияние на повседневную речь, создавая новые формы коммуникации, которые активно внедряются в повседневную жизнь. В особенности это заметно в социальных сетях, мессенджерах и других онлайн-платформах, где пользователи стремятся обмениваться информацией быстро и эффективно. В результате появляется новое поколение лексических и грамматических конструкций, адаптированных к цифровым условиям общения.

Одним из самых ярких примеров таких изменений является использование сокращений, акронимов и специфических символов. В сообщениях в социальных сетях и мессенджерах, а также в онлайн-играх активно применяются сокращенные формы слов и фраз, такие как "lol" (laugh out loud), "brb" (be right back), "omg" (oh my god) и другие. Это позволяет ускорить обмен информацией и снизить нагрузку на пользователя, особенно при взаимодействии в реальном времени. Эти формы выражения стали настолько привычными, что они постепенно начали проникать в повседневную речь, иногда даже в письменную форму общения, как в деловых переписках или учебных заданиях.

Кроме того, эмодзи, мемы и другие графические элементы стали важными составляющими цифровой коммуникации. Эти визуальные символы помогают передать эмоции, настроение или контекст, что компенсирует отсутствие невербальных знаков в текстовой переписке. В результате, цифровое общение становится более насыщенным и многозначным, что влияет на восприятие и структуру языка в целом.

Такое использование сокращений и визуальных элементов также затрудняет традиционное разделение письменной и устной речи, создавая новые формы языковых норм. Это может привести к возникновению "языков" внутри отдельных цифровых сообществ, где нормы общения могут существенно отличаться от общепринятых. Например, специфическая лексика, используемая в онлайн-играх, может сильно отличаться от той, что применяется в реальной жизни, и быть понятной только участникам этих сообществ.

С другой стороны, цифровые технологии оказывают влияние на глобализацию языка. Особенно это проявляется в распространении английского языка, который становится своего рода "международным кодом" для общения людей разных национальностей и культур. В условиях онлайн-коммуникации английский язык используется как общий язык для взаимодействия, что способствует унификации лексики и стилистических особенностей речи. Это также может привести к утрате уникальных черт национальных языков, поскольку многие традиционные выражения и фразы заменяются англицизмами или же переработанными в соответствии с цифровыми нормами.

Таким образом, влияние цифровых технологий на повседневную речь многогранно. Они не только способствуют изменению лексики и грамматики, но и приводят к возникновению новых форм общения, которые затрудняют разделение между устной и письменной речью, а также влияют на сохранение языковых традиций и уникальности.

Проблемы и риски цифровых технологий для языкового развития. Несмотря на положительные аспекты, цифровизация языка также вызывает ряд проблем и рисков. Одним из них является уменьшение качества письменной речи, особенно среди молодежи. Постоянное использование чат-форматов и социальных сетей может привести к сокращению словарного запаса, неправильному использованию грамматических конструкций и ухудшению орфографии.

Существуют также опасения, что из-за массового использования автоматических переводчиков и других цифровых инструментов люди могут утратить способность к самостоятельному анализу и построению предложений, полагаясь на технологии для решения даже базовых задач. Более того, с ростом использования голосовых помощников, таких как Siri и Alexa, возможен спад интереса к классическим методам письма, что влияет на развитие навыков письма.

Цифровая грамотность как часть языкового образования. Цифровая грамотность становится важным компонентом современного образования. Она включает в себя не только способность эффективно использовать цифровые инструменты для коммуникации и обучения, но и критическое осмысление информации, получаемой в цифровых форматах. В условиях, когда многие источники информации становятся доступными только в онлайн-формате, важно научить учащихся грамотно работать с цифровыми текстами, понимать их контекст и различать достоверные и недостоверные данные.

Цифровая грамотность также включает в себя умение работать с различными видами цифровых коммуникаций, такими как блоги, форумы, социальные сети, что оказывает влияние на формирование лексической и грамматической базы у молодежи. Это также способствует развитию навыков письменной коммуникации, но уже в условиях новых цифровых медиа.

Перспективы развития и заключение. С развитием цифровых технологий продолжится их влияние на языковое развитие. В ближайшем будущем можно ожидать появления новых технологий и платформ, способствующих улучшению языковых навыков, а также увеличения разнообразия форм коммуникации в цифровом пространстве. Важно, чтобы системы образования и культуры научились интегрировать эти технологии, сохраняя при этом богатство и разнообразие языков, их способность к адаптации и развитию.

Цифровизация оказывает как положительное, так и отрицательное влияние на языковое развитие. В условиях цифровой эпохи необходимо адаптировать учебные процессы и развивать цифровую грамотность, чтобы сохранить культурное наследие языков и обеспечить их устойчивое развитие в новом технологическом контексте.

Список литературы

1. Wierzbicka A.L. The Language of Digital Communication / A.L. Wierzbicka. – Oxford, 2021. 280 p.
2. Crystal D. Language and the Internet / D. Crystal. – Cambridge, 2006. 384 p.
3. García-Sánchez P. (Ed.) The Oxford Handbook of Language and Society / P. García-Sánchez (Ed.). – Oxford, 2020. 720 p

Информация об авторах:
Беглиева Дженнет, преподаватель, Туркменский государственный институт культуры, Ашхабад, Туркменистан
Бекмурадова Бахар, преподаватель, Туркменский государственный институт культуры, Ашхабад, Туркменистан
Беллиева Майса, преподаватель, Туркменский государственный институт культуры, Ашхабад, Туркменистан
Беглиев Алланур, преподаватель, Туркменский национальный институт мировых языков им. Довлетмаммета Азади, Ашхабад, Туркменистан
Jennet Beglieva, Lecturer, Turkmen State Institute of Culture, Ashgabat, Turkmenistan
Bekmuradova Bahar, Lecturer, Turkmen State Institute of Culture, Ashgabat, Turkmenistan
Bellieva Maisa, Lecturer, Turkmen State Institute of Culture, Ashgabat, Turkmenistan
Begliyev Allanur, lecturer, Turkmen National Institute of World Languages. Dovletmammeta Azadi, Ashgabat, Turkmenistan

УДК 378.147

Асадова Х. А., Бабаджанова Ш.
Туркменский государственный педагогический институт им С. Сейди
г. Туркменабат, Туркменистан

Инновационные методы преподавания биологии: цифровые технологии и активное обучение

Аннотация Современное образование требует внедрения инновационных методик, особенно в таких дисциплинах, как биология. В данной статье рассматриваются цифровые технологии и активные методы обучения, их преимущества и влияние на эффективность образовательного процесса. Проанализированы практические кейсы использования современных подходов, а также перспективы их дальнейшего развития.
Ключевые слова: инновации в образовании, цифровые технологии, активное обучение, биология, интерактивные методы.

Asadova H. A., Babajanova S.

Innovative teaching methods in biology: digital technologies and active learning

Abstract Modern education requires the implementation of innovative methodologies, especially in disciplines such as biology. This article examines digital technologies and active learning methods, their advantages, and their impact on the effectiveness of the educational process. Practical cases of modern approaches are analyzed, as well as prospects for their further development.
Keywords: educational innovations, digital technologies, active learning, biology, interactive methods.

Введение Современные образовательные процессы стремительно развиваются под влиянием цифровизации и новых педагогических подходов. Биология, как наука, тесно связанная с практическими исследованиями и визуализацией, особенно выиграла от внедрения инновационных методов преподавания [1]. Цель данной статьи — рассмотреть применение цифровых технологий и активных методов в преподавании биологии, а также их влияние на успеваемость и вовлеченность студентов.

Цифровые технологии в преподавании биологии Современные цифровые технологии позволяют сделать обучение более наглядным, интерактивным и эффективным [2]. Рассмотрим основные инструменты:

Виртуальная и дополненная реальность (VR/AR). Позволяют моделировать сложные биологические процессы, создавать виртуальные лаборатории и погружать студентов в изучаемый материал.

Интерактивные платформы и симуляции. Такие ресурсы, как Labster, PhET или BioMan, помогают учащимся проводить виртуальные эксперименты и анализировать биологические явления.

Онлайн-курсы и видеолекции. Использование платформ Coursera, Khan Academy и YouTube значительно расширяет возможности самообразования.

Использование искусственного интеллекта (ИИ). Системы адаптивного обучения анализируют прогресс студентов и предлагают индивидуальные траектории обучения.

Активные методы обучения в биологии Интерактивные подходы играют ключевую роль в образовательном процессе. Основные методы активного обучения:

Проблемно-ориентированное обучение (PBL). Студенты решают реальные биологические задачи, применяя полученные знания на практике.

Кейс-метод. Рассмотрение реальных случаев из биологической практики помогает студентам глубже понять материал.

Проектная деятельность. Работа в группах над исследовательскими проектами способствует развитию навыков самостоятельного мышления и анализа.

Геймификация. Использование игровых механик (квестов, викторин, симуляций) мотивирует студентов и делает обучение более увлекательным.

Практический опыт внедрения инновационных методов В различных учебных заведениях мира уже успешно применяются инновационные методы преподавания биологии. Например, в Финляндии внедрение PBL показало значительное улучшение понимания сложных биологических тем. В США использование VR в изучении анатомии позволило студентам более эффективно усваивать материал.

Примером успешного использования геймификации является программа «Foldit» — компьютерная игра, в которой студенты решают задачи по сворачиванию белков, помогая реальным биологическим исследованиям.

Таблица 1 – Сравнение традиционных и инновационных подходов

Метод	Преимущества	Недостатки
Традиционное обучение (лекции, учебники)	Структурированность, доступность	Малая вовлеченность студентов, пассивное усвоение материала
Цифровые технологии	Интерактивность, доступность материалов	Требует технического оснащения и цифровой грамотности
Активное обучение	Развитие критического мышления, вовлечение	Требует значительных временных затрат на подготовку

Оценка эффективности методов и перспективы внедрения Исследования показывают, что использование цифровых технологий и

активного обучения увеличивает вовлеченность студентов на 30–50% и способствует лучшему усвоению материала по сравнению с традиционными методами. В частности, эксперименты с виртуальными лабораториями показывают, что студенты запоминают на 40% больше информации.

Однако внедрение этих технологий сопровождается рядом проблем:

Недостаточное техническое оснащение учебных заведений.

Необходимость дополнительного обучения преподавателей.

Сопротивление традиционным методам обучения.

Перспективы развития включают:

Повышение доступности технологий.

Разработка новых образовательных платформ.

Более активное внедрение адаптивных методов обучения с ИИ.

Совмещение различных методов для создания индивидуальных образовательных траекторий.

Будущие тренды в преподавании биологии С развитием технологий и внедрением новых образовательных методик, преподавание биологии, как и других научных дисциплин, претерпевает значительные изменения. Ожидается, что в ближайшие десятилетия педагогика биологии будет ориентироваться на персонализированный подход, использование высоких технологий и более глубокую интеграцию современных научных достижений. Рассмотрим возможные тренды, которые будут определять будущее преподавания биологии.

Использование нейросетей для адаптации учебных программ под потребности каждого студента

Одним из наиболее перспективных направлений в образовательном процессе является интеграция нейросетевых технологий для персонализации учебных программ. Искусственный интеллект уже активно используется в различных областях, и биология не станет исключением. Нейросети смогут анализировать индивидуальные особенности студентов: их уровень подготовки, интересы и особенности восприятия материала. На основе этих данных искусственный интеллект сможет адаптировать учебный процесс, предлагая студентам наиболее подходящие задания, дополнительные материалы и способы объяснения сложных тем. Это позволит каждому студенту идти своим темпом, получая необходимую поддержку и развивая свои уникальные способности.

Развитие биоинформатики в образовании — интеграция больших данных и генетических исследований в учебный процесс

С развитием биоинформатики на фоне эволюции генетических исследований и анализа больших данных, преподавание биологии будет охватывать все более сложные и специализированные темы. Биоинформатика, как область, объединяющая биологию, информатику и математику, станет неотъемлемой частью учебных программ. Студенты

будут обучаться использованию специализированных программных продуктов для анализа генетических данных, работы с базами данных, моделирования биологических процессов. Такие навыки станут необходимыми для будущих биологов и исследователей, так как умение работать с большими данными открывает новые горизонты для разработки медицинских препаратов, диагностики заболеваний и решения других задач биологии.

Применение 3D-биопринтинга для создания реальных биологических моделей в лабораторных условиях

Технология 3D-печати, или биопринтинг, представляет собой метод создания живых тканей и органов с помощью принтеров, использующих биосовместимые материалы. В образовательных учреждениях это открывает уникальные возможности для создания реальных биологических моделей, которые студенты смогут изучать и использовать в лабораторных работах. Например, 3D-биопринтинг позволит создавать модели человеческих органов, которые будут использоваться для изучения их строения, функций, а также для тестирования новых медицинских препаратов. Такая практика может не только повысить качество обучения, но и стать важным инструментом для внедрения инновационных технологий в медицинское образование.

Широкое внедрение дистанционных лабораторий

С развитием технологий виртуальной и дополненной реальности, а также прогрессом в области дистанционного обучения, возможным станет создание дистанционных лабораторий. Эти лаборатории будут использовать инновационные платформы, позволяющие студентам проводить эксперименты онлайн в реальном времени. Например, студенты смогут работать с виртуальными лабораторными установками, проводить эксперименты с биологическими образцами, моделировать биологические процессы, анализировать результаты. Дистанционные лаборатории могут стать доступными для студентов по всему миру, независимо от их физического местоположения, что значительно расширяет возможности для обучения и практических занятий. Будущее преподавания биологии связано с активным использованием новых технологий и персонализированного подхода к обучению. Нейросети, биоинформатика, 3D-биопринтинг и дистанционные лаборатории создадут новые горизонты для изучения биологических наук, сделают процесс обучения более увлекательным и эффективным, а также дадут студентам возможность более глубоко погрузиться в исследования и эксперименты. Внедрение этих технологий окажет значительное влияние на развитие науки и образования в области биологии, обеспечивая более глубокое понимание биологических процессов и стимулируя научные достижения в различных областях.

Заключение Инновационные методы преподавания биологии, основанные на цифровых технологиях и активном обучении, значительно повышают качество образования, делая процесс изучения науки более наглядным, увлекательным и эффективным. Несмотря на существующие трудности, интеграция новых подходов в учебный процесс является важным шагом к модернизации образования.

Список литературы

1. Мынбаева А.К., Садвакасова З.М. Инновационные методы обучения, или как интересно преподавать. М., 2020. 240 с.
2. Мухина С.А., Соловьёва А.А. Современные инновационные технологии обучения. М., 2019. 220 с.

Информация об авторах:
Асадова Хасият Ахмедовна, канд. пед. наук, старший преподаватель кафедры “Биология и методика её преподавания” Туркменский государственный педагогический институт им С. Сейди, г. Туркменабат, Туркменистан.
Бабаджанова Шемсие, канд. пед. наук, старший преподаватель кафедры “Биология и методика её преподавания” Туркменский государственный педагогический институт им С. Сейди, г. Туркменабат, Туркменистан

Asadova H. A., PhD in Pedagogical Sciences, Senior Lecturer Department of "Biology and Methods of Teaching It" Turkmenabat, Turkmenistan
Babajanova Shemsiye, PhD in Pedagogical Sciences, Senior Lecturer Department of "Biology and Methods of Teaching It". Turkmen State Pedagogical Institute named after S. Seydi, Turkmenabat, Turkmenistan

УДК 004.77

Пучков Г.Ю.
ФКУ НПО «СТиС», Москва, Россия

Принципы построения основных компонентов современных информационно-аналитических систем

Аннотация. В статье рассматриваются общие принципы создания информационно-аналитических систем (ИАС) федеральных органов исполнительной власти, базовые принципы создания телекоммуникационных подсистем и подсистем рабочих мест пользователей, проводится анализ состава и структуры телекоммуникационных подсистем ИАС, приводятся требования к основным каналам и услугам связи, описываются нюансы организации мобильного доступа к ИАС, рассматриваются различные типы автоматизированных рабочих мест.
Ключевые слова: информационно-аналитическая система, автоматизированное рабочее место, телекоммуникационная система, коммутационный узел, ИТ-инфраструктура.

Puchkov G.Y.

Principles of constructing the main components of modern information and analytical systems

Abstract. The article examines the general principles of creating information and analytical systems (IAS) of federal executive bodies, the basic principles of creating telecommunications subsystems and subsystems of user workstations, analyzes the composition and structure of telecommunications subsystems of IAS, formulates requirements for the main communication channels and services, describes the nuances of organizing mobile access to IAS, and examines various types of automated workstations
Keywords: information and analytical system, automated workplace, telecommunication system, switching node, IT infrastructure

В условиях цифровой трансформации государственных структур особое значение приобретает развитие информационно-аналитических систем (ИАС), способных эффективно обрабатывать большие объемы данных, автоматизировать процессы управления и повышать оперативность принятия решений.

Современные ИАС представляют собой сложные программно-аппаратные комплексы, включающие базы данных, аналитические модули, средства машинного обучения и технологии искусственного интеллекта. Они позволяют не только собирать и структурировать информацию, но и выявлять скрытые закономерности, прогнозировать развитие ситуаций и обеспечивать поддержку при принятии решений [1, 2].

Создание ИАС является сложной научно-технической задачей, решение которой требует применения современных методов системного

анализа, математического моделирования, алгоритмов обработки данных, а также использования передовых информационных технологий и программно-аппаратных средств. В данной статье рассматриваются общие принципы создания ИАС, анализируются ключевые элементы этих систем, такие как телекоммуникационная система и автоматизированные рабочие места.

Материалы статьи позволят не только определить текущее состояние информационно-аналитических систем федеральных органов исполнительной власти, но и наметить векторы их дальнейшего совершенствования в условиях стремительного технологического прогресса.

Общая архитектура ИАС, как правило, состоит из подсистемы централизованной обработки данных, телекоммуникационной подсистемы, подсистемы информационной безопасности, подсистемы мониторинга и управления, а также подсистемы рабочих мест пользователей [2].

В настоящей статье мы остановимся на общих принципах создания ИАС, базовых принципах создания телекоммуникационной подсистемы и подсистемы рабочих мест пользователей.

Общие принципы создания ИАС.

ИАС ФОИВ как правило строятся на следующих принципах:

– унификация и централизация средств автоматизации деятельности ФОИВ;

– централизованное управление разработкой, внедрением и сопровождением ИАС ФОИВ на основании единой технологической политики с учетом отраслевых государственных, национальных и адаптированных к отечественным условиям международных стандартов;

– создание прикладных информационных систем по модели «программное обеспечение как услуга» (SaaS);

– предоставление ИТ-инфраструктуры для разработки специализированных прикладных информационных систем по модели «инфраструктура как услуга» (IaaS);

– переход от построения собственных линий связи к аренде каналов и услуг связи на конкурсной основе;

– обеспечение совместимости (интероперабельности) информационных систем ФОИВ;

– обеспечение информационной безопасности и защиты персональных данных в соответствии с требованиями законодательства Российской Федерации;

– модернизация используемых информационных систем и разработка новых компонентов Систем с учетом максимально возможного сохранения существующих программно-технических средств;

– однократный ввод и многократное использование первичной информации;

– обеспечение интеграции с введенными в промышленную эксплуатацию компонентами «Электронного Правительства».

При разработке ИАС должна обеспечиваться поддержка конкуренции среди производителей специализированных прикладных информационных систем, а также информационных систем, автоматизирующих задачи общего назначения, включая административно-хозяйственную деятельность.

Для выполнения выше указанных задач ИАС должна обеспечивать реализацию следующих основных функций:

– автоматизация прикладных функций;

– централизованное хранение и обработка данных;

– комплексный анализ данных;

– обеспечение доступа к ресурсам.

Состав и базовые принципы создания телекоммуникационной подсистемы ИАС.

Телекоммуникационная подсистема (ТС) является составной частью ИАС и предназначена для предоставления пользователям доступа к централизованным информационным ресурсам, региональным и федеральным прикладным системам. Кроме того, ТС может являться транспортной средой для взаимодействия между другими подсистемами ИАС.

В состав ТС, как правило, входят следующие функциональные подсистемы:

– магистральная сеть на базе технологий DWDM, SDH, или IP/MPLS (на базе магистральных каналов связи и сетей российских операторов связи);

– сеть проводного доступа (на базе собственных кабелей связи, а также каналов связи, арендуемых у российских операторов проводной связи);

– сеть беспроводного доступа (на базе собственных и арендуемых у российских операторов сетей беспроводной связи);

– ведомственная телефонная сеть;

– контакт-центр;

– ведомственная система видеоконференцсвязи;

– подсистема мониторинга и управления (в части управления сетью);

– подсистема информационной безопасности (в части сетевой безопасности).

Зачастую ТС имеет трехуровневую структуру:

– уровень ядра – центр обработки данных, главный коммутационный узел, опорные коммутационные узлы (размещаются в федеральных округах Российской Федерации);

– региональный уровень – коммутационные узлы размещаются в субъектах Российской Федерации;

– уровень доступа – узлы районов и городов.

Подход к организации сети каждого уровня различен – у оператора связи арендуются различные типы каналов и сетей (услуг). При этом для объединения в сеть режимных объектов должны использоваться собственные линии связи ФОИВ, либо специально выделенные из состава государственных систем связи.

Основными требованиями к каналам и услугам связи являются [3]:

– резервирование основных направлений опорных коммутационных узлов федеральных округов Российской Федерации;

– разделения трафика по классам обслуживания (ClassofService, CoS);

– организация линий доступа (линий «последней мили») с использованием линейно-кабельных сооружений связи, радиодоступа, радиорелейных линий связи, подвижной радиосвязи, спутникового сегмента;

– параметры качества линий связи («круговая» сетевая задержка прохождения IP-пакета, вариация сетевой задержки, коэффициент потери пакетов, сроки восстановления канала) должны соответствовать установленным законодательством РФ нормам и требованиям.

Предоставляемые оператором связи каналы связи делятся на несколько типов:

– высокоскоростные – 10 Гбит/с для подключения центров обработки данных;

– среднескоростные – не менее 1 Гбит/с для подключения опорных коммутационных узлов федеральных округов Российской Федерации и, частично, для подключения областных коммутационных узлов по субъектам Российской Федерации;

– низкоскоростные – не менее 2 Мбит/с для подключения районных коммутационных узлов.

Услуги связи, как правило, закупаются централизовано у оператора связи, выбираемого на конкурсной основе. Резервные каналы связи для подключения центров обработки данных закупаются централизовано на конкурсной основе у альтернативного оператора связи.

Зона ответственности оператора связи заканчивается на внутреннем порту каналообразующего оборудования на площадке ФОИВ. Таким образом, управление и мониторинг состояния оборудования, находящегося на балансе ФОИВ, осуществляется специалистами ФОИВ.

Отдельным направлением развития ТС как транспортной среды для ИАС в целом, является организация мобильного доступа к ресурсам ИАС [4]. Это позволяет мобильным абонентам ФОИВ получать удаленный доступ к информационным ресурсам ИАС и работать с ними непосредственно на месте проведения мероприятий.

Мобильный доступ абонентов к информационным ресурсам обеспечивается как за счет строительства собственных сетей беспроводного широкополосного доступа, так и с использованием 3G/4G сетей Операторов связи. При необходимости, в удаленных регионах могут быть использованы системы спутниковой связи.

При организации беспроводного доступа к ресурсам Системы особое внимание уделяется вопросам информационной безопасности: предотвращению несанкционированного доступа к информационным ресурсам, утечки информации, в том числе персональных данных граждан Российской Федерации и другой конфиденциальной информации.

Для организации внешнего информационного взаимодействия ФОИВ с гражданами и организациями обеспечивается защищенный шлюз между ТС и сетью Интернет.

Для организации внешнего голосового взаимодействия ФОИВ с гражданами и организациями обеспечивается шлюз между ТС и взаимоувязанной сетью связи Российской Федерации.

Состав и принципы организации автоматизированных рабочих мест пользователей.

Доступ пользователей к централизованным ресурсам ИАС осуществляется при помощи автоматизированных рабочих мест (АРМ). Данные АРМ делятся по типам согласно критериям универсальности и мобильности.

По универсальности АРМ делятся на следующие типы:

– АРМ для работы со специальными приложениями. АРМ данного типа должны удовлетворять критериям защищенности, соответствующим требованиям для работы с информацией, обладающей разной степенью конфиденциальности. Они должны быть унифицированы и не должны зависеть от типа приложения [5];

– универсальные АРМ для работы с обеспечивающими системами. АРМ данного типа оснащаются обеспечивающие подразделения ФОИВ и не могут быть использованы для работы с конфиденциальной информацией;

– универсальные АРМ для работы в сетях общего пользования. АРМ данного типа используются для работы с сетями общего пользования и открытой информацией. Эти АРМ не могут быть использованы для работы вместо АРМ 1-го и 2-го типов.

Для каждого из типов АРМ устанавливаются требования по защищенности информации, согласно степени конфиденциальности информации, обрабатываемой на конкретном типе АРМ.

Каждый из указанных типов АРМ может быть разделен на подтипы, в зависимости от степени мобильности данного АРМ:

– стационарные АРМ – АРМ, не предназначенные для работы за пределами ИАС;

– возимые АРМ – АРМ, предназначенные для работы как в ИАС, так и за ее пределами;

– носимые АРМ – АРМ, предназначенные для работы за пределами ИАС и имеющие возможность подключения к стационарным АРМ.

Для каждого типа АРМ централизованно устанавливаются стандарты на аппаратное и программное обеспечение, входящее в его состав. Стандарты устанавливаются из критериев максимальной унификации АРМ, а также с преимущественным использованием программного обеспечения с открытым кодом и свободно распространяемого программного обеспечения. Стандарты на АРМ там, где это возможно, должны предусматривать отказ от программного обеспечения производства компании Microsoft и переход на программное обеспечение, работающее под управлением ОС Linux. Стандарты на АРМ пересматриваются не чаще одного раза в год, и не реже одного раза в три года.

Срок службы стандартного АРМ составляет, как правило, не менее 5 лет. Критерий устаревания – несоответствие требованиям стандарта на АРМ.

При списании АРМ (в случае морального устаревания или выхода из строя) принимаются меры к уничтожению информации, содержащейся на конкретном АРМ, исходя из типа АРМ.

Стационарные АРМ подключаются к ИАС как правило при помощи проводного соединения.

Носимые и возимые АРМ могут подключаться к ИАС посредством беспроводного соединения, при условии организации защищенного канала связи между АРМ и ИАС, удовлетворяющего требованиям защищенности для конкретного типа АРМ.

Для всех типов стандартизованного программного обеспечения, требующего лицензирования, вне зависимости от типа АРМ, в котором оно используется, вводится система централизованного лицензирования. При этом с производителем программного обеспечения заключается единое, в рамках ФОИВ, соглашение. Использование «пиратского» программного обеспечения и программного обеспечения, лицензированного вне ведомственных договоров, запрещается.

Для обеспечения доступа к централизованным ресурсам ИАС, каждый мобильный пользователь при помощи своего АРМ проходит процедуру

регистрации в системе. При этом регистрация в системе является централизованной и обеспечивает предоставление доступа пользователя ко всем информационным ресурсам, на которые он авторизован при однократной регистрации (Singlesign-on – SSO).

В рамках ИАС предусматривается стандартизация периферийного оборудования. Требования к срокам жизни стандартов аналогичны требованиям к стандартам на АРМ. При этом стандарты должны предусматривать максимальное использование периферийного оборудования, предназначенного для многопользовательской работы и подключаемого непосредственно к ИАС, а не к конкретному АРМ.

Для каждого вида периферийного оборудования устанавливаются нормативы закупки расходных материалов. Нормативы устанавливаются исходя из количества АРМ, использующих конкретный экземпляр оборудования, типа систем, для которого используется оборудование, а также рекомендаций производителя оборудования. Использование расходных материалов, не предусмотренных производителем оборудования, запрещается.

Требования к организации АРМ с ПЭВМ должны соответствовать нормам СанПиН 2.2.2/2.4.1340-03 «Гигиенические требования к персональным электронно-вычислительным машинам и организации работы».

Обслуживание АРМ пользователей, оборудования ИАС объектов и периферийных устройств осуществляется, как правило, силами сторонних организаций, специализирующихся на данном виде услуг, обладающих всеми необходимыми квалификациями и лицензиями. Организации выбираются на конкурсной основе, согласно Законодательству Российской Федерации.

В заключении необходимо отметить, что соблюдение основных принципов создания крупномасштабных ИАС ФОИВ позволяет существенно сократить финансовые и временные затраты, уменьшить риски принятия неэффективных решений и обеспечить надлежащий уровень информационной безопасности системы.

Список литературы:

1 Скрыпников А.В., Берестовой А.А., Никульчева О.С., Зиновьева В.В. Оптимизация информационно-телекоммуникационных систем с использованием нейронных сетей: повышение эффективности и безопасности // Вестник Воронежского института ФСИН России. 2024. № 4. С. 135-139.

2 Пучков Г.Ю. Применение технологий искусственного интеллекта для управления трафиком и предотвращения сбоев и отказов в работе систем передачи данных // Искусственный интеллект. Теория и практика. 2024. № 3 (7). С. 75-77.

3 Ледовских Т.В., Щербакова Е.Н. Требования к устойчивости сетей электросвязи органов государственной власти и подведомственных им организаций // Труды ЦНИИС. Санкт-Петербургский филиал. 2018. Т. 2. № 6. С. 26-34.

4 Пучков Г.Ю., Павелкин Д.П., Киян А.И. Организация крупномасштабных систем подвижной радиосвязи на базе комплекса «АПЕКС» // Электросвязь. 2022. № 9. С. 27-34.
5 Кубасов И.А., Пучков Г.Ю. Основы математической модели надежности функционирования инфокоммуникационных систем внутренних дел российской федерации // Научно-технический портал МВД России. 2022. № 3 (43). С. 12-19.

Сведения об авторе:
Пучков Геннадий Юрьевич, кандидат технических наук, ведущий научный сотрудник ФКУ НПО «СТиС», Москва, Россия
Puchkov Gennady Yuryevich, Candidate of Technical Sciences, Leading Researcher, Federal State Institution Scientific and Production Association, «STiS», Moscow, Russia

УДК 004.42

Окин Г. А., Новоселова О.В.
ФГБОУ ВО "Московский государственный технологический университет "СТАНКИН", Москва, Россия

Модернизация интегрированной среды (ИС-2) для автоматизации проектирования сложных систем

Аннотация. Статья посвящена модернизации архитектуры интегрированной среды (ИС-2), реализующей автоматизацию процесса проектирования сложных систем на основе методологии автоматизации интеллектуального труда (МАИТ). В статье представлен переход от существующего однозвенного приложения к трехзвенной архитектуре для улучшения взаимодействия и масштабируемости системы. Рассматриваются ключевые моменты текущей реализации, такие как автономность работы приложения, его ограниченная функциональность для нескольких пользователей и отсутствие централизованного хранилища проектов. Также обсуждается планирование модернизации в виде монолитного приложения с возможной трансформацией в микросервисы в будущем.

Ключевые слова: методология автоматизации интеллектуального труда, проектирование автоматизированных систем, системное проектирование, трехзвенная архитектура, монолит, микросервисы

Okin G. A., Novoselova O.V.

Modernization of an integrated environment (IS-2) for automating the design of complex systems

Abstract.The article is devoted to the modernization of the architecture of an integrated environment (IS-2), which implements automation of complex systems design processes based on the methodology of intelligent labor automation (ILA). The transition from a single-tier application to a three-tier architecture for improved interaction and scalability is presented in the article. Key aspects of the current implementation are considered, such as the autonomy of the application's operation, its limited functionality for multiple users, and the lack of a centralized project repository. Additionally, plans for modernizing it into a monolithic application with potential transformation into microservices in the future are discussed.

Keywords: methodology of intellectual labor automation, automated systems design, systems design, three-tier architecture, monolith, microservices.

Введение

По мере развития автоматизированных систем и технологий в целом, процесс проектирования различного рода систем становится комплексным, что требует к себе внимания множества различных специалистов и значительных временных затрат. Методология автоматизации интеллектуального труда (МАИТ)[1] описывает системный подход к этому процессу на всех его этапах и предлагает промышленный способ создания автоматизированных систем.

Для реализации методологии, на кафедре ИТиВС МГТУ “СТАНКИН”, была разработана специальная интегрированная среда (ИС-2)[2, 3], которая

позволяет работать с моделями на разных этапах проектирования автоматизированных систем (АС): начальном, концептуальном, инфологическом. На каждом этапе она позволяет формировать статические (информационные) и динамические (функциональные) структуры, взаимоувязанное представление этих структур, а также выполнять их обработку. ИС-2 в нынешнем варианте представляет собой однозвенное приложения для персонального компьютера [4]. Такое решение имеет как свои преимущества, так и недостатки. Далее в статье приведены пояснения на примере концептуальной модели и реализующего его программного решения.

Например, приложение способно функционировать независимо, без подключения к интернету. Однако доступ к нему возможен лишь одному пользователю одновременно, что исключает возможность коллективной работы над одним проектом несколькими разработчиками. Также отсутствуют функции автоматического обновления приложения, поэтому пользователь вынужден устанавливать их вручную. Кроме того, нет централизованного хранилища проектов, каждый из них сохраняется локально на компьютере разработчика. Для расширения возможностей интегрированной среды было решено перенести автоматизированную среду на архитектуру трёхзвенного приложения. В настоящей статье рассматривается предлагаемая архитектура для данного приложения.

Основная часть

При анализе существующего приложения был выделен ряд компонентов, таких как:

Приложение для начального моделирования;

Приложение для концептуального моделирования, которое включает:

построение концептуальной структуры;

построение системы предметных зависимостей;

формирование увязки концептуальной структуры и системы предметных зависимостей;

Приложение для инфологического моделирования.

Структура приложения начального и концептуального моделирования описана в диссертационной работе Гаврилова А.Г.[5] Важно отметить, что текущее приложение имеет модульную структуру, за счет чего является достаточно гибким в плане его модернизации.

Модернизация интегрированной среды (ИС-2) планируется путем реализации трехзвенной архитектуры, включающей клиента, сервер приложений и север баз данных. В настоящее время разработаны клиент и сервер баз данных, в данной работе рассмотрено проектирование сервера приложений и его взаимодействие с другими звеньями.

Следует отметить, что сама МАИТ развивается, и каждый год по методологии публикуются статьи, в которых описаны различные аспекты такие как оптимизация доступов при концептуальном проектировании,

разработка методологии описания графического интерфейса на этапе даталогического моделирования и много другое. Все это говорит о необходимости построения такой структуры сервера приложения, которая бы могла свободно расширяться, путем добавления новых компонентов.

Был проведен анализ существующих подходов к проектированию серверов приложения. Из которого следует что наиболее подходящим подходом при решении поставленной задачи может являться:

монолит;

микросервисы.

На основе этого было принято решение в качестве начальной точки выбрать подход, в котором система представляет собой монолитное приложение. Однако стоит учесть то, что в будущем потребуется трансформировать этот монолит в набор микросервисов[7,8,9]. Что накладывает определенные ограничения на связность монолита.

Для конечного пользователя интегрированная среда должна представлять простое приложение, как рисунке 1.

Рисунок 1. Контекст использования клиентом будущей системы интегрированной среды

Систему могут использовать клиенты, которые будут работать над так называемыми проектами. Сама по себе система интегрированной среды на данном рисунке является квази - элементарной. То есть на данном рисунке не отображены конкретные детали работы над проектом, а отображен сам факт того, что система используется для работы с проектами.

Детали системы отображены на рисунке 2.

Рисунок 2. Структура системы интегрированной среды

Система будет состоять из нескольких компонентов, таких как:
клиентского приложения;
балансировщика нагрузки;
приложения интегрированной среды;
базы данных.

Каждый из компонентов представляет собой отдельный сервис или приложения, при этом компоненты общаются между собой по различным каналам. В данном случае используя протокол передачи гипертекста HTTP[10], используя при этом JSON в качестве структур, которые передаются по HTTP.

На данный момент существует клиентское приложение ИС-2, оно реализовано на языке C++, с помощью фреймворка QT. Предполагается его модернизировать таким образом, чтобы в зоне ответственности этого компонента осталась логика отображения моделей, таких как начальная структура, концептуальная структура и система предметных зависимостей.

Клиентское приложение будет вызывать API сервера приложений, путем отправки на него HTTP запроса. Запросы приходят на сервер, проходя через API gateway, который в первой реализации будет выполнять роль балансировщика нагрузки [6]. Данный компонент обязателен, так как система должна быть предназначена для работы со многими пользователями. Также данный компонент в будущем может использоваться для:

авторизации и аутентификации;
направления запросов в нужные сервисы, когда монолит будет разделен на множество микросервисов.

Балансировщик нагрузки, как уже было сказано ранее, будет направлять запросы на сервер приложения. Следует помнить о том, что речь идет о работе с множеством пользователей, поэтому инстансов, копий приложения, приложения должно быть несколько, следовательно, балансировщик должен знать их конечные адреса для направления запроса в нужную точку.

Итак, запрос прошел балансировщик нагрузки и был направлен в монолит – Приложение интегрированной среды. Само приложение представляет сервер, который может обрабатывать HTTP трафик. Он состоит из нескольких компонентов - структура приложения приведена на рисунке 3.

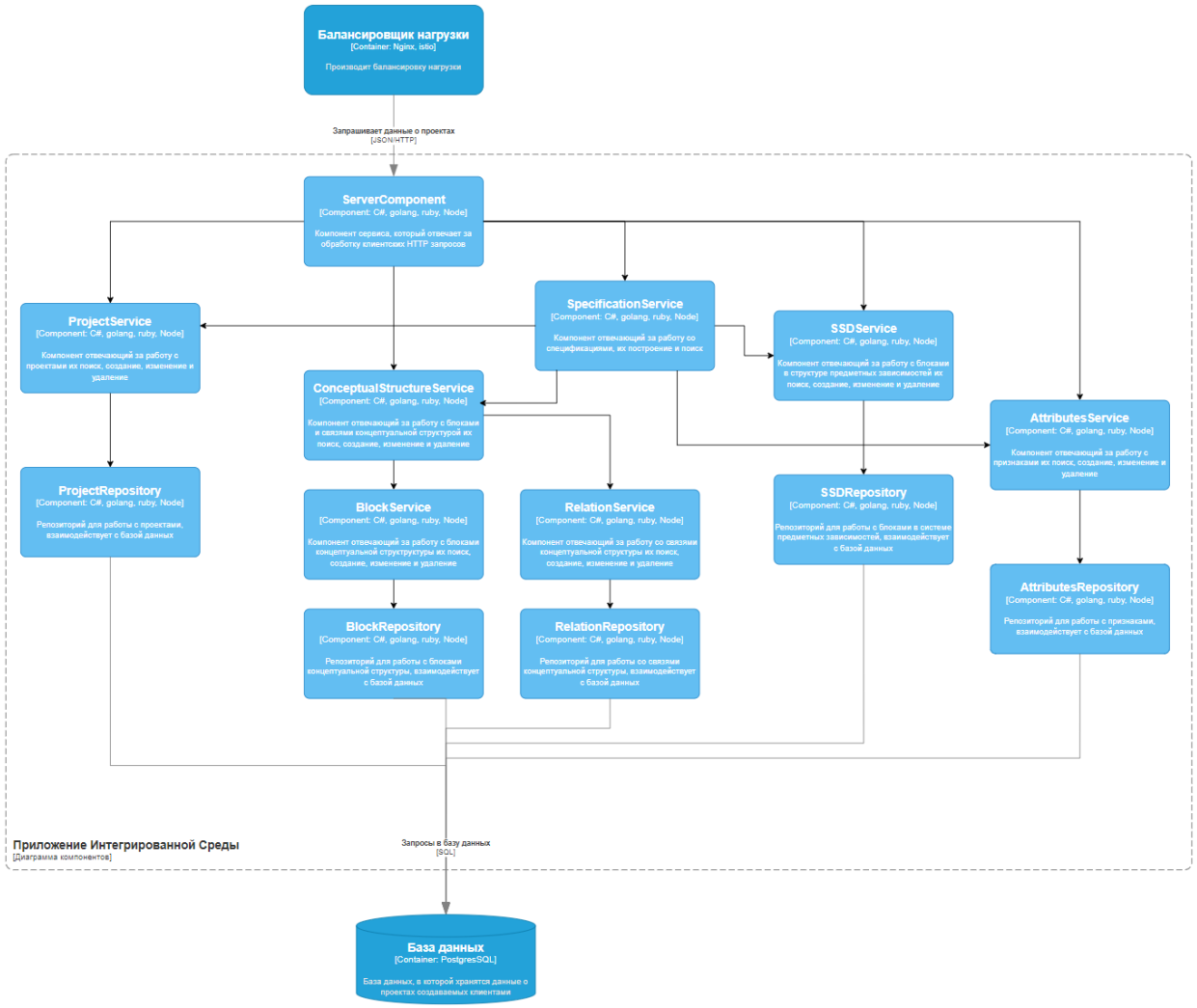

Рисунок 3. Структура приложения интегрированной среды

Приложение будет представлять собой совокупность компонентов, каждый из которых будет обладать определенной ответственностью. Это позволит уменьшить связность, так как в будущем монолит будет разбит на множество микросервисов. Все компоненты можно поделить на три больших группы:

компонент сервис;

компонент репозиторий;

служебный компонент.

В компонентах сервисах будет находиться бизнес-логика работы приложения, построение различных структур, обработка ошибок и так далее. Такие компоненты могут вызывать репозитории, в которых будет лежать логика работы с базой данных. А также могут вызывать другие компоненты сервисы.

К компонентам сервисам относятся:

ProjectService – компонент предназначен для работы с сущностью проекта - его создание, редактирование и удаление, а так же поиск;

ConceptualStructureService – компонент, отвечающий за работу с концептуальной структурой, поиском, созданием, редактированием, удалением блоков и связей. Компонент может вызывать:

BlockService;

RelationService.

SSDService – компонент для работы с блоками в структуре предметных зависимостей;

AttributeService – компонент по поиску, созданию, редактированию и удалению признаков;

SpecificationService – компонент предоставления различного рода спецификаций, а так же матричной диаграммы. Может вызывать все вышеописанные компоненты, так как для его работы необходима практически вся информация о проекте;

BlockService – компонент, отвечающий за работы с блоками концептуальной структуры их поиск, создание, редактирование и удаление;

RelationService – компонент работы со связями в концептуальной структуре, его зона ответственности - это поиск, создание, редактирование и удаление связей между блоками концептуальной структуры.

Все компоненты сервисы могут вызывать компоненты репозитории, в них будет содержаться логика по работе с базой данных, сформированные SQL запросы, валидация данных перед записью в базу данных. К таким компонентам относятся:

ProjectRepository;

BlockRepository;

RelationRepository;

SSDRepository;

AttributeRepositoty.

Данный подход позволяет упростить тестирование, так как при написании тестов можно будет подменять различные компоненты без их инициализации. Также у каждого компонента будет свой интерфейс, который позволит в будущем переносить функционал отдельных компонентов сервисов в отдельные микросервисы, благодаря интерфейсу компонента.

Служебные же компоненты необходимы для осуществления различных функций, связанных с работой системы. На данный момент это будет один компонент – ServerComponent. Он предназначен для развертки HTTP сервера, который будет принимать клиентские запросы. Также данный модуль будет содержать логику соединения URI запроса на конкретную функцию в коде, которая будет осуществлять бизнес-логику.

Как видно из рисунка 3, система содержит компонент базы данных. В нашем случае схемы БД уже разработаны и известны, поэтому база данных должна быть реляционной. С поддержкой репликации и шардирования.

Заключение

Предложенный проект сервера приложений в трехзвенной архитектуре позволит расширить возможности при работе с интегрированной средой ИС-2 - организовать коллективную работу над проектами, централизованное хранилище проектов и др. Предусмотрено, что в дальнейшем можно будет перевести монолитное решение на микросервисное при необходимости, что обеспечит более легкое масштабирование и развертывание интегрированной среды, гибкость при дополнении функциональности, оптимальное использование ресурсов.

Список литературы

1. Волкова, Г.Д. Методология автоматизации проектно-конструкторской деятельности в машиностроении: учеб. пособие. – М. : МГТУ «СТАНКИН», 2000. – 81 с.
2. Гаврилов, А. Г. Инструментальная среда поддержки процессов создания систем автоматизированного проектирования / А. Г. Гаврилов, Г. Д. Волкова, О. В. Новоселова // Информационные технологии в проектировании и производстве. – 2018. – № 2. – С. 30-36.
3. Гаврилов, А. Г. Инструмент проектирования информационно-активных систем интегрированная среда «ИС-2» / А. Г. Гаврилов, Г. Д. Волкова, О. В. Новоселова // Моделирование нелинейных процессов и систем (MNPS-2020): материалы пятой международной конференции. – М. : Янус-К, 2021. – С. 129-130.
4. Гаврилов А.Г., Волкова Г.Д., Новоселова О.В. Программный комплекс «ИС-2» и его особенности // Цифровая экономика: технологии, управление, человеческий капитал [Текст]: материалы III всероссийской научно-практической конференции, г. Вологда, 25 сентября 2020 г. – Вологда: ООО «Маркер», 2020. – 80 с. – С. 10-13.
5. Гаврилов, А. Г. Разработка метода моделирования и средств поддержки управления развитием визуальной интегрированной среды проектирования автоматизированных систем: специальность 23.10.00: диссертация на соискание ученой степени кандидата технических наук / Гаврилов Андрей Геннадьевич, 2022. – 224 с. – EDN IOCDAF.
6. Клеппман, М. Высоконагруженные приложения. Программирование, масштабирование, поддержка / М. Клеппман. – СПб.: Питер, 2019. – 640 с.
7. Мартин, Р. Чистая архитектура. Искусство разработки программного обеспечения. – М.: Вильямс, 2020. – 352 с.
8. Фаулер, М. Рефакторинг: улучшение проекта существующего кода. – М.: Символ-Плюс, 2019. – 432 с.
9. Architectural Styles and the Design of Network-based Software Architectures. [Электронный ресурс]. – 2000. – URL: https://www.ics.uci.edu/~fielding/pubs/dissertation/top.htm (дата обращения: 21.12.2024).
10. Стандарт HTTP. [Электронный ресурс]. – 2025. – URL: https://datatracker.ietf.org/doc/html/rfc2616 (дата обращения: 22.12.2024).

Сведения об авторах:
Окин Григорий Андреевич: магистрант «Информационные технологии и вычислительные системы», ФГБОУ ВО "Московский государственный технологический университет "СТАНКИН", Москва, Россия
Новоселова Ольга Вячеславовна: заведующий кафедрой «Информационные технологии и вычислительные системы» ФГБОУ ВО "Московский государственный технологический университет "СТАНКИН", Москва, Россия
Okin Grigory Andreevich: Graduate Student, Department of Information Technologies and Computing Systems Moscow State University of Technology "STANKIN", Moscow, Russia
Novoselova Olga Vyacheslavovna: Head of the Department, Department of Information Technologies and Computing Systems Moscow State University of Technology "STANKIN", Moscow, Russia

УДК 681.3.053

Ильюшкин А.С.
Санкт-Петербургский государственный университет телекоммуникаций им. проф. М.А. Бонч-Бруевича, Санкт-Петербург, Россия

Сравнительный анализ алгоритмов обработки видеоизображений для автоматического распознавания подозрительного поведения

Аннотация. В статье проведен сравнительный анализ алгоритмов обработки видеоизображений для автоматического распознавания подозрительного поведения. Рассмотрены методы вычитания фона, оптического потока, сверточных нейронных сетей и инкрементного обучения. Оценена их эффективность, вычислительная сложность и области применимости. Особое внимание уделено гибридным подходам, сочетающим традиционные алгоритмы и методы глубокого обучения. Выявлены преимущества и ограничения каждого метода, а также возможности их использования в системах безопасности для повышения точности обнаружения аномального поведения

Ключевые слова: Автоматическое распознавание, обработка видеоизображений, подозрительное поведение, нейросети, глубокое обучение, оптический поток, инкрементное обучение, компьютерное зрение, аномалия, видеонаблюдение, безопасность, идентификация объектов, машинное обучение, алгоритмы детекции

Ilyushkin A.S.

Comparative analysis of video image processing algorithms for automatic recognition of suspicious behavior

Abstract. The paper presents a comparative analysis of video image processing algorithms for automatic recognition of suspicious behavior. The methods of background subtraction, optical flow, convolutional neural networks and incremental learning are considered. Their efficiency, computational complexity and areas of applicability are evaluated. Special attention is paid to hybrid approaches combining traditional algorithms and deep learning methods. The advantages and limitations of each method are identified, as well as the possibilities of their use in security systems to improve the accuracy of anomalous behavior detection.

Keywords: Automatic recognition, video image processing, suspicious behavior, neural networks, deep learning, optical flow, incremental learning, computer vision, anomaly, video surveillance, security, object identification, machine learning, detection algorithms.

В современном мире системы видеонаблюдения играют ключевую роль в обеспечении безопасности общественных и частных пространств. С развитием технологий обработки видеоизображений и искусственного интеллекта (ИИ) стало возможным автоматическое распознавание подозрительного поведения, что значительно повышает эффективность превентивных мер и оперативного реагирования на потенциальные угрозы. Однако разнообразие существующих алгоритмов и методов требует тщательного анализа их эффективности и применимости в различных условиях. Цель данной статьи — провести сравнительный анализ алгоритмов

обработки видеоизображений для автоматического распознавания подозрительного поведения, выявить их преимущества, недостатки и области оптимального применения.

В последние годы проведено множество исследований, посвященных разработке и совершенствованию алгоритмов автоматического распознавания подозрительного поведения на основе анализа видеоизображений. Одним из ключевых направлений является использование методов обнаружения аномалий, позволяющих выявлять отклонения от нормального поведения в наблюдаемых сценах.

В работе Шкодырева В.П., Ягафарова К.И. и Баштовенко В.А. «Обзор методов обнаружения аномалий в потоках данных» (2017) представлен детальный анализ различных подходов к идентификации аномалий во временных рядах [1]. Авторы классифицируют аномалии на точечные, контекстуальные и коллективные, что позволяет более точно выбирать соответствующие методы для их обнаружения. Особое внимание уделено методам, основанным на статистическом анализе и машинном обучении, которые демонстрируют высокую эффективность в условиях больших объемов данных и динамически изменяющихся параметров среды. Данное исследование подчеркивает важность правильного выбора модели для конкретных задач мониторинга и безопасности.

В другой работе, выполненной Шаталиным Р.А., Фидельманом В.Р. и Овчинниковым П.Е., «Инкрементное обучение алгоритма обнаружения нехарактерного поведения на основе главных компонент» (2020), предложена схема инкрементного обучения для алгоритмов, основанных на методе главных компонент [2]. Авторы акцентируют внимание на необходимости адаптации моделей в реальном времени при поступлении новых данных, что особенно актуально для систем видеонаблюдения в динамичных условиях. Результаты экспериментов показывают, что предложенный подход позволяет существенно сократить время обучения без значительной потери точности обнаружения аномалий. Это исследование подчеркивает значимость разработки адаптивных алгоритмов, способных быстро реагировать на изменения в наблюдаемой среде.

Оба рассмотренных исследования вносят значительный вклад в область автоматического распознавания подозрительного поведения, предлагая эффективные методы и алгоритмы для обнаружения аномалий в видеопотоках.

Далее рассмотрим алгоритмы обработки видеоизображений, направленные на автоматическое распознавание подозрительного поведения, и приведём их математическое обоснование.

Одним из базовых этапов является выделение динамических объектов в видеопотоке. Пусть $I(t, x, y)$ — яркостное значение пикселя в кадре, полученном в момент времени t в позиции (x, y). Для устранения статического фона часто используется метод вычитания фона [3]. Пусть

$B\ (x,y)$ — модель фона, которая может быть оценена, например, как медианное значение яркости для каждого пикселя на протяжении некоторого

$$B(x,y) = median\{I(t,x,y)\}_{t=1}^{N} \quad 1)$$

временного интервала, что отображено в формуле 1:

$$D\ (t,x,y) = |I(t,x,y) - B(x,y)| \quad 2)$$

Определим разностное изображение в формуле 2:

После применения пороговой функции Θ для устранения шумов получаем бинарную маску выделения движущихся объектов, что выражено в

$$M(t,x,y) = \Theta(D(t,x,y) - T) \quad 3)$$

формуле 3:

Где T — порог, определяемый эмпирически или с помощью методов адаптивной пороговой обработки.

Следующим этапом является извлечение динамических характеристик. Один из распространенных методов — вычисление оптического потока. Пусть в окрестности точки (x,y) движение описывается вектором $v(x,y) = \big(u(x,y), v(x,y)\big)$. Метод Лукаса-Канаде основывается на предположении, что интенсивность пикселя сохраняется при движении, что

$$I\ (t,x,y) = I(t + \Delta t, x + u\Delta t, y + v\Delta t) \quad 4)$$

отображено в формуле 4:

Линейное приближение приводит к уравнению, которое выражено в

$$I_x(x,y)u(x,y) + I_y(x,y)v(x,y) + I_t(x,y) = 0 \quad 5)$$

формуле 5:

Где I_x, I_y и $, I_t$ — частные производные по координатам и времени соответственно. Решение системы таких уравнений в малой окрестности позволяет оценить вектор движения, что является важным признаком динамики объектов.

Для классификации поведения выделенные объекты подвергаются анализу с использованием методов машинного обучения. Одним из наиболее эффективных подходов является применение сверточных нейронных сетей (CNN). Пусть на вход сети подается фрагмент видео $P \in R^{H \times W \times C}$, где H и W — высота и ширина кадра, C — число каналов [4]. На первом слое сети

осуществляется свертка с ядром K и смещением b, что отображено в

$$F(x,y) = \sigma(\sum_{i,j} K(i,j) \times P(x+i, y+j)) \quad 6)$$

формуле 6:

Где σ — функция активации, например, ReLU. На выходе сети применяется софтмакс-классификация, которая позволяет оценить вероятность того, что поведение объекта является подозрительным, что

$$p_i = \frac{e^{z_i}}{\sum_j e^{z_j}} \quad 7)$$

отображено в формуле 7:

Где z_i — выходное значение для i-го класса. Таким образом, с учетом пространственно-временной информации и динамических характеристик, алгоритмы могут эффективно различать нормальное и аномальное поведение.

Кроме того, для повышения точности распознавания часто применяются методы инкрементного обучения, позволяющие адаптировать модель к изменяющимся условиям видеонаблюдения. Например, инкрементное обновление весов нейронной сети может осуществляться с использованием стохастического градиентного спуска (SGD) по функции потерь L, что

$$w_{t+1} = w_t - \eta \nabla_w L(w_t, P_t) \quad 8)$$

представлено в формуле 8:

Где w_t — вектор весов на шаге t, η — скорость обучения, а P_t — подмножество обучающих данных, отражающее текущую динамику видеопотока.

Далее проведем сравнительный анализ рассмотренных алгоритмов обработки видеоизображений для автоматического распознавания подозрительного поведения, учитывая их точность, вычислительную сложность и область применимости, что отображено в таблице 1 ниже.

Таблица 1 - Сравнительный анализ алгоритмов обработки видеоизображений для автоматического распознавания подозрительного поведения.

Алгоритм	Преимущества	Недостатки	Область применимости
Вычитание фона	Простота реализации, высокая скорость обработки, подходит для статичных сцен	Чувствителен к изменению освещения, трудно применять в динамических сценах	Видеонаблюдение в статичных зонах

Алгоритм	Преимущества	Недостатки	Область применимости
Оптический поток	Позволяет детектировать движение объектов независимо от сцены	Высокая вычислительная сложность, трудно обрабатывать быстрые движения	Анализ движений в реальном времени
Алгоритм	Преимущества	Недостатки	Область применимости
Сверточные нейронные сети (CNN)	Высокая точность классификации, способность к обучению, применимы в сложных сценах	Требуют больших объемов данных и вычислительных ресурсов	Распознавание сложных паттернов поведения
Инкрементное обучение (SGD)	Адаптация к новым данным, уменьшение необходимости переобучения	Может привести к деградации модели при неконтролируемом обновлении	Динамические системы безопасности

Проведенный анализ показывает, что выбор алгоритма для автоматического распознавания подозрительного поведения зависит от условий применения и требований к точности и скорости обработки. Традиционные методы, такие как вычитание фона и оптический поток, остаются эффективными в задачах мониторинга простых сцен, однако они не обладают достаточной адаптивностью для сложных и динамически изменяющихся условий.

Современные алгоритмы машинного обучения, особенно сверточные нейронные сети, обеспечивают высокую точность распознавания сложных аномалий, но требуют значительных вычислительных ресурсов и предварительного обучения на больших массивах данных [5]. Инкрементное обучение может частично решить эту проблему, позволяя моделям адаптироваться к новым сценариям без необходимости полного переобучения.

Оптимальным подходом для реальных систем безопасности является комбинация традиционных методов обработки изображений с глубоким обучением, что позволяет эффективно извлекать динамические признаки движения, а затем классифицировать их с помощью нейросетевых моделей. Такой гибридный подход способен обеспечивать баланс между вычислительной эффективностью и точностью распознавания, что делает его перспективным направлением для дальнейших исследований и практического внедрения в интеллектуальные системы безопасности.

Список литературы

1. Шкодырев В.П., Ягафаров К.И., Баштовенко В.А. Обзор методов обнаружения аномалий в потоках данных // CEUR Workshop Proceedings. 2017. Т. 1864. С. 286-297. URL: https://ceur-ws.org/Vol-1864/paper_33.pdf (дата обращения: 20.02.2025).

2. Шаталин Р.А., Фидельман В.Р., Овчинников П.Е. Инкрементное обучение алгоритма обнаружения нехарактерного поведения на основе главных компонент // Компьютерная оптика. 2020. Т. 44, № 3. С. 454-460. DOI: 10.18287/2412-6179-CO-644. URL: https://www.computeroptics.ru/KO/PDF/KO44-3/440320.pdf (дата обращения: 20.02.2025).

3. Орлов Г. А., Красов А. В., Гельфанд А. М. Применение Big Data при анализе больших данных в компьютерных сетях //Наукоемкие технологии в космических исследованиях Земли. – 2020. – Т. 12. – №. 4. – С. 76-84.

4. Пашкевич А.Д., Абламейко С.В. Определение направления движения группы людей на видео на основе вычисления оптического потока нейронной сетью // Белорусская академия связи. URL: https://belai.by/ru/research/opredelenie-napravleniya-dvizheniya-gruppy-lyudej-na-video-na-osnove-vychisleniya-opticheskogo-potoka-nejronnoj-setyu/ (дата обращения: 23.02.2025).

5. Бекназарова С.С., Мухамадиев А.Ш., Жаумытбаева М.К. Интеллигентные видео системы: Учебное пособие. – Ташкент: ТУИТ им. Мухаммада аль-Хорезми, 2020. URL: https://lib.tiet.uz/file/20220813092445.pdf (дата обращения: 27.02.2025

Сведения об авторе:
Ильюшкин Александр Сергеевич, магистр, Санкт-Петербургский государственный университет телекоммуникаций им. проф. М.А. Бонч-Бруевича, Санкт-Петербург, Россия
Ilyushkin Alexander Sergeevich, Master's Degree, Department of Information Security St. Petersburg State University of Telecommunications named after Prof. M.A. Bonch-Bruevich Saint Petersburg, Russia

УДК 632.15

Ялалова З.Р., Салихова Р.Р.
Казанский государственный энергетический университет, Казань, Россия

Устойчивые практики в теплоснабжении: выгоды от экологически чистой организации производства

Аннотация: Теплоснабжение остается важным фактором внедрения современных городов, однако традиционные методы производства тепла, основанные на ископаемом топливе, становятся все менее устойчивыми в условиях климатических изменений и роста тарифов. Переход к экологически чистым практикам в этой сфере открывает новые возможности, снижает затраты, повышает эффективность и создает долгосрочные конкурентные преимущества. В данной статье рассматриваются основные устойчивые технологии в теплоснабжении — от использования возобновляемых источников энергии до цифровизации систем управления — и их влияние на аварийные предприятия и регионы. Например, проекты из Европы, Северной Америки и Азии, такие как «зеленые» решения, сокращают выбросы углерода, оптимизируют ресурсы и развивают новые рынки. Особое внимание уделяется государственной политике, механизмам финансирования и преодолению препятствий на пути развития инноваций. Исследование доказывает, что устойчивая организация производства тепла не только соответствует глобальным экологическим тенденциям, но и становится драйвером экономического роста, связанного с деятельностью предприятий и повышением качества жизни населения.
Ключевые слова: теплоснабжение, производство, экология, цифровизация, экономические выгоды.

Yalalova Z.R., Salikhova R.R.

Sustainable heat supply practices: benefits from an environmentally friendly production organization

Abstract: Heat supply remains an important factor in the introduction of modern cities, but traditional methods of heat production based on fossil fuels are becoming less sustainable in the face of climate change and rising tariffs. The transition to environmentally friendly practices in this area opens up new opportunities, reduces costs, increases efficiency and creates long-term competitive advantages. This article examines the main sustainable technologies in heat supply — from the use of renewable energy sources to the digitalization of control systems — and their impact on emergency enterprises and regions. For example, projects from Europe, North America, and Asia, such as green solutions, reduce carbon emissions, optimize resources, and develop new markets. Special attention is paid to public policy, financing mechanisms and overcoming obstacles to the development of innovation. The study proves that the sustainable organization of heat production not only corresponds to global environmental trends, but also becomes a driver of economic growth associated with the activities of enterprises and improving the quality of life of the population.
Keywords: heat supply, production, ecology, digitalization, economic benefits.

Введение

Теплоснабжение — это кровеносная система современных городов, от которой зависят комфорт миллионов людей. Однако традиционные методы производства тепла, основанные на сжигании угля, газа или газа, сегодня сталкиваются с тройным кризисом: экологическим, экономическим и энергетическим. Выбросы CO_2, растущие тарифы и зависимость от импортного топлива заставляют общество пересматривать подходы к организации этого сектора. Надежные методы, сочетающие экологичность и эффективность, обеспечивают выход из тупика, превращение теплоснабжения из проблем в экономические возможности.

Главный парадокс традиционных систем — их расточительность. По данным Международного энергетического агентства (МЭА), до 30% тепла происходит в изношенных сетях, а КПД многих котельных не достигает 60%. Это приводит к перерасходу топлива, росту себестоимости и удорожанию услуг для конечных потребителей. Экологически чистая организация производства начинается с ограничения этих потерь.

Традиционное производство часто напоминает черный ящик: на входе — тонны сырья и энергии, на выходе — продукт и сложные процессы. По данным ООН, промышленность несет ответственность за 20% мировых выбросов CO_2 и 54% общего потребления энергии. Однако технологии и инновационные подходы позволяют перевернуть эту парадигму. Например, концепция «циркулярной экономики», где на каждом этапе жизненного цикла продукт проектируется для повторного использования, уже есть такие отрасли, как текстильное производство и строительство. Компания Patagonia, перерабатывая старую одежду в новую, сокращает потребление воды на 80% и увеличивает прибыль на 30% за счет лояльности экосознательных потребителей [1].

Ключевым элементом устойчивого производства становится энергоэффективность. Замена устаревшего оборудования, установка IoT-датчиков для расходов и использование возобновляемых источников энергии (ВИЭ) — базовые шаги. На заводе Siemens в Людвигсхафене умные системы управления снизили энергопотребление на 20%, а солнечные панели обеспечивают 40% потребностей предприятия. В Дании концерн Novo Nordisk полностью перешел на ВИЭ, сократив расходы на углеродные квоты в размере 12 миллионов евро в год. Однако настоящий прорыв происходит там, где производство интегрируется с учетом требований. Завод BMW в Лейпциге использует сбор дождевой воды — сбор дождевой воды для охлаждения станков, экономя 30 миллионов литров в год.

Еще один пласт — переосмысление отходов. В мире, где 91% пластика не перерабатывается, компании ищут способы превратить мусор в ресурс. Adidas совместно с Parley for the Oceans выпускает кроссовки из переработанного океанского пластика, продав 30 миллионов пар за 5 лет.

Но инновации идут дальше: шведская фирма Renova разработала «биоразлагаемый асфальт», одновременно переработанные подгузники, а голландский стартап Ocean Cleanup создал барьеры для сбора пластика в реках, предотвращая попадание 80 тыс. тонн отходов в океан. Такие решения не только экологичны, но и рентабельны — рынок переработанных материалов к 2030 году достигнет $500 млрд [2].

Сырьевая база — еще один фронт изменений. Производители отказываются от использования консервативных материалов в медицинских целях. Итальянская компания Orange Fiber выпускает ткани из цитрусовых отходов, которые использует Gucci для коллекции аксессуаров. В строительстве набирают популярность «живые» материалы: американский стартап Ecovative производит упаковки и мебель из грибных мицелий, разлагающиеся в течение месяца. Эти доказательства показывают, что природа может быть не только следствием, но и вдохновением для технологий.

Государственная политика играет ключевую роль в ускорении преобразований. Директива ЕС об энергоэффективности обязывает предприятия снижать энергопотребление на 3% в год, «зеленый курс» США стимулирует инвестиции в экопроизводство посредством налоговых льгот. Однако наиболее эффективны меры, сочетающие регуляторику и поддержку. В программе Top Runner установлены динамичные японские стандарты для техники: каждый новый продукт должен быть эффективным. Это подтолкнуло компанию вроде Panasonic к созданию приборов наблюдения с двойным включением энергопотребления.

Экономические выгоды экологически чистого производства часто недооцениваются. Помимо прямой экономии на ресурсах и штрафах, компании получают доступ к «зеленым» финансам. Согласно исследованию Moody's, предприятия с переменами ESG-рейтингами привлекают кредиты на 0,5–1% дешевле. Кроме того, сопротивление становится маркетинговым явлением: 66% потребителей готовы платить больше за экотовары. Бренд Lush, отказавшийся от пластиковой упаковки, увеличил продажи на 40% даже при росте цен.

Критики утверждают, что экологичность — привилегия крупных корпораций. Но малый бизнес тоже не находит ниши. Британская фирма BrewDog стала углеродно-нейтральной, высадив лес на 2 тыс. тонн. Акров, индийская FabIndia продвигает одежду из органического сырья, захватив 15% рынка. Технологии ограничения порога входа: Платформа Circularise позволяет малым производителям отслеживать поставки цепочек через подвеску, гарантируя прозрачность.

Будущая экологическая безопасность производства зависит от трех факторов: технологий, регулирования и потребительского света. К 2030 году 70% новых промышленных объектов, по прогнозам McKinsey, будут построены с учетом регулирования циркулярной экономики. Уже сегодня

такие гиганты, как Apple и Tesla, демонстрируют успех, устойчивость которого совместима с прибылью. Но настоящая революция произойдет, когда экологичность не станет исключать такую норму, как электричество или Интернет.

Экологически чистая организация производства — это не жертва ради планеты, инвестиции в будущий бизнес. Она меняет правила игры, предусматривающие переосмысление каждого процесса — от сырья до упаковки. Как показывают опытные лидеры, будь то крошечный стартап или транснациональная корпорация, поддержка открывает двери к инновациям, экономии и лояльности. В мире, где ресурсы истощаются, климат становится непредсказуемым, единственный способ выжить — стать частью проблемы и стать частью решения.

Результаты исследования

Один из ключевых трендов — переход к возобновляемым источникам энергии (ВИЭ). Геотермальные станции, солнечные тепловые коллекторы и биогазовые установки постепенно вытесняют угольные котлы. В Исландии, где 90% земель отапливается за счет геотермальной энергии, стоимость тепла для населения на 40% ниже, чем в странах ЕС, использующих газ. В шведском городе Векшё, полностью перешедшем на биотопливо из древесных отходов, выбросы CO_2 от теплоснабжения сократились на 95% за 20 лет, что привлекло в регион инвестиции в «зеленые» технологии на сумму более 500 миллионов евро [3].

Однако сейчас революция запускает цифровизацию. Внедрение IoT-датчиков, AI-алгоритмов для прогнозирования солнечной энергии и цифровых двойников теплосетей позволяет оптимизировать производство в режиме реального времени. В газовой компании Fortum используется система на базе искусственного интеллекта, которая анализирует погоду, графики работы предприятий и даже поведение жителей, корректируя температуру в трубах. Это снизило потребление энергии на 15%, затраты на обслуживание — на 25%. В быстром запуске BrainBox AI внедрил аналогичный метод в 100 школах Монреаля, сократив их расходы на отопление на 1,2 миллиона долларов в год.

Экономические выгоды от таких решений лежат в основе прямых последствий издержек. Во-первых, «зеленое» тепло становится конкурентным преимуществом для регионов. В Польше, где 70% теплоснабжения по-прежнему зависит от угля, города, внедрившие солнечные тепловые станции (как Краков), отмечают приток туристов и бизнеса, ориентированного на ESG-принципы. Во-вторых, устойчивые практики создают новые рынки. В Норвегии компании, производящие биогаз из определенных отходов, к 2025 году планируют закрыть 20% энергии на тепло, создав 10 тыс. рабочие места. Наконец, сокращение импорта топлива улучшит торговый баланс. Украина, заменившая 30% российского газа биомассой, сэкономила $1,5 млрд за 5 лет [4].

Государственная поддержка остается решающим фактором успеха. Механизмы варьируются от прямых субсидий (в США программа IRA покрывает 30% затрат на геотермальные тепловые насосы) до налоговых льгот. В Китае соблюдаются «зеленые тарифы», гарантирующие высокие цены на тепло из ВИЭ, а в Японии вводятся штрафы за котельные, превышающие нормы ЕС. Однако наиболее эффективны комплексные стратегии. В Нидерландах закон обязывает все муниципалитеты к 2030 году перевести 50% теплоснабжения на устойчивые источники, параллельно финансируя НИОКР в области водородных котлов и тепловых аккумуляторов.

Несмотря на прогресс, существуют препятствия. Высокие капитальные затраты отпугивают малые предприятия: строительство геотермальной станции мощностью 10 МВт обходится в 20–30 млн евро. Решением становятся модели совместного финансирования. В Германии созданы энергетические кооперативы, где жители объединяют средства для прогрессивных локальных сетей, получая затем дивиденды от экономии. Другая проблема — отсутствие квалифицированных кадров. В результате эту задачу решают с помощью программы «Тепло 4.0», обучающие инженеров работают с цифровыми платформами и возобновляемыми технологиями [5].

Важным элементом участия теплоснабжения становится интеграция с другими отраслями. «Умные» сети, объединяющие ТЭЦ, солнечные панели и аккумуляторы, позволяют продавать избытки энергии в пиковые часы. В Копенгагене система теплоснабжения связана с ветропарками: при сильном ветре электроэнергия направляется на нагрев воды в накопителях, что снижает потребность в газе зимой. Такие проекты повышают устойчивость энергосистем.

Особый интерес представляют местные решения. В результате климатических изменений компания Husk Power устанавливает мини-ТЭЦ на биомассе, обеспечивающую более дешевое тепло и электричество в 300 деревень. Это не только сократило вырубку леса на дрова, но и создало 2 тыс. руб. рабочих мест по сбору сельскохозяйственных отходов. Аналогичные проекты в Кенении и Гане показывают, что устойчивое тепло может стать двигателем развития даже в бедных регионах.

К 2030 году мировой рынок «зеленого» теплоснабжения, по оценке BloombergNEF, достигнет $850 млрд. Уже сейчас компании, внедрившие устойчивые практики, получают преимущества: снижение риска из-за углеродного налога, доступ к «зеленым» кредитам, лояльность клиентов. Однако для массового перехода необходима смена парадигмы мышления — от постепенной экономии к долгосрочным инвестициям. Как показывает опыт Стокгольма, где переход на тепловые насосы с подогревом от Балтийского моря окупился за 7 лет, такие вложения способны трансформировать не только предприятия, но и весь регион [6].

Заключение

В заключение, устойчивое теплоснабжение — это не утопия, а прагматичный выбор. Оно вкладывает затраты, создает рабочие места и повышает энергонезависимость. Но его успех зависит от синергии технологий, политической воли и содействия обществу к изменениям. Как доказывают кейсы из Скандинавии в Индию, будущее тепло — в умном управлении силой, где экология и экономика становятся союзниками, а не врагами.

Список литературы

1. Балацкий Е.В. Глобальные вызовы четвертой промышленной революции // Terra Economicus. 2019. - № 17(2). С. 6-22.
2. Гашо Е.Г. Предпосылки и приоритеты нового энергетического уклада // Даниловские чтения. Пленарные доклады. 2021. - С. 3-8.
3. Гетманов В.В., Дрождинина А.И. Обоснование концепции энергетической безопасности и устойчивого развития теплоснабжающих предприятий // Вестник МГТУ № 4. 2020. - Т. 9. С. 601-605.
4. Данилов Н.И., Щелоков Я.М. Основы энергосбережения: учебник. Екатеринбург: ГУ СО «Институт энергосбережения». 2024. - 526 с.
5. Ибраимова С.С., Горуновский Г.П. (2015). Перспективы седьмого технологического уклада в России и за рубежом. // Научно-аналитический журнал «Наука и практика» Российского экономического университета им. Г.В. Плеханова. 2022. - № 4 (20). С. 56-62.
6. Каменик Л.Л. Эколого-экономическая сбалансированность - стратегия управления инновационным развитием общества XXI века // Вопросы инновационной экономики. 2023. - № 1. Т. 8. С. 25-38.

Сведения об авторах:
Ялалова Зарема Рузаловна, студент, Казанский государственный энергетический университет, Казань, Россия
Салихова Регина Рафаилевна, преподаватель, к.эк.н., доцент, Казанский государственный энергетический университет, Казань, Россия
Yalalova Zarema Ruslanovna, student, Kazan State Power Engineering University, Kazan, Russia
Salikhova Regina Rafaelevna, lecturer, Candidate of Economics, Associate Professor, Kazan State Power Engineering University, Kazan, Russia

УДК 004

Васильев Б.Я.
UST, г. Бойнтон-Бич, Флорида, США

Способы применения SQL NOSQL баз данных для управляемого данными тестирования (DDT)

Аннотация. Статья посвящена исследованию методов применения реляционных (SQL) и нереляционных (NoSQL) баз данных для организации управляемого данными тестирования (DDT). Рассмотрены преимущества и недостатки каждого типа баз данных, подробно описаны сценарии использования и представлены примеры кода для интеграции данных решений в тестирование. Сделан вывод о целесообразности комбинированного подхода с учетом специфики задач. Наиболее эффективным подходом является комбинированное применение, позволяющее использовать преимущества каждого решения для различных этапов и задач в рамках DDT.
Ключевые слова: Data Driven Testing, SQL, NoSQL, базы данных, автоматизация тестирования, управление тестовыми данными.

Boris Vasilev

Ways to use SQL NOSQL databases for data-driven testing (DDT)

Annotation. The article is devoted to the study of methods of using relational (SQL) and relational (NoSQL) databases for the organization of data-driven testing (DDT). The advantages and disadvantages of each type of database are considered, usage scenarios are described in detail, and code examples for integrating these solutions into testing are presented. The conclusion is made about the expediency of a combined approach, taking into account the specifics of the tasks. The most effective approach is a combined application that allows you to take advantage of each solution for different stages and tasks within the DDT framework.
Keywords: Data Driven Testing, SQL, NoSQL, databases, test automation, test data management.

Цель данной статьи – всесторонне рассмотреть применение SQL и NoSQL баз данных в контексте DDT, выявить их сильные и слабые стороны, предложить практические рекомендации по интеграции и привести конкретные примеры реализации.

Проблема исследования состоит в том, что управляемое данными тестирование (Data Driven Testing, DDT) является одним из наиболее эффективных подходов в автоматизации тестирования программного обеспечения, позволяющим отделить тестовую логику от входных данных. Это значительно повышает гибкость и масштабируемость тестов, обеспечивая возможность проведения множества проверок при минимальном изменении сценариев. Для реализации такого подхода используются различные типы баз данных, среди которых наиболее

популярны SQL и NoSQL решения. Выбор конкретной базы данных существенно влияет на эффективность тестирования, поэтому актуальным является глубокий анализ данных технологий. Исследование основано на обзоре литературы, анализе практических примеров и собственном опыте автора. Были рассмотрены такие SQL базы данных, как MySQL и PostgreSQL, а также NoSQL решения – MongoDB и Redis. Для иллюстрации использовались языки программирования Python и JavaScript[1].

Data-Driven Testing представляет собой подход к тестированию, который использует наборы данных для управления процессом проверки программного обеспечения. Суть DDT заключается в том, что тестовые скрипты создаются с расчётом на извлечение параметров и входных данных из внешних источников, таких как базы данных, файлы XML, Excel, JSON или CSV. Это отделение тестовых данных от логики тестирования упрощает поддержку тестов и делает их более гибкими. Преимущества Data-Driven Testing:

1. Увеличение тестового покрытия

Одним из основных преимуществ DDT является возможность использования различных наборов данных, что ведет к увеличению тестового покрытия. Тестирование с разными входными параметрами позволяет охватить широкий спектр сценариев и комбинаций, что, в свою очередь, помогает выявить проблемы, которые могут возникнуть в реальных условиях эксплуатации.

2. Повторное использование тестовых скриптов

Структурирование тестовых сценариев с учетом их повторного использования значительно экономит время и ресурсы. Разработанные тестовые скрипты можно эффективно применять для различных наборов данных, что упрощает процесс тестирования при изменении требований или добавлении новых функциональных возможностей.

3. Быстрое обнаружение багов

DDT способствует оперативному выявлению ошибок и аномалий в системе. Тестирование различных комбинаций входных данных позволяет разработчикам и тестировщикам быстро находить баги на ранних стадиях разработки. Это, в свою очередь, сокращает время на отладку и повышает общее качество продукта[7].

4. Адаптивность тестов

Благодаря возможности настройки тестов под разные условия и изменения в бизнес-логике, DDT позволяет быстро реагировать на изменения в разработке. Это делает подход особенно ценным в быстро меняющихся условиях Agile-разработки.

5. Упрощение поддержки тестов

Поскольку логика тестирования отделена от данных, обновление тестов становится менее трудоемким процессом. Разработчики могут более

эффективно управлять изменениями, не затрагивая логику тестирования, что способствует повышению общей надежности процесса тестирования.

Разработка программного обеспечения управление данными является одной из ключевых задач, и SQL (Structured Query Language) базы данных занимают в этом процессе важное место. Одной из основных особенностей SQL баз данных является строгая типизация данных и предопределенная схема. Каждая таблица в SQL базе имеет фиксированную структуру, где каждый столбец характеризуется определенным типом данных. Например, в таблице учета пользователей могут быть столбцы для имени, электронной почты и даты рождения, каждый из которых имеет свой тип данных (строка, дата и т.д.). Это создает четкие границы и правила для данных, что особенно важно при проведении тестирования. Предопределенная схема позволяет легко обнаруживать несоответствия и ошибки на этапе разработки, что в свою очередь повышает качество тестирования. SQL базы данных также соответствуют принципам ACID (Atomicity, Consistency, Isolation, Durability), которые являются необходимыми для транзакционных систем. Эти принципы гарантируют сохранность данных и предсказуемость работы базы данных[5].

Использование транзакционной модели в SQL базах данных позволяет сохранять целостность данных и обеспечивает отказоустойчивость. При тестировании это важно, поскольку в процессе выполнения тестов могут возникать ошибки и неполадки. Например, если одна из операций в тесте не может быть выполнена, база данных может быть возвращена в стабильное состояние до начала теста, что предотвращает повреждение данных и гарантирует, что последующие тесты будут выполняться на чистых данных. SQL базы данных имеют возможности для резервного копирования и восстановления, что еще больше укрепляет их надежность. Процессы резервного копирования позволяют сохранять состояния базы данных в определенные моменты времени, что может быть полезно при необходимости откатиться к данным до конкретного теста или при сбоях.

SQL базы данных часто используются в системах, требующих высокой надежности и согласованности данных. К таким системам относятся банковские приложения, бухгалтерские системы, платформы электронной коммерции и другие критичные к данным приложения. Их структура и функциональные возможности идеально подходят для обеспечения целостности тестовых данных в контексте DDT.

Пример работы с SQL базой данных (MySQL):

```
import mysql.connector
def get_test_data():
    conn = mysql.connector.connect(host='localhost', database='test_db', user='user', password='password')
    cursor = conn.cursor()
    cursor.execute("SELECT input, expected FROM test_cases")
```

```
    data = cursor.fetchall()
    conn.close()
    return data
```

В последние годы NoSQL-базы данных становятся все более популярными среди разработчиков и компаний, которым необходимо обрабатывать большие объемы данных с высокой скоростью. В отличие от традиционных реляционных баз данных, NoSQL предлагает более гибкие и адаптивные решения, что представляет особенно большой интерес в условиях быстро меняющихся технологических ландшафтов. Одним из основных преимуществ NoSQL-баз является их гибкость в отношении структуры данных. Они позволяют хранить разные типы данных, начиная от простых пар «ключ-значение» до сложных иерархических структур. Это позволяет разработчикам легко адаптироваться к изменяющимся требованиям проекта, не беспокоясь об изменениях в схеме базы данных[2].

NoSQL-базы данных обладают высокой горизонтальной масштабируемостью, что позволяет легко расширять систему за счет добавления новых узлов в кластер. Это особенно важно для приложений, обрабатывающих большие объемы данных, так как по мере роста нагрузки на систему можно добавлять новые серверы, не останавливая работу существующих. Благодаря этой особенности NoSQL решения, такие как MongoDB, подходят для работы с типичными требованиями больших данных, позволяя обрабатывать миллионы запросов и терабайты информации. Производительность NoSQL-баз данных в большинстве случаев превосходит показатели традиционных реляционных систем. Это связано с тем, что данные в NoSQL-хранилищах часто распределены по множеству узлов, что минимизирует время доступа к данным и увеличивает скорость их обработки. Во многих случаях NoSQL-базы позволяют обрабатывать запросы параллельно, обеспечивая высокую скорость чтения и записи данных[4].

Еще одной значимой особенностью NoSQL-баз является отсутствие жесткого схематизма, который характерен для реляционных систем. Разработчики могут не беспокоиться о предварительном определении структуры данных, что упрощает процесс разработки и изменения приложений. Это предоставляет большую гибкость при оптимизации хранения и обработки данных, особенно в ситуациях, когда структура данных может изменяться со временем.

Нереляционные базы данных (NoSQL) предлагают альтернативный подход к хранению и обработке данных. Они могут быть документными, графовыми, колоночными или ключ-значение. Примеры NoSQL баз — MongoDB, Cassandra и Redis. Примером документо-ориентированной NoSQL-базы является MongoDB. Она хранит записи данных в структурах (документах) и позволяет группировать несколько документов в структуры

(коллекции), которые можно дополнительно объединять в отдельные базы данных. MongoDB применяется для хранения и обработки неструктурированной информации и выяснения закономерностей в больших объемах записей. Формат хранения данных в виде JSON-документов обеспечивает высокую скорость обработки и масштабируемость. Это делает ее идеальным инструментом для быстрой разработки приложений, адаптации тестовых сценариев и сбора аналитики[6].

Пример работы с MongoDB:

```
const { MongoClient } = require('mongodb');
async function getTestData() {
    const client = new MongoClient('mongodb://localhost:27017');
    await client.connect();
    const collection = client.db('test_db').collection('test_cases');
    const data = await collection.find({}).toArray();
    await client.close();
    return data;
}
```

Одним из главных решений, с которыми сталкиваются инженеры, является выбор между реляционными базами данных (SQL) и нереляционными системами (NoSQL). Этот выбор зависит от конкретных требований приложения, объемов данных, нагрузки, а также требований к отказоустойчивости и масштабируемости.

SQL базы данных обеспечивают высокую степень согласованности, что подтверждается принципами ACID (атомарность, согласованность, изолированность, долговечность). Это делает SQL идеальным выбором для приложений, где критически важны финансовые транзакции, например, в банковском деле и бухгалтерии. В таких системах ошибки могут привести к серьезным последствиям, и необходимость строгого контроля над состоянием данных будет определяющей. NoSQL базы данных отлично справляются с полуструктурированными и неструктурированными данными, которые распространены, например, в социальных сетях или IoT-приложениях. Такие системы предоставляют гибкость в хранении и обработке данных, позволяя легко адаптировать структуру под изменяющиеся условия[3].

Таким образом, рассмотренные технологии SQL и NoSQL баз данных имеют существенные отличия, каждое решение имеет свои уникальные преимущества и недостатки. Наиболее эффективным подходом является комбинированное применение, позволяющее использовать преимущества каждого решения для различных этапов и задач в рамках DDT. При применении DDT (Data-Driven Technology) интеграция различных типов баз данных позволяет обеспечить гибкость и адаптивность, которые необходимы для успешной работы в условиях постоянных изменений.

Список литературы

1. Kaner C., Bach J., Pettichord B. Lessons Learned in Software Testing. Wiley, 2002. 2

2. Fowler M., Sadalage P.J. NoSQL Distilled: A Brief Guide to the Emerging World of Polyglot Persistence. Addison-Wesley, 2012. 192 p.

3. Elmasri R., Navathe S.B. Fundamentals of Database Systems. Pearson, 7th Edition, 2015. 1272 p.

4. Jain P., Chauhan R. An Approach to Automate Test Data Generation Using SQL Queries. International Journal of Computer Science, 2015, vol. 12, no. 2, pp. 35–41.

5. Hsieh S., Wang C. A Data-Driven Testing Framework Using MongoDB. IEEE International Conference on Software Quality, Reliability and Security Companion (QRS-C), 2017, pp. 541-544.

6. Куприянчик Е.М., Зудилова Т.В., Ананченко И.В., Осипов Н.А., Осетрова И.С. Сравнительные характеристики SQL и NOSQL СУБД, влияющие на разработку приложений баз данных // Современные наукоемкие технологии. 2022. № 7. С. 74-78; URL: https://top-technologies.ru/ru/article/view?id=39236 (дата обращения: 23.03.2025).

7. Болотников М. А., Ханафиев Н. А., Андреев С. В. NoSQL как логичная замена SQL в современных реалиях // Новые горизонты науки: стратегии и направления развития: сборник научных трудов по материалам Международной научно-практической конференции 14 февраля 2024г. Белгород: ООО Агентство перспективных научных исследований (АПНИ), 2024. С. 29-32. URL: https://apni.ru/article/8488-nosql-kak-logichnaya-zamena-sqlv-sovremennikh

Сведения об авторах:
Васильев Борис Яковлевич, магистр, инженер по тестированию программного обеспечения, UST, Бойнтон-Бич, Флорида, США
Boris Vasilev, master, software quality assurance engineer, UST, City Boynton Beach, Florida, USA

УДК 004.92:338

Абаева А., Мухаммедова Д., Аннаовезова Б., Джарчыева А.
Туркменская государственная школа культуры и искусств, г. Ашхабад, Туркменистан

Цифровая система: концепции, технологии и перспективы

Аннотация. В данной статье представлен детальный анализ систем, основанных на современных технологиях обработки и передачи информации. Рассматриваются фундаментальные принципы их функционирования, ключевые направления технологического развития и возможные перспективы их интеграции в различные сферы деятельности. Особое внимание уделяется вопросам автоматизации, безопасности данных и влиянию инновационных решений на экономику, промышленность и социальную среду.

Ключевые слова: информационные технологии, автоматизация, искусственный интеллект, системы управления, инновации, безопасность данных.

Abaeva A., Mukhammedova J., Annaovezova B., Dzharchyeva A.

Digital System: Concepts, Technologies, and Prospects

Abstract. This article provides a detailed analysis of systems based on modern information processing and transmission technologies. The fundamental principles of their functioning, key technological development directions, and potential prospects for their integration into various fields of activity are discussed. Special attention is given to issues of automation, data security, and the impact of innovative solutions on the economy, industry, and social environment.

Keywords: information technology, automation, artificial intelligence, management systems, innovations, data security.

Введение. В эпоху глобальной трансформации информационные системы играют ведущую роль в формировании нового технологического уклада. Их распространение охватывает все сферы жизни, включая промышленность, науку, здравоохранение, финансовый сектор и государственное управление. Современные системы обработки и хранения информации представляют собой сложные программно-аппаратные комплексы, позволяющие повысить производительность, оптимизировать бизнес-процессы и создать безопасную и устойчивую инфраструктуру управления.

Основные концепции информационных систем Современные технологии позволяют осуществлять быстрый доступ к данным, анализировать большие объемы информации, автоматизировать процессы и обеспечивать взаимодействие различных компонентов системы. Основные принципы построения таких систем включают:

- централизованное и распределенное хранение информации;
- использование интеллектуальных алгоритмов обработки данных;
- внедрение адаптивных механизмов управления ресурсами;
- повышение уровня информационной безопасности.

Современные информационные системы (ИС) играют ключевую роль в развитии экономики, науки и общества. Они обеспечивают обработку, хранение и передачу информации, что критически важно для эффективного функционирования организаций. Развитие цифровых технологий способствует созданию новых моделей бизнеса и управления, что делает изучение ключевых технологий информационных систем особенно актуальным. Основные технологии информационных систем:

Облачные вычисления. Облачные технологии представляют собой распределенные вычислительные системы, предоставляющие пользователям возможность удаленного хранения и обработки данных. Они реализуются через виртуализацию ресурсов и распределение нагрузок, обеспечивая масштабируемость и высокую доступность вычислительных мощностей.

Большие данные (Big Data). Технологии обработки больших данных включают методы параллельных вычислений, использование распределенных файловых систем и машинного обучения для выявления сложных закономерностей в информации. Они применяются в научных исследованиях, моделировании сложных систем и прогнозировании различных процессов.

Искусственный интеллект (ИИ) и машинное обучение. Искусственный интеллект использует методы статистического анализа, нейросетевые алгоритмы и оптимизационные подходы для обработки информации и автоматизации сложных задач. В основе машинного обучения лежат методы градиентного спуска, регрессии и кластеризации, что позволяет моделировать интеллектуальные системы.

Блокчейн. Блокчейн представляет собой распределенный реестр, состоящий из последовательности зашифрованных блоков данных. Важной особенностью этой технологии является децентрализованное управление и неизменяемость записей, что делает её востребованной в системах цифровой идентификации, логистики и смарт-контрактов.

Кибербезопасность. Кибербезопасность охватывает широкий спектр методов и технологий, направленных на защиту информации от несанкционированного доступа. Важными аспектами являются обнаружение аномалий в трафике, модели машинного обучения для выявления угроз и применение криптографических методов для защиты данных.

Технологии информационных систем способствуют развитию автоматизированных процессов управления, повышению эффективности обработки информации и созданию интеллектуальных решений. Их дальнейшее развитие направлено на интеграцию новых подходов к анализу данных, повышению надежности цифровых систем и развитию адаптивных алгоритмов обработки информации.

Ключевые технологии информационных систем. Современные системы управления базируются на нескольких фундаментальных технологиях, обеспечивающих их эффективность и безопасность. Рассмотрим наиболее значимые из них. Информационные системы (ИС) представляют собой комплекс программных и аппаратных средств, предназначенных для сбора, хранения, обработки и передачи данных. Они активно используются в различных сферах — от бизнеса и государственного управления до здравоохранения и образования. Ключевыми компонентами ИС являются базы данных, программное обеспечение, сети и устройства ввода-вывода. Современные технологии, такие как облачные вычисления, биг дата, искусственный интеллект и машинное обучение, значительно изменяют подходы к построению ИС и позволяют повысить их эффективность.

Искусственный интеллект и интеллектуальные алгоритмы. Применение интеллектуальных технологий значительно расширяет возможности автоматизированных систем. Они позволяют прогнозировать развитие событий, оптимизировать решения, повышать эффективность анализа данных и снижать влияние человеческого фактора. Искусственный интеллект охватывает широкий спектр технологий и методов, включая машинное обучение (ML), обработку естественного языка (NLP), компьютерное зрение, робототехнику и многие другие. ИИ стремится сделать системы более автономными, чтобы они могли адаптироваться к меняющимся условиям, обучаться на основе данных и принимать решения с минимальным вмешательством человека.

Основной целью ИИ является создание алгоритмов, которые могут решать задачи, ранее доступные только человеку, такие как анализ больших объемов данных, принятие стратегических решений и даже взаимодействие с людьми. Первоначально концепция ИИ была формализована в середине XX века, однако быстрый прогресс в вычислительных мощностях и доступности больших данных в последние десятилетия способствовал бурному развитию технологий ИИ.

Хотя технологии ИИ и интеллектуальные алгоритмы развиваются с огромной скоростью, существует несколько значительных вызовов. Среди них — этические вопросы, связанные с прозрачностью алгоритмов и их влиянием на частную жизнь; риски для рабочих мест, вызванные автоматизацией; а также проблемы, связанные с безопасностью и управлением ИИ-системами.

Однако будущее ИИ представляется весьма перспективным. Внедрение более совершенных алгоритмов и методов, таких как квантовое вычисление и новые подходы к машинному обучению, может привести к созданию систем, обладающих способностью к еще более глубокому пониманию мира и принятию решений.

Интеллектуальные алгоритмы и их виды. Интеллектуальные алгоритмы являются основой искусственного интеллекта. Это программы, которые способны анализировать входные данные, выявлять закономерности и, на основе этих данных, принимать решения или делать прогнозы.

Машинное обучение — это метод, при котором алгоритмы обучаются на данных, чтобы делать прогнозы или классифицировать объекты. Этот подход отличается от традиционных алгоритмов, где программирование фокусируется на создании точных инструкций для решения задач. В отличие от этого, в машинном обучении алгоритмы могут совершенствоваться по мере накопления новых данных.

Основные методы машинного обучения включают:

Обучение с учителем — использование размеченных данных для обучения модели.

Обучение без учителя — алгоритм анализирует данные без предварительных меток и самостоятельно находит структуры.

Обучение с подкреплением — модель обучается путем взаимодействия с окружающей средой, получая «награды» или «штрафы» за свои действия.

Нейронные сети – это алгоритмы, вдохновленные структурой человеческого мозга, которые состоят из узлов (нейронов), связанных между собой. Нейронные сети являются основой глубокого обучения, одной из наиболее мощных технологий ИИ.

Глубокие нейронные сети способны решать задачи, такие как обработка изображений, распознавание речи, генерация текста и даже игра в сложные игры, такие как шахматы или го. Данная технология развивается быстрыми темпами и уже находит широкое применение в таких областях, как медицина (для диагностики заболеваний), финансы (для прогнозирования финансовых рынков) и автомобильная промышленность (для создания автономных транспортных средств).

Алгоритмы поиска используются для нахождения решений в заданных пространствах состояний, что особенно важно в задачах оптимизации. Применяются в таких сферах, как планирование маршрутов, финансовое прогнозирование, логистика и другие.

Системы управления и автоматизации процессов. Интеграция технологий автоматизации позволяет повысить точность выполнения задач, снизить затраты и минимизировать влияние человеческого фактора. Современные системы управления активно применяются в промышленности, транспорте, энергетике и здравоохранении.

Современные системы управления и автоматизации процессов играют ключевую роль в повышении производственной эффективности и управлении различными аспектами бизнеса. С их помощью можно минимизировать человеческий фактор, повысить точность и скорость

выполнения задач, а также снизить затраты. Автоматизация процессов охватывает широкий спектр областей, включая управление производственными процессами, энергетические системы, логистику, а также управление качеством и безопасность.

Система управления представляет собой комплекс, включающий оборудование, программное обеспечение и методы управления для организации процессов. Автоматизация, в свою очередь, заключается в применении технологий для автоматического выполнения задач, которые ранее требовали человеческого вмешательства. В основе таких систем лежат различные математические модели, алгоритмы и инструменты мониторинга, а также автоматическое регулирование и управление процессами в реальном времени.

Современные технологии, такие как **искусственный интеллект** (ИИ) и **Интернет вещей** (IoT), активно используются для повышения эффективности систем управления. ИИ позволяет системе обучаться на основе данных, что способствует лучшему принятию решений и адаптации к изменениям в процессе. IoT помогает создать взаимосвязанную сеть устройств, которая может отслеживать состояние оборудования и параметров процессов в реальном времени, улучшая мониторинг и контроль.

Информационная безопасность и защита данных. Рост числа угроз в киберпространстве требует совершенствования методов защиты данных. Современные системы безопасности включают механизмы шифрования, многофакторную аутентификацию, а также постоянный мониторинг потенциальных уязвимостей.

Информационная безопасность — это состояние защищенности информационных систем, при котором обеспечивается защита информации от несанкционированного доступа, использования, разрушения, изменения, раскрытия и других угроз. С учетом того, что информационные технологии активно используются в различных областях — от бизнеса до медицины и государственного управления — защита данных становится не только технической, но и социальной, экономической проблемой.

Угрозы информационной безопасности. Существуют различные типы угроз, которые могут повлиять на конфиденциальность, целостность и доступность данных:

Внешние угрозы: хакерские атаки, фишинг, вирусы и вредоносные программы, кибершпионаж.

Внутренние угрозы: несанкционированный доступ сотрудников, утечка информации по ошибке или из-за халатности.

Технические угрозы: сбои в оборудовании, недостаточная защита программного обеспечения.

Природные угрозы: стихийные бедствия, утрата данных из-за аппаратных сбоев.

Методы защиты данных. Для обеспечения информационной безопасности применяются различные методы защиты:

Шифрование: использование криптографических методов для кодирования данных, что делает информацию нечитаемой без соответствующего ключа.

Аутентификация и авторизация: системы, проверяющие личность пользователя и предоставляющие доступ только авторизованным лицам.

Брандмауэры и антивирусные программы: защита от вирусов и внешних угроз через фильтрацию входящего трафика.

Резервное копирование: создание копий данных для восстановления информации в случае утраты.

Управление доступом: контроль прав доступа к информации на разных уровнях организации, чтобы предотвратить несанкционированный доступ.

Перспективы развития информационных технологий. Будущее развитие технологических систем связано с совершенствованием интеллектуальных алгоритмов, интеграцией автономных решений и развитием концепции самоуправляемых инфраструктур. Наиболее значимые направления развития включают:

создание адаптивных самоуправляемых систем;

разработку технологий сверхбыстрой обработки информации;

интеграцию биометрических и нейросетевых решений;

внедрение высокоэффективных методов защиты данных.

Заключение. Информационные технологии продолжают стремительно развиваться, оказывая значительное влияние на все сферы деятельности. Их дальнейшее совершенствование будет определять будущее экономики, науки и социальной среды. Развитие адаптивных и интеллектуальных систем позволит повысить эффективность бизнеса, повысить уровень безопасности и создать новые возможности для инновационного роста.

Список литературы

1. Безукладников К.Э. Информационные технологии в образовании и науке. М.: Издательство Академии Наук, 2020. 320 с.
2. Вербницкая М.В. Основы автоматизированных систем управления. СПб.: Политехнический университет, 2019. 280 с.
3. Берман Н.Д. Технологии обработки больших данных. Екатеринбург: Уральский федеральный университет, 2018. 290 с.

Сведения об авторах:
Абаева Айна, преподаватель, Туркменская государственная школа культуры и искусств, г. Ашхабад, Туркменистан, **Мухаммедова Джемал**, преподаватель, Туркменская государственная школа культуры и искусств, г. Ашхабад, Туркменистан, **Аннаовезова Бахар**, преподаватель, Туркменская государственная школа культуры и искусств, г. Ашхабад, Туркменистан, **Джарчыева Аннатач**, преподаватель, Туркменская государственная школа культуры и искусств, г. Ашхабад, Туркменистан
Abaeva Aina, lecturer, Turkmen State School of Culture and Arts Ashgabat, Turkmenistan, **Mukhammedova Jemal**, lecturer, Turkmen State School of Culture and Arts Ashgabat, Turkmenistan **Annaovezova Bahar**, lecturer, Turkmen State School of Culture and Arts Ashgabat, Turkmenistan, **Dzharchyeva Annatatch**, lecturer, Turkmen State School of Culture and Arts Ashgabat, Turkmenistan

УДК 614.8

Пашутин В. Д.
Казанский национальный исследовательский технологический университет, Казань, Россия

Управление средствами индивидуальной защиты в России: контроль соответствия

Аннотация. Статья посвящена методам контроля соответствия средств индивидуальной защиты (СИЗ) требованиям российского законодательства и отраслевым стандартам. Рассмотрены этапы специальной оценки условий труда (СОУТ), алгоритмы подбора СИЗ на основе ГОСТов, а также практические примеры из нефтегазовой, металлургической и пищевой промышленности. Особое внимание уделено расчёту классов условий труда, нормативам для респираторов, касок и спецодежды. Материал основан на данных Роструда, отчётах предприятий и требованиях Трудового кодекса РФ.
Ключевые слова: СИЗ, контроль соответствия, СОУТ, ГОСТ, Роспотребнадзор.

Pashutin V.D.

Management of personal protective equipment in russia: compliance control

Abstract. The article focuses on methods for controlling the compliance of personal protective equipment (PPE) with Russian legislative requirements and industry standards. The stages of the special assessment of working conditions (SAWC), algorithms for selecting PPE based on GOST standards, and practical examples from the oil and gas, metallurgical, and food industries are discussed. Special attention is paid to the calculation of working condition classes, standards for respirators, helmets, and protective clothing. The material is based on Rostrud data, enterprise reports, and the Labor Code of the Russian Federation.
Keywords: PPE, compliance control, SAWC, GOST standards, Rospotrebnadzor.

Введение. Контроль соответствия средств индивидуальной защиты (СИЗ) является ключевым элементом системы охраны труда. Согласно статьям 209 и 221 Трудового кодекса РФ, работодатель обязан обеспечивать сотрудников СИЗ, соответствующими характеру их деятельности, и проводить их регулярную проверку. Однако данные Роструда за 2023 год свидетельствуют о том, что до 40% нарушений в сфере охраны труда связаны с некорректным подбором или отсутствием СИЗ. Для понимания российской специфики важно учитывать международный контекст. Например, в ЕС директива 89/656/ЕЕС обязывает работодателей проводить оценку рисков перед выбором СИЗ, что схоже с процедурой СОУТ в России. Однако, по данным Международной организации труда (МОТ), в странах СНГ уровень травматизма из-за несоответствия СИЗ на 15–20% выше, чем в Западной Европе. Это подчёркивает необходимость не только соблюдения локальных норм, но и адаптации лучших мировых практик.

Нормативная база и классификация СИЗ. Федеральный закон № 426-ФЗ [2] регламентирует проведение специальной оценки условий труда (СОУТ), которая должна выполняться не реже одного раза в пять лет. Однако на предприятиях с повышенным уровнем риска, таких как химические производства или горнодобывающие комплексы, оценку рекомендуется проводить ежегодно. Приказ Минтруда № 328н [3] дополняет эти требования, обязывая работодателей вести журнал учёта выдачи СИЗ, где фиксируются даты выдачи, сроки эксплуатации и замены средств защиты.

Государственные стандарты (ГОСТ). ГОСТ 12.4.011-89 [5] устанавливает общие требования к маркировке, срокам годности и правилам хранения спецодежды. ГОСТ Р 12.4.280-2014 [4] регулирует средства защиты органов дыхания, разделяя респираторы на три класса: FFP1, FFP2 и FFP3. Для работы с асбестом или химическими аэрозолями обязательны респираторы FFP3. Российские во многом похожи с международными. ГОСТ Р 12.4.280-2014 для респираторов соответствует европейскому EN 149:2001. Однако различия заключаются в том, что в ГОСТ отсутствуют требования к эргономике масок, что критично для длительной работы в условиях Крайнего Севера.

Новые инициативы. С 2024 года Роспотребнадзор планирует внедрить цифровую маркировку СИЗ через систему «Честный знак», что даст возможность отслеживать подлинность продукции и сроки эксплуатации в режиме реального времени.

Классификация СИЗ по зонам защиты включает несколько категорий. Для защиты головы используются каски, соответствующие ГОСТ Р 12.4.207-2019, которые делятся на два типа: тип 1 предназначен для защиты от ударов сверху, тип 2 — от ударов сбоку. Средства защиты органов дыхания, такие как респираторы FFP1-FFP3, подбираются исходя из концентрации вредных веществ. При работе с лакокрасочными материалами, где предельно допустимая концентрация (ПДК) составляет 0.1 мг/м³, требуется респиратор класса FFP2.

Контроль соответствия СИЗ: методы и практика. Специальная оценка условий труда (СОУТ) — регламентированный законодательством метод проверки соответствия средств индивидуальной защиты характеру и уровню производственных рисков. СОУТ проходит в несколько этапов (рис. 1):

Рисунок 1 – Этапы СОУТ.

На этапе идентификации рисков эксперты анализируют рабочие места для выявления потенциально вредных или опасных факторов. К ним относятся физические воздействия (шум, вибрация, уровень освещения, радиация), химические риски (наличие пыли, токсичных газов или жидкостей), биологические угрозы (микроорганизмы, аллергены). Оценивают тяжесть труда (необходимость подъёма тяжестей, работы в неудобной позе и др.) и психоэмоциональные нагрузки (включая стресс, монотонность операций). После выявления рисков проводятся инструментальные измерения с использованием с использованием разного спец. оборудования: шумомеров, газоанализаторов, люксметров и других приборов. Замеры выполняются в разных точках рабочей зоны и при различных режимах работы, чтобы получить объективные данные. На основе результатов замеров каждому фактору присваивается класс опасности. Классы делятся на: оптимальный (1 класс, безопасные условия), допустимый (2 класс, риски в пределах нормы), вредный (подклассы 3.1–3.4 с возрастающей степенью вреда) и опасный (4 класс, требующий немедленного устранения угрозы). Для минимизации воздействия вредных факторов сотрудникам подбирают средства индивидуальной защиты. Это могут быть респираторы для фильтрации воздуха, противошумные наушники, спецодежда или каски. Важно, чтобы СИЗ соответствовали выявленным рискам и имели сертификаты. Заключительный этап — разработка мер по улучшению условий труда. План может включать технические решения (модернизацию вентиляции, установку шумоизоляции), организационные изменения (сокращение времени контакта

с вредными факторами), медицинские мероприятия (дополнительные обследования) или обучение сотрудников [8].

В соответствии с Федеральным законом № 426-ФЗ, оценка включает два этапа: идентификацию вредных факторов и расчёт класса условий труда. На первом этапе выявляются химические, физические и биологические риски. Например, на химическом заводе ООО «Еврохим» были идентифицированы 12 опасных веществ, включая аммиак и формальдегид, на металлургическом комбинате ПАО «НЛМК» — шум свыше 80 дБ и вибрация.

Расчёт класса условий труда:

$$K = \sum_{i=1}^{n}(B_i * W_i),$$

Bi — балл опасности фактора (от 1 до 4), Wi— его вес в общей оценке. [6] Для сварщика АО «Уралмаш» были учтены УФ-излучение (B_1=4, W_1=0.5), искры (B_2=3, W_2=0.3) и шум (B_3=2, W_3=0.2). Результат расчёта (k=3.3) отнёс условия труда к вредным 3-й степени, что потребовало применения респиратора FFP3, огнестойкого костюма и защитных очков с затемнёнными стёклами.

Подбор СИЗ по нормативам требует учёта конкретных параметров рабочей среды.

Для респираторов используется формула минимального уровня защиты:

$$MPC = \frac{C_{max}}{\text{ПДК}},$$

C_{max} — максимальная концентрация вещества, ПДК — предельно допустимая концентрация. [4] На химическом производстве ООО «ФосАгро» при работе с аммиаком (C_{max}=1.5 мг/м^3, ПДК=0.2 мг/м^3) расчёт показал необходимость использования респиратора FFP3 с дополнительным фильтром.

Огнестойкие костюмы (ГОСТ Р 53264-2009), которые применяются при температуре до 800°С, на АО «Магнитогорский металлургический комбинат» заменяются каждые 4 месяца, это снизило количество ожогов на 25%. Сигнальные жилеты (ГОСТ 12.4.281-2014), обязательные в зонах движения транспорта, на складах ПАО «НЛМК» их отсутствие привело к трём ДТП в 2022 году.

Практические кейсы контроля соответствия. В нефтегазовой отрасли контроль соответствия СИЗ сталкивается с уникальными вызовами. В 2021 году в ООО «Лукойл-Коми» [7] было зафиксировано 12 нарушений, связанных с износом огнестойких костюмов. Решением было внедрение графика замены костюмов каждые 6 месяцев, проверку их соответствия ГОСТ Р 53264-2009 через аккредитованные лаборатории и ежеквартальные аудиты. К 2023 году это позволило снизить количество нарушений на 30% и полностью исключить случаи возгорания спецодежды.

В 2022 году на АО «Уралвагонзавод» отсутствие защитных очков стало причиной 23 случаев травм. Внедрение обязательного использования очков, соответствующих ГОСТ Р 12.4.013-97, ежемесячные проверки и введение штрафов за нарушения привели к снижению травматизма на 45% и экономии на страховых выплатах в размере 2.3 млн рублей ежегодно.

На ООО «Вимм-Билль-Данн» в 2023 году Роспотребнадзор выдал 5 предписаний из-за нарушений гигиены. Введение ежедневного контроля за использованием масок (ГОСТ Р 58396-2019) и закупка СИЗ только у сертифицированных поставщиков позволили устранить нарушения за 3 месяца и получить положительную оценку контролирующих органов.

На ПАО «ЛенСпецСМУ» неисправные страховочные пояса повлекли несколько инцидентов. Замена поясов на модели с амортизаторами (ГОСТ Р 12.4.205-2019) и еженедельная проверка креплений снизили травматизм на 40% в 2023 году.

Заключение. Контроль соответствия средств индивидуальной защиты требует системного подхода, основанного на законодательных нормах, ГОСТах и практическом опыте. Регулярная оценка условий труда, строгий подбор СИЗ позволяют снизить травматизм на 30–45%. Одними из ключевых направлений развития являются автоматизация учёта, адаптация международного опыта и повышение ответственности работодателей. Эти меры помогут сохранить здоровье сотрудников, формируя устойчивую систему охраны труда.

Список литературы:

1. Трудовой кодекс Российской Федерации (с изменениями на 2023 год). М.: Проспект, 2023.
2. Федеральный закон № 426-ФЗ «О специальной оценке условий труда» // Собрание законодательства РФ. 2023. № 15. Ст. 2345.
3. Приказ Минтруда России № 328н «Об утверждении Правил обеспечения работников средствами индивидуальной защиты» // Российская газета. 2021. № 127. С. 12-15.
4. ГОСТ Р 12.4.280-2014 «Система стандартов безопасности труда. Средства индивидуальной защиты органов дыхания. Общие технические условия». М.: Стандартинформ, 2014.
5. ГОСТ 12.4.011-89 «Система стандартов безопасности труда. Средства индивидуальной защиты. Общие требования и классификация». М.: Изд-во стандартов, 1989.
6. Руководство по специальной оценке условий труда (утв. Приказом Минтруда РФ № 33н от 24.01.2014). М.: НИИ труда, 2014.
7. Отчёт ООО «Лукойл-Коми» по специальной оценке условий труда (2022–2023 гг.). Ухта: Изд-во ООО «Лукойл-Коми», 2023.
8. Охрана труда. [Электронный ресурс]. URL: https://ru.m.wikipedia.org/wiki/Охрана_труда (дата обращения: 23.03.2025).

Сведения об авторе:
Пашутин Владислав Дмитриевич, магистрант, Казанский национальный исследовательский технологический университет, Казань, Россия
Pashutin Vladislav Dmitrievich, Postgraduate Student, Kazan National Research Technological University, Kazan, Russia

УДК: 004.056

Тимонин В. А.[1], Уткин А.В.[2], Козлова Ю. Д.[3]
[1]Digital IQ, Анталья, Турция;
[2]Digital-IQ, Дирфилд Бич, США
[3]SimbirSoft, Ульяновск, Россия

Уязвимости и риски облачных технологий в контексте обеспечения информационной безопасности облачных сервисов

Аннотация. В условиях стремительного развития цифровых технологий облачные сервисы становятся неотъемлемой частью информационно-технологической инфраструктуры предприятий, обеспечивая гибкость, масштабируемость и экономическую эффективность. Однако их широкое распространение сопровождается ростом киберугроз и уязвимостей, что делает вопросы информационной безопасности облачных технологий особенно актуальными. Целью настоящей статьи является анализ ключевых уязвимостей и рисков облачных сервисов, а также рассмотрение методов их минимизации. В рамках исследования проведена систематизация угроз, таких как утечка данных, атаки на облачную инфраструктуру, проблемы аутентификации и несанкционированный доступ. Результаты работы демонстрируют, что эффективное обеспечение безопасности облачных сервисов требует комплексного подхода, включающего механизмы шифрования, многофакторную аутентификацию, управление доступом, аудит событий и применение лучших практик киберзащиты. Материалы статьи могут быть полезны специалистам в области информационной безопасности, разработчикам облачных решений и IT-менеджерам, позволяя глубже понять риски облачных технологий и разработать стратегию их защиты в контексте обеспечения безопасности облачных сервисов.

Ключевые слова. Облачные технологии, облачные сервисы, облачные вычисления, информационная безопасность, защита, угроза.

Timonin V.A., Utkin A.V., Kozlova I.D.

Vulnerabilities and risks of cloud technologies in the context of information security of cloud services

Abstract. With the rapid development of digital technologies, cloud services are becoming an integral part of the information technology infrastructure of enterprises, providing flexibility, scalability and cost-effectiveness. However, their widespread use accompanied by an increase in cyber threats and vulnerabilities, which makes cloud technology information security issues particularly relevant. The purpose of this article is to analyze the key vulnerabilities and risks of cloud services, as well as to consider methods for minimizing them. The study systematized threats such as data leakage, attacks on cloud infrastructure, authentication problems, and unauthorized access. The results of the work demonstrate that effective security of cloud services requires an integrated approach, including encryption mechanisms, multifactor authentication, access control, event auditing, and the use of best cyber defense practices. The materials of the article can be useful to information security specialists, cloud solution developers and IT managers, allowing them to better understand the risks of cloud technologies and develop a strategy for their protection in the context of ensuring the security of cloud services.

Key words. Cloud technologies, cloud services, cloud computing, information security, protection, threat.

Облачные технологии представляют собой модель предоставления вычислительных ресурсов, при которой пользователи получают доступ к серверам, хранилищам данных и различным приложениям через интернет [1]. На момент 2025 года они играют ключевую роль в информационно-технологическом обеспечении предприятий, позволяя компаниям эффективно управлять IT-инфраструктурой, снижать затраты и ускорять цифровую трансформацию. Как отмечают в своем исследовании Ю.Д. Козлова и ВА. Тимонин (2024), возможность гибкого масштабирования облачных ресурсов дает организациям значительное преимущество, позволяя оперативно адаптироваться к изменениям рыночной среды и технологическим вызовам [2]. Также, использование облачных решений позволяет компаниям экономить на капитальных затратах, связанных с приобретением и обслуживанием оборудования, а также получать доступ к передовым разработкам, включая технологии искусственного интеллекта, анализа больших данных и кибербезопасности.

Актуальность облачных технологий в последние годы подтверждается динамичным ростом инвестиций в этот сектор. По данным аналитического агентства Synergy Research Group, в четвертом квартале 2024 года корпоративные расходы на облачные сервисы по всему миру достигли 91 млрд долларов, что на 17 млрд (22 %) больше по сравнению с аналогичным периодом 2023 года. За весь 2024 год глобальный рынок облачных услуг увеличился до 330 млрд долларов, что на 60 млрд больше по сравнению с 2023 годом и на 102 млрд больше, чем в 2022 году [3]. Подобная динамика обусловлена повышенным спросом на облачные решения среди бизнеса и государственных организаций, стремящихся повысить эффективность работы, улучшить безопасность данных и ускорить развертывание IT-систем.

Рост популярности облачных технологий наблюдается не только на мировом уровне, но и на российском рынке. Согласно исследованию DataPy.Облако, опубликованному в марте 2025 года, объем российского рынка облачных инфраструктурных сервисов увеличился на 36,3% и достиг 165,6 млрд рублей [4]. Этот показатель значительно выше по сравнению с предыдущим годом, когда объем рынка составлял 121,5 млрд рублей. В условиях активного импортозамещения и роста спроса на отечественные IT-решения российские компании все чаще выбирают облачные платформы для построения цифровых экосистем, повышения отказоустойчивости инфраструктуры и защиты данных. Это подтверждает важность дальнейшего развития и совершенствования облачных

технологий в контексте информационной безопасности (далее – ИБ) и стратегического планирования.

Столь широкое и повсеместное распространение облачных технологий, их интеграция в ключевые бизнес-процессы, государственные системы управления и инфраструктурные проекты на момент 2025 года ведут к значительному расширению информационного периметра предприятий. В условиях цифровизации возрастает объем обрабатываемых и передаваемых данных, что неизбежно сопровождается увеличением рисков, связанных с утечками, несанкционированным доступом, нарушением целостности и конфиденциальности информации. Компании, переходящие на облачные сервисы, сталкиваются с новыми вызовами, требующими пересмотра существующих моделей информационной безопасности, адаптации стратегий защиты и внедрения более совершенных механизмов мониторинга, выявления угроз и реагирования на инциденты.

Также следует отметить, что проведенное компанией Check Point исследование показывает, что наибольшее количество подобных инцидентов зафиксировано в государственных учреждениях - 13%, компаниях ИТ-сектора - 12% и предприятиях промышленной отрасли - 11%, что отражено на рис. 1 [5]. В данных сегментах наблюдается высокий уровень интеграции и использования облачных сервисов, что также актуализирует задачу обеспечения их информационной безопасности.

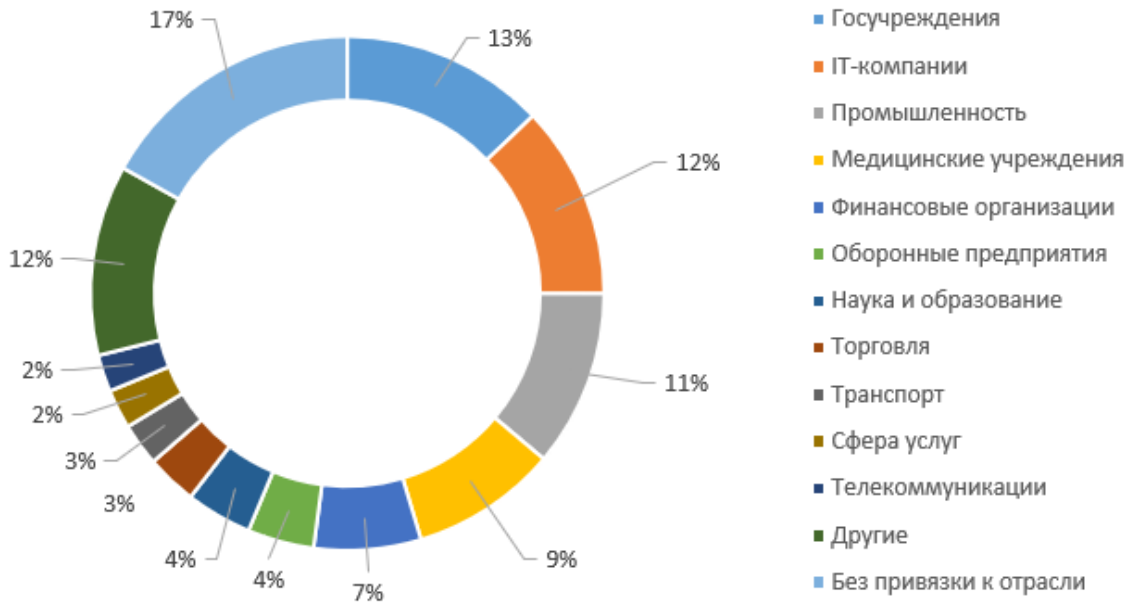

Рис. 1. Распределение инцидентов утечек ПД по отраслям

Совокупность выше представленных факторов подтверждает актуализацию проблемы обеспечения информационной безопасности облачных сервисов, поскольку именно этот аспект во многом определяет

надежность и устойчивость цифровой инфраструктуры. По оценке автора, ключевая сложность заключается в том, что традиционные методы защиты, ориентированные на локальные вычислительные мощности, в облачной среде оказываются недостаточно эффективными. Централизация данных в дата-центрах провайдеров требует принципиально иного подхода к вопросам разграничения доступа, предотвращения атак, управления криптографическими ключами и обеспечения отказоустойчивости. Дополнительные риски возникают из-за возможных уязвимостей в программном обеспечении облачных платформ, несовершенства механизмов шифрования и угроз, связанных с внутренними злоумышленниками.

По мнению автора М.Р. Акбарова, (2022), важнейший аспект обеспечения безопасности облачных сервисов заключается в контроле над распределением и обработкой данных, поскольку современные атаки все чаще направлены не только на нарушение работы сервисов, но и на извлечение и модификацию критически важной информации [6]. Н.В. Беспалова (2024) отмечает, что одной из наиболее уязвимых точек в облачных средах остается слабая защищенность учетных данных и механизмов аутентификации пользователей [7]. Это создает условия для атак с использованием украденных или скомпрометированных учетных записей, что может привести к масштабным утечкам конфиденциальных данных. На основе вышеизложенного можно сделать вывод, что вопросы безопасности облачных технологий требуют комплексного подхода, включающего совершенствование нормативно-правового регулирования, внедрение инновационных технических решений и повышение уровня осведомленности пользователей. Учитывая рост значимости облачных сервисов в цифровой экономике, дальнейшее исследование данной проблемы становится необходимым условием для обеспечения устойчивости и защиты критической информационной инфраструктуры.

На текущем этапе исследования необходимо произвести тщательный анализ и систематизацию угроз и уязвимостей, с которыми сталкиваются облачные сервисы. Как отмечают А С. Тонких и Е Ю. Авксентьева (2024), среди наиболее актуальных угроз можно выделить утечку данных, атаки на облачную инфраструктуру, проблемы аутентификации и несанкционированный доступ [8]. Эти угрозы представляют собой критические риски для безопасности облачных сервисов, что требует внедрения комплексных методов защиты. Рассмотрим каждую из угроз более подробно. Облачные сервисы, как и другие информационные системы, подвергаются множеству типов атак. Одной из самых значительных угроз является утечка данных. Данные в облаке часто хранятся в централизованных хранилищах, что делает их привлекательными для хакеров. Утечка может происходить по разным причинам, включая недостаточную защиту данных на уровне шифрования

или ошибки при передаче данных через ненадежные каналы связи. Атаки на облачную инфраструктуру могут быть как внешними, так и внутренними. Внешние атаки могут включать DDoS-атаки, направленные на блокирование сервисов, а также атакующие эксплуатируют уязвимости в программном обеспечении облачных платформ. Внутренние угрозы могут быть связаны с действиями недобросовестных сотрудников облачных провайдеров или пользователей сервисов, что может привести к доступу к конфиденциальным данным.

Проблемы аутентификации представляют собой ещё одну важную уязвимость. По мнению В.Р. Нестеренко и М.А. Масловой (2021), использование слабых паролей, отсутствие многофакторной аутентификации и низкий уровень защиты учетных данных пользователей могут привести к несанкционированному доступу к облачным сервисам [9]. Технически это может быть связано с уязвимыми интерфейсами API, которые предоставляют доступ к облачным системам без должной защиты, либо с недоразвитыми механизмами управления правами доступа. Также возникает проблема несанкционированного доступа, который может происходить как по вине пользователей, так и в результате атак на слабые места системы. Когда данные не должным образом защищены, а аутентификация недостаточно эффективна, существует угроза того, что злоумышленники смогут получить доступ к чувствительной информации. Систематизация угроз и уязвимостей, связанных с облачными технологиями, позволяет глубже понять масштабы проблемы и разработать эффективные стратегии защиты. В представленной далее табл. 1 отражены основные уязвимости, риски и угрозы, с которыми сталкиваются облачные сервисы на текущий период времени.

Таблица. 1. – Уязвимости, риски и угрозы облачных технологий в контексте обеспечения ИБ облачных сервисов

№	Уязвимость/ Угроза	Описание	Последствия
1	Утечка данных	Ненадежное шифрование данных, утечка данных из-за ошибок настройки	Утрата конфиденциальности, финансовые потери, репутационные риски
2	Атаки на облачную инфраструктуру	DDoS-атаки, взлом сервисов, уязвимости в программном обеспечении	Прекращение работы облачных сервисов, потеря данных, недоступность сервисов
3	Проблемы аутентификации	Слабые пароли, отсутствие многофакторной аутентификации	Несанкционированный доступ, кража данных, вредоносное вмешательство

№	Уязвимость/ Угроза	Описание	Последствия
4	Несанкционированный доступ	Логин с украденными учетными данными, недостаточно жесткая защита прав доступа	Неавторизованные изменения в данных, разрушение целостности данных
5	Уязвимости API	Ненадежные API-интерфейсы без должной защиты	Проникновение через API, возможность манипуляций с данными
6	Нарушение контроля доступа	Ошибки в настройках прав доступа или их отсутствие	Неавторизованный доступ к системам и данным, нарушение работы сервисов
7	Уязвимости в программном обеспечении	Использование устаревших версий ПО, отсутствующие патчи	Эксплуатация уязвимостей, угроза целостности данных и работы сервисов

В результате анализа уязвимостей и угроз, с которыми сталкиваются облачные технологии в контексте обеспечения информационной безопасности, можно выделить несколько ключевых моментов. Представленная табл. 1 отражает систематизацию основных угроз, таких как утечка данных, атаки на облачную инфраструктуру, проблемы с аутентификацией и несанкционированный доступ. Каждый из этих факторов несет серьезные потенциальные последствия, такие как утрата конфиденциальности данных, финансовые потери, репутационные риски и недоступность сервисов. В табл. 1 отражено, что угрозы могут иметь как технические, так и организационные корни. Например, проблемы с аутентификацией и недостаточная защита API-интерфейсов могут привести к несанкционированному доступу и манипуляциям с данными. Нарушение контроля доступа и уязвимости в программном обеспечении создают угрозу для целостности и доступности сервисов. Так, приведенные угрозы и уязвимости подчеркивают важность комплексного подхода к обеспечению информационной безопасности в облачных сервисах. Это включает в себя как технические меры защиты (например, шифрование данных, внедрение многофакторной аутентификации), так и организационные (правильная настройка прав доступа, регулярное обновление программного обеспечения и патчей).

Согласно оценкам экспертов «Телеком 2024», в ближайшее время рынок облачных сервисов может вырасти ещё на 33%, что свидетельствует о продолжающемся расширении облачных технологий и увеличении их использования в различных отраслях [10]. Однако этот рост сопровождается значительными вызовами, среди которых главным

является безопасность инфраструктуры. По мере того как облачные сервисы становятся неотъемлемой частью бизнес-процессов, требования к их защите растут, и в связи с этим необходимость обеспечения высокого уровня информационной безопасности становится актуальной как никогда. В условиях бурного роста возникает неотложная потребность в разработке комплексного решения, которое будет охватывать все аспекты безопасности облачных сервисов, обеспечивая защиту на всех уровнях инфраструктуры и данных. Такое комплексное решение должно включать как организационные аспекты, так и технические компоненты, которые вместе смогут эффективно минимизировать риски и угрозы. В табл. 2 представлены основные составляющие комплексного решения обеспечения информационной безопасности облачных сервисов, включающее комбинацию организационных аспекты и технических компонентов.

Таблица 2. – Комбинация организационных и технических решений для обеспечения ИБ облачных сервисов

№	Решение	Описание
Организационные аспекты		
1	Управление рисками	Внедрение системы управления рисками, включающей регулярную оценку угроз, уязвимостей и анализ последствий для бизнеса. Организация должна разрабатывать и внедрять политики безопасности, соответствующие нормативным требованиям и лучшим практикам.
2	Обучение и повышение осведомленности сотрудников	Проведение регулярных тренингов и программ повышения квалификации для всех пользователей облачных сервисов, чтобы минимизировать риски, связанные с человеческим фактором, такими как фишинг-атаки или неправильная настройка доступа.
3	Управление доступом и правами пользователей	Создание и внедрение политик управления доступом, основанных на принципе минимальных привилегий, с использованием многофакторной аутентификации и регулярным пересмотром прав доступа.
4	Шифрование данных	Обеспечение безопасности данных на всех этапах их хранения и передачи через облачные сервисы, включая использование шифрования для данных в покое и при передаче (например, SSL/TLS протоколы).

№	Решение	Описание
Технические компоненты		
5	Мониторинг и управление инцидентами безопасности	Использование систем мониторинга и обнаружения вторжений (IDS/IPS), а также систем управления инцидентами безопасности (SIEM), для оперативного выявления аномалий и угроз безопасности в облачной инфраструктуре.
6	Тестирование на проникновение и регулярные аудиты	Регулярное проведение тестов на проникновение для обнаружения уязвимостей и оценки защиты системы, а также регулярные аудиты конфигураций для устранения выявленных проблем.
7	Бэкап и восстановление данных	Создание эффективной системы резервного копирования данных и восстановления после инцидентов для защиты от утечек, потерь или повреждения данных в случае атак или сбоев.
8	Интеграция с внешними системами безопасности	Интеграция облачных сервисов с внешними инструментами и сервисами безопасности (антивирусные системы, фаерволы, защита от DDoS-атак) для создания многоуровневой защиты.

Предложенные решения, представленные в табл. 2, составляют комплексную систему защиты облачных сервисов и направлены на минимизацию различных рисков и угроз, с которыми сталкиваются современные облачные технологии. Каждое из решений играет ключевую роль в обеспечении информационной безопасности и нацелено на конкретные задачи, такие как защита данных, оперативное реагирование на инциденты, предотвращение уязвимостей и восстановление данных. Шифрование данных обеспечивает конфиденциальность и целостность информации как при ее хранении, так и при передаче, что значительно снижает риски утечек и перехвата данных. Системы мониторинга и управления инцидентами безопасности, такие как SIEM и IDS/IPS, позволяют оперативно выявлять и предотвращать атаки в реальном времени, обеспечивая высокий уровень защиты от внешних и внутренних угроз. Тестирование на проникновение и регулярные аудиты позволяют выявить слабые места в инфраструктуре, предотвращая использование уязвимостей злоумышленниками. Резервное копирование данных и системы восстановления гарантируют восстановление данных в случае инцидентов, таких как утечка или повреждение данных, обеспечивая непрерывность бизнес-процессов. Интеграция с внешними системами безопасности, такими как антивирусные программы и фаерволы, создаёт дополнительный уровень защиты, который значительно снижает риски от

атак, включая DDoS и вирусные угрозы. В результате, комплексный подход к обеспечению безопасности облачных сервисов, включающий как организационные, так и технические компоненты, помогает эффективно защитить данные и инфраструктуру, минимизируя возможные риски и угрозы в облачной среде.

При этом особый интерес представляет техническая часть решения, которая включает в себя конкретные инструменты и технологии, обеспечивающие безопасность облачных сервисов. Каждый элемент технического решения решает определенные задачи, направленные на защиту от различных рисков и угроз. На рис. 2 представлена разработанная авторами настоящей статьи архитектура многослойной системы защиты с применением конкретных технологических решений для обеспечения безопасности облачных сервисов.

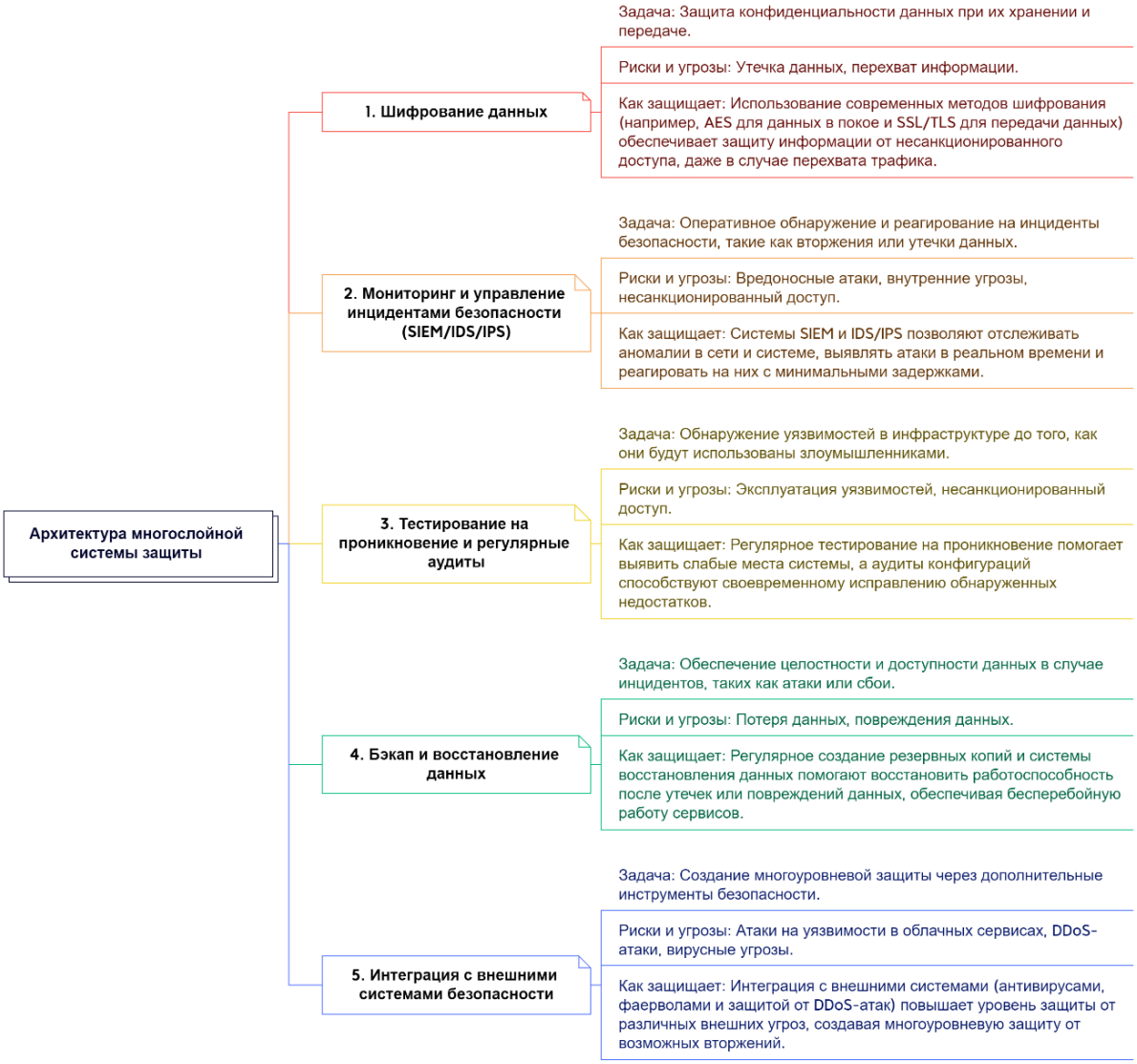

Рис. 2. Многослойная система защиты облачных сервисов

Представленный комбинированный подход к обеспечению информационной безопасности облачных сервисов предлагает

значительные преимущества по сравнению с традиционными методами. Во-первых, он обеспечивает комплексную защиту, охватывающую как технические, так и организационные аспекты. Как отмечают Е.Э. Кулеш Е. Э., Р.А. Смирнов и Г.В. Попков (2022), это позволяет минимизировать риски, которые могут возникнуть в отдельных областях безопасности, и избежать их пересечения [11]. Традиционные методы зачастую фокусируются на отдельных элементах безопасности, что делает систему уязвимой к многослойным атакам и угрозам.

Во-вторых, данный подход ориентирован на про-активное выявление и устранение угроз на всех этапах работы облачных сервисов, начиная с защиты данных и заканчивая реакцией на инциденты. Это в отличие от традиционных методов, которые часто ориентированы на пассивную защиту, что снижает их эффективность в условиях динамично меняющихся угроз. Включение систем мониторинга и тестирования на проникновение позволяет не только выявлять уязвимости, но и предсказывать возможные риски, что значительно повышает уровень защиты.

В-третьих, важным преимуществом является интеграция с внешними системами безопасности, что обеспечивает многоуровневую защиту от атак различного рода, включая DDoS-атаки, вирусные угрозы и попытки несанкционированного доступа [12]. В отличие от традиционных подходов, которые могут ограничиваться стандартными средствами защиты, наш метод создает гибкую и масштабируемую инфраструктуру безопасности, способную адаптироваться к постоянно меняющимся угрозам. Как результат, комбинированный подход позволяет не только значительно повысить уровень безопасности, но и обеспечить более эффективное управление рисками, оперативное реагирование на инциденты и защиту данных, что особенно важно в условиях высоких требований к облачным сервисам и их безопасности.

В ходе проведенного исследования были систематизированы основные угрозы и уязвимости облачных технологий, такие как утечка данных, атаки на облачную инфраструктуру, проблемы аутентификации и несанкционированный доступ. Анализ текущего состояния информационной безопасности облачных сервисов показал, что с ростом их распространения и интеграции в бизнес-процессы организаций, значительно увеличивается количество угроз, требующих новых подходов к защите. Так, объем российского рынка облачных инфраструктурных сервисов увеличился на 36,3% за 2024 год, достигнув 165,6 млрд рублей (согласно исследованиям экспертов DataPy.Облако). По прогнозам экспертов, в 2025 году ожидается быстрый рост рынка на 33% (согласно оценкам экспертов «Телеком 2024»). В условиях высокой динамики развития технологий и усложнения атак, традиционные методы защиты не могут гарантировать достаточный уровень безопасности. В связи с этим

была предложена комплексная система обеспечения безопасности облачных сервисов, включающая как технические, так и организационные компоненты.

В рамках работы были разработаны и представлены ключевые механизмы защиты, включая шифрование данных, многофакторную аутентификацию, управление доступом, мониторинг и аудит событий, а также применение лучших практик киберзащиты. Мы пришли к выводу, что эффективное обеспечение безопасности облачных сервисов требует комбинированного подхода, который включает использование современных технологий защиты, а также организационных мер для минимизации рисков и повышения осведомленности сотрудников. В частности, важнейшей частью решения является разработка и внедрение систем управления рисками и регулярное проведение тестирований на проникновение для выявления уязвимостей.

Проведенная работа позволила оценить текущее состояние и выявить основные проблемы, с которыми сталкиваются организации при обеспечении безопасности облачных сервисов. Разработанная система, объединяющая организационные и технические решения, предоставляет универсальный подход для защиты облачной инфраструктуры, который может быть адаптирован под различные типы угроз и уязвимостей. В дальнейшем предполагается использование предложенной системы в реальных условиях, что позволит оценить ее эффективность и внести необходимые улучшения.

Список литературы:

1. Куликова И.В., Некрасова В.С. Особенности применения облачных технологий в бухгалтерском учете // Ученые записки Алтайского филиала Российской академии народного хозяйства при Президенте Российской Федерации. 2021. №19 (19). С. 95-99.
2. Козлова Ю.Д., Тимонин В.А. Актуальность разработки и применения интеллектуальных облачных решений // EESJ. 2024. №5-1 (102-103). С. 4-8.
3. Облачный рынок вырос до $330 млрд в 2024 году, половину прироста обеспечил генеративный ИИ. Электронный ресурс. Режим доступа: https://servernews.ru/1118586 (дата обращения 26.02.2025 г.).
4. Облачные сервисы (рынок России). Электронный ресурс. Режим доступа: https://clck.ru/3JGrQp (дата обращения 02.03.2025 г.).
5. Утечки данных первой половины 2024 года: ИТ-компании — в топ-3 отраслей. Электронный ресурс. Режим доступа: https://clck.ru/3Htqyh (дата обращения 02.03.2025 г.).
6. Акбарова М.Р. Безопасность и защита данных в облачных технологиях // Universum: технические науки. 2022. №10-1 (103). С. 17-19.
7. Беспалова Н.В. Безопасность облачных технологий // Computational nanotechnology. 2024. №5. С. 124-132.
8. А С. Тонких, Е Ю. Авксентьева Угрозы безопасности в облачных технологиях и методы их устранения // Международный журнал гуманитарных и естественных наук. 2024. №1-2 (88). С. 232-238.

9. Нестеренко В.Р., Маслова М.А. Современные вызовы и угрозы информационной безопасности публичных облачных решений и способы работы с ними // Научный результат. Информационные технологии. 2021. №1. С. 48-54.
10. Безопасность в облаке: почему защита инфраструктуры становится ключевой задачей бизнеса? Электронный ресурс. Режим доступа: https://clck.ru/3JGvqk (дата обращения 10.03.2025 г.).
11. Кулеш Е. Э., Смирнов Р. А., Попков Г. В. Комплексная защита информации на производственном предприятии // Интерэкспо Гео-Сибирь. 2022. №1. С. 122-126.
12. Всяких А. Д. Что такое DDOS-атаки: угрозы и эффективные способы их предотвращения // Вестник науки. 2024. №11 (80). С. 1112-1118.

Сведения об авторах:
Тимонин Вадим Андреевич, системный инженер, “Digital IQ”, Анталья, Турция;
Уткин Александр Владимирович, старший системный инженер, Международный системный ИТ-интегратор “Digital-IQ”, Дирфилд Бич, Соединенные Штаты Америки
Козлова Юлия Дмитриевна, ведущий инженер по обеспечению качества, “SimbirSoft”, Ульяновск, Россия
Timonin Vadim Andreevich, Systems Engineer, “Digital IQ”, Antalya, Turkey;
Utkin Alexander Vladimirovich, Senior Systems Engineer, International Systems Integrator "Digital-IQ", Deerfield Beach, United States of America
Kozlova Iuliia Dmitryevna - Lead QA Engineer, International Software Developer “SimbirSoft”, Ulyanovsk, Russia

УДК: 347.4

Ростовцев Г.А., Баранова Е.М.
Тульский государственный университет, Тула, Россия

Автоматизированный аудит исполнения смарт-контрактов для цифровых сделок: принципы и инструменты

Аннотация. В статье рассматриваются принципы и инструменты автоматизированного аудита исполнения смарт-контрактов для цифровых сделок. Актуальность темы обусловлена ростом использования смарт-контрактов в различных областях, включая финансовые, юридические и коммерческие сделки. Процесс автоматизированного аудита становится критически важным для обеспечения прозрачности, безопасности и правовой силы цифровых сделок, заключаемых с помощью смарт-контрактов. Целью статьи является рассмотрение основных принципов автоматизированного аудита, анализ доступных инструментов для оценки исполнения смарт-контрактов, а также освещение значимости автоматизации аудиторских процессов в контексте цифровых сделок. В результате работы выявлены ключевые принципы автоматизированного аудита, рассмотрены эффективные инструменты и подходы, которые позволяют минимизировать риски и повышать доверие к смарт-контрактам. Статья может быть полезна для разработчиков смарт-контрактов, аудиторов, специалистов по блокчейн-технологиям и юридических специалистов, так как предоставляет комплексный обзор современных методов и практик в области аудита цифровых сделок, заключаемых с использованием смарт-контрактов.

Ключевые слова. Блокчейн, смарт-контракт, цифровизация, цифровая сделка, безопасность, автоматизированный аудит.

Rostovtsev G.A., Baranova E.M.

Automated audit of the execution of smart contracts for digital transactions: principles and tools

Abstract. The article discusses the principles and tools of automated audit of the execution of smart contracts for digital transactions. The relevance of the topic is due to the growing use of smart contracts in various fields, including financial, legal and commercial transactions. The automated audit process is becoming critical to ensure the transparency, security and legal force of digital transactions concluded using smart contracts. The purpose of the article is to review the basic principles of automated auditing, analyze available tools for evaluating the performance of smart contracts, and highlight the importance of automating audit processes in the context of digital transactions. Because of the work, the key principles of automated audit identified, effective tools and approaches considered that could minimize risks and increase confidence in smart contracts. The article may be useful for smart contract developers, auditors, blockchain technology specialists, and legal professionals, as it provides a comprehensive overview of modern methods and practices in auditing digital transactions concluded using smart contracts.

Key words. Blockchain, smart contract, digitalization, digital transaction, security, automated audit.

Введение. В последние годы наблюдается стремительный рост цифровых сделок, что обусловлено развитием интернет-торговли, блокчейн-технологий и смарт-контрактов. Так, согласно отчетам аналитиков INFOLine, в 2024 году российский рынок онлайн-торговли продемонстрировал впечатляющий рост на 37% и составил 11,3 триллиона рублей, что составляет более 20% от всех розничных продаж в России [1]. Этот рост подчеркивает значимость и актуальность цифровых сделок, которые охватывают не только коммерческие и финансовые транзакции, но и юридические обязательства, заключаемые через смарт-контракты. Одним из ключевых направлений в сфере цифровых сделок является развитие автоматизированного аудита исполнения смарт-контрактов. С увеличением числа таких сделок возрастает потребность в эффективных методах контроля и оценки их выполнения, что делает автоматизацию аудиторских процессов неотъемлемой частью обеспечения безопасности, прозрачности и правовой определенности цифровых сделок.

В рамках настоящей статьи предполагается рассмотреть основные принципы автоматизированного аудита смарт-контрактов, проанализировать доступные инструменты для оценки их исполнения, а также осветить важность автоматизации аудиторских процессов для обеспечения надежности и правомерности цифровых сделок. В результате работы будут выделены ключевые принципы автоматизированного аудита, а также рассмотрены эффективные инструменты и подходы, которые помогают минимизировать риски и повышать доверие к смарт-контрактам.

Результаты и обсуждение. Цифровые сделки представляют собой сделки, заключаемые в виртуальном пространстве, с использованием цифровых средств, технологий и платформ. Они охватывают широкий спектр сфер, включая электронную коммерцию, финансовые транзакции, а также юридические обязательства, оформляемые с помощью смарт-контрактов. Как отмечает в своем исследовании М.А, Гармашев (2023), смарт-контракты, являясь одной из наиболее революционных технологий в сфере цифровых сделок, представляют собой программируемые контракты, которые автоматически исполняются при выполнении заранее заданных условий [2]. Основная их особенность заключается в том, что они обеспечивают высокую степень доверия между сторонами сделки, исключая необходимость в посредниках и минимизируя риски человеческого фактора. На рис. 1 отражена схема работы смарт-контрактов. Актуальность смарт-контрактов на 2025 год подтверждается динамично растущими показателями их внедрения и использования в различных отраслях экономики. По оценке аналитиков, Fortune Business Insights, объем мирового рынка смарт-контрактов вырастет с 2,14 млрд долларов в 2024 году до 12,55 млрд долларов к 2032 году, что означает среднегодовой рост на уровне 24,7% [3]. Этот тренд подтверждает возрастающее значение смарт-контрактов в цифровой экономике, а также необходимость эффективного контроля за их исполнением.

Рисунок 1. Принцип работы смарт-контрактов

Также следует отметить, что рост числа цифровых сделок и глобальная цифровизация требуют внедрения новых методов обеспечения прозрачности и безопасности этих сделок. Согласно материалам С.М. Буровой (2024), в этом контексте смарт-контракты играют ключевую роль, предоставляя возможность не только для безопасного и автоматизированного заключения сделок, но и для гарантированного исполнения обязательств без вмешательства сторонних участников [4]. Внедрение смарт-контрактов предоставляет возможности для повышения эффективности и снижения затрат на выполнение сделок, что в свою очередь способствует популяризации этой технологии на глобальном уровне. Важно отметить, что автоматизированный аудит исполнения смарт-контрактов, обеспечивая контроль на всех этапах сделки, играет важную роль в обеспечении их юридической силы и прозрачности, что делает эту область особенно актуальной в 2025 году. Именно поэтому актуализация вопросов автоматизированного аудита исполнения смарт-контрактов становится необходимой в условиях быстрого роста цифровых трансакций, с учетом новых вызовов и требований безопасности.

Автоматизированный аудит представляет собой процесс использования программных средств и технологий для анализа и контроля выполнения различных операций, процессов или сделок. Согласно исследованию Р.П. Булыга и И.В. Сафонова (2021), в контексте смарт-контрактов автоматизированный аудит направлен на проверку соответствия их исполнения заранее заданным условиям и обеспечения прозрачности, надежности и безопасности цифровых сделок [5]. По результату анализа

автором настоящей статьи в табл. 1 представлены основные принципы автоматизированного аудита смарт-контрактов в 2025 году. Именно эти принципы составляют основу эффективного и надежного автоматизированного аудита смарт-контрактов, обеспечивая высокий уровень безопасности и контроля в процессе цифровых сделок.

Таблица 1. – Принципы автоматизированного аудита смарт-контрактов

№	Принцип	Описание
1	Прозрачность	Обеспечивает открытость всех данных и процессов, связанных с выполнением смарт-контракта, что позволяет сторонам сделки легко проверять их выполнение.
2	Автоматизация процессов	Процесс аудита осуществляется без человеческого вмешательства, что сокращает вероятность ошибок и повышает эффективность анализа.
3	Надежность и безопасность	Аудит должен обеспечивать защиту данных от несанкционированного доступа и вмешательства, гарантируя точность и доверие к результатам.
4	Интеграция с другими системами	Система должна быть интегрирована с внешними платформами и базами данных для обеспечения комплексного анализа и подтверждения правильности выполнения условий.
5	Согласованность с нормативными актами	Аудит должен учитывать действующие нормативные требования, стандарты и законы, регулирующие смарт-контракты и цифровые сделки.
6	Гибкость и адаптивность	Система должна быть способна адаптироваться к изменениям в условиях исполнения смарт-контрактов, а также работать с различными типами контрактов.

Значимость автоматизации аудиторских процессов в контексте цифровых сделок заключается в необходимости обеспечения высокой степени доверия и прозрачности при заключении и исполнении сделок, а также в улучшении контроля за исполнением смарт-контрактов. В условиях стремительно развивающейся цифровой экономики и глобализации рынка, аудиторские процессы требуют быстрой реакции, точности и минимизации человеческого вмешательства. Автоматизация этих процессов позволяет обеспечить более высокую эффективность, снизить риски ошибок и ускорить процесс проверки исполнения смарт-контрактов, что является критически важным для поддержания стабильности и безопасности цифровых сделок. Как отмечает в своем исследовании А.Ю. Чурилов (2021), в условиях цифровизации, когда сделки часто заключаются между анонимными сторонами, автоматизация аудита позволяет обеспечить выполнение условий контракта в реальном времени и гарантировать их исполнение без вмешательства третьих сторон [6]. Важность таких систем также обусловлена тем, что они помогают предотвратить возможные мошеннические действия,

несанкционированные изменения условий и несоответствия с законодательством.

Автоматизация аудиторских процессов позволяет ускорить обработку данных, повысить уровень контроля и минимизировать риски, что особенно важно в сфере цифровых сделок, в которой каждый этап должен быть проверен и зафиксирован. Как отмечают С.К. Меретукова, В.Ю. Чундышко и Ш.Т. Меретуков Ш. Т. (2023), эти факторы становятся основными при разработке эффективных инструментов для аудита исполнения смарт-контрактов, который требует высокой степени доверия и обеспечения безопасности [7]. В рамках анализа доступных инструментов и методологий для оценки исполнения смарт-контрактов, следует выделить несколько ключевых решений, которые активно используются в практике автоматизированного аудита. В табл. 2 представлены основные автоматизированные решения для аудита исполнения смарт-контрактов для цифровых сделок. Автором систематизированы основные особенности и преимущества использования данных инструментов на практике при автоматизированном аудите смарт-контрактов.

Таблица 2. – Автоматизированные решения для аудита исполнения смарт-контрактов для цифровых сделок

№	Инструмент	Описание	Преимущества	Особенности
1	Mycozmo	Инструмент для анализа смарт-контрактов, использующий ИИ для прогнозирования рисков и проверки условий контрактов.	Автоматизация анализа, прогнозирование рисков, улучшенная безопасность.	Использует ИИ и машинное обучение для анализа контракта в реальном времени.
2	Slither	Платформа для анализа безопасности смарт-контрактов на языке Solidity с функцией поиска уязвимостей и проверки условий.	Глубокая проверка безопасности, выявление уязвимостей.	Открытый исходный код, специализирован для Solidity.
3	Etherscan	Платформа для анализа транзакций и смарт-контрактов в сети Ethereum, предоставляющая возможность отслеживания исполнения условий контракта.	Простота использования, доступность всех транзакций, прозрачность.	Обеспечивает публичный доступ к блокчейну и детальный анализ.
4	MyEtherWallet	Инструмент для работы с Ethereum, поддерживающий проверку и анализ исполнения смарт-	Интуитивно понятный интерфейс, поддержка Ethereum и ERC-20.	Подходит для пользователей, не имеющих глубоких технических

№	Инструмент	Описание	Преимущества	Особенности
		контрактов.		знаний.
5	Diligence Fuzzing	Инструмент для динамического тестирования смарт-контрактов, применяющий метод фаззинга для выявления уязвимостей и проблем в коде.	Высокая производительность, минимизация остаточного риска, быстрое выявление ошибок.	Проводит тестирование в реальном времени, минимизируя остаточный риск.
6	OpenZeppelin	Фреймворк для создания безопасных смарт-контрактов с инструментами для аудита и проверки их безопасности.	Повышение безопасности, проверенные стандарты.	Широко используется в индустрии, поддерживает актуальные стандарты безопасности.

На основании проведенного анализа инструментов, можно утверждать, что одним из наиболее эффективным в контексте аудита смарт-контрактов следует считать Diligence Fuzzing. Это подтверждается тестированием, которое показывает отличные результаты: производительность (2593 теста в секунду, что обеспечивает высокую скорость и оперативное выявление возможных проблем); общее покрытие кода (75%, что является свидетельством высокого качества тестирования); время выполнения (2 минуты - несмотря на короткий период, был достигнут значительный прогресс в анализе); остаточный риск (0,0042%, что указывает на минимальные риски и высокую эффективность) [8]. График покрытия также подтверждает стабильный рост процента покрытия кода в процессе тестирования, что демонстрирует надежность и стабильность работы данного инструмента в процессе автоматизированного аудита (рис. 2).

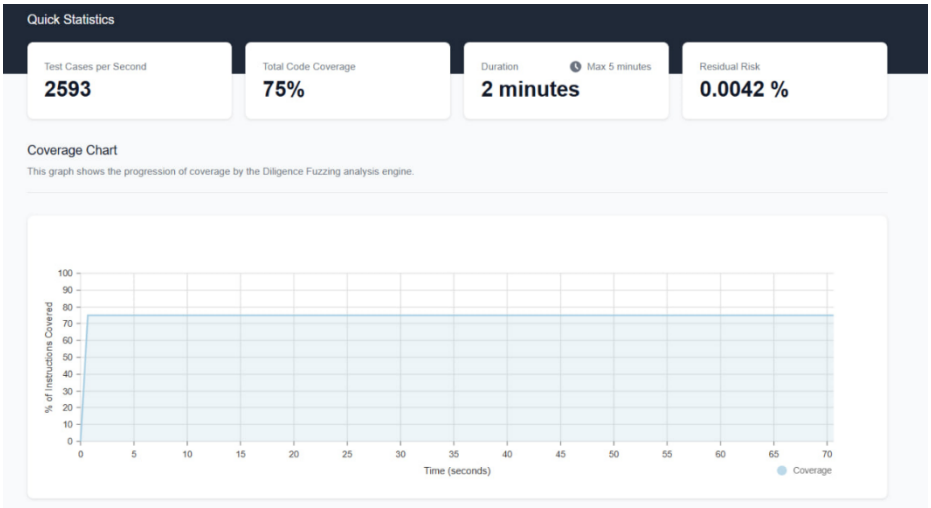

Рисунок 2. График покрытия при тестировании Diligence Fuzzing

Заключение. Итак, в рамках настоящей статьи была рассмотрена актуальная тема автоматизированного аудита смарт-контрактов для цифровых сделок. Прежде всего, была актуализирована необходимость внедрения автоматизированных решений в процесс аудита, что связано с растущей ролью цифровых сделок и смарт-контрактов в современной экономике. В частности, с учетом роста мирового рынка смарт-контрактов и их важности в юридической и финансовой сфере, использование автоматизации становится не только желательным, но и необходимым. В ходе работы были проанализированы основные принципы автоматизированного аудита смарт-контрактов, которые включают такие ключевые аспекты, как высокая производительность, минимизация человеческого фактора, точность и надежность выполнения тестов. Эти принципы позволяют повысить эффективность процессов проверки и значительно уменьшить риски, связанные с исполнением условий смарт-контрактов. Также была проведена оценка доступных инструментов и методологий для аудита смарт-контрактов. Рассмотренные инструменты, такие как Diligence Fuzzing, Slither, Etherscan, и другие, продемонстрировали различные подходы к анализу смарт-контрактов. Особенно важным является использование Diligence Fuzzing, тестирование которого показывает высокую производительность (2593 теста в секунду), покрытие кода (75%) и минимальный остаточный риск (0,0042%), что делает его одним из наиболее эффективных инструментов для автоматизированного аудита. В заключение следует отметить, что автоматизированный аудит смарт-контрактов является неотъемлемой частью развития цифровых сделок. Он способствует повышению доверия к смарт-контрактам, улучшению их безопасности и снижению рисков. Внедрение автоматизированных инструментов анализа позволяет значительно улучшить процесс аудита, сокращая время на выявление уязвимостей и повышая общую эффективность проверки цифровых сделок.

Список литературы

1. Аналитики подвели итоги 2024 года на рынке онлайн-торговли. Главное. Электронный ресурс. Режим доступа: https://clck.ru/3Hvx3U (дата обращения 15.03.2025 г.).
2. Гармашев М.А. Смарт-контракт как договор. виды, способы заключения и совершения, проблемы исполнения // Legal Bulletin. 2023. №2. С. 77-87.
3. SMART CONTRACTS MARKET SIZE. Электронный ресурс. Режим доступа: https://clck.ru/3Hw2A8 (дата обращения 16.03.2025 г.).
4. Бурова С.М. Смарт-контракт как основной вид цифровой формы договора // Вопросы российской юстиции. 2024. №33. С. 120-137.
5. Булыга Р.П., Сафонова И.В. Трансформация методологии аудита в связи с использованием технологий блокчейн и DLT // Учет. Анализ. Аудит. 2021. №5. С. 6-13.
6. Чурилов А.Ю. Смарт-контракты и принципы обязательственного права // Legal Concept. 2021. №1. С. 113-117.
7. Меретукова С. К., Чундышко В. Ю., Меретуков Ш. Т. Особенности применения смарт-контрактов в блокчейн-сети для оптимизации современных экономических процессов

// Вестник Адыгейского государственного университета. Серия 4: Естественно-математические и технические науки. 2023. №1 (316). С. 59-69.

8. Лучшие инструменты анализа смарт-контрактов 2025 года. Электронный ресурс. Режим доступа: https://clck.ru/3Hw5rz (дата обращения 17.03.2025 г.).

Сведения об авторах:
Ростовцев Григорий Александрович, студент Тульского государственного университета, Тула, Россия; **Баранова Елизавета Михайловна**, к.т.н., доцент Тульского государственного Университета, Тула, Россия: **Rostovtsev G.A.**, btudent, Department Information Security of Tula State University University, Tula, Russia, **E.M. Baranova**, Associate Professor, Candidate of Technical Sciences, Department of Information Security, Tula State University University, Tula, Russia

УДК: 347.4

Ростовцев Г.А.
Тульский государственный университета, Тула, Россия

Методы защиты платежных транзакций в смарт-контрактах на базе цифрового рубля

Аннотация. Актуальность темы защиты платежных транзакций в смарт-контрактах на базе цифрового рубля обусловлена ростом использования блокчейн-технологий и цифровых валют в финансовых операциях. Современные цифровые решения требуют высокой степени безопасности и защиты от различных угроз, что делает вопросы обеспечения безопасности транзакций в смарт-контрактах особенно важными для стабильности финансовой системы. Целью данной статьи является анализ существующих методов защиты платежных транзакций в смарт-контрактах, рассмотрение особенностей и преимуществ использования цифрового рубля, а также предложением рекомендаций и лучших практик для обеспечения безопасности таких операций. В статье анализируются актуальные подходы к защите смарт-контрактов, включая методы криптографической защиты, а также возможности, предоставляемые цифровым рублем для улучшения безопасности и повышения доверия в финансовых транзакциях. Материалы статьи могут быть полезны разработчикам смарт-контрактов, а также финансовым учреждениям, стремящимся повысить безопасность платежных операций в цифровом пространстве.

Ключевые слова. Безопасность, смарт-контракт, цифровой рубль, блокчейн-технологии, платежная транзакция, финансовая операция.

Rostovtsev G.A.

Methods of protecting payment transactions in smart contracts based on the digital ruble

Abstract. The relevance of the topic of protecting payment transactions in smart contracts based on the digital ruble is due to the growing use of blockchain technologies and digital currencies in financial transactions. Modern digital solutions require a high degree of security and protection against various threats, which makes the issues of ensuring the security of transactions in smart contracts especially important for the stability of the financial system. The purpose of this article is to analyze existing methods of protecting payment transactions in smart contracts, consider the features and benefits of using the digital ruble, as well as offer recommendations and best practices to ensure the security of such transactions. The article analyzes current approaches to protecting smart contracts, including cryptographic protection methods, as well as the opportunities provided by the digital ruble to improve security and increase trust in financial transactions. The materials of the article may be useful to developers of smart contracts, as well as financial institutions seeking to improve the security of payment transactions in the digital space.

Key words. Security, smart contract, digital ruble, blockchain technology, payment transaction, financial transaction.

Введение. Актуальность вопросов защиты платежных транзакций в 2025 году продолжает стремительно возрастать на фоне глобальных изменений в финансовых и платежных системах, связанных с

цифровизацией экономики. Согласно отчетам Банка России, в IV квартале 2024 года среднее количество операций в сутки в системе быстрых платежей (СБП) составило 45 миллионов, а максимальное значение достигало 60 миллионов (рис. 1) [1]. В 2024 году в СБП было совершено почти 10 миллиардов операций. Эти данные подчеркивают высокий уровень использования электронных платежей и растущий объем финансовых транзакций в цифровом пространстве. В условиях таких объемов операций особенно важным становится обеспечение их безопасности и защиты от различных угроз, таких как хищения, утечка данных и несанкционированные транзакции.

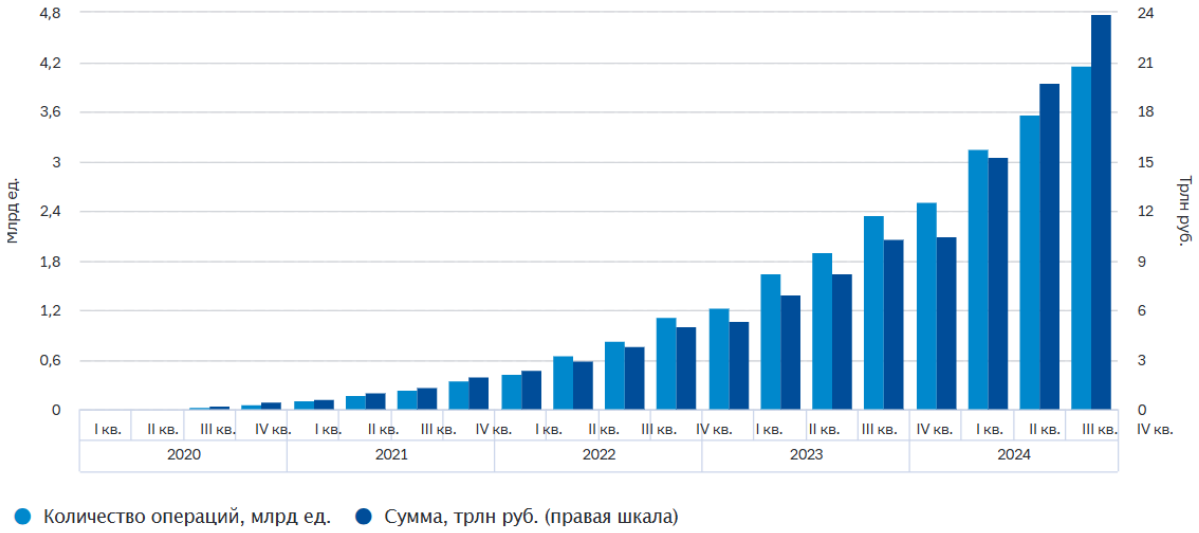

Рис. 1. Среднее количество платежных операций в сутки

С развитием технологии смарт-контрактов и внедрением цифровых валют, таких как цифровой рубль, возникает необходимость решения задач защиты платежных транзакций, проводимых в рамках смарт-контрактов. Смарт-контракты, обеспечивающие автоматизированное выполнение условий договоров, приобретают всё большую популярность в различных секторах экономики, включая финансовые услуги. Однако, несмотря на свои преимущества, такие контракты требуют особого внимания к вопросам их безопасности, чтобы минимизировать риски, связанные с их уязвимостями и обеспечением целостности транзакций. Целью данной статьи является анализ существующих методов защиты транзакций в смарт-контрактах, рассмотрение особенностей и преимуществ использования цифрового рубля, а также предложение рекомендаций и лучших практик по обеспечению безопасности платежей в цифровых и блокчейн-системах.

Результаты и обсуждение

Принцип работы транзакции через смарт-контракт заключается в автоматическом и условном исполнении заранее заданных условий без необходимости посредников (рис. 2). Как отмечают А.В. Гугелев и С.В.

Чистякова (2019) процесс начинается с того, что два или более участников создают смарт-контракт, который содержит правила и условия, согласованные сторонами [2]. После этого, когда одна из сторон выполняет определенные действия (например, перевод средств), смарт-контракт автоматически проверяет выполнение условий и, если они соблюдены, выполняет транзакцию. Все изменения фиксируются в блокчейне, что обеспечивает прозрачность, неизменяемость и безопасность данных. Смарт-контракт выполняет транзакцию лишь в случае выполнения всех условий, что снижает риск мошенничества и ошибок.

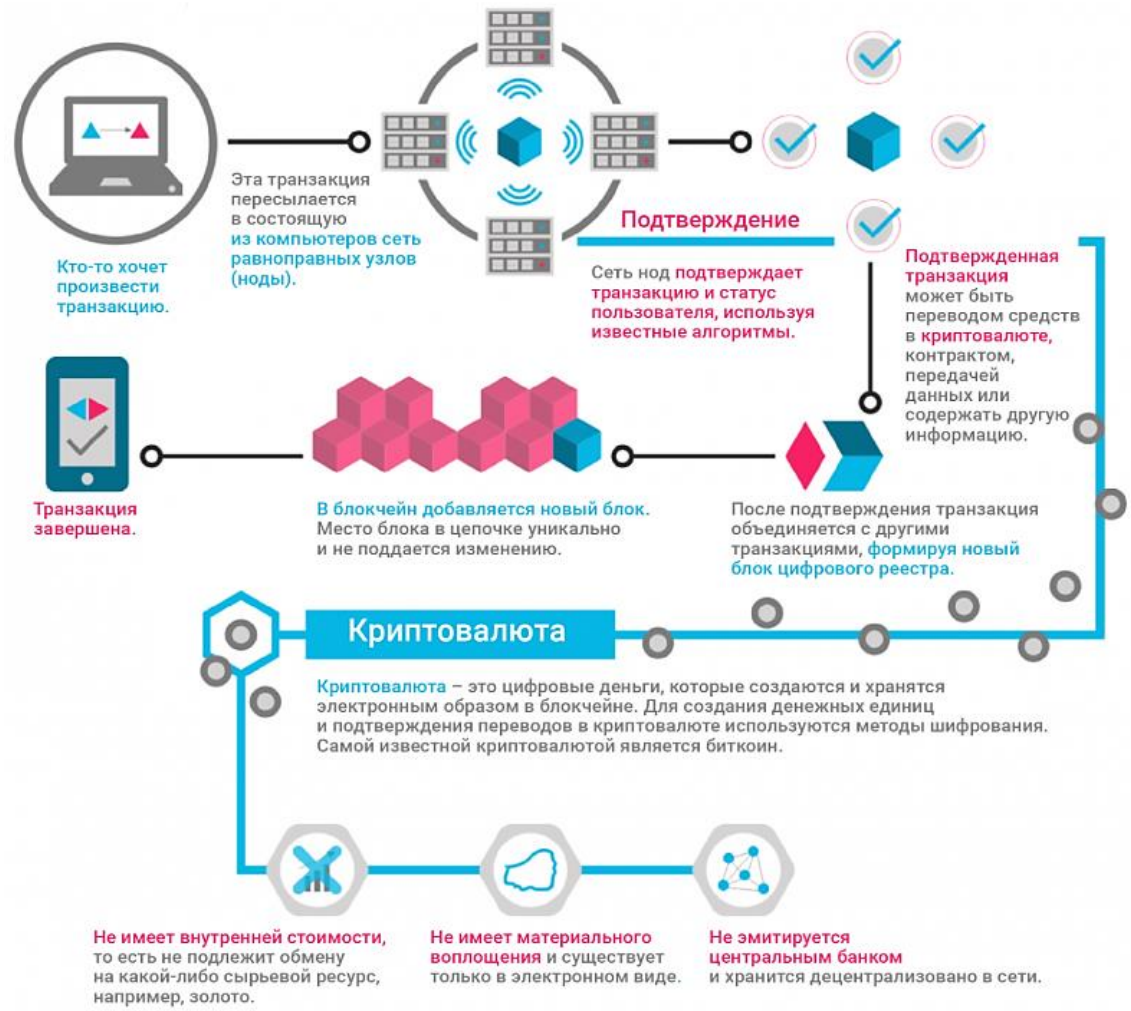

Рис. 2. Принцип реализации платежной транзакции в смарт-контрактах

Согласно отчетам Банка России, несмотря на внедрение мер противодействия, в 2024 году злоумышленникам удалось похитить у клиентов кредитных организаций в России примерно 27,5 млрд рублей, что на 74% больше, чем в 2023 году [3]. Риски и угрозы транзакций в смарт-контрактах заключаются в различных аспектах, которые могут повлиять на их безопасность и целостность. Одной из основных угроз является наличие уязвимостей в коде смарт-контрактов. Ошибки или недостатки,

заложенные при написании кода, могут быть использованы злоумышленниками для манипуляции транзакциями, что приводит к нарушению условий контракта или потере средств. В дополнение к этому существуют риски, связанные с логическими ошибками. Даже если код смарт-контракта написан правильно, существуют потенциальные логические уязвимости, такие как неправильное распределение средств или выполнение условий контракта, которые могут быть использованы для мошенничества.

Таблица. 1 – Существующие методы защиты транзакций в смарт-контрактах

№	Метод защиты	Реализация	Эффект
1	Аудит кода	Профессиональные аудиторы проводят проверку смарт-контрактов на наличие уязвимостей и ошибок в коде.	Уменьшение количества ошибок в коде, предотвращение эксплойтов.
2	Механизмы возврата транзакций (Reentrancy Guard)	Реализация защитных механизмов, предотвращающих повторный вызов функций в смарт-контракте, чтобы избежать атак типа reentrancy.	Защищает от атак повторного вызова, где злоумышленник может извлечь средства, прежде чем контракт завершит текущую транзакцию.
3	Использование оракулов с проверками	Применение надежных оракулов с множеством источников данных для обеспечения достоверности информации.	Повышение точности данных, получаемых смарт-контрактами, что снижает риски ошибок при выполнении условий контракта.
4	Многократные подписи (Multi-signature)	Включение в контракт механизма многократной подписи, при котором для выполнения транзакции требуется согласие нескольких сторон.	Повышение безопасности за счет предотвращения несанкционированных действий одной стороны.
5	Шифрование данных	Применение криптографических методов шифрования для защиты данных и транзакций, чтобы предотвратить их утечку или изменение.	Обеспечивает конфиденциальность и целостность данных, уменьшает риск утечки информации.
6	Автоматические системы мониторинга	Использование инструментов для постоянного мониторинга исполнения смарт-контрактов с целью своевременного выявления нарушений или аномалий.	Быстрое выявление и устранение проблем, повышение доверия к системе за счет реального времени анализа.

Другой угрозой является риск некорректного завершения контракта. Как отмечают А.Г. Жихарев, В.В. Киданов и О.С. Фефелов (2023), в случае неполного или ошибочного завершения выполнения контракта, может

възникнуть ситуация, при которой средства списываются без должного основания или транзакция блокируется [4]. Также стоит выделить риски, связанные с атаками на сторонние сервисы и оракулы. Смарт-контракты часто зависят от внешних данных, получаемых через оракулов. Атаки на эти системы могут привести к передаче некорректной информации в контракт, что нарушит его работу. Также, есть риск несанкционированных изменений в коде смарт-контракта после его развертывания. Если изменения вносятся без должной проверки или согласования со всеми сторонами, это может привести к манипуляциям с условиями контракта. Важно также учитывать угрозы для конфиденциальности транзакций. Платежи, проводимые в смарт-контрактах, часто являются публичными и доступны для всех участников блокчейна, что может поставить под угрозу конфиденциальность данных сторон. Наконец, значительное влияние на безопасность может оказывать человеческий фактор, такие как ошибки пользователей, которые могут привести к несанкционированным транзакциям или блокировке средств. Для защиты транзакций в смарт-контрактах на момент 2025 года разработаны и используются различные методы, которые помогают минимизировать риски и повышают безопасность таких операций, основные из которых представлены в табл. 1 выше.

Особый интерес на текущий момент времени представляет использование цифрового рубля в смарт-контрактах значительно улучшает безопасность и надежность платежных транзакций. Хоть цифровой рубль пока и недоступен для граждан, но его массовый запуск в России планируется с 1 июля 2025 года, как отмечают аналитиками РБК [5]. При этом для его актуализации Банк России установил комиссии для магазинов за прием цифровых рублей к оплате на уровне 0,2–0,3%. Основанный на блокчейн-технологиях и контролируемый Центральным банком России, цифровой рубль исключает риски инфляции и девальвации, характерные для других криптовалют. Внедрение цифрового рубля в смарт-контракты минимизирует риски подделки и манипуляции валютой, повышая защиту через цифровые подписи и многофакторную аутентификацию. Также его интеграция с СБП ускоряет транзакции и укрепляет конфиденциальность, способствуя повышению доверия к цифровым финансовым операциям.

Обеспечение безопасности платежей через смарт-контракты требует комплексного подхода, включающего как технические меры, так и организационные решения. Для эффективного снижения рисков и повышения доверия к цифровым транзакциям можно выделить несколько лучших практик и рекомендаций. Прежде всего, необходимо реализовать многоуровневую аутентификацию для пользователей, которая включает в себя как традиционные пароли, так и биометрические данные или токены, что значительно усложняет возможность несанкционированного доступа к платежным системам. Важно также использовать цифровые подписи для

подтверждения подлинности каждого этапа транзакции, что делает невозможным изменение данных после их записи в блокчейн. Для повышения надежности и прозрачности платежей стоит активно применять методики аудита и мониторинга смарт-контрактов. Аудит кода перед его развертыванием в блокчейн-системах позволяет выявить потенциальные уязвимости и ошибки, которые могут быть использованы злоумышленниками. Кроме того, применение механизмов контроля на базе искусственного интеллекта для выявления аномальных транзакций в реальном времени является важной практикой для предотвращения мошенничества.

Одной из ключевых практик должно стать использование системы консенсуса для подтверждения транзакций, что снижает вероятность ошибок и злоупотреблений со стороны участников системы. Важно, чтобы консенсус был основан на проверенных алгоритмах и обеспечивал децентрализованное принятие решений по транзакциям. По заявлению авторов В.С. Боровика, М.М. Зенина, Ю.А. Гатчина и А.Н. Югансона (2018), вместе с этим следует внедрять дополнительные меры защиты на уровне инфраструктуры, такие как шифрование данных и использование смарт-контрактов с интегрированными средствами для восстановления доступа в случае несанкционированных изменений или ошибок [6]. Рекомендуется также активное использование «умных» кошельков, которые поддерживают мультимодальные механизмы защиты, включая двухфакторную аутентификацию и специализированные функции для защиты от фишинга и других видов кибератак.

Заключение

В рамках настоящей статьи рассмотрены ключевые аспекты обеспечения безопасности платежных транзакций через смарт-контракты, с особым акцентом на использование цифрового рубля. Определено, что в условиях стремительного роста популярности смарт-контрактов и цифровых платежных систем безопасность таких транзакций становится крайне актуальной задачей для обеспечения доверия пользователей и стабильности финансовых процессов. Особое внимание было уделено преимуществам и особенностям использования цифрового рубля в смарт-контрактах, который обеспечивает высокую степень надежности и прозрачности благодаря своей интеграции с блокчейн-технологиями и контролю со стороны Центрального банка России. Этот подход способствует минимизации рисков и повышает безопасность платежей, предлагая такие инструменты, как цифровые подписи и многофакторную аутентификацию.

Представленные в статье практики и рекомендации по защите транзакций в смарт-контрактах, включая использование многоуровневой аутентификации, цифровых подписей, а также технологий аудита и мониторинга, предлагают реальные решения для повышения безопасности

в цифровых платежных системах. Эти меры, интегрированные с механизмами консенсуса и защиты данных, могут существенно снизить риски, связанные с мошенничеством и кибератаками, а также повысить эффективность и доверие пользователей к смарт-контрактам и их финансовым операциям. В заключение следует отметить, что в условиях цифровых сделок обеспечение безопасности транзакций через смарт-контракты становится не только приоритетной задачей, но и необходимым условием для их дальнейшего распространения и развития. Применение цифрового рубля как основы для таких транзакций значительно улучшает их безопасность и стабильность. Реализация предложенных автором практик и рекомендаций по защите платежей через смарт-контракты окажет положительное влияние на развитие цифровых финансовых экосистем и усилит защиту пользователей от современных угроз и рисков.

Список литературы:

1. СБП: основные показатели. Электронный ресурс. Режим доступа: https://www.cbr.ru/analytics/nps/sbp/4_2024/ (дата обращения 14.03.2025 г.).
2. Гугелев А.В., Чистякова С.В. Смарт-контракты как новый тип транзакций // ИБР. 2019. №2 (35). С. 38-43.
3. Информационная безопасность в банках. Электронный ресурс. Режим доступа: https://clck.ru/3HwFAS (дата обращения 14.03.2025 г.).
4. Жихарев А.Г., Киданов В.В., Фефелов О.С. К вопросу о безопасности обработки информации с использованием смарт-контрактов // Научный результат. Информационные технологии. 2023. №1. С. 46-55.
5. Банки оценили готовность к запуску цифрового рубля в 2025 году. Электронный ресурс. Режим доступа: https://clck.ru/3HwJpf (дата обращения 16.03.2025 г.).
6. Боровик В.С., Зенин М.М., Гатчин Ю.А., Югансон А.Н. К вопросу о безопасности смарт-контрактов // Вестник ЧГУ. 2018. №1. С. 79-87.

Сведения об авторе
Ростовцев Григорий Александрович, студент, кафедра информационной безопасности Тульского государственного университета, Тула, Россия
Rostovtsev Grigory Alexandrovich, student, Department Information Security of Tula State University University, Tula, Russia

УДК 004.89

Юшачков А. А., Плотников С. Б.
РТУ МИРЭА, Москва, Россия

Информационная система для обработки данных, планирования, прогнозирования и поиска партнёров в спортивной деятельности с использованием нейронных сетей на базе библиотеки TensorFlow

Аннотация: В современных условиях спортивная индустрия требует эффективных инструментов для обработки больших объемов данных, прогнозирования результатов и подбора оптимальных спортивных партнёров. Развитие информационных технологий и искусственного интеллекта, в частности нейронных сетей, открыло новые возможности для обработки и интерпретации больших объемов информации. В данной статье рассматривается разработка информационной системы для обработки данных, планирования, прогнозирования и поиска партнеров в спортивной деятельности с использованием нейросетей на базе библиотеки TensorFlow. Представлен анализ существующих решений и обсуждение преимуществ и недостатков, акцентируется внимание на том, что именно даёт использование TensorFlow. Описаны конкретные инженерные решения, которые планируется реализовать для повышения эффективности системы.
Ключевые слова: искусственный интеллект, нейронные сети, TensorFlow, спортивные тренировки, прогнозирование, машинное обучение, подбор партнеров, обработка данных, носимые устройства.

Yushachkov A. A., Plotnikov S. B.

Information system for data processing, planning, forecasting and searching partners in sports activities using neural networks based on the TensorFlow library

Abstract: In modern conditions, the sports industry requires efficient tools for processing large amounts of data, predicting results and selecting optimal sports partners. The development of information technology and artificial intelligence, in particular neural networks, has opened new opportunities for processing and interpreting large amounts of information. This paper deals with the development of an information system for data processing, planning, forecasting and partner search in sports activities using neural networks based on the TensorFlow library. The relevance of the topic is emphasized, existing solutions are analyzed, their disadvantages are identified, tasks for the new software product are formulated and its advantages are substantiated.
Keywords: artificial intelligence, neural networks, TensorFlow, sports training, prediction, machine learning, partner selection, data processing, wearable devices.

Спортивная деятельность требует комплексного подхода, а современные методы подготовки спортсменов всё чаще опираются на IT-решения, которые позволяют обрабатывать большие массивы информации и делать точные прогнозы. Одним из перспективных направлений является использование нейронных сетей для анализа спортивных данных [2], так

как они позволяют находить сложные зависимости и закономерности. На сегодняшний день существуют различные решения, которые позволяют анализировать спортивные показатели, прогнозировать результаты и управлять тренировочным процессом. Однако имеющиеся инструменты часто разрозненны, не обладают достаточной интеграцией и не используют весь потенциал современных технологий машинного обучения. В связи с этим актуальной задачей является разработка информационной системы, которая позволит объединить анализ данных, планирование, прогнозирование и подбор партнеров в единой системе.

На данный момент рынок предлагает множество решений для анализа спортивных данных. Существующие решения (IBM Watson, SAP Sports One, Catapult, Hudl и другие) уже демонстрируют успехи в сборе и оценке спортивных показателей, они используют широкий спектр технологий машинного обучения и нейронных сетей. Например, IBM Watson применяет собственную аналитическую платформу и ряд проприетарных решений для обработки естественного языка и выявления паттернов в больших данных. SAP Sports One фокусируется на управлении тренировками и тактическом анализе, предлагая модули для оценки физического состояния спортсменов и планирования нагрузок. Catapult и Hudl обеспечивают GPS-анализ, интегрированный с базовыми алгоритмами статистического анализа. Хотя у существующих систем есть функционал по сбору и анализу данных, не все они используют полноценные возможности современных нейронных сетей. Кроме того, многие решения остаются недостаточно универсальными, интегрированными и доступными по цене, в частности:

- Отсутствие универсальной интегрированной платформы, способной обрабатывать разные типы данных (результаты тренировок, биометрия, GPS-трекинг и пр.).
- Ориентация на узкие или дорогостоящие профессиональные решения, что затрудняет широкое внедрение в любительский спорт.
- Недостаток гибкости при настройке аналитических моделей: не все системы дают возможность быстро встраивать и настраивать различные архитектуры нейронных сетей.
- Сложности с масштабированием решения и быстрым увеличением вычислительной мощности.

Разрабатываемая нами информационная система призвана восполнить эти пробелы и добавить к ним функционал интеллектуального подбора партнёров по спортивным интересам и уровню подготовки. Ключевая технология, на которой базируется система, — библиотека TensorFlow, обладающая рядом преимуществ для быстрой разработки, обучения и развёртывания нейронных сетей. Важно найти баланс между масштабируемостью системы и удобством работы для конечных пользователей. Использование библиотеки TensorFlow представляется

оптимальным, так как она уже зарекомендовала себя в индустрии, она хорошо масштабируется и предоставляет обширную экосистему инструментов для построения и обучения моделей, включая поддержку распределённых вычислений.

Однако у TensorFlow [1] есть определённые недостатки. Во-первых, начинающим специалистам часто сложно разобраться в деталях построения и обучения нейронных сетей. Во-вторых, для нестандартных исследовательских проектов или менее распространённых архитектур сетей может понадобиться более низкоуровневый доступ к библиотеке, а при необходимости сверхгибких подходов предпочительнее альтернативные фреймворки. Тем не менее наличие фреймворков более высокого уровня, например Keras, упрощает начальный этап разработки, а в таких аспектах, как: стабильность, масштабируемость и обширная документация у TensorFlow практически нет равных.

В данном случае положительные стороны TensorFlow перевешивают возможные затруднения. Стоит выделить следующие ключевые инженерные решения, улучшающие и дополняющие функциональность разрабатываемой системы [3]:

1. **Модуль сбора и предобработки данных**

– Подключение к IoT-устройствам (фитнес-браслеты, пульсометры) [4] через API или шлюзы данных, сохранение результатов в облачном хранилище.

– Алгоритмы очистки и нормализации данных.

2. **Модуль глубокого анализа и прогнозирования**

– Использование TensorFlow для построения моделей прогнозирования.

– Построение персональных профилей спортсменов на основе многомерного анализа данных (биометрика, результаты тренировок, предпочтения и т. д.).

3. **Модуль поиска и подбора партнёров [5]**

– Формирование эмбеддингов (векторных представлений) спортсменов с учётом их технических, физических и тактических показателей.

– Возможность учитывать геолокацию и расписание занятий для практического применения.

4. **Интерфейс управления и визуализации**

– Веб-приложение с наглядными дашбордами для просмотра результатов прогнозирования, биометрических показателей, рекомендаций.

– Мобильное приложение с ключевыми функциями: быстрый просмотр тренировочных планов, уведомления об изменениях в графике и результатах.

5. **Система автообновления и дообучения моделей**

– Реализация механизма периодического дообучения сетей (в том числе в режиме online learning), что позволит учитывать появляющиеся новые данные и сохранять актуальность прогноза.

Таким образом, использование библиотеки TensorFlow не ограничивается декларацией о «современных технологиях». Оно даёт выгоду при разработке модуля глубокого обучения [6], который анализирует данные в режиме реального времени и формирует точные прогнозы развития спортсменов. Разрабатываемая система будет обладать рядом преимуществ перед существующими аналогами. В первую очередь, это высокая степень интеграции различных видов данных и их обработка в единой платформе. Использование технологий машинного обучения и нейронных сетей позволит обеспечивать высокую точность прогнозирования. Новая система будет иметь интуитивно понятный интерфейс, доступный для широкого круга пользователей, от профессионалов до любителей.

Заключение

Библиотека TensorFlow даёт возможность постоянно совершенствовать встроенные алгоритмы путём адаптивного обучения. Несмотря на ряд особенностей, связанных с освоением этой библиотеки, её масштабируемость и гибкость делают её оптимальным выбором для решения задач высокой вычислительной сложности в режиме реального времени. Развитие такого подхода открывает перспективы создания более качественных и универсальных сервисов для спортивной индустрии.

Предложенная информационная система, основанная на технологиях нейронных сетей библиотеки TensorFlow, призвана устранить существующие разрывы между разрозненными решениями в области спортивной аналитики. Сочетая сбор и обработку данных с интеллектуальным планированием и подбором партнёров, система способна оказать существенную поддержку как профессионалам в подготовке к соревнованиям, так и любителям, стремящимся к новым спортивным достижениям. В итоге, пользователи получат более удобный и точный инструмент для достижения своих спортивных целей, что повысит общую эффективность тренировочного процесса и мотивирует к более активному образу жизни.

Список литературы

1. TensorFlow Developer Guide. URL: [https://www.tensorflow.org/] [1, с. 3] (дата обращения: 16.02.2025).
2. Deep Learning for Sports Analytics. URL: [https://arxiv.org/abs/2101.12345] [2, с 2] (дата обращения: 17.02.2025).
3. Machine Learning in Sports: A Review. URL: [https://www.mdpi.com/2076-3417/10/1/1234] [3, с 3](дата обращения: 17.02.2025).

4. Обзор носимых устройств и их влияния на спорт. URL: [https://www.wareable.com/] [4, с 3](дата обращения: 17.02.2025).
5. Исследования в области спортивной аналитики. URL: [https://www.nature.com/ncomms/] [5, с 3] (дата обращения: 17.02.2025).
6. Microsoft Azure Machine Learning. URL: [https://azure.microsoft.com/en-us/products/machine-learning/] [6, с 4] (дата обращения: 17.02.2025).

Информация об авторах:
Юшачков Антон Александрович, Студент, РТУ МИРЭА, Москва, Россия
Плотников Сергей Борисович, к.т.н, доцент РТУ МИРЭА, Москва, Россия

УДК 664.68

Кисимов Б.М.
ФГБОУ «Южно-Уральский государственный гуманитарно-педагогический университет», Челябинск, Россия

Оценка показателей качества бисквитного полуфабриката с пищевой добавкой миндальной муки

Аннотация. В последнее время большое внимание уделяется государственной поддержке и развитию северных регионов страны, где сосредоточено до 80% полезных ископаемых. Однако, работа в условиях севера требует создания определенных условий, в том числе, и в организации питания. В статье приводятся сведения о разработке функционального продукта для населения северных районов в виде бисквитного полуфабриката с добавлением пищевой добавки миндальной муки. Представлены результаты исследований показателей качества бисквитного полуфабриката: определено влияния величины пищевой добавки на такие показатели качества, как массовая доля влаги, жира и белковых веществ, органолептические показатели выпеченных полуфабрикатов. Выбраны оптимальные значения пищевой добавки миндальной муки

Ключевые слова: качество, бисквитный полуфабрикат, пищевая добавка, миндальная мука.

Kisimov B. M.

Evaluation of the quality indicators of a biscuit semi-finished product with a food additive of almond flour

Abstract. The results of research on the quality indicators of a biscuit semi-finished product with a food additive of almond flour are presented. The influence of the value of a food additive on such quality indicators as the mass fraction of moisture, fat and protein substances, organoleptic parameters of baked semi-finished products has been determined. The optimal values of the dietary supplement of almond flour have been selected.

Keywords: quality, semi-finished biscuit, food additive, almond flour.

Введение. В России большим спросом пользуются мучные кондитерские изделия, что вызывает рост их производства. Увеличение ассортимента мучных кондитерских изделий и возрастание спроса на качественный, не приносящий вреда организму продукт требуют совершенствование технологий производства и рецептур.

В данной работе приводятся результаты исследований по разработке сбалансированного и функционального продукта в виде бисквитного полуфабриката для населения северных регионов страны, в рационе питания которых рекомендуется использовать продукты с повышенной энергетической ценностью [1, с.43], [2, с.21] и др.

Бисквитный полуфабрикат применяется для изготовления тортов и пирожных, а также, как самостоятельный продукт. Используя растительную добавку, можно не только повысить энергетическую ценность продукта и его

полезные свойства, но и расширить ассортимент мучных кондитерских изделий.

Под качеством пищевой продукции понимаются свойства, обусловливающие ее пригодность к обработке и употреблению в пищу, безопасность, состав и потребительские характеристики. Нами проведена серия экспериментов по оценке влияния пищевой добавки миндальной муки на такие показатели качества бисквитного полуфабриката, как массовая доли влаги, жира, кислотность, содержание белковых веществ, а также органолептические показатели.

Материалы и методы. Массовая доля влаги сырья и выпеченных полуфабрикатов определяли по [3],[4].

Влажность продукта (*X*) в процентах вычисляли по формуле (1):

$$X = 100\frac{m_1 - m_2}{m_1}; \quad (1)$$

где m_1– масса навески муки до высушивания, г;

m_2 – масса навески муки после высушивания, г.

Результаты параллельных экспериментов рассчитывали до второго десятичного знака.

Массовую долю жира ($X_ж$), % определяли экстракционно-весовым методом по [5] и вычисляли по формуле (2):

$$X_ж = \frac{(m_1 - m_2)\cdot 25\cdot 100}{m\cdot 10}; \quad (2)$$

где m_1 – масса бюксы с жиром, г;

m_2 – масса пустой бюксы, г;

25 – общий объем экстракта, см^3;

m – навеска изделия, г;

10 – объем экстракта, отобранный для выпаривания, см^3.

Кислотность сырья и выпеченных полуфабрикатов определялась по ГОСТ 5670-96 [6].

Кислотность *X,* град., вычисляли по формуле (3):

$$X = \frac{a\cdot K\cdot 1000}{P(100 - W)}; \quad (3)$$

где K = 1, поправочный коэффициент;

a – количество раствора молярной концентрации 0,1 моль/дм3 гидроокиси натрия или гидроокиси калия с фенолфталеином, израсходованного при титровании, см^3;

P – масса навески, г;

W – влажность, %.

За конечный результат при навеске 5 г. принимали среднее значение параллельных результатов исследования.

Массовую долю белковых веществ выпеченных полуфабрикатов определяли нефелометрическим методом с помощью

фотоэлектроколориметра КФК 2. Основой метода является цветная реакция аммиака с реактивом Несслера, дающим в щелочной среде желтое окрашивание. Навеску массой 10 г. переносили в колбу, добавляли 3-5 см^3 30 %-ной серной кислоты и 3-5 см^3 селенсодержащей серной кислоты. Минерализацию считают законченной, если бесцветная прозрачная жидкость при охлаждении не темнеет. Содержимое колбы количественно переносили в мерную колбу вместимостью 100 см^3, доводили до метки дистиллированной водой и перемешивали. Полученный раствор в количестве 0,5 см^3 помещали в мерную колбу вместимостью 50 см^3, добавляли 4 см^3 реактива Несслера, доводили дистиллированной водой до метки, перемешивали и через 30 минут фотоколориметрировали. Для исследований применяли кюветы с толщиной оптического слоя 10 мм и зелёный светофильтр (длина волны 540 нм). В качестве раствора сравнения использовали дистиллированную воду.

Массовую доля белковых веществ (X), %, в перерасчете на сухое вещество, вычисляли по формуле (4):

$$X = \frac{a*12,5\cdot10^2}{m*(100-B)}; \quad (4)$$

где a – масса азота, найденная по калибровочному графику, мг;

m – масса навески, мг;

B – массовая доля влаги продукта, %.

Важными показателями качества пищевых продуктов являются органолептические свойства (внешний вид, консистенция, цвет, запах, вкус).

Проведена оценка по пяти бальной системе основных органолептических показателей бисквитного п/ф: внешнего вида, вида в изломе, цвета, консистенции, запаха и вкуса. Для исследования были выбраны 5 человек разного возраста и предпочтений, что позволило точнее оценить потребительские свойства готового продукта.

Результаты. Определение массовой доли влаги в сырье и выпеченных полуфабрикатах показало, что значения находятся в допустимых рецептурой границах (табл.1,2).

Таблица 1. – Массовая доля влаги в сырье

Сырье	Массовая доля влаги, %	Показатели по ГОСТ
Мука пшеничная в/с	14,5	Не более 15 %
Мука миндальная	5,8	Не более 6,5 %

Таблица 2. – Массовая доля влаги выпеченных полуфабрикатов

Образец	Массовая доля влаги, %
Контрольный образец	23,1
9 % миндальной муки	22,8

11 % миндальной муки	22,7
13 % миндальной муки	22,5

Установлено, что с увеличением величины добавки миндальной муки значения массовой доля жира, кислотности и содержание белковых веществ повышаются (табл. 3,4,5).

Таблица 3. –Массовая доля жира выпеченных полуфабрикатов

Выпеченный полуфабрикат	Массовая доля жира, %
Контрольный образец	3,75
9 % миндальной муки	5
11 % миндальной муки	5,6
13 % миндальной муки	6,1

Таблица 4. – Кислотность выпеченных полуфабрикатов

Образец	Кислотность, град.
Контрольный образец	0,2
9 % миндальной муки	0,3
11 % миндальной муки	0,4
13 % миндальной муки	0,5

Таблица 5. – Массовая доля белковых веществ в выпеченных полуфабрикатов

Образец	Массовая доля белковых веществ, %
Контрольный	0,8
9 % миндальной муки	1,008
11 % миндальной муки	1,012
13 % миндальной муки	1,017

Обсуждение. Исследования массовой доли влаги в сырье показали, что влажность миндальной муки значительно ниже, чем пшеничной. Это стало причиной уменьшения влажности готового изделия. Однако, ее значение остается в допустимых рецептурой границах (табл1,2).

Массовая доля жира бисквитного полуфабриката с применением добавки в пределах от 9 до 13% увеличивается более, чем на 60% по сравнению с контролем, что свидетельствует о повышении энергетической ценности изделия.

Повышение кислотности полуфабрикатов с добавкой миндальной муки (табл. 4) способствует более интенсивному протеканию процессов гидролиза сахарозы в процессе формирования теста и укреплению белкового каркаса теста [7, с.25].

Проведенные эксперименты показали, что применение указанного количества растительной добавки миндальной муки приводит к повышению содержания белковых веществ в пределах 26…27%.

Таблица 6. – Органолептические показатели бисквитного полуфабрикатов

Показатель	Контрольный образец	С добавлением миндальной муки		
		9 %	11 %	13 %
Внешний вид	Изделие заданной формы	«То же»	«То же»	«То же»
Вкус	Сладкий, с яичным привкусом	Свойственный бисквитному п/ф	Свойственный бисквитному п/ф	Появляется вкус миндаля
Консистенция	Пористая, мягкая	Пористая, мягкая	Пористая, мягкая	Пористая, мягкая. Изделие стало более эластичным
Цвет	Золотистая корочка, цвет мякиша с желтоватым оттенком	Золотистая корочка, цвет мякиша с желтоватым оттенком	Золотистая корочка, цвет мякиша с желтоватым оттенком	Золотистая корочка, цвет мякиша с желтоватым оттенком
Запах	Сладкий, с яичным оттенком	Свойственный бисквитному п/ф	Свойственный бисквитному п/ф	Появляется запах миндаля
Средний балл	4,83	4,83	4,97	4,85
Вид в изломе	Пропеченные изделия, с равномерной хорошо развитой пористостью, без пустот и комков.			

В результате органолептической оценки установлено, что все образцы имели хороший внешний вид, правильную форму. С добавлением миндальной муки вкус и запах образцов изменился в лучшую сторону. По консистенции образцы с добавкой стали более разрыхленными (табл.6).

Заключение. Проведенные исследования показали, что применение миндальной муки позволяет существенно повысить энергетическую ценность изделия, что важно для населения, проживающих в северных регионах. При этом увеличивается содержание белковых масс. Повышение кислотности улучшает реологические и технологические показатели. Замена 11% пшеничной муки на миндальную позволяет получить бисквитный полуфабрикат с наилучшими показателями.

Список литературы

1. Еганян Р.А. Особенности питания жителей Крайнего Севера России // Профилактическая медицина. № 16 (5). С. 41 – 47.

2. Н. А. Никифорова, Т. А. Карапетян, Н. В. Доршакова. Особенности питания жителей Севера // Экология человека 2018. №11. С. 20 – 24.
3. ГОСТ 9404-88. Мука и отруби. Метод определения влажности.
4. ГОСТ 5900-14. Изделия кондитерские. Методы определения влаги сухих веществ.
5. ГОСТ 31902-2012 Изделия кондитерские. Методы определения массовой доли жира.
6. ГОСТ 5670-96 Хлебобулочные изделия. Методы определения кислотности.
7. Рущиц А.А. Использование тыквенной муки в производстве бисквитного полуфабриката // Вестник ЮУрГУ. Серия «Пищевые и биотехнологии». 2015 Т. 3, № 4 С. 23–29.

Сведения об авторах
Кисимов Борис Михайлович, доцент, канд. тех. наук, ФГБОУ «Южно-Уральский государственный гуманитарно-педагогический университет», Челябинск, Россия
Kisimov Boris Mikhailovich, Associate Professor, Candidate of Technical Sciences, South Ural State Humanitarian Pedagogical University, Chelyabinsk, Russia

УДК 72.727

Садыкова С.Ш., Сайлаубеков А.А.
Евразийский национальный университет им. Л.Н. Гумилева, Астана, Казахстан

Модульные школы: быстрое строительство и гибкость

Аннотация: В данной статье рассматриваются особенности проектирования и строительства модульных школ, а также их влияние на качество образовательной среды. Проведён анализ современных исследований, посвящённых преимуществам и недостаткам модульного подхода в школьном строительстве. Отмечено, что использование сборных конструкций позволяет существенно сократить сроки возведения зданий и снизить затраты за счёт стандартизации процессов. Рассматриваются различные технологии модульного строительства, включая быстровозводимые школы из сэндвич-панелей, учебные заведения на основе морских контейнеров и Prefab-модульные школы с интегрированными инженерными коммуникациями. Приведены примеры успешных проектов, таких как школа Het Epos в Роттердаме и комплекс модульных начальных школ в Мюнхене, иллюстрирующие преимущества данного подхода. Отдельное внимание уделено вопросам энергоэффективности, гибкости планировочных решений и экологичности модульных зданий. Определены основные направления дальнейшего развития данного формата в контексте современных требований к образовательной инфраструктуре.
Ключевые слова: модульные школы, сборные конструкции, быстровозводимые здания, образовательная среда, энергоэффективность, Prefab-модульные школы, адаптивное проектирование.

Sadykova S.Sh., Sailaubekov A.A.

Modular schools are fast to build and flexible

Abstrect: This article examines the features of designing and constructing modular schools and their impact on the quality of the educational environment. An analysis of recent studies devoted to the advantages and disadvantages of the modular approach in school construction is presented. It is noted that the use of prefabricated structures significantly reduces construction time and costs through process standardization. Various modular construction technologies are discussed, including fast-erected schools using sandwich panels, educational institutions based on repurposed shipping containers, and prefab modular schools with integrated engineering systems. Examples of successful projects—such as the Het Epos School in Rotterdam and a modular primary school complex in Munich—illustrate the benefits of this approach. Special attention is given to issues of energy efficiency, flexible spatial planning, and the ecological sustainability of modular buildings. The article identifies the main directions for further development of this format in the context of modern requirements for educational infrastructure.
Keywords: modular schools, prefabricated structures, fast-erected buildings, educational environment, energy efficiency, prefab-modular schools, adaptive design.

Введение. В современных условиях проблема нехватки образовательных учреждений и устаревшей архитектуры школьных зданий становится всё более актуальной. Однако данная ситуация постепенно меняется благодаря развитию новых подходов к строительству школ,

среди которых особое место занимают инновационные, экологичные и комфортные учебные пространства.

В данной статье рассматривается концепция модульных школ, которые представляют собой своеобразные «конструкторы» XXI века, состоящие из предварительно изготовленных блоков, которые собираются на месте. Каркас может быть выполнен из металла, дерева или композитных материалов.

Внутренняя планировка предусматривает — аудитории, лаборатории, спортивные и административные помещения [1]. Этот формат образовательных учреждений не только позволяет значительно сократить сроки реализации проектов, но и способствует формированию нового архитектурного языка учебных пространств, ориентированного на цифровизацию и баланс между функциональностью и экологичностью.

Востребованность модульных школ обусловлена необходимостью оперативного строительства, бюрократическими сложностями и нехваткой ресурсов. Современное общество предьявляет новые требования к образовательной среде, что делает традиционные школы и способы их возведения менее эффективными.

Модульные школы разрушают устоявшиеся представления о проектировании учебных заведений, задавая новые архитектурные тенденции. Их концепция основана на использовании современных технологий и инновационных решений, что позволяет создать комфортную и адаптивную образовательную среду.

Анализ современных публикаций. В научных исследованиях активно обсуждаются как преимущества, так и возможные недостатки модульных кол. В ряде работ отмечается, что применение модульных конструкций способствует сокращению сроков строительства на 30-50% и снижению затрат за счёт стандартизации процессов и использования сборных элементов. Кроме того, современные материалы и инновационные инженерные решения повышают энергоэффективность зданий.

Модульная система позволяет легко адаптировать планировку школьных помещений в соответствии с актуальными потребностями, создавая гибкие и функциональные образовательные пространства. Однако данный подход имеет и определённые ограничения. В научной литературе отмечаются проблемы, связанные с акустическими характеристиками таких зданий, ограниченным выбором — строительных материалов и конструктивными — особенностями. Тем не менее, современные архитектурные разработки и технологические решения помогают эффективно справляться с этими вызовами, обеспечивая комфортные условия для обучения [2].

Исходя из этого, нужно выявить ключевые особенности и преимущества, важность проектирования и т.п. это все нужно чтобы

определить его влияние на качество образовательной среды и процесса. Для данной цели нужно проанализировать современные аналоги и описать основные архитектурные и функциональные характеристики таких школ , изучить их влияние на эффективность и комфорт учеников, определить перспективные решения и направления развития данного формата школ в условиях современного градостроительства и образовательной политики [3].

Существует множество технологий и методов строительства модульных школ, каждая из которых обладает своими особенностями. Один из распространённых подходов — использование быстровозводимых конструкций из сэндвич -панелей.

Такие школы состоят из предварительно изготовленных модулей, выполненных на основе металлических каркасов и сэндвич-панелей с утеплителем, таким как пенополиуретан или минеральная вата. Данный метод обеспечивает высокую скорость возведения зданий, а также способствует энергоэффективности за счёт современных материалов.

Другой вариант — строительство школ на основе морских контейнеров, что особенно актуально в зонах стихийных бедствий или вооружённых конфликтов. Переоборудованные контейнеры позволяют оперативно организовать учебный процесс даже в условиях ограниченных ресурсов, обеспечивая временное или постоянное функционирование образовательных учреждений.

Наиболее популярным решением являются Prefab -модульные школы, отличающиеся наличием интегрированных инженерных коммуникаций, таких как электроснабжение и водоснабжение. Их производство осуществляется в заводских условиях, после чего готовые модули доставляются на строительную площадку и собираются в единую конструкцию. Несмотря на различия в методах строительства, все модульные школы объединяет экологичность, гибкость планировочных решений и возможность — автономного — функционирования, что делает их востребованным решением в современной образовательной среде [4].

Одним из интересных примеров модульных школ является проект школы «Net Epos» в Роттердаме, разработанный архитектурным бюро SeARCH. Данная школа была создана с целью улучшения образовательных инфраструктур в социально-экономически неблагополучных районах Роттердама.

Уникальность школы является в том что он состоит из 75 предварительно изготовленных деревянных модулей, что в свою очередь позволяет с легкостью демонтировать, перемещать, увеличивать или расширять школу по мере необходимости.

Использование деревянных модулей не только способствует экологичности, но и создает теплую и уютную атмосферу для учащихся.

В зависимости от угла обзора и погодных условий можно заметить что фасад школы сочетает зеркальные и черные деревянные поверхности с вертикальными ламелями, создавая эффект изменяющегося облика здания.

Эти аспекты подчеркивают преимущества модульных школ в плане гибкости, скорости строительства и адаптивности к изменяющимся потребностям образовательных учреждений [5]

Рисунок 1. Проект школы «Net Epos»

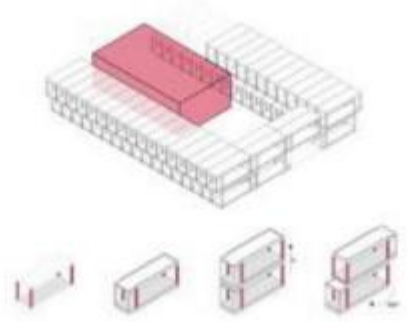

Рисунок 2. Сехама школы «Net Epos» в Роттердаме

В условиях современных образовательных требований проектирование и строительство учебных заведений требует гибкости и адаптации к изменяющимся потребностям. Одним из примеров успешной реализации модульного подхода является проект «Четыре начальных школы в модульном дизайне» в Мюнхене, получивший признание в профессиональной среде и удостоенный ряда архитектурных наград. Этот проект демонстрирует ключевые преимущества модульного строительства, включая высокую скорость возведения, устойчивость, эстетическую выразительность и возможность адаптации к различным условиям эксплуатации.

Школа, спроектированная архитектурным бюро wulf archiekten и реализованная в 2017 году, была структурирована в виде отдельных автономных блоков. В каждый из них входят четыре классных помещения, две взаимосвязанные зоны для продлённого дня, рабочее пространство для педагогов и персонала, а также центральное общее пространство, предназначенное для отдыха и совместных мероприятий.

Архитектурное решение предусматривает прямой выход из всех помещений на улицу через окружающие их галереи, что не только соответствует требованиям пожарной безопасности, но и обеспечивает удобный доступ к открытым пространствам. Использование модульного проектирования позволило гибко адаптировать архитектуру зданий под особенности конкретных участков. Конструкция школы состоит из отдельных учебных модулей, которые могут быть скомбинированы различными способами в зависимости от характеристик местности и потребностей образовательного учреждения. Чтобы избежать однообразия в дизайне модульных зданий, применены выразительные архитектурные элементы, такие как цилиндрические своды, способствующие созданию комфортной атмосферы и формированию уникального облика школы.

Дополнительно, внутренние перегородки выполнены из стекла и могут трансформироваться, обеспечивая прозрачность, вариативность и удобство в организации учебного процесса.

Данное решение способствует эффективному использованию пространства, позволяя менять формат образовательной деятельности и организовывать как индивидуальные занятия, так и групповые мероприятия, что особенно актуально для школ с программами полного дня [6].

Рисунок 3. «Четыре начальных школы в модульном дизайне» в Мюнхене

Рисунок 4. Схема школы в Мюнхене

Выводы. Проведённый анализ показал, что модульные школы являются перспективным направлением в развитии образовательной инфраструктуры, позволяя существенно сократить сроки строительства, оптимизировать затраты и повысить энергоэффективность зданий.

Благодаря стандартизации строительных процессов и использованию сборных конструкций удаётся обеспечить не только скорость возведения, но и гибкость архитектурных решений. Одним из ключевых преимуществ модульного строительства является возможность адаптации учебного пространства под изменяющиеся требования образовательного процесса.

Гибкость планировочных решений способствует созданию комфортной среды для обучения, а также позволяет легко модифицировать конфигурацию помещений в зависимости от потребностей школы.

Кроме того, мобильность модульных зданий делает их востребованным решением в условиях демографических изменений и необходимости быстрого развертывания образовательных учреждений в различных регионах.

Несмотря на очевидные преимущества, данный подход имеет и определённые ограничения. Среди них можно выделить вопросы, связанные с акустикой, ограниченный выбор строительных материалов, а также необходимость дополнительного проектирования инженерных коммуникаций.

Однако современные архитектурные и технологические разработки позволяют минимизировать данные проблемы, обеспечивая высокое качество образовательной среды.

Рассмотренные примеры реализации модульных школ, такие как «Het Epos» в Роттердаме и проект модульных начальных школ в Мюнхене, подтверждают эффективность данного подхода, демонстрируя его соответствие современным требованиям к образовательным учреждениям.

Эти проекты подчёркивают важность модульных решений не только с точки зрения архитектуры, но и в контексте устойчивого развития, энергоэффективности и адаптивности образовательной среды.

В перспективе дальнейшее развитие модульных школ может быть связано с внедрением экологически безопасных материалов, интеграцией инновационных инженерных систем и расширением функциональных возможностей учебных пространств.

Таким образом, данный формат строительства может стать одним из ключевых направлений модернизации образовательной инфраструктуры, способствуя созданию современных, удобных и устойчивых школ, соответствующих требованиям XXI века.

Список литературы

1. Modular Architecture in Scholarly Publishing: Enhancing Flexibility and Scalability. [Электрон.ресурс] - URL: https://www.highwirepress.com/blog/modular-architecture-in-scholarly-publishing-enhancing-flexibility-and-scalability/
2. A Critique of Smith & Johnson's Research Study Titled: "The Impact of Early Childhood Education on Academic Achievement" [Электрон.ресурс] - URL: https://mycustompaper. com/wp-content/uploads/2023/10/Sample-Article-Critique-Essay-The-Impact-of-Early-Childhood-Education-on-Academic-Achievement.pdf
3. Modular School Buildings: Sustainable Solutions for Modern Education [Электрон.ресурс] - URL: https://www.rotunda.co.uk/post/modular-school-buildings - sustainable-solutions -for-modern-education
4. 5 Modular School Design Trends to Watch in 2022 [Электрон.ресурс] URL: https://www.americanmodular.com/modular-school-design/
5. Het Epos School [Электрон.ресурс] - https://www.archdaily.com/943260/het-epos-school-search
6. Four Primary Schools in Modular Design / wulf architekten [Электрон.ресурс] - URL: https://www.archdaily.com/900013/four-primary-schools-in-modular-design-wulf-architekten

Сведения об авторах
Садыкова Сара Шангереевна, кандидат архитектуры, профессор Евразийского национального университета им. Л.Н. Гумилева, Астана, Казахстан
Сайлаубеков Алибек Айдынбекович, магистрант, студент магистрант Евразийского национального университета им. Л.Н. Гумилева, Астана, Казахстан
Sadykova S.Sh. corresponding author, Candidate of Architecture, Associate professor of the Eurasian National University named after. L.N. Gumilyov, Astana, Kazakhstan.
Sailaubekov A.A. – Master's degree in Architecture, Master's student, L.N. Gumilyov Eurasian National University, Astana, Kazakhstan.

УДК 336

Параничев А.В., Григорьев М.Д.
Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича, Санкт-Петербург, Россия

Мобильное управление персональными финансами

Аннотация. В статье рассматриваются способы ведения учета персональных финансов. Одним из привычных способов являются: ручной учет, когда вся информация фиксируется в блокнот или тетрадь; электронные таблицы, позволяющие частично автоматизировать учет; метод конвертов, при котором происходит искусственное разделение финансов на траты по категориям, и так далее. Однако в настоящее время наиболее эффективным является управление персональными финансами через мобильное приложение, позволяющее вести учет с гаджета, имеющее интуитивно понятный интерфейс и возможность синхронизации с банковскими счетами.

Ключевые слова: мобильное приложение, финансы, расходы, доходы, гаджет

Paranichev A.V., Grigoriev M.D.

Mobile personal finance management

Annotation. The article discusses ways to keep personal finance records. One of the usual methods is manual accounting, when all information is recorded in a notebook or notebook; spreadsheets that partially automate accounting; the envelope method, which artificially divides finances into expenses by category, and so on. However, currently the most effective way is to manage personal finances through a mobile application that allows you to keep records from a gadget, has an intuitive interface and often has the ability to synchronize with bank accounts.

Keywords: mobile application, finance, expenses, income, gadget

Введение

В настоящее время мобильные устройства и приложения являются неотъемлемой частью комфортного существования в современном мире. Любой возникающий вопрос, появившаяся проблема находят ответ и решение через гаджеты. Они позволяют быть в курсе многих новостей во всем мире, контролировать самочувствие, повышать продуктивность, управлять временем и финансами. Многие мобильные приложения влияют на разные аспекты жизни, в том числе на обучение, работу, развлечения. В этой статье мы раскроем как преимущества, так и недостатки применения мобильных приложений. Рассмотрим, как мобильные приложения позволяют эффективно управлять персональными доходами и расходами, а также влиять на повседневную жизнь.

Цель исследования: определить влияние мобильных приложений для учета персональных финансов на различные аспекты жизни человека.

Объектом исследования являются мобильные приложения, реализующее функционал контроля финансовых потоков.

Для достижения цели в ходе исследования были решены следующие задачи:

1) изучить предметную область данной темы,

2) провести анкетирование пользователей на предмет выявления преимуществ и недостатков мобильных приложений,

3) проанализировать статистику данных,

4) определить критерии отбора мобильных приложений пользователями.

Материалы и методы

Исследование включало в себя на первом этапе сбор данных с использованием анкетирования на предмет выявления преимуществ и недостатков мобильных приложений. На втором этапе с использованием новых данных были определены критерии отбора пользователями мобильных приложений как востребованных и конкурентоспособных приложений для учета финансов. Для определения согласованности мнений экспертов была проведена математическая обработка (экспертиза) полученных данных.

В качестве экспертов выступали 117 пользователей разного возраста и уровня достатка. Из них пользователи в возрасте 50-65 лет – 16 человек, 35-50 лет – 53 человека, 25-35 лет – 22 человека, 18-25 лет – 26 человек.

Результаты и обсуждение

Записи финансовых трат позволяют выяснить, какие расходы были действительно необходимыми, а без каких можно было обойтись. Строгий учет один из первых шагов, позволяющий управлять своими финансами и следить за тем, разумно ли расходуется семейный бюджет. Подробная фиксация трат необходима, если у человека есть стремление к экономии. Контролировать прибытие и убытие финансовых потоков не трудно, а результат может оказаться удивительным и привести в итоге к финансовой стабильности. Для того, чтобы учет был действительно строгим и точным, необходимо фиксировать даже все мелочи, на которые были потрачены финансовые средства. Этому делу рачительными хозяевам огромного внимание уделялось с давних времен, немалое значение в свое время придавала, например, Екатерина Великая. Она поражалась тому, что никто ранее всерьез не занимался планированием доходной части бюджета. Она записывала не просто потраченные суммы, но с тщательностью фиксировала с точностью до копейки стоимость и краткую характеристику каждого подарка, подаренную сумму денег, стоимость имения или поста, приносящего доход, награды [1, с. 114].

Умение эффективно распоряжаться личными финансами помогает не только быстрее добиваться намеченных целей, но и ощущать себя спокойно и уверенно в абсолютно любых, даже самых нестабильных обстоятельствах во время финансовой турбулентности. Финансовая стабильность невозможна без грамотно разработанного плана и поэтапных действий. Под действиями подразумевается контроль доходов и расходов

за определенный период времени и удобнее это делать при помощи мобильного приложения с различными аналитическими функциями [2].

Доходы. Данный раздел мобильного приложения заполняется информацией обо всех денежных поступлениях. Это может быть заработная плата с основного места работы, доход от дополнительной деятельности, доход от сдаваемого в аренду помещения, проценты по вкладам, подарки в виде денежной суммы и т.д. Четкое понимание о наличии конкретной суммы в определенный период времени позволит понять свои реальные возможности и определить перспективы при распределении расходов.

Расходы. Этот раздел мобильного приложения требует набольших затрат времени и внимания, так как от качественного заполнения данного раздела зависит объективность анализируемой информации. Сюда записываются все траты, осуществляемые ежедневно в определенный промежуток времени. Их можно подразделять на обязательные и необязательные. К обязательным расходам относятся фиксированные траты, такие как платеж по кредиту, за коммунальные услуги, оплата интернета, телефона и т.д. К необязательным относятся траты на импульсивные покупки, развлечения и др.

По итогам определенного временного интервала в мобильном приложении появляется аналитическая информация, позволяющая учитывать в дальнейшем, каких импульсивных трат можно избежать, без каких покупок обойтись, как уменьшить расходы без ущерба для привычного образа жизни. Мобильное приложение помогает принимать взвешенные решения и не поддаваться влиянию извне [3].

Применение мобильного приложения для учета финансов помогает более эффективно управлять деньгами, избегая ненужных трат и создавая финансовую подушку безопасности на будущее [5]. Из предложенного функционала мобильных приложений для учета персональных финансов большинством экспертов были выявлены следующие позиции, которые представлены в Таблице 1.

Таблица 1. Сравнительный анализ функционала приложения для мобильного управления персональными финансами

I. Преимущества мобильных приложений	
Удобство использования	Мобильные приложения просты в обращении и легки в использовании. Есть возможность запустить их работу одним касанием, чаще всего имеют удобный и интуитивно понятный интерфейс
Доступность	Мобильные приложения доступны в любое время, где существует доступ к Интернету. Доступ к приложениям можно получить в любой момент и из любой точки мира
Прозрачность	Ясная картина того, куда потрачены деньги. Это позволяет контролировать ненужные финансовые траты и определить

	направления, где возможно сэкономить
Возможность планировать будущее	Полное понимание того, какая сумма есть в наличии и какую можно потратить на приобретение необходимой вещи
Возможность ставить и достигать конкретные финансовые цели	В мобильных приложениях удобно осуществлять накопления, например, на автомобиль, ремонт квартиры, образование, поездку или пенсионное накопление на будущее
Избежание накопления долгов	Постоянный контроль финансов помогает избежать финансовых трудностей, так как человек постоянно осведомлен о своих возможностях и ограничениях
Повышение уровня экономической самостоятельности	Учет финансов в режиме онлайн снижает стресс от неожиданно возникающих финансовых проблем, что повышает уровень уверенности в своем будущем
Улучшение продуктивности	Многие мобильные приложения улучшают эффективность человека. Они позволяют организовать наши цели и время, а также повысить продуктивность нашей работы
II. Минусы мобильных приложений	
Платная версия	Это один из главных минусов, названных пользователями, так как они не готовы платить за приложение, которое предназначено научить их экономить
Наличие рекламы	В бесплатной версии мобильных приложений есть наличие рекламы. Переход на платную версию позволяет отключить навязчивые всплывающие окна и бегущие строки

По результатам проведенного исследования определены критерии отбора мобильных приложений пользователями. Выбор обычно останавливается на тех приложениях, которые обладают наибольшим количеством плюсов. Также важно не забывать о безопасности при использовании приложений и по возможности вносить минимум своих персональных данных.

Умение сохранять, зарабатывать и приумножать – это разные навыки. Каждый из них требует особого подхода [4, с. 13]. Мобильные средства позволяют это сделать наилучшим образом.

Заключение

Каждый человек стремится сделать свою жизнь более комфортной, в том числе и в финансовом плане, поэтому важно систематически контролировать и анализировать свои персональные финансовые потоки. Преимущества управления личными финансами заключаются в планировании покупок, контроль доходов и трат, избегание ненужных и неоправданных трат, создание подушки безопасности, обеспечение будущего.

Чтобы управлять персональными финансами, можно применять различные инструменты, в том числе разнообразные мобильные приложения, в которых есть возможность подробного анализа личной финансовой грамотности. Это поможет понять и возможно

скорректировать свое отношение к финансам, а в будущем даже заняться инвестированием.

В современном мире какие бы альтернативные пути ведения персонального бюджета человек ни выбирал, наиболее удобным и функциональным является мобильное управление финансами через мобильные приложения. Гаджет с установленной программой постоянно находится под рукой, не нужно спустя время воспроизводить в памяти всю информацию о доходах и расходах, которые были произведены в течение дня. Достаточно простым касанием пальцев зафиксировать информацию, а мобильное приложение проделает остальную аналитическую работу и представит необходимый результат.

Список литературы

1. Огарев Г. 27 законов экономного ведения хозяйства / Георгий Огарев. - Саратов: Научная книга, 2024. - 336 с.
2. Подрез И. Система финансового выздоровления: как освободиться от внутренних ограничений, приумножить доходы и забыть об ощущении бедности / Ирина Подрез. – Москва: Эксмо, 2023. – 352 с.
3. Степанов П. Н. Создание инструментария для оптимизации расходов за один рабочий день. Интерактивный бюджет: персональный, семейный, для малого бизнеса / П. Н. Степанов // Проблемы современной науки и образования. – 2017. – № 28 (110). – С. 23-28.
4. Туралиева И. Финансовый интеллект. Как управлять личными финансами, чтобы жить в достатке и благополучии. Москва: Бомбора, 2023. – 320 с.
5. Федотенко М. А. Разработка мобильных приложений. Москва: Лаборатория знаний, 2020. – 335 с.

Сведения об авторах:
Параничев Андрей Викторович, старший преподаватель кафедры Информационных управляющих систем, Санкт-Петербургский государственный университет телекоммуникаций им. проф. М.А. Бонч-Бруевича, Санкт-Петербург, Россия
Григорьев Максим Дмитриевич, студент, Кафедра Информационных управляющих систем, Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича, Санкт-Петербург, Россия
Paranichev Andrey Viktorovich, Senior Lecturer at the Department of Information Management Systems, St. Petersburg State University of Telecommunications named after Prof. M.A. Bonch-Bruevich, St. Petersburg, Russia
Grigoriev Maxim Dmitrievich, student, Department of Information Management Systems, St. Petersburg State University of Telecommunications named after Prof. M. A. Bonch-Bruevich, St. Petersburg, Russia

Оглавление