

The background features a complex digital visualization. On the left, a hand is shown pointing at a bar chart with a white arrow. The chart has several bars in shades of blue and purple. To the right, there is a candlestick chart with a white line graph overlaid. The background is filled with a grid of white dots and lines, creating a sense of depth and data. Various numerical values are scattered throughout, including '1070.01', '1000.0', '959.41', '1051.32', 'Vol 2,870.11M', '28.00', '14.00', '0.00', '-14.00', '7.91', '53.9', '34.91', and '15.91'.

Цифровая трансформация общества и информационная безопасность

Материалы III Всероссийской научно-практической конференции
(Екатеринбург, 17 мая 2024 г.)

Министерство науки и высшего образования Российской Федерации
Уральский государственный экономический университет



ЦИФРОВАЯ ТРАНСФОРМАЦИЯ ОБЩЕСТВА И ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

Материалы

III Всероссийской научно-практической конференции

(Екатеринбург, 17 мая 2024 г.)

Екатеринбург
2024

УДК 004.056(08)+338(08)
ББК 32.973я4+65.0я4
Ц75

Ответственный за выпуск

кандидат экономических наук, доцент
А. Ю. Коковихин

Ответственный редактор

кандидат экономических наук
М. А. Панов

Ц75

Цифровая трансформация общества и информационная безопасность : материалы III Всероссийской научно-практической конференции (Екатеринбург, 17 мая 2024 г.) / Министерство науки и высшего образования Российской Федерации, Уральский государственный экономический университет ; ответственный за выпуск А. Ю. Коковихин ; ответственный редактор М. А. Панов. — Екатеринбург : УрГЭУ, 2024. — 150 с.

Обсуждаются вопросы информационной безопасности и компьютерных технологий, цифровых решений для бизнеса и общества, проблемы трансформации и рисков цифрового общества.

Для научных работников, студентов, участвующих в научно-исследовательской работе, магистрантов и аспирантов, преподавателей, представителей научных и бизнес-сообществ, государственных структур.

УДК 004.056(08)+338(08)
ББК 32.973я4+65.0я4

- © Авторы, указанные в содержании, 2024
- © Уральский государственный экономический университет, 2024

Информационная безопасность и компьютерные технологии

Е. А. Ищенко, М. А. Панов

Уральский государственный экономический университет, г. Екатеринбург

Угрозы информационной безопасности при использовании корпоративных систем для обмена мгновенными сообщениями

Аннотация. Статья посвящена исследованию угроз информационной безопасности при использовании систем обмена мгновенными сообщениями в корпоративной среде. Рассматриваются виды угроз с последующими рекомендациями по превентивным мерам защиты. Результаты исследования могут послужить отправной точкой для пересмотра политик безопасности компании с последующим более детальным изучением проблемы.

Ключевые слова: корпоративные системы; обмен мгновенными сообщениями; угрозы информационной безопасности; меры защиты; риски.

В период развития информационных технологий в корпоративных средах немаловажным является скорость реакции участников на возникающие события. Ключевую роль в этом занимают каналы, по которым осуществляется передача информация. Одним из таких каналов являются системы обмена мгновенными сообщениями, которые позволяют организовать взаимодействие сотрудников как внутри компании, так и за ее пределами. Такие системы позволяют оперативно решать возникшие проблемы, обсуждать проекты или мгновенно делиться любой информацией между заинтересованными лицами. На их базе реализуют командную работу для выполнения определенных задач. В связи с этим они становятся одним из инструментов по управлению проектами. И это позволяет командам эффективно координировать свою работу [4].

Из-за всеохватывающего использования систем обмена мгновенными сообщениями в корпоративной среде предприятия возникает серьезная проблема — обеспечение безопасности обмена информации. Принципы корпоративной информационной безопасности вытекают из организационной структуры корпорации. Такой субъект информационной безопасности может представлять собой крупное предприятие с работантными в соответствии с потребностями организации ценностями и структурой. Основным отличием от типичной структуры информационной безопасности является увеличенная роль персонала в обеспечении защиты данных.

Условно угрозы можно разделить на внутренние и внешние. Внутренние угрозы — это угрозы, которые исходят от сотрудников предпри-

ятия. Такие угрозы сложны в предотвращении и могут привести к значительным финансовым и репутационным потерям. Внешние угрозы дешевле определить и дешевле предотвратить. Например, запретить доступ к системе за пределами сети компании. Тем самым пропадает внешний вектор атаки.

Угрозы можно классифицировать на следующие категории [2, с. 9]:

- несанкционированный доступ к данным или утечка конфиденциальной информации;
- фишинг и социальная инженерия;
- вредоносное программное обеспечение;
- отказ в обслуживании (DDoS).

Несанкционированный доступ к данным — доступ к информации, нарушающий правила разграничения доступа с использованием штатных средств, предоставляемых средствами вычислительной техники или автоматизированными системами¹. Осуществляется через существующий или специально созданный канал доступа [3, с. 74]. Может возникать по ряду причин:

- перехват сетевого трафика системы — если данные передаются через незашифрованные или ненадежные сети, то появляется возможность перехватывать их с помощью снифферов. В качестве закрытия угрозы применяют: зашифрованное соединение (например, https), настройка корпоративной сети VPN, E2EE;

- компрометация учетных данных — получение доступа к чужой учетной записи. Возникает, когда компания использует слабые парольные политики (или вовсе не использует их) или когда сотрудник не следит за своим рабочим местом. Например, ушел с рабочего места и оставил не заблокированным компьютер. Одним из решений является повышение парольных политик или настройка автоблокировок компьютера при неактивном состоянии. Обязательным требованием для систем мгновенного обмена сообщениями должно быть использование двухфакторной аутентификации. При этом предпочтение должно отдаваться приложениям-аутентификаторам (например, «Яндекс.Ключ»), так как перехватить код аутентификации будет невозможно (в отличие от смс);

- распространение информации на широкую аудиторию системы обмена мгновенными сообщениями — сотрудники могут случайно поделиться информацией с коллегами, которые не имеют доступа к информации. Автоматического решения угрозы не существует, так как невозможно определить имеет тот или иной сотрудник официальный доступ к информации. Решается путем ограничения передаваемой информации

¹ Нормативно-правовые акты ФСТЭК. Руководящий документ «Защита от несанкционированного доступа к информации. Термины и определения».

(например, запрет на передачу персональных данных клиента) с последующим автоматическим мониторингом за отправляемыми сообщениями и ручным разбором ситуации, когда определили передачу запрещенных данных.

Фишинг и социальная инженерия — методы манипуляции, которые используются злоумышленниками для обмана сотрудников и получения конфиденциальной информации или доступа к защищенным системам. Основная цель фишинга — выманить пользователя системы за его пределы на заранее созданные поддельные интернет-ресурсы (почта, веб-сайты, мобильные приложения, корпоративные сервисы) с последующей компрометацией учетных данных пользователя.

Меры, которые могут минимизировать угрозы фишинга:

- обучение персонала — проведение регулярного обучения сотрудников по распознаванию фишинговых попыток и признаков социальной инженерии;

- мониторинг активности — регулярное отслеживание и анализ активностей пользователей в системе для выявления подозрительных паттернов поведения;

- фильтрация входящих и исходящих сообщений — автоматическая блокировка сообщений, содержащих признаки фишинга или вредоносных вложений;

- регулярное обновление системы — обновление системы до последних версий для исправления известных уязвимостей.

Вредоносное программное обеспечение — программа, предназначенная для осуществления несанкционированного доступа к информации или воздействия на информацию или на ресурсы информационной системы¹. Метод направлен на запуск вредоносного кода на устройстве пользователя системы. Распространение вредоносного кода осуществляется как вложение к сообщению от доверенных источников (например, от потенциального клиента, либо от коллеги). Запуск вредоносного кода может привести:

- к потере конфиденциальной информации — вредоносное программное обеспечение может собирать и передавать конфиденциальные данные, находящиеся на устройстве;

- утрате контроля над системой — производятся действия без согласия владельца. Например, уничтожение данных на устройстве;

- финансовым потерям — перевод денежных средств с лицевого счета компании на счета злоумышленников;

- юридическим последствиям — спровоцировать компанию на нарушение законодательства или на получение штрафов.

¹ ГОСТ Р 50922-2006 «Защита информации. Основные термины и определения».

Меры, которые помогут минимизировать угрозы от вредоносного программного обеспечения:

- наличие антивирусных программ на устройствах сотрудников с актуальными базами сигнатур;
- запрет на установку и запуск программного обеспечения не входящих в белый список;
- обучение сотрудников;
- наличие песочницы для запуска подозрительного программного обеспечения.

DDoS — атака, направленная на отказ в обслуживании ресурса или канала [1, с. 199]. Достигается путем перегрузки сетевой инфраструктуры большим количеством запросов с разных источников. По отношению к системе обмена мгновенными сообщениями целью DDoS является нарушение коммуникаций между сотрудниками компании. В свою очередь отсутствие коммуникации может привести к ущербу репутации, потере дохода, потере данных.

Способы защиты от DDoS [1, с. 202]:

- использование распределенных систем, обнаружение и предотвращение DDoS-атак;
- использование алгоритмов машинного обучения и искусственного интеллекта;
- использование технологий CDN;
- внедрение системы фильтрации и контроля трафика;
- реализация технологии блокировки IP-адресов;
- развитие сетевой инфраструктуры (обновление, увеличение пропускной способности).

На основе поведенного анализа потенциальных угроз были определены необходимые стандарты безопасности, которым должна соответствовать корпоративная система обмена мгновенными сообщениями:

- использование безопасных каналов связи;
- использование E2EE;
- управление доступом;
- многофакторная аутентификация;
- аудит и мониторинг;
- регулярные обновления ПО;
- обучение персонала информационной безопасности в корпоративных системах;
- наличие защиты от внешних угроз;
- встроенное антивирусное программное обеспечение для проверки вложений;
- защита от DDoS-атак;
- наличие физической безопасности серверов системы.

Корпоративная безопасность достигается за счет комплексного подхода. Комбинация этих мер позволяет компании эффективно обеспечивать безопасность корпоративной тайны и защищать свои интересы как от внешних угроз, так и от внутренних.

Библиографический список

1. *Баранова Е. К.* Информационная безопасность и защита информации: учеб. пособие. 4-е изд., перераб. и доп. М.: РИОР: ИНФРА-М, 2019. 322 с.
2. *Верецагина Е. А.* Исследование проблем информационной безопасности в банковской сфере. М.: РУСАЙНС, 2023. 178 с.
3. *Гришина Н. В.* Основы информационной безопасности предприятия: учеб. пособие. 2-е изд., доп. М.: ИНФРА-М, 2023. 216 с.
4. *Панов М. А., Ищенко Е. А.* Архитектура системы обмена мгновенными сообщениями Mattermost // Цифровая трансформация общества и информационная безопасность: материалы II Всерос. науч.-практ. конф. (Екатеринбург, 19 мая 2023 г.). Екатеринбург: УрГЭУ, 2023. С. 110–115.

К. А. Каткова

Уральский государственный экономический университет, г. Екатеринбург

Кибербезопасность в условиях цифровой трансформации: новые угрозы и методы защиты

Аннотация. В статье рассматривается тема кибербезопасности в эпоху цифровизации. Приведены понятия кибербезопасности в цифровой трансформации, основные угрозы для пользователя при использовании сети Интернет. Описаны существующие методы защиты от преступлений в сети.

Ключевые слова: кибербезопасность; цифровизация; кибератаки; информационные технологии; защита.

В эру цифровых технологий компьютеры используются как в повседневной жизни, так и в рабочих процессах. Люди оставляют все больше информационных следов в Интернете, чем пользуются киберпреступниками. В этом контексте киберугрозы относятся к киберпреступникам, которые пытаются получить несанкционированный доступ к компьютерным системам или сетям, используя различные методы [6, с. 89]. Именно поэтому в наше время остро стоит проблема информационной безопасности, ведь без должной защиты жертвой может стать любой, как частное лицо, так и компания. В статье рассматриваются новые угрозы в сети и методы защиты от них.

Перейдем к определениям. Цифровизация — это глобальный процесс, включающий в себя разработку передовых производственных технологий, сквозных информационных технологий, искусственного интеллекта [3, с. 7]. Кибербезопасность — это условия защищенности от

физических, духовных, финансовых, политических, эмоциональных, профессиональных, психологических или других типов воздействий или последствий аварии, повреждения, ошибки, несчастного случая, вреда или любого другого события в киберпространстве, которые могли бы считаться нежелательными [4, с. 216].

Основная проблема состоит в том, что с развитием технологий появляются не только новые возможности для пользователей, но и новые опасности. Рост числа кибератак влияет на эффективность работы организаций промышленного сектора, использующих уязвимости сетевых машин. Цифровая трансформация сопряжена с определенными рисками, особенно в том, что касается кибербезопасности [5, с. 1]. Это вынуждает адаптироваться под новые условия, чтобы обезопасить себя. Самыми актуальными угрозами в данный момент являются: фишинг, малварь, DDoS-атака, мошенничество с использованием искусственного интеллекта, инсайдинг. Разберем их подробнее.

Фишинг — это один из методов интернет-мошенничества, при котором пользователю приходит ложное электронное письмо от имени банков или популярных организаций. Целью же является получение конфиденциальной информации: логины и пароли, данные банковских карт. В письме часто содержится ссылка на веб-страницу. После перехода по ссылке киберпреступники пытаются подтолкнуть пользователя ввести свои личные данные.

Следующая угроза пусть и давно известна, но от этого не менее опасна. Малварь — вредоносное программное обеспечение, целью которого является навредить компьютеру пользователя или его содержимому [1]. Примерами таких программ являются трояны и вирусы. Также может являться шпионской программой или кейлоггером, которая собирает личную информацию. Шпионская программа собирает информацию из менеджера паролей, где могут также храниться данные банковских карт. Кейлоггер запоминает нажатие на клавиатуру и мышшь, тем самым, запоминая пароли. В большинстве случаев такие программы можно удалить с помощью антивируса, однако некоторые вирусы обладают такой высокой степенью защиты, что их почти невозможно удалить после запуска.

Еще одним вызовом является DDoS-атака. Если простыми словами DDoS-атака — это попытка загрузить сервис так, чтобы он перестал работать. Делается это путем большого количества автоматических запросов, которые посылаются одновременно с нескольких устройств. При крупных атаках количество компьютеров может быть около сотни и больше. Интересно, что устройства, с которых отправляются запросы, принадлежат не хакерам, а их жертвам. Сами запросы отправляются через вредоносное ПО. Причины атак могут различаться. Нападать могут

на сайты государственных учреждений и банков по политическим мотивам, ради кражи информации частных компаний или из-за конкуренции в бизнесе, для отвода глаз и параллельного мошенничества, вымогательства и даже ради развлечения. Защититься от этого можно, повышая степень защищенности сайта/приложения или используя специализированные программы.

Инсайдинг — одна из самых распространенных угроз для компаний. Работающий либо уволенный работник компании выступает возможным преступником, таких работников называют инсайдерами. Инсайдер знаком с внутренними тонкостями фирмы и может вмешаться в работу компьютерной системы или передать конфиденциальные данные злоумышленникам или конкурентам. Инсайдерские угрозы сильно недооцениваются компаниями. Но, зная конфиденциальную информацию компании, киберпреступники могут заразить системы безопасности организаций. Если организации и дальше будут недооценивать эту проблему, им будет сложно остановить деструктивное и неосторожное поведение своих сотрудников, бросающее вызов заранее установленным безопасным протоколам кибербезопасности.

Мошенничество с использованием искусственного интеллекта — это самый новый вид киберпреступления. Искусственный интеллект может использоваться мошенниками для автоматического создания фишинговых писем и подделки голоса или документов. Также мошенники могут воспользоваться несовершенствами в системе компаний. Многие компании внедряют ИИ в свой рабочий процесс. ИИ может использоваться для управления наборами данных и хранения информации. Основная лазейка заключается в том, что пароли и другие данные часто изменяются пользователями и другими участниками системы, благодаря чему легко выяснить такие детали, как адрес, банковские реквизиты и т. д.

Главная проблема профилактики борьбы с киберпреступностью состоит в существующем серьезном несоответствии нормативно-правовой базы современным стандартам правоприменительной практики. Несмотря на введение в 2012 г. в Уголовном кодексе РФ новых квалифицирующих признаков составов мошенничества, в том числе с использованием платежных карт и в сфере компьютерной информации (ст. 159.1, 159.2, 159.3 и 159.6), статистика наглядно показывает устойчивый рост киберпреступности в финансовом секторе. К категории, представляющей наибольшую общественную опасность для финансового сектора, можно отнести более десяти составов преступлений, предусмотренных Уголовным кодексом Российской Федерации [3, с. 9]. Возникает вопрос: как можно обезопасить себя? Одним из наиболее эффективных методов является шифрование данных. Шифрование данных позволяет

защищать данные от несанкционированного доступа и предотвратить их утечку [1, с. 28]. Немаловажно использование антивирусных программ, которые предотвращают возможность установки вредоносного ПО. Также не стоит забывать про внимательность: использование сложных уникальных паролей, скачивание файлов только из проверенных источников и регулярное обновление антивирусной программы и программного обеспечения позволят обезопасить себя от утечки личных данных. Немаловажно улучшать культуру кибербезопасности, обучать пользователей и устанавливать соответствующие политики безопасности в компаниях. Необходимо проводить семинары, тренинги для поддержания культуры информационной безопасности. На уровне компаний уже давно распространена цифровая гигиена. Она предполагает внедрение как систем защиты от внешних проникновений, так и определенных прав доступа к информации, блокирования целого спектра ресурсов на рабочих станциях [2, с. 84].

Переходя к заключению, можно сделать выводы о том, что наравне с технологическим прогрессом также растет и уровень преступности в сети. В эпоху цифровизации проблема киберпреступлений стала глобальной. И каждый человек должен знать, какие есть методы защиты от кибератак. Следует повышать уровень осведомленности пользователей в этой теме, а также совершенствовать меры безопасности.

Библиографический список

1. *Безделов А. Д., Логинова Е. В.* Инновационные формы управления и кибербезопасность безналичных расчетов в условиях цифровизации банковской экосистемы // Научные исследования и разработки. Экономика фирмы. 2020. Т. 9, № 3. С. 25–31.
2. *Горулев Д. А.* Экономическая безопасность в условиях цифровой экономики // Техничко-технологические проблемы сервиса. 2018. № 1 (43). С. 77–84.
3. *Корнев Л. В.* Обеспечение информационной безопасности в условиях цифровизации // Молодой ученый. 2022. № 12 (407). С. 7–11.
4. *Слипачук Л. А.* Принципы функционирования модели интегрированной отраслевой ИСУ сектором национальной кибербезопасности // Актуальные научные исследования в современном мире. 2020. № 3-1 (59). С. 75–85.
5. *Azambuja A. J. G. de, Plesker C., Schützer K., Anderl R., Schleich B., Almeida V. R.* Artificial Intelligence-Based Cyber Security in the Context of Industry 4.0 — A Survey // Electronics. 2023. Vol. 8, iss. 12. P. 1–18.
6. *Möller D. P. F.* Cybersecurity in Digital Transformation Scope and Applications. Springer Cham, 2020. 136 p.

Применение ассоциативного анализа в сфере информационной безопасности

Аннотация. В статье приведено понятие метода машинного обучения — ассоциативного анализа. Исследованы преимущества и недостатки данного метода по сравнению с другими. Рассмотрено применение ассоциативного анализа в области информационной безопасности.

Ключевые слова: метод машинного обучения; ассоциативный анализ; применение ассоциативного анализа в сфере ИБ; сетевой трафик.

Методы машинного обучения играют все более важную роль в современном обществе, они применяются в различных областях, начиная от медицины и финансов и заканчивая маркетингом и информационной безопасностью. Один из подходов к анализу данных, который получил широкое распространение, — метод ассоциативного анализа. Именно этому методу посвящено множество исследований и статей в научной литературе. Так, о данном методе в своих работах говорили И. С. Вершинин [1] и Р. Ф. Гибадуллин в соавторстве с А. Д. Леоновым и М. Ю. Перухиным [2]. В этой статье мы рассмотрим метод ассоциативного анализа, его преимущества, недостатки, практическое применение и использование в области информационной безопасности.

Ассоциативный анализ — это метод машинного обучения, который используется для обнаружения взаимосвязей и закономерностей в наборах данных [3]. Он используется для выявления скрытых закономерностей и паттернов в больших объемах информации.

Метод ассоциативного анализа имеет свои преимущества, к ним относятся:

- помощь в выявлении скрытых зависимостей между различными элементами данных, что позволяет получить новые инсайты и прогнозы;
- помощь в выявлении паттернов и тенденций в данных, что облегчает принятие более обоснованных решений;
- автоматическое выявление взаимосвязи в данных, что экономит время и усилия аналитиков;
- прогнозирование будущих событий на основе выявленных взаимосвязей в данных;
- оптимизация различных процессов;
- легкая интерпретация, что делает результаты ассоциативного анализа доступными для широкого круга пользователей, не являющихся специалистами в области данных;
- обнаружение новых возможностей для бизнеса;
- универсальность применения в различных областях;

- интуитивно понятный интерфейс, что делает данные простыми в использовании даже для новичков;
- быстрые и наглядные результаты, что позволяет оперативно реагировать на изменения в данных.

Метод ассоциативного анализа также имеет свои недостатки:

- возможность ошибочных выводов из-за случайных совпадений в данных;
- необходимость большого объема данных, что может быть проблематично, особенно в небольших компаниях;
- сложность некоторых результатов для интерпретации, особенно в случае сложных взаимосвязей между данными;
- мультиколлинеарность, когда переменные сильно коррелируют друг с другом;
- неустойчивость к выбросам в данных, что может исказить результаты и привести к ошибочным выводам;
- выявление корреляции между данными, что не всегда позволяет определить причинно-следственные связи;
- сложность решения некоторых задач методом ассоциаций, что ограничивает его применимость;
- необходимость определять пороговые значения, что может потребовать дополнительного исследования;
- потребность в значительных вычислительных ресурсах;
- при динамически изменяющихся данных анализ ассоциаций не всегда учитывает временные аспекты.

Метод ассоциативного анализа является универсальным инструментом, который широко применяется в различных сферах для выявления скрытых взаимосвязей и паттернов в данных.

В области информационной безопасности этот метод может быть применен для обнаружения необычных или вредоносных паттернов, выявления аномалий и прогнозирования потенциальных угроз.

Одним из наиболее распространенных примеров использования метода ассоциативного анализа в области информационной безопасности является анализ сетевого трафика для выявления атак или вредоносных действий. На основе совместного появления определенных типов сетевого трафика или событий можно выявить подозрительные активности, которые могли бы пройти незамеченными при обычном ручном анализе. Например, если определенные виды сетевого трафика часто сопровождаются попытками несанкционированного доступа к системе, то ассоциативный анализ может помочь автоматически выявить такие связи и предупредить об угрозе.

На рисунке показан пример схемы выявления вредоносного трафика на основе ассоциативного анализа.



Выявление вредоносного трафика на основе ассоциативного анализа

Также метод ассоциативного анализа может использоваться для обнаружения внутренних угроз и утечек данных. Анализируя совместное появление различных событий в информационной системе, можно выявить аномальное поведение пользователей или системных процессов, что свидетельствует о возможных нарушениях безопасности.

Таким образом, метод ассоциативного анализа представляет собой мощный инструмент для обеспечения информационной безопасности, позволяя автоматизировать процесс обнаружения потенциально опасных событий и реагировать на них оперативно.

Метод ассоциативного анализа является мощным инструментом в арсенале методов машинного обучения. Его применение позволяет выявлять новые закономерности в данных и использовать их для улучшения бизнес-процессов и повышения эффективности принимаемых решений. В сочетании с другими методами машинного обучения ассоциативный анализ открывает широкие возможности для применения в различных областях человеческой деятельности, что делает его важным инструментом в современном мире.

Библиографический список

1. Вершинин И. С. Реляционная база данных картографических сцен с ассоциативной защитой // Computational Nanotechnology. 2023. Т. 10, № 3. С. 101–108.

2. Гибадуллин Р. Ф., Леонов А. Д., Перухин М. Ю. Разделение пространственных данных для масштабируемой обработки запросов // Вестник Технологического университета. 2017. Т. 20, № 8. С. 83–86.

3. Тушканова О. Н., Городецкий В. И. Ассоциативная классификация: аналитический обзор. Часть 2 // Труды СПИИРАН. 2015. № 2 (39). С. 212–240.

Д. Ю. Мельников

*Уральский федеральный университет
имени первого Президента России Б. Н. Ельцина, г. Екатеринбург*

Обоснование применимости метода машинного обучения «градиентный бустинг» для алгоритма системы обнаружения компьютерных атак

Аннотация. В статье представлен обзор релевантной литературы в области применения методов машинного обучения для обнаружения компьютерных атак. Обоснована применимость метода «градиентный бустинг» при разработке систем обнаружения компьютерных атак.

Ключевые слова: машинное обучение; компьютерная атака; система обнаружения атак; информационная безопасность.

Постоянное развитие информационных технологий влечет за собой развитие угроз информационной безопасности. На первое место выходят мероприятия по выявлению компьютерных атак (далее — КА). Системы обнаружения компьютерных атак (далее — СОА) имеют большое значение в сфере информационной безопасности, и их использование дает ряд преимуществ. Применение СОА является одной из обязательных технических мер в комплексе по обеспечению безопасности критической информационной инфраструктуры (далее — КИИ).

Современные компьютерные атаки становятся все более сложными и многоуровневыми, включая различные векторы атак и комбинированное использование разных методов. Такие сложные атаки могут обходить традиционные методы обнаружения компьютерных атак, требуя использования новых подходов, таких как использование алгоритмов машинного обучения. Существует теорема No Free Lunch, суть которой заключается в том, что не существует алгоритма, который оказался бы лучшим выбором для каждой задачи [6]. Необходимо опробовать различные методы машинного обучения, чтобы проверить их эффективность в решении вопросов обнаружения КА.

В исследовании [4] представлен метод обнаружения КА типа «Инъекция кода SQL» (SQL Injection) на основе многослойного перцептрона, обученного в режиме автоассоциативной памяти. По мнению автора исследования, основной сферой применения данного подхода являются системы с фиксированной функциональностью и обслужива-

нием. Узкая сфера применения обусловлена одним из недостатков данного метода, а именно чувствительностью к изменению вычислительной среды сервера и последующему изменению нормального профиля работы. Уникальность данного метода заключается в независимости обработки протокола, а также возможности выявления аномалий при работе с зашифрованными запросами без их расшифровки. В исследовании не уточняется объем обучающей выборки. Метод малоприменим в современных информационных системах из-за своих недостатков и ограничений.

В работе [3] рассматриваются вопросы построения и практической реализации модели обнаружения компьютерных атак на основе методов машинного обучения. В качестве набора данных авторами был выбран CICIDS2017. У данного набора отмечаются проблемы дисбаланса классов, сложность файловой структуры. Была произведена оценка качества наиболее распространенных моделей машинного обучения на наборе данных. По результатам оценки с учетом минимального времени выполнения в качестве модели машинного обучения был выбран алгоритм «случайный лес» (RF). Авторы приходят к выводу о возможности применения методов машинного обучения для поиска аномалий и обнаружения КА, а также необходимости разработки универсальных алгоритмов обнаружения КА, которые не будут опираться на физическую структуру сети и настройку используемого оборудования, а также использовании технологий глубокого обучения нейронных сетей, демонстрирующих преимущество по сравнению с другими методами при решении различного перечня задач [5]. Алгоритмы KNN, CART, LR, AdaBoost, также показывают наилучшие результаты и могут быть применены для обучения на иных выборках для обнаружения других видов КА.

В исследовании [2] рассматривается подход к сравнению систем обнаружения компьютерных атак, который выявил достоинства и недостатки СОА на основе методов машинного обучения. Сравнение проводилось по четырем сценариям — внедрение и эксплуатация Shell-кода, получение несанкционированного доступа к ресурсам системы на основе подбора или скрытого изменения пароля пользователя, моделирование эксплуатации 0-day уязвимости и комплексное тестирование. В исследовании было установлено, что качество выявленных атак зависит от временных характеристик передачи данных. Автор исследования отмечает основное преимущество СОА на основе машинного обучения, заключающееся в более частом выявлении ранее неизвестных атак. В сравнительном анализе данного исследования учитываются сигнатурные и основанные на методах машинного обучения СОА, но отсутствует сравнение СОА, основанными на аномалиях.

В работе [1] рассматривается выбор метода машинного обучения для решения задачи оценки текущего качества ИТ-услуги. В качестве критериев сравнения выступали F -мера и длительность обучения. По результатам исследования метод градиентного бустинга и нейронная сеть показали наилучшие результаты. Длительность обучения градиентного бустинга более чем в 16 раз меньше длительности обучения нейронной сети, при примерно равных показателях F -меры. Применение в СОА метода машинного обучения с наименьшим временем обучения и высокой точностью позволит оперативнее выявлять воздействие на информационную инфраструктуру.

В рассмотренных работах подробно описываются возможные варианты применения методов машинного обучения с оценкой точности обнаружения КА.

В данный момент присутствует потребность в создании СОА на основе методов машинного обучения, которые обладают высокой точностью и способны идентифицировать комплексные компьютерные атаки на ранней стадии. Это требует использования моделей машинного обучения, способных адаптироваться к различным атакам и обнаруживать новые варианты атак.

Количество КА на КИИ в области атомной энергетики возрастает, Применение СОА в КИИ является необходимой технической мерой и позволяет выявлять КА на ранней стадии и минимизировать негативное воздействие на информационную инфраструктуру. Злоумышленники используют новые и нестандартные методы КА. Необходимо разрабатывать новые алгоритмы для СОА способные решать возникающие сложности в опросах обнаружении КА.

Представим критерии оценки СОА в виде таблицы (см. таблицу).

Критерии оценки систем обнаружения компьютерных атак

Критерий	Описание
Точность обнаружения	СОА должна иметь высокую точность обнаружения КА
Обнаружение новых и неизвестных атак	СОА должна с высокой точностью обнаруживать новые и ранее неизвестные КА
Работа в режиме реального времени	СОА должна обрабатывать данные в режиме реального времени и идентифицировать КА
Производительность	СОА должна уметь обрабатывать большое количество данных
Работа с разнородными типами данных	СОА должна уметь работать с разнородными типами данных
Способность обнаружения комплексных КА	СОА должна уметь обнаруживать комплексные КА

Необходимо исследовать и разрабатывать методы, которые позволяют достичь высокой точности обнаружения комплексных компьютерных атак, сохраняя при этом способность моделей к обобщению и обнаружению новых вариантов атак. Исходя из выбранных критериев, в качестве одного из возможных вариантов решения данной проблемы можно применить метод градиентного бустинга. Он может работать с различными видами данных, включая числовые и категориальные признаки. Данная особенность важна в контексте комплексных компьютерных атак, где данные могут иметь различные форматы и характеристики.

Метод градиентного бустинга стремится к уменьшению ошибки и улучшению точности прогнозов. Это может привести к стабильным результатам и более надежной работе в реальных условиях.

Библиографический список

1. *Большаков М. А., Молодкин И. А., Пугачев С. В.* Сравнительный анализ методов машинного обучения для оценки качества ИТ-услуг // Защита информации. Инсайд. 2020. № 4 (94). С. 36–43.
2. *Гетьман А. И., Горюнов М. Н., Мацкевич А. Г., Рыболовлев Д. А.* Сравнение системы обнаружения вторжений на основе машинного обучения с сигнатурными средствами защиты информации // Труды Института системного программирования РАН. 2022. Т. 34, № 5. С. 111–126.
3. *Горюнов М. Н., Мацкевич А. Г., Рыболовлев Д. А.* Синтез модели машинного обучения для обнаружения компьютерных атак на основе набора данных CICIDS2017 // Труды Института системного программирования РАН. 2020. Т. 32, № 5. С. 81–94.
4. *Гурина А. О., Елисейев В. Л., Петренко А. С., Петренко С. А.* Обнаружение аномалий на основе машинного обучения // Защита информации. Инсайд. 2019. № 4 (88). С. 52–62.
5. *McAfee A., Brynjolfsson E.* Machine, Platform, Crowd: Harnessing Our Digital Future. W. W. Norton & Company, 2017. 288 p.
6. *Wolpert D. H., Macready W. G.* No free lunch theorems for optimization // IEEE Transactions on Evolutionary Computation. 1997. Vol. 1, no. 1. P. 67–82.

А. В. Сарапульцева

Уральский государственный экономический университет, г. Екатеринбург

Цифровая безопасность как часть информационной культуры

Аннотация. В статье рассматриваются гуманитарные аспекты изменений, связанных с цифровой трансформацией. Выделяется феномен цифровой культуры, дается обзор основных подходов к объяснению цифровой культуры и видению ее функций; проводится анализ информационной безопасности как важнейшего фактора социализации и части информационной культуры.

Ключевые слова: цифровая культура; информационная безопасность; социализация; цифровая трансформация; информационное пространство.

Актуальность выбранной темы определяется все более возрастающим влиянием цифровой трансформации на все сферы человеческой жизни. Процесс перехода от аналоговой экономики к полностью цифровой, составляющий суть цифровой трансформации общества, имеет ряд гуманитарных аспектов, связанных с формированием глобального социокультурного цифрового пространства, выделением нового типа социокультурного взаимодействия и новых форм и отношений в системе «общество — человек», «общество — государство» и т. п. В социальной сфере, в сфере образования и культуры многие процессы переносятся в цифровое пространство, что приводит к необходимости в том числе поиска ответов на вопросы о месте человека в цифровом обществе, его правах и обязанностях, его возможности подготовиться и подготовить к новым реалиям. Методологической основой исследований данного рода проблем выступает гуманистическая парадигма, которая предполагает, что цифровая трансформация в этих сферах осуществляется для человека и во имя его интересов, используется также социокультурный подход, подразумевающий анализ процесса цифровой трансформации исходя из интеграции социокультурной сферы в цифровое пространство.

Ценностные ориентации современного потребителя задают основу для производства с помощью новых цифровых технологий продукта в самом широком смысле отвечающего новой индустриально-цифровой идеологии, формируемой глобальной цифровой трансформацией. Продукт, который отвечает этим требованиям, должен быть результатом использования инновационных технологий и ресурсов, его производство меняет сущность взаимодействия человека и техники, производителя и потребителя, расширяет понимание феномена труда в целом, и, соответственно, повышает значимость диалога социальной и производственной сфер. Переход в цифровое пространство многих социально-экономических процессов делает их, с одной стороны, достаточно нестабильными, а с другой стороны, обеспечивает рост скорости изменений в этих

сферах. Технологический инновационный поток, который формирует сегодня общество, опосредует доступ к вещам и людям, определяет социальное и межличностное взаимодействие. Коммуникативные связи изменяются существенно, переносясь в виртуальную сферу (социальные сети, прежде всего), теряя в предметности и «телесности», резко выигрывают в скорости и всеохватности. Размывается граница между публичным и частным в сфере коммуникации. Меняются формы коммуникаций, соответственно, меняются поведенческие паттерны, отношение к работе с информацией и способы этой работы, меняется то, как человек в целом воспринимает окружающий мир. Мы наблюдаем формирование постнеклассической научной картины мира, основанной на новых познавательных и научных стандартах (например, сближения технических и гуманитарных наук); цифровое искусство ярко заявляет о себе; на сферу художественного творчества, в свою очередь, очень сильно повлияло развитие генеративного искусственного интеллекта (нейросети). Все выше изложенное позволяет нам утверждать, что цифровая культура становится неотъемлемой частью жизни современного общества и выступает как феномен и социальный и технологический одновременно, является продуктом цифровой трансформации общества и выступает как фактор ее реализации.

Понятие цифровой культуры используется для характеристики трансформации традиционной культуры, источником которой (трансформации) стали цифровые технологии. Понятие «культура» шире понятия «цифровая культура» и включает его в себя. Цифровая культура может рассматриваться как современный этап развития общечеловеческой культуры или как одно из ее направлений, возникающих в результате синтеза цифровых технологий, новейших семиотических систем и современной художественной культуры.

Первым о цифровой культуре писал Ч. Гир, определяя ее как сферу медиа- и интернет-технологий. Сегодня цифровая культура рассматривается в более широком смысле: в качестве уровней ее функционирования выделяются, например, образовательная цифровая культура, политическая цифровая культура, научно-цифровая и т. д. Позиция Гира может быть определена как технологический детерминизм в рамках трансгуманистического направления исследования феномена цифровой культуры. Приверженцы этой концепции рассматривают цифровое общество как продукт технологической тотальности, дигитализации окружающей среды. Цифровая культура здесь — культура искусственной жизни [1].

Более востребован в современной науке гуманитарный подход, предполагающий системный анализ цифровой культуры. В рамках гу-

манитарного подхода исследуется трансформация человеческой идентичности в цифровом пространстве; цифровая культура рассматривается как закономерный исторический этап развития культуры, выделяются ее специфика, предпосылки и возможные пути и формы развития; выявляются связи Интернета с традиционными сферами духовной деятельности человека. В рамках этого подхода даются ответы на актуальнейшие вопросы существования человека в условиях цифровой трансформации: как влияет цифровизация на человека и человечество, насколько допустима и чем ограничена дигитализация человеческой жизни; каковы перспективы дигитализации образования и культуры и в принципе возможна ли полная дигитализация этих сфер жизни [2].

В условиях все большей коммуникативной свободы мира, цифровая среда становится основным пространством для работы, общения и деятельности. Однако в связи с этим возникают и новые угрозы, такие как кибератаки, кибершпионаж, киберпреступления и др. Информационная безопасность становится необходимой защитой от этих угроз, а развитие информационной культуры помогает людям лучше понимать эти риски и эффективнее защищаться от них. Информированный человек, осведомленный о потенциальных опасностях в онлайн-пространстве, может принимать более обоснованные решения и обеспечивать безопасность как себе, так и своему окружению.

Информационная культура должна включать в себя не только знание о том, как использовать технологии, но и о том, как защитить себя и свою информацию от возможных угроз. Важнейшей частью цифровой культуры является информационная безопасность. Ее смысл в гуманитарном аспекте видится в снижении, нивелировании деструктивного влияния цифровых технологий на личность. На современном этапе цифровая культура представляет собой один из мощнейших факторов социализации, направленный на использование позитивного потенциала цифровой трансформации общества, именно она должна выполнять функцию социального фильтра в информационном пространстве, чтобы оградить человека от негативного в информационном потоке, позволить ему быть субъектом цифрового общества и одновременно сохранить ценностные и смысловые ориентации. В отличие от традиционной культуры в цифровой культуре практически отсутствует адаптационная функция, связанная с передачей традиций, ориентиров и ценностей в цифровое пространство, позволяющая селективно осваивать материал опыта во взаимодействии с другими культурами и их ценностями, поэтому роль информационной безопасности в цифровой культуре возрастает многократно.

Сегодня совершенствование цифровых технологий в целом и в области культуры и образования в частности интересует не только IT-ком-

пании, эти процессы входят и в сферу интересов государства, исполнительной власти и законодательных органов. Примером может служить федеральный проект «Цифровая культура», созданный для обеспечения широкого внедрения цифровых технологий в культурное пространство страны. Комиссия Совета Федерации по развитию информационного общества вместе с соответствующими государственными структурами подготовила методические рекомендации по преподаванию основ информационной безопасности в учебных заведениях. Эти рекомендации ориентированы на решение следующих задач: повышение цифровой грамотности преподавателей и педагогических работников; необходимости акцентирования в процессе обучения на новейшие информационные технологии [3]. Опыт успешных программ и проектов в области информационной безопасности должен активно обмениваться между государствами, организациями и образовательными учреждениями. Это позволит совершенствовать методики обучения и подходы к информационной безопасности на основе лучших практик. Информационная безопасность является основой для стабильного и устойчивого развития информационного общества. При наличии высокого уровня информационной культуры общество становится более защищенным от киберугроз, что способствует сохранению экономической, социальной и политической стабильности.

Частью цифровой культуры становится цифровая этика, принципы которой еще формируются. Возможно, что в скором времени нас ждет информационный этос, закрепляющий этические нормы функционирования в информационном пространстве. В любом случае общепризнанным фактом уже является необходимость включения предмета «информационная безопасность» в дисциплинарный пул средних и высших учебных заведений с целью формирования соответствующих компетенций выпускников, обеспечивающих высокий уровень цифровой культуры молодых специалистов. В целом информационная безопасность должна рассматриваться не только как техническая проблема, но и как культурный аспект, важный для формирования осознанного и ответственного отношения к использованию информационных технологий. Ее интеграция в информационную культуру общества необходима для обеспечения его устойчивого развития и защиты от современных киберугроз.

Библиографический список

1. *Елькина Е. Е.* Цифровая культура: понятие, модели и практики // Информационное общество: образование, наука, культура и технологии будущего. 2018. № 2. С. 195–203.

2. *Левицкая И. А.* Цифровая трансформация социокультурной динамики как системный информационный процесс // *Международный научно-исследовательский журнал*. 2021. № 8 (110). Ч. 3. С. 153–156.

3. *Чернышов А. Г.* Стратегия и философия цифровизации // *Власть*. 2018. Т. 26, № 5. С. 13–21.

С. А. Сидоров

Уральский государственный экономический университет, г. Екатеринбург

Безопасность веб-ресурсов и их защита от вредоносных атак

Аннотация. В статье рассматриваются современные методы обеспечения безопасности веб-ресурсов и их защиты от вредоносных атак. Основное внимание уделяется анализу различных видов угроз, таких как SQL-инъекции, межсайтовый скриптинг (XSS), атаки на отказ в обслуживании (DDoS), а также методы их обнаружения и предотвращения. Описаны лучшие практики по использованию шифрования, аутентификации и авторизации, внедрению веб-файрволов и систем обнаружения вторжений. Особое внимание уделено значению регулярного обновления программного обеспечения и проведения аудитов безопасности.

Ключевые слова: CSRF; XSS; CORS; SQL injection; clickjacking; session hijacking; security misconfiguration.

В нашем технологическом веке существует огромное множество различных веб-ресурсов, т. е. сайтов, и каждый раз на эти множества сайтов происходят множества атак. Разработчики за время научились обрабатывать подобные атаки и нашли некоторые общие способы защиты против этого множества атак.

В самом начале рассмотрим один из популярных способов защиты аутентификации пользователя, а именно JSON Web Token (JWT) и Refresh Token. И в первую очередь рассмотрим, как злоумышленникам удается получать доступ к авторизованным аккаунтам, а именно:

– перехват через атаку перехвата сетевого трафика. Данный способ взлома заключается в перехвате сетевого трафика между клиентом и сервером, используя различные методы (подмена протокола DNS, атака ARP-подмены, использование незащищенной сети Wi-Fi и др.);

– атака на хранилище токенов на клиентской стороне. В случае, если токен аутентификации хранится в локальном хранилище на стороне клиента (например, LocalStorage и CookieStorage), злоумышленник может использовать XSS-атаку для выполнения вредоносного JavaScript-кода на странице и извлечения токена аутентификации из хранилища;

– утечка через недостаточную защиту куки. В случае, если токен хранится в CookieStorage без должной защиты, например, без использо-

вания флага `HttpOnly`, который предотвращает доступ к куки из JavaScript-кода, злоумышленник может использовать XSS-атаку для получения доступа к содержимому куки.

Для защиты от утечки JWT-токенов и других подобных токенов, подтверждающих аутентификацию пользователя, требуется использовать HTTPS для шифрования сетевого трафика, хранить токены в безопасных хранилищах и использовать безопасные заголовки запросов.

Существуют и иные способы защиты данных пользователя, а также защиты аккаунта. Ранее упоминался Refresh Token, который используется в двух практиках веб-разработчиками.

Первый — это осуществление функционала сайта для пользователей с функцией запоминания аутентификации пользователя, которая необходима для удобства использования ресурса. Второй — это защита от взлома аккаунта и утери JWT-токена. Суть в том, что при каждом обновлении страницы, переходе на новый URL домена происходит проверка — действителен ли JWT-токен. Если токен не действителен, то происходит вторая проверка на действительность Refresh Token'a, в обеих реализациях данного токена обновляется JWT-токен без потери аутентификации пользователя.

Также ранее описывался способ атаки XSS¹ (Cross-Site Scripting), который предусматривает внедрение JavaScript-кода на странице веб-сайта с целью получения данных из локального и куки хранилищ. Этот вид атаки невероятно популярен у злоумышленников, и если веб-разработчик работает в популярной компании, то он обязательно сталкивается с множеством подобных атак. Злоумышленник способен внедрить JavaScript-код в веб-ресурс с помощью выведения текста на странице.

На многочисленных сайтах появляется возможность оставить комментарий, публикацию или простое введение текста и какое-либо его проявление на сайте. Суть в том, что если внедрить под видом обычного текста JS-код, то браузер воспринимает его не как обычный текст, а, соответственно, как код.

Способы защиты имеются разные, самый простой из решений — запретить пользователям вводить специальные символы, такие как: `<`, `>`. Данные символы обозначают HTML-теги, а через него имеется возможность писать JS-код.

Рассмотрим похожий вид атаки под названием CSRF² (Cross-Site Request Forgery). CSRF — это атака на веб-приложение, при которой

¹ Что такое XSS-уязвимость и как тестировщику не пропустить ее // Хабр. 2020. 16 июля. URL: <https://habr.com/ru/articles/511318/> (дата обращения: 15.04.2024).

² CSRF-уязвимости все еще актуальны // Хабр. 2018. 4 июня. URL: <https://habr.com/ru/companies/oleg-bunin/articles/412855/> (дата обращения: 15.04.2024).

злоумышленник заставляет авторизованного пользователя выполнить нежелательные действия без его ведома. Атаки CSRF могут влиять на любые действия, которые выполняются веб-приложением в контексте аутентифицированной сессии пользователя.

Под способы защиты от данного вида атаки является CSRF токен, его особенности:

- для каждой пользовательской сессии генерируется уникальный и высокоэнтропийный токен;
- токен вставляется в DOM HTML страницы или отдается пользователю через API;
- пользователь с каждым запросом, связанным с какими-либо изменениями, должен отправить токен в параметре или в HTTP-заголовке запроса;
- так как атакующий не знает токен, то классическая CSRF-атака не работает.

Это один из самых популярных способов защиты от CSRF-атаки. Но также имеются такие виды защиты, как: Double submit cookie, Content-Type based protection, Referer-based protection, Password confirmation / websudo, SameSite Cookies в Chrome, Opera.

Также сразу рассмотрим такой механизм защиты, как CORS. CORS — это механизм, позволяющий веб-странице запрашивать ресурсы с другого источника (домена), чем тот, с которого была загружена сама страница. Он регулирует доступ к ресурсам между разными источниками веб-страниц и помогает предотвратить атаки, такие как межсайтовый скриптинг (XSS).

Рассмотрим следующую атаку на веб-ресурсы — SQL-инъекция¹ (SQLi). Данный вид атаки предусматривает внедрение SQL-запросов по входным полям сайта с целью получения доступа к базе данных.

Рассмотрим пример: `http://localhost:8080/index?id='1'`. Предположим, что по данной URL происходит GET-запрос на получение персональной информации по пользователю с `id`, равным 1. Как в принципе возможна инъекция SQL-запросов — с помощью URL запросов. В самом начале злоумышленник попытается убедиться, что не происходит каких-либо фильтров для подобного вида атак.

Какая возможна защита для предыдущей ссылки? С помощью преобразования `id` в целочисленный тип данных `int`, что уже выведет ошибку SQL-запроса. Но чаще всего злоумышленник получает доступ ко всей базе данных, точнее полностью ее копируя с помощью команд `UNION, SELECT`.

¹ SQL-инъекции' union select null,null,null -- // Хабр. 2021. 16 февр. URL: <https://habr.com/ru/companies/pentestit/articles/542190/> (дата обращения: 15.04.2024).

Следующий вид атаки — Clickjacking¹. Это способ атаки, который предусматривает собой скрытие какого-либо элемента (невидимого, прозрачного) поверх легитимных элементов веб-сайта, чтобы пользователи незаметно кликали по данным элементам выполняя нежелательные действия соответственно для самого пользователя.

С помощью данного вида атаки злоумышленники получают различные персональные данные пользователей ресурса, а также просто различные махинации.

Данный вид атаки в свое время был очень популярным в социальной сети Facebook². С помощью этого пользователи не по собственному желанию добавлялись в друзья, удаляли друзей или публиковали различные публикации.

Наверное, следующий вид атаки на веб-ресурсы знаком каждому, а именно DDoS-атака³ — это атака, при которой злоумышленник осуществляет большую нагрузку на сервер или сеть, направляя на них огромное количество запросов, что приводит к отказу обслуживания легитимных пользователей.

В целом от подобного вида атак произошло еще иное количество других видов атак, такое же произошло и с Clickjacking'ом. Также данный вид атаки является довольно трудозатратным, чтобы остановить работу популярных сервисов, которые были готовы к подобным видам атак. Рассмотрим способы минимизации зоны атаки:

- настроить firewall сервера. В политиках ни в коем случае нельзя оставлять настройки по дефолту. Важно закрыть все, кроме доверенных адресов и сетей;

- скрыть все реальные IP-адреса инфраструктуры. Периодически их менять;

- по возможности отказаться от нешифрованного трафика. Перестать использовать HTTP и перейти на HTTPS. Это важно для безопасности в целом, но и защищает от DDoS — чтобы злоумышленники не смогли подсмотреть ваши пакеты и понять, как вы их формируете, чтобы потом подделать;

- проверить бизнес-логику, чтобы понять, как и куда ваш легитимный клиент должен делать запросы. Так вы научитесь распознавать нелегитимные;

¹ Новые виды атак на основе технологии кликджекинга // Хабр. 2011. 12 июля. URL: <https://habr.com/ru/articles/123923/> (дата обращения: 15.04.2024).

² Facebook принадлежит компании Meta, которая является экстремистской организацией, деятельность которой запрещена на территории РФ.

³ DDoS-атаки в 2022 и методы защиты от них // Хабр. 2022. 30 июня. URL: <https://habr.com/ru/companies/slurm/articles/674218/> (дата обращения: 15.04.2024).

– если на физическом сервере находится не один сервис, важно тщательно разграничить их по ресурсам. Чтобы упавший сервис не мог съесть все ресурсы и повредить другим сервисам.

Существует также несколько видов атак: транспортный и сетевой. Транспортный — это вид атаки, где запросы происходят по транспортным протоколам (TCP, UDP). Сетевой — это вид атаки, где запросы происходят по сетевым каналам (IPv4, IPv6, ICMP).

Рассмотрим следующий вид атаки, он непопулярен и прост — Session Hijacking. Данный вид атаки предусматривает захват злоумышленником сеанса аутентификации пользователя, обычно угадыванием или перехвата его идентификатора сеанса, что позволяет ему выдавать себя за этого пользователя.

Security Misconfiguration. Неправильная настройка безопасности — это уязвимость, возникающая при неправильной настройке серверов, приложений или компонентов сети, что может привести к различным атакам, таким как незащищенный доступ к файлам, базам данным и другим ресурсам.

В заключение отметим, что существует большое количество видов и подвидов атак на различные ресурсы и не только веб-ресурсы, что влечет за собой расширение и увеличение способов защиты от подобных видов атак, которые были описаны в статье. Цель веб-ресурсов не только в предоставлении какого-либо функционала пользователям, а также в защите их персональных данных. В статье были рассмотрены лишь базовые примеры решения проблем для различных видов атак.

И. Ю. Хайрутдинов

Уральский государственный экономический университет, г. Екатеринбург

Актуальность уязвимостей Spectre и Meltdown и угрозы информационной безопасности

Аннотация. Рассматриваются уязвимости процессорных архитектур Intel, ARM и AMD, получивших названия Spectre и Meltdown, и их актуальность в 2024 г. Рассматривается также ущерб, который эти уязвимости могут (или могли) нанести информационной безопасности систем и устройств во всем мире при их эксплуатации.

Ключевые слова: уязвимость процессоров; угроза безопасности; архитектура Spectre и Meltdown; эксплуатация уязвимостей.

Мы знаем, что исходный код программ и операционных систем составляется программистом (или программистами) так, чтобы их программы выполняла задачи по целевому назначению. То же самое и с процессорами, а точнее с их архитектурами — их программируют так,

чтобы все назначенные функции (например, оптимизацию работы системы) выполнялись без ошибок. Но написать программу (за исключением совсем простых по функционалу) или запрограммировать процессор так, чтобы все задачи выполнялись полностью без ошибок и так называемых багов, очень сложно, а зачастую и невозможно. И если одни баги на работу программы не влияют, или влияют незначительно, то другие могут сильно затруднить работу с программой или системой в целом, вплоть до внезапной остановки работы программ и операционных систем в целом. Некоторые баги могут быть использованы в недобросовестных целях, таких как кража данных или несанкционированное управление компьютером или устройством. Такие баги называются уязвимостями. Они являются следствием недоработок со стороны разработчиков программного обеспечения или оборудования, как например процессоров. И если уязвимости ПО можно исправить путем изменения кода программы (что и делается в обновлениях к ПО и ОС), то уязвимости в структуре оборудования, особенно те, что существовали длительное время, исправить получается довольно сложно, а то и вовсе невозможно в силу разных причин. Примерами последних служат уязвимости Spectre и Meltdown.

Spectre и Meltdown — это уязвимости процессоров, которые основаны на способности процессоров к спекулятивному выполнению команд. Это означает, что процессоры на основе предыдущих выполненных команд пытаются «предугадать», какая команда будет идти следующей. Если же «предсказание» в корне неверно или не удовлетворяет каким-либо параметрам, то текущий ход конвейера процессора сбрасывается, и кусочек кода начинает вычисляться сначала [3]. Компьютерная система выполняет некоторую задачу, которая может оказаться ненужной. Работа выполняется до того, как станет известно, действительно ли она необходима, чтобы предотвратить задержку, которая может возникнуть при выполнении работы после того, как станет известно, что она необходима¹. За счет этого достигается высокая производительность современных процессоров. Но спекулятивное выполнение команд очень рискованно с точки зрения безопасности памяти. Все «предугаданные» действия выполняются с реальными данными, которые в таком случае защищены крайне слабо [1]. Суть уязвимостей Meltdown и Spectre заключается именно в этом, и именно в этом плане они очень опасны с точки зрения защиты данных.

Уязвимость Meltdown основана на определении искомого адреса X по скорости ответа процессора и последующего вычисления значения

¹ Спекулятивное исполнение // Википедия. URL: https://ru.wikipedia.org/wiki/Спекулятивное_исполнение (дата обращения: 16.04.2024).

по этому адресу с помощью косвенной адресации [3]. Эту уязвимость очень легко эксплуатировать с точки зрения программного кода, но как оказалось позднее, ее также легко и исправить путем простого обновления операционной системы. Беда в том, что обновления для устранения уязвимости сильно замедляют работу операционной системы, и компании постепенно от них начали отказываться. Вместо этого уязвимость компании-производители процессоров устраняли на аппаратном уровне, тем более что AMD официально заявила о неуязвимости их продуктов к Meltdown в январе 2018 г. Попытка же Intel обновить свои старые чипы для защиты от Meltdown оказалась неудачной, но тем не менее компания с 2019 г. выпускала процессоры, защищенные от уязвимости Meltdown. 15 марта 2018 г. Intel анонсировала линейки процессоров Xeon Scalab и Core 8-го поколения. По словам Intel, они будут лишены уязвимостей Meltdown и Spectre, в частности, за счет внедрения новой системы сегментирования [2].

Совсем другая ситуация обстоит с уязвимостью Spectre. Реализация этих уязвимостей на уровне программного кода гораздо сложнее — она подразумевает выполнение какой-либо программы, примерное представление выполняемых ею задач, загрузка защищенной информации в кэш процессора и вывод данных из него сторонними методами или посредством самой выполняемой программы. От этой уязвимости полностью в настоящее время избавиться невозможно, она касается в том числе процессоров AMD и новейших процессоров Intel поколения Alder Lake, архитектура которых разрабатывалась на основе архитектуры ARM.

Обеими уязвимостями подвержены практически все процессоры, выпущенные с конца 1990-х гг. Ниже приведена таблица наличия уязвимостей у аппаратных продуктов различных производителей.

Подверженность оборудования разных архитектур Spectre и Meltdown [1]

Фирма	Meltdown	Spectre
AMD	–	+
Intel	+	+
Apple	+	+
ARM (не все)	+	+
IBM	+	+
VIA	+	+

Из процессоров на архитектуре ARM (часто встречающиеся в Android-устройствах) подвержены следующие архитектуры: Cortex-R7, -R8, -A8, -A9, -A12, -A15, -A17, -A57, -A72, -A73, -A75 [1].

Как видно из данных таблицы, названные уязвимости еще актуальны и сегодня, особенно если учитывать то, что некоторые предприятия используют устаревшие компьютерные системы

по причине отсутствия необходимых средств на покупку более современных. Уязвимости не могут нанести ущерб самим данным в ком-

пьютерных системах, но они наносят огромный ущерб конфиденциальности данных в оперативной памяти. В частности, если пользователь открывает какую-нибудь страницу с конфиденциальными данными (например, портал «Госуслуги» или онлайн-банк), и вместе с тем неизвестный ему сайт или устанавливает как бы легитимную программу с неизвестных источников, то открытый им сайт или программа может прочитать данные из оперативной памяти, что создает угрозу кражи паролей и прочих секретных данных о пользователе. А если речь идет о корпорациях, это может создать угрозу безопасности данных, содержащих коммерческую тайну, что может сказаться на рынке в целом.

Таким образом, исходя из вышесказанного, можно сделать вывод, что уязвимости Meltdown и Spectre все еще актуальны в 2024 г. Если современное оборудование подвержено Meltdown все реже, то Spectre останется актуальной еще некоторое время, пока корпорации полностью не перейдут на современное оборудование (возможно, созданное в будущем), в котором эти и будущие, еще неизвестные уязвимости будут исправлены на аппаратном уровне. Пока что методы защиты от последствий этих уязвимостей остаются все те же — обновлять систему, а по возможности и оборудование, избегать сомнительных сайтов, использовать лицензионное ПО, не переходить по неизвестным ссылкам и не открывать файлы от незнакомых лиц, в том числе отправленные посредством электронной почты.

Библиографический список

1. Алиева А. Б., Аджиев Р. Д. Уязвимости Spectre и Meltdown // Общество и личность: теория и практика гуманизации в современных реалиях: материалы X Всерос. науч.-практ. конф. (Ставрополь, 13 мая 2022 г.). Ставрополь: СКСИ, 2022. С. 197–201.
2. Гужанков Е. Г., Воробьев Д. С., Уваровский В. В. Уязвимости Meltdown и Spectre микропроцессоров производителей AMD, ARM и Intel // Научные исследования и современное образование: сб. материалов II Междунар. науч.-практ. конф. (Чебоксары, 26 марта 2018 г.). Чебоксары: Центр научного сотрудничества «Интерактив плюс», 2018. С. 213–215.
3. Садилов А. В., Гонтовой С. В. О проблемах информационной безопасности, связанных с устранением уязвимостей Meltdown и Spectre // Автоматизированные системы управления и информационные технологии: материалы Всерос. науч.-техн. конф.: в 2 т. (Пермь, 17 мая 2018 г.). Пермь: ПНИПУ, 2018. Т. 2. С. 315–321.

Н. А. Шаидова

Уральский государственный экономический университет, г. Екатеринбург

Исследование методов обеспечения безопасности данных на серверах хостинга

Аннотация. Анализируются разнообразные методы обеспечения безопасности данных на серверах провайдеров хостинга. В частности, исследованы такие аспекты, как применение шифрования, реализация многофакторной аутентификации, осуществление постоянного контроля безопасности. Это исследование ценно тем, что рассмотренные методы способствуют повышению степени защищенности информации на веб-сайтах и снижению риска утечки данных.

Ключевые слова: методы защиты данных на серверах; шифрование; многоуровневая аутентификация; мониторинг безопасности.

Исследование методов обеспечения безопасности информации на серверах хостинга приобретает особую актуальность в контексте современных технологических реалий, где защита данных является критически важной. Анализ различных способов защиты информации, таких как шифрование, реализация многоуровневой аутентификации и управление безопасностью, позволит не только оценить наличие защитных механизмов на серверах хостинга, но и выработать рекомендации для укрепления защиты данных на интернет-платформах с целью предотвращения возможных угроз.

Современный бизнес стал зависимым от информационных технологий и требует необходимой защиты. Важно понимать, что угроза может прийти отовсюду и поэтому необходима комплексная стратегия защиты¹.

Защита данных на серверах, которые предоставляют услуги хостинга, является ключевым аспектом в сфере информационной безопасности. Для обеспечения надежной защиты информации на таких серверах используются различные технологии и методы:

– шифрование данных — это процесс преобразования информации в зашифрованный формат, который может быть прочитан только с использованием специального ключа². Шифрование данных на серверах хостинга помогает защитить конфиденциальные данные от несанкционированного доступа;

¹ Миценко Д. Е., Панов М. А. Актуальность информационной безопасности в условиях цифровой экономики // Цифровая трансформация общества и информационная безопасность: материалы II Всерос. науч.-практ. конф. (Екатеринбург, 19 мая 2023 г.). Екатеринбург: УрГЭУ, 2023. С. 21–24.

² Компьютерная безопасность и информационная безопасность: в чем разница? URL: <https://uchet-jkh.ru/i/kompyuternaya-bezopasnost-i-informacionnaya-bezopasnost-v-chem-raznica/> (дата обращения: 18.04.2024).

– многоуровневая аутентификация требует от пользователей предоставить несколько форм идентификации для доступа к системе. Это может включать в себя комбинацию пароля, биометрических данных, одноразовых кодов и других методов, чтобы обеспечить дополнительный уровень безопасности;

– осуществление мониторинга безопасности включает непрерывное наблюдение и исследование действий, происходящих на серверах хостинга, для выявления возможных опасностей. Такой подход помогает оперативно откликаться на угрозы безопасности и предупреждать утечки информации;

– регулярное обновление программного обеспечения и установка патчей безопасности помогают устранять потенциальные уязвимости, которые могут быть использованы злоумышленниками для осуществления атак на серверы хостинг-провайдеров.

Эти стратегии и технологии служат фундаментом для гарантии безопасности данных на серверах хостинг-провайдеров. Их совместное применение позволит воплотить в жизнь эффективную систему защиты информации, а также предотвратить потенциальные риски для безопасности.

Цифровые решения для бизнеса и общества

А. О. Алексеева

Уральский государственный экономический университет, г. Екатеринбург

Необходимость сбора ценовых данных и их обработки на предприятиях оптовой торговли

Аннотация. В статье рассматривается этап ценообразования на предприятии оптовой торговли. Обсуждается то, как специфика составления цен изменилась с развитием информационных технологий. Предложен метод автоматизации сбора и обработки ценовых данных других участников рынка для компании сегмента B2B.

Ключевые слова: ценообразование; оптовая торговля; анализ информации; информационные технологии.

За последние годы развитие информационных технологий происходит со стремительной скоростью. В настоящий момент существует огромное разнообразие различных программ и IT-продуктов, каждый из которых имеет свои функции, особенности и возможности. Таким образом, то или иное предприятие стремится автоматизировать каждый процесс и выполняемые функции внедрением этих технологий. Соответственно, со временем стало так, что многие процедуры происходят в Интернете, будь это продажа, покупка, поиск нужного товара и др.

С частичным перемещением взаимодействий розничной торговли в онлайн-режим, потребители стали экономить время на совершение покупок, а некоторые потребители по тем или иным причинам не хотят приобретать товары в локальных магазинах, предпочитая заказывать товар из другого города или даже страны [1, с. 80].

Добыть какую-либо информацию теперь очень просто, достаточно лишь иметь некий гаджет с выходом в Интернет. Но что же будет результатом этой самой «добычи информации»? Тут разработчик уже позаботился о том, чтобы пользователь обращал внимание на определенные предложения продавцов, «выталкивая» конкретные позиции выше других. Но есть вероятность, что предложенные данные пользователя не устроят, ведь продвигают не лучший товар, а наиболее прорекламированный. Да, с одной стороны, каждый продавец может приблизить свое предложение заинтересованному пользователю за счет применения рекламных технологий. Но есть и другая сторона — сам пользователь. Его уже не так-то просто «заманить» на свое предложение только при помощи рекламы. Современный покупатель умеет сам, не прилагая

особых усилий, найти варианты решения своих потребностей, в том числе в обход рекламных объявлений поставщиков. И зачастую варианты, отобранные пользователем, для него являются более приемлемыми. Ни для кого не будет открытием, что выбор часто будет падать в пользу того поставщика, чей продукт или услуга решит потребность покупателя с минимальными затратами для последнего.

На этом этапе подходим к важному моменту для продавца: грамотное выставление цен на товары и услуги.

Ценообразование — это процесс, посредством которого компания устанавливает цену, по которой она будет продавать свои продукты и услуги, и может быть частью маркетингового плана компании. При установлении цен бизнес будет учитывать цену, по которой он может приобрести товары, стоимость производства, рынок, конкуренцию, рыночные условия, бренд и качество продукта.

Исходим из того, что производитель и поставщик — это прежде всего коммерческие организации, в результате деятельности которых должна образовываться прибыль и налогооблагаемая база, и цена напрямую влияет на этот показатель. Соответственно, тут очень важно соблюдать баланс. С одной стороны, товар не должен быть слишком дешевым, тем самым пренебрегая прибылью предприятия, а с другой стороны, не отпугнув покупателя ценой выше, чем аналогичные предложения. Говоря иначе, цена должна полностью покрывать все затраты и одновременно быть приемлемой для покупателя, а также генерировать прибыль, из которой и будут платиться налоги.

В то время, когда еще IT-технологии не были достаточно развиты, менеджеры по закупке и продажам вынуждены были очень много своих ресурсов вкладывать в изучение предложений конкурентов и предпочтений потребителей. Информацию о предложениях поставщиков приходилось добывать практически вручную, путем направления писем с запросом на коммерческие предложения. Затем уходило достаточно много времени на сравнение полученных предложений, расчет себестоимости и формирование вариантов своей цены предложения. А проводить анализ цен предложения конкурентов в полном объеме вообще было нереальной задачей. В массовом сегменте постоянно как открывались новые производители и продавцы, так и закрывались те, по которым информация была уже собрана и обработана, и по сути, такие данные очень быстро теряли свою актуальность. Именно в тот период, от преуспевающих менеджеров по закупке и продажам часто можно было услышать известную фразу: «Кто владеет информацией, тот владеет миром».

Владея необходимой информацией, можно владеть информацией о варьировании чужих цен и ассортимента товаров для изменения собственного прайса, который станет наиболее привлекательным для клиентов [2, с. 275].

И это так. Только вот с развитием IT-технологий «владеющих миром» стало настолько много, что в наши дни актуальна уже другая фраза, автором которой является Генри Форд: «Тот, кто сможет дать потребителю лучшее качество по низшим ценам, непременно станет во главе индустрии — безразлично, какие бы товары он ни производил. Это непреложный закон».

В данной статье фактор качества будет опущен, будем считать, что «некачественный» товар долго на рынке не задержится и будет подвержен критике. Автором рассматривается сегмент B2B, иначе говоря, оптовые предприятия. Здесь уже не все так очевидно, как на розничном рынке. Найти розничную цену на товар в Интернете занимает несколько секунд — и это правда. Например, тот же «Яндекс» обладает весьма внушительными возможностями для сбора ценовых предложений различных игроков сегмента B2C. Но большинство розничных игроков не являются производителями или крупными оптовыми компаниями, а закупают большие партии у более крупных продавцов с целью дальнейшей перепродажи. Соответственно, наш условный производитель должен ориентироваться на цену предложения оптовых поставщиков аналогичного нашему товару. А эту информацию уже не так просто раздобыть. Оптовая цена может быть весьма индивидуальна и даже включена в состав коммерческой тайны при заключении договоров между покупателем и продавцом. Тут мы подходим к вопросу: «Чем можно воспользоваться предприятию B2B?». В качестве решения «рабочей» методикой может быть некая программа, производящая сбор розничных данных, интересующих нашего условного производителя конкретных магазинов, с последующим анализом. Выяснить наценку на интересующий товар не так сложно, хотя точное значение наценки у каждого розничного магазина будет свое, как и входящие условия тоже будут несколько отличаться, но уже будет на что опираться. Второй важный момент, который необходимо учесть, это то, что по сути один товар может продаваться под разными названиями, брендами и в разных упаковках, но на самом деле являться абсолютно идентичным продуктом. Не секрет, что некоторые производители сами могут выпускать идентичный товар в разных по дизайну упаковках с другим названием, преследуя цель занять побольше места на полке потенциального посредника при продвижении своей продукции. Поэтому при анализе цен необходимо четко понимать всю линейку товаров-субститутов. По сути разрабаты-

ваемому IT-решению нужно прямо указать, с каких товарных позиций нужно собрать данные. Еще один момент — это расходная составляющая на перемещение изготовленной продукции от места производства до места ее реализации через розничную сеть. Поэтому нашего заказчика, безусловно, будет интересовать еще и география реализации выпускаемой готовой продукции, так как в любом случае, чем дальше от производства предполагается реализовывать продукцию конечному покупателю, тем будут выше накладные расходы. И конкурировать с местными производителями будет сложнее. Что касается самого сбора, то многие розничные магазины, а особенно торговые сети выкладывают свои ценовые предложения в открытый доступ посредством своих интернет-магазинов.

Предприятию, выпускающему определенную продукцию, достаточно будет собрать информацию о том, по какой цене на определенной территории реализуется интересующая продукция. И потом математически рассчитать цену закупа и сформировать свое предложение потенциальному покупателю.

Весь процесс может выглядеть следующим образом.

1. Маркетолог предприятия проводя анализ покупателей, в том числе и через полевые исследования, составляет список товаров-субститутов, т. е. товаров, аналогичных товару нашего производителя.

2. Маркетолог определяет список web-ресурсов, которые необходимо исследовать, т. е. список интернет-магазинов, которые работают на интересующей нас территории.

3. При помощи IT-продукта с заданной периодичностью и детализацией производится сбор ценовых данных на конкретный момент времени путем извлечения данных с web-страниц конкретных позиций.

4. Далее программа соотносит полученные данные с аналогичными товарными позициями списка.

5. В зависимости от рассчитанной себестоимости на основе заложенных алгоритмов IT-решение предлагает тот или иной вариант возможного ценового предложения для потенциального оптового покупателя нашей продукции.

Весь процесс после ввода начальных настроек, которые описаны в п. 1 и п. 2, происходит полностью автоматически. То есть на практике сбор данных и формирование предложений для принятия решений реализуется практически в режиме онлайн. Задача работника предприятия только в том, чтобы дополнять список по необходимости и запускать саму программу.

В последующем в разрабатываемый продукт можно включить расширенный функционал. Например, IT-решение может уведомлять об

определенных изменениях на исследуемых ресурсах из подготовленного в п. 2 списка.

Таким образом, в ходе статьи была проанализирована часть процесса ценообразования предприятия оптовой торговли и был предложен вариант ее автоматизации.

Библиографический список

1. Бурик М. В., Паршикова М. А. Оптовая торговля в современных тенденциях развития интернет-торговли // Актуальные проблемы развития хозяйствующих субъектов, территорий и систем регионального и муниципального управления: материалы XV Междунар. науч.-практ. конф. (Курск, 24–25 мая 2020 г.). Курск: ЮЗГУ, 2020. Вып. 3. С. 80–83.

2. Смирнова Л. И., Короткова В. И., Романченко А. Д. Анализ цен конкурентов в условиях современных технологий // Вестник Академии знаний. 2022. № 49 (2). С. 275–278.

М. А. Анисимова

Уральский государственный экономический университет, г. Екатеринбург

Формирование в здравоохранении технологии блокчейна, ориентированной на пациента

Аннотация. Рассмотрена необходимость формирования технологии блокчейна в здравоохранении как условия оптимизации клинических рабочих процессов. Представлено изложение взглядов специалистов на развитие блокчейна. На основе обобщения мирового опыта показаны выгоды блокчейна для пациентов. Предложен вариант технического аспекта реализации технологии блокчейна в здравоохранении.

Ключевые слова: здравоохранение; блокчейн; пациент; смарт-контракт.

Актуальность темы исследования определяется необходимостью цифрового преобразования отрасли здравоохранения в новый формат, предопределяющий современные информационные изменения. Пандемия выявила ограничения при устранении чрезвычайных ситуаций в области общественного здравоохранения с использованием существующих технологий цифрового здравоохранения. В последнее время ряд исследователей сосредоточились на разработке и совершенствовании прорывных технологий, таких как блокчейн, чтобы улучшить рабочий процесс цифрового здравоохранения, обеспечить децентрализованный обмен медицинскими данными, защищая конфиденциальность пользователей, расширяя возможности данных и обеспечивая надежное управление [1; 4]. Технология блокчейна позволяет существенно преобразовать существующую экосистему здравоохранения за счет оптимизации клинических рабочих процессов.

Блокчейн представляет собой цепочку блоков, в которой транзакции записываются в цифровом виде, что позволяет хранить данные о пациентах в цифровом реестре. Внутренняя гибкость достигается децентрализованным способом, при котором данная технология может обеспечить пациентов и медицинские организации информацией с использованием смарт-контрактов, в которых заложены заранее определенные условия между участниками, позволяющие автоматизировать процессы аудита, управления цепочками поставок медицинских товаров, осуществлять удаленный мониторинг пациентов.

Вместе с тем условия хозяйствования в отрасли здравоохранения ужесточились под влиянием ряда новых факторов: пандемия, необходимость обеспечения конфиденциальности и безопасности данных о здоровье и ряда других. Ряд исследователей по проблемам развития блокчейна сосредоточены на рассмотрении его роли как способа хранения данных электронных медицинских карт пациентов, управлении данными [2; 6]. Другие исследования были посвящены инструментам принятия управленческих решений специалистами в области здравоохранения с использованием технологий искусственного интеллекта [7]. Проблема безопасности и конфиденциальности медицинских данных пациентов решалась с использованием сети серверно-клиентской архитектуры на основе блокчейна. Однако решение данной задачи было осложнено к склонности серверно-клиентских архитектур к сбою. Специалистами была разработана система мониторинга пациентов в режиме реального времени для записи данных и обмена этой информацией с медицинскими работниками. Основной целью этой системы являлось устранение третьих лиц и проблем с уязвимостями при удаленном мониторинге [3]. Высокую актуальность имела разработка платформы на основе блокчейна, на которой обсуждались важные приложения блокчейна для решения проблем, возникающих в связи с пандемией COVID-19 [5].

Однако в этих обзорах отсутствовало исследование технологии блокчейна, основанное на подходе, ориентированном на пациента. Недостаточная изученность и большое значение для здравоохранения развитие общей архитектуры блокчейна как способа преобразования традиционной экосистемы здравоохранения предопределили содержание данной работы.

Развитие блокчейна в здравоохранении все в большей мере необходимо ориентировать на пациента путем объединения технологии искусственного интеллекта и блокчейна для чего данную структуру необходимо разделить на три уровня: блокчейн, искусственный интеллект и уровень децентрализованного хранилища через смарт-контракты напрямую, что позволит обеспечить доступность данной технологии одновременно регулирующим органам, поставщикам медицинской тех-

ники и лекарственных препаратов, больницам извлекать выгоду из приложений, ориентированных на пациента. Смарт-контракты не только облегчают доступность на основе правил, но и обеспечивают гибкость для реализации блокчейна.

Как показывает мировой опыт, технология блокчейна позволяет получать максимальную выгоду пациенту:

- обеспечить конфиденциальность и безопасность медицинских данных;
- предоставление полного контроля над медицинской информацией и данными;
- безопасный обмен личной информацией с медицинской организацией;
- предоставление персонализированных медицинских услуг пациентам и здоровым людям;
- помощь при стихийных бедствиях и эпидемиях.

Большие данные всех участников отрасли здравоохранения шифруются и хранятся в децентрализованной системе хранения с использованием функций конфиденциальности и безопасности. Преимущества использования децентрализованной системы хранения включают безопасность, конфиденциальность, отсутствие единой точки отказа и экономическую эффективность. Важной целью децентрализованной системы хранения является предоставление сетям хранения данных вне и внутри сети для облегчения ориентированного на пациента управления данными. Таким образом, объединение механизмов хранения данных в цепочке позволяет создать децентрализованную систему хранения, которая безопасно подключается к другим базам данных.

Новым структурообразующим ядром системы блокчейна могут стать узлы-провайдеров, пользовательские узлы и обучающие узлы. Организации здравоохранения имеют узел провайдера для хранения и обновления информации о каждом пациенте (имя, уникальный идентификатор пациента, назначенные лекарства и сводки о выписке) в реестре блокчейна. Кроме того, узлы провайдеров передают право собственности на медицинские данные пациента на блокчейне, а также хранят электронные медицинские записи такие как компьютерная томография, рентгенография грудной клетки и медицинские отчеты. Пользовательский узел состоит из пациентов, которые управляют и контролируют свои наборы данных на блокчейн-платформах. Эта операция может быть достигнута путем реализации смарт-контракта, обеспечивающего доступ к контролю и безопасности конфиденциальных данных пациентов без использования централизованной инфраструктуры. Участники ориентированной на пациента экосистемы здравоохранения синхронизируются с сетью блокчейна, чтобы обмениваться сообщениями отно-

сительно доступа к данным пациентов для разработки стратегий управления данными. Ориентированная на пациента структура, основанная на блокчейне, может предложить ряд возможных решений, связанных с улучшенной функциональной совместимостью между различными структурными подразделениями здравоохранения, такими как страховые и фармацевтические компании, больницами, логистика и управленческие клиническими данными.

С учетом вышесказанного возможен следующий вариант технического аспекта организации технологии блокчейна, в котором объединились медицинские организации с целью создания автоматического анализа медицинских данных о пациентах. При данной системе блокчейна:

1) получение каждой медицинской организацией для локализации копии модели искусственного интеллекта;

2) передача обновленных параметров модели искусственного интеллекта участвующим организациям здравоохранения для продолжения обучения на местах, что обеспечивает более качественные и точные прогнозы, поскольку содержит самую актуальную информацию о заболеваниях пациентов;

3) заключение смарт-контрактов в рамках обеспечивает доверие между участниками, определяя правила и обязательства;

4) распределение технологией блокчейн параметров модели искусственного интеллекта по медицинским организациям.

Обученная модель в сети блокчейн обеспечивает более качественные и точные прогнозы, поскольку содержит самую актуальную информацию.

Таким образом, важная роль блокчейна, ориентированная на пациента определяется его специфическими особенностями. Во-первых, это улучшает взаимодействие различных заинтересованных сторон отрасли здравоохранения. Во-вторых, пациенты безопасно хранят медицинские записи на блокчейн-платформах и владеют своими конфиденциальными данными. В-третьих, блокчейн соединяет наборы данных пациентов и улучшает медицинские исследования и лечение за счет использования моделей искусственного интеллекта для прогнозной диагностики и анализа. Безусловно, реализация технологии блокчейна в здравоохранении будет способствовать пациенту в облегчении доступа к своим медицинским данным, облегчая персонализированное лечение.

Библиографический список

1. Берсенева Е. А., Умнов С. В., Умнов М. С., Агамов З. Х. Технология блокчейн как компонент цифровизации здравоохранения // Профилактическая медицина. 2023. № 26 (4). С. 95–99.

2. *Воронов Е. Ю.* Разработка и применение блокчейн технологий в медицине // Вызовы современности и стратегии развития общества в условиях новой реальности: материалы XV Междунар. науч.-практ. конф. (Москва, 15 марта 2023 г.). М.: Алеф, 2023. С. 295–298.

3. *Гайда Н. Д., Федоров М. И., Скороходова Л. А.* Особенности применения блокчейн технологий в здравоохранении // Актуальные вопросы современной медицинской науки и здравоохранения: сб. ст. VIII Междунар. науч.-практ. конф. молодых ученых и студентов (Екатеринбург, 19–20 апреля 2023 г.). Екатеринбург: УГМУ Минздрава России, 2023. С. 3352–3356.

4. *Каем К.* Цифровая медицина — основа новой парадигмы здравоохранения // Sk Альманах. Цифровая экономика. 2017. С. 40–45.

5. *Кузнецова В. П., Вардомацкая Л. П., Тропинова Е. А.* Блокчейн в здравоохранении // Экономика и управление. 2018. № 7. С. 16–20.

6. *Куракова Н. Г., Черченко О. В., Цветкова Л. А.* Технологии блокчейн в здравоохранении: позиции России на глобальном публикационном ландшафте // Врач и информационные технологии. 2021. № 1. С. 25–39.

7. *Цыганов С. Н.* Применение технологии блокчейн для хранения данных электронных медицинских карт пациентов // Технические науки. 2017. № 11. С. 338–343.

Г. П. Бутко

Уральский государственный экономический университет, г. Екатеринбург

М. А. Меньшикова

Технологический университет

*имени дважды Героя Советского Союза, летчика-космонавта А. А. Леонова,
г. Королев, Московская область*

Информационные технологии как фактор повышения эффективности в контексте рисков общества

Аннотация. В статье рассмотрены вопросы повышения эффективной деятельности на основе информационных технологий с позиции рисков общества. Представлены перспективы кластерного подхода с учетом рыночных параметров. Уточнены возможности инновационного развития с предотвращением рисков. Акцентировано внимание на взаимозаменяемости ресурсов и введения конструктивного подхода на основе оценочной системы индикаторов. Перспективы развития и эффективный механизм реализации авторских подходов позволяют обосновать возможность использования цифровых технологий на перспективный период в контексте рисков общества и условиях обеспечения экономической безопасности.

Ключевые слова: информационные технологии; рисковое общество; этапы развития; бизнес-структуры; эффективность; оценка; инновации.

На современном этапе развития информационные технологии являются флагом во многих предпринимательских направлениях и сферах деятельности.

Именно информационные технологии (ИТ) позволяют автоматизировать бизнес-процессы, совершенствовать многочисленные операции, настроить эффективные каналы продвижения работ и услуг, а также снижать расходы на их производство и реализацию.

Сегодня ведущее значение информационные технологии представляют в электронной коммерции. На основе информационных технологий возможно снизить затраты на операции и поднять конверсию и продажи.

Если рассматривать проблему в динамике [1; 2; 3; 4; 5; 6], можно отметить, что бизнес-процессы на основе электронной коммерциализации выступают все более масштабными для предпринимателей и потребителей как в отечественной практике, так и зарубежной.

На заключительном этапе оценки эффективности результатов информационных технологий используют следующий алгоритм:

- выбор метода оценки эффективности;
- проведение количественного анализа;
- создание модели реальных бизнес-процессов;
- апробация инструментов расчета эффективности.

Первоначально выполняется качественный анализ с последующей детализацией по таким параметрам:

- емкость рынка;
- масштаб производства.

В основе анализа предлагается кластерный подход, базирующийся на полной полезности объекта исследования с минимизацией рисков.

Непосредственно процесс формирования экономического кластера на основе ИТ возможно провести по следующей схеме:

- научное обоснование по новым продуктам ИТ (видам услуг, процессам);
- перспективы развития рынка новых продуктов ИТ (услуг) и обоснование перспективных направлений развития производства;
- выбор новых видов производства продуктов, услуг;
- оценка поступления без рискованных инвестиций для создания кластера ИТ инновационного типа.

Как правило, важным является обоснование кластера на основе максимума дохода при минимизации финансовых рисков.

Для выбора приоритетных направлений развития ИТ целесообразно исследование конкурентной устойчивости в следующем формате.

1. Глубокая взаимозаменяемость продукции разных отраслей бизнеса.
2. Комплексное и многоцелевое использование взаимозаменяемых видов ресурсов в разрезе бизнес-структур.

3. Взаимообусловленность информационных технологий и производственных процессов на основе инновационного подхода.

Существенное значение при реализации предлагаемой модели представляют бизнес-структуры как научно-производственные центры (НПЦ). Роль и значение их состоит в востребованности инноваций в различных структурных секторах экономики.

Для фирм среднего бизнеса при развитии ИТ целесообразно использовать ряд следующих методов:

1) метод сопоставления данных — дает возможность сопоставлять уровни настоящего и предыдущих периодов;

2) бюджетный метод — позволяет оценить состояние бюджетов на ИТ по периодам.

Главным и отправным моментом подходом по методике оценки эффективности деятельности фирмы является разработка бизнес-плана по внедрению ИТ на фирме с обоснованием цепочки «вход по информационным ресурсам — бизнес-процессы — выход по результатам».

Важность выдвигаемых позиций обусловлена и необходимостью учета влияния эндогенных и экзогенных параметров, влияющих на уровень информационной безопасности во взаимной связи с учетом дифференциации уровня рисков.

По мнению авторов, необходимо ввести в практику систему индикаторов ИТ для последующего мониторинга бизнес-структур. Также имеет смысл выделить в системе индикаторов четыре фактора: влияния, сохранения, стабилизации и развития с последующей оценкой эффективности ИТ.

Среди существенных и важных параметров роста эффективности ИТ целесообразно учесть динамизм системы ценообразования в развитии с учетом рисков общества.

Неоспоримым фактором продвижения ИТ является проблема состояния нормативно-правовой базы, устойчивых позиций с разработчиками, базирующихся на цифровых решениях, состоянии экономической безопасности.

Библиографический список

1. *Бутко Г. П.* Цифровые технологии в бизнес-проектировании // VI-технологии и корпоративные информационные системы в оптимизации бизнес-процессов цифровой экономики: материалы IX Междунар. науч.-практ. оч.-заоч. конф. (Екатеринбург, 2 декабря 2021 г.). Екатеринбург: УрГЭУ, 2022. С. 36–40.
2. *Бутко Г. П., Перепелкина Л. А., Шурмина О. А.* Повышение конкурентоспособности как фактор обеспечения экономической безопасности / под ред. Г. П. Бутко. Екатеринбург: УГЛТУ, 2019. 142 с.

3. Ильин С. М., Самарская Н. А., Симанович С. В. Исследование взаимосвязи плотности коммуникативного пространства и условий труда работников индустрии гостеприимства и общественного питания // Экономика труда. 2023. Т. 10, № 6. С. 923–936.

4. Кочкин К. Б., Кожухина К. А. Проблемы совершенствования управления рисками в предпринимательской деятельности // Экономика и экологический менеджмент. 2019. № 1. С. 171–182.

5. Куразова Д. А., Джентамиров М. Х. Информационная технология как неотъемлемый атрибут эффективного управления предприятием и ее влияние на хозяйственный процесс // Экономика и социум. 2017. № 1-2 (32). С. 1669–1673.

6. Максименко И. А. Архитектура факторов конкурентной устойчивости бизнеса // Экономика, предпринимательство и право. 2022. Т. 12, № 2. С. 709–728.

Е. В. Буценко

Уральский государственный экономический университет, г. Екатеринбург

Мониторинг меню ресторана на основе методов интеллектуального анализа данных

Аннотация. В статье представлена разработка и создание системы мониторинга меню ресторана с использованием языков программирования Python и C#. Рассмотрены методы получения данных о меню ресторанов. Разработан алгоритм парсинга данных и осуществлена его программная реализация с помощью Python. Выполнена программная реализация системы мониторинга меню ресторана с использованием C# и показано ее практическое применение.

Ключевые слова: мониторинг; парсинг данных; ресторан; извлечение данных; анализ данных; интеллектуальный анализ данных.

Введение. Новые технологии внесли огромное влияние во все сферы человеческой жизни, не исключением стала и сфера общепита. Очень часто люди сталкиваются с проблемой выбора блюд. Мир кулинарии стал очень разнообразным, появились различные способы приготовления, способы тепловой обработки, сочетания несочетаемых продуктов, что сильно усложняет выбор. В настоящее время разработаны различные приложения для доставки, где представлено меню ресторанов с фото и ценами блюд. При личном посещении заведений общепита официант подробно описывает предлагаемые блюда.

Когда клиент приходит в дорогой ресторан, в меню чаще всего представлено только название блюд. Для удобства выбора можно предложить ему скачать приложение и уже непосредственно в нем с фото и описанием выбрать блюдо. При этом немаловажную роль также играет модификатор цены, чтобы посетитель смог ориентироваться на подходящую цену. Благодаря такому приложению можно существенно ускорить поиск нужного блюда, разработав систему интеллектуального анализа

данных, позволяющую по полученным входным параметрам быстро подобрать оптимальное блюдо. Однако для таких систем прежде всего нужны данные в структурированном виде. Поэтому при разработке систем анализа для поиска и подготовки данных гораздо удобнее использовать уже готовое решение [2]. Таким решением может стать разработанное приложение. Его создание предоставляет возможность получения всей необходимой для последующего анализа информации в удобном для пользователя виде.

Предметом исследования является автоматизация процессов мониторинга позиций блюд в меню ресторана. Объект исследования — сайты ресторанов. Цель исследования — разработка информационно-аналитической системы мониторинга меню ресторанов для автоматизированного подбора блюд, реализованная с помощью языков программирования Python и C#. Данное программное обеспечение разработано для платформы Windows.

Для достижения поставленной цели необходимо изучить сайты сети ресторанов «Реста Менеджмент», проанализировать основные характеристики позиций блюд в меню, выбрать необходимые параметры запросов пользователя системы мониторинга, разработать алгоритмы работы системы мониторинга и создать программное приложение.

Методы исследования. Для разработки и построения приложения мониторинга меню ресторана необходимо собрать и проанализировать информацию о популярных ресторанах Екатеринбурга, а также исследовать существующие методы и системы получения данных о ресторанах.

Рассмотрим одну из популярных сетей сферы общепита «Реста Менеджмент». Данная группа компаний является крупнейшим ресторанным холдингом Екатеринбурга, объединяющим 10 заведений. Это известные рестораны и пабы города, представляющие самые популярные гастрономические традиции мира, такие как «Троекуровъ», «Уральские пельмени», The Rosy Jane Pub & Whisky bar, James, Pan Smetan, RatsKeller, «Креп Де Шин café & bar», «Креп Де Шин», «Паштет», «Хмели Сунели».

Одним из методов получения данных о ресторанах является парсинг, который предполагает автоматизированный сбор и структурирование информации с сайтов при помощи программы или сервиса. Задачей такой программы-парсера является сбор информации в соответствии с заданными параметрами. Эта методика основывается на преобразовании неструктурированных данных в сети Интернет в структурированные данные, такие как базы данных или электронные таблицы. Разработка парсера подразумевает написание скрипта, используемого для автоматического сбора информации со страниц сайта и предостав-

ление ее пользователю в структурированном виде. Парсинг сайта включает в себя доступ к сети Интернет напрямую через протокол HTTP или через веб-браузер.

Среди имеющихся на данный момент средств извлечения данных с веб-ресурсов рассмотрим два наиболее близких конкурентных решения — программу для парсинга различных сайтов Datacol и сервис сбора и агрегации отзывов Mneniya.pro. Парсер Datacol работает с регулярными выражениями и с XPath-запросами, имеет настройки для парсинга большого количества площадок. Интерфейс программы позволяет пользователю самостоятельно настроить парсер. Однако для вышеуказанных целей данный продукт обладает такими недостатками, как закрытый исходный код, ручная настройка парсера и ограниченность бесплатной версии.

Сервис Mneniya.pro также является платным, не имеет открытого исходного кода и ориентирован на вывод отзывов на сайт клиента. Большинство аналогичных решений — парсеры с графическим интерфейсом, являющиеся отдельным продуктом, в нашем же случае необходимо решение для легкого включения в более сложные системы, без лишнего функционала. Разрабатываемая система должна иметь бóльшую гибкость при включении в системы интеллектуального анализа и открытый исходный код, доступный для модификации и расширения.

Результаты исследования. Для получения информации с сайта ресторана «Троекуровъ» необходимо создать подключение по ссылке¹. На запрос браузера сервер выдает ответ с кодом состояния, помогающим понять результат запроса. Успешная загрузка страницы HTTP-ответ определяется получением в HTTP-ответе кода 200, однако на данном этапе есть вероятность получения в HTTP-ответе кода с ошибкой. После успешного подключения к сайту начинается выгрузка кода страницы в программу, при этом алгоритм не сохраняет весь код, а лишь необходимые части. Алгоритм в первую очередь создает карточки блюд, в которых хранится название, цена, а также ссылка на отдельную страницу блюда. После чего полученный лист карт отправляется в модуль парсинга характеристик (array_sd,array_tn). В нем по заранее определенным характеристикам происходит отбор блюд для последующего анализа.

Выгрузка данных происходит одновременно с получением информации со страницы, при получении данных о первом блюде, они сразу заносятся в таблицу Excel.

¹ Ковалёв М. Ю. Меню Троекуров. URL: <https://troekurov.ru/catalog> (дата обращения: 10.05.2023).

Общая схема алгоритма работы системы мониторинга меню ресторанов

Шаг 1. Подключение к объекту парсинга.

Шаг 2. Фильтрация исходного кода по шаблону *lxml*.

Шаг 3. Поиск необходимых данных в исходном коде.

Шаг 4. Извлечение данных с отделением от исходного кода.

Шаг 5. Получение значений отделенных элементов.

Шаг 6. Формирование отчета согласно требованиям.

Шаг 7. Визуализация для пользователя.

Шаг 8. Конец алгоритма.

В качестве инструмента для разработки выбраны два языка Python и C#. Python как язык программирования общего назначения с открытым исходным кодом хорошо подходит для работы с большими данными. Не менее важным аспектом выбора является наличие большого количества подключаемых библиотек для работы с веб-ресурсами [1]. В данной системе для реализации пользовательского интерфейса используется C#. Он удобен при построении пользовательских программ благодаря расширению Windows Forms [3].

Реализация HTTP-запросов. Подключение к сайту происходит при помощи библиотеки *Requests*. Для ее использования необходимо указать параметры подключения (headers).

При помощи библиотеки *Beautiful Soup* полученный код страницы обрабатывается и редактируется по шаблону *LMXL*. Без использования данной библиотеки полученный код запроса будет иметь вид обычного текста, что в свою очередь замедлит работу программы.

Для получения информации по всем блюдам использован Кард-лист, массив категорий блюд, с названием и ссылкой на отдельную страницу списка блюд. Чаще всего товары сгруппированы в одном элементе страницы, что позволяет работать лишь с одним элементом, без необходимости поиска по всему коду страницы.

Схема алгоритма представлена на рис. 1.

После получения массива категорий блюд программа методом перебора получает параметры каждого блюда, последовательно переходя по каждой ссылке на блюдо.

При работе с отдельной страницей методом поиска выбраны повторяющиеся элементы кода, хранящие в себе характеристику, вследствие чего обрабатывается не весь код, а лишь нужные элементы. В этом помогает функция *find* или ее вариация *Find_all*.

Блок схема алгоритма представлена на рис. 2.

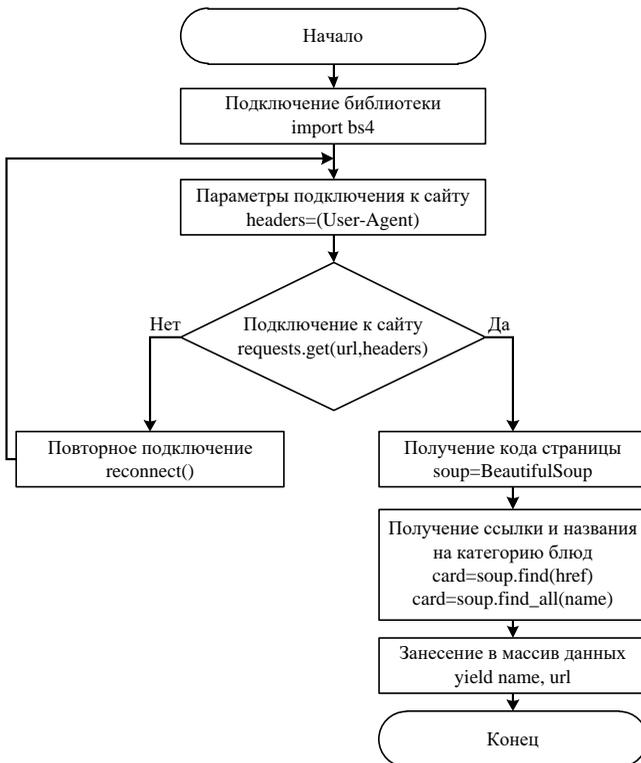


Рис. 1. Получение списка категорий блюд

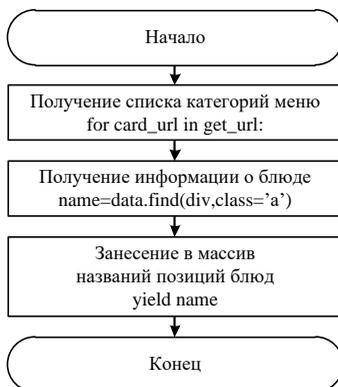


Рис. 2. Получение параметров блюда

Для работы с файлами типа *xlsx* используется библиотека *xlsxwriter*. При вызове алгоритма записи происходит подключение к файлу данного типа. Формирование оглавления столбцов и занесение данных происходит с помощью функции *write*.

Блок-схема данного алгоритма представлена на рис. 3.

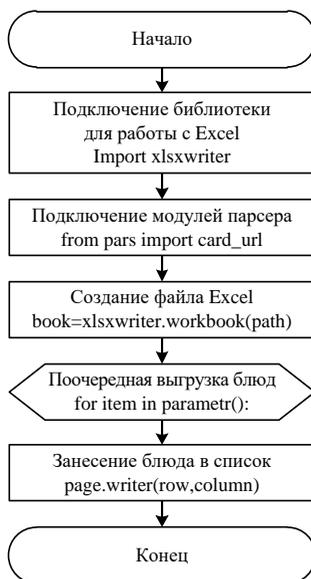


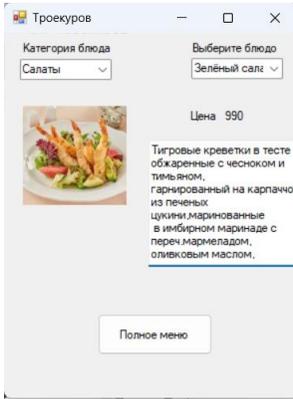
Рис. 3. Занесение данных в таблицу

При запуске исполняемого файла открывается окно программы, в котором пользователь может просмотреть все меню ресторана с актуальными ценами.

Для отображения изображений блюд используется элемент *listimage*, подключенный к файлу *Excel*, в котором они хранятся. При отображении данные уже отсортированы, пользователь может выбрать интересующую его категорию и блюдо. С помощью элемента *textbox* отображается состав блюда.

Скриншот работы программы представлен на рис. 4а. Анализ данных осуществляется в созданном файле *Excel* (рис. 4б).

Результат анализа данных в виде построенных графиков по двум категориям блюд (салаты и супы) представлен на рис. 5.



а

1	2	3	4
фото	название	Описание	цена
	Салаты Зелёный салат с тигровыми креветками и грибами-фунгоми	Тигровые креветки в тесте обжаренные с чесноком и тимьяном, гарнированные на карпаччо из печёных цуккини, маринованные в имбирном маринаде с перцем мармеладом, оливковым маслом, сервируются дольками грибов-фунгоми, обжаренные брокколи и авокадо, дополненный классическим салатом.	990
	Краб с овощами и соусом из черной карри	Камчатский краб с овощами: авокадо, томаты чери и мюслиевые горошины, сервируются на соусе из черной карри, украшается акурными овощными	890
	Салат из свежего тушица и овощей	Овощной салат с тушицом татаки. Состав: фасоль струч, черри, вареный картофель, перепрынутое яйцо, болгарский перец, листья салата, лук красный, сабаудж, катерси, маслина.	890
	Салат запеканка по семейному рецепту шеф-повара	Яйцо белок, масса м.с, лук, морковь, майонез, сыр голландский, слив масло, яйцо белок, майонез, желток.	890

б

Рис. 4. Отображение меню (а) и хранилище данных в файле Excel (б)

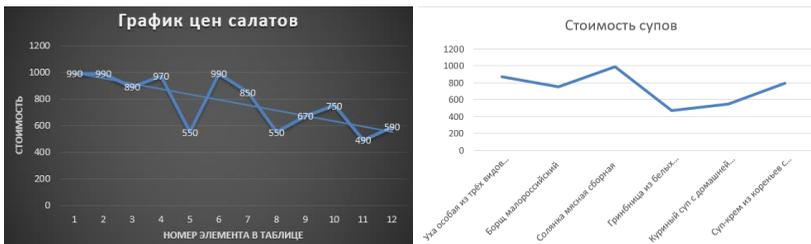


Рис. 5. Анализ стоимости двух категорий блюд

Полученная таблица отображает полный перечень категорий и блюд ресторана, с возможностью просмотра фотографий блюда. Как видно из графиков на рис. 5, средняя стоимость салата варьируется от 700 до 800 р., средняя стоимость супов находится в этом же диапазоне.

Закключение. В исследовании на основе методов интеллектуального анализа данных разработан алгоритм и осуществлена реализация парсинга интернет-ресурсов с данными о меню ресторана, выполнено проектирование и разработка пользовательского интерфейса программы мониторинга меню ресторана, создано приложение на статически типизированном объектно-ориентированном языке C#. При этом реализована возможность легко модифицировать систему, например, при добавлении новых площадок для парсинга, изменении наборов извлекаемых данных и других опций, поскольку данная разработка ориентирована на включение в системы анализа данных.

Дальнейшая разработка системы возможна за счет расширения новыми данными из перечня филиалов сети ресторанов, добавления возможности учета истории динамики цен блюд, создания возможности сохранения файла с выходными данными в текстовом формате и реализации других функций.

Библиографический список

1. Башарина О. Ю., Баландин М. А., Шильникова И. С. Анализ рынка заказной веб-разработки в Рунете инструментальными средствами BI-платформ // Международный журнал прикладных наук и технологий Integral. 2023. № 5. С. 1484–1495.
2. Буценко Е. В. Технология мониторинга объектов недвижимости на основе парсинга данных // Наукосфера. 2024. № 1-2. С. 263–270.
3. Лотка Р. C# и CSLA .NET Framework. Разработка бизнес-объектов. М.: Вильямс, 2010. 816 с.

А. В. Горев, Н. В. Тонких

Уральский государственный экономический университет, г. Екатеринбург

Smart-технологии управления «гибридным» персоналом

Аннотация. В статье исследуются smart-технологии управления «гибридным» персоналом, включающим как удаленных, так и офисных сотрудников. Обсуждаются возможности и преимущества применения таких технологий, как искусственный интеллект, машинное обучение, облачные решения и Интернет вещей (IoT), для повышения эффективности и продуктивности сотрудников. Особое внимание уделяется инструментам для организации работы команд, управления проектами, мониторинга производительности и обеспечения кибербезопасности. Описаны примеры успешной интеграции smart-технологий в процессы управления персоналом в различных организациях. Представлены рекомендации по внедрению и адаптации smart-технологий для создания эффективной и адаптивной гибридной рабочей среды.

Ключевые слова: smart; цифровое управление; цифровизация; гибридный график; удаленная работа; умные технологии; управление персоналом.

Актуальность цифровизации управления персоналом обусловлена не только широким распространением IT-технологий, но и глобальными изменениями в организации труда, вызванными пандемией COVID-19. В 2020 г. наблюдался скачок роста дистанционной занятости в связи с введением ограничительных мер по распространению вируса. Ранее в России нормативное поле применения удаленной формы занятости не было проработано. Реальность потребовала внесения изменений и поправок в Трудовой кодекс РФ, в результате введен в действие Федеральный закон № 407-ФЗ. Опыт экстренного перехода на дистанционную работу выявил как плюсы, так и минусы удаленного формата. В текущее

время все более популярной становится гибридная форма, вытесняя удаленную практику [2].

Гибридная организация труда представляет собой комбинацию удаленной и офисной формы, нивелирует минусы «дистанта», предоставляя сотрудникам возможность гибко управлять своим временем и местом работы. Эксперты отмечают сохранение тренда распространения гибридной формы занятости, который, очевидно, будет доминировать в компаниях в ближайшие годы. Данный тренд становится все более значимым в условиях глобальной цифровой трансформации.

Эффективное управление гибридной формой работы требует инновационных подходов, разработки и внедрения smart-технологий управления персоналом на базе цифровых решений. Идея состоит в замене стандартных методов управления рабочим временем сотрудника на управление результатом, что предполагает адаптацию и внедрение в менеджмент методологии «управления по целям» под конкретные организационные условия. Нужны smart-решения, позволяющие разбить рабочую неделю сотрудника на задачи. При этом важно учесть индивидуальные особенности членов команды, следует выделять задачи, которые обычно лучше всего подходят для конкретного специалиста (например, встречи, обучающие мероприятия или наставничество в рабочие дни), и те, которые лучше всего подходят индивидуально, например чтение, письмо или заниматься программированием дома.

Эффективная организация командной работы сотрудников, часть которых выполняет работу удаленно, а другая — в офисе, возможна с помощью современных цифровых smart-технологий. Данные инновации позволяют автоматизировать рутинные процессы, что способствует эффективному взаимодействию и повышению производительности, что в свою очередь приведет к повышению продуктивности и снижению издержек, данным технологиям присуждена высокая степень внутренней самоорганизации [1; 3].

Современные технологии помогают существенно упростить коммуникацию в гибридной среде, к ним относятся такие smart-технологии, как мессенджеры, видеоконференции и другие платформы для совместной работы. С помощью таких технологий обеспечивается возможность эффективного взаимодействия между сотрудниками, примерами могут быть обмен идеями, проведение видеовстреч и совещаний, независимо от того, в какой локации находится сотрудник.

В контексте цифровизации труда данные технологии могут предоставить ряд преимуществ.

1. Улучшение доступа к информации.

Умные технологии, независимо от того, работает сотрудник удаленно/гибридно или в офисе, предоставляют быстрый и удобный доступ

к необходимым данным. Работать с файлами и документами стало проще, с помощью таких решений, как облачное хранилище данных, электронные документы и системы управления проектами, обмен информацией стал быстрее и эффективнее.

2. Мониторинг и управление производительностью.

Современные технологии Smart предоставляют руководителям инструменты, с помощью которых можно мониторить производительность труда удаленных сотрудников. IT-сервисы позволяют отслеживать количественные параметры времени работы, проводить анализ активности на корпоративных порталах и использование систем управления проектами и задачами. Данные технологии помогают руководству оценивать производительность работы персонала и принимать соответствующие меры для повышения эффективности работы.

3. Онлайн-доступность коммуникаций.

Инструменты видеоконференций обеспечивают проведение онлайн-встреч для сотрудников с удаленным участием. Данные сервисы позволяют проводить виртуальные встречи в реальном времени независимо от того, где находится работник и какое у него местоположение. С помощью виртуальных пространств сотрудники могут проводить совещания, обсуждать стратегии, обмениваться идеями и решать поставленных задачи в команде, не выходя из своих рабочих кабинетов или удаленных офисов, что сокращает время на принятие решений и выполнения поставленных задач.

При всех своих преимуществах необходимо разумно подходить к выбору smart-технологий, которые помогают осуществлять управление гибридной формой занятости. В таблице представлены примеры плюсов и минусов наиболее распространенных цифровых решений и сервисов, как за рубежом, так и в России, для взаимодействия и управления рабочим процессом.

Примеры цифровых и сервисных решений при управлении удаленными и гибридными формами работы

Решение	Описание	Преимущества	Недостатки
Инструменты для совместной работы: Slack, MyOffice, «Сбер-Бизнес»	Обеспечивают общение, обмен файлами и видеоконференции для удаленных сотрудников	Повышение продуктивности, улучшение командной работы, снижение расходов на офис	Может потребоваться обучение, некоторые сотрудники могут предпочитать личное общение
Инструменты управления задачами: Asana, Trello, Jira, GanttPRO	Помогают в постановке задач, отслеживании прогресса и совместной работе над проектами	Повышение организации, улучшение контроля за рабочим процессом, стимулирование подотчетности	Может привести к чрезмерному контролю, некоторые сотрудники могут предпочитать более гибкий подход к работе

Окончание таблицы

Решение	Описание	Преимущества	Недостатки
Облачные хранилища: Dropbox, Google Drive, Vox, «Яндекс.Диск», «Mail облако»	Обеспечивают доступ к файлам с любого устройства	Повышение доступности и совместной работы, снижение зависимости от локальных хранилищ	Может потребоваться большое количество места для хранения, некоторые сотрудники могут иметь проблемы с конфиденциальностью
Инструменты видеоконференций: Zoom, Google Meet, ВКС «Контур.Толк»	Дают доступ к проведению видеовстреч с удаленными сотрудниками, клиентами и партнерами	Улучшение работы в команде в дистанционном формате, сокращение деловых поездок	Может потребоваться высокоскоростное подключение к Интернету, некоторые сотрудники могут испытывать трудности при работе с приложением

Стоит отметить, что использование smart-технологий при управлении гибридной/удаленной занятостью приносят организациям дополнительные бонусы, которые выражаются в увеличении продуктивности, согласованности командной работы и сокращением расходов. Основным преимуществом гибридной организации труда является, в первую очередь, гибкость рабочего времени и места работы, что так привлекает сотрудников. Согласно последним исследованиям, не менее 25 % сотрудников проявляет интерес к переходу с очного формата работы на гибридный. Респонденты часто отмечают следующие улучшения в гибридном графике: повышение гармонии между работой и семьей, планирование самостоятельно рабочего дня, делая перерывы и работая в часы, когда сотрудник наиболее продуктивен. Немаловажным преимуществом частичной работы из дома является сокращение времени на дорогу до офиса и обратно, что приводит к значительной экономии личного времени у сотрудников, которые проживают далеко от офиса. Сокращение «транспортного» времени снижает усталость и положительно отражается на доходах персонала: работники в гибридном или полностью удаленном формате экономят значительное количество средств на бензине, общественном транспорте и парковке.

Однако необходимо учитывать, что каждая технология имеет свои достоинства и недостатки и требует дополнительной адаптации со стороны сотрудников. Эффективное внедрение и использование таких инструментов необходимо для успешного преодоления новых вызовов в области занятости и эффективного управления рабочими процессами в современной бизнес-среде.

Одним из полезных инструментов в smart-технологиях может быть использование виртуальных помощников для управления зада-

чами в гибридной форме работы. Для интегрирования приложения в рабочие процессы необходимо выполнить ряд этапов.

В первую очередь важно выбрать подходящего виртуального помощника для управления задачами. Это может быть система управления задачами, интегрированная в электронную почту или мессенджер, или специализированное программное обеспечение для управления проектами. После выбора подходящего помощника необходимо перейти к внедрению его в компанию, что включает установку и настройку приложения, регистрацию участников (сотрудников) и их обучение.

На этапе обучения сотрудников пользованию виртуального помощника для управления задачами, возможно, потребуются проведение тренингов, создания инструкций и руководств по использованию приложения. Данный этап является ответственным в компании.

После проведения обучения необходимо перейти к этапу интегрирования виртуального помощника в рабочие процессы компании, что включает в себя определение этих процессов управления задачами, установление правил и стандартов использования программного обеспечения, настройку для совместного использования с коллегами.

После этапа интегрирования важно оценить эффективность и влияние внедрения виртуального помощника на производительность и эффективность работы сотрудников. Оценка результативности выполняется с помощью анализа статистических данных о выполненных задачах, времени, затраченном на выполнение задач, и уровне удовлетворенности сотрудников использованием приложения.

В заключение хочется отметить, что умные технологии играют ключевую роль в управлении гибридной формой занятости, делая ее более эффективной и удобной для всех участников. Они обеспечивают улучшение коммуникации, повышают доступность к информации и возможность мониторинга производительности персонала в организации. Внедрение smart-технологий в рабочие процессы помогает компании адаптироваться к современным требованиям быстро меняющегося мира и успешно управлять гибридной формой работы.

Библиографический список

1. *Макаркин Д. А.* Преимущества Smart-технологий // Теория и практика современной науки. 2017. № 8 (26). С. 142–144.
2. *Никольский Я. А.* Практика и перспективы удаленного и гибридного форматов работы в современных компаниях // Ученые записки Российской академии предпринимательства. 2024. Т. 23, № 1. С. 93–101.
3. *Симонова М. М.* Поведение сотрудников организации в условиях гибридной формы работы // Аудиторские ведомости. 2024. № 1. С. 173–176.

А. Д. Гордилова

Уральский государственный экономический университет, г. Екатеринбург

Влияние цифровизации на жизнь пожилых людей

Аннотация. В статье рассматривается влияние цифровизации на жизнь пожилых людей, исследуются как положительные аспекты, так и возникающие проблемы. С развитием цифровых технологий пожилые люди сталкиваются с новыми возможностями и вызовами. Особое внимание уделено барьерам, с которыми сталкиваются пожилые люди при освоении новых технологий: недостаток цифровой грамотности, сложности в использовании современных устройств и программного обеспечения, а также риски, связанные с кибербезопасностью. В статье также представлены примеры успешных программ и инициатив, направленных на преодоление этих барьеров и повышение цифровой включенности пожилых людей. В заключение приводятся рекомендации для разработчиков технологий, социальных служб и политиков по созданию более доступной и поддерживающей цифровой среды для старшего поколения.

Ключевые слова: информационные технологии; старшее поколение; цифровизация; цифровая среда; пожилые люди; безопасность.

Одной из актуальных проблем прогрессивного мира в области информационных технологий является тема адаптации в цифровой среде старшего поколения. По причине слишком резких скачков с открытием Интернета, позволяющим с каждым днем внедрять больше сайтов, IT-ресурсов и прочего, старшее поколение, что редко заинтересовано по сравнению с молодыми людьми следить за последними новинками и трендами, все больше сталкивается с непониманием из-за интеграций цифровых решений практически во все сферы нашей жизни. Отсутствие компетенций в данной сфере делает пожилых людей легкими жертвами мошенников, больше проблема напомнила о себе во время пандемии, когда число случаев телефонных и киберпреступлений в стране возросло в 1,5 раза¹.

Дальнейшая цифровая трансформация, вместе с множеством возможностей и плюсов, неизбежно несет риски, снижение которых возможно избежать только в случае внедрения комплексной системы мер цифровой безопасности при доработке всей существующей законодательной базы [1].

Нынешние реалии требуют повышенного навыка владения компьютером и Интернетом для свободы доступа к любой информации, большого выбора от продуктов до других специальных товаров, возмож-

¹ *Ликбез для дедушки: как повысить цифровую грамотность пожилых людей / РБК.*
URL: <https://trends.rbc.ru/trends/education/622b8a749a79470543ba9a8d> (дата обращения: 09.05.2024).

ность дистанционно оплачивать связь и коммунальные услуги, записываться на прием к врачу, общаться с близкими и т. д.

К сожалению, от людей пожилого возраста, которые пытаются получить информацию или услугу привычным для них путем, могут отмахнуться, предложив воспользоваться помощью детей и родственников или самим ориентироваться на сайте. В итоге использование услуг, не вписывающихся в привычное понимание человека взаимодействия с миром и не учитывающих его особенности, усугубляет отреченность от цифрового мира.

К препятствиям на пути вовлечения пожилых людей в цифровое пространство также является высокая стоимость оборудования, отсутствие поддержки во время учебного процесса со стороны родных, слишком большие и быстрые инструкции и сложность пользовательского интерфейса [2].

На цифровой разрыв между поколениями немало влияют ситуации на работе, когда руководители отдают предпочтение в обучении новым программам или использованию современного оборудования молодым сотрудникам и реже заинтересованы в обучении работников предпенсионного возраста. Опросы показывают: владение цифровыми навыками в профессиональной деятельности у лиц старше 50 лет почти в два раза ниже, чем у более молодых сотрудников¹. Отстранение пожилых людей от цифровизации будет снижать их мотивацию на обучение цифровой грамотности.

Ловушки для людей, не имеющих навыков коммуникации в сети, тоже играют не маловажную роль. Приемы мошенничества и обмана увеличиваются по мере того, как больше пожилых людей приобщается к цифровому миру. Из-за ограниченной способности пользователей старшего возраста распознавать информацию и недостаточных возможностей выявлять онлайн-слухи и фейки, а также адекватно реагировать на них, пожилые люди легко становятся объектом манипуляций [3].

Для простого и легкого использования всех благ, которые предоставляет Интернет, а также для возможности оставаться уверенным в защищенности своих данных пожилому человеку необходимо освоить базовые принципы использования гаджета и умения адаптироваться в сети.

Простая регистрация в социальных сетях или на портале «Госуслуги» требует создания учетной записи, нередко при создании необ-

¹ *Социологи* СПбГУ: около 50 % пожилых людей не владеют электронными поисковыми сервисами // СПбГУ. 2022. 11 марта. URL: <https://spbu.ru/news-events/novosti/sociologi-spbgu-okolo-50-pozhilykh-lyudey-ne-vladeyut-elektronnyimi-poiskovymi> (дата обращения: 09.05.2024).

ходимо вместо телефона указать электронную почту, для двухфазной проверки на почту могут прислать код для подтверждения входа и т. д. Несложные манипуляции, которых не существовало в таком избытке несколько лет назад, заставляют теряться, запоминать множество паролей, что может быстро утомить человека любого возраста.

Большинство компаний уже сейчас разрабатывают решения для повышения использования старшего поколения их интернет-ресурса. Например, компания «Энергосбыт» выдает специальные брошюры для пенсионеров и неопытных пользователей с инструкцией оплаты услуг и регистрации на своем портале. Сейчас на множестве рекламных баннеров и листовках можно встретить предупреждение о киберпреступниках с убедительной просьбой не предоставлять информацию о счетах и прочую конфиденциальную информацию.

С целью помочь пенсионерам адаптироваться в цифровой среде, благотворительный фонд «Менора» разработал проект на тему «Методы дистанционной работы с пожилыми», в котором учувствовали специалисты социальной защиты из Екатеринбурга, Первоуральска, Верхней Пышмы и Магнитогорска.

Цель проекта заключалась в улучшении качества жизни у пенсионеров с помощью цифровых технологий. В ходе исследования специалисты обнаружили, что люди от 70 лет способны успешно осваиваться в цифровой среде в группе сверстников, начинающих, как и они, с нуля. Также в своей статье они отметили благоприятное влияние на проекте сверстников, уже освоившихся в цифровой культуре и на своем примере доказавших успешность семинара.

По окончании проекта больше половины участников не хуже молодых используют Интернет для информирования и личных целях, ведут активную жизнь в социальных сетях, следят за новостями. Многие пенсионеры научились самостоятельно оплачивать коммунальные услуги через Интернет, скачивать любимую музыку, фильмы и прочий развлекательный контент. Сейчас участники проекта развиваются в цифровой среде самостоятельно, без помощи родственников или волонтеров¹.

Введение районных программ социальной и цифровой грамотности поможет решить проблему как для пенсионеров, так для других неуверенных пользователей. Подобного рода образовательный процесс должен базироваться не только на личных прихотях каждого участника,

¹ *Цифровые технологии: повысить качество жизни пожилых! /* Общественная палата Свердловской области. 2022. 1 нояб. URL: <https://www.opsob66.ru/na-povestkednya/novosti-nko/2785-tsifrovye-tehnologii-povysit-kachestvo-zhizni-pozhilykh.html> (дата обращения: 09.05.2024).

но и индивидуальных возможностей. Это позволит обеспечить ключевые принципы образования: гибкость, вариативность, адаптивность и технологичность [4].

Программа может представлять из себя небольшой курс с экзаменом в конце во избежание недостаточно ответственного подхода к изучению цифровой среды. На языке старшего поколения психологически комфортнее будет воспринимать курс от человека, близкого по возрасту, который разбирается в соответствующей теме. На курс должен иметь возможность записаться любой желающий бесплатно, потому что каждый пенсионер должен иметь возможность владеть базовыми знаниями взаимодействия с гаджетом и Интернетом так же, как и ребенок имеет право на бесплатное образование. В курс обязательно должно входить знакомство с самыми важными приложениями, такими как онлайн-банк, гос. услуги, интернет-магазин и социальная сеть.

Тема безопасности, умение распознавать злоумышленников и соблюдение этики в Интернете не менее важная часть, которая может быть уместна на курсе. Поскольку курс должен быть бесплатным, его содержанием может заниматься либо государство, либо компании, заинтересованные в популяризации своего интернет-ресурса среди пенсионеров, например, компании с доставкой продуктов на дом.

В интернет-ресурсе «Бибосс», разрабатывающем бизнес-идеи, существует статья с похожим предложением, заключающаяся в найме персональных тренеров для пенсионеров. Они выделили ряд недостатков, которые одинаково актуальны для небольшого курса для всех желающих пенсионеров и неуверенных пользователей:

- большая разница в уровне начальных знаний, вынуждающая приспосабливаться к различным потребностям, разработав индивидуальные программы обучения;

- недостаточная осведомленность о наличии таких услуг требует дополнительные усилия по просвещению и привлечению внимания пожилых людей к услуге;

- физические ограничения могут затруднить использование определенных цифровых устройств. Необходимо адаптировать обучение и предложить альтернативные способы использования технологий, учитывая физические возможности каждого клиента¹.

Можно сделать вывод, что реализация бесплатного курса цифровой грамотности для пенсионеров имеет очевидные сложности, но на каждую проблему уже существуют способы решения, так как программа

¹ *Бизнес-идея: Персональные тренеры по цифровой грамотности для пожилых людей / Бибосс. 2023. 12 июля. URL: <https://www.beboss.ru/bizideas/6057-personalnye-trenery-po-cifrovoy-gramotnosti-dlya-pozhilyh-lyudey> (дата обращения: 09.05.2024).*

имеет схожесть с любой уже известной формой обучения, как и везде результат во многом зависит от обоюдной заинтересованности.

Видимо, повлиять на успех курсов цифровой грамотности среди пожилых людей, с учетом добросовестного наставника и должной подготовки, может только предание его огласке: упоминания о семинаре в пенсионных фондах, в компаниях, пользующихся постоянным вниманием старшего поколения, в брошюрах или напрямую от социальных работников и пр. — пока каждый человек, в первую очередь пожилого возраста, испытывающий сложность при взаимодействии с цифровой средой, сомневающийся и неуверенный в необходимости посещения курсов, не уверится в актуальности данной проблемы и не прекратит видеть в нововведенной системе обучения ненадежного и нестабильного последователя моды.

Курсы цифровой грамотности являются достаточно трендовой идеей, так как без современной проблемы ее бы не существовало, однако ее актуальность имеет шанс остаться надолго, потому что программа обучения может подстраиваться под изменения в цифровом мире.

Библиографический список

1. *Грохотова Е. В.* Формирование цифровой грамотности людей третьего возраста на основе курса-трансформера // *Номо Cyberus*. 2022. № 2 (13). URL: http://journal.homocyberus.ru/Grokhotova_EV_2_2022 (дата обращения: 09.05.2024).

2. *Даринская Л. А., Молодцова Г. И., Москвичева Н. Л.* Пожилой человек и цифровое пространство: точки соприкосновения // *Человек и образование*. 2016. № 3 (48). С. 151–157.

3. *Синицкая Н. Я.* Развитие цифровой экономики: широкие возможности и возможные риски // *Фундаментальные исследования*. 2023. № 11. С. 95–99.

4. *Чэнь С.* Актуальные проблемы адаптации пожилых людей к новым технологиям коммуникации в цифровую эпоху // *Современная урбанистика: социальное благополучие и цифровая трансформация города: сб. материалов Междунар. науч.-практ. конф. (Минск, 30 ноября 2023 г.)*. Минск: БГУ, 2024. С. 477–480.

Н. С. Кольева, Д. И. Чугайнова

Уральский государственный экономический университет, г. Екатеринбург

Разработка программного комплекса для ведения телефонного справочника предприятия

Аннотация. Цель работы заключается в разработке программного комплекса для ведения телефонного справочника предприятия. Данный программный комплекс предоставляет пользователю возможность для просмотра базы абонентов, редактирования базы и поиска по ней. Программный комплекс «Телефонный справочник» решает следующие задачи: ведение телефонного справочника; заполнение данными; поиск информации. Разработанный программный комплекс преследует следующие цели: снижение трудоемкости поиска данных; удобное хранение телефонных номеров для связи. К программному комплексу предъявляются следующие требования: база данных должна быть способна хранить информацию о более 500 сотрудниках; интерфейс пользователя должен иметь удобную навигацию, простоту в обращении и невысокие программные требования.

Ключевые слова: телефонный справочник; программный комплекс; базы данных 4 Python; библиотека KivyMD.

В процессе работы приложение будет получать сведения для решения своей задачи. Задача телефонного справочника — хранить контактную информацию и давать возможность просмотра всех контактов. Следовательно, входной информацией при создании приложения «Телефонный справочник» являются введенные пользователем номера телефонов и имя пользователя. По окончании работы телефонный справочник должен занести в базу новый номер телефона, иметь возможность его удалить и так же вывести все доступные контакты. Следовательно, выходной информацией является список имеющихся контактов, возможность поиска по имени или телефону.

Создание телефонного справочника будет реализовано в среде программирования Visual Studio Code, для дизайна приложения будет использована библиотека KivyMD.

Идея приложения — приложение состоит из двух экранов. Первый экран для поиска внесенных в базу телефонов, а также удаление из списка контактов. Второй экран же реализует функционал добавления нового номера телефона (или нескольких в одном контакте). Для реализации такого подхода среди готовых компонентов есть MDToolbar. Kivy реализует подход разделения обязанностей. Часть, отвечающая за визуальную структуру приложения Kivy, предлагает вынести в отдельный файл со своим синтаксисом со своими командами, а часть, отвечающую за логику, функциональную начинку оставить в файлах питона, классические классы, функции, методы и т. д. Для того чтобы вынести этот функционал в отдельный файл, используются специальные файлы .kv.

Для того чтобы приложение Kivu автоматически находило этот файл, имя файла должно совпадать с именем класса приложения, за исключением того, что должны быть использованы маленькие буквы [1; 2].

Хранение данных будет происходить в базе данных SQLite, которая встроена в язык Python. Для более удобной работы дополнительно будет использована SQLAlchemy, которая является ORM и позволяет работать с базой данных с классами и объектами. То есть таблица в базе данных описывается в виде класса и соответственно строки в таблице являются объектами из этого класса. Для того чтобы описать весь функционал, который будет отвечать за взаимодействие с базой данных создаем отдельный модуль `models.py`. Здесь будет источник данных, который будет получать данные, сохранять и выполнять поиск. Импортируем необходимые компоненты. Главная задача — получить объект сессии, с которым в дальнейшем идет работа, указать файл хранения. Таблицы, в которых мы будем хранить данный необходимо описать в виде классов. Таблица будет наследоваться от класса `Base`, в строке `tablename` указываем, с каким именем будет создана таблица в базе данных. Создаем поле `id`, которое является первичным ключом, поле `name`, где будет храниться имя контакта типа `string`, и вспомогательное поле `relationship`, которое позволит «ходить» по связям с другой таблицей, в которой будут храниться телефонные номера [3].

Чтобы кнопки и строки поиска не накладывались друг на друга, нужно создать еще один `MDBoxLayout`, который будет содержать их в себе. Он будет располагаться на первой навигационной странице, в нем элементы должны располагаться вертикально, один под другим.

Под блоком поиска контактов и поиска телефонов должен располагаться блок с результатами поиска. Для этого подходит элемент `TwoLineAvatarIconListItem` — список, в котором каждая строчка списка содержит аватар, текст, состоящий из двух строк и иконку удаления элемента списка. Вставляем `ScrollView`, внутри которого будет содержаться `MDList`, внутри которого будут отображаться элементы поиска.

Рассмотрим реализацию функционала программного комплекса. Необходимо к кнопкам поиска добавить обработчики. Каждая кнопка при нажатии может генерировать ряд событий. Нас интересует событие «Отпустить кнопку» т. е. в момент, когда кнопка отпускается, будет произведен запуск. Это событие называется `on_release`, в событии описываем, что оно должно делать при отпускании кнопки. Здесь будет ссылка на обработчик, который будет выполнять код. В файле `main.py`, в классе `PhoneBookApp`, нужно создать метод обработчика нажатия на кнопку поиска по имени [4; 5].

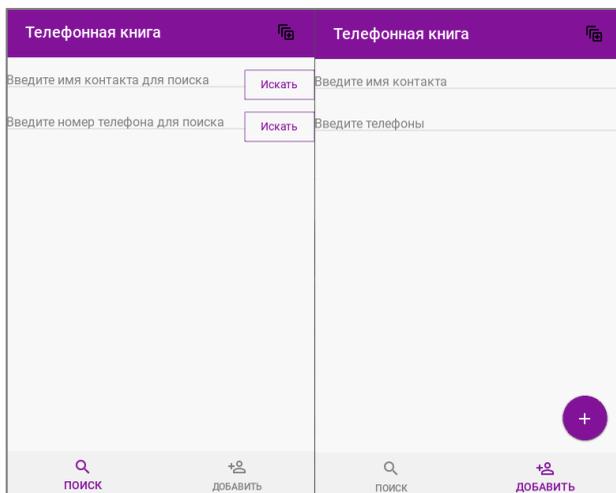
Для того чтобы в дальнейшем получить результаты поиска, будем использовать специальный виджет. Он представляет из себя элемент

с двумя строчками, первая строчка — имена, вторая строчка — телефоны. При этом в базе данных все это хранится в связанной форме, т. е. пользователь будет отдаваться с привязанными телефонами и поэтому нужно преобразовать это так, что отдавались отдельно имена и отдельно телефоны. Для этого подойдет элемент tuple. Список будет отдавать элемент user, которого он его достанет из модели User, с помощью метода find_by_name. Таким образом, на вход мы получим имя. Внутри tuple будут находиться:

- 1) user с атрибутом name;
- 2) phone.

Вторым элементом внутри tuple является список объектов (нам нужна строка). Необходимо это преобразовать. Преобразовываем это следующим образом — сначала создаем список телефонов, который возьмем из объекта user и его атрибута phones. Этим самым мы формируем список, состоящий из телефонов, уже не сложных объектов, а из простых строковых значений. Затем с помощью метода join преобразовываем все это в строку.

На рисунке представлен интерфейс программного комплекса «Телефонный справочник».



Экран приложения

Таким образом, программный комплекс для ведения телефонного справочника предприятия предоставляет пользователю возможность для просмотра базы абонентов, редактирования и поиска по базе. При

разработке проекта была использована база данных, встроенная в язык программирования Python SQLAlchemy и вспомогательная библиотека SQLAlchemy. Разработка самого приложения происходила в среде программирования Visual Studio Code.

Библиографический список

1. *Заика И. В., Кумов Д. О.* Использование SQL-запросов как инструмента для взаимодействия с базами данных // Вестник Таганрогского института имени А. П. Чехова. 2023. № 2. С. 29–34.

2. *Кольева Н. С., Боруцкий Г. И.* Разработка справочника образовательных учреждений в Telegram // Современные тренды высшего образования: коллективная монография / отв. ред. А. Ю. Нагорнова. Ульяновск: Зебра, 2023. С. 565–576.

3. *Новичков К. А., Ляпин А. А.* Автоматизация и повышение эффективности процесса учета сотрудников предприятия в телефонном справочнике // Актуальные проблемы науки и техники: материалы нац. науч.-практ. конф. (Ростов-на-Дону, 25–27 марта 2020 г.). Ростов н/Д: ДГТУ, 2020. С. 838–840.

4. *Чепкая Д. С.* Методика разработки проекта поисковой информационной системы «Телефонный справочник СГУГИТ» // Интерэкспо Гео-Сибирь. 2020. Т. 7, № 1. С. 187–194.

5. *Iklassova K. E., Kozhakhmetova R. N.* Modeling the dynamic semantics of a computer program // Цифровые модели и решения. 2023. Т. 2, № 4. С. 5–12.

Я. В. Малыгин

Уральский государственный экономический университет, г. Екатеринбург

Информатика ЕГЭ: решение заданий на выигрышную стратегию с использованием функции выигрыша

Аннотация. В статье рассматривается вариант программного решения заданий 20 и 21 ЕГЭ по информатике и ИКТ на поиск выигрышной стратегии с использованием функции выигрыша в играх. Приводятся примеры решения таких задач на языке программирования Python в форме, легко воспроизводимой как школьниками при сдаче ЕГЭ, так и студентами, изучающими дисциплины, связанные с рекурсией и динамическим программированием.

Ключевые слова: ЕГЭ; Единый государственный экзамен; информатика и ИКТ; выигрышная стратегия; рекурсия; функция выигрыша; Python.

Поиск выигрышной стратегии для задач 20–21 ЕГЭ по информатике, как правило, выполняется с помощью создания дерева позиций и анализа выигрышной стратегии в узлах этого дерева. Составляется функция выигрыша; первый игрок своими ходами старается увеличить ее значение, а второй игрок — уменьшить. Чтобы избежать повторных вычислений и уменьшить время работы программы, значения функции

выигрыша для уже рассмотренных игровых позиций запоминаются. Однако при решении задач из ЕГЭ не требуется большая глубина анализа. Поэтому можно обойтись обычной рекурсией, без запоминания результатов промежуточных вычислений, что упрощает описание программы и ее понимание.

Предлагаемые при типовом разборе таких заданий программы, на мой взгляд, выглядят излишне громоздко и различаются для заданий 20¹ и 21².

Однако существуют и более интересные алгоритмы, связанные с перебором всех вариантов и учетом текущего и требуемого количества ходов в игре³.

Опишем еще один подход к созданию простой и универсальной (т. е. одной на оба задания 20 и 21) программы для поиска выигрышной стратегии при сильнейшей игре обоих игроков с использованием функции выигрыша.

Как правило, задания 19–21 описывают одну игру, но с различными начальными условиями. Рассмотрим типовой пример с одной кучей камней⁴.

Задание 20

Два игрока, Петя и Ваня, играют в следующую игру. Перед игроками лежит куча камней. Игроки ходят по очереди, первый ход делает Петя. За один ход игрок может: добавить в кучу один камень (действие А) или утроить количество камней в куче, а затем убрать из кучи один камень (действие Б). Например, имея кучу из 10 камней, за один ход можно получить кучу из 11 или 29 камней. У каждого игрока, чтобы делать ходы, есть неограниченное количество камней. Игра завершается в тот момент, когда количество камней в куче становится более 32. Победителем считается игрок, сделавший последний ход, т. е. первым получивший кучу, в которой будет 33 или больше камней. В начальный момент в куче было S камней, $1 \leq S \leq 32$.

Говорят, что игрок имеет выигрышную стратегию, если он может выиграть при любых ходах противника. Описать стратегию игрока — значит описать, какой ход он должен сделать в любой ситуации, которая ему может встретиться при различной игре противника.

¹ *Задания*. Тип 20 № 27417 / ЕГЭ–2024, информатика: задания, ответы, решения. URL: <https://inf-ege.sdangia.ru/problem?id=27417> (дата обращения: 08.04.2024).

² *Задания*. Тип 21 № 27418 / ЕГЭ–2024, информатика: задания, ответы, решения. URL: <https://inf-ege.sdangia.ru/problem?id=27418> (дата обращения: 08.04.2024).

³ *Поляков К.* 19-21. URL: <https://kpolyakov.spb.ru/download/ege1921.doc> (дата обращения: 08.04.2024).

⁴ *Вариант № 12604555 / ЕГЭ–2024*, информатика: задания, ответы, решения. URL: <https://inf-ege.sdangia.ru/test?id=12604555> (дата обращения: 08.04.2024).

Найдите два таких значения S , при которых у Пети есть выигрышная стратегия, причем одновременно выполняются два условия:

- Петя не может выиграть за один ход;
- Петя может выиграть своим вторым ходом независимо от того,

как будет ходить Ваня.

Найденные значения запишите в ответе в порядке возрастания без разделительных знаков.

Задание 21

В условиях предыдущей задачи найдите минимальное значение S , при котором одновременно выполняются два условия:

- у Вани есть выигрышная стратегия, позволяющая ему выиграть первым или вторым ходом при любой игре Пети;
- у Вани нет стратегии, которая позволит ему гарантированно выиграть первым ходом.

Пусть значение функции выигрыша будет положительным, если данный игрок выиграл, и отрицательным в случае победы противника. Для дальнейшего конструирования функции выигрыша, которую каждый игрок стремится увеличить, переформулируем цели игроков: каждый стремится к своей победе за наименьшее число ходов n , а если это невозможно, то старается как можно сильнее продлить партию. Такая формулировка не влияет на итоговое решение задачи, но теперь выигрышная стратегия и понятие сильнейших ходов будет не только у игрока, который побеждает, но у проигравшего, цель которого теперь также увеличить свою «функцию выигрыша». Таким образом, зависимость функции выигрыша $f(n)$ от продолжительности партии должна быть следующей: при победе данного игрока функция положительна и с ростом n должна уменьшаться, а при победе противника — отрицательна и с ростом n должна увеличиваться (т. е. уменьшаться по модулю).

В качестве функции выигрыша, удовлетворяющей обоим этим условиям, была выбрана $f(n) = \pm 1/n$, где числитель равен 1 или -1 в зависимости от того, кто побеждает, сам игрок или его противник, а знаменатель n — количество полуходов в данной партии. Такую функцию выигрыша каждый игрок своим ходом стремится увеличить.

Составим таблицу значений функции выигрыша для Пети (первого игрока) для первых восьми полуходов (см. таблицу).

Значения функции выигрыша для первого игрока

Кто и на каком ходу победил	Номер полухода n	Функция выигрыша $f(n)$
Петя на своем 1-м ходу	1	1,0
Ваня на своем 1-м ходу	2	-0,5
Петя на своем 2-м ходу	3	0,333333...
Ваня на своем 2-м ходу	4	-0,25

Окончание таблицы

Кто и на каком ходу победил	Номер полухода n	Функция выигрыша $f(n)$
Петя на своем 3-м ходу	5	0,2
Ваня на своем 3-м ходу	6	-0,166666...
Петя на своем 4-м ходу	7	0,1428571...
Ваня на своем 4-м ходу	8	-0,125

Вычисление функции выигрыша удобнее производить лишь на следующем полуходе, т. е. оценивать с точки зрения противника, а значит, с противоположным знаком. Из этого следует, что наилучший для игрока оказывается ход, для которого значение функции выигрыша с точки зрения противника наименьшее. Вычисление функции выигрыша указано в следующей формуле:

$$f(s, n) = -\min(f(s_1, n+1), f(s_2, n+1), \dots),$$

где s — текущая позиция игры (количество камней); s_1, s_2 и т. д. — позиции, которые игрок своим ходом может достичь из текущей; n — номер полухода.

В динамическом программировании такая формула называется уравнением Беллмана¹. Составим программу на языке Python (рис. 1).

```
#s-количество камней в куче, n - номер полухода
def hod(s,n):
    #если игра закончилась, то победил противник
    # (знак отрицательный) на предыдущем полуходе (n-1)
    if s>=33: return -1/(n-1)
    #рекурсивное вычисление функции выигрыша с учетом
    #возможности добавить в кучу один камень или утроеить
    #количество камней и вычесть один камень.
    return -min(hod(s+1,n+1),hod(3*s-1,n+1))

#Вывод значений функции выигрыша для различного начального
#количества камней в куче от 1 до 33
for s0 in range(1,33): print(s0,hod(s0,1))
```

Рис. 1. Текст программы для типового примера

Предложенная программа, состоящая всего из четырех строк (не считая комментариев), выдает следующий результат (рис. 2).

В соответствии с этим результатом при начальном количестве камней в куче от 12 до 32 камней выигрывает Петя на своем 1-м ходу (значение функции выигрыша равно 1). Если $S = 11$, то выигрывает Ваня на

¹ *Бабичев С. Л.* Лекции по алгоритмам и структурам данных: учеб. пособие. М.: МАКС Пресс, 2019. 344 с.

своём первом ходу (значение функции выигрыша равно $-0,5$) и т. д. в соответствии с таблицей.

1	-0.125	12	1.0	23	1.0
2	0.14285714285714285	13	1.0	24	1.0
3	-0.16666666666666666	14	1.0	25	1.0
4	0.3333333333333333	15	1.0	26	1.0
5	-0.125	16	1.0	27	1.0
6	0.14285714285714285	17	1.0	28	1.0
7	-0.16666666666666666	18	1.0	29	1.0
8	0.2	19	1.0	30	1.0
9	-0.25	20	1.0	31	1.0
10	0.3333333333333333	21	1.0	32	1.0
11	-0.5	22	1.0		

Рис. 2. Результат работы программы из рис. 1

В задании 20 необходимо определить два начальных значения S , при которых Петя гарантированно выигрывает на своём втором ходу, т. е. $n = 3$, а значение функции выигрыша должно быть $1/3 = 0,3333333\dots$ в соответствии с таблицей. Из результатов работы программы видно, что такое значение достигается при $S = 4$ и $S = 10$.

В задании 21 необходимо определить минимальное начальное значение камней в куче, при котором Ваня гарантированно выигрывает на своём втором ходу, т. е. $n = 4$, $f(n) = -0,25$. Из результатов работы программы определяем, что минимальное (и оно же единственное) $S = 9$.

Рассмотрим ещё один пример, где возможность сделать ход зависит от количества камней в обеих кучах (СТАТГРАД, вариант ИН2210301 от 14.02.2023):

Задание 20

Два игрока, Петя и Ваня, играют в следующую игру. Перед игроками лежат две кучи камней. Игроки ходят по очереди, первый ход делает Петя. За один ход игрок может добавить в меньшую кучу любое количество камней от одного до количества камней в этой куче. Изменять количество камней в большей куче не разрешается. Если кучи содержат равное количество камней, добавлять камни можно в любую из них. Пусть, например, в начале игры в первой куче 3 камня, а во второй — 5 камней, будем обозначать такую позицию $(3, 5)$. Петя первым ходом должен добавить в первую кучу от 1 до 3 камней, он может получить позиции $(4, 5)$, $(5, 5)$ и $(6, 5)$. Если Петя создаёт позицию $(4, 5)$, то Ваня своим ходом может добавить от 1 до 4 камней в первую кучу, а если Петя создаёт позицию $(6, 5)$, то Ваня может добавить от 1 до 5 камней во вторую кучу, так как теперь она стала меньшей. В позиции $(5, 5)$ Ваня может добавить от 1 до 5 камней в любую кучу.

Игра завершается, когда общее количество камней в кучах становится более 45. Победителем считается игрок, сделавший последний

ход, т. е. первым получивший 46 или больше камней в двух кучах. В начальный момент в первой куче было 5 камней, а во второй — S камней, $1 \leq S \leq 40$.

Укажите минимальное и максимальное из таких значений S , при которых Петя не может выиграть первым ходом, но у Пети есть выигрышная стратегия, позволяющая ему выиграть вторым ходом при любой игре Вани. В ответе запишите сначала минимальное значение, затем максимальное.

Задание 21

В игре, описанной в предыдущем задании, в начальный момент в первой куче было 5 камней, а во второй — S камней, $1 \leq S \leq 40$.

Найдите минимальное из таких значений S , при котором у Вани есть стратегия, позволяющая ему выиграть вторым ходом при любой игре Пети, но у Вани нет стратегии, которая позволяла бы ему гарантированно выиграть первым ходом.

Для решения этих задач составляем программу, аналогичную предыдущей. Теперь позиция игры определяется двумя числами s_1 и s_2 — количеством камней в первой и второй кучах соответственно. Без ограничения общности решения будем предполагать, что, делая ход, кучу с меньшим количеством камней (которую предполагается увеличивать) игроки объявляют первой кучей.

При рекурсивном вычислении функции выигрыша в соответствии с формулой перечисляем все возможные позиции, которые можно достичь из данной. Поиск минимального значения функции выигрыша среди допустимых ходов осуществляется в цикле. Критерий завершения партии — сумма камней не менее 46.

Для уменьшения времени работы программы ограничим глубину анализа 7 полуходами. Если партия превышает указанную длительность, то будем считать, что функция выигрыша равна 0. Такая глубина анализа избыточна, ведь даже в задании 21 поиск идет только до 4-го полухода (второй ход Вани). Код программы приведен на рис. 3.

```
def hod(s1,s2,n):
    if n>7: return 0
    if s1+s2>=46: return -1/(n-1)
    a=min(s1,s2)
    b=max(s1,s2)
    m=10000000.0
    for i in range(1,a+1): m=min(m,hod(a+i,b,n+1))
    return -m

for i in range(1,35):
    #в начальный момент в первой куче 5 камней
    print(i,hod(5,i,1))
```

Рис. 3. Текст программы для примера с двумя кучами

Эта программа выдает следующий результат (рис. 4).

1 0	13 0.2	25 0.3333333333333333
2 0	14 0.2	26 0.3333333333333333
3 0	15 0.2	27 0.3333333333333333
4 0	16 0.2	28 0.3333333333333333
5 0	17 0.2	29 0.3333333333333333
6 0	18 0.2	30 0.3333333333333333
7 0	19 0.2	31 0.3333333333333333
8 0	20 -0.25	32 0.3333333333333333
9 -0.1666666666666666	21 -0.25	33 0.3333333333333333
10 -0.1666666666666666	22 -0.25	34 -0.5
11 0.2	23 -0.25	
12 0.2	24 0.3333333333333333	

Рис. 4. Результат работы программы из рис. 3

В соответствии с этим результатом Петя побеждает на своем втором ходу ($n = 3$, $f(n) = 1/3 = 0,333333\dots$) при начальном количестве камней S от 24 до 33, а Ваня побеждает на своем втором ходу ($n = 4$, $f(n) = -1/4 = -0,25$) при значениях S от 20 до 23.

Если программа работает слишком медленно, во второй строке кода глубину поиска можно ограничить еще сильнее (например, 6 или 5).

Данный алгоритм является рекурсивным, поиск осуществляется обходом по дереву с коэффициентом ветвления d , равным количеству вариантов хода у каждого игрока, и высотой, равной глубине поиска n . Поэтому количество рассматриваемых вариантов примерно пропорционально d^n (на самом деле меньше, так как при кратном увеличении камней в куче игра закончится раньше).

Вычислительная сложность, соответственно, будет экспоненциальной $O(d^n)$, что может приводить к слишком большому времени работы программы. Однако, учитывая, что для большинства задач с одной кучей камней коэффициент ветвления не превышает 3, а в задачах с двумя кучами этот коэффициент обычно не больше 4, рекурсивный алгоритм перебора всех узлов дерева будет выдавать результат очень быстро при глубине поиска, не превышающей 4–5 полуходов. А большая глубина поиска в задачах ЕГЭ на выигрышную стратегию пока не требуется.

Цифровая трансформация системы управления в сфере обслуживания противопожарных систем

Аннотация. Обслуживание систем противопожарной защиты сводится к проверке и ремонту. К сожалению, «невидимость» этих систем в обычной ситуации создает соблазн у участников рынка выполнять работу недобросовестно. В статье рассматриваются причины такого явления и предлагаются решения как на уровне исполнителя, так и на уровне заказчика, которые позволят повысить уровень работоспособности систем, тем самым снизив материальный ущерб и число погибших и пострадавших от пожаров.

Ключевые слова: пожарная безопасность; противопожарные системы; ущерб от пожаров; автоматизация; МЧС.

По данным МЧС, в течение 2023 г. в России произошло более чем 350 тыс. пожаров, в которых погибло порядка 7,2 тыс. чел.¹ Материальный ущерб от пожаров составляет десятки миллиардов рублей каждый год. Так, 3 августа 2022 г. сгорел склад Ozon в Подмоскowie, ущерб составил свыше 10 млрд р.² Пожар 13 января 2024 г. на складе Wildberries в Шушарах привел к ущербу 10–20 млрд р.³ В обоих случаях современные складские комплексы, возведенные буквально в последние несколько лет, сгорели практически полностью вместе со всем товаром.

В последние годы при любом крупном пожаре в сети появляются видеозаписи очевидцев, свидетельствующие о частичной или даже полной неработоспособности систем противопожарной защиты (СПЗ). По понятным причинам администрация объектов утверждает обратное, чтобы снизить вероятность штрафа или даже уголовных дел со стороны проверяющих инстанций⁴.

Согласно п. 54. Правил противопожарного режима в Российской Федерации, руководитель обязан организовывать обслуживание СПЗ на своем объекте⁵. При этом на практике большинство руководителей от-

¹ В России в 2023 году произошло 350 тыс. пожаров / ТАСС. 2023. 25 дек. URL: <https://tass.ru/proisshestiya/19623885> (дата обращения: 12.04.2024).

² Страховщики оценили ущерб от пожара на складе Ozon в 10 млрд рублей / RG.ru. 2022. 3 авг. URL: <https://rg.ru/2022/08/03/strahovshchiki-ocenili-ushcherb-ot-pozhara-na-sklade-ozon-v-10-mlrd-rublej.html> (дата обращения: 10.04.2024).

³ Батыров Т. Ущерб от пожара на складе Wildberries оценили в 10–20 млрд рублей / Forbes. 2024. 13 янв. URL: <https://www.forbes.ru/biznes/504212-userb-ot-pozara-na-sklade-wildberries-ocenili-v-10-20-mlrd-rublej> (дата обращения: 07.04.2024).

⁴ Пять лет со дня пожара в ТЦ «Зимняя вишня». Истории пострадавших и очевидцев / Газета.Ru. 2023. 25 марта. URL: <https://www.gazeta.ru/social/2023/03/25/16453675.shtml> (дата обращения: 05.04.2024).

⁵ Об утверждении Правил противопожарного режима в Российской Федерации: постановление Правительства РФ от 16 сентября 2020 г. № 1479.

носятся к этой задаче добросовестно, как минимум это актуально для крупных складских комплексов, где в силу конструктивных особенностей (большие открытые пространства без противопожарных перегородок) огонь может распространяться особенно быстро. Но в то же время регулярно происходят крупные пожары с миллиардными убытками.

Ключевая причина этого — неправильный подход к организации обслуживания СПЗ со стороны заказчиков. Формально процесс обслуживание СПЗ прост: готовится регламент обслуживания, проводится тендер, выбирается исполнитель, который выполняет условия договора. Но при реализации процесса на практике заказчик сталкивается с несколькими проблемами.

Первая важная проблема — «невидимость» результата работы сервисной компании для стороннего наблюдателя. Пожары в реальности для каждого конкретного объекта являются редким явлением, а стороннему наблюдателю до момента самого пожара вообще непонятно, насколько работоспособна система, ведь только часть неисправностей можно определить по индикации приборов, а некоторые проблемы выявляются только при непосредственной проверке. Поэтому сервисный персонал может из-за лени, забывчивости или цейтнота пренебрегать своими обязанностями (не выполнять проверки или не делать ремонты), и это никаким образом нельзя обнаружить.

Далее, поскольку боевые сработки СПЗ для каждого объекта редки, экономически выгодно экономить при монтаже и обслуживании СПЗ буквально на всем. Одновременно в силу ряда физических и технических особенностей СПЗ более подвержены к воздействию ТВР и механических повреждений чем, например, водопровод. Поэтому с точки зрения безопасности людей на объекте качественно обслуживать «пожарку» важнее, чем иные инженерные системы. Но в реальности сервисный техник по указанным выше причинам может пропускать операции регламента без риска быть «пойманным с поличным», после чего при реальном пожаре СПЗ оказываются полностью или частично неработоспособны, что может привести к материальному ущербу большему, чем при полноценном функционировании систем, а также к появлению пострадавших или погибших, что категорически недопустимо.

Вторая проблема в сфере обслуживания СПЗ — большое количество информации, касающейся ремонтов, каждый из которых может находиться на разных стадиях устранения: получена заявка, идет или уже проведена диагностика, заказано оборудование, оборудование в пути, идет или уже закончен ремонт, работа сдана заказчику с подписание акта.

При большом количестве мелких деталей на каждом из десятков объектов среднестатистической сервисной компании с сотнями ремон-

тов без использования специализированных (excel- или гугл-таблицы не подходят) ведет к тому, что периодически информация теряется, а какие-то ремонты «зависают».

Третья проблема — структура участников рынка. Большая часть сервисных компаний — это микробизнес, включающий не более 7 чел., у которых бизнес-мышление работает на соответствующем уровне и нет финансов для внедрения современных информационных систем.

Наконец, четвертая проблема — сложившаяся практика поиска подрядчиков через тендера. Логика ФЗ-44, согласно которому выигрывает подрядчик с самой низкой ценой вместе с неумением большинства даже крупных заказчиков грамотно составлять ТЗ приводит к тому, что тендера выигрывают компании, которые заведомо и осознанно настроены на фальсификацию деятельности с выполнением только части проверок. При таком подходе многие поломки в системе не обнаруживаются, накапливается недоремонт, а в момент боевой сработки система оказывается неработоспособной.

При этом ответственные представители заказчика, даже видя явную халтуру, часто никак с ней не борются, во-первых, потому что уверены, что «все компании такие», во-вторых, потому что руководители (особенно бюджетных учреждений) заинтересованы экономить деньги в ходе тендеров, а сэкономленное направить на другие нужды своих организаций.

И далее такое положение дел приводит к тому, что качественно работающая организация понимает, что после халтурщиков накапливается огромный недоремонт, т. е. ей придется за свой счет исправлять ошибки других людей, как правило, не получая за это деньги. При этом в отрасли приняты некоторые нормативные документы (в частности ГОСТ Р 59638-2021, требующий в п. 6.5.1 устранять любые неисправности в течение 24 ч после обнаружения), выполнение которых невозможно, а невыполнение их может привести к отзыву лицензии и потере бизнеса¹. Это приводит к замкнутому кругу, в результате которого на объекте «закрепляются» заведомо недобросовестные исполнители.

Решением проблемы могла бы стать разработка современной информационной системы, управляющей процессом обслуживания и делающей прозрачными все этапы работы. ООО «Север» как лицензированная организация, обслуживающая СПЗ на более чем 100 объектов в Екатеринбурге и окрестностях, разработала подобную ИС «Молния», которая состоит из мобильной части (мобильное приложение на ОС

¹ ГОСТ Р 59638-2021. Системы пожарной сигнализации. Руководство по проектированию, монтажу, техническому обслуживанию и ремонту. Методы испытаний на работоспособность (утв. и введен в действие приказом Росстандарта от 24 августа 2021 г. № 791-ст).

Android устанавливается на смартфоны техников) и серверной частей. Изначально система, которая сейчас обросла уже многими функциями, создавалась для решения двух проблем:

1) пропуск сервисным персоналом каких-либо операций в рамках регламентных проверок СПЗ;

2) потери персоналом информации о ремонтах и зависание на промежуточных стадиях ремонтов, до которых «не доходят руки».

Обеспечение добросовестного выполнения регламентных проверок в ИС «Молния» обеспечивается следующим образом.

1. Все операции в рамках регламентной проверки заносятся в чек-лист на сервер с указанием способа подтверждения (фото, видео или ввод данных).

2. При начале регламентной проверки на объекте техник открывает на смартфоне чек-лист в мобильном приложении «Молния», выполняет регламент и подтверждает выполнение каждой операции указанным в чек-листе способом.

3. Чек-лист с подтверждениями загружается на сервер в тот момент, когда владелец смартфона оказывается в зоне покрытия Wi-Fi.

4. Бригадир для проверки качества работы на сервере проверяет каждую операцию в чек-листе, ориентируясь на фото- или видео-подтверждение.

В ООО «Север» в каждый момент времени на разных этапах находится около 450–500 ремонтов. Очевидно, что контролировать такой объем информации без современной информационной системы невозможно. Для решения проблемы контроля большого количества ремонтов бизнес-процесс «Ремонт» разбит на следующие этапы.

1. Подтверждение неисправности. Данный этап необходим, потому что в некоторых случаях пользователь считает неисправностью штатную работу системы.

2. Диагностика неисправности, результатом которой является понимание ремонтной операции, которую надо совершить, чтобы привести систему в работоспособное состояние. По времени диагностика может быть как мгновенной, так и занимать время до нескольких суток.

3. Устранение неисправности, или ремонт, после чего система переходит в работоспособное состояние. Данный этап может выполняться практически мгновенно (например, при нахождении места обрыва в шлейфе восстановления занимает считанные минуты), так и длиться очень долго (например, если необходимо менять оборудование в сложных условиях, или выполнять работы по перепрограммированию системы).

4. Сдача работы заказчику с подписанием со стороны представителя заказчика Акта устранения неисправности и визированием им же записи в Журнале технического обслуживания (Журнал ТО).

Аналогично бизнес-процессу «Регламентная проверка» при реализации бизнес-процесса «Ремонт» от техника требуется выполнять фото- или видео-подтверждение всех ключевых точек описанного процесса. Также выполняется видеofиксация инцидентов (т. е. ситуаций, когда не удастся попасть в помещение либо подписать с заказчиком какой-либо юридический или технический документ) с целью минимизации потенциальных претензий со стороны заказчика или проверяющих органов в будущем и вытекающих из этого юридических последствий.

За последние несколько лет некоторые заказчики ООО «Север», выбирающие подрядчика для обслуживания СПЗ при помощи тендерных процедур согласно ФЗ-44 и ФЗ-223, уже научились в тендерную документацию вносить требования к подрядчику выполнять фото- и видеofиксацию всех операций в рамках регламентных проверок и ремонтов. Тем самым они в значительной степени защищают себя от заключения договоров с некачественными подрядчиками.

Таким образом, отрасль обслуживания систем противопожарной защиты, являясь узкой специфической сферой деятельности, также испытывает на себе цифровую трансформацию, но еще находится в начале пути. Мы надеемся, что предложенные нами подходы к обеспечению качества работы позволят повысить уровень работоспособности систем и тем самым снизить материальный ущерб и число погибших и пострадавших от пожаров.

И. А. Овчинников, А. Е. Посягин

Уральский государственный экономический университет, г. Екатеринбург

Российский 3D-движок UNIGINE. Применение, особенности, место в промышленности и игровой индустрии, перспективы развития

Аннотация. Выделены основные преимущества и недостатки 3D-движка UNIGINE в различных сферах его применения: создании симуляторов, создании цифровых двойников, работе с дополненной и виртуальной реальностями, применении в индустрии развлечений. Проведено сравнение UNIGINE с зарубежными игровыми движками Unity и Unreal Engine. Выявлены перспективы развития движка.

Ключевые слова: UNIGINE; российский 3D-движок; 3D-графика; отечественные разработки; импортозамещение в IT; игровая индустрия; виртуальная реальность; цифровой двойник.

Игровой движок — комплекс прикладных программных модулей, которые обеспечивают графическую визуализацию, звуковое сопровождение, перемещение объектов и персонажей, их действия в соответствии

со скриптами, а также взаимодействие по сети, соблюдение физических эффектов и законов и многое другое. Проще говоря — это модули, которые «оживляют» трехмерные миры.

На сегодняшний день в мире самыми известными бесплатными для использования игровыми движками являются зарубежные Unity и Unreal Engine. Но мало кому известен также бесплатный для использования российский игровой движок UNIGINE. Сейчас, когда импортозамещение в Российской Федерации становится крайне востребовано, очень важно понимать, какие продукты, в том числе и информационные, уже созданы у нас в стране и оказывать им должное внимание, так как развитие собственного продукта играет важную роль как для страны, так и для всех ее сфер деятельности. Одним из таких продуктов, способных в будущем составлять конкуренцию за рубежом, является UNIGINE.

Разработка UNIGINE началась в 2002 г. с open-source-проекта Александра Запругаева и Дениса Шеринга в Томске. В 2005 г. разработчики перевели свой движок на коммерческую лицензию и основали компанию UIGINE Holding. До 2020 г. движок распространялся исключительно по коммерческой лицензии. 10 апреля 2020 г. вышла первая бесплатная версия движка UNIGINE 2 Community Edition. Все проекты UNIGINE Holding, в том числе и сам UNIGINE поддерживают минимум две платформы: Windows и Linux.

Прежде чем говорить о преимуществах и недостатках UNIGINE, стоит рассмотреть, для каких целей могут использоваться игровые движки.

Первое, для чего может использоваться игровой движок, — для создания видеоигр. Движок, на котором создаются видеоигры, должен обладать широконаправленным набором инструментов, чтобы на нем возможно было создавать видеоигры в разных жанрах и графических стилях, также такой движок должен поддерживать разработку под современные игровые платформы.

Вторым назначением игрового движка может быть создание цифровых двойников — так называемых копий реального объекта или процесса в цифровом пространстве, позволяющих решать широкий список бизнес-задач на различных предприятиях. Движок для создания цифровых двойников должен с высокой точностью воспроизводить множество физических процессов.

Третьей целью может быть создание симуляторов и тренажеров. Эта цель во многом схожа с целью создания цифровых двойников, за исключением того, что симуляторы и тренажеры должны испытывать навыки и умения людей, а не виртуальные процессы.

Четвертое, для чего может понадобиться игровой движок, — создание виртуальной и дополненной реальности (VR и AR). Технологии VR и AR совмещаются с прошлыми тремя целями.

На данный момент UNIGINE не может похвастаться множеством игровых проектов. Таких всего около десяти, среди них: Syndicates of Arkon, Petshop, Oil Rush, Demolicious, Cradle, Tryst, RF-X, Sumoman, Dual Universe. Такое количество игровых проектов связано со специфической архитектурой движка, которая разрабатывалась для симуляторов (подробнее об этом в следующих абзацах) и отсутствия поддержки Android и MacOS. Так, например, из специфических решений UNIGINE в движке используются 64-битные координаты объектов (так называемые числа двойной точности или Double Precision). Таким образом, движок без просадок способен отображать локации размером около 400 игровых километров, в отличие от Unity и Unreal Engine, которые используют 32-битные координаты объектов и без просадок могут отображать лишь около 30 игровых километров. Такая особенность UNIGINE позволяет создавать на движке локации размером с солнечную систему, но большей части видеоигр такой размах вовсе не нужен, а числа двойной точности лишь дают дополнительную нагрузку на компьютер, однако в перспективе движок может показать себя с лучшей стороны.

Если на UNIGINE не делают игры, то зачем он вообще кому-то нужен? Хотя движок и позиционируется как игровой, сейчас он занимает нишу в неигровых проектах. А именно в симуляциях и цифровых двойниках. Благодаря своей архитектуре UNIGINE способен с высочайшей точностью воспроизводить физические процессы из реального мира в виртуальном. Те же числа двойной точности для координат объектов позволяют создавать детальнейшие авиационные и космические симуляторы с впечатляющей дальностью прорисовки объектов. Также в томском движке уделено немало внимания графике и визуальным эффектам. Порой UNIGINE способен выдавать графику, ничем не уступающую мастодонту 3D-движков — Unreal Engine. Особенно впечатляет то, с какой точностью отечественный движок воспроизводит объемные воду и облака, промышленные объекты, свет, тени и отражения.

Сегодня UNIGINE используется преимущественно в промышленных отраслях, таких как авиация, судостроение, космонавтика, нефтегазовая и горнодобывающая отрасли, ОПК, городское планирование, грузоперевозки, строительство и др. Во всех этих отраслях он используется в основном при создании симуляционных моделей или как в случае с ОПК и авиацией в качестве виртуальных тренажеров. В своих проектах UNIGINE используют крупные российские компании из списка топ-500 РБК: Алмаз-Антей, Ростех, Росатом, Аэрофлот, РЖД, ОСК, Сбербанк, Газпром, Роснефть, Лукойл и др.

Примеры проектов, созданных на UNIGINE: полная копия Московского метрополитена¹, профессиональная проектировка и симуляция автомобиля², симулятор диспетчера аэропорта и симулятор БПЛА (беспилотный летательный аппарат)³.

Стоит отметить, что UNIGINE поддерживает работоспособность с большими данными (Big Data). Данная особенность позволяет создавать проекты, которые требовательны к обработке и визуализации цифровой информации.

UNIGINE не обошла стороной и поддержка VR и AR. Движок в своей базовой комплектации поддерживает Oculus Rift, HTC Vive и HTC Vive Pro, а также имеет все необходимые модули для работы с технологиями виртуальной и дополненной реальностями.

Также томская технология известна своими бенчмарками, помогающими людям испытать стабильность и производительность своих ПК. Среди этих бенчмарков: Heaven, Valley и Superposition, поддерживающий VR.

На сегодняшний день сравнивать открытую бесплатную версию UNIGINE с аналогичными версиями Unity и Unreal Engine не следует. Пока на Unreal и Unity всюду разрабатываются множество игровых проектов, UNIGINE не сильно торопится развиваться в этом направлении. Приоритетом UNIGINE Holding является разработка программ для бизнес-целей, а не универсальность и массовость для разработчиков игр. Но все же игровая направленность UNIGINE постепенно развивается, и периодически выпускаются новые бесплатные открытые версии движка. Сама компания-разработчик создает на своем движке видеоигры и делится наработками движка в этой сфере. Вполне может быть, что в будущем на рынке игровых 3D-движков вместе с Unity и Unreal Engine будет одинаково востребован и UNIGINE.

Из особенностей движка, говорящих о том, что UNIGINE развивается в сторону открытости и массовости, можно выделить следующее: наличие множества официальных открытых документаций и видеоуроков для UNIGINE разработчиков; поддержка языков программирования C#, C++ и UnigineScript (также компанией разрабатывается язык визуального программирования для UNIGINE, наподобие Blueprints в Unreal Engine); собственная площадка с ассетами для движка. В документации

¹ 11 новых симуляторов ЖД транспорта на базе UNIGINE 2 Sim, разработанных Smart Simulation в 2022 / UNIGINE. 2022. 20 дек. URL: <https://unigine.com/ru/news/2022/11-train-simulators-powered-by-unigine-in-2022> (дата обращения: 04.05.2024).

² Solutions for Virtual Test Driving / IPG Automotive. URL: <https://ipg-automotive.com/en/> (дата обращения: 04.05.2024).

³ UFA, Inc — Air Traffic Control Training / Tower & Radar Simulator. URL: <https://www.ufainc.com> (дата обращения: 04.05.2024).

к UNIGINE можно выделить тот факт, что существуют отдельные разделы для людей, переходящих на томский движок с зарубежных движков Unity¹ и Unreal Engine². Тот факт, что движок поддерживает три языка программирования, два из которых очень распространены, а также используются в Unreal Engine и Unity, позволяет почти любому программисту легко влиться в разработку программ на UNIGINE. Площадка с ассетами для движка Unigine Asset Store на данный момент содержит в себе только контент от самой Unigine Holding, но площадку планируется развивать. В будущем туда добавят возможность добавления ассетов пользователями движка, а также компанией ведутся переговоры с крупными разработчиками контент-паков, заинтересованных в размещении своих библиотек 3D-сканов. Кроме того, благодаря развитию движка в промышленной среде для создания реалистичных моделей различных объектов, Unigine имеет большой потенциал для того, чтобы на этом движке делали AAA-игры с красивой графикой. Добавление новых функций, технологий и улучшение движка в целом способствуют развитию проекта, тем самым создавая конкурентоспособность на рынке, что в свою очередь заставляет развиваться всю игровую индустрию.

Таким образом, 3D-движок UNIGINE обладает мощным инструментарием для реализации очень правдоподобных объектов из реального мира, но при этом пока не способен быть массовым движком для разработки видеоигр. Постоянное развитие, добавление новых инструментов, обновление старых, поддержка VR/AR и многое другое показывает, что у разработчиков есть четкий план развития и постоянная поддержка комьюнити. Этот движок уже занимает свою нишу на рынке программного обеспечения для создания симуляций и цифровых двойников, а сейчас медленно, но верно начинает осваивать рынок игровой индустрии. Данные перспективы играют важную роль как в развитии проекта, так и всей индустрии движков.

¹ *Переход* на UNIGINE с Unity — Документация / Unigine Developer. URL: https://developer.unigine.com/ru/docs/latest/migration/from_unity/ (дата обращения: 04.05.2024).

² *Переход* на UNIGINE с Unreal Engine — Документация // Unigine Developer. URL: https://developer.unigine.com/ru/docs/latest/migration/from_ue/?rlang=cpp (дата обращения: 04.05.2024).

Разработка алгоритма анализа архитектуры информационной системы предприятий

Аннотация. В статье рассматривается процесс разработки алгоритма анализа архитектуры информационной системы (ИС) предприятий, который базируется на области знаний об архитектурном подходе при проектировании, включает в себя формирование общего представления о предприятии, его стратегии, бизнес-модели, оценку внутренних и внешних факторов влияния, характеристику процессов, технико-экономических факторов, составление критериев оценки соответствия архитектуры предприятия и проектируемой информационной системы. Предложенный алгоритм позволит архитекторам ИС предприятия всецело оценить текущее состояние существующих систем, выявить возможные улучшения и разработать план по их внедрению.

Ключевые слова: алгоритм анализа; архитектура предприятия; архитектура информационных систем; технологии.

Информационные системы играют ключевую роль в успешной деятельности современных предприятий. Они обеспечивают эффективное управление ресурсами, оптимизацию процессов и поддержку принятия решений. Однако в современный период опережающих темпов изменений, ужесточения санкционного влияния в сфере цифрового развития РФ для достижения гибкости, адаптивности и максимальной эффективности бизнес-моделей необходимо проводить анализ архитектуры информационной системы предприятия. В статье рассматривается алгоритм анализа архитектуры информационной системы, который поможет предприятиям повысить комплексность проектирования, оценить текущее состояние своих систем и выявить возможные улучшения.

При разработке алгоритма анализа архитектуры информационной системы предприятий авторы использовали ГОСТ Р 59792-2021 «Информационные технологии. Комплекс стандартов на автоматизированные системы. Виды испытаний автоматизированных систем». Это стандарт, который определяет виды испытаний автоматизированных систем (АС) в области информационных технологий. В целом ГОСТ Р 59792-2021 направлен на обеспечение качества и эффективности автоматизированных систем путем проведения соответствующих видов испытаний, что является важным фактором в современной информационной индустрии.

Основы области знаний об архитектуре ИС предприятия глубоко рассмотрены в научных трудах Е. П. Зараменских, Е. А. Троицкой, Л. А. Артюшиной [1; 2], в которых описана история развития архитектуры предприятия, рассматриваются современные практики и накопленные знания, основные компоненты архитектуры предприятия и ме-

тамодели, процессы применения архитектурного подхода, методология структурного анализа и проектирования, инструменты совершенствования и развития архитектуры предприятия, критерии оценки эффективности бизнес-процессов.

Исследование информационного поля в области проектирования архитектуры предприятия позволило авторам разработать алгоритм анализа архитектуры информационной системы, который включает следующие блоки.

1. Формирование общего представления о предприятии:
 - а) факторы, формирующие организационную структуру и бизнес-модель;
 - б) предоставляемые услуги;
 - в) стратегия предприятия.
2. Определение внутренних и внешних факторов, влияющих на развитие предприятия:
 - а) привлекательность продукции;
 - б) привлекательность для сотрудников;
 - в) инвестиционная привлекательность;
 - г) макроэкономическое влияние;
 - д) конкуренция.
3. Характеристика процессов, происходящих на предприятии:
 - а) производственная мощь;
 - б) контроль производительности;
 - в) влияние рынка;
 - г) масштабирование производства;
 - д) социальная политика;
 - е) факторы, влияющие на капитал;
 - ж) возможности продолжения деятельности.
4. Выявление технико-экономических факторов формирования организационной структуры предприятия:
 - а) организационная структура;
 - б) технологическая, производственная, хозяйственная структуры;
 - в) BSC и KPI подразделений и предприятия.
5. Составление критериев оценки автоматизированных систем:
 - а) составление критериев для оценки;
 - б) составление карты рисков.
6. Построение функциональной модели предприятия с использованием методологий структурного анализа и проектирования:
 - а) функциональная модель IDEF;
 - б) анализ модели и выявление уязвимостей;
 - в) рекомендации по устранению недостатков моделей.

7. Построение информационной архитектуры предприятия:
 - а) тип и объем необходимой информации для оптимизации процессов;
 - б) связь понятий архитектуры информационных данных;
 - в) модели информации на различных уровнях абстракции (концептуальный, логический, физический, уровень представления данных).
8. Построение архитектуры приложений предприятия:
 - а) портфель прикладных систем;
 - б) модель для построения архитектуры приложений.
9. Построение технологической архитектуры предприятия:
 - а) технологическая архитектура в разрезе технологий;
 - б) выявление наиболее важных технологий.
10. Формирование многослойной архитектуры предприятия:
 - а) комплексная модель архитектуры предприятия в разрезе слоев;
 - б) выявление наиболее важных слоев архитектуры.
11. Анализ и оценка построенной архитектуры (мобильность, гибкость, выгодность для предприятия, применимость к предприятию);
 - а) оценка критериев;
 - б) выявление недочетов и рисков;
 - в) оценка построенной архитектуры;
 - г) рекомендации по исправлению недочетов.

Анализ архитектуры информационной системы предприятия является важным этапом в обеспечении ее эффективной работы. Используя предложенный алгоритм, предприятия смогут оценить текущее состояние своих систем, выявить возможные улучшения и разработать план по их внедрению. Это, в свою очередь, приведет к повышению производительности, улучшению безопасности данных и оптимизации затрат на поддержку информационных систем, а в перспективе превращение ИС в ядро бизнес-модели.

Библиографический список

1. *Зараменских Е. П., Кудрявцев Д. В., Арзуманян М. Ю.* Архитектура предприятия / под ред. Е. П. Зараменских. 2-е изд., перераб. и доп. М.: Юрайт, 2024. 436 с.
2. *Троицкая Е. А., Артюшина Л. А.* Информационные технологии в разработке архитектуры предприятия: учеб. пособие. Владимир: Изд-во ВлГУ, 2020. 318 с. URL: <https://dSPACE.www1.vlsu.ru/bitstream/123456789/8647/1/02069.pdf> (дата обращения: 05.05.2024).

Применение отечественных СУБД в различных отраслях экономики: преимущества и особенности использования

Аннотация. Проведен сравнительный анализ функциональных возможностей отечественных систем управления базами данных (СУБД). Выявлены преимущества и недостатки при работе в различных отраслях экономики. Рассмотрены популярные отечественные СУБД и их особенности.

Ключевые слова: системы управления базами данных; СУБД; отечественное программное обеспечение; ПО; преимущества и недостатки отечественных СУБД; отечественные разработки; автоматизация процессов; управление информацией.

В XXI в. количество информации увеличивается ежесекундно. Такие большие потоки данных необходимо качественно обрабатывать и хранить. Для этого необходимы надежные инструменты, такие как системы управления базами данных (СУБД). С 2022 г. экономика Российской Федерации столкнулась с угрозой блокировки зарубежного программного обеспечения (ПО). По этой причине важность разработки отечественного ПО значительно выросла [1]. Но в каких отраслях экономики используются СУБД и какими они обладают преимуществами и особенностями использования?

Отечественные СУБД обладают широким набором инструментов для управления информацией в различных сферах экономики. Среди самых востребованных являются следующие СУБД¹:

– ClickHouse — колоночная СУБД, работающая на языке запросов SQL с открытым кодом для анализа данных;

– Postgres Pro — СУБД на основе PostgreSQL с переписанным и улучшенным кодом, обладающая большим количеством инструментов для обработки данных [4];

– ЛИНТЕР — реляционная СУБД, предназначенная для автоматизации бизнес-процессов компании [5];

– СУБД Лира-Р — реляционная СУБД на основе СУБД PostgreSQL 10, которая обладает хорошей защитой информации и обработкой данных ограниченного распространения;

– Jatoba — СУБД с многопользовательским доступом к данным с разным уровнем конфиденциальности [2];

¹ *Альтернатива есть!* Обзор 6 российских СУБД для миграции // Хабр. 2023. 15 июня. URL: <https://habr.com/ru/companies/k2tech/articles/741980/> (дата обращения: 13.05.2024).

- Квант-Гибрид — объектно-реляционная СУБД для обработки информации с повышенными требованиями к надежности, быстродействию, безопасности и секретности;
- Ред БД — СУБД с открытым кодом и совместимостью почти со всеми платформами;
- ProximaDB — СУБД на основе PostgreSQL, совместимая с 1С;
- Arenadata PG — СУБД с гибким механизмом программирования обработки данных.

Это далеко не весь список отечественных СУБД, которые успешно справляются с программой импортозамещения ПО [3]. Каждая система обладает своим функционалом и подходит под определенную отрасль экономики.

Однако чем же отличаются эти СУБД и какие у них есть преимущества и недостатки?¹ Для ответа на данный вопрос составлена сравнительная таблица самых распространенных отечественных СУБД (см. таблицу) [6].

Преимущества и недостатки отечественных СУБД

Характеристики	ClickHouse	Postgres Pro	ЛИНТЕР	СУБД Лира-Р
Бесплатность	Да	Да	Нет	Нет
Лицензия	Apache 2.0	Open Source	Проприетарная	Проприетарная
Язык запросов	SQL	SQL	SQL	SQL
Поддержка JSON	Да	Да	Да	Да
Распределенная обработка	Да	Да	Нет	Нет
Поддержка транзакций	Ограниченная	Да	Да	Да
Поддержка репликации	Да	Да	Да	Да
Тип	Columnar	Relational	Relational	Relational
Производительность	Высокая	Высокая	Средняя	Средняя
Поддержка индексов	Да	Да	Да	Да

Сравнительная таблица самых распространенных отечественных программных продуктов взята только по основным характеристикам. Стоит отметить, что каждая СУБД предназначена для определенных областей экономики. Однако существуют такие СУБД, которые могут использоваться в разных сферах деятельности. Для этого необходимо реализовать продукт таким образом, чтобы он имел большой функционал и подходил множеству компаний.

¹ *Топ* российских СУБД 2022 года / Дзен. 2022. 11 нояб. URL: <https://dzen.ru/a/Y23MTU2Be2VxT7gH> (дата обращения: 13.05.2024).

Исходя из анализа СУБД и таблицы, можно объединить все особенности и преимущества отечественных разработок в сфере СУБД:

- высокая эффективность и производительность: основная часть отечественных СУБД известна своей высокой эффективностью и производительностью при работе с большими данными, так как обладают хорошей оптимизацией и современными инструментами обработки данных;

- гибкость: большинство СУБД разработаны таким образом, что затрагивают сразу несколько отраслей в сфере экономики, тем самым удовлетворяют потребностям большого числа компаний;

- защита данных: современное ПО обладает высоким уровнем защиты информации с помощью различных способов шифрования данных, аутентификации, настройки многопользовательского доступа и контроля за ним;

- экономическая сторона: разработка отечественных продуктов намного выгоднее в долгосрочной перспективе, так как прибыль от конечного продукта будет оставаться в стране, а не уходить зарубежным компаниям. Кроме того, защита от утечки информации также остается за контролем той компании, которая разрабатывает и поддерживает работоспособность собственного ПО.

Таким образом, разработка и поддержка отечественного разработчика СУБД играет очень важную роль для государства, так как исключает риск ухода зарубежных компаний, минимизирует шанс утечки информации и влияет на развитие страны в информационной сфере.

Анализируя рынок отечественных СУБД, стоит отметить и их сферы применения:

- финансовый сектор: работа с финансовыми данными, управление клиентскими счетами, проведение транзакций и многое другое;

- промышленный сектор: управление производственными данными, мониторинг производственных предметов, планирование производства и многое другое;

- здравоохранение: хранение данных о пациентах и истории болезни, анализ заболеваемости и их причинах и многое другое;

- транспорт и логистика: хранение данных о транспорте, путях доставки, количестве товара и многое другое.

Это лишь часть всех сфер, где используются СУБД. В данный список входят телекоммуникации, государственный, научный и многие другие сектора экономики. Однако насколько успешно отечественные СУБД внедряют в данные сферы деятельности? Для этого разберем некоторые примеры успешного использования отечественного продукта в России.

Финансовый сектор: Банк «Открытие» использует для работы с большими данными ClickHouse. Благодаря данной системе банк проводит анализ финансовых данных и на их основе выявляет риски. Внедрение позволило увеличить скорость обработки данных, снизить затраты на их анализ и повысить качество принятия управленческих решений.

Промышленный сектор: компания «Уралмашзавод» использует ClickHouse для анализа производственных данных, мониторинга производственных процессов и оптимизации производственных операций. Благодаря СУБД «Уралмашзавод» смог увеличить эффективность использования оборудования, что привело к сокращению затрат и к повышению производительных мощностей.

Здравоохранение: государственная клиника «Здоровье» использует СУБД ЛИНТЕР, которая позволяет им хранить данные о всех пациентах в электронном формате. Данное внедрение улучшает качество медицинских услуг и сокращает время обслуживание пациентов.

Примеров внедрения отечественных СУБД в разные сферы деятельности огромное количество, что положительно сказывается на развитии информационных технологий в нашей стране.

На рис. 1 представлен график распределения расходов на СУБД в разных сферах деятельности.



Рис. 1. Расходы на разные секторы экономики¹

Согласно статистике Strategy Partners на сентябрь 2023 г. рынок СУБД сократился более чем на 50 %. На рис. 2 представлена динамика

¹ *Источник* рис. 1 и 2: СУБД (рынок России) / TAdviser. URL: [https://www.tadviser.ru/index.php/Статья:СУБД_\(рынок_России\)](https://www.tadviser.ru/index.php/Статья:СУБД_(рынок_России)) (дата обращения: 13.05.2024).

изменения доли отечественных и международных поставщиков СУБД в Российской Федерации.



Рис. 2. Динамика объема российского рынка СУБД, млн р.

По данным графиков видно, что рынок отечественных поставщиков СУБД вырос с 2021 г., заменив ушедших международных вендоров. Аналитики прогнозируют к 2030 г. значительный рост и повышение импортозамещения в сфере отечественных СУБД.

Таким образом, использование отечественных СУБД в экономике имеет ряд преимуществ и способствует повышению эффективности бизнес-процессов. Дальнейшие исследования в этой области могут способствовать развитию информационных технологий и повышению конкурентоспособности отечественных компаний.

Библиографический список

1. *Воинова Я. Е.* Системы управления данными как инструмент обеспечения их безопасности в условиях цифровизации // Актуальные вопросы развития национальной экономики: материалы I Всерос. с междунар. участием науч.-практ. конф. (Пермь, 28 февраля 2022 г.). Пермь: ПГНИУ, 2022. С. 72–80.
2. *Гарипова А. Р.* Отечественный аналог СУБД «Jatoba» // XXVI Туполевские чтения (школа молодых ученых): материалы Междунар. молодежной науч.

конф.: сб. докл. (Казань, 9–10 ноября 2023 г.). Казань: ИП Сагиев А. Р., 2023. С. 2159–2164.

3. *Глибкина Е. В.* Импортозамещение в системах управления базами данных // Дискуссионные вопросы пенитенциарной науки и практики: сб. науч. тр. профессорско-преподавательского состава ВИПЭ ФСИН России: в 4 ч. / под общ. ред. В. Н. Некрасова. Вологда: ВИПЭ ФСИН России, 2022. Ч. 4. С. 25–29.

4. *Ерохин А. Г., Ванина М. Ф., Фролова Е. А.* PostgreSQL как альтернатива зарубежным реляционным СУБД: образовательная практика // Информатизация образования и методика электронного обучения: цифровые технологии в образовании: материалы VII Междунар. науч. конф. (Красноярск, 19–22 сентября 2023 г.). Красноярск: КГПУ, 2023. С. 283–287.

5. *Зольник В. В., Вознюк А. В.* Организация систем хранения данных с использованием отечественных систем управления базами данных (на примере СУБД «ЛИНТЕР») // Техника и безопасность объектов уголовно-исполнительной системы: сб. материалов Междунар. науч.-практ. конф. (Воронеж, 18–19 мая 2022 г.). Иваново: ПресСто; Воронежский институт ФСИН России, 2022. Т. 1. С. 438–440.

6. *Столярчук Н. М., Измайлова Н. А., Гринева А. Г., Радченко М. В.* Сравнение современных систем управления базами данных // Цифровизация экономики: направления, методы, инструменты: сб. материалов V Всерос. науч.-практ. конф. (Краснодар, 16–21 января 2023 г.). Краснодар: Кубанский ГАУ, 2023. С. 145–148.

Е. А. Привалова

*Уральский федеральный университет
имени первого Президента России Б. Н. Ельцина, г. Екатеринбург*

Преимущества выбора сервиса технической поддержки на базе «1С:ITILUM»

Аннотация. Рассматриваются преимущества выбора сервиса технической поддержки для государственного предприятия. Производится сравнительный анализ процессной модели для управления услугами, кроссплатформенности решения, интеграционных возможностей со сторонними решениями.

Ключевые слова: техническая поддержка; Service Desk; цифровизация; автоматизация.

С каждым годом промышленные предприятия все больше уделяют внимание увеличению производительности и повышению эффективности работы. С активным внедрением цифровизации на рабочих местах¹ часть рутинных задач пользователя перекладывается на программное обеспечение. В силу того, что существуют нестандартные ситуации, возникают технические и обусловленные человеческим фактором сбои

¹ *Цифровизация промышленности в России.* URL: <https://www.comnews.ru/content/227400/2023-07-13/2023-w28/cifrovizaciya-promyshlennosti-rossii> (дата обращения: 14.05.2024).

и ошибки, необходимость поддержки информационных систем остается актуальной. На данный момент представлен обширный спектр систем автоматизации данного технического процесса, но предпочтение необходимо отдавать системе, которая более полно удовлетворяет потребностям конкретного предприятия за счет гибкой настройки. В статье рассматриваются основные проблемы существующих программных аналогов¹ по автоматизации создания обращений в техническую поддержку, дальнейшей маршрутизации обращения исполнителю.

Необходимость закупки программного обеспечения для технической поддержки продиктована тем, что в настоящее время на предприятии используется устаревшая версия системы Service Desk, а именно — ИнфраМенеджер 5.4 2012 г.² В связи с этим некоторые функции, положительно влияющие на автоматизацию процессов обработки обращений и взаимодействия со сторонним программным обеспечением, невозможно использовать при данной версии системы.

Произведя оценку текущих потребностей предприятия, были выявлены следующие факторы, играющие важную роль в выборе Service Desk: управление инцидентами, запросами, изменениями, проблемами, уровнем сервиса, конфигурациями и активами; ведение базы знаний по обращениям; наличие отчетности и аналитики; возможность интеграции системы с имеющимся программным обеспечением.

В данной статье идет ориентир на выбор системы Service Desk для промышленного предприятия, входящего в госсектор. Согласно Приказу ФНС России от 18 января 2018 г. № 44-ФЗ «Об утверждении Стратегии ФНС России по импортозамещению ИТ-инфраструктуры и программного обеспечения, применяемых в автоматизированных информационных системах ФНС России, с учетом перехода на преимущественное использование продуктов и решений отечественных производителей»³, на предприятиях, относящихся к госсектору, возможна закупка только отечественного программного обеспечения и решений. Следовательно, импортные системы в статье не рассматриваются.

В настоящее время существует несколько Service Desk и ITSM-систем, входящих в рейтинг систем 2024 по Российской Федерации⁴. Для

¹ *Топ 10: Системы технической поддержки.* URL: https://www.helpdeski.ru/tags/sistemy_tehnicheskoy_podderzhki/ (дата обращения: 14.05.2024).

² *Рейтинг Service Desk систем 2024.* URL: https://crmindex.ru/ratings/service_desk (дата обращения: 14.05.2024).

³ *Импортозамещение 44-ФЗ.* URL: [https://www.consultant.ru/law/podborki/importozameschenie_44-fz/#:~:text=Подборка наиболее важных документов по консультации экспертов и многое другое](https://www.consultant.ru/law/podborki/importozameschenie_44-fz/#:~:text=Подборка%20наиболее%20важных%20документов%20по%20консультации%20экспертов%20и%20много%20другое) (дата обращения: 14.05.2024).

⁴ *Рейтинг Service Desk систем 2024.* URL: https://crmindex.ru/ratings/service_desk (дата обращения: 14.05.2024).

сравнительного анализа были выбраны системы российских производителей с наилучшим рейтингом и представлены в таблице с указанием наличия/отсутствия ключевых характеристик, необходимых для полноценной работы на предприятии¹.

Сравнительные характеристики систем

Характеристика	1С:ИТИЛИУМ	ИнфраМенеджер
Для чего подходит?	Для автоматизации управления услугами в средних и крупных компаниях как в области информационных технологий, так и в других функциональных областях	Для автоматизации ITSM-процессов
Функциональность	Отслеживание активов. Портал самообслуживания. Управление изменениями. Управление конфигурацией. Управление проблемами. Управление происшествиями. Управление релизами и развертыванием	Отслеживание активов. Портал самообслуживания. Управление происшествиями
Поддерживаемые платформы	Windows. WEB. iOS. Android	Cloud. SaaS. Web
Техническая поддержка	Рабочее время. Онлайн	Онлайн
Варианты обучения	Онлайн. Документация. Персонально	Документация
Интеграция с программным обеспечением	1С:ERP. 1С:ДО. 1С:Закупки. ActiveDirectory	ActiveDirectory

ИнфраМенеджер позволяет управлять только комплексным предоставлением ИТ-услуг² без возможности доработки конфигурации системы. Функциональность ИнфраМенеджер сильно ограничена по сравнению с функциональностью 1С:ИТИЛИУМ. ИнфраМенеджер не поддерживает десктопное клиентское приложение и имеет только веб-версию, что уменьшает удобство установки на рабочие места пользователей. В отличие от 1С:ИТИЛИУМ в ИнфраМенеджер меньше возможностей получить оперативную техническую поддержку и квалифицированное обучение пользователей/администраторов системы Service Desk.

¹ Сравнение решений для ITSM. URL: <https://picotech.ru/catalog/itsm-software/compare/1c-tilium-vs-inframenedzher-itsm/> (дата обращения: 14.05.2024).

² Что такое управление ИТ-услугами? / Atlassian. URL: <https://www.atlassian.com/ru/itsm> (дата обращения: 14.05.2024).

Исследование информационных систем на данном предприятии показало, что информационные системы, с которыми необходима интеграция Service Desk, работают на платформе 1С. В силу того, что «1С:ITIL IUM разработан на основе 1С:Предприятие 8»¹, настройка интеграции с информационными системами, работающими на этой же платформе, будет выполнена проще и эффективнее. Это позволит снизить количество ошибок при передаче данных из одной системы в другую.

Таким образом, благодаря анализу удалось выявить лидирующие системы Service Desk, их преимущества и недостатки. Исходя из требований предприятия к программному обеспечению, наиболее подходящим вариантом является система Service Desk на базе 1С:ITIL IUM. Данная система имеет большую функциональность в отличие от подобного программного обеспечения, гибкую настройку и интеграцию с уже имеющимися системами на базе 1С:Предприятие 8.

Е. В. Радковская

Уральский государственный экономический университет, г. Екатеринбург

Оптимизация распределения трудовых ресурсов на предприятии

Аннотация. В статье исследуются методы и стратегии оптимизации распределения трудовых ресурсов на предприятии, направленные на повышение эффективности и продуктивности работы. Рассматриваются современные подходы к анализу и планированию рабочих процессов. Особое внимание уделяется вопросам автоматизации рутинных задач, гибкости рабочих процессов и мотивации сотрудников. Приводятся примеры успешной реализации оптимизационных стратегий в различных отраслях промышленности. В статье также рассматриваются организационные и социальные аспекты оптимизации распределения трудовых ресурсов, такие как управление изменениями, повышение квалификации сотрудников и улучшение условий труда. В заключение предлагаются практические рекомендации для менеджеров и руководителей предприятий по внедрению эффективных систем управления трудовыми ресурсами.

Ключевые слова: назначение персонала; оптимальное распределение; трудовые ресурсы; симплекс-метод; оптимизация.

В современных условиях трудно представить работу какого-либо предприятия без использования цифровых технологий. Часть из них направлена на организацию непосредственно операционной деятельности компании, часть — на организацию учета и документооборот, часть — на взаимодействие с клиентами. Чем крупнее организация, тем

¹ 1С:ITIL IUM — выпуск нового продукта. Исключение 1С:ITIL из прайс-листа / 1С. 2023. 29 дек. URL: [https://solutions.1c.ru/news/981218/#:~:text=Продукт 1С AITIL IUM разработан и в других функциональных областях \(дата обращения: 15.05.2024\).](https://solutions.1c.ru/news/981218/#:~:text=Продукт 1С AITIL IUM разработан и в других функциональных областях (дата обращения: 15.05.2024).)

более обширный и разнообразный набор информационных технологий она использует для своей деятельности [2]. Многие компании объединяют функционал различных обслуживающих информационных систем в единый комплекс, обеспечивающий наиболее полное сопряжение всех рабочих блоков за счет доступа к единым базам данных и сведениям об изменениях в процессе и результатах функционирования.

Одной из важнейших задач, стоящих в этих условиях перед компаниями, становится грамотное распределение кадров для решения всех видов рабочих задач предприятия [1]. Для распределения трудовых ресурсов можно использовать задачу назначения персонала, позволяющую математически обоснованно определить соответствие между работами и выполняющими их работниками таким образом, чтобы не только учесть конкретные условия организации работ, но и достичь заранее поставленной цели.

Для решения задач назначения персонала используется общий подход к поиску оптимального решения, базирующийся на использовании симплексного метода. Симплекс-метод относится к арсеналу методов математического программирования и осуществляется с помощью матричных операций на основе алгоритма последовательного выбора базисных строк и столбцов с тем, чтобы в конечном счете определить оптимальный набор. Решение может быть получено как с помощью ручных матричных расчетов, так и с помощью программных пакетов. Однако многие из них выдают в качестве результата лишь основное решение, не выводя данных для анализа устойчивости решения.

Для примера рассмотрим задачу распределения программистов.

На фирме по разработке программного обеспечения на условиях совместительства работают 12 программистов. У каждого из них своя производительность и, соответственно, почасовая оплата труда. Все программисты работают автономно. Данные о производительности и почасовой оплате труда каждого из программистов приведены в табл. 1.

Т а б л и ц а 1

Производительность и оплата труда работников

Работник	Производительность в час (строк кода)	Оплата в час (р.)
Программист 1	163	440
Программист 2	132	370
Программист 3	86	310
Программист 4	193	490
Программист 5	25	180
Программист 6	122	370
Программист 7	119	340
Программист 8	35	190

Работник	Производительность в час (строк кода)	Оплата в час (р.)
Программист 9	63	250
Программист 10	204	510
Программист 11	211	520
Программист 12	28	170

Фирма получила заказ на разработку пяти программных продуктов. Оценены предположительные объемы программ (в строках кода):

- программа 1 — 3 000;
- программа 2 — 19 000;
- программа 3 — 9 900;
- программа 4 — 17 100;
- программа 5 — 4 900.

Необходимо определить, кому из программистов лучше поручить разработку программ в случае, когда: а) фирма хочет минимизировать общее время на разработку программ; б) фирма хочет минимизировать расходы на оплату труда программистов.

При известных объемах кода, который нужно написать, зная производительность труда всех программистов, несложно рассчитать время, которое понадобится каждому из них для написания любой из программ. А при известной ставке почасовой оплаты легко вычислить сумму оплаты за каждую программу. Опираясь на эти величины, можно записать формулы для расчета общего времени, которое затратят все программисты на написание всех программ, а также общей суммы оплаты их труда. Именно эти значения нужны для математической постановки цели данной задачи — для записи целевой функции.

Собственно решением в этом случае будет таблица распределения программистов по выполняемым заданиям. Поскольку индивидуальные показатели затрат времени и получаемой оплаты рассчитаны заранее, то в качестве значений переменных, являющихся решением, вполне достаточно признака выполнения работы. Поэтому логичным является выбор — в качестве управляемых — бинарных двухиндексных переменных x_{ij} , принимающих значение «1» в случае поручения программисту i задачи j и «0» — в случае, если программист i данную программу j писать не будет. Очевидно, что количество управляемых переменных зависит от числа программистов n и числа задач m и представляет собой произведение $n \times m$ ($i = 1, \dots, n; j = 1, \dots, m$).

В случае, когда задача является закрытой ($n = m$), каждый программист будет занят на разработке одной программы, и все программы будут написаны. Если же, как в нашем примере, задача открытая ($n \neq m$), необходимо введение дополнительных переменных, отражающих фик-

тивные работы или фиктивных работников — наличие единичного признака в таких переменных показывает недостаток или, наоборот, избыток работников для выполнения запланированных работ. В принципе можно избежать введения фиктивных переменных в математическую модель, учтя неравнозначность n и m в ограничениях задачи.

При отсутствии дополнительных условий на выполнение комплекса работ, задача назначения персонала будет содержать лишь два вида ограничений. Одно из них касается работников и отражает условие, что каждый работник выполняет только одну работу (в нашем случае, каждый программист разрабатывает только одну программу). Математически это можно выразить как равенство единице суммы выполняемых конкретным программистом заданий (сумма по строке исполнителя). Второй вид ограничений относится к работам (программам) и отражает условие, что каждая программа разрабатывается лишь одним программистом (сумма по столбцу работы должна быть равна единице). Дополнительно задаваемым ограничением является условие бинарности, накладываемое на управляемые переменные x_{ij} .

Для решения задачи назначения персонала можно использовать симплекс-метод, традиционно применяемый для поиска оптимального решения — наилучшего среди множества возможных. Для нашего примера численное решение для случая минимизации общего времени на разработку комплекса программ приведено табл. 2.

Таблица 2

**Численное решение
при условии оптимизации общего времени разработки**

Работник	Программа				
	1	2	3	4	5
Программист 1	0	0	0	0	1
Программист 2	1	0	0	0	0
Программист 3	0	0	0	0	0
Программист 4	0	0	1	0	0
Программист 5	0	0	0	0	0
Программист 6	0	0	0	0	0
Программист 7	0	0	0	0	0
Программист 8	0	0	0	0	0
Программист 9	0	0	0	0	0
Программист 10	0	0	0	1	0
Программист 11	0	1	0	0	0
Программист 12	0	0	0	0	0

Величина целевой функции (общее время на разработку комплекса программ) составила в этом случае 227,95 ч.

Как видно из полученного решения, оптимальное (по времени) распределение представляет собой таблицу соответствия программ работникам. Здесь:

- разработчик программы 1 — программист 2;
- разработчик программы 2 — программист 11;
- разработчик программы 3 — программист 4;
- разработчик программы 4 — программист 10;
- разработчик программы 5 — программист 1.

Таким образом, все необходимые программы имеют разработчиков. Однако поскольку у нас открытая задача, то некоторые программисты оказались не задействованы в выполнении данного комплекса. Видно, что в нашем случае не будут работать над его выполнением программисты 3, 5, 6, 7, 8, 9, 12.

Здесь при определении оптимального распределения использовалась функция суммы произведений управляемых переменных на время написания программ каждым из программистов. Общее время минимизировалось. В случае, если необходимо математически оптимизировать другую цель, т. е. достичь максимума или минимума другого показателя, целевая функция будет включать в себя сумму произведений значений этого показателя на переменные x_{ij} . Например, при оптимизации фонда оплаты труда программистов минимальное возможное значение в условиях нашего примера составило 136 345,44 р.

Вообще в качестве целевой функции задачи назначения персонала может быть выбран практически любой показатель, достижение оптимального значения которого является критически важным для компании. В более сложных, комплексных случаях может быть поставлена задача многокритериальной оптимизации, которая решается в два этапа, на первом этапе оптимизируется один из заданных параметров, а на втором — его оптимальное значение используется в качестве ограничения.

Задача оптимального распределения трудовых ресурсов является довольно универсальной в смысле возможностей введения в математическую модель дополнительных ограничений, накладываемых на деятельность предприятия. При этом очевидна актуальность подобной задачи для большинства предприятий, особенно крупных, где число решаемых производственных задач и численность персонала не дают возможности выполнить оптимальное распределение без использования математических методов.

Библиографический список

1. Кочкина Е. М., Силин Е. А. Математическое моделирование в организации работы малого предпринимательства // Актуальные проблемы и тенденции

развития современной экономики и информатики: материалы Междунар. науч.-практ. конф. (Бирск, 22–24 ноября 2023 г.). Бирск: УУНиТ, 2023. С. 88–91.

2. *Панов М. А.* Перспективы роста национальной и региональной экономики в условиях кризиса // Вестник Челябинского государственного университета. 2022. № 6 (464). С. 94–105.

Н. В. Сербина

Уральский государственный экономический университет, г. Екатеринбург

Платформенная занятость студентов как старт в профессию

Аннотация. В статье поднимаются вопросы, связанные с кадровым дефицитом на рынке труда молодых специалистов и нежеланием работодателей предлагать студентам-выпускникам без профильного опыта работы достойные условия трудоустройства. Рассматриваются преимущества платформенной занятости как возможности получения навыков по выбранной профессии и как инструмента трудовой социализации студентов.

Ключевые слова: занятость студентов; трудоустройство выпускников; платформенная занятость; молодые специалисты.

Актуальность. Вопросы трудоустройства выпускников вузов и колледжей не теряют своей актуальности даже на фоне современного дефицита трудовых ресурсов. С одной стороны, при прочих равных характеристиках потенциальных сотрудников компании предпочитают выбирать более опытные кадры. Декларируемый работодателями курс на привлечение и удержание молодых специалистов еще не принес ощутимых результатов. Для подавляющего большинства российских компаний кадровый голод остается острой проблемой. С другой стороны, активное развитие нового сегмента рынка труда — платформенной занятости — повлекло за собой перераспределение трудовых ресурсов. Благодаря привлекательным условиям трудоустройства и низкому порогу вхождения этот формат занятости притягивает все большее внимание соискателей работы, в том числе целевой группы — студентов старших курсов без опыта работы и выпускников профессиональных учебных заведений, что задает актуальность заявленной темы.

Цель исследования — изучение возможностей, которые предлагает формат платформенной занятости студентам старших курсов для получения первого опыта профессиональной деятельности. Для достижения поставленной цели необходимо было решить ряд задач: проанализировать ситуацию на рынке труда и условия трудоустройства молодых специалистов без опыта работы, исследовать потребности данной целевой группы касательно трудоустройства и карьерного продвижения, оценить потенциал платформенной занятости как технологии получения студентами первого профессионального опыта.

Степень изученности. Являясь одним из трендов современного рынка труда, платформенная занятость находится под пристальным вниманием и государства, и общества. Этот новый вид отношений между экономически активными гражданами и цифровыми платформами изучают эксперты из различных отраслей гуманитарного знания. Количество трудов, посвященных платформенной занятости, постоянно растет, и они связаны с вопросами структуры платформенной занятости, гендерного состава ее участников, степени их социальной защищенности, проблемой правового регулирования и т. д. Важно, что потенциал платформенной занятости и ее последствия для рынка труда и экономики в целом еще досконально не изучены и требуют дополнительных исследований. Практическая значимость работы продиктована потребностью трудовой социализации и повышения конкурентоспособности студентов-выпускников как потенциальных сотрудников и получения ими первого профессионального опыта уже во время обучения в вузе, облегчая тем самым дальнейший выход на рынок труда.

Согласно данным Росстата за 2022–2023 гг., количество работников возрастной группы до 35 лет сократилось на 1,3 млн чел., и, по мнению экспертов, в ближайшие 5–7 лет новых кадров будет еще меньше, а спрос на них продолжит расти¹.

На профильных мероприятиях, посвященных актуальным кадровым вопросам, работодатели все чаще говорят о нехватке молодежи и об усилиях, которые они предпринимают для привлечения молодых специалистов. Чаще всего звучат проекты по сотрудничеству с учебными заведениями, организации стажировок и конкурсов, трансформации корпоративной культуры под потребности поколения Z и т. д.

Однако, как показало исследование, проведенное hh.ru в январе 2024 г., для молодых специалистов подходят не более 9 % представленных на рынке вакансий. Это предложения в сферах продаж — до 47 % от общего количества вакансий без опыта работы; логистика и розничная торговля — по 27 %; административный персонал — до 22 %². Среди вакансий с постоянной занятостью лидируют предложения по профессиям менеджера по продажам, секретаря и учителя; среди вакансий на подработку — исключительно неквалифицированные профессии — курьера, оператора, упаковщика или официанта.

¹ Численность населения Российской Федерации по полу и возрасту / Федеральная служба государственной статистики. URL: <https://rosstat.gov.ru/compendium/document/13284> (дата обращения: 04.04.2024).

² Рынок труда молодых специалистов: итоги 2023 года / Head Hunter. URL: <https://ekaterinburg.hh.ru/article/32301> (дата обращения: 05.04.2024).

При этом студенты старших курсов, обучающиеся по программам профессионального образования, чаще всего не склонны рассматривать неквалифицированные профессии. Их запросы на построение карьеры включают быстрое вхождение в выбранную специальность, в то время как работодатели не готовы обучать и мотивировать молодежь, о чем свидетельствуют результаты опроса, проведенного в конце 2023 г. компанией Kontakt Intersearch Russia среди 410 компаний и 395 студентов¹.

Подобного мнения придерживаются и рекрутинговые агентства, сотрудничающие с малыми и средними компаниями: у работодателей нет ресурсов временных и финансовых, чтобы обучать молодых специалистов и им гораздо проще нанять опытных сотрудников [2]. Таким образом, значительное число работодателей не могут предложить выпускникам достойные условия первого трудоустройства, объясняя свою позицию отсутствием у последних профессионального опыта, а сами выпускники нацелены на совсем другой уровень работы, подразумевающий и включенность в бизнес-процессы компании, и возможности творческого подхода к деятельности, и более высокий уровень ответственности.

Важной особенностью молодых специалистов поколения Z является их потребность ощущать значимость своей работы, своего вклада в общее дело: более 42 % выпускников стремятся к экспертному профессиональному развитию и предпочитают выбирать небольшие компании в качестве первого работодателя [1].

С этой особенностью поколения Z связаны и проблемы удержания молодых специалистов в компаниях. Зачастую ценности и ориентиры работодателей не находят отклика в сердцах молодежи, а устоявшаяся практика мотивации не работает, что приводит в итоге к увольнениям и текучести молодых кадров. Новые ценности, клиповость мышления, многозадачность, погруженность в цифровой мир и про-активная позиция поколения Z вынуждают их искать иные, нетрадиционные форматы трудоустройства, с более гибким графиком и балансом работы и отдыха, с широкими возможностями самовыражения и географической мобильности.

Пандемия 2020 г. спровоцировала масштабный переход компаний на удаленный формат работы и дала мощный импульс для развития платформенной или гиг-экономики. В 2022 г. по данным Росстата в платформенную занятость были вовлечены 3,5 млн чел., из них: для 1,7 млн чел. она являлась основной, еще для 1,7 млн чел. — регулярной

¹ Рынок труда молодых специалистов: итоги 2023 года / Head Hunter. URL: <https://ekaterinburg.hh.ru/article/32301> (дата обращения: 05.04.2024).

подработкой¹. В 2023 г. число занятых на цифровых платформах увеличилось до 5 млн чел.; к 2024 г. она стала основным источником дохода для 79 % респондентов; для 90 % опрошенных платформенная занятость приносит более половины их дохода².

В рамках современного проектного подхода к бизнес-процессам для многих компаний стало актуальным создание временных рабочих команд с особыми гибкими условиями сотрудничества; привлечение на временные проекты фрилансеров стало привычным делом. Агрегируя в едином пространстве информацию о заказах и исполнителях, цифровая платформа предлагает своим пользователям технологические решения для коммуникаций, внедряет банковские и страховые инструменты для обеспечения скорости и эффективности взаимодействия.

Легкость регистрации на платформе, отсутствие привязки к фиксированному графику и месту работы, значительная клиентская база — все это дает выбор и большую свободу, нежели работа в офисе. Среди платформенных занятых есть те, кто реализует свои предпринимательские амбиции; те, кто испытывает сложности на традиционном рынке труда (к примеру, пенсионеры или молодые мамы); и есть те, кому нужен дополнительный доход.

Важно, что уже во время обучения с помощью платформенной занятости студент может не только попробовать свои силы в выбранной профессии, самостоятельно выбрав заказ и комфортные для себя условия, но и получить за свою работу достойное вознаграждение. К основным преимуществам платформенной занятости относятся [2]:

- гибкие условия труда: самостоятельное планирование рабочего времени и рабочего места, что позволяет начать профессиональную карьеру еще до получения диплома об образовании;
- финансовые возможности: самостоятельная оплата своего профессионального обучения как альтернатива образовательному кредиту;
- комфортные условия и низкий порог для «вхождения» в профессию — как «первое рабочее место»;
- географическая мобильность и цифровое кочевничество: отсутствие вынужденной «привязки» к конкретному региону, возможность путешествовать и открывать для себя мир;
- преимущества предпринимательской карьеры и запуска своего микробизнеса без больших вложений и затрат;
- легкая смена профессиональной траектории: возможность попробовать себя в разных профессиях и экономических ролях;

¹ Численность населения Российской Федерации по полу и возрасту / Федеральная служба государственной статистики. URL: <https://rosstat.gov.ru/compendium/document/13284> (дата обращения: 04.04.2024).

² Там же.

– соблюдение баланса работы и семьи: возможность совмещения молодыми родителями работы, профессионального развития и воспитания детей.

Таким образом, как бы ни были различны представления о ценностях жизни и смысле трудовой деятельности у работодателей и студентов-выпускников поколения Z, последним нужен дополнительный источник дохода и возможность получить рабочий опыт еще до окончания учебы. Как вариант первичной трудовой социализации формат платформенной занятости снимает указанную проблему. К «слабостям» платформенной занятости пока еще относится недостаточная правовая защищенность участников данного сегмента рынка, однако в этом направлении уже делаются соответствующие шаги. Результаты масштабного опроса самозанятых, проведенного сервисом медиахолдинга Rambler & Co в конце 2023 г., показали, что: 18 % респондентов нужна работа по специальности, дополняющая их учебу, а еще 17 % респондентов ожидают от платформенной занятости достижения самостоятельности и независимости от родителей¹.

Вывод. Масштабное распространение цифровых технологий и их проникновение в разные сферы нашей жизни трансформировало существующие экономические системы, оказав влияние на трудовые и социальные отношения. Выделение нового сегмента рынка труда — платформенной занятости, позволило значительно расширить традиционные форматы взаимодействия работодателей и работников. Учитывая рост потребности работодателей в опытных сотрудниках, для студентов-выпускников надежным способом получения первого практического опыта работы по выбранной профессии является платформенная занятость. Платформенная занятость предполагает ряд существенных преимуществ перед традиционной: самостоятельность в планировании времени, в интенсивности труда, ощущение свободы, отсутствие жестких организационных рамок и схем, отсутствие дискриминации по оплате труда в привязке к опыту. Все это соответствует ценностям поколения Z и стимулирует студентов и молодых специалистов к этой форме взаимодействия с работодателем.

Библиографический список

1. Колесник Е. А. Платформенная занятость в структуре стратегий занятости молодежи // Государственная молодежная политика: практики и стратегии:

¹ Для 90 % платформенных занятых эта работа основной источник дохода / Центр стратегических разработок. 2024. 25 янв. URL: <https://www.csr.ru/ru/news/dlya-90-platfornennykh-zanyatykh-eta-rabota-osnovnoy-istochnik-dokhoda/> (дата обращения: 04.04.2024).

материалы Междунар. науч.-практ. конф. (Новосибирск, 2–3 июня 2022 г.). Новосибирск: Изд-во СибАГС, 2023. С. 72–76.

2. *Сербина Н. В.* Актуальные вопросы цифровой занятости для студентов вузов // Социально-политические науки. 2023. Т. 13, № 6. С. 112–118.

Д. Н. Смирнова

Уральский государственный экономический университет, г. Екатеринбург

Технологии формирования геометро-графических навыков в дистанционном формате

Аннотация. В статье автор представляет методики формирования геометро-графических навыков в дистанционном формате. Исследование включает в себя как отечественные, так и зарубежные мнения ученых-педагогов. Автор приходит к выводу, что невозможно эффективно развивать геометро-графические навыки полностью в дистанционном формате, однако, используя определенные методики, часть занятий можно сделать более эффективными, чем в офлайн-формате.

Ключевые слова: геометро-графические навыки; дистанционное обучение; методики преподавания дистанционно; инженерия; высшее образование.

Сегодня актуальность преподавания в дистанционном формате наиболее высока. Прошедший период масштабных локдаунов показал нам, что удаленное обучения можно реализовать на всех его этапах.

Однако определенные трудности испытали преподаватели высших учебных заведений в отдельных дисциплинах. К таковым относятся предметы, связанные с развитии геометро-графических навыков: начертательной геометрии, инженерной графики и т. д. Это обусловлено тем, что обучение данным дисциплинам тесно связано с использованием наглядного материала, примеров, макетов, эскизов и т. д.

Для инженеров крайне важно не только визуально изучить деталь, но и «почувствовать» материал.

В данной статье мы отразим различные технологии, которые уже спешно используют как в мировой, так и в отечественной практике для дистанционного преподавания дисциплин связанных с получением геометро-графических навыков.

Отметим, что на выбор программного продукта для организации видеоконференцсвязи со студентами и передачи контента в режиме реального времени в период удаленного доступа повлияли методические указания образовательной организации, доступность программного продукта в бесплатной версии, личные предпочтения преподавателя и другие факторы [2].

Самыми популярными решениями были Zoom, Microsoft Teams и др. Для проведения дистанционного занятия требуется четкая струк-

тура урока и определенные правила. Они доводятся до сведения участников заранее: порядок включения/выключения микрофонов и видео, поддержка чата для обратной связи, при необходимости видеозапись. Цифровой формат лекций и практических занятий привел к использованию таких программных продуктов, как:

- menti.com, pollev.com, wooclap.com;
- nowcomment.com, perusal.com для цифрового взаимодействия;
- Canva — онлайн-сервис презентаций и многое другое.

Как утверждают ученые Bircham International University, дистанционное высшее образование не лучший вариант для исследовательских или инженерных должностей в области высоких технологий, которые обычно требуют традиционно аккредитованных квалификаций. Программа дистанционного обучения не может предлагать возможности личного участия в инженерных, архитектурных или научных проектах. Однако это не исключает возможности проведения ряда занятий в дистанционном формате.

Как отмечают в своей статье Р. Р. Анамова и Г. К. Хотина, для эффективного развития геометро-графических навыков в рамках преподавания необходимо использовать следующие методики:

- 1) методика, которая включает в себя использования современные, инновационных технологий с возможностью демонстрации реалистичных изображений;
- 2) методика, которая включает в себя возможность демонстрации виртуальных реалистичных моделей;
- 3) методика, благодаря которой можно будет реализовать показ изделий, деталей онлайн с высокой четкостью;
- 4) методика, основанная на интерактивных 3D-дизайнах [1].

В статье Z. N. Khan [4] предлагают использование онлайн-лабораторий для построения эффективного обучения геометро-графических навыков. Так, инженерные лаборатории являются неотъемлемой частью инструкций, которые требуют практического применения фундаментальных понятий, изученных в классе.

Такие лабораторные среды, искусственно создаются через Интернет, чтобы предоставить студентам все основные инструменты для проведения лабораторных работ. Существует множество таких моделей, например, разработка и реализация интерактивной виртуальной лаборатории системы управления для студентов бакалавриата по электротехнике и вычислительной технике. Такие платформы также реализованы для интерактивного испытательного стенда для двигателей постоянного тока, чтобы продемонстрировать фундаментальные концепции мехатроники [3].

Сегодня использование виртуальных лабораторий способно объединить студентов и преподавателей со всего мира, и даже если границы будут закрыты, совместные разработки могут продолжаться, как в рамках учебной деятельности, так и научной.

Отметим, что в основном поставщики программного обеспечения для создания онлайн лабораторий — зарубежные компании, что в свете геополитических событий может негативно сказаться на его поставках. Это обуславливает необходимость разработки отечественного обеспечения.

Практически все методики необходимые для эффективной реализации программ дистанционного обучения требуют определенного программного продукта, однако, не всегда он отвечает требованиям стандартов образования. Для того, чтобы исключить это, программное обеспечение следует разрабатывать в России, в строгом соответствии с рекомендациями Министерства образования.

Таким образом, использование информационных технологий в обучении геометро-графических навыков позволяет сделать процесс обучения более интерактивным, эффективным и доступным для студентов. Использование современных программных средств для создания и анализа геометро-графических моделей позволяет студентам лучше понять и применить теоретические знания на практике.

Поддержка видеороликов и видеоуроков также способствует более глубокому пониманию материала и помогает студентам освоить новые навыки и умения. Такой подход к обучению открывает новые возможности для самостоятельного изучения и повышения квалификации, что важно для развития профессионализма и конкурентоспособности выпускников.

Интеграция информационных технологий в образовательный процесс в области геометро-графических навыков в дистанционном формате имеет большой потенциал для улучшения качества обучения и повышения интереса студентов к данной дисциплине.

Библиографический список

1. *Анамова Р. Р., Хотина Г. К.* Методики и средства обучения для дистанционных занятий по геометро-графическим дисциплинам // Наука и школа. 2021. № 3. С. 137–153.

2. *Панов М. А., Бальцер А. А.* Системы дистанционного обучения // Цифровая экономика. Новое время — новые технологии. Росинфоком-2020: материалы VI Всерос. науч.-техн. конф. (Самара, 18 ноября 2020 г.). Самара: ПГУТИ, 2020. С. 92–93.

3. *Alves G. R., Fidalgo A. V., Marques M. A., Viegas C.* International Cooperation for Remote Laboratory Use / M. Nascimento, G. Alves, E. Morais (eds.) // Con-

tributions to Higher Engineering Education. Singapore: Springer, 2018. P. 1–31. DOI: 10.1007/978-981-10-8917-6_1.

4. Khan Z. H., Abid M. I. Distance learning in engineering education: Challenges and opportunities during COVID-19 pandemic crisis in Pakistan // International Journal of Electrical Engineering & Education. 2021. P. 1–20. DOI: 10.1177/0020720920988493.

И. А. Чечулин

Уральский государственный экономический университет, г. Екатеринбург

Перспективные траектории цифровой трансформации в сфере жилищно-коммунального хозяйства

Аннотация. Цифровая трансформация в ЖКХ находит свое отражение в повышении уровня открытости отрасли, качества принятия управленческих решений и платежной дисциплины населения через внедрение интеллектуальных приборов учета и сопутствующей инфраструктуры. Перспективным и недостаточно разработанным направлением цифровой трансформации является внедрение цифровых финансовых активов для реализации концессионных соглашений в ЖКХ. Автор делает обзор хода цифровой трансформации и дает рекомендации по наращиванию скорости ее проведения.

Ключевые слова: цифровая трансформация в ЖКХ; умные счетчики; стейкхолдеры проекта.

Введение. Коммунальный сектор является жизненно важным компонентом экономики, поскольку он ориентирован на предоставление основных услуг, необходимых для функционирования общества. Ее роль как поставщика ресурсов для всех других отраслей подчеркивает важность обеспечения ее экономической стабильности и внедрения инноваций, повышающих эффективность отрасли.

В 2007 г. по решению Президента РФ был создан Фонд содействия реформированию жилищно-коммунального хозяйства (далее — Фонд), который осуществляет функции по предоставлению финансовой поддержки для проведения капитального ремонта и переселения граждан. С 2013 г. средства Фонда также направляются на модернизацию систем коммунальной инфраструктуры и внедрение ресурсосберегающих технологических решений, что способствует улучшению жилищно-коммунального хозяйства в целом.

Комплекс показателей, учитываемых Фондом при реализации проектов концессионного финансирования, включает количественные и качественные показатели по профилю деятельности коммунального предприятия, однако не учитывает вопросы цифровой трансформации [5], что создает предпосылки к повышению эффективности концессионных проектов в ЖКХ путем наращивания темпов внедрения современных цифровых решений.

Внедрение цифровых решений в ЖКХ может осуществляться по двум направлениям — внедрение интеллектуальных приборов учета и использование цифровых финансовых активов для финансирования инвестиционных проектов, рассмотрим их по отдельности.

Внедрение интеллектуальных приборов учета. С 1 июля 2020 г. ответственность за приборы учета электроэнергии перешла к гарантирующим поставщикам, на которых теперь возложена задача обеспечить их исправное функционирование. Это изменение привело к более эффективному подходу к выявлению неисправностей и обеспечению точных измерений. Кроме того, с 1 января 2022 г. начался плановый переход на интеллектуальные приборы учета, использующие технологии телеметрии. Однако важно отметить, что данное нововведение не коснется других приборов учета, например, используемых для водоснабжения и канализации, а также газоснабжения. Кроме того, внедрение телеметрии теплоснабжения в некоторых случаях может быть нецелесообразным из-за вертикального расположения системы отопления во многих зданиях, что делает индивидуальный учет нецелесообразным в российских климатических условиях.

Однако в энергетике внедрение интеллектуальных приборов учета успешно реализуется в рамках программ инновационного развития, в частности в ПАО «МРСК Урала» эта программа была запущена в 2021 г. и рассчитана до 2030 г. Доля импортных поставок составляет всего 3,97 %¹, что обеспечивает относительную стабильность затрат и успешную реализацию проекта.

Внедрение интеллектуальных приборов учета производится в рамках реализации цифровой трансформации одновременно по нескольким направлениям, которые взаимодополняют друг друга и включают в себя:

- переход к цифровым подстанциям различного класса напряжения;
- переход к цифровым активно-адаптивным сетям с распределенной интеллектуальной системой автоматизации и управления;
- использование данных цифровых подстанций и сетей для принятия управленческих решений в режиме реального времени.

Переход на цифровые подстанции подразумевает не только наличие локальной системы контроля и управления, но и создание протоколов передачи данных по стандарту МЭК 61850². Внедрение приводит

¹ *Годовой отчет* Открытого акционерного общества «Межрегиональная распределительная сетевая компания Урала» за 2022 г. (утв. протоколом от 9 июня 2023 г. № 20). URL: <https://rosseti-ural.ru> (дата обращения: 09.04.2024).

² *ГОСТ Р* МЭК 61850-5-2011. Сети и системы связи на подстанциях. Часть 5. Требования к связи для функций и моделей устройств (перизд.) (дата введ.: 1 апреля 2020 г.).

к снижению эксплуатационных затрат за счет увеличения интервалов ремонта, использования низкочастотного оборудования, сокращения времени восстановления работы сети, уменьшения вероятности аварий и повреждений, применения системы определения места повреждения и удаленного управления коммутационными аппаратами. Информационная безопасность при такой схеме приема, обработки и ретрансляции данных обеспечивается применением на серверах сбора данных межсетевых экранов и средствами антивирусного контроля [3].

Отметим наличие институционального фактора реализации проектов внедрения цифровых подстанций, заключающегося в недостаточной конкретности требований стандарта МЭК 61850, что оставляет большую свободу для сторон проекта. Этот фактор оценивается исследователями по-разному, как с положительной [4], так и с отрицательной [2] точки зрения.

Интеллектуальные приборы учета позволяют в режиме реального времени контролировать потребление электроэнергии, данные передаются в диспетчерский центр сетевой компании и отображаются потребителю на электронном дисплее. Использование двустороннего обмена данными через GSM/GPRS позволяет точно контролировать процесс подачи электроэнергии, оперативно выявлять технические потери и попытки хищения электроэнергии.

Одновременно производится реконструкция вводов в жилые дома с заменой провода старого поколения на самонесущий изолированный провод, что обеспечивает более качественное электроснабжение и сводит к минимуму возможность несанкционированного подключения и позволяет дистанционно ограничивать и восстанавливать электроснабжение.

Помимо непосредственно повышения качества и своевременности принятия управленческих решений, цифровая трансформация способствует формированию «зрелого собственника» жилой недвижимости, с высокой платежной дисциплиной, осуществляющего осознанное потребление и добросовестно реализующего своим права и обязанности.

Цифровые финансовые активы в ЖКХ. Выпуск и обращение цифровых финансовых активов представляют собой новое явление на финансовом рынке, которое открывает перед инвесторами и компаниями новые возможности для финансовых операций и инвестиций. Основным преимуществом цифровых финансовых активов является их основа на технологии распределенных реестров, также известной как блокчейн. Применение смарт-контрактов позволяет автоматизировать исполнение сделок, повысить уровень прозрачности взаимоотношений различных групп стейкхолдеров в ЖКХ, что уменьшает риски и упрощает процесс выполнения финансовых операций.

Технология блокчейн позволяет хранить информацию о каждой сделке в цепочке блоков, которая не может быть изменена без согласия всех участников сети. Это снижает риски манипуляции данными и обеспечивает высокий уровень доверия к финансовым операциям. Кроме того, технология блокчейн позволяет упростить процесс обращения цифровых финансовых активов, так как все сделки могут быть автоматически исполнены с помощью смарт-контрактов. Это уменьшает необходимость участия посредников в финансовых операциях, что снижает издержки и ускоряет процесс обращения цифровых финансовых активов.

Обеспечением бесперебойного функционирования информационных систем, в которых осуществляется выпуск и учет цифровых финансовых активов, занимаются операторы информационной системы, которыми могут быть только российские юридические лица, включенные Банком России в реестр таких операторов¹.

Большой научный вклад в развитие института дистанционного финансирования внесло исследование Д. Е. Матыцина [1], которое в большей мере посвящено правовому регулированию взаимоотношений стейкхолдеров и обеспечению открытости и добросовестности посредством создания моделей договорных конструкций для участников сделок.

Для развития ЖКХ широко применяются инструменты концессионного финансирования, позволяющие объединить частный и государственный капитал, нарастить темпы обновления фондов и повысить качество оказания услуг.

Отсутствие широкого инструментария долгосрочных инвестиций в отечественной деловой практике отрицательно сказывается на привлекательности долгосрочного сбережения гражданами [6]. Использование цифровых финансовых активов поможет широкому кругу концессионных проектов в ЖКХ открыть доступ к накоплениям граждан и будет способствовать вовлечению большего числа жителей в долгосрочную и социально важную инвестиционную активность. Также преимуществом инвестиций в отрасль ЖКХ является прогнозируемость финансовых результатов за счет функционирования в условиях местных монополий и регулирования цен.

На данный момент цифровые финансовые активы еще не получили широкого применения в отечественной деловой практике, и для их активизации необходимо создание открытой онлайн-площадки инвестиционных проектов в сфере ЖКХ. Реализация такого проекта может быть осуществлена силами некоммерческого объединения участников

¹ *О цифровых финансовых активах, цифровой валюте и о внесении изменений в отдельные законодательные акты Российской Федерации: Федер. закон от 31 июля 2020 г. № 259-ФЗ.*

рынка оборота цифровых финансовых активов. При этом не потребуются внесение изменений в текущую законодательную базу.

Выводы. Можно заключить, что в России создана сильная институциональная база для проведения успешной цифровой трансформации ЖКХ, имеются технологические решения для наращивания объемов инвестиций в отрасль. Успешное развитие отрасли зависит от эффективного целеполагания заинтересованных сторон, транспарентности и инклюзивности взаимоотношений между ними.

Библиографический список

1. *Матыцин Д. Е.* Дистанционные инвестиционные сделки: регулирование взаимных интересов и защита прав участников: дис. ... д-ра юрид. наук: 5.1.3. Волгоград, 2023. 386 с.

2. *Никитин В. В., Эзирбаев Т. Б., Варавин А. С., Магомадов Р. А. М.* Практическая реализация требований серии стандартов МЭК 61850 на энергетических объектах России // Грозненский естественнонаучный бюллетень. 2022. Т. 7, № 2 (28). С. 118–127.

3. *Носенко А.* Реализация передачи телеметрической информации в протоколах стандартов МЭК 60870-5и МЭК 61850 по сетям сотовых операторов // Электроэнергия. Передача и распределение. 2022. № 4 (27). С. 8–13.

4. *Рябов С. И., Елфимов С. А., Гончаров Е. С.* Особенности организации цифрового обмена по МЭК-61850 // Colloquium-Journal. 2020. № 2-2 (54). С. 95–97.

5. *Чечулин И. А., Ткаченко И. Н.* Повышение кризисной адаптации малых предприятий сферы ЖКХ путем внедрения интеллектуальных приборов учета // Отходы и ресурсы. 2023. Т. 10, № 1. Ст. 41. DOI: 10.15862/45ECOR123.

6. *Ярин В. Ю.* Перспективы формирования личного инвестиционного бюджета физическими лицами // Вестник Алтайской академии экономики и права. 2023. № 6-2. С. 272–288.

Р. Д. Шатров

Уральский государственный экономический университет, г. Екатеринбург

Применение нейросетевых технологий для реализации искусственного интеллекта в видеоиграх

Аннотация. Рассматриваются основные подходы к реализации искусственного интеллекта в видеоиграх, сравниваются их преимущества и недостатки. Проводится анализ существующих кейсов применения нейросетей в видеоигровой индустрии, а также возможных новых методов применения данной технологии с развитием вычислительных мощностей.

Ключевые слова: нейросеть; искусственный интеллект; видеоигры.

Искусственный интеллект (ИИ) уже давно используется в видеоиграх для описания поведения неигровых персонажей, или NPC (non-

playable character)¹. Благодаря развитию технологий, сейчас разработчики могут использовать как классические алгоритмы, так и нейронные сети для реализации ИИ в играх.

Основным подходом к реализации ИИ в видеоиграх можно считать написание дерева алгоритмов (рис. 1), на основе которого NPC принимают решения внутри игрового движка.

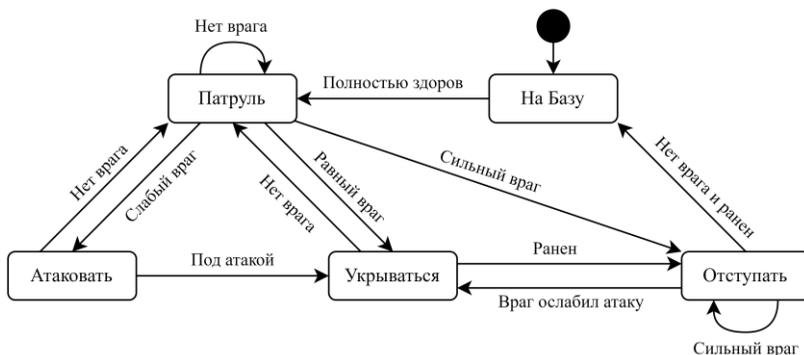


Рис. 1. Пример алгоритма для NPC вражеского солдата

Такой подход отличается простотой интерпретации, так как логика принятия тех или иных решений использует понятия для человека условия: если X, то Y. Это предоставляет возможность разработчикам легко изменять любые параметры поведения NPC, редактируя параметры условий или изменяя целые ветви дерева алгоритма.

Однако при большой сложности требуемой модели поведения NPC внесение изменений в такой алгоритм потребует от разработчика понимания работы всех аспектов модели поведения изменяемого NPC, что в свою очередь может понести большие временные затраты на разработку.

Другим существенным минусом такого подхода является производительность. Это выражается в необходимости последовательной проверки всех требуемых условий для принятия одного решения, а также в сложности параллелизации одновременной работы многих NPC, так как на аппаратном уровне вычисление дерева условий будет выпол-

¹ NPC / English meaning — Cambridge Dictionary. URL: <https://dictionary.cambridge.org/dictionary/english/npc> (дата обращения: 03.05.2024).

няться на центральном процессоре компьютера, которые зачастую будут иметь не больше 8 ядер¹.

Существует также альтернативный подход для создания ИИ — создание нейросетевой модели (нейросети) поведения NPC. Нейросеть представляет собой граф, в котором группы вершин разделены на «слои» и соединены с вершинами другой группы парными связями (рис. 2).

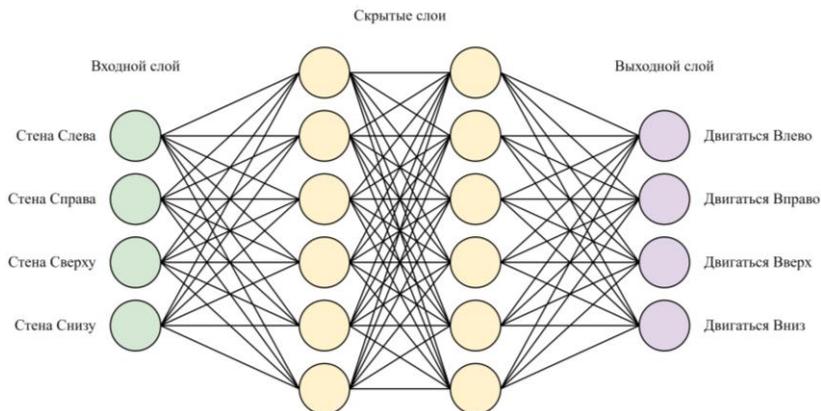


Рис. 2. Пример модели нейросети для прохождения лабиринта

Подобные нейросети строятся и оперируют по принципу работы биологических нейронных сетей — сетей нервных клеток живого организма, поэтому вершины в такой модели называются «нейронами», и, как живые нервные клетки, они имеют соединения с другим нейронами, представленные ребрами (парными связями) на графе. Парные связи в такой модели имеют определенный «вес» — числовое значение силы той или иной связи, которое задается без вмешательства разработчика при тренировке данной нейросети.

Тренировка нейросети происходит по принципу множественных проб и ошибок: в самом начале сеть будет использовать случайные веса и параметры для принятия решений. Те параметры, которые смогли приблизить сеть к искомому поведению, будут использованы вновь, но с небольшими случайными «мутациями» в новом поколении. Так будет повторяться до тех пор, пока сеть не достигнет модели поведения, вы-

¹ Данные об оборудовании и ПО пользователей: April 2024 / Steam. URL: <https://store.steampowered.com/hwsurvey/Steam-Hardware-Software-Survey-Welcome-to-Steam> (дата обращения: 03.05.2024).

полняющей все заданные разработчиком цели, или пока модель не перестанет совершать прогресс — в таком случае разработчику предстоит пересмотреть входные данные или изменить построение слоев. При успешно выполненной тренировке такая нейросеть сможет послужить основой искусственного интеллекта NPC, который будет принимать решения на основе построенных нейронных связей, вместо алгоритмов с условиями. При достаточном объеме и вариативности тренировочных данных, такой NPC сможет оперировать даже в незнакомых ему ранее окружениях.

Такой подход отбирает у разработчика опцию изменять параметры алгоритма поведения NPC — его алгоритм превращается в «черный ящик», содержимое которого невозможно интерпретировать человеком. Но в то же время открывается возможность создания самообучающейся сети, которая сама будет варьировать веса нейронных связей в зависимости от ее успешности достижения поставленных целей во время игрового процесса.

Ответная реакция на действия игрока и постоянно изменяющееся окружение — одни из самых сложных аспектов разработки ИИ в видеоиграх, которые практически нереализуемы с использованием алгоритмического подхода, поскольку разработчикам пришлось бы предсказать и запрограммировать все возможные состояния игры заранее. Один из ранних примеров использования нейросети для управления NPC стала гоночная игра «Colin McRae Rally 2.0», вышедшая в 2001 г.

Поскольку игра представляла из себя ралли-симулятор с различными типами дорожных покрытий и возможностью соревноваться сразу с несколькими соперниками, управляемыми компьютером, разработчиком было принято решение внедрить нейросетевую модель управления машиной, обученной проезжать по сложным извилистым трассам с разной степенью сцепления с дорогой и в то же время уходить от возможных столкновений с оппонентами, в том числе — с игроком. Обучение модели происходило при помощи записи вводов управления реальными людьми, тестирующих игру¹.

Нейросети также принесли пользу и другому жанру игры — стратегиям. Так, например, в игре «Supreme Commander 2» игрок и компьютер управляют военными отрядами на огромном поле боя, где соотношение сил сторон может поменяться в любую секунду. Для создания реалистичного игрового процесса разработчиками было принято решение использовать нейросеть, оценивающую соотношения всех доступ-

¹ *Ai-junkie*. URL: <http://ai-junkie.com/misc/hannan/hannan.html> (дата обращения: 03.05.2024).

ных игровых показателей «силы» отрядов (всего 17 показателей) и принимающую решения, опираясь на них¹. Такой подход позволил ИИ создавать свою стратегию войска, не опираясь на заранее запрограммированные действия и в то же время облегчил труд разработчиков.

Обучение и вычисление выходного слоя нейросети сводятся к решению множества линейных уравнений, что требует большого количества однотипных вычислений. Графические процессоры (ГП), благодаря большому количеству ядер и возможности эффективно обрабатывать параллельные задачи, позволяют проводить множество вычислений над большими наборами данных значительно быстрее, чем центральные процессоры.

С появлением технологии CUDA (Compute Unified Device Architecture) — архитектуры параллельных вычислений, разработанной компанией NVIDIA, для разработчиков открылась возможность использования графических процессоров для выполнения всевозможных математических расчетов, в том числе для создания сложных нейронных сетей, значительно сокращая время их тренировки и увеличивая их производительность².

В 2017 г. NVIDIA представила аппаратную разработку, направленную на увеличение производительности нейросетей глубокого обучения — тензорные ядра, встроенные в графические ускорители³. Данные ядра представляют собой математические сопроцессоры смешанной точности, специализирующиеся на матричной арифметике⁴.

По данным цифрового дистрибьютора игр «Steam» на январь 2024 г. 44,3 % пользователей имеют ГП с тензорными ядрами⁵, что свидетельствует о готовности рынка к использованию сложных ИИ с самообучающимися возможностями уже сегодня. Применение такой технологии способно создать реалистичное поведение неигровых персона-

¹ *Robbins M.* Using Neural Networks to Control Agent Threat Response. URL: https://www.gameaiopro.com/GameAIPro/GameAIPro_Chapter30_Using_Neural_Networks_to_Control_Agent_Threat_Response.pdf (дата обращения: 03.05.2024).

² *CUDA C++ Programming Guide.* URL: <https://docs.nvidia.com/cuda/cuda-c-programming-guide/index.html> (дата обращения: 03.05.2024).

³ *NVIDIA A100 Tensor Core GPU Architecture.* Unprecedented Acceleration at Every Scale. URL: <https://images.nvidia.com/aem-dam/en-zz/Solutions/data-center/nvidia-ampere-architecture-whitepaper.pdf> (дата обращения: 03.05.2024).

⁴ *Harris M.* CUDA 9 Features Revealed: Volta, Cooperative Groups and More / NVIDIA. 2017. May 11. URL: <https://developer.nvidia.com/blog/cuda-9-features-revealed/> (дата обращения: 03.05.2024).

⁵ *Данные об оборудовании и ПО пользователей: April 2024 / Steam.* URL: <https://store.steampowered.com/hwsurvey/Steam-Hardware-Software-Survey-Welcome-to-Steam> (дата обращения: 03.05.2024).

жей, а также существенно сократить время разработки при большом объеме переменных.

Однако возложение на нейросеть контроля над всеми аспектами ИИ может пагубно сказаться на качестве такой модели и сделает отладку практически невозможной, поэтому наиболее оптимальным подходом к разработке ИИ в таком случае будет смешанное использование традиционного набора логических алгоритмов и нейросетевых моделей с обменом данными в обе стороны.

Проблемы трансформации и риски цифрового общества

К. В. Аронов

Уральский государственный экономический университет, г. Екатеринбург

Этические и нормативные последствия искусственного интеллекта в банковском деле

Аннотация. Внедрение искусственного интеллекта (ИИ) в банковское дело открывает новые перспективы для повышения эффективности, персонализации услуг и управления рисками. Однако расширение использования ИИ сопровождается этическими и нормативными вызовами, требующими тщательного рассмотрения и регулирования. В статье анализируются ключевые этические проблемы, связанные с применением ИИ в банковской сфере, а также обсуждаются необходимые нормативные меры для обеспечения ответственного и этичного развития ИИ.

Ключевые слова: искусственный интеллект; ИИ; банковское дело; этика; регулирование; алгоритмическая предвзятость; прозрачность; конфиденциальность; ответственность.

Современный банковский сектор стремительно трансформируется под влиянием инновационных технологий, среди которых особое место занимает искусственный интеллект (ИИ) [2, с. 898]. Способность ИИ к анализу больших данных, прогнозированию и автоматизации открывает перед банками невиданные ранее возможности. ИИ уже сегодня используется для оценки кредитных рисков, предотвращения мошенничества, персонализации услуг и многого другого [3, с. 55].

Вместе с этими возможностями возникают и новые вызовы. Применение ИИ в банковском деле сопряжено с рядом этических и нормативных проблем, требующих внимания и решений. Без четкого понимания этих проблем и выработки соответствующих регуляторных мер мы рискуем столкнуться с негативными последствиями для как для банковской системы, так и для общества в целом.

Одной из наиболее острых этических проблем, связанных с применением ИИ в банковском деле, является алгоритмическая предвзятость¹. Алгоритмы, на которых базируется работа ИИ, обучаются на огромных объемах данных. Если эти данные отражают существующие в обществе предубеждения и стереотипы, алгоритмы могут перенести их в свои решения, что приведет к дискриминации определенных групп

¹ *О предвзятости искусственного интеллекта* / Центр стратегических оценок и прогнозов. URL: <https://csef.ru/ru/nauka-i-obshchestvo/direction-topics/o-predvzyatosti-iskusstvennogo-intellekta-6459/> (дата обращения: 05.05.2024).

клиентов. Например, система оценки кредитоспособности может необоснованно отказывать в кредитах представителям определенных профессий или социальных групп, опираясь на усвоенные из данных стереотипы. Модели ИИ могут наследовать предубеждения от данных, на которые они обучены, потенциально приводящие к несправедливым или дискриминационным результатам при принятии решений. Например, системы ИИ, используемые в кредитной оценке, могут непреднамеренно увековечить существующее социальное неравенство.

Другой важной проблемой является непрозрачность работы алгоритмов ИИ¹. Сложность и недоступность для понимания принципов работы многих алгоритмов делает их решения непрозрачными для клиентов. Человек, получивший отказ в кредите или застрахованный по завышенной ставке, не всегда сможет получить понятное объяснение причин такого решения. Эта непрозрачность подрывает доверие к ИИ и создает почву для подозрений в нечестности и манипуляциях.

Нельзя забывать и о защите конфиденциальности данных [1]. ИИ в банковском деле оперирует огромным объемом личной информации о клиентах. Необходимо гарантировать безопасность этих данных и исключить их использование в целях, не предусмотренных законодательством и не согласованных с клиентами. Утечки конфиденциальных данных могут нанести репутационный и финансовый ущерб как банкам, так и их клиентам. Сбор и использование конфиденциальной финансовой информации должны быть обработаны ответственным и этическим образом.

Наконец, возникает вопрос об ответственности за решения, принимаемые ИИ². Если алгоритм допускает ошибку, приводящую к убыткам для клиента, кто должен нести за это ответственность? Разработчик алгоритма? Банк, использующий этот алгоритм? Или сам клиент, согласившийся на использование ИИ в обслуживании³? Ответственность за действия ИИ — сложный вопрос, требующий разработки новых правовых норм и механизмов.

Все вышеперечисленные проблемы и их возможные решения представлены в таблице.

Чтобы смягчить этические и нормативные риски, связанные с ИИ в банковском деле, финансовые учреждения могут создать этические руководящие принципы: реализовать четкие и всеобъемлющие этические

¹ *В чем сила: ждать ли гонки искусственного интеллекта между государствами?* / Embedika. URL: <https://embedika.ru/blog/likbez-ii/> (дата обращения: 05.05.2024).

² *Ответственность людей и решения искусственного интеллекта* // Хабр. 2021. 18 нояб. URL: <https://habr.com/ru/articles/589913/> (дата обращения: 05.05.2024).

³ Там же.

ские рекомендации, которые регулируют разработку и использование систем ИИ.

Ключевые этические и нормативные проблемы ИИ в банковском деле

Проблема	Описание	Возможные решения
Предвзятость	Алгоритмы ИИ могут воспроизводить предубеждения, заложенные в обучающих данных	Тщательный анализ данных на наличие предубеждений, использование методов коррекции, разработка этических принципов для разработчиков
Непрозрачность	Принципы работы алгоритмов ИИ могут быть непонятны для клиентов	Создание механизмов объяснения решений ИИ, повышение прозрачности алгоритмов, разработка понятных для пользователей интерфейсов
Конфиденциальность	ИИ в банковском деле оперирует огромными объемами личной информации о клиентах	Строгое соблюдение законодательства о защите данных, шифрование данных, строгий контроль доступа к данным
Ответственность	Необходимо определить, кто несет ответственность за ошибки, допущенные ИИ	Разработка правовых норм, определяющих ответственность за действия ИИ, создание механизмов расследования инцидентов

Проводить тщательное тестирование и валидацию. Строгое тестирование и проверка алгоритмов ИИ для обеспечения справедливости, точности и смягчения смещения.

Предоставлять прозрачность и подотчетность. Объяснить клиентам, как их данные используются системами ИИ, обеспечить четкие механизмы для возмещения.

Соблюдать регуляторы, чтобы понять развивающиеся правила, регулирующие ИИ в банковском деле.

Внедрение ИИ в банковское дело открывает огромные перспективы для повышения эффективности и улучшения качества услуг. Однако для того, чтобы эти перспективы реализовались в полной мере, необходимо решить ряд этических и нормативных проблем [3, с. 57]. Требуется обеспечить прозрачность работы алгоритмов, исключить дискриминацию в их решениях, гарантировать защиту конфиденциальности данных и разработать механизмы ответственности за действия ИИ. Решение этих задач потребует сотрудничества со стороны регуляторов, разработчиков ИИ, самих банков и общества в целом. Только при условии ответственного и этичного подхода ИИ сможет реализовать свой потенциал в банковском секторе, принеся пользу как банкам, так и их клиентам.

Этические и нормативные последствия ИИ в банковском деле являются значительными и требуют тщательного рассмотрения. Устойчивые решение этих проблем финансовые учреждения могут использовать как преобразующий потенциал ИИ, минимизируя связанные с ними

риски¹. Этическая и ответственная практика ИИ в конечном итоге укрепит цифровизацию (или диджитализацию) банка — это система мер, направленных на углубление сотрудничества с финансово-техническими начинаниями с целью достижения долгосрочных целей развития, связанных с внедрением инновационных методов работы, новых банковских продуктов и услуг для увеличения и расширения клиентской базы и повышения конкурентоспособности банка.

Библиографический список

1. *Денисьев А. И., Ковязин С. Л.* Искусственный интеллект защитит персональные данные пользователя // Научный аспект. 2023. № 5. URL: <https://na-journal.ru/5-2023-informacionnye-tehnologii/5218-iskusstvennyi-intellekt-zashchitit-personalnye-dannye-polzovatelya/> (дата обращения: 05.05.2024).

2. *Рябичева О. И.* Цифровизация розничных банковских услуг в Российской Федерации на современном этапе // Журнал прикладных исследований. 2021. № 6. С. 896–904.

3. *Солтаханов А. У., Захарова Д. С.* Развитие цифровых технологий в финансовых и кредитных организациях // Транспортное дело России. 2021. № 1. С. 54–57.

Научный руководитель: А. Ю. Коковихин,
кандидат экономических наук, доцент

Т. Р. Боднарук, Д. А. Сиваков

Уральский государственный экономический университет, г. Екатеринбург

Цифровая трансформация логистических предприятий на основе платформенных решений

Аннотация. В статье исследуется необходимость создания и развития платформенных решений в рамках цифровой трансформации логистического предприятия. Рассматривается и описывается уровень развития цифровых платформ логистики в России. Выделяются конкретные платформенные решения, применяемые в контейнерном бизнесе, их возможности и функции.

Ключевые слова: цифровая трансформация; цифровые платформы; логистика; сервис; программная среда; развитие; информационная система; контейнерный терминал.

В современном динамично развивающемся мире цифровая трансформация становится обязательным условием успешного ведения биз-

¹ *О предвзятости искусственного интеллекта / Центр стратегических оценок и прогнозов.* URL: <https://csef.ru/ru/nauka-i-obshchestvo/direction-topics/o-predvzyatosti-iskusstvennogo-intellekta-6459/> (дата обращения: 05.05.2024); *В чем сила: ждать ли гонки искусственного интеллекта между государствами? / Embedika.* URL: <https://embedika.ru/blog/likbez-ii/> (дата обращения: 05.05.2024).

неса, и логистическая отрасль не исключение. Компании сталкиваются с необходимостью адаптации к растущим потребностям и требованиям клиентов к качеству сервиса и к быстро меняющейся внешней среде, чтобы обеспечить свою конкурентоспособность, т. е. противостоять конкурентному давлению со стороны лидеров рынка. Одним из перспективных направлений цифровой трансформации предприятия является разработка и развитие цифровых платформ и решений, создающих возможности для совершенствования бизнес-процессов и более оперативного и эффективного взаимодействия между участниками логистической цепи.

Цифровая трансформация определяет внедрение платформенных решений как определенную систему взаимоотношений участников, которые реализуются в едином информационном пространстве при помощи использования различных цифровых технологий работы с данными, тем самым обеспечивая выгодность от взаимодействия, т. е. создавая ценность для всех сторон¹.

Цифровая трансформация по отношению к логистической инфраструктуре состоит в том, что все этапы логистической цепи, а также транспортное средство или другие объекты, задействованные в процессе предоставления услуг, должны быть оцифрованы и доступны в любое время в программной среде [4].

Актуальность темы обуславливается тем, что цифровые платформы будут приобретать все большее значение в логистике, позволяя малым, средним, более инновационным компаниям конкурировать на равных с признанными гигантами отрасли. В обозримом будущем борьба за формирование эффективных платформ и решений станет главным фактором, определяющим, какие предприятия все же добьются успехов, а какие потерпят неудачу в сфере цифровой логистики [3].

Цифровая платформа представляет собой информационную среду, которая объединяет различных участников товарно-денежных отношений, предоставляя им цифровое пространство для взаимодействия, обмена информацией и оказания услуг, а также сохраняет результаты кооперации в электронном виде².

По состоянию на 2024 г. рынок цифровых платформ в секторе логистики в России продолжает развиваться, так как в результате ухода западных вендоров начался усиленный переход к технологической не-

¹ *Подходы к определению и типизации цифровых платформ / АНО Цифровая экономика.* URL: https://files.data-economy.ru/digital_platforms_project.pdf (дата обращения: 24.04.2024).

² *Цифровые платформы / Высшая школа экономики.* URL: <https://hsbi.hse.ru/articles/tsifrovye-platfomy/> (дата обращения: 24.04.2024).

зависимости. Платформенные решения охватывают все больше новых сервисов: трекинг грузов и электронный документооборот, автоматический расчет стоимости, выставление счетов, поиск и подбор поставщиков транспортных услуг, отслеживание статусов и получение уведомлений, анализ данных для выявления областей для улучшения и создание настраиваемых отчетов и панелей мониторинга, а также другие сервисы, которые способствуют проникновению в отрасль цифровых форм взаимодействия¹.

Российские поставщики программного обеспечения предлагают цифровые логистические платформы — CARGO.RUN и xPlanet, которые объединяют работу грузовладельцев и перевозчиков в едином окне, обеспечивая вторым загрузку из любой точки страны на регулярной основе. Платформы производят поиск заявки под транспортное средство, передают всю информацию водителю, планируют и выстраивают оптимальный маршрут, отображают статусы заявки или указывают примерное время задержки, отправляют автоматические уведомления в систему, а также дублируют их на электронную почту. Таким образом, перевозчик даже с автопарком в одну или несколько транспортных средств может конкурировать с крупными транспортными компаниями на равных, а не заключать субподрядные договоры и терять прибыль².

Стоит отметить, что на текущий момент не во всех областях логистики есть универсальное платформенное решение, которое удовлетворяло бы потребности компаний и соответствовало их специфике деятельности. Тем не менее развитие технологий и рост спроса на цифровую трансформацию будут способствовать и в дальнейшем появлению новых инновационных и всеобщих программных сред, повышающих уровень прозрачности процессов цепей поставок³.

По результатам экспертного опроса, оценкам ИСИЭЗ НИУ ВШЭ, спрос на передовые цифровые решения в логистической отрасли к 2030 г. достигнет до 627 млрд р., что в 7 раз больше, чем в 2020 г. [2].

И хотя интерес к разработке и развитию логистических платформ набирает обороты, все же их внедрение требует тщательной подготовки и анализа бизнес-процессов, что неизбежно приводит к значительным инвестициям как в обучение персонала, так и в поддержку и обновление информационной системы, поэтому процесс может быть затянут, вызывая трудности в работе компании. В том числе их использование тре-

¹ *Отрасль стремительного роста: в чем феномен цифровой логистики / РБК Тренды.* URL: <https://clck.ru/3AZu7i> (дата обращения: 24.04.2024).

² *Как цифровая платформа xPLANET трансформирует логистику / РБК Отрасли.* URL: <https://clck.ru/3AaGWp> (дата обращения: 24.04.2024).

³ *Как цифровая трансформация в логистике повышает эффективность / Unitcode.* URL: <https://clck.ru/3AaJCK> (дата обращения: 24.04.2024).

бует обмена данными между стейкхолдерами, а это служит риском утечки конфиденциальной информации и нарушению приватности, если данные недостаточно защищены и безопасность поставлена под угрозу. Помимо этого, возможным риском для логистических предприятий является зависимость от деятельности самой цифровой платформы, которая может прекратить ее либо поменять условия пользования, например, изменение договора может повлечь за собой дополнительные затраты, которые компания не в силах нести. Потому есть предприятия, занимающиеся формированием персональных цифровых решений собственными силами, исходя из специфики своей деятельности [1].

В качестве примера динамически развивающегося бизнеса, основанного на формировании собственных платформ, можно привести контейнерный терминал «С.І.Т.»¹, предоставляющий полный комплекс услуг по обработке контейнеров и по организации их приема и отправки, хранению и комплектованию, в том числе услуг по перевозкам грузов в составе ускоренных контейнерных поездов.

В работе контейнерного терминала применяется уникальная программная среда собственной разработки с помощью платформы .NET Framework — СТМС (Container Terminal Management System, что переводится как система управления контейнерным терминалом), благодаря которой все процессы контролируются и учитываются в режиме online. Учет ведется по всем операциям с грузом и тарой: от прибытия или отправления поезда до перегруза груза в транспортное средство или на склад временного хранения, и до выпуска таможенным органом. В любой момент времени доступна информация о статусах контейнера или же о грузе, его состоянии и произведенных операциях с указанием ответственных на каждом из этапов. Кроме того, в настоящее время система интегрирована с платформой «ІС:Предприятие», с системами электронного документооборота, софтом ВЭД-склад. По мере дальнейшего развития цифрового продукта планируется его интеграция с информационной системой ОАО «РЖД», что обеспечит ускорение внутренних и внешних процессов терминала и улучшит коммуникацию с контрагентами.

Также система включает в себя сайт и личный кабинет, в которых клиенты получают исчерпывающую информацию и размещают заявки на оказание услуг. К примеру, им доступна информация о статусах или об операциях с контейнером на терминале в любое время суток, о тарифах и услугах или о состоянии очереди обслуживания, возможность резервирования временного слота. Реализуется ряд нововведений

¹ Контейнерный терминал «С.І.Т.» — новые технологии логистики. URL: <https://cit-ekb.ru> (дата обращения: 24.04.2024).

в online-информировании: оплата услуг прямо в личном кабинете, прогнозируемое время ожидания выполнения заявки за счет фиксации операций перемещения через мобильное приложение для планшетов рич-стакеров, которое указывает место, примерное время копки контейнера в стоке и другие функции.

Еще одним платформенным решением являются приложения для охраны и водителей. Первое позволяет с помощью камер и датчиков распознавать номер транспортного средства или контейнера и передавать данные в систему, а также уведомлять клиентов об их прибытии, а второе — взаимодействовать водителю с терминалом полностью в электронном виде, например, передавать, подписывать документы, не выходя из кабины, брать талон электронной очереди. Следующим этапом будет внедрение новой функции: оформление электронной транспортной накладной для полной цифровой кооперации.

Перечисленные цифровые решения — это результат активной, многолетней и самостоятельной разработки. Все они интегрируются как между собой, так и с приложениями контрагентов с помощью API и других технологий, что позволяет им обмениваться данными и создавать новые возможности для пользователей. А взаимосвязанные платформы в дальнейшем сформируют цифровую экосистему, что станет следующим шагом в цифровой трансформации.

Таким образом, платформенные решения становятся ключевым элементом в цифровой трансформации логистических предприятий ввиду того, что отрасль логистики стремительно развивается, а клиенты выдвигают все более высокие и жесткие требования. Это не просто тренд, а необходимость, диктуемая временем. Это движущая сила, которая позволяет малым или средним предприятиям выйти на новый уровень, предлагая инновационные сервисы, способные конкурировать наравне с ведущими игроками рынка. Они оптимизируют процессы и улучшают взаимодействие с партнерами и клиентами, но для успешной реализации нужна не только технология, но и готовность к трансформации.

Библиографический список

1. Тимофеева Т. Б., Оздоева Э. А. Анализ мирового опыта в создании цифровых платформ и связанных с ними рисков // Управление. 2020. Т. 8, № 3. С. 112–122.

2. *Цифровая трансформация отраслей: стартовые условия и приоритеты:* докл. к XXII Апр. Междунар. науч. конф. по проблемам развития экономики и общества (Москва, 13–30 апреля 2021 г.) / Г. И. Абдрахманова, К. Б. Быховский, Н. Н. Веселитская и др. М.: Изд. дом ВШЭ, 2021. 239 с.

3. Foma A. A. K., Mohammed I. Digital Transformation in the Logistics Industry. Jönköping International Business School, 2018. 56 p.

4. Gaponenko T., Hvoevskaya L. Digital transport platforms: reality and prospects // Transportation Research Procedia. 2022. Vol. 63. P. 1185–1191.

М. Р. Гарипов

Уральский государственный экономический университет, г. Екатеринбург

Макроэкономические проблемы цифровизации экономики

Аннотация. Обсуждение процессов цифровизации в общем и цифровой экономики в частности занимает сегодня ведущую позицию среди многих ученых и общественных деятелей. Мнения неоднозначны: одни утверждают, что процесс всеобщей цифровизации несет обществу пользу, другие видят в нем угрозу для дальнейшей экономической стабильности. В данном ключе актуальными становятся исследования, раскрывающие сущность цифровой экономики, ее методы, содержание и закономерности.

Ключевые слова: цифровая безопасность; информационные технологии; цифровизация экономики.

Цифровые технологии стремительно проникают в различные сферы общества и приводят к существенным изменениям в экономике. Цифровизация становится приоритетным направлением экономического развития большинства стран мира. В последние несколько лет общество наблюдает стремительную цифровую трансформацию практически всех сфер его жизнедеятельности. Повсеместное внедрение информационных технологий приводит к глобальным изменениям в сферах государственной политики, управления и экономики. Цифровизация экономики в настоящее время предполагает, помимо производства компьютеров, компьютерных систем и программных продуктов, создание цифровых платформ, предоставляющих бизнесу и населению координационные услуги, упрощающие деятельность участников рынка, облегчающие заключение сделок и проведение расчетов, улучшающие производительность труда и экономическое развитие в целом. На современном этапе развития информационных технологий нет единого определения понятия «цифровая экономика». В одних экономических исследованиях данное понятие укладывается в целую систему общественных отношений; в других определяется как часть мировой экономики, основанной на информационных подсистемах; у третьей группы авторов считается моделью совершенно новой ветви развития экономики и общества. Например, авторы монографии под редакцией профессора А. В. Бабкина считают, что цифровой экономикой является сфера деятельности, где основным производственным фактором представлена информация в цифровой форме, а ее обработка и применение

в большом объеме способствует повышению качества, продуктивности и эффективности в разных производственных отраслях, а также в сферах оборудования и технологий в процессе потребления, доставки, продажи и хранения продукции и услуг [1, с. 16]. Согласно программе развития, утвержденной правительством РФ, цифровая экономика представляет собой хозяйственную деятельность, ключевым фактором производства в которой являются данные в цифровой форме, и способствует формированию информационного пространства с учетом потребностей граждан и общества в получении качественных и достоверных сведений, развитию информационной инфраструктуры Российской Федерации, созданию и применению российских информационно-телекоммуникационных технологий, а также формированию новой технологической основы для социальной и экономической сферы¹. Таким образом, научные подходы к понятию «цифровая экономика» разделились на системный, определяющий ее как совокупность экономической деятельности, основанной на цифровых технологиях и их глобальном внедрении; и технологический, который сосредоточен на инновациях исключительно в производственных сферах. В российской и европейской экономике преобладает системный подход, американские компании идут по пути технологического развития.

В современных реалиях государственная политика разных стран сосредоточена на процессе цифровизации. Подтверждение можно найти в стратегиях и программах развития цифровой экономики, утвержденных правительствами большинства государств. Среди приоритетных секторов и направлений технологического развития рассматриваются: биотехнологии, разработка программного обеспечения, кибербезопасность, искусственный интеллект, базы данных, робототехника и др. Повсеместное внедрение цифровых технологий во многом оказывает положительное влияние на мировую экономику. Однако, анализ мировой ситуации показывает, что глобальная цифровизация может также приводить к проблемам международного уровня. Одной из основных проблем цифровизации в настоящее время является то, что современные экономики стран мира развиваются в ситуации нарастающего технологического разрыва между ними. Например, по данным доклада ООН о цифровой экономике (2019 г.) в развивающихся государствах доступ к Интернету имеет лишь каждый пятый житель, в то время как в высокоразвитых странах им пользуется большинство². В других областях

¹ *Об утверждении программы «Цифровая экономика Российской Федерации»:* распоряжение правительства РФ от 28 июля 2017 г. № 1632-р.

² *Доклад о цифровой экономике за 2019 г. «Создание стоимости и получение выгод: последствия для развивающихся стран».* Обзор / ООН. Женева, 2019. 16 с.

использования цифровых данных разрыв между государствами колоссальный. Страны со слабо развитым инновационным потенциалом в технологическом смысле находятся в отстающем положении в сравнении, например, с США и Китаем, которые обладают большей частью глобального рынка программных и ИТ-услуг, что позволяет им устанавливать контроль над некоторыми сегментами мировой высокотехнологичной продукции. Таким образом, в развивающихся странах наблюдается зависимость от зарубежных производителей технологий, что неминуемо создает угрозы развитию национальных экономик. Тем самым усиливается разбалансировка мировой экономики, что влечет за собой неравномерное распределение выгод от использования информационных технологий. Негативное влияние цифровизация оказывает и на рынок занятости, так как внедрение новых технологий влечет за собой сокращение потребности в рабочей силе. Перед обществом остро встают задачи, предполагающие развитие новых компетенций и навыков. Однако национальные системы образования многих стран мира не готовы к быстрым перестройкам, так как нуждаются в длительных процессах реформирования и модернизации, и в короткой перспективе не могут обеспечить открывающийся рынок труда специалистами с соответствующими профессиональными навыками. Наибольшему риску подвержены опять-таки развивающиеся страны, так как их экономики по многим аспектам не способны адаптироваться к происходящим трансформациям.

В Российской Федерации в развитии цифрового сектора также существует ряд проблем, которые могут препятствовать процессам цифровизации экономики. Опираясь на доклад НИУ ВШЭ к XXIII Ясинской (Апрельской) международной научной конференции по проблемам развития экономики и общества можно выделить следующие проблемы в развитии отрасли: наличие сильной зависимости от иностранного программного обеспечения, средств электроники и телекоммуникационного оборудования почти всех классов; рост стоимости инвестиционных ресурсов; нехватка квалифицированных ИТ-специалистов; недостаточность затрат на НИОКР, связанных с цифровыми технологиями; несостоятельность системы обеспечения экономической безопасности и рост киберпреступности [2].

Следует отметить, что процесс цифровизации российской экономики стремительно набирает обороты. В настоящее время страна достигла значительного прогресса в реализации проекта информационного государства в части создания электронного правительства, систем электронного документооборота, предоставления государственных услуг в электронной форме.

Таким образом, в научных публикациях концепция формирования цифровой экономики занимает ведущее место среди других экономических задач. К числу наиболее обсуждаемых на международных площадках проблем цифровизации мировой экономики относятся:

- рост технологического разрыва между государствами;
- неравномерное распределение получаемых доходов и преимуществ;
- усиление конкуренции и нестабильности в условиях взаимозависимости национальных экономик;
- постоянно меняющаяся рыночная ситуация и необходимость поиска решений для выстраивания новых бизнес-моделей;
- высокие темпы роста производственных и технологических процессов, требующие больших вложений в НИОКР;
- проблемы обучения и перепрофилирования кадров для трансформирующегося рынка труда;
- возрастающий уровень безработицы среди низкоквалифицированных профессий;
- проблемы, связанные с киберпреступностью.

Соответственно, цифровизация экономики в обязательном порядке влечет за собой глобализацию и рост взаимозависимости ее участников, требуя догоняющего развития всех областей жизнедеятельности.

С одной стороны, цифровая экономика способна повысить уровень образования нации, дать стимул для эффективного использования ресурсов, полностью автоматизировать государственные и бизнес-процессы. С другой стороны, при переходе к цифровой модели развития она должна быть взаимосвязана с реальной экономикой, так как ее развитие предполагает разработку мощной нормативной базы и технологических внедрений.

В первую очередь цифровизация требует увеличения затрат на проведение НИОКР и усовершенствование качества разработок в области отечественных программных продуктов. Уровень развития человеческого потенциала, кадровый резерв, экономически активное население — все это важнейшие факторы стимулирования развития цифровой экономики. Создание необходимого законодательства, поддержание необходимого уровня кибербезопасности также являются неотъемлемыми мерами в реализации проектов цифровизации экономики.

Библиографический список

1. *Формирование цифровой экономики и промышленности: новые вызовы* / А. В. Александрова, А. А. Алетдинова, У. В. Афтахова и др.; под ред. А. В. Бабкина. СПб.: Изд-во Политехнического ун-та, 2018. 659 с.

2. *Цифровая трансформация: ожидания и реальность: доклад НИУ ВШЭ: к XXIII Ясинской (Апрельской) международной научной конференции по проблемам развития экономики и общества, 2022 г. / Г. И. Абдрахманова, С. А. Васильковский, К. О. Вишневецкий и др.; ред. группа: Т. С. Зинина, П. Б. Рудник. М.: Изд. дом ВШЭ, 2022. 219 с.*

*Научный руководитель: А. Н. Головина,
доктор экономических наук, профессор*

О. Д. Головина

Уральский государственный экономический университет, г. Екатеринбург

Управление цифровым наследием: что происходит с нашими онлайн-аккаунтами после того, как мы уходим

Аннотация. Рассматривается тема управления цифровым наследием, показаны проблемы, которые возникают после нашего ухода. Также рассмотрены возможные способы предотвращения нежелательных ситуаций, которые могут произойти с нашими онлайн-аккаунтами. Указаны способы защиты своего цифрового наследия.

Ключевые слова: цифровое наследие; личные данные; онлайн-аккаунты; социальные сети; Интернет.

В эпоху цифровизации мы все чаще начали использовать технологии для хранения всей нашей личной информации, воспоминаний и интересов. Если раньше люди получали в наследство фотографии, пластинки, книги, личные письма и т. д., то сейчас вся личная информация остается на страницах в социальных сетях, облачных хранилищах и различных сайтах. Но что же произойдет со всей информацией, оставленной нами на наших аккаунтах? Кто сможет получить к ней доступ и как выставить определенные условия конфиденциальности? Ведь не каждый захочет, чтобы все их личные данные оказались наследованы.

Цифровое наследие — новый вид наследия, объединяющий «ресурсы, относящиеся к области культуры, образования, науки и управления, а также информацию технического, правового, медицинского и иного характера, которые создаются в цифровой форме либо переводятся в цифровой формат путем преобразования существующих ресурсов на аналоговых носителях»¹.

Цифровой след, который мы оставляем, с годами становится все больше. Интернет затрагивает огромные аспекты нашей жизни, люди

¹ Горлова И. И., Гуцалов А. А., Зорин А. Л. Сохранение цифрового наследия в России: методология, опыт, правовые проблемы и перспективы. М.: Ин-т Наследия, 2021. С. 25.

ежедневно заходят в социальные сети, приложения банков и электронную почту. Это приводит к огромному количеству личной информации, хранящейся на серверах и в учетных записях.

Цель сохранения цифрового наследия заключается в том, чтобы оно оставалось доступным для общества. Соответственно, доступ к материалам цифрового наследия, особенно к тем, которые относятся к области общественного пользования, должен быть свободным от необоснованных ограничений. В то же время засекреченная и частная информация должны защищаться от любых форм посягательства¹.

Именно поэтому в наше время так важно управление цифровым наследием, нам нужно заранее обозначить, как стоит распоряжаться учетными записями, онлайн-счетами и прочей цифровой информацией.

Управление цифровым наследием сопряжено с рядом проблем. Одной из них является неосведомленность людей в сфере цифрового наследия.

Вы когда-нибудь задумывались, что будет с вашими онлайн-аккаунтами после смерти? Большинство людей и правда не придают этому большого значения, но если вы хотите обезопасить свои личные данные, то уже сейчас стоит начать составлять план, что должно будет произойти с вашими личными страницами после ухода. Просто представьте, какое огромное количество информации мы оставляем в Интернете, наши аккаунты в социальных сетях действительно могут быть важны для близких нам людей, они смогут смотреть наши фотографии и видео, читать вашу с ними переписку. Это действительно может помочь многим справиться с потерей. Но что произойдет, если доступ получат мошенники, которые начнут использовать вашу личную информацию в корыстных целях?

Еще одной проблемой является вопрос конфиденциальности. Наши учетные записи часто содержат личную информацию, которую мы не хотели бы разглашать после нашего ухода. Как пример, личные переписки, онлайн-покупки или информация, затрагивающая конфиденциальность третьих лиц. Наследование такой информации приведет к нарушению наших прав и свобод. Получается, что при передаче нашего онлайн-аккаунта стоит исключить возможность попадания его в плохие руки или ограничить доступ к определенным функциям в социальных сетях.

Также важно отметить, что существуют некоторые проблемы в юридических вопросах. В ст. 141.1 «Цифровые права» ГК РФ было введено понятие цифровых прав, и это могло помочь решить проблему

¹ *Хартия о сохранении цифрового наследия* / ЮНЕСКО. URL: https://www.un.org/ru/documents/decl_conv/conventions/digital_heritage_charter.shtml (дата обращения: 09.05.2024).

управления цифровым наследием, но аспекты наследования онлайн-аккаунтов она не затрагивает. К сожалению, в Российской Федерации на данный момент нет отдельных законов о цифровом наследии, что может затруднить процесс его передачи из-за отсутствия четких норм.

Более того, политика многих интернет-сервисов имеет четкие требования к передаче доступа к учетной записи умершего человека. Рассмотрим варианты, которые предлагают пользователям популярные сервисы социальных сетей.

«ВКонтакте» предоставляет возможность удалить страницу или оставить ее как память для близких. Для этого нужно будет предоставить в службу поддержки копию свидетельства о смерти или другое документальное подтверждение. Если близкие выберут оставить страницу на память, то возможности авторизоваться уже не будет. «Одноклассники» предоставляют такие же функции, как и «ВКонтакте». В сервисе Google можно назначить наследника аккаунта и указать, к каким данным он получит доступ после деактивации вашего аккаунта. Компания «Яндекс» не предоставляет доступ ни к каким данным, можно только удалить личную страницу, предоставив необходимые документы. Мессенджеры Telegram и WhatsApp также не предоставляют доступа к аккаунтам умерших, так как это противоречит политике конфиденциальности и закону о тайне переписки.

Управление цифровым наследием содержит в себе внушительный ряд проблем, но стоит только подумать, какой ряд возможностей оно открывает. При правильном плане решений, который стоит предпринять с вашим онлайн-аккаунтом после ухода, можно четко обозначить, какие воспоминания и опыт будут сохранены для будущего поколения. Уже сейчас существуют платформы и услуги управления цифровым наследием. Решение данного вопроса стало намного проще с появлением определенных сервисов. Платформы, созданные для управления цифровым наследием, позволяют своим пользователям выбирать доверенное лицо, которое после нашего ухода получит доступ к личным страницам и цифровым архивам. Сервисы обеспечивают безопасный способ хранения паролей, инструкции по управлению нашим цифровым наследием и информацию о личных страницах в социальных сетях. Просто представьте, насколько данные платформы могут облегчить сохранение нашего цифрового следа, на важных для нас условиях. Мы самостоятельно создадим план действий для нашего аккаунта после нашей смерти, и он гарантированно будет отражать наши ценности и убеждения.

Несмотря на наличие проблем, связанных с цифровым наследием, существуют решения, которые помогут вашим близким справиться со

сложностями, возникшими после вашего ухода. Вам стоит заранее позаботиться о своих наследниках и подготовить свое цифровое наследие, выполнив ряд действий.

1. Создание плана цифровой недвижимости. В нем будут содержаться все ваши учетные записи и пароли к ним. Также в плане стоит подробно указать действия, которые необходимо предпринять с вашими онлайн-аккаунтами. Обязательно назначьте список доверенных лиц, которые получат доступ к данной информации.

2. Используйте специальные платформы, созданные для управления цифровым наследием. Сервисы помогут безопасно сохранить ваши личные данные и впоследствии, предоставить доступ к ней вашим доверенным лицам, также платформа поможет указать ваши пожелания, относительно управления личной информации наследником. Только важно, чтобы это был человек, которому вы полностью доверяете, чтобы он выполнил ваши пожелания и относился ответственно к вашим цифровым учетным записям. Это намного облегчит вашим близким людям доступ к вашим цифровым активам и онлайн-аккаунтам.

3. Держите своих близких в курсе. Обязательно сообщите родным о своих пожеланиях относительно вашего плана цифровой недвижимости и о том, как они смогут получить доступ к вашим онлайн-аккаунтам. Расскажите, каким вы видите свое дальнейшее присутствие в Интернете и как это организовать. Предложенные действия помогут избежать недоразумений и конфликтов в семье после вашего ухода.

Таким образом, правильное сохранение нашего цифрового наследия очень важно. Цифровой след, который мы оставляем, может быть очень важен для наших близких. Чтобы правильно предоставить им доступ, который не будет нарушать наших пожеланий и обезопасит конфиденциальную информацию, нужно заблаговременно спланировать управление цифровым наследием. Это будет гарантировать, что с вашими онлайн-аккаунтами будут обращаться в соответствии с вашими пожеланиями. Неважно, какие из предоставленных решений вы будете использовать, чтобы обезопасить свое цифровое наследие: создание цифрового плана недвижимости, использование специальных платформ или уведомление близких о своих пожеланиях. Принятие мер уже будет важным шагом и обеспечит спокойствие вам и вашим близким.

Т. А. Камарова, А. В. Вербенская

Уральский государственный экономический университет, г. Екатеринбург

Цифровая трансформация экономики и социальной сферы¹

Аннотация. Статья посвящена вопросам развития цифровой трансформации экономики и социальной сферы. В результате контент-анализа научных публикаций выявлены основные возможности и риски внедрения цифровизации в ключевые сферы общества.

Ключевые слова: цифровизация; цифровая экономика; цифровые формы занятости; цифровые навыки.

Современная трансформация всех сфер жизнедеятельности характеризуется развитием цифровизации, автоматизации, глобальной информационной сети, информационно-коммуникационных технологий (ИКТ).

Фокус приоритетных национальных целей Российской Федерации направлен на осуществление прорывного научно-технологического и социально-экономического развития страны².

Цифровая трансформация представляет собой одну из стратегических задач развития РФ на период до 2030 г., решением которой является внедрение цифровых технологий в экономику и социальную сферу.

Цифровая трансформация является исследовательским полем и представляет большой научный интерес для многих ученых. Так, в каталоге научной электронной библиотеки eLIBRARY.RU было получено 58 774 источника по поисковому запросу «цифровая трансформация», общее количество публикаций на момент запроса составляло 51 083 524 (дата обращения: 25 февраля 2024 г.). Можно отметить, что 2018 г. стал началом пиковой активности исследований в данной области, количество публикаций составило 2 455, в последующие года интерес к тематике цифровых трансформаций только возрастает, так, в 2023 г. количество публикаций достигло 13 954. Анализ распределения публикаций в области «цифровая трансформация» среди тематических рубрик позволил выявить тройку тематик, вызывающих наибольший интерес среди ученых: «Экономика. Экономические науки»; «Народное образование. Педагогика»; «Государство и право. Юридические науки». В результате анализа ключевых слов в публикациях можно отметить основные: «цифровая трансформация», «цифровизация», «цифровая экономика», «цифро-

¹ Исследование выполнено за счет гранта Российского научного фонда № 22-18-00614, <https://rscf.ru/project/22-18-00614/>.

² *О национальных целях и стратегических задачах развития Российской Федерации на период до 2024 года:* указ Президента РФ от 7 мая 2018 г. № 204; *О национальных целях развития Российской Федерации на период до 2030 года:* указ Президента РФ от 21 июля 2020 г. № 474.

вые технологии», «искусственный интеллект», «информационные технологии».

Понятие сущности «цифровая трансформация» не так давно вошло в профессиональную и научную среду и еще не получило общепринятого его определения. Так, Ю. А. Лебедева рассматривает цифровую трансформацию как замену ручных процессов новыми технологиями, внедрение цифровых платформ, автоматизации и искусственного интеллекта (ИИ) в деятельность организации с целью повышения эффективности труда [3, с. 26]. С точки зрения А. А. Барановой, цифровая трансформация представляет собой внедрение интеллектуальных систем и технологий: облачные вычисления, искусственный интеллект, аналитика данных и т. п.; процесс преобразования информации в цифровую форму [1, с. 173]. А. В. Юртайкин отмечает, что «цифровая трансформация — это движение от традиционной человекоцентричной системы управления к новой модели, основанной на постоянном поиске возможности замены человеческого труда машинным для повышения эффективности и безопасности» [7, с. 82]. Теоретизация сущности понятия «цифровая трансформация» говорит о ее многогранности и широком толковании. Следовательно, под цифровой трансформацией необходимо понимать «качественные изменения в бизнес-процессах и способах осуществления экономической деятельности, в результате внедрения цифровых технологий и инструментов, которые приводят к значительным социально-экономическим эффектам» [5, с. 15].

Триггером развития цифровизации стала пандемия коронавируса COVID-19. В период вынужденной изоляции организации практически всех сфер деятельности вынуждено перешли на удаленный формат работы, не прекращали функционировать. Образовательные организации, используя дистанционные технологии, не останавливали процесс обучения. Было отмечено, что в тех организациях, в которых до пандемии уже применялись цифровые и информационно-коммуникационные технологии, переход на удаленный формат произошел быстрее.

Цифровизация носит амбивалентный характер: это связано с рядом преимуществ и угроз ее применения. Проведя контент-анализ публикаций, нами были выявлены основные возможности и риски цифровизации в сфере экономики и социальной сфере (см. таблицу).

Цифровизация процессов и автоматизация позволяют снизить ручной труд и повысить эффективность работы сотрудников. Автоматизированные системы позволяют упростить процессы и сократить время на выполнение задач, что приводит к повышению производительности.

Несомненно, цифровизация несет в себе ряд преимуществ как в сфере экономики, так и в социальной сфере; однако процессы ее раз-

вития сопряжены с угрозами, которые необходимо учитывать при применении. Для эффективного использования благ цифровизации во всех сферах необходимо предусмотреть и уделять внимание возможным ее рискам, чтобы они не стали барьерами, препятствующими дальнейшему развитию цифровизации.

Основные возможности и риски цифровизации в сфере экономики и социальной сфере

	<i>Возможности</i>	<i>Риски</i>
<i>Сфера экономики</i>	Повышение эффективности, результативности, скорости выполнения и качества работ	Высвобождение человеческих ресурсов вследствие автоматизации производственных процессов
	Цифровизация рутинных операций (снижение ручного труда)	Изменение рынка труда: сокращение потребности в рабочих кадрах, работниках интеллектуального труда
	Развитие цифровых форм занятости (удаленной, платформенной и др.)	Информационная безопасность в организациях
	Появление новых сфер деятельности	Недостаток цифровых навыков у специалистов при использовании новых цифровых технологий
	Экологизация производственных процессов, снижение их ресурсоемкости	Риски в платежных системах
<i>Социальная сфера</i>	Улучшение предоставления и доступности услуг населению	Снижение информационной безопасности
	Увеличение возможностей в социализации и коммуникации	Неэтичное использование ИИ (различные виды манипуляций и пр.)
	Развитие интернет-продаж	Вероятность глобальных кибератак
	Создание площадок для развития социальных технологий, методов и услуг	Утечка персональных данных
	Развитие дистанционных форм/технологий обучения	Вероятность отслеживания поведенческого профиля человека

Примечание. Сост. по: [1; 2; 3; 4; 7].

Можно выделить общую необходимость практически для каждого человека в цифровую эпоху, которая заключается в обучении навыкам, позволяющим пользоваться цифровыми технологиями во всех сферах.

По результатам исследования, проведенного в декабре 2022 г. Всероссийским центром изучения общественного мнения (ВЦИОМ) об отношении россиян к реализации национального проекта «Цифровая экономика», 75 % опрошенных считают, что цифровая грамотность людей повысилась¹. Результаты коррелируют с другими исследованиями, про-

¹ *Национальные проекты — 2022: цифровая экономика / ВЦИОМ Новости. 2023. 31 янв. URL: <https://wciom.ru/analytical-reviews/analiticheskii-obzor/nacionalnye-proekty-2022-cifrovaja-ehkonomika> (дата обращения: 28.02.2024).*

водимыми учеными НИУ ВШЭ, за период 2018–2021 гг. прослеживается тенденция увеличения цифровых навыков населения [6]. Интересны данные о «цифровой» взаимопомощи в семьях: так, 58 % опрошенных респондентов в возрасте 14–17 лет приходилось оказывать «цифровую» помощь своим членам семьи, наибольшая доля обращений за подобной помощью прослеживается в возрасте 55–59 лет, эта доля составила 29 % [6].

Еще один важный момент, который будет способствовать развитию цифровизации и позволит обеспечить условия для разработки и эффективного внедрения инноваций, — формирование нормативно-правовой базы. Несмотря на то, что цифровую трансформацию общества в настоящее время регламентирует указ Президента РФ от 9 мая 2017 г. № 203 «О Стратегии развития информационного общества в Российской Федерации на 2017–2030 годы», в рамках которого реализуются основные направления развития информационного общества страны: повышение качества цифровых услуг, развитие инфраструктуры связи, обеспечение информационной безопасности, содействие цифровизации образования и экономики, а также укрепление позиций страны в мировом информационном пространстве, требуется дальнейшее развитие и совершенствование нормативно-правовой базы.

Подводя итоги, можно сделать вывод, что цифровая трансформация — это процесс интеграции цифровых технологий во все сферы деятельности. Она представляет собой изменения, основанные на использовании современных информационно-коммуникационных технологий. Цифровая трансформация позволяет организациям и человеку адаптироваться к изменяющимся условиям, повышать эффективность и качество своей деятельности и жизни.

Вопросы цифровизации, несомненно, являются актуальным научным полем. Можно отметить целесообразность дальнейших исследований в этой области с целью избегания возможных рисков внедрения цифровизации в ключевые сферы экономики и социальную сферу. Авторы планируют дальнейшие исследования, в частности возможного влияния процессов цифровизации занятости на репродуктивные планы среди мужчин и женщин, на родительское благополучие.

Библиографический список

1. *Баранова А. А.* Риски безопасности цифровой трансформации // Культура информационной безопасности: вызовы времени: материалы XIV Междунар. науч.-практ. конф. студентов, аспирантов и молодых ученых (Москва, 23–24 ноября 2023 г.). М.: Моск. гос. лингвист. ун-т, 2024. С. 171–175.

2. *Ларионов В. Г., Шереметьева Е. Н., Горшкова Л. А.* Цифровая трансформация экономики: вызовы и новая реальность // Вестник Астраханского

государственного технического университета. Серия: Экономика. 2022. № 1. С. 7–14. DOI: 10.24143/2073-5537-2022-1-7-14.

3. *Лебедева Ю. А.* Цифровая трансформация государственного сектора // Государственное и муниципальное управление: вчера, сегодня, завтра: материалы науч.-практ. конф. (с междунар. участием): в 3 ч. (Луганск, 29–30 ноября 2023 г.). Луганск: Ноулидж, 2024. С. 24–40.

4. *Федорова Н. В., Минченкова О. Ю., Макеева В. Г.* Возможности и риски цифровизации экономики и общества // Наука и искусство управления / Вестник Института экономики, управления и права Российского государственного гуманитарного университета. 2020. № 3/4. С. 25–37.

5. *Цифровая трансформация отраслей: стартовые условия и приоритеты: доклад к XXII Апр. междунар. науч. конф. по проблемам развития экономики и общества (Москва, 13–30 апреля 2021 г.) / Г. И. Абдрахманова, К. Б. Быховский, Н. Н. Веселитская и др.* М.: НИУ ВШЭ, 2021. 239 с.

6. *Цифровая экономика: 2023: краткий стат. сб. / Г. И. Абдрахманова, С. А. Васильковский, К. О. Вишневский и др.* М.: НИУ ВШЭ, 2023. 120 с.

7. *Юртайкин А. В.* Генезис и эволюция понятия цифровой трансформации предприятия // Вестник Самарского государственного экономического университета. 2023. № 4 (222). С. 78–85. DOI: 10.46554/1993-0453-2023-4-222-78-85.

Е. М. Кочкина

Уральский государственный экономический университет, г. Екатеринбург

Влияние информационных и коммуникационных технологий на производительность труда в регионах Урала

Аннотация. В статье выполнен анализ производительности труда в регионах Урала, которая рассматривалась как отношение валового регионального продукта к численности занятого населения. Дано обоснование влияния информационных и коммуникационных технологий на региональную производительность труда с использованием методов регрессионного анализа.

Ключевые слова: производительность труда; информационные и коммуникационные технологии; регион; нормирование; корреляция; регрессионный анализ.

IT-отрасль в России активно развивается, хотя все еще наблюдается отставание от ведущих мировых держав. В послании президента Российской Федерации Федеральному Собранию отмечалось, что одной из ключевых задач, стоящих перед страной на современном этапе, является повышение производительности труда. По мнению президента, в современных условиях повышение эффективности всех сфер производительности труда неразрывно связано с цифровизацией, с использованием технологий искусственного интеллекта. К 2030 г. планируется сформировать цифровые платформы во всех ключевых отраслях экономики и социальной сферы. Запущен национальный проект «Экономика

данных», на реализацию которого будет выделено не менее 700 млрд р. По мнению президента, темпы роста инвестиций в отечественные IT-решения должны минимум вдвое превышать темпы роста экономики.

Что касается регионов Урала, то наиболее высокие затраты на внедрение и использование цифровых технологий наблюдаются в Свердловской области (45 623,1 млн р.), а наиболее низкие — в Курганской области (2 376,8 млн р.).

По мере развития общественного производства объективно происходит улучшение условий и организации процесса труда. Результатом этих процессов является рост производительности труда, который повышает территориальную конкурентоспособность, приводит к снижению издержек производства, является фактором снижения цен и условием повышения качества произведенной продукции, поэтому в итоге его можно рассматривать как один из источников увеличения национального дохода [5].

Традиционно производительность труда оценивается отношением совокупного объема произведенной продукции к объему затраченного труда. Опираясь на приведенное определение, региональную производительность труда можно рассматривать как отношение валового регионального продукта к численности занятого населения. Несмотря на определенную долю условности, предложенный подход к оценке производительности труда вполне оправдан.

Анализ выбранного показателя в регионах Урала показал его рост. Однако с учетом существующей неравномерности развития территорий, значения региональной производительности труда отличаются в выбранных для анализа регионах. Наиболее благоприятная ситуация наблюдается в Свердловской области, которая на выбранном для анализа промежутке времени занимает первые и вторые места. Наименее благоприятная ситуация наблюдается в Курганской области, которая на указанном промежутке стабильно находится на последнем месте (рис. 1).

Использование информационных и коммуникационных технологий (ИКТ) позволяет оказать влияние на различные направления социально-экономического развития, а именно повысить качество медицинских услуг, снизить трудоемкость управления логистикой, розничной торговлей и т. д., в том числе повысить производительность труда. Различия в величине региональной производительности труда обусловлены влиянием большого количества разнообразных факторов, оказывающих как позитивное, так и негативное влияние. Несомненно, в состав этих факторов входит использование ИКТ.

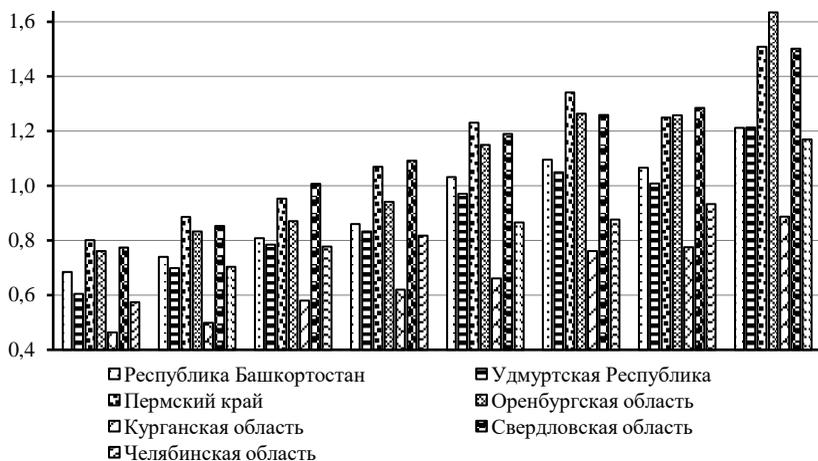


Рис. 1. Динамика производительности труда в регионах Урала

В регионах Урала развитие ИКТ, как и других показателей, подвержено региональной дифференциации. Регион может лидировать по одним показателям и отставать по другим. В целом результаты использования ИКТ в регионах Урала находятся на достаточно высоком уровне [3].

Отметим, что в уральских регионах фиксированный Интернет получил более широкое распространение, чем мобильный. В Оренбургской области отмечается самая высокая доля организаций, использующих фиксированный Интернет. Мобильный Интернет наиболее активно используется в Свердловской области. Использование широкополосного доступа к сети Интернет в регионах Урала превышает среднероссийский показатель. Наиболее активно использует Интернет население Оренбургской области, а наименее активно — Удмуртской Республики.

Количество персональных компьютеров на сто работников в регионах Урала по сравнению с 2005 г. увеличилось почти на 40 %. Использование специальных программных средств наблюдается в 70 % обследованных организаций Урала.

Автором ставилась задача выявить влияние ИКТ на региональную производительность труда. В официальной статистике представлены разнообразные показатели, характеризующие развитие ИКТ. Однако исследование влияния каждого отдельного показателя на производительность труда мало информативно. Ставилась задача разработать интегральный показатель, который смог бы аккумулировать влияние всех имеющихся показателей.

С этой целью была собрана информация по 17 показателям, характеризующим развитие ИКТ. Для каждого периода данные по регионам нормировались на максимальное значение, так как все используемые для исследования показатели носят позитивный характер. Далее определялось среднее значение нормированных показателей, которое можно рассматривать как уровень использования ИКТ в каждом регионе [1; 2].

Практически во все исследуемые периоды по величине интегрального показателя использования ИКТ лидирует Свердловская область. Однако в последние годы Свердловская область уступила первенство Оренбургской области, занимавшей ранее пятое место, и переместилась на второе. На протяжении всего исследуемого периода наиболее низкие значения интегрального показателя отмечаются в Курганской области (рис. 2).

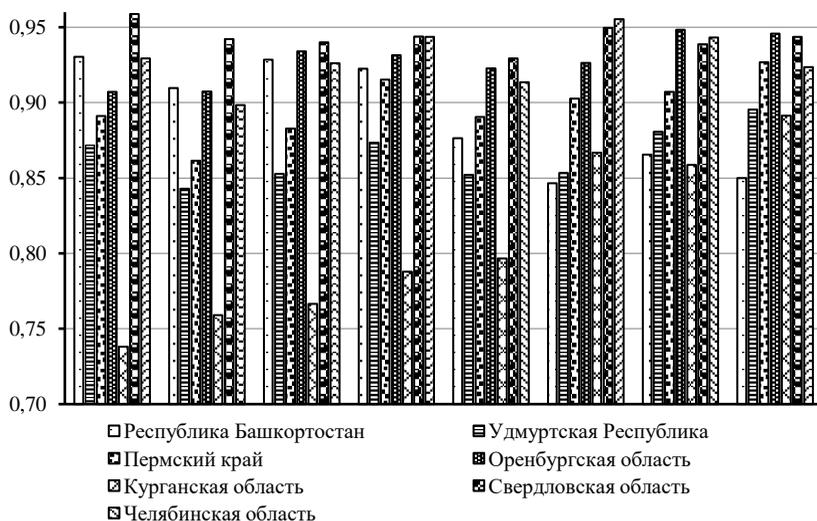


Рис. 2. Интегральный индекс использования ИКТ в регионах Урала

Далее ставилась задача исследовать влияние рассчитанного интегрального показателя на производительность труда во всех регионах Урала. Для этого был использован аппарат регрессионного анализа. В качестве зависимой переменной рассматривалась производительность труда, а в качестве факторной переменной — интегральный показатель развития ИКТ [4].

Для одних регионов Урала связь между выбранными показателями существует и оценивается как средняя. Коэффициент корреляции для

этих регионов не превышает значения 0,6. В других регионах, таких как Пермский край, Свердловская и Челябинская области, коэффициент корреляции демонстрирует тесную связь между выбранными показателями, так как превышает значение 0,7. Такой результат был ожидаемым, так как помимо ИКТ на производительность труда оказывают влияние и другие факторы экономического развития, влияние которых может быть более существенным, в результате чего влияние ИКТ оценивается как среднее.

Исходя из величины коэффициента детерминации для регионов Урала от 30 до 65 % разброса данных объясняется построенной регрессионной моделью. Проверка статистической гипотезы для коэффициента детерминации показала, что для построения модели в двух регионах (Республика Башкортостан и Челябинская область) недостаточный объем исходной статистической информации. На текущем этапе устранить этот недостаток модели не представляется возможным.

Для всех регионов Урала реальные значения производительности труда существенно от модельных не отклоняются, т. е. отсутствуют статистические выбросы. Коэффициенты, определяющие меру влияния интегрального показателя использования ИКТ на производительность труда, имеют существенный разброс по регионам, при этом для всех регионов наблюдаемая зависимость является прямой. Наиболее значительное влияние отмечается в Свердловской области, а наиболее низкое — в Курганской.

Учитывая, что формула производительности труда содержит денежную составляющую, в результате чего наблюдается выраженный тренд, что наглядно показано на рис. 1, данные по производительности труда освободились от тренда. С использованием данных, освобожденных от тренда, повторялась процедура регрессионного анализа. Однако теснота связи между показателями практически не изменилась. Сохранились и другие качественные характеристики моделей.

Безусловно, построенные модели не позволяют выделить влияние отдельных показателей развития ИКТ на производительность труда. Однако использование интегрального показателя в проведенном исследовании подтвердило предположение о влиянии ИКТ на производительность труда.

Библиографический список

1. Денежкина К. Л., Радковская Е. В. Статистический анализ работы российских авиакомпаний и аэропортов // Глобальный научный потенциал. 2022. № 8 (137). С. 192–195.

2. *Кочкина Е. М.* Многомерные статистические методы в анализе экономического развития // VI-технологии и корпоративные информационные системы в оптимизации бизнес-процессов цифровой экономики: материалы IX Междунар. науч.-практ. очно-заочной конф. (Екатеринбург, 2 декабря 2021 г.). Екатеринбург: УрГЭУ, 2022. С. 8–10.

3. *Плетнев Д. А.* Цифровизация и производительность труда // Вестник Челябинского государственного университета. 2023. № 12 (482). С. 5–7.

4. *Радковская Е. В., Дианова Л. С.* Использование регрессионного анализа в исследовании локального потребительского рынка // Перспективы науки. 2021. № 6. С. 36–38.

5. *Ямашкин Ю. В.* Проблемы и перспективы реализации национального проекта «производительность труда»: региональный и национальный аспект // Russian Economic Bulletin. 2024. Т. 7, № 1. С. 181–187.

А. А. Окунев

Уральский государственный экономический университет, г. Екатеринбург

Анализ рынка виртуализации в России

Аннотация. Статья посвящена анализу цифровых санкций, в частности, можно ли их классифицировать и концептуализировать в более широких рамках традиционных экономических санкций. Для оценки масштаба и потенциальной значимости цифровой экономики проведен обзор и анализ исследования ЮНКТАД по измерению электронной коммерции и цифровой экономики.

Ключевые слова: экономические санкции; цифровая экономика; анализ эффективности; ЮНКТАД.

В эпоху цифровых преобразований структура и применение экономических санкций претерпели изменения, которые расширились от традиционных торговых эмбарго до современных цифровых и финансовых санкций. Недавние мировые конфликты спровоцировали широкий спектр действий со стороны западных стран, нацеленных на цифровой сектор экономики других государств. Санкции включают в себя ограничения на квантовые вычисления, ИТ-услуги, производство, аэрокосмические технологии и другие меры, которые могут помешать цифровой трансформации страны. В данной статье рассматривается основной исследовательский вопрос — можно ли рассматривать санкции, направленные на цифровые технологии и развитие, как передовую форму экономических санкций. По мере того как цифровая трансформация продолжает революционизировать экономику во всем мире, это исследование показывает, что санкции в области цифровых технологий имеют существенные экономические последствия для целевых стран. Исследование дает представление о меняющемся ландшафте механизмов санкций и дипломатии в цифровой век.

Под экономическими санкциями понимается дипломатическая тактика, заключающаяся в прекращении или угрозе прекращения экономических отношений со страной-объектом в целях изменения или отмены дипломатических решений. Страна — объект санкций рассчитывает ожидаемые экономические потери от предлагаемых санкций, и, если она изменит или отменит свои внешнеполитические решения, чтобы минимизировать возможные потери, санкции считаются эффективными. Таким образом, экономические санкции должны быть направлены на причинение значительного экономического ущерба стране — объекту санкций.

В более раннюю эпоху глобализации, когда торговые отношения между странами быстро расширялись, политики считали, что потеря торговли может существенно повлиять на принятие страной внешнеполитических решений. Поэтому большинство экономических санкций включают торговые эмбарго. Сегодня финансовые санкции применяются все чаще, поскольку возможности финансовых операций превышают возможности торговли сырьевыми товарами. Кроме того, финансовые санкции относительно свободны от этической критики, поскольку они наносят ущерб только конкретной группе или отдельным лицам и, таким образом, оказывают ограниченное воздействие на уязвимое население целевой страны.

Современная эпоха цифровой трансформации оказала значительное влияние на экономическую деятельность в различных секторах, причем цифровые операции становятся все более распространенным явлением. Поэтому все более настоятельной становится необходимость пересмотра тех видов экономических санкций, которые могут фактически наносить существенный ущерб странам — объектам санкций.

Рассмотрим классификацию мер, связанных с цифровыми технологиями, в качестве одной из форм экономических санкций. Во-первых, это механизмы и оперативные аспекты экономических санкций, а также меры, применяемые в качестве экономических санкций. Во-вторых, демонстрацию того, что по мере укрепления структуры цифровой экономики меры, связанные с цифровыми технологиями, могут эффективно функционировать как своего рода экономические санкции.

Мера может рассматриваться в качестве экономической санкции, если она, как ожидается, приведет к экономическим потерям или если потенциальный экономический ущерб от этой меры воспринимается страной — объектом санкций как угроза. Если та или иная мера не приводит к достаточным экономическим потерям или если страна, против которой она направлена, не знает о потенциальных потерях, которые

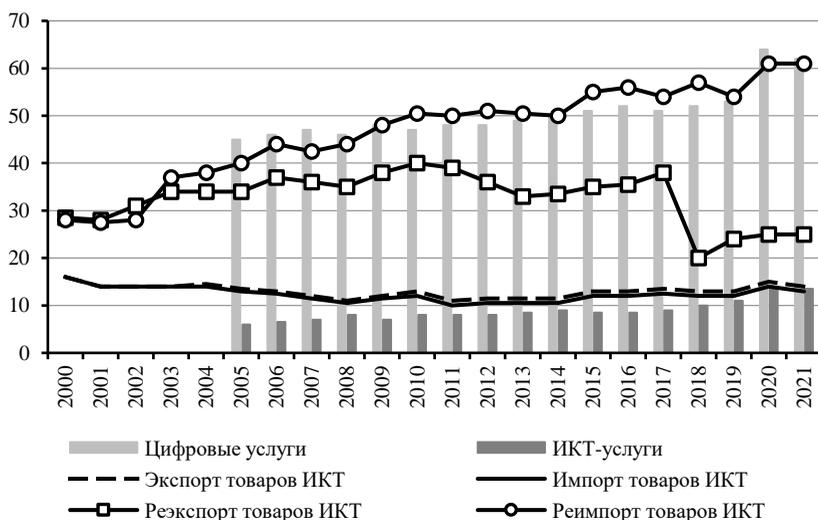
она может понести, то классифицировать эту меру как экономические санкции становится трудно.

Эффективность экономических санкций оценивается на основе того, в какой степени эта мера влияет на процесс принятия дипломатических решений в стране — объекте санкций. Если ожидаемые или понесенные в результате этой меры экономические потери являются достаточно значительными для того, чтобы побудить к изменению дипломатических решений, то они могут рассматриваться как эффективные экономические санкции, в противном случае они будут считаться неэффективными. Таким образом, для того чтобы та или иная мера квалифицировалась как вид экономической санкции, она должна либо причинять, либо потенциально причинять экономический ущерб стране-объекту санкций. В соответствии с этой концепцией прекращение торговых отношений или приостановление финансовых операций, которые непосредственно ведут к ожидаемым экономическим потерям, воспринимается как один из видов экономических санкций.

Далее рассмотрен вопрос о том, каким образом меры, связанные с цифровыми технологиями, могут быть концептуально сформулированы с точки зрения экономических последствий. В настоящее время существует лишь ограниченное число исследований, в которых цифровые санкции конкретно описываются как отдельная категория экономических санкций. Вместе с тем меры, связанные с цифровыми технологиями, осуществляются в различных целях, как в дипломатических, так и в экономических целях. Например, в 2019 г. США ввели санкции против Huawei, известного китайского производителя телекоммуникационного оборудования, из-за угрозы национальной безопасности. Эти санкции ограничили доступ Huawei к технологическим ресурсам США, в том числе к полупроводникам и программному обеспечению, что привело к заметным сбоям в его глобальных операциях и закупке ключевых компонентов. Они также привели к тому, что Huawei была вынуждена прекратить на время свою деятельность.

Необходимо также рассмотреть вопрос о том, в какой степени меры, связанные с цифровыми технологиями, могут отразиться на экономических потерях государств, осуществляющих цифровое преобразование. Чтобы ответить на этот вопрос, необходимо оценить размеры цифровой экономики. Обзор исследования Конференции Организации Объединенных Наций по торговле и развитию (ЮНКТАД) по измерению электронной торговли и цифровой экономики поможет понять масштабы цифровой экономики и, следовательно, ее потенциальное экономическое воздействие на цели политики, связанной с цифровыми технологиями.

Цифровая экономика — это та часть экономического результата, которая получается исключительно или в первую очередь за счет цифровых технологий с бизнес-моделью, основанной на цифровых товарах или услугах. Согласно резюме докладов ЮНКТАД, основные и узкие области цифровой экономики связаны с инфраструктурой информационных и коммуникационных технологий (ИКТ), сектором производства ИКТ, цифровыми и платформенными услугами, а широкая сфера охвата включает использование цифровых технологий в различных видах экономической деятельности, в том числе в электронной торговле. На основе этих определений ЮНКТАД разработала девять соответствующих категорий данных. Однако между этими категориями существуют расхождения в информации, обусловленные различиями в подготовке статистических данных по конкретным странам. Если мы рассмотрим размер цифровой экономики в отдельных странах, мы можем использовать все имеющиеся данные, если они предлагаются правительством. Однако в этом контексте рассматриваются общие глобальные масштабы цифровой экономики. С этой целью целесообразно использовать три основных показателя: доля товаров, связанных с ИКТ, а именно реимпорт и реэкспорт; международная торговля услугами, предоставляемыми в цифровом формате, и международная торговля услугами ИКТ, которые позволяют оценить общий глобальный объем товаров ИКТ. Объем торговли цифровыми товарами и услугами представлен на рисунке.



Доля цифровой экономики в мировой экономике, %

По состоянию на 2021 г. доля международной торговли цифровыми услугами между отдельными странами и различными группами стран составляла около 60 %, а доля услуг ИКТ — около 15 %. С точки зрения физического объема торговли на импорт и экспорт товаров ИКТ приходится 14 % совокупного импорта и экспорта, а на реимпорт — около 60 % от общего объема. Кроме того, при рассмотрении изменений в масштабах цифровой экономики можно отметить заметную тенденцию к росту, особенно в категории цифровых услуг и услуг ИКТ. Кроме того, доля физического объема торговли оставалась относительно стабильной, в то время как доля реимпорта продолжала демонстрировать устойчивую повышательную тенденцию.

Таким образом, можно сделать вывод о том, что цифровая экономика занимает значительную долю в мировой экономике и относительно значительную долю в плане мобильности услуг. Очевидно, что меры, связанные с цифровыми технологиями, могут рассматриваться как форма экономических санкций, поскольку они могут привести к значительным экономическим потерям. Особенно в настоящее время, когда промышленная революция быстро повышает значение цифровой экономики и приводит к изменениям в структуре промышленности, аналогичным предыдущей эпохе глобализации и роста мировой торговли. На основе этих данных весьма вероятно, что введение цифровых санкций может быть применено в качестве одной из форм экономических санкций на международных переговорах. В нынешних условиях расширяющейся цифровой экономики относительно ясно, что цифровые меры могут служить формой экономических санкций, учитывая их потенциальную возможность причинять экономические потери. Это лишний раз подкрепляет идею о том, что меры в области цифровых технологий могут рассматриваться как своего рода экономические санкции в рамках растущей цифровой экономики.

Л. А. Сазанова, Н. А. Зенков

Уральский государственный экономический университет, г. Екатеринбург

Алгоритмическая прозрачность как аспект цифровой трансформации и направления ее обеспечения

Аннотация. В статье поднимается вопрос о проблемах реализации принципа прозрачности алгоритмов, используемых в системах искусственного интеллекта. Выделены основные принципы алгоритмической прозрачности и основные направления, ее обеспечивающие. Сопоставлены различные мнения касательно трактовки данного понятия и возможностей достижения качества прозрачности алгоритмами, реализуемыми современными ИТ в различных предметных областях. Отмечены препятствия, возникающие при достижении выполнения требований полного открытия кода или архитектуры моделей искусственного интеллекта.

Ключевые слова: алгоритмическая прозрачность; автоматизированная обработка данных; объяснимость работы алгоритма; интеллектуальные информационные системы; цифровые технологии.

В условиях постоянного развития и совершенствования современных информационных технологий понятие алгоритмической прозрачности является немаловажным для оценки качества алгоритмов, реализуемых в системах искусственного интеллекта (ИИ), а также в связи с растущими требованиями к обеспечению безопасности персональных и иных данных, получаемых в ходе обработки их алгоритмическим путем. Одна из популярных трактовок рассматривает алгоритмическую прозрачность как совокупность двух следующих качеств, присущих алгоритмам ИИ [4]:

- объяснимости принципов работы алгоритма, а также процесса получения результатов в ходе его применения;
- обеспечения недискриминационного доступа пользователей ко всей информации, связанной с алгоритмами ИИ, используемыми в современных информационных системах.

Алгоритмическая прозрачность напрямую определяется деталями реализации информационной модели, позволяющими получить представление о логике функционирования системы, области ее использования и направлениях дальнейшего развития. Можно сказать, что данное понятие подразумевает наличие «видимости» пользователями и разработчиками причин, влияющих на решения, принимаемые теми или иными алгоритмами ИИ.

Предложенное в 2016 г. Н. Дьякопулосом и М. Колиской в работе о роли алгоритмов в принятии решения, данное понятие восходит к появлению в 1970-х гг. первых автоматизированных систем оценки потребительских кредитов. По ряду причин, среди которых — различия трак-

товки термина, присущие юристам, разработчикам, экономистам и другим категориям пользователей, а также многообразии последствий влияния степени прозрачности на процессы цифровизации, однозначное определение алгоритмической прозрачности до сих пор отсутствует. Законодательства ряда европейских государств предусматривают регулирование применения систем ИИ посредством принятия законов о персональных данных, однако общепринятые регламенты по защите данных не возлагают юридической обязанности на контролеров раскрывать техническую информацию субъекту персональных данных, в отношении которого алгоритм принимает решение. В США вопросы подотчетности алгоритмов регламентируются путем принятия ряда антидискриминационных актов, регулирующих отдельные сферы жизнедеятельности человека и имеющих фрагментарный характер. Можно сказать, что как в мире, так и в России правовое регулирование алгоритмической прозрачности и подотчетности находится на этапе становления. Эти обстоятельства порождают ряд проблем как в области законодательного регулирования, так и по части развития ИТ-технологий, поскольку сохраняются правовые и этические риски применения непрозрачной технологии и цифровое неравенство среди пользователей информационных систем. В этой связи задача формулирования более четкого определения понятия и выделения соответствующих принципов является весьма актуальной, хоть и достаточно трудной.

Эксперты Сообщества справедливости, подотчетности и прозрачности в области машинного обучения предлагают в качестве основных принципов алгоритмической прозрачности рассматривать следующие [1]:

- 1) объяснимость;
- 2) справедливость;
- 3) проверяемость;
- 4) точность работы;
- 5) ответственность разработчиков.

При этом трактовка каждого из вышеперечисленных качеств, коим должен, по мнению специалистов, обладать алгоритм ИИ, может быть неоднозначной и иметь варианты понимания и использования, и все перечисленные выше пять качеств взаимосвязаны между собой. В частности, понятия о справедливости и объяснимости у представителей различных сфер деятельности сильно отличаются. Например, по мнению ряда экспертов, объяснимость должна давать возможность пользователю понять, почему алгоритм выдал те или иные результаты при том, что многие алгоритмы, связанные с машинным обучением, в этом смысле представляют собой «черный ящик» [2]. Однако, когда алго-

ритм используется для принятия критически важного решения и цена ошибки высока, нужно понимать причины, лежащие в основе полученных результатов. Например, объяснимый алгоритм диагностики заболевания помогает понять врачу, наличие или отсутствие каких именно признаков привело к постановке диагноза системой и почему рекомендуется тот или иной протокол лечения. Если у врача возникают сомнения по поводу результатов, он должен иметь возможность вернуться и перепроверить конкретные характеристики на точность. В таком случае подход «черного ящика» для диагностической системы явно недостаточен. Объяснимость алгоритма имеет особое значение для алгоритмов машинного обучения в плане повышения доверия к используемой для принятия решений модели. В машинном обучении выделяют две стратегии, обеспечивающие объяснимость алгоритмов:

1) предоставление детальной информации обо всей модели; этот способ обеспечивает глобальную объяснимость;

2) обоснование для одного или нескольких отдельных прогнозов, сделанных обученной моделью, что делает модель локально объяснимой.

Разумеется, реализовать вторую стратегию проще, что не всегда удовлетворит пользователя. Считается, что некоторая «закрытость» деталей алгоритмов ИИ, работающих с большими массивами входных данных, вполне уместна для многих систем машинного обучения, в том числе и в силу специфичности информации, характерной для ряда предметных областей. В то же время при принятии решений в сферах бизнеса, государственного управления, здравоохранения и обеспечения безопасности надежность и обоснованность получаемых системой результатов является жизненно необходимой в силу серьезности возможных последствий и высокой цены ошибок.

Мнения специалистов по поводу требований справедливости и ответственности также неоднозначны. Например, Э. В. Талапина высказывает следующую точку зрения: поскольку программный код алгоритма формализует логику его работы, прозрачность может рассматриваться как инструмент контроля и стандартизации взаимодействия ИТ-разработчиков с рядовыми пользователями и органами власти [3]. В то же время часть разработчиков с этим не согласны. По их мнению, раскрытие логики работы алгоритма не должно противоречить требованиям законодательства об интеллектуальной собственности, поскольку интеллектуальные права на алгоритм принадлежат его правообладателям. Следствием данного противоречия является ограниченность перечня подконтрольных ситуаций, к которым на сегодняшний день относятся прежде всего критические процессы, связанные с безопасностью.

Использование соответствующих обеспечивающих информационных систем, а также сервисов, связанных с хранением и обработкой персональных данных, регламентируется более жесткими нормами правового и технического регулирования. Нет сомнений, что проблема защиты персональных данных с каждым годом встает все острее, повышая актуальность решения задачи обеспечения открытости логики работы алгоритмов информационных технологий со стороны законодательной власти. Однако при этом остается не очевидным, обеспечивают ли прозрачность того или иного алгоритма ИИ и возможность понимания его логики защиту пользовательским данным, в том числе конфиденциальным?

Наконец, сложность многих современных алгоритмов ИИ, привлекающих разнообразный математический инструментарий, часто не позволяет формализовано описать их так, чтобы логика была понятна рядовому пользователю, не имеющему компетенций в области программирования, а иногда — даже специалисту. Можно сказать, что многие алгоритмы, лежащие в основе программного обеспечения систем ИИ, продолжают оставаться «черными ящиками» даже для части разработчиков. В этой связи обвинения последних в непрозрачности обучаемых ими в составе систем ИИ алгоритмов не всегда достаточно обоснованы и могут быть оспорены. Кроме того, по причине сложности сама проверка того, реализовано ли требование о раскрытии логики алгоритма, также может оказаться весьма затруднительной.

Согласно Концепции развития регулирования отношений в сфере технологий искусственного интеллекта и робототехники до 2024 г.¹, проблема обеспечения алгоритмической прозрачности относится к основным направлениям регулирования отношений в сфере технологий ИИ и робототехники. Указанная трактовка подразумевает включение технологических разработок в области ИИ в сферу государственного управления и контроля и постоянный анализ социальных, технических и регулятивных проблем, создаваемых алгоритмическими системами ИИ. Таким образом государство пытается регулировать некоторые этические аспекты использования ИИ, а также вопросы обеспечения информационной безопасности и защиты данных в таких сферах, как государственное управление, банковская деятельность, страхование, реализация сложных и долговременных проектов, затрагивающих интересы большого числа граждан, но процесс этот далек от завершения. В свете вышесказанного остается ожидать, когда критерий понятности

¹ *Об утверждении* Концепции развития регулирования отношений в сфере технологий искусственного интеллекта и робототехники до 2024 года: распоряжение Правительства РФ от 19 августа 2020 г. № 2129-р.

информации для пользователей обретет свою четкую формулировку на уровне закона.

Не подлежит сомнению необходимость соблюдения многостороннего баланса между возможностями и преимуществами развивающихся ИТ, точностью и объяснимостью результатов их работы, требованием защиты персональных данных, определением границ регулирования сферы ИИ и контролем результата или прогноза, выдаваемого ИИ со стороны разработчика или пользователя. Обеспечение такого баланса позволит минимизировать риски, связанные с неправомерным получением и обработкой больших пользовательских данных, с раскрытием информации о частной жизни пользователей, и, наконец, с ошибками при принятии решений специалистами, воспользовавшимися конкретной системой, содержащей алгоритм ИИ в условиях неопределенности при обращении к различным и многоформатным хранилищам информации. Это также позволит улучшить качество самих алгоритмов и, как следствие, результатов обработки данных (например, получаемых с их помощью результатов диагностики ситуаций, прогнозов и оценок).

Таким образом, можно сделать вывод об актуальности идеи компромисса между возможностями современных технологий, правами разработчиков и других участников общественных процессов и требованиями со стороны законодательных и контролирующих органов. Однако достижение такого компромисса представляет весьма сложную задачу и вряд ли возможно в ближайшем будущем. Это же можно сказать относительно развивающейся области — инженерии знаний, в рамках которой используются и совершенствуются алгоритмы ИИ. Если действия таких алгоритмов, делающих знания явными и доступными, основаны на логике, то процедура получения знаний может быть объяснена и понятна, поэтому востребованность интеллектуальных систем, интегрирующих инженерию знаний и машинное обучение с высокой степенью объяснимости результатов, продолжает расти.

В заключение отметим следующее. Повышению алгоритмической прозрачности будет способствовать реализация следующих направленных действий:

- развитие стандартизации и сертифицирования моделей и алгоритмов, применяемых в области информационной безопасности;
- включение в правовые акты требований о разработке технологий, соответствующих нормам стандартизации;
- совершенствование законодательства в части совместного использования общедоступных и отраслевых информационных ресурсов и ответственности за выполняемые действия;
- совершенствование методов машинного обучения;

- изучение отечественного и международного опыта защиты частной жизни пользователей цифровых технологий;
- повышение информационной грамотности населения в области информационных технологий.

Последовательные и системные законодательные, технологические и интеллектуальные усилия общества в указанных направлениях способствуют достижению высокого качества и безопасности информационных систем, снижению проблемы цифрового неравенства среди различных групп пользователей и признанию искусственного интеллекта заслуживающим доверия со стороны всех заинтересованных в нем пользователей, обеспечивая устойчивое и справедливое развитие цифрового общества.

Библиографический список

1. *Жарова А. К.* Достижение алгоритмической прозрачности и управление рисками информационной безопасности при принятии решений без вмешательства человека: правовые подходы // *Journal of Digital Technologies and Law*. 2023. Т. 1, № 4. С. 973–993.
2. *Кутейников Д. Л., Ижаев О. А., Зенин С. С., Лебедев В. А.* Алгоритмическая прозрачность и подотчетность: правовые подходы к разрешению проблемы «черного ящика» // *Lex Russica (Русский закон)*. 2020. Т. 73, № 6 (163). С. 139–148.
3. *Талатина Э. В.* Алгоритмы и искусственный интеллект сквозь призму прав человека // *Журнал российского права*. 2020. № 10. С. 25–39.
4. *Харитонова Ю. С.* Правовые средства обеспечения принципа прозрачности искусственного интеллекта // *Journal of Digital Technologies and Law*. 2023. Т. 1, № 2. С. 337–358.

Содержание

Информационная безопасность и компьютерные технологии

Ищенко Е. А., Панов М. А. Угрозы информационной безопасности при использовании корпоративных систем для обмена мгновенными сообщениями.....	3
Каткова К. А. Кибербезопасность в условиях цифровой трансформации: новые угрозы и методы защиты	7
Лаптева Е. А., Пермякова К. С. Применение ассоциативного анализа в сфере информационной безопасности	11
Мельников Д. Ю. Обоснование применимости метода машинного обучения «градиентный бустинг» для алгоритма системы обнаружения компьютерных атак	14
Сарапульцева А. В. Цифровая безопасность как часть информационной культуры.....	18
Сидоров С. А. Безопасность веб-ресурсов и их защита от вредоносных атак.....	22
Хайрутдинов И. Ю. Актуальность уязвимостей Spectre и Meltdown и угрозы информационной безопасности	26
Шаидова Н. А. Исследование методов обеспечения безопасности данных на серверах хостинга	30

Цифровые решения для бизнеса и общества

Алексеева А. О. Необходимость сбора ценовых данных и их обработки на предприятиях оптовой торговли	32
Анисимова М. А. Формирование в здравоохранении технологии блокчейна, ориентированной на пациента	36
Бутко Г. П., Меньшикова М. А. Информационные технологии как фактор повышения эффективности в контексте рискованного общества	40
Буценко Е. В. Мониторинг меню ресторана на основе методов интеллектуального анализа данных	43
Горев А. В., Тонких Н. В. Smart-технологии управления «гибридным» персоналом	50
Городилова А. Д. Влияние цифровизации на жизнь пожилых людей.....	55
Кольева Н. С., Чугайнова Д. И. Разработка программного комплекса для ведения телефонного справочника предприятия	60
Малыгин Я. В. Информатика ЕГЭ: решение заданий на выигрышную стратегию с использованием функции выигрыша	63
Медведев П. М. Цифровая трансформация системы управления в сфере обслуживания противопожарных систем	70

Овчинников И. А., Посягин А. Е. Российский 3D-движок UNIGINE. Применение, особенности, место в промышленности и игровой индустрии, перспективы развития	74
Паруни Н. И., Попов К. В., Сурнина Н. М. Разработка алгоритма анализа архитектуры информационной системы предприятий	79
Посягин А. Е. Применение отечественных СУБД в различных отраслях экономики: преимущества и особенности использования	82
Привалова Е. А. Преимущества выбора сервиса технической поддержки на базе «1С:ITILUM»	87
Радковская Е. В. Оптимизация распределения трудовых ресурсов на предприятии	90
Сербина Н. В. Платформенная занятость студентов как старт в профессию	95
Смирнова Д. Н. Технологии формирования геометро-графических навыков в дистанционном формате	100
Чечулин И. А. Перспективные траектории цифровой трансформации в сфере жилищно-коммунального хозяйства	103
Шатров Р. Д. Применение нейросетевых технологий для реализации искусственного интеллекта в видеоиграх	107

Проблемы трансформации и риски цифрового общества

Аронов К. В. Этические и нормативные последствия искусственного интеллекта в банковском деле	113
Боднарук Т. Р., Сиваков Д. А. Цифровая трансформация логистических предприятий на основе платформенных решений	116
Гарипов М. Р. Макроэкономические проблемы цифровизации экономики	121
Головнина О. Д. Управление цифровым наследием: что происходит с нашими онлайн-аккаунтами после того, как мы уходим	125
Камарова Т. А., Вербенская А. В. Цифровая трансформация экономики и социальной сферы	129
Кочкина Е. М. Влияние информационных и коммуникационных технологий на производительность труда в регионах Урала	133
Окунов А. А. Анализ рынка виртуализации в России	138
Сазанова Л. А., Зенков Н. А. Алгоритмическая прозрачность как аспект цифровой трансформации и направления ее обеспечения	143

Научное издание

Цифровая трансформация общества и информационная безопасность

Материалы

III Всероссийской научно-практической конференции

(Екатеринбург, 17 мая 2024 г.)

Печатается в авторской редакции и без издательской корректуры

Компьютерная верстка

И. В. Засухиной

Поз. 38. Подписано в печать 12.08.2024.

Формат 60 × 84¹/₁₆. Бумага офсетная. Печать плоская.

Уч.-изд. л. 8,8. Усл. печ. л. 8,4. Печ. л. 9,5. Тираж 10 экз. Заказ 368.

Издательство Уральского государственного экономического университета

620144, г. Екатеринбург, ул. 8 Марта / Народной Воли, 62/45

Отпечатано с готового оригинал-макета в подразделении оперативной полиграфии

Уральского государственного экономического университета



УРАЛЬСКИЙ ГОСУДАРСТВЕННЫЙ
ЭКОНОМИЧЕСКИЙ УНИВЕРСИТЕТ

1037.06 1051.32 1037.04 1051.32 102
Open High Low Close

