МЕЖДУНАРОДНЫЙ ЦЕНТР НАУЧНОГО СОТРУДНИЧЕСТВА
«НАУКА И ПРОСВЕЩЕНИЕ»

НАУКА и ПРОСВЕЩЕНИЕ
МЕЖДУНАРОДНЫЙ ЦЕНТР НАУЧНОГО СОТРУДНИЧЕСТВА

АКТУАЛЬНЫЕ ВОПРОСЫ НАУКИ, ТЕХНОЛОГИЙ И ОБЩЕСТВА

МОНОГРАФИЯ

ПЕНЗА
МЦНС «НАУКА И ПРОСВЕЩЕНИЕ»
2025

УДК 001.1
ББК 60
А43

Р е ц е н з е н т ы:

Гетманская Елена Валентиновна – доктор педагогических наук, профессор, доцент кафедры методики преподавания литературы ФГБОУ ВО «Московский педагогический государственный университет»

Колесников Геннадий Николаевич – доктор технических наук, профессор, заведующий кафедрой ФГБОУ ВО «Петрозаводский государственный университет»

Удут Владимир Васильевич – доктор медицинских наук, профессор, член-корреспондент РАН, заместитель директора по научной и лечебной работе, заведующий лабораторией физиологии, молекулярной и клинической фармакологии НИИФиРМ им. Е.Д. Гольдберга Томского НИМЦ.

Авторский коллектив

Аленичева Т.С., Аменицкий А.В., Аменицкий Д.А., Аршун В.В., Атьман В.В., Балтабеков С.Б., Веремеев Р.Д., Зинюков Ю.В., Зонненберг Ю.Е., Колосова Е.Г., Кочергин И.Г., Куницын В.И., Лаврикова Н.И., Мамаев О.А., Мамаева Н.А., Расторгуева К.М., Рудикова-Фронхёфер Л.В., Рухович И.В., Сидорова И.Г., Фролов С.В., Хамчиев К.М., Хамчиева З.К.

А43

АКТУАЛЬНЫЕ ВОПРОСЫ НАУКИ, ТЕХНОЛОГИЙ И ОБЩЕСТВА: монография / Под общ. ред. Г. Ю. Гуляева — Пенза: МЦНС «Наука и Просвещение». — 2025. — 236 с.

ISBN 978-5-00236-852-5

В монографии представлены теоретические подходы и концепции, аналитические обзоры, практические решения в конкретных сферах науки, технологий и общества.

Издание может быть интересно российским и зарубежным ученым, руководителям и служащим государственного аппарата, руководителям и специалистам учреждений и хозяйственных организаций, педагогам, аспирантам и студентам высших учебных заведений.

Ответственность за аутентичность и точность цитат, имен, названий и иных сведений, а также за соблюдение законодательства об интеллектуальной собственности несут авторы публикуемых материалов.

УДК 001.1
ББК 60

ISBN 978-5-00236-852-5

ОГЛАВЛЕНИЕ

РАЗДЕЛ I. СОВРЕМЕННЫЕ ТЕХНОЛОГИИ КАК ФАКТОР И РЕЗУЛЬТАТ ИННОВАЦИОННОГО РАЗВИТИЯ

УДК 001.891.5

ГЛАВА 1. МЕТОДОЛОГИЧЕСКИЕ ОСОБЕННОСТИ ТЕХНОЛОГИЧЕСКОГО ИНСТРУМЕНТАРИЯ В ЭКСПЕРИМЕНТАЛЬНОЙ НАУКЕ

Лаврикова Наталия Игоревна
д.э.н., доцент,
сотрудник Академии ФСО России
Кочергин Игорь Геннадьевич
к.и.н., доцент,
доцент кафедры истории, политологии и государственной политики
Среднерусского института управления - филиал РАНХиГС
Зинюков Юрий Владимирович,
Веремеев Роман Денисович
сотрудники
Академии ФСО России

Аннотация: Целью данного исследования является анализ взаимосвязи между техническими достижениями и научными открытиями, а также изучение влияния технологий на методы научного исследования. Для достижения этой цели необходимо решить ряд задач: выявить исторические и современные примеры взаимодействия науки и техники, проанализировать влияние технологий на развитие научных методов и определить перспективы дальнейшего взаимодействия технических и научных знаний.

Выбор темы обусловлен ее значимостью для понимания механизмов научного прогресса. В условиях современного научно-технического развития, когда технологии активно внедряются во все сферы науки, важно осознать их роль и влияние. Это позволит не только оценить текущее состояние, но и прогнозировать будущие изменения, что делает данное исследование актуальным и востребованным.

Ключевые слова: технологический инструментарий, экспериментальная наука, наука и техника, современные технологии, искусственный интеллект.

METHODOLOGICAL FEATURES OF TECHNOLOGICAL INSTRUMENTATION IN EXPERIMENTAL SCIENCE

Lavrikova Natalia Igorevna,
Kochergin Igor Gennadievi,
Zinyukov Yuri Vladimirovich,
Veremeev Roman Denisovich

Abstract: The purpose of this study is to analyze the relationship between technical achievements and scientific discoveries, as well as to study the influence of technology on the methods of scientific research. To achieve this goal, it is necessary to solve a number of problems: to identify histor-

ical and modern examples of the interaction of science and technology, to analyze the influence of technology on the development of scientific methods and to determine the prospects for further interaction of technical and scientific knowledge.
The choice of the topic is due to its importance for understanding the mechanisms of scientific progress. In the context of modern scientific and technological development, when technologies are actively introduced into all areas of science, it is important to understand their role and influence. This will allow not only to assess the current state, but also to predict future changes, which makes this study relevant and in demand.
Key words: technological tools, experimental science, science and technology, modern technologies, artificial intelligence.

Современный мир характеризуется стремительным развитием технологий, которые оказывают значительное влияние на все аспекты человеческой деятельности. Наука, как одна из ключевых сфер, не является исключением. Взаимодействие науки и техники, их взаимное влияние и развитие представляют собой важную область исследований, поскольку именно технические достижения зачастую становятся основой для новых научных открытий, а научные теории и открытия, в свою очередь, стимулируют развитие технологий. Именно поэтому изучение роли техники и технологий в научном прогрессе является актуальной задачей.

Из покон веков техника играла ключевую роль в развитии науки, способствуя накоплению знаний и открытию новых горизонтов. Механические устройства, такие как водяные часы и астролябии, служили инструментами для измерения времени и изучения небесных тел. Эти достижения позволяли ученым формировать представления о природе и космосе, что стало основой для дальнейших научных исследований. Наука и техника пронизывают все стороны жизни человечества на протяжении всей истории.

Эпоха Возрождения ознаменовалась значительным прогрессом в технике, что привело к началу научно-технической революции. Важным шагом стало изобретение печатного станка Иоганном Гутенбергом в 1440 году, которое ускорило распространение научной информации и способствовало обмену идеями между учеными. В 1609 году Галилео Галилей создал телескоп, позволивший сделать революционные открытия в астрономии, такие как наблюдение фаз Венеры и спутников Юпитера. Эти примеры показывают, как технические достижения эпохи Возрождения стали катализаторами научных открытий.

Современные технические достижения играют ключевую роль в содействии научным открытиям. В 2019 году была впервые получена фотография черной дыры, что стало возможным благодаря алгоритму обработки данных Event Horizon Telescope. Этот проект объединил усилия множества телескопов по всему миру, а вычислительные технологии позволили обработать огромные объемы данных для создания изображения. Научное исследование включает в себя не только наблюдение и эксперимент, но и применение различных методов и алгоритмов для анализа данных, выявления закономерностей и формулирова-

ния выводов [1, с.54]. Это достижение подтвердило теоретические предсказания и открыло новые горизонты в астрофизике, демонстрируя, как технологии способствуют расширению научного познания.

Современные технологии оказывают значительное влияние на методы проведения научных исследований, трансформируя подходы к сбору и анализу данных. Проект CRISPR, связанный с редактированием генома, стал возможен благодаря достижениям в области биоинформатики и технологий секвенирования ДНК. Эти инструменты позволяют ученым с высокой точностью изменять генетический материал, открывая новые возможности в медицине и биологии. При этом необходимым является изучение механизмов взаимосвязи научных исследований с развитием техники и технологий. Но сама наука переживает серьезные трансформации: изменяется организация науки, модифицируются способы и методы получения научного знания [5, с.5]. Таким образом, технологии не только способствуют открытиям, но и изменяют саму природу научного исследования, делая его более эффективным и точным.

Технические инструменты играют ключевую роль в научных открытиях, предоставляя исследователям возможность наблюдать и анализировать явления, недоступные для человеческих органов чувств. Изобретение микроскопа Галилеем в 1609 году стало важным шагом в развитии науки, открыв доступ к изучению микромира. Этот инструмент стал основой для фундаментальных открытий, таких как существование клеток и микроорганизмов, что положило начало микробиологии и существенно изменило представления о строении живой материи [11, с.290]. Пример с микроскопом иллюстрирует, как технические достижения способствуют расширению границ научного познания, позволяя ученым исследовать ранее недоступные области. Важность научных открытий подчеркивает В.И.Вернадский, который указывает на огромную роль в научном и экономическом развитии страны, ответственность ученых за применение научных открытий, рассматривая науку в качестве средства развития человечества [2, с.80]. Таким образом, технические инструменты не только открывают новые горизонты для исследования, но и требуют осознанного подхода к их применению в интересах общества.

Некоторые технические достижения не только способствуют новым открытиям, но и кардинально меняют подходы к научным исследованиям. Например, разработка ускорителя частиц, такого как Большой адронный коллайдер, позволила исследовать фундаментальные свойства материи и привела к открытию бозона Хиггса в 2012 году. Это открытие подтвердило существование механизма, объясняющего, как элементарные частицы приобретают массу, что стало важным вкладом в стандартную модель физики. Такие технологии дают возможность проводить эксперименты на ранее недостижимом уровне точности и масштаба, открывая новые горизонты для научных исследований [12, с.98].

Спектроскопы и микроскопы являются одними из ключевых инструментов экспериментальной науки, позволяя исследователям углубляться в микроскопические и атомарные уровни материи. Изобретение микроскопа в 1590 году

Захариасом Янсеном стало революционным шагом, открывшим доступ к изучению микромира, что дало начало таким дисциплинам, как микробиология и клеточная биология. Современные спектроскопические методы, включая масс-спектрометрию, предоставляют возможность анализа химического состава веществ с точностью до атомного уровня, что имеет огромное значение для химии, физики и материаловедения. Эти технологии позволяют ученым получать точные данные, которые являются основой для разработки новых материалов и понимания сложных химических процессов.

Современные технологии моделирования и анализа играют важную роль в экспериментальной науке, предоставляя ученым мощные инструменты для изучения сложных систем. Компьютерное моделирование позволяет исследовать явления, которые невозможно наблюдать напрямую, такие как процессы в космосе или поведение молекул в организме. Технологии анализа данных, включая машинное обучение и искусственный интеллект, помогают обрабатывать огромные объемы информации, выявляя закономерности и создавая прогнозы, которые невозможно было бы сделать вручную. Эти достижения значительно расширяют возможности научных исследований, позволяя ученым решать задачи, ранее считавшиеся неразрешимыми. С другой стороны, наука и техника решают определенные задачи перед обществом и личностью, однако изменить человеческую природу ни наука, ни техника не в силах [7, с.480].

Информационные технологии играют ключевую роль в обработке больших данных, которые стали неотъемлемой частью современного научного исследования. С увеличением объема данных, создаваемых человечеством, который к 2020 году достиг 44 зеттабайт, традиционные методы обработки оказались недостаточно эффективными. Благодаря информационным технологиям стало возможным разрабатывать алгоритмы и системы, способные справляться с анализом и обработкой огромных объемов данных, что способствует получению новых знаний и открытий. Например, использование облачных технологий и распределенных вычислений позволяет ученым обрабатывать данные в масштабах, которые ранее были невозможны. Таким образом, информационные технологии обеспечивают основу для анализа больших данных, значительно ускоряя процесс научного познания [13, с.230].

Современное программное обеспечение играет важнейшую роль в научных исследованиях, предоставляя ученым мощные инструменты для анализа данных и моделирования. Такие программы, как MATLAB и Python, используются более чем в 80% научных исследований, благодаря своей универсальности и возможности адаптации под различные задачи. Эти инструменты позволяют проводить сложные вычисления, визуализировать данные и создавать модели, что делает их незаменимыми в научной среде. Благодаря таким программам, ученые могут эффективно анализировать результаты экспериментов, прогнозировать поведение систем и разрабатывать новые гипотезы. Таким образом, программное обеспечение становится неотъемлемым элементом современного научного процесса, способствуя его развитию.

Автоматизация научных процессов предоставляет исследователям значительные преимущества, включая повышение точности, воспроизводимости и эффективности экспериментов. Например, роботизированные лаборатории, разработанные в Университете Манчестера, способны выполнять сотни экспериментов за неделю, что значительно превышает возможности традиционных методов. Это позволяет ученым сосредоточиться на анализе результатов и разработке новых гипотез, минимизируя временные затраты на рутинные операции. При этом автоматизация снижает влияние человеческого фактора, что способствует уменьшению вероятности ошибок и увеличению надежности полученных данных. В контексте автоматизации важно отметить, что многие задачи дискретной оптимизации сводятся к следующей постановке: определить вектор x = {xi} с дискретными компонентами, минимизирующий аддитивную функцию [8, с.144]. Эта задача является ключевой в автоматизации процессов, поскольку оптимизация позволяет более эффективно распределять ресурсы и время в рамках научных исследований.

Современные технологические достижения, такие как алгоритмы машинного обучения и робототехника, играют ключевую роль в автоматизации научных процессов. Например, алгоритм AlphaFold, разработанный компанией DeepMind, продемонстрировал способность предсказывать структуру белков с высокой точностью, что является значительным шагом в биомедицинских исследованиях. Эти технологии позволяют автоматизировать сложные аналитические процессы, которые ранее требовали значительных временных и человеческих ресурсов, открывая новые возможности для исследований и ускоряя научный прогресс. Вместе с тем приобретение и реализация на практике полученных знаний требует объединенных усилий, интеграции образования, науки и экономики [3, с.119].

Технические знания играют ключевую роль в создании и развитии новых научных методов, способствуя прогрессу в различных областях науки. Изобретение микроскопа в XVII веке стало важной вехой в истории, поскольку оно позволило Роберту Гуку исследовать клеточную структуру растений и впоследствии способствовало формированию клеточной теории. Этот пример демонстрирует, как технические достижения открывают новые горизонты для научных исследований, предоставляя ученым инструменты для более глубокого понимания природы. Важно отметить, что, как подчеркивает Карпов, «метод научных исследований vs метод проектов» [4, с. 16] акцентирует необходимость применения современных технологий для достижения значительных результатов в науке.

Технические знания не только способствуют развитию новых методов, но и играют значительную роль в создании инновационных технологий. Ярким примером этого является разработка квантовой механики в начале XX века, которая стала возможной благодаря сложным математическим методам и техническим инструментам, таким как спектроскопия [14, с.128]. Эти достижения изменили наше представление о микромире и стали основой для множества со-

временных технологий, включая лазеры и полупроводниковые устройства. Современные исследования показывают, что на протяжении XX века изменялись не только основы науки, но и ее организация, что связано с нарастающими процессами технологизации научной деятельности [6, с.6].

Интердисциплинарные подходы играют ключевую роль в современной науке, объединяя знания из различных областей для решения комплексных задач. Эти подходы позволяют использовать методы и концепции одной дисциплины для изучения явлений в другой, что способствует углублению понимания и открытию новых перспектив. Например, проект «Геном человека» стал успешным благодаря объединению усилий биологов, химиков, информатиков и других специалистов, что позволило достичь уникальных результатов в секвенировании генома человека. Этот пример демонстрирует, как взаимодействие различных дисциплин может привести к значительным научным достижениям.

Междисциплинарное взаимодействие имеет важное практическое значение, так как позволяет решать сложные задачи, требующие интеграции различных знаний и навыков. В частности, исследования в области искусственного интеллекта иллюстрируют необходимость сотрудничества между специалистами различных областей, таких как компьютерные науки, психология, нейробиология и этика [15, с.40]. Такое взаимодействие способствует созданию более эффективных и ответственных технологий, которые могут применяться в самых разных сферах, от медицины до образования. Это подчеркивает, что междисциплинарные подходы не только развивают науку, но и оказывают значительное влияние на повседневную жизнь.

Технические знания играют ключевую роль в решении современных экологических проблем, предоставляя ученым и инженерам инструменты и методы для разработки эффективных решений. Например, использование технологий возобновляемой энергии, таких как солнечные панели и ветрогенераторы, способствовало значительному снижению выбросов углекислого газа. Согласно отчету ООН, в 2020 году благодаря этим технологиям выбросы сократились на 10%. Это подчеркивает важность внедрения технических знаний в экологические проекты, направленные на сохранение окружающей среды и снижение антропогенного воздействия. Вместе с тем, необходимо учитывать, что техника рассматривается как явление культуры, взаимосвязанное с наукой, политикой, экономикой и моралью. Такой комплексный подход необходим для эффективного решения экологических задач, поскольку он позволяет учитывать различные аспекты и факторы, влияющие на состояние окружающей среды.

Инновационные технологии предоставляют уникальные возможности для обеспечения устойчивого развития, способствуя рациональному использованию природных ресурсов и минимизации вреда окружающей среде [16, с.152]. Примером такого подхода являются батареи Powerwall, представленные компанией Tesla в 2018 году, которые позволяют эффективно хранить энергию, полученную от солнечных панелей. Эти технологии демонстрируют, как технические знания могут быть применены для создания решений, поддерживающих устойчивое

развитие, и подчеркивают необходимость дальнейшего инвестирования в инновации, направленные на устойчивость и экологическую безопасность.

Искусственный интеллект (ИИ) становится важным инструментом в научных исследованиях благодаря своей способности анализировать огромные массивы данных с высокой скоростью и точностью. В 2020 году ИИ был использован для анализа данных о COVID-19, что значительно ускорило разработку вакцин. Это демонстрирует, как современные технологии могут способствовать быстрому решению глобальных научных задач. С другой стороны, ИИ активно применяется в таких областях, как астрономия, биология и медицина, где он помогает моделировать сложные системы и прогнозировать их поведение. Как отмечается, на сегодняшний день имеется достаточно много научно обоснованных наработок по вопросам реализации возможностей информационных технологий в различных сферах деятельности, развития у пользователей уровня культуры их применения [9, с.80]. Таким образом, искусственный интеллект открывает новые горизонты для науки, повышая ее эффективность и расширяя возможности исследований.

Биотехнологии играют ключевую роль в развитии современной науки, предоставляя новые инструменты и методы для изучения и изменения биологических систем. Одним из ярких примеров является деятельность компании CRISPR Therapeutics, которая использует технологии редактирования генома для разработки методов лечения генетических заболеваний. Эти достижения становятся возможными благодаря сочетанию научных знаний и технических инноваций, что позволяет решать задачи, ранее считавшиеся неподъемными. Биотехнологии оказывают влияние на такие области, как медицина, сельское хозяйство и экология, изменяя подходы к решению глобальных проблем и создавая новые перспективы для научных исследований.

Этические аспекты применения научных технологий становятся все более актуальными по мере их развития. Ярким примером служит технология CRISPR-Cas9, используемая для редактирования генома человека. Эта инновация открывает значительные возможности для лечения генетических заболеваний, однако одновременно поднимает множество этических вопросов. Вмешательство в наследственный материал может оказать влияние на будущие поколения, что порождает опасения относительно непредвиденных последствий. Кроме того, существует риск злоупотребления данной технологией, что подчеркивает необходимость разработки строгих этических норм и международного регулирования. При этом важно учитывать, что для обеспечения устойчивого развития науки и техники необходимо внедрять отечественные системы и продукты. Это, в свою очередь, поможет насытить рынок продукцией, которая будет постепенно интегрироваться в производство и использование [10, с.124].

Социальные последствия внедрения инноваций также играют важную роль в оценке их влияния. Технологии искусственного интеллекта, например, вызывают обеспокоенность относительно их воздействия на рынок труда и конфиденциальность данных. Согласно исследованию Pew Research Center, 72% аме-

риканцев считают, что такие технологии должны быть строго регулируемы для предотвращения негативных социальных последствий. Это подчеркивает необходимость общественного диалога и разработки соответствующих законодательных мер, чтобы минимизировать риски и обеспечить справедливое распределение выгод от использования новых технологий.

Прогнозирование научных открытий основывается на современных методах анализа данных и моделирования. Ключевым подходом является применение искусственного интеллекта и машинного обучения для выявления скрытых закономерностей в больших объемах научной информации. Эти технологии не только предсказывают возможные направления исследований, но и оптимизируют процесс поиска решений сложных задач. Важно отметить, что научное исследование является фундаментальным процессом, лежащим в основе развития знаний и практического применения в различных областях науки и техники [7, с.487]. Проект Human Brain Project, начатый в 2013 году, иллюстрирует использование прогнозирования для создания компьютерной модели человеческого мозга, что в свою очередь способствует развитию нейронаук и медицины.

Успешные примеры прогнозирования научных открытий на основе технических достижений включают разработку алгоритмов, таких как AlphaGo от Google DeepMind, который в 2016 году продемонстрировал потенциал искусственного интеллекта в решении сложных задач. Этот успех подчеркивает важность использования передовых технологий для достижения новых высот в науке. Стоит отметить, что переход к инновационному развитию страны был определен как основная цель государственной политики в области развития науки и технологий [10, с.123]. С другой стороны, в области биологии и медицины прогнозирование на основе анализа геномных данных открывает возможности для разработки персонализированных подходов к лечению заболеваний, что, в свою очередь, способствует улучшению качества жизни.

Таким образом, в ходе проведенного исследования была рассмотрена роль техники, технологий и технического знания в развитии науки. Мы проанализировали исторические примеры, начиная с древности до современности, которые иллюстрируют, как технические достижения способствовали научным открытиям. Рассмотрены современные технологии, которые трансформируют методы научного исследования и способствуют развитию новых направлений. Исследование подтвердило, что техника и технологии являются неотъемлемой частью научного прогресса.

На основании проведенного анализа можно сделать вывод, что техническое знание играет ключевую роль в развитии науки. Оно способствует созданию новых инструментов и методов, которые позволяют ученым достигать более глубокого понимания изучаемых явлений. Современные технологии, такие как автоматизация и информационные системы, значительно повышают эффективность научных исследований. Кроме того, междисциплинарный подход, основанный на использовании технических знаний, открывает новые горизонты для научных открытий.

Перспективы дальнейших исследований в данной области включают изучение влияния новых технологий, таких как искусственный интеллект и квантовые вычисления, на развитие науки. Также важно рассмотреть этические и социальные аспекты применения технических достижений. Будущие работы могут сосредоточиться на разработке интегративных подходов, объединяющих технические знания из различных областей, для решения глобальных научных и прикладных задач.

Список источников

1. Галимова, А. Д. особенности культурологической оценки техники / А. Д. Галимова // Ростовский научный вестник. – 2022. – № 1. – С. 54-55.
2. Жилкина, А. А. Наука и техника как предмет философской рефлексии / А. А. Жилкина // Вестник Тюменского государственного института культуры. – 2023. – № 4(30). – С. 79-81.
3. Калиновская, Т. Г. Треугольник знаний как фактор инновационного развития / Т. Г. Калиновская, С. А. Косолапова, А. В. Прошкин // Современные наукоемкие технологии. – 2010. – № 10. – С. 118-120.
4. Карпов, А. О. Метод научных исследований VS метод проектов / А. О. Карпов // Педагогика. – 2012. – № 7. – С. 14-25.
5. Лаврикова, Н. И. Инновационная экономика: технологические стандарты и конкурентное поведение / Н. И. Лаврикова, И. Г. Кочергин // Экономические и гуманитарные науки. – 2024. – № 5(388). – С. 3-13. – DOI 10.33979/2073-7424-2024-388-5-3-13.
6. Лаврикова, Н. И. тенденции развития инновационной экономики в рамках технологической сингулярности / Н. И. Лаврикова, Л. А. Третьякова // Экономические и гуманитарные науки. – 2023. – № 12(383). – С. 3-11. – DOI 10.33979/2073-7424-2023-383-12-3-11.
7. Новосельский, С. О. Характеристика цифровизации науки и образования / С. О. Новосельский, В. П. Сморчкова, И. Г. Морозова // Евразийский Союз: вопросы международных отношений. – 2023. – Т. 12, № 5(51). – С. 474-486. – DOI 10.35775/PSI.2023.51.5.004.
8. Ребров, С. Д. Взаимосвязь научно-технического потенциала и экономической безопасности / С. Д. Ребров, И. А. Агафонов // Вестник Алтайской академии экономики и права. – 2018. – № 7. – С. 142-147.
9. Русяева, Е. Ю. Концептуальные основы теории активных систем, их развитие в теории управления организационными системами: тенденции и перспективы / Е. Ю. Русяева, С. А. Салтыков // Проблемы управления. – 2017. – № 4. – С. 74-83.
10. Санина, А. Г. Условия интеграции науки, образования и бизнеса в современной России / А. Г. Санина // Социологические исследования. – 2010. – № 7(315). – С. 122-129.

11. Степанова, Т. А. Обзор качества данных / Т. А. Степанова, Л. Н. Измайлова // Russian Economic Bulletin. – 2023. – Т. 6, № 4. – С. 285-293.

12. Хамдамов, Т. В. Трансцендентальное учение Канта или пользовательская методичка разработчика компьютерных симуляций научных экспериментов / Т. В. Хамдамов // Речевые технологии. – 2020. – № 3-4. – С. 96-106. – DOI 10.58633/2305-8129_2020_3-4_96.

13. Чеботарева, Е. Э. Проекты Digital Humanities как этап развития гуманитарной науки: попытка метацифрового взгляда / Е. Э. Чеботарева // Эпистемология и философия науки. – 2023. – Т. 60, № 2. – С. 224-240. – DOI 10.5840/eps202360234.

14. Штейнберг, В. Э. Визуальные дидактические регулятивы как инструменты учебной деятельности: развитие и прикладные аспекты / В. Э. Штейнберг, Н. Н. Манько, Л. В. Вахидова, Д. Р. Фатхулова // Образование и наука. – 2021. – Т. 23, № 6. – С. 126-152. – DOI 10.17853/1994-5639-2021-6-126-52.

15. Kornelaki, A. C. Educational Program «Thunderbolt Hunt»: An Analysis with the «Experimental-Genetic Method» / A. C. Kornelaki, K. Plakitsi // Cultural-Historical Psychology. – 2020. – Vol. 16, No. 3. – P. 38-46. – DOI 10.17759/chp.2020160305.

16. Zhang, Ch. The specificity of virtual reality technology in treating depression in adolescents / Ch. Zhang // Психология когнитивных процессов. – 2022. – No. 11. – P. 151-156.

УДК 04.91:7.067

ГЛАВА 2. О ПРОЕКТИРОВАНИИ УНИВЕРСАЛЬНОЙ СИСТЕМЫ АНАЛИЗА И ВИЗУАЛИЗАЦИИ МИГРАЦИОННЫХ ДАННЫХ

Рудикова-Фронхёфер Лада Владимировна
к. ф.-м. наук, доцент,
Аршун Валерий Валерьевич
магистрант,
Учреждение образования «Гродненский государственный университет имени Янки Купалы»

Аннотация: в работе описываются подходы к проектированию системы анализа и представления в визуальной форме миграционных данных по странам мира. Демонстрируется возможность применения различных методов, например, методов прогнозирования данных, машинного обучения и др. Соответственно, приводятся примеры подходящих методов для реализации универсальной системы анализа и визуализации соответствующих данных миграционного типа.
Ключевые слова: миграция населения, методы описательной статистики, методы прогнозирования данных, машинное обучение, проектирование, анализ данных.

APPLICATION OF MACHINE LEARNING ON GRAPHS IN PREDICTING TRANSPORT TRAFFIC ACROSS THE COUNTRY

Rudikova-Fronhoefer Lada Vladimirovna,
Arshun Valery Valerievich

Abstract: The article describes approaches to designing a system for analyzing and visualizing migration data by countries in the world. It demonstrates the possibility of using various methods, such as data forecasting methods, machine learning, etc. Accordingly, examples of suitable methods for implementing a universal system for analyzing and visualizing the corresponding migration-type data are given.
Key words: migration of population, methods of descriptive statistics, methods of data forecasting, machine learning, design, data analysis.

Миграцией населения является любое территориальное перемещение населения, связанное с пересечением как внешних, так и внутренних границ на постоянной или временной основе. Более глобальным явлением можно считать внешний подтип миграции, который охватывает перемещение населения из одной страны в другую или даже несколько. Внутренний подтип миграции рассматривает перемещение населения в пределах какой-то конкретной страны, а,

именно, из одной её части в другую. Внешняя миграция подразделяется на иммиграцию, а именно переезд населения в другую страну по какому-либо постоянному или временному поводу, и эмиграцию – выезд из своей страны на постоянной или временной основе.

Миграция человека задолго до начала «нашей эры» ускоряла передачу знаний и, следовательно, развитие человечества в различных отраслях. После налаживания взаимоотношений между большинством стран мира и расширения глобализации миграция приобрела характер, более развивающий в экономическом и демографическом плане, поэтому она является крайне востребованной для изучения даже сейчас.

Результатами изучения миграционных процессов являются обработанные статистические данные в той или иной форме, которые отражают ситуацию как на сегодняшний день, так и позволяют построить тренды для ближайшего будущего. Первопричины различия этих данных на конкретном временном отрезке зачастую учитываются отдельно при дальнейшем рассмотрении.

Для личного изучения первичных миграционных данных имеется возможность их получения из открытых государственных источников или учреждений, занимающихся их сбором и обработкой. Однако такие данные являются неудобными для анализа с помощью каких-либо программных инструментов, так как из каждого источника они получаются в разном формате и в некоторых случаях содержат излишнюю информацию.

Анализ миграционных данных как процесс обработки, исследования и интерпретации информации используется для выявления их закономерностей и принятии решений относительно полученных результатов. Он включает в себя сбор, очистку, обработку, визуализацию и моделирование данных. Сбор данных может быть осуществлен из баз данных, опросов или API, а сами данные изначально могут быть как структурированы (например, таблицах), так и неструктурированы (текст или изображения) [5]. Очистка данных осуществляет удаление пропущенных или аномальных значений, приведение них к общему формату, их нормализацию и стандартизацию. Исследование данных может представлять из себя вычисление статистик (среднего, медианы или дисперсии), определение выбросов или аномалий и разработку визуальных форм представления (гистограмм или диаграмм рассеивания). моделирование и прогнозирование данных в результате может предоставить регрессионные модели (линейные или экспоненциальные), классификационные формы (деревья решений или нейросети) или кластерные формы (k-means или DBSCAN) [13].

Второй основной функцией, кроме анализа данных, является их последующее отображение и визуализация в различных формах. Результаты такой обработки должны быть представлены наглядно, чтобы в дальнейшем можно было сделать достаточно быстрый прогноз.

Целью исследования данной работы является проектирование и реализация прототипа системы анализа и представления миграционных данных по странам мира, которая может быть как расширена в основном функционале, так

и за счет отдельных функциональных блоков.

Проектирование архитектуры системы для анализа и представления миграционных данных основывается на методологии структурного анализа и проектирования, которая позволяет построить такие модели как модель данных, модель функций и модель интерфейсов системы.

В моделировании данных используются графические средства и приемы, позволяющие наглядно описать используемую в системе информацию [10, 19]. Так, основой моделирования является, как правило, ER-методология, которая описывает основные сущности и их взаимосвязи. В процессе проектирования данных получается концептуальная, логическая и физическая модели. В первой абстрактно представляются данные без привязки в СУБД, где описываются основные сущности, их свойства и взаимосвязи. Вторая предоставляет более детализированную структуру объектов, где отображаются их типы и ограничения. В третьей модели описывается реализация для конкретной СУБД, где учитывается уникальные для неё компоненты и оптимизация хранения и запросов.

При моделировании функций используются графические средства, позволяющие отобразить взаимодействие пользователей с системой, последовательность работы с ней, ее компоненты и их структуру. Как правило, при моделировании функций применяются UML-нотации, которые позволяют отобразить различные аспекты системы с помощью соответствующих инструментов, и получить диаграммы различных типов – диаграмму вариантов использования, диаграмму последовательности, диаграмму компонентов и т.д.

Для обработки нормализированных и стандартизированных данных применяются методы описательной статистики, методы прогнозирования или машинного обучения, результатами использования которых могут быть как промежуточные данные для других операций, так и окончательные данные для формирования каких-либо заключений.

Описательная статистика является совокупностью методов, помогающих описывать и интерпретировать данные. Она позволяет понять основные характеристики данных и выявить их закономерностей и аномалии.

Среднее арифметическое определяет среднее значение всех наблюдений:

$$x^{-} = \frac{1}{2}\sum_{n=1}^{\infty} x_i,$$

где x^{-} – среднее,

x_i – значение выборки,

n – количество элементов.

Метод чувствителен к экстремально большим или маленьким значениям.

Медиана сортирует данные и берёт центральное значение. Если n – нечетное, то $x^{-} = x_{\frac{n+1}{2}}$, если n – четное, то $x^{-} = \frac{x_{\frac{n}{2}} + x_{\frac{n+1}{2}}}{2}$.

Медиану лучше использовать при наличии выбросов, так как она не учитывает крайние значения:

$$x^{-} = \frac{1}{2}\sum_{n=1}^{\infty} x_i,$$

где $\bar{x}$ – среднее,

x_i – значение выборки,

n – количество элементов.

Метод чувствителен к экстремально большим или маленьким значениям.

Размах показывает, насколько данные различаются в выборке:

range = $x_{max} - x_{min}$.

Размах неустойчив к выбросам [8].

Дисперсия является средним квадратом отклонений от среднего:

$$r^2 = \frac{1}{n}\sum_{i=1}^{n}(x_i - \bar{x})^2.$$

Для выборочной дисперсии:

$$r^2 = \frac{1}{n-1}\sum_{i=1}^{n}(x_i - \bar{x})^2,$$

где n – используется для корректировки смещения в малых выборках генеральной совокупности. Квадратный корень из дисперсии информирует о том, что чем он больше, тем более разбросанные данные.

Эксцесс показывает, на сколько остроконечно распределение:

$$k = \frac{\frac{1}{2}\sum_{i=1}^{n}(x_i - \bar{x})^4}{r^4} - 3.$$

Если $k > 0$ – имеет место острое распределение, если $k = 0$ – нормальное распределение, если $k < 0$ – плоское распределение.

Асимметрия показывает, есть ли перекос в данных:

$$s = \frac{\frac{1}{n}\sum_{i=1}^{n}(x_i - \bar{x})^3}{r^3}.$$

Если $s > 0$ – имеет место правосторонняя асимметрия, если $s = 0$ – симметричное распределение, если $s < 0$ – левосторонняя асимметрия.

Коэффициент Спирмена используется в том случае, если данные не нормальны или зависимость нелинейная:

$$s = 1 - \frac{6*\sum_{i=1}^{n}(x_i)^2}{n*(n^2-1)},$$

где x_i – разница между x и y,

n – количество наблюдений.

Данный коэффициент аналогичен коэффициенту Пирсона, но подходит для монотонных зависимостей (возрастающих или убывающих) и не обязательно линейных. Он также не чувствителен к выбросам.

Методы для прогнозирования данных основываются на временных рядах, которые являются последовательностью наблюдений, упорядоченных по времени, например, ежемесячные продажи или число мигрантов по годам). Их можно представить в виде:

$$y_i = T_i + S_i + C_i + \varepsilon_i,$$

где T_i – долгосрочная тенденция,

S_i – периодические колебания,

C_i – непериодические колебания,

ε_i – случайные шумы.

Данная модель содержит независимые и немасштабируемые компоненты.

Эффекты компонентов мультипликативной модели усиливаются при росте тренда: $y_i = T_i * S_i * C_i * \varepsilon_i$.

Методами вычисления долгосрочной тенденции являются скользящее среднее:

$$MA_k = \frac{1}{k}\sum_{i=0}^{k-1} y_{t-i},$$

где k – окно усреднения,

и линейная регрессия:

$$y_k = a + b * t,$$

где a и b находятся методом наименьших квадратов.

Периодические колебания выявляются при наличии периодических колебаний с помощью метода скользящего среднего $S_i = y_i - T_i$.

При зависимости текущего значения ряда от предыдущих, то используется автокорреляция по формуле:

$$r_k = \frac{\sum_{t=1}^{n-k}(y_t - \bar{y})(y_{t+k} - \bar{y})}{\sum_{t=1}^{n}(y_t - \bar{y})^2},$$

где k – задержка во времени.

Для прогнозирования временных рядов может использоваться линейная регрессия при отсутствии периодических колебаний:

$$y_k = a + b * t + \varepsilon_i,$$

а также – экспоненциальная регрессия, если следует учитывать более новые наблюдения:

$$S_i = a * y_i - (1 - a) * S_i,$$

где S_i – сглаженное значение,

a – параметр от 0 до 1 [4, 9].

Модель ARIMA (p, d, q) одновременно использует предыдущие значения для предсказания будущих, скользящее среднее (прошлые ошибки модели) и убирает долгосрочную тенденцию с помощью дифференцирования [3, 12]. Она использует формулу:

$$y_t = c + \phi_1 * y_{t-1} + \phi_2 * y_{t-2} + \phi_p * y_{t-p} + \varepsilon_t,$$

где ϕ_1, ϕ_2 и т.д. – коэффициенты регрессии,

ε_t – случайная ошибка,

p – количество автопредсказаний,

d – степень дифференцирования, убирающая долгосрочную тенденцию,

q – количество запаздывающих ошибок.

Машинное обучение является областью искусственного интеллекта, благодаря которой имеется возможность определять закономерности в данных и делать прогнозы без явного программирования правил [2, 15]. Она особенно важна в работе со сложными данными, например, с большим числом признаков, когда данные не подчиняются линейным закономерностям или с большим объемом данных [14].

Обучение с учителем основывается на создании модели, которая учится

предсказывать целевую переменную y по входным данным X с формальной постановкой

$$y = f(X) + \varepsilon,$$

где ε – случайная ошибка.

Обучение с учителем используется для формирования логистической регрессии, линейной регрессии и т.п.

Обучение без учителя не имеет целевой переменной, а модель находит скрытые структуры в данных, которые впоследствии используются для их кластеризации или снижения размерности [16, 17].

Обучение с подкреплением основывается на изучении «агентом» взаимодействия со средой, максимально увеличивая вознаграждение за верные решения, определяемые разработчиком [18]. Формальная модель:

$Q(s,a)=R(s,a)+\gamma*maxQ(s',a')$,

где $Q(s,a)$ – ценность a в состоянии s,

где $R(s,a)$ – награда за действие,

γ – коэффициент учета будущих наград. Оно может применяться в таких областях как робототехника, обучение искусственного интеллекта игре в шахматы и т.п.

Одним из популярных методов моделирования объектно-ориентированных систем является язык UML. Он позволяет отображать комплексную систему в виде простых частей, которые могут быть изучены отдельно друг от друга. В результате использование моделирования решает две задачи по ходу проектирования системы, а именно понятность и повторное использование. Это также позволяет сразу решать возможные возникшие проблемы на уровне простых частей, к примеру, их функциональную или структурную избыточность.

На рисунке 1 представлена диаграмма вариантов использования для системы анализа и визуализации миграционных данных. Основными пользователями итоговой системы являются администратор и конечный пользователь. Первый предоставляет актуальные нормализированные данные по странам мира, с которыми работает второй. Дополнительно у него имеется возможность проверить с помощью функционала системы корректность отображения конкретных данных, если в этом есть необходимость. Как было отмечено ранее, второй пользователь является ответственным за наличие первичных данных в системе, так как он может них добавлять, удалять и редактировать по своему усмотрению. Также он имеет доступ к работе с глобальной картой и графиками для визуализации обработанных данных. другой – на корреляции трафика между близкими вершинами. Диаграмма вариантов использования приведена на рисунке 1.

Диаграмма последовательности отображает взаимодействия объектов, упорядоченных по времени их проявления. Она представлена в двух осях. Вертикальная ось содержит все объекты, участвующие в общем взаимодействии, в виде прямоугольников с их названием внутри. Объекты расположены сверху вниз в зависимости от их времени начала участия во взаимодействии. От каж-

дого объекта в горизонтальной оси протянута линия, от которой протягиваются второстепенные вертикальные линии, характеризующие определённое действие и содержащее его название, к горизонтальным линиям других объектов. Зачастую на линии, к которой обращено действие, отображается прямоугольник, характеризующий однозначность направления действия. На линии, которая отправляла сообщение на действие, прямоугольник для ответной линии не содержится Горизонтальные линии каждого объекта протянуты на всю горизонтальную плоскость, так как они существуют в системе на протяжении всей ещё работы.

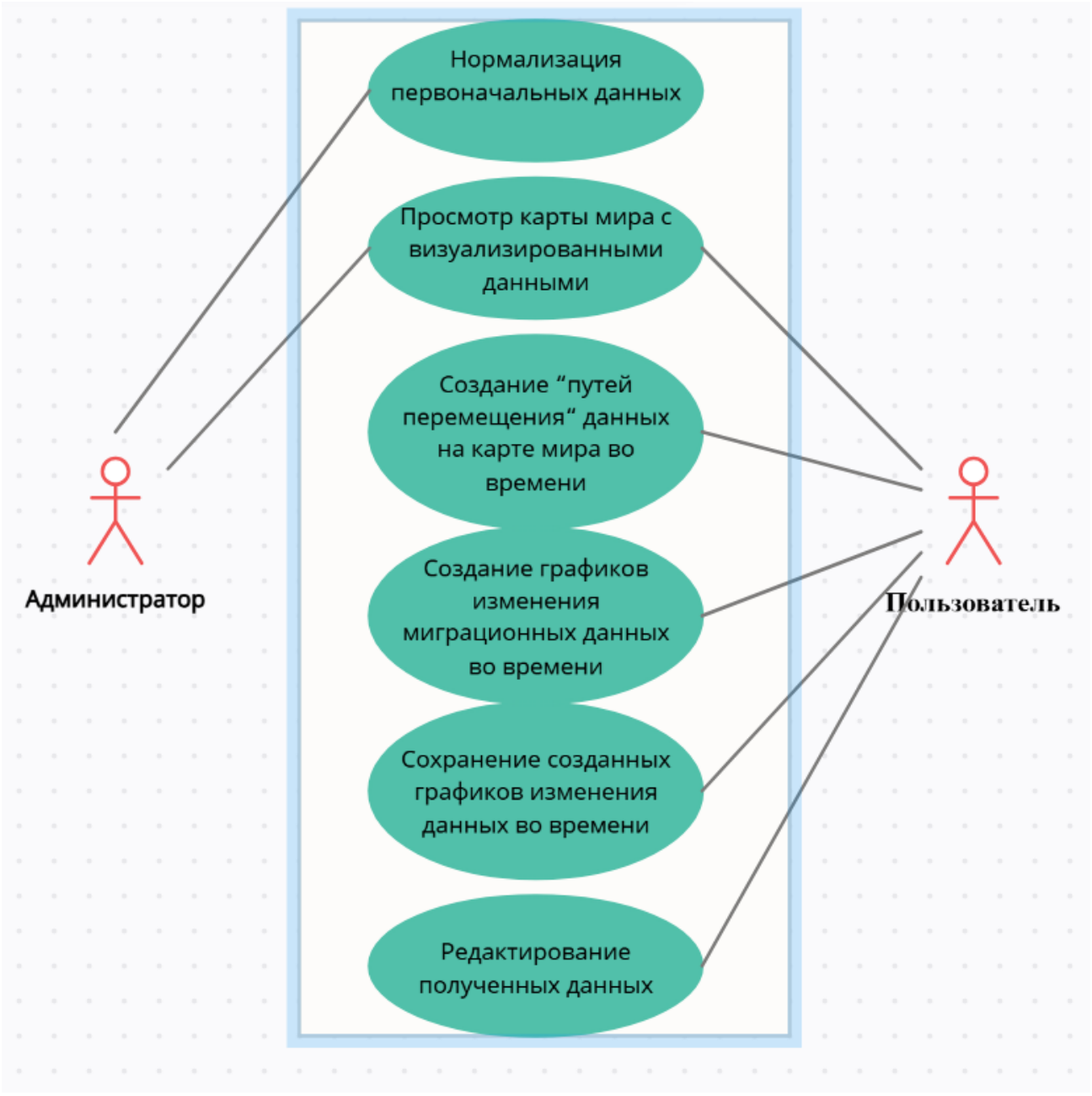

Рис. 1. Диаграмма вариантов использования

Диаграмма последовательности системы представлена на рисунке 2.

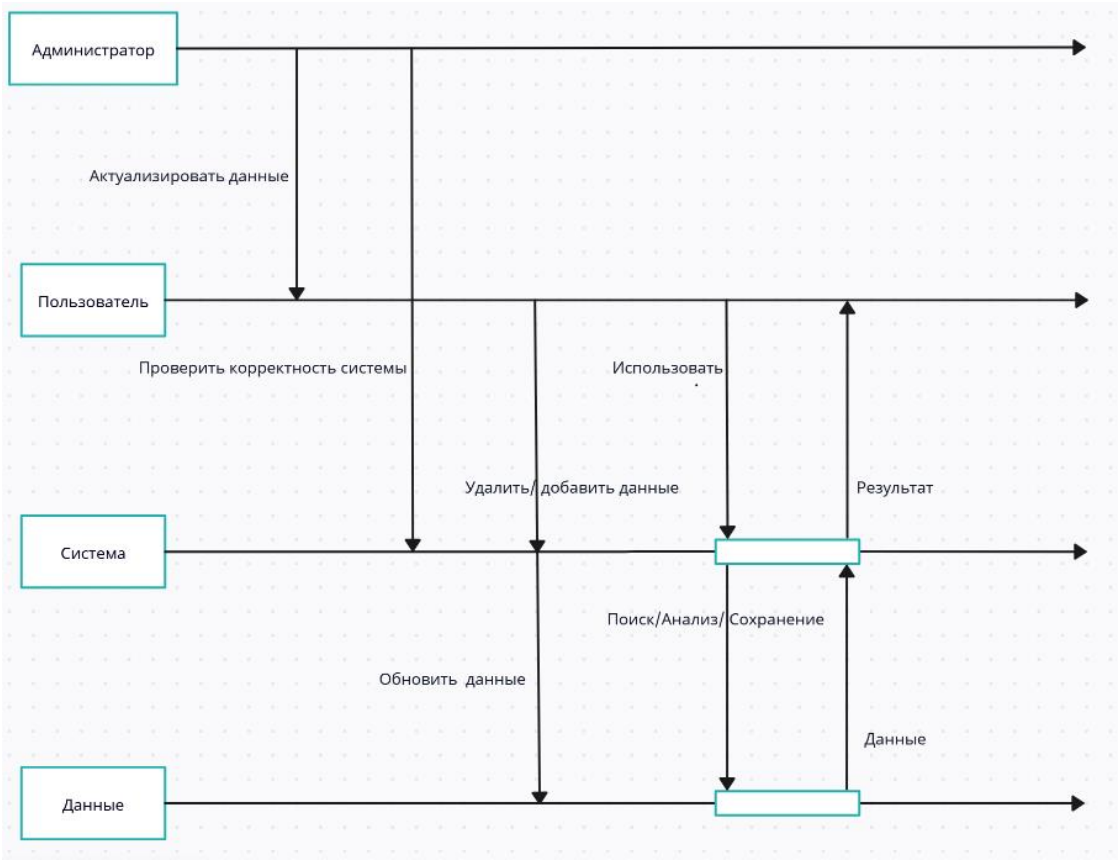

Рис. 2. Диаграмма вариантов использования

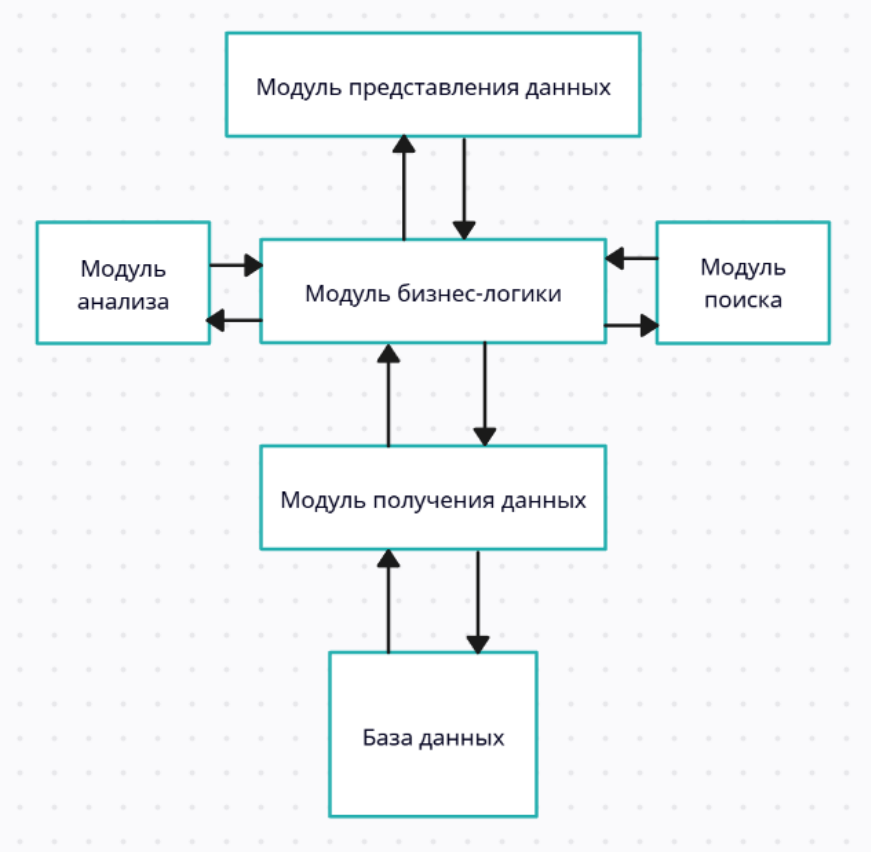

Рис. 3. Диаграмма компонентов

Диаграмма компонентов отображает отдельные структурные элементы системы и их зависимость между друг другом. Физически они могут быть как программными модулями или библиотеками, так и исполняемыми файлами.

На рисунке 3 представлена диаграмма компонентов разрабатываемой системы. Файлы с первичными данными являются основой моделей данных, создаваемых конечным пользователем, которые поставляются в модуль получения. В него отправляет запрос модуль бизнес-логики, который сочетает в себе функции анализа и поиска данных, которые через него модуль представления данных передает конечному пользователю. Сохраненные графики передаются в обратном порядке в базу данных.

Определение степени линейной взаимосвязи между двумя переменными может быть определено с использованием коэффициента корреляции Пирсона. Он используется в случаях, если данные нормально распределены, имеют линейную зависимость и являются интервальными или метрическими шкалами.

Коэффициент вычисляется по следующей формуле:

$$x = \frac{\sum(x_i - \bar{x})(y_i - \bar{y})}{(\sum(x_i - \bar{x})^2 * \sum(y_i - \bar{y})^2)^{0.5}},$$

где x_i, y_i – значения двух переменных,

$\bar{x}$ и $\bar{y}$ – их средние значения:

$\bar{x} = \frac{1}{2}\sum_{n=1}^{\infty} x_i$, $\bar{y} = \frac{1}{2}\sum_{n=1}^{\infty} y_i$,

где n – количество парных наблюдений. Если $n > 1$ – имеет место идеальная прямая зависимость, $n = 1$ – имеет место идеальная обратная зависимость, $n = 0$ – нет связи между переменными.

Коэффициент широко применяется в статистике и машинном обучении за счет простоты вычисления и интерпретации, но при этом он чувствителен к выбросам, не выявляет нелинейные зависимости и требует нормального распределения данных.

Отметим также, что поиск подстроки в строке списка стран мира может быть реализован с помощью алгоритма Хорспула [6]. Вместо последовательного сравнения символов, как в наивном поиске, он использует таблицу сдвигов, чтобы пропустить ненужные сравнения, перемещая шаблон дальше по строке.

Алгоритм Хорспула использует эвристическое смещение для ускоренного поиска подстроки в тексте [7]. Для каждого символа с в шаблоне кроме последнего, смещение определяется как:

$$shift(c) = m - 1 - i,$$

где m – длина шаблона,

i – индекс символа c в шаблоне, начиная с 0. Если символ отсутствует в шаблоне, смещение принимается равным m по умолчанию. После сравнения, если совпадения не найдено, следующий индекс рассчитывается по формуле:

$$i = i + shift(text[i]),$$

где $text[i]$ – текущий символ в тексте на позиции i.

Применение алгоритма перспективно в длинных строках с большим алфавитом и за счет простой реализации, но он не учитывает некоторые улучшения

от алгоритма Бойера-Мура, который является неупрощенным.

Прогнозирование данных с определённым экспоненциальным ростом или уменьшением в сфере миграции может быть реализовано с помощью экспоненциальной регрессии. Для её получения определяются форма и коэффициенты регрессии, а её качество регулируется вследствие полученных с помощью неё результатов.

Уравнение экспоненциальной регрессии высчитывается по формуле:

$$y = a * e^{b*x},$$

где y – предсказанное значение,

x – независимая переменная,

a и b – коэффициенты, определяемые методом наименьших квадратов,

e – математическая константа, приблизительно равная 2,718.

Экспоненциальная регрессия используется для моделирования и анализа зависимости между целевой переменной и несколькими независимыми. При её использовании важно учитывать необходимость использования сложных моделей для нелинейных зависимостей и возможную высокую корреляцию между независимыми переменными.

Для реализации универсальной системы анализа и визуализации миграционных данных рекомендуется использовать шаблон MVC, который позволяет разбить систему на четкие функциональные модули с возможностью расширения и минимальной зависимостью друг от друга [11].

Отметим, что MVC (Model-View-Controller) – шаблон разбиения данных приложения и управляющей логики на модель, представление и контроллер так, чтобы изменение элементов системы осуществлялось независимо друг от друга. Модель предоставляет данные и реагирует на команды контроллера, изменяя своё состояние. Представление отвечает за отображение данных модели пользователю, реагируя на изменения модели. Контроллер интерпретирует действия пользователя, оповещая модель о необходимости изменений.

В данной системе шаблон MVC может быть представлен следующим образом: слой модели, взаимодействующий с первичными данными, слой контроллера, содержащий сервисы и бизнес-логику и взаимодействующий с моделью и представлением, слой представления, визуализирующий проанализированные данные.

Создание системы может быть осуществлено с помощью игрового движка Godot, благодаря которому программная реализация системы выполнена встроенными инструментами. Он использует собственный оптимизированный скриптовый язык GDScript, обладающий простым синтаксисом и высокой интеграцией, уникальную структуру сцены, состоящую из узлов, которая позволяет создавать сложные игровые объекты через комбинацию простых элементов, гибкую систему анимаций, включающую анимационные деревья, графы и редактор AnimationPlayer, механизм сигналов, позволяющий узлам взаимодействовать друг с другом без жёсткой привязки к конкретным объектам и другой востребованный функционал, с помощью которого имеется возможность реали-

зовать спроектированную систему.

Универсальная система анализа и визуализации миграционных данных может быть использована любыми организациями или предприятиями, работа которых частично или полностью основывается на постоянном или временном экономико-социальном перемещении населения [1, 19].

Список источников

1. Министерство связи и информатизации Республики Беларусь [Электронный ресурс] / О проекте «Умные города Беларуси» – Режим доступа: https://mpt.gov.by/ru/o-proekte-umnye-goroda-belarusi. – Дата доступа: 14.04.2025.

2. VK Cloud [Электронный ресурс] / 17 примеров применения машинного обучения в 5 отраслях бизнеса – Режим доступа: https://mcs.mail.ru/blog/17-primerov-mashinnogo-obucheniya. – Дата доступа: 4.04.2025.

3. Karen Simonyan, Very Deep Convolutional Networks for Large-Scale Image Recognition [Electronic resource] // Karen Simonyan, Andrew Zisserman // arXiv.org e-Print archive – Mode of access: https://arxiv.org/abs/1409.1556. – Date of access: 4.04.2025.

4. Хабр [Электронный ресурс] / LSTM – сети долгой краткосрочной памяти – Режим доступа: https://habr.com/ru/companies/wunderfund/articles/331310/. – Дата доступа: 14.04.2025.

5. Ashish Vaswani, Attention Is All You Need [Electronic resource] / Ashish Vaswani [et al.] // arXiv.org e-Print archive – Mode of access: https://arxiv.org/abs/1706.03762. – Date of access: 10.04.2025.

6. Rex Ying, Graph Convolutional Neural Networks for Web-Scale Recommender Systems [Electronic resource] / Rex Ying [et al.] // 24th ACM SIGKDD Conference on Knowledge Discovery and Data Mining, London, 19-23 August, 2018 // arXiv.org e-Print archive – Mode of access: https://arxiv.org/abs/1806.01973. – Date of access: 14.04.2025.

7. Marinka Zitnik, Modeling polypharmacy side effects with graph convolutional networks [Electronic resource] / Marinka Zitnik, Monica Agrawal, Jure Leskovec // 26th Conference of Intelligent Systems for Molecular Biology, Chicago, 6-10 July, 2018 // arXiv.org e-Print archive – Mode of access: https://arxiv.org/abs/1802.00543. – Date of access: 10.04.2025.

8. Department of Mathematics. Ohio State University [Electronic resource] / Random Walks on Graphs – Mode of access: https://people.math.osu.edu/husen.1/teaching/571/random_walks.pdf. – Date of access: 14.04.2025.

9. Petar Veličković, Graph Attention Networks [Electronic resource] / Petar Veličković [et al.] // 6th International Conference on Learning Representations, 2018 // arXiv.org e-Print archive – Mode of access: https://arxiv.org/abs/1710.10903. – Date of access: 11.04.2025.

10. Thomas N. Kipf, Semi-Supervised Classification with Graph Convolutional

Networks [Electronic resource] / Thomas N. Kipf, Max Welling // 5th International Conference on Learning Representations, 2017 // arXiv.org e-Print archive – Mode of access: https://arxiv.org/abs/1609.02907. – Date of access: 11.04.2025.

11. DeepMind [Electronic resource] / ETA Prediction with Graph Neural Networks in Google Maps – Mode of access: https://www.deepmind.com/publications/eta-prediction-with-graph-neural-networks-in-google-maps. – Date of access: 11.04.2025.

12. Renhe Jiang, MegaCRN: Meta-Graph Convolutional Recurrent Network for Spatio-Temporal Modeling [Electronic resource] / Renhe Jiang [et al.] // arXiv.org e-Print archive – Mode of access: https://arxiv.org/abs/2212.05989. – Date of access: 14.04.2025.

13. Zezhi Shao, Pre-training Enhanced Spatial-temporal Graph Neural Network for Multivariate Time Series Forecasting [Electronic resource] / Zezhi Shao [et al.] // 28th ACM SIGKDD Conference on Knowledge Discovery and Data Mining, Washington, 14-18 August, 2022 // arXiv.org e-Print archive – Mode of access: https://arxiv.org/abs/2206.09113v2. – Date of access: 8.04.2025.

14. DeepMind [Electronic resource] / AlphaFold: a solution to a 50-year-old grand challenge in biology – Mode of access: https://www.deepmind.com/blog/alphafold-a-solution-to-a-50-year-old-grand-challenge-in-biology. – Date of access: 10.04.2025.

15. DeepMind [Electronic resource] / Learning to Simulate Complex Physics with Graph Networks – Mode of access: https://www.deepmind.com/open-source/learning-to-simulate-complex-physics-with-graph-networks. – Date of access: 12.04.2025.

16. Seyed Mehran Kazemi, Time2Vec: Learning a Vector Representation of Time [Electronic resource] / Seyed Mehran Kazemi [et al.] // arXiv.org e-Print archive – Mode of access: https://arxiv.org/abs/1907.05321. – Date of access: 14.04.2025.

17. Aditya Grover, node2vec: Scalable Feature Learning for Networks [Electronic resource] / Aditya Grover, Jure Leskovec // 22th ACM SIGKDD Conference on Knowledge Discovery and Data Mining, San Francisco, 13-17 August, 2016 // arXiv.org e-Print archive – Mode of access: https://arxiv.org/abs/1607.00653. – Date of access: 14.04.2025.

18. Keras [Electronic resource] / Traffic forecasting using graph neural networks and LSTM – Mode of access: https://keras.io/examples/timeseries/timeseries_traffic_forecasting/. – Date of access: 12.04.2025.

19. Rudikowa, L. General Concept of the Storage and Analytics System for Human Migration Data // L. Rudikowa, V. Denilchik, I. Savenkov, A. Nenko, S. Sobolevsky / Communications in Computer and Information Science / Digital Transformation and Global Society: Third International Conference, DTGS 2018 St. Petersburg, Russia, May 30 – June 2, 2018 Revised Selected Papers, Part I. – Springer Nature Switzerland AG, 2018. – P. 266-276.

УДК 004.91:7.067

ГЛАВА 3. О ПОДХОДАХ К ПРОЕКТИРОВАНИЮ И РАЗРАБОТКЕ ИНФОРМАЦИОННО-АНАЛИТИЧЕСКОЙ СИСТЕМЫ ОЦЕНКИ КАЧЕСТВА ГОРОДСКОЙ СРЕДЫ ДЛЯ РЕСПУБЛИКИ БЕЛАРУСЬ

Рудикова-Фронхёфер Лада Владимировна
к. ф.-м. наук, доцент,
Атьман Владислав Владимирович
магистрант,
Учреждение образования «Гродненский государственный университет имени Янки Купалы»

Аннотация: в данной главе представлена инновационная методология проектирования и реализации информационно-аналитической системы для комплексной оценки индекса качества жизни (ИКЖ) в городах Республики Беларусь. Разработана оригинальная модульная архитектура системы, включающая девять взаимосвязанных индексов: демографический потенциал, занятость и условия труда, доступность образования, здоровье и медицинское обслуживание, материальное благополучие, социальная поддержка, жилищные условия, безопасность и правопорядок, а также развитие человеческого капитала. Особое внимание уделено адаптации международных методик к специфике белорусских городов, включая введение коэффициента урбанизации (K) для нивелирования различий между городами разного масштаба. Применен комплексный аналитический подход, сочетающий методы нормализации данных, определение весовых коэффициентов через метод главных компонент (PCA) и алгоритмы агрегации показателей. Система обеспечивает автоматизированный сбор данных из разнородных источников (официальная статистика, социологические опросы, сенсорные сети), их многоуровневую обработку и интерактивную визуализацию результатов. Практическая апробация проведена на выборке городов Беларуси, продемонстрировавшая возможность выявления территориальных диспропорций и «точек роста». Предлагаемая система позволит органам управления осуществлять мониторинг городского развития (urban-развития), оценивать эффективность социально-экономических программ и принимать обоснованные управленческие решения.

Ключевые слова: информационно-аналитическая система, индекс качества жизни, урбанистика, метод главных компонент (PCA), весовые коэффициенты, коэффициент урбанизации, социально-экономические индикаторы, нормализация данных, агрегация показателей, визуализация данных, управление городским развитием, мониторинг urban-развития, региональная специфика.

ON APPROACHES TO DESIGNING AND DEVELOPING AN INFORMATION AND ANALYTICAL SYSTEM FOR ASSESSING THE ENVIRONMENT IN THE DARK REPUBLIC

Rudikova-Fronhoefer Lada Vladimirovna,
Atsman Vladislav Vladimirovich

Abstract: The article presents an innovative methodology for designing and implementing an information and analytical system for a comprehensive assessment of the quality-of-life index (QLI) in the cities of the Republic of Belarus. An original modular architecture of the system has been developed, including nine interrelated indices: demographic potential, employment and working conditions, accessibility of education, health and medical care, material well-being, social support, housing conditions, security and law and order, as well as human capital development. Particular attention is paid to the adaptation of international methods to the specifics of Belarusian cities, including the introduction of the urbanization coefficient (K) to level out the differences between cities of different sizes. A comprehensive analytical approach is used, combining data normalization methods, determination of weighting coefficients through the principal component analysis (PCA) and indicator aggregation algorithms. The system provides automated data collection from diverse sources (official statistics, sociological surveys, sensor networks), their multi-level processing and interactive visualization of the results. Practical testing was carried out on a sample of Belarusian cities, demonstrating the possibility of identifying territorial disproportions and "growth points". The developed tool allows government bodies to monitor urban development, evaluate the effectiveness of socio-economic programs and make informed management decisions.
Keywords: information and analytical system, quality of life index, urban studies, principal component analysis (PCA), weighting factors, urbanization coefficient, socio-economic indicators, data normalization, indicator aggregation, data visualization, urban development management, urban development monitoring, regional specifics.

В современных урбанизированных обществах измерение качества жизни становится критически важным инструментом для принятия управленческих решений и разработки социально-экономической политики. Однако существующие методики оценки часто оказываются недостаточно адаптированными к региональным особенностям, что особенно актуально для Республики Беларусь, где комплексные системы мониторинга качества жизни городов только начинают развиваться. Основная проблема заключается в отсутствии унифицированной информационно-аналитической системы, способной интегрировать разнородные данные из различных источников (государственной статистики, социологических опросов, данных сенсоров) в единый индекс, отражающий реальное положение дел в белорусских городах. Как отмечают исследователи, большинство международных индексов качества жизни, таких как Mercer Quality of Living Index или Economist Intelligence Unit Ranking, фокусируются преимущественно на крупных мегаполисах и не учитывают специфику постсоветских городов среднего размера, которые преобладают в Беларуси [1]. Важной методологической проблемой является выбор и взвешивание показателей. Как показали исследования, традиционные экономические индикаторы (ВВП на душу, уровень безработицы) часто не отражают субъективное восприятие

качества жизни жителями [2]. В белорусском контексте особую значимость приобретают такие факторы, как доступность социальной инфраструктуры, экологическое состояние городской среды и транспортная связанность, которые в существующих международных методиках представлены недостаточно. При этом, как отмечает Национальный статистический комитет Республики Беларусь, данные по многим из этих показателей собираются разрозненно и публикуются в форматах, затрудняющих их автоматизированную обработку [3].

Техническая сложность разработки системы такого рода усугубляется необходимостью обработки больших массивов неструктурированных данных. Современные исследования подчеркивают, что традиционные подходы к проектированию информационно-аналитических систем часто не справляются с задачами интеграции данных из разнородных источников, таких, как государственные базы данных, опросы общественного мнения и данные IoT-устройств [4].

Практическая значимость решения этой проблемы заключается в возможности создания инструмента для объективного межгородского сравнения и выявления «точек роста». Как показал опыт соседних стран, внедрение подобных систем позволяет муниципальным властям более эффективно распределять ресурсы и отслеживать результаты реализации социальных программ [5]. Современные коммерческие платформы для городского планирования требуют существенных финансовых вложений и не учитывают специфику национального законодательства в сфере обработки данных. Таким образом, разработка специализированной информационно-аналитической системы для оценки качества жизни в городах Беларуси представляет собой актуальную научно-практическую задачу, решение которой требует комплексного подхода, сочетающего современные методы data science с глубоким пониманием региональной специфики [6-9].

Цель данного исследования заключается в разработке методологии проектирования и реализации специализированной информационно-аналитической системы для комплексной оценки индекса качества жизни в городах Республики Беларусь. Система призвана интегрировать разнородные данные из официальных статистических источников, социологических опросов и сенсорных сетей, обеспечивая автоматизированный расчет показателей и наглядную визуализацию результатов. Особое внимание уделяется адаптации международных методик оценки к региональным особенностям белорусских городов, включая специфику их социально-экономического развития и инфраструктурной организации.

В рамках исследования предстоит решить ряд ключевых задач: определение оптимального набора показателей и разработка алгоритмов их агрегации в интегральный индекс; проектирование архитектуры системы с модулями сбора, обработки и визуализации данных; создание рабочего прототипа на основе современных технологий обработки информации; апробация системы на примере конкретных городов с оценкой ее эффективности и точности получаемых результатов. Особый акцент делается на обеспечении достоверности данных и

удобства интерпретации результатов для потенциальных пользователей – представителей органов государственного управления и местного самоуправления.

Объектом исследования выступают процессы проектирования и разработки информационно-аналитических систем для оценки социально-экономических показателей, в то время как предметом исследования является конкретная методология создания системы расчета индекса качества жизни, адаптированной к условиям белорусских городов. Исследование охватывает широкий круг вопросов – от выбора и верификации исходных данных до разработки алгоритмов их обработки и способов наглядного представления результатов. Полученные решения могут быть применены не только в белорусском контексте, но и адаптированы для других регионов со схожими социально-экономическими условиями.

Новизна предлагаемого исследования заключается в разработке принципиально нового подхода к оценке качества жизни, специально адаптированного для городов Беларуси с учетом их уникальных социально-экономических и инфраструктурных особенностей. В отличие от существующих международных методик, которые преимущественно ориентированы на крупные мегаполисы, предлагаемая система учитывает специфику средних и малых городов, характерных для белорусской урбанистической структуры. Особую научную новизну представляет разрабатываемая методика агрегации разнородных показателей, сочетающая традиционные статистические данные с новыми источниками информации, включая данные сенсорных сетей и результаты социологических опросов, что позволяет получить более объективную и многомерную оценку качества городской среды.

Оценка качества жизни является комплексной задачей, требующей учета множества социально-экономических, демографических и инфраструктурных факторов. В рамках проектирования информационно-аналитической системы «Индекс качества жизни в городах Республики Беларусь» был проведен анализ доступных статистических данных, предоставляемых Национальным статистическим комитетом Беларуси. На основе этого анализа выделено девять ключевых индексов, которые в совокупности позволяют сформировать целостную картину условий жизни в городах страны.

Основой для выбора индексов послужили несколько аспектов. Во-первых, учитывалась доступность данных на официальном портале Белстата, где представлена статистика по областям. Во-вторых, принимались во внимание международные методики оценки качества жизни, такие как Индекс человеческого развития ООН, рейтинги Mercer и Economist Intelligence Unit. В-третьих, рассматривалась специфика белорусских городов, включая их экономическую структуру, демографические тенденции и социальную политику государства.

В основу разработанной системы легли принципы Индекса человеческого развития (ИЧР), разработанного ООН, который объединяет показатели здоровья (ожидаемая продолжительность жизни), образования (грамотность и охват обучением) и уровня дохода (ВВП на душу) в единый интегральный показа-

тель. Этот подход был выбран благодаря его универсальности и признанию на международном уровне. Однако, в отличие от ИЧР, где все компоненты равнозначны, в данной работе весовые коэффициенты были скорректированы с учетом специфики Беларуси. Например, больший вес получили доступность социальной инфраструктуры и экологические показатели, которые слабо отражены в оригинальном ИЧР, но критически важны для белорусских городов.

Формула для расчета интегрального индекса качества жизни:

$$f(x) = \sum_{i=1}^{n} w_i \times \left(\frac{x_i - x_{i,min}}{x_{i,max} - x_{i,min}}\right) \times K_i \quad (1)$$

где: x_i – значение i-го показателя для конкретного города;

$x_{i,min}$ и $x_{i,max}$ – минимальное и максимальное значения показателя по всем городам;

w_i – весовой коэффициент, отражающий важность показателя (сумма коэффициентов равна 1);

K_i – коэффициент урбанизации, учитывающий долю населения города в области.

Классический ИЧР использует только «прямые» показатели (рост значения улучшает индекс), однако в данной работе были введены обратные индикаторы для таких параметров, как уровень преступности, заболеваемость или доля аварийного жилья. Например, если в ИЧР высокая продолжительность жизни увеличивает индекс, то здесь высокая заболеваемость (ММ) снижает его за счет параметров формулы (2). Это позволило учесть негативные факторы, характерные для постсоветских городов, таких как старение инфраструктуры или миграционный отток.

$$1 - \frac{x_i - x_{i,min}}{x_{i,max} - x_{i,min}} \quad (2)$$

Введение коэффициента урбанизации K_i в расчет различных параметров индекса качества жизни обусловлено необходимостью учета существенных различий между городскими поселениями разного типа и масштаба. Данный коэффициент, рассчитываемый как отношение численности населения конкретного города к среднему показателю по региону, позволяет нивелировать систематические различия между крупными областными центрами и малыми городами, обеспечивая сопоставимость результатов оценки. Особую значимость этот подход приобретает в контексте Беларуси, где наблюдается выраженная концентрация экономических и социальных ресурсов в региональных столицах, что может искажать прямые сопоставления показателей. Применение коэффициента K_i к таким параметрам, как миграционный прирост, доступность социальной инфраструктуры и уровень занятости, позволяет более точно отразить реальные условия жизни с поправкой на масштаб и статус населенного пункта, исключая преимущественное положение крупных городов, обусловленное их административными функциями и агломерационными эффектами.

Для объективного расчета весовых коэффициентов в составе интегральных индексов качества жизни был применен метод главных компонент (PCA), реа-

лизованный средствами вычислительных библиотек Python. Данный подход обеспечил статистически обоснованное определение значимости каждого параметра на основе анализа многомерных пространств социально-экономических показателей.

На подготовительном этапе осуществлялась стандартизация исходных данных посредством z-преобразования, что позволило устранить различия в масштабах измеряемых величин и обеспечить сопоставимость разнородных показателей. Последующий анализ главных компонент проводился с выделением первой компоненты, объясняющей максимальную долю дисперсии в исходном наборе данных. Весовые коэффициенты определялись на основе факторных нагрузок первой главной компоненты с последующей их нормализацией до единичной суммы.

Применительно к индексу занятости и условий труда, включающему пять параметров (уровень занятости, безработица, количество вакансий, численность работников во вредных условиях и отработанные человеко-часы), данный метод позволил получить весовые коэффициенты, отражающие объективный вклад каждого фактора в интегральный показатель. Анализ объясненной дисперсии подтвердил репрезентативность выделенной компоненты, что свидетельствует об адекватности построенной модели.

Основными преимуществами примененного подхода являются: статистическая объективность в определении значимости параметров, учет скрытых взаимосвязей между показателями, адаптивность к особенностям исходных данных и возможность регулярного обновления весовых коэффициентов при поступлении новых статистических сведений. Полученные результаты демонстрируют высокую устойчивость при валидации на различных временных срезах и территориальных выборках.

Метод был последовательно применен ко всем девяти составляющим индекса качества жизни. Использование PCA позволило минимизировать субъективность в определении весовых коэффициентов и создать надежный инструмент для межтерриториальных сопоставлений.

Первым и фундаментальным индексом стал Индекс демографического потенциала, основанный на статистике населения и миграции. Этот показатель отражает устойчивость развития территории через численность и плотность населения, возрастную структуру и миграционную динамику. Для городов Беларуси, где наблюдается отток молодежи в региональные центры и зарубежье, данный индекс особенно важен.

Формула индекса демографического потенциала (ИДП) представлена в следующем виде:

$$\text{ИДП} = w_1 \times \left(\frac{R-R_{min}}{R_{\max}-R_{min}}\right) + w_2 \times \left(\frac{N-N_{min}}{N_{\max}-N_{min}}\right) + w_3 \times \left(\frac{M-M_{min}}{M_{\max}-M_{min}}\right) \times K + w^4 \times \left(1 - \frac{A-A_{min}}{A_{max}-A_{min}}\right) + w^5 \times \left(\frac{D-D_{min}}{D_{\max}-D_{min}}\right), \quad (3)$$

где: R – уровень рождаемости (количество рождений на 1000 населения);

R_{max} – максимальная рождаемость по стране;

N – естественный прирост населения (на 1000 населения);
N_{max} – максимальный естественный прирост;
M – миграционный прирост;
M_{max} – максимальное миграционное сальдо;
K – коэффициент урбанизации;
A – коэффициент старения населения (%);
D – плотность населения в городе;
D_{max} – максимальная плотность населения;
w_1-w_5 – весовые коэффициенты, которые в сумме дают 1.

Следующий критически значимый показатель – Индекс занятости и условий труда, формируемый на основе статистики труда. Уровень занятости, средняя заработная плата и динамика безработицы прямо влияют на благосостояние горожан. В условиях трансформации экономики Беларуси, включающей цифровизацию и сокращение рабочих мест в традиционных отраслях, мониторинг этого индекса позволяет своевременно выявлять проблемные территории.

Формула индекса занятости и условий труда (ИЗУТ) предствляется по формуле (4):

$$\text{ИЗУТ} = w_1 \times \left(\frac{E - E_{min}}{E_{max} - E_{min}}\right) + w_2 \times \left(1 - \frac{U - U_{min}}{U_{max} - U_{min}}\right) + \\ + w_3 \times \left(\frac{(V - V_{min}) \times K}{(V_{max} - V_{min}) \times K}\right) + w_4 \times \left(\frac{(H - H_{min}) \times K}{(H_{max} - H_{min}) \times K}\right) + w_5 \times \left(\frac{(T - T_{min}) \times K}{(T_{max} - T_{min}) \times K}\right), \quad (4)$$

где: E – уровень занятости (%);
E_{max} – максимальный уровень занятости по стране;
U – уровень безработицы (%);
U_{max} – максимальный уровень безработицы;
V – количество вакансий в области;
V_{max} – максимальное количество вакансий по стране;
H – численность работников во вредных условиях;
H_{max} – максимальное значение по стране;
T – отработанные человеко-часы;
T_{max} – максимальное значение по стране;
K – коэффициент урбанизации;
w_1-w_5 – весовые коэффициенты, которые в сумме дают 1.

Индекс доступности образования учитывает количество учебных заведений, численность студентов и преподавателей, а также бюджетные расходы на образование. В белорусских городах, где сохраняется высокая концентрация образовательных учреждений в крупных центрах, этот индекс помогает оценить неравенство возможностей для жителей разных населенных пунктов.

Формула индекса доступности образования (ИДО):

$$\text{ИДО} = w_1 \times \left(\frac{D - D_{min}}{D_{\max} - D_{min}}\right) + w_2 \times \left(\frac{S - S_{min}}{S_{\max} - S_{min}}\right) + w_3 \times \left(\frac{T - T_{min}}{T_{\max} - T_{min}}\right) + w_4 \times \\ \times \left(\frac{I - I_{min}}{I_{\max} - I_{min}}\right) + w_5 \times \left(\frac{C - C_{min}}{C_{\max} - C_{min}}\right), \quad (5)$$

где: D – доступность дошкольного образования (мест на 100 детей);

D_{max} – максимальная доступность дошкольного образования (лучший показатель среди городов);

S – доступность школьного образования (учеников на 1 учителя);

S_{max} – минимальное отношение учеников к учителю (наилучшее значение);

T – охват техническим/профессиональным образованием (%);

T_{max} – максимальный охват техническим/профессиональным образованием (%);

I – инклюзивность (доля детей-инвалидов в образовании);

I_{max} – максимальная доля детей-инвалидов, охваченных образованием (%);

C – качество образования (доля награжденных учащихся);

C_{max} – максимальная доля награжденных учащихся (%);

w_1-w_5 – весовые коэффициенты (сумма = 1).

Сфера здравоохранения представлена Индексом здоровья и медицинского обслуживания, включающим данные о количестве больниц, обеспеченности врачами и уровне заболеваемости. В условиях централизованной системы здравоохранения Беларуси подобные метрики позволяют оценить, насколько сбалансированно распределяются ресурсы между городскими и сельскими регионами.

Формула индекса здоровья и медицинского обслуживания (ИЗМО):

$$ИЗМО = w_1 \times \left(\frac{V - V_{min}}{V_{max} - V_{min}}\right) + w_2 \times \left(\frac{B - B_{min}}{B_{max} - B_{min}}\right) + w_3 \times \left(1 - \frac{M - M_{min}}{M_{max} - M_{min}}\right) + w_4 \times \left(1 - \frac{I - I_{min}}{I_{max} - I_{min}}\right) + w_5 \times \left(\frac{L - L_{min}}{L_{max} - L_{min}}\right), \quad (6)$$

где: V – обеспеченность врачами (на 10 000 населения);

V_{max} – максимальная обеспеченность врачами (на 10 000 населения);

B – обеспеченность больничными койками (на 10 000 населения);

B_{max} – максимальная обеспеченность больничными койками (на 10 000 населения);

M – заболеваемость (случаев на 100 000 населения);

M_{max} – максимальная заболеваемость (наихудший показатель, используется в обратной форме);

I – уровень инвалидизации (на 10 000 населения);

I_{max} – максимальный уровень инвалидизации (наихудший показатель, используется в обратной форме);

L – ожидаемая продолжительность жизни (лет);

L_{max} – максимальная ожидаемая продолжительность жизни (лет);

w_1-w_5 – Весовые коэффициенты (сумма = 1).

Материальное благополучие граждан оценивается через Индекс материального благополучия, куда входят среднедушевые доходы, уровень бедности и потребительские расходы. В условиях инфляции и экономических санкций этот индекс становится ключевым для анализа социальной стабильности в городах.

Формула индекса материального благополучия (ИМБ):

$$ИМБ = w_1 \times \left(\frac{(D - D_{min}) \times k}{(D_{max} - D_{min}) \times k}\right) + w_2 \times \left(1 - \frac{E - E_{min}}{E_{max} - E_{min}}\right) + w_3 \times$$

$$\left(\frac{(C-C_{min})\times k}{(C_{max}-C_{min})\times k}\right) + w_3 \times \left(\frac{H-H_{min}}{H_{max}-H_{min}}\right) + w_5 \times \left(\frac{F-F_{min}}{F_{max}-F_{min}}\right), \quad (7)$$

где D – Среднедушевые доходы (в месяц);

D_{max} – максимальные среднедушевые доходы (лучший показатель среди городов);

E – доля расходов на медицину (%);

E_{max} – максимальная доля расходов на медицину (наихудший показатель, используется в обратной форме);

C – потребление продуктов питания (калорий/день);

C_{max} – максимальное потребление продуктов питания (калорий/день);

H – жилищные условия (м²/чел);

H_{max} – лучшие жилищные условия (макс. м²/чел);

F – обеспеченность товарами длит. пользования (% домохозяйств);

F_{max} – максимальная обеспеченность товарами длительного пользования (% домохозяйств);

w_1-w_5 – весовые коэффициенты (сумма = 1).

Индекс социальной поддержки, основанный на статистике социальной защиты, показывает, насколько эффективно государство и местные власти помогают уязвимым группам населения. Пенсионное обеспечение, льготы и программы адресной помощи особенно важны для малых городов с проблемой старения населения (aging population). Формула индекса социальной поддержки (ИСП) рассчитывается по формуле:

$$\text{ИСП} = w_1 \times \left(\frac{P-P_{min}}{P_{max}-P_{min}}\right) + w_2 \times \left(\frac{S-S_{min}}{S_{max}-S_{min}}\right) + w_3 \times \left(1 - \frac{O-O_{min}}{O_{max}-O_{min}}\right) + w_4 \times \left(\frac{F-F_{min}}{F_{max}-F_{min}}\right) + w_5 \times \left(\frac{C-C_{min}}{C_{max}-C_{min}}\right) \quad (8)$$

где P – средний размер пенсий (в % от БПМ);

P_{max} – максимальный уровень пенсий относительно БПМ;

S – охват семей социальными пособиями (доля семей с детьми, получающих адресную помощь);

S_{max} – лучший показатель охвата пособиями;

O – доля детей-сирот в интернатах (на 10 000 детского населения);

O_{max} – наихудшая доля сирот в интернатах (используется в обратной форме);

F – обеспеченность семейными формами устройства (доля детей в приёмных/опекунских семьях от общего числа сирот);

F_{max} – максимальная доля семейного устройства;

C – доступность социальных услуг (число центров соцобслуживания на 100 000 населения);

C_{max} – наилучшая обеспеченность соцуслугами.

Жилищные условия, являющиеся одним из базовых элементов качества жизни, оцениваются через Индекс жилищных условий. Обеспеченность жильем, его качество и доступность коммунальных услуг напрямую влияют на удовлетворенность жизнью. В малых городах Беларуси, где значительная часть

жилой инфраструктуры требует обновления, такой индекс может стать инструментом для определения приоритетных зон развития и привлечения инвестиций. Формула индекса жилищных условий (ИЖУ):

$$ИЖУ = w_1 \times \left(\frac{S-S_{min}}{S_{max}-S_{min}}\right) + w_2 \times \left(1 - \frac{D-D_{min}}{D_{max}-D_{min}}\right) + w_3 \times \left(\frac{W-W_{min}}{W_{max}-W_{min}}\right) + w_4 \times \left(\frac{U-U_{min}}{U_{max}-U_{min}}\right) + w_5 \times \left(\frac{P-P_{min}}{P_{max}-P_{min}}\right) \quad (9)$$

где S – площадь на человека (м²/чел);

D – доля ветхого и аварийного фонда (%);

W – доля получивших жильё от числа нуждающихся;

U – уровень благоустройства жилищного фонда (%);

P – протяжённость уличных сетей (км на 1000 чел.).

Безопасность и правопорядок, отраженные в Индексе безопасности и правопорядка, формируются на основе статистики правонарушений и деятельности судов. В городах с активными миграционными процессами или экономическими сложностями подобный показатель может отражать уровень социальной стабильности. Формула индекса безопасности и правопорядка (ИБП):

$$ИБП = w_1 \times \left(1 - \frac{P - P_{min}}{P_{max} - P_{min}}\right) + w_2 \times \left(1 - \frac{N - N_{min}}{N_{max} - N_{min}}\right) + w_3 \times \times \left(1 - \frac{S-S_{min}}{S_{max} - S_{min}}\right) + w_4 \times \left(1 - \frac{D-D_{min}}{D_{max}-D_{min}}\right) + w_5 \times \left(1 - \frac{C-C_{min}}{C_{max}-C_{min}}\right) \quad (10)$$

где: P – уровень преступности (количество преступлений на 100 000 населения),

P_{max} – максимальный уровень преступности по стране;

N – число преступлений, связанных с наркотиками;

N_{max} – максимальное число наркопреступлений по стране;

S – численность осужденных по приговорам судов;

S_{max} – максимальное число осужденных по стране;

D – количество ДТП по вине водителей в состоянии опьянения;

D_{max} – максимальное число таких ДТП по стране;

C – численность детей, чьи родители лишены прав;

C_{max} – максимальное число таких детей по стране;

w_1–w_5 – весовые коэффициенты (в сумме = 1).

И, наконец, важнейшим аспектом является индекс развития человеческого капитала, включающий данные о культуре, спорте и СМИ, отражает нематериальные аспекты качества жизни. Наличие библиотек, музеев, спортивных объектов и доступ к информации критически важны для формирования современной городской среды. Формула индекса развития человеческого капитала (ИРЧК) может быть рассчитана по формуле:

$$ИРЧК = w_1 \times \left(\frac{K-K_{min}}{K_{max}-K_{min}}\right) + w_2 \times \left(\frac{B-B_{min}}{B_{max}-B_{min}}\right) + w_3 \times \left(\frac{S-S_{min}}{S_{max}-S_{min}}\right) + w_4 \times \left(\frac{M-M_{min}}{M_{max}-M_{min}}\right) + w_5 \times \left(\frac{P-P_{min}}{P_{max}-P_{min}}\right) \quad (11)$$

C – число организаций культуры на 1000 населения;
C_{max} – максимальное значение по стране;
V – число посещений культурных учреждений на 1000 населения;
V_{max} – максимальное значение по стране;
B – библиотечная обеспеченность;
B_{max} – максимальное значение по стране;
A – охват детским творческим образованием;
A_{max} – максимальное значение по стране;
S – уровень развития спортивной инфраструктуры;
S_{max} – максимальное значение по стране.

Объединение этих девяти индексов в единую систему позволяет не только оценить текущее состояние городов, но и выявить диспропорции в их развитии. Например, областные центры могут демонстрировать высокие показатели в образовании и здравоохранении, но отставать по уровню доходов или безопасности. Кроме того, предложенная методика дает возможность отслеживать динамику изменений под влиянием государственных программ или экономических кризисов.

Важно отметить, что используемые данные имеют определенные ограничения, связанные с отсутствием детализации по отдельным городам. Однако предлагаемая система индексов разработана с учетом возможности ее адаптации по мере появления более точных статистических сведений. В перспективе это позволит перейти от областного уровня к анализу конкретных населенных пунктов, что особенно актуально для разработки адресных программ развития городской инфраструктуры и социальной сферы в Беларуси.

Список источников

1. Mercer [Электронный ресурс] / Quality of Living City Ranking 2024 – Режим доступа: https://www.mercer.com/insights/total-rewards/talent-mobility-insights/quality-of-living-city-ranking/. – Дата доступа: 01.04.2025

2. Europastat [Электронный ресурс] / Quality of life indicators – measuring quality of life – Режим доступа: https://ec.europa.eu/eurostat/statistics-explained/index.php?title=Quality_of_life_indicators_-_measuring_quality_of_life#Framework_for_measuring_quality_of_life/. – Дата доступа: 01.04.2025

3. Белта – Новости Беларуси [Электронный ресурс] / Цифровизация, конфиденциальность и единая система статданных: Медведева о развитии Белстата – Режим доступа: https://belta.by/interview/view/tsifrovizatsija-konfidentsialnost-i-edinaja-sistema-statdannyh-medvedeva-o-razvitii-belstata-8328/. – Дата доступа: 01.04.2025

4. Сетевое издание «Экономические исследования» [Электронный ресурс] / Информационно-аналитические системы как инструмент управления технологиями в цифровой экономике – Режим доступа: https://myeconomix.ru/informatsionnye-tekhnologii-v-ekonomike/informatsionno-

analiticheskie-sistemy-kak-instrument-upravleniya-tekhnologiyami-v-tsifrovoy-ekonomik/. – Дата доступа: 01.04.2025

5. Группа Всемирного банка [Электронный ресурс] / Всемирный банк поддерживает диалог по денежным переводам и развитию в регионе СНГ – Режим доступа: https://www.vsemirnyjbank.org/ru/news/press-release/2012/09/10/world-bank-supporting-dialogue-on-remittances-and-development-in-cis-region/. – Дата доступа: 01.04.2025.

7. Рудикова-Фронхёфер, Л.В. О некоторых подходах к построению прагматической модели города // Л.В. Рудикова-Фронхёфер, С.А. Митягин // Проблемы современной экономики: глобальный, национальный и региональный контекст: сб. науч. ст./ ГрГУ им. Я. Купалы; редкол.: М. Е. Карпицкая (гл. ред.), С. Е. Витун (зам. гл. ред.) [и др.]. – Гродно: ГрГУ, 2022. – С. 382-392.

8. Рудикова, Л.В. О разработке системы данных городской среды на основе технологии складирования данных // Л.В. Рудикова, Д.С. Друтько // Наука, инновации, образование: актуальные вопросы и современные аспекты: Монография / Под общ. ред. Г. Ю. Гуляева. – Пенза: МЦНС «Наука и Просвещение». – 2021. – С. 268-278.

9. Рудикова-Фронхёфер, Л.В. Применение машинного обучения на графах при прогнозировании транспортного трафика // Л.В. Рудикова-Фронхёфер, Н.И. Игнатенко // Современная наука и технологии: актуальные вопросы, достижения и инновации: Монография / Под общ. ред. Г. Ю. Гуляева. – Пенза: МЦНС «Наука и Просвещение». – 2023. – С. 33-43.

10. Рудикова-Фронхёфер, Л.В. О некоторых подходах к построению информационных моделей городов / Л.В. Рудикова-Фронхёфер // Algoritmlar va dasturlashning dolzarb muammolari. Xalqaro ilmiy-amaliy anjuman materiallari to'plami. 2023 yil 19-20 may. Qarshi. Qarshi davlat universiteti. – 2023. – P. 17-22.

УДК 004.91:7.067

ГЛАВА 4. О ПОДХОДАХ К РАЗРАБОТКЕ УНИВЕРСАЛЬНОЙ СИСТЕМЫ ОБЪЕКТОВ ХУДОЖЕСТВЕННОЙ И ИСТОРИЧЕСКОЙ ЦЕННОСТИ

Рудикова-Фронхёфер Лада Владимировна
к. ф.-м. наук, доцент,
Учреждение образования «Гродненский государственный университет имени Янки Купалы»

Аннотация: в данной галве монографии изложена основная концепция к разработке универсальной системы хранения и обработки данных объектов художественной и исторической ценности. В работе приводятся общие подходы к архитектурной реализации системы, основные фрагменты физической модели для OLTP-систем данных объектов художественной и исторической ценности, а также основные модули для универсальной системы с их расширенными характеристиками.
Ключевые слова: произведения художественной ценности, объекты исторической значимости, универсальная система, структурная методология, модули системы, архитектура системы, модель данных, модель функций.

ON THE DEVELOPMENT OF A UNIVERSAL SYSTEM OF OBJECTS OF ARTISTIC AND HISTORICAL VALUE

Rudikova-Fronhoefer Lada Vladimirovna

Abstract: The monograph describes the basic concept for developing a universal system for storing and processing data on objects of artistic and historical value. The work provides general approaches to the architectural implementation of the system, the main fragments of the physical model for OLTP systems of data on objects of artistic and historical value, as well as the main modules for the universal system with their extended characteristics.
Key words: works of artistic value, objects of historical significance, universal system, structural methodology, system modules, system architecture, data model, function model.

Введение. В современном информационном обществе сохранение, анализ и доступ к информации об историческом и художественном наследии становятся неотъемлемой частью культурной и научной деятельности. Программные решения, способные эффективно накапливать и анализировать данные в этой области, играют ключевую роль в сохранении и распространении знаний о культурном наследии человечества. Необходимость в разработке таких систем обусловлена как разнообразием и объемом культурных данных [1, 2], так и требованиями современного общества к их доступности и удобству использования.

Создание универсальной системы хранения и обработки данных объектов художественной и исторической ценности должно способствовать хранению и обработке информации о культурных объектах с высокой точностью и эффективностью [3-5]. Эта система должна быть способна обрабатывать как исторические данные, касающиеся археологических находок, памятников архитектуры и артефактов, так и художественные данные, включая картины, скульптуры и другие произведения искусства. Кроме этого, система должна поддерживать надежное хранение информации и предоставление возможности для дальнейших исследований и анализа.

Таким образом, разработка универсальной системы хранения и обработки данных объектов художественной и исторической ценности имеет большое значение не только для профессиональных исследователей и историков искусства, но и для широкой аудитории. Она будет полезна студентам, педагогам, любителям истории и искусства, а также обществу в целом, поскольку открывает доступ к культурному наследию и способствует его пониманию и ценности. Такая система будет способствовать сохранению культурного наследия и его передаче будущим поколениям, а также обогащению знаний о прошлом искусстве и истории человечества.

Важно отметить, что существующие информационные ресурсы не всегда обеспечивают полный и систематизированный доступ к данным об историческом и художественном наследии. Информация часто разбросана по различным источникам, нередко неструктурирована и недоступна для анализа в целом. Это создает сложности как для специалистов, так и для широкой публики, которая стремится получить достоверную информацию о культурном наследии.

Следовательно, разработка системы накопления и анализа информации об историческом и художественном наследии становится не только вопросом удобства, но и важным шагом в обеспечении доступности и объективности данных. Такая система должна учитывать разнообразие форматов и типов данных, их географическое и временное разнообразие, а также особенности интересующих пользователей и их потребностей. Она должна быть гибкой и масштабируемой, способной адаптироваться к изменяющимся потребностям и требованиям современного информационного общества.

Излагаемые подходы к разработке универсальной системы объектов художественной и исторической ценности являются актуальными для специалистов, которые работают в области информационных технологий, технологий накопления и обработки данных, занимаются разработкой программных систем различной сложности, расширением структурной методологии и анализом данных широкого профиля. Отметим, что результаты будут востребованы и актуальны как для многих исследователей и разработчиков программного обеспечения, так и для специалистов, которые занимаются исследованием культурного и исторического наследия.

1. Об архитектурной концепции системы объектов художественной и исторической ценности. Главной целью разработки системы хранения и обра-

ботки данных объектов художественной и исторической ценности является создание наиболее совершенной, удобной и надежной платформы, которая позволяет собирать, систематизировать и обрабатывать всевозможные данные о различных объектах культуры и искусства, таких как исторические памятники архитектуры, высокохудожественные произведения, музейные экспонаты и многое другое. Благодаря использованию системы пользователи смогут не только получить доступ к обширной базе данных, содержащей информацию об объектах культурного наследия, но и активно воспользоваться данными в проведении глубоких исследований, широкой популяризации и долгосрочного сохранения культурного наследия, которое является непреходящим источником вдохновения и эталона прекрасного для современного поколения и будущих поколений.

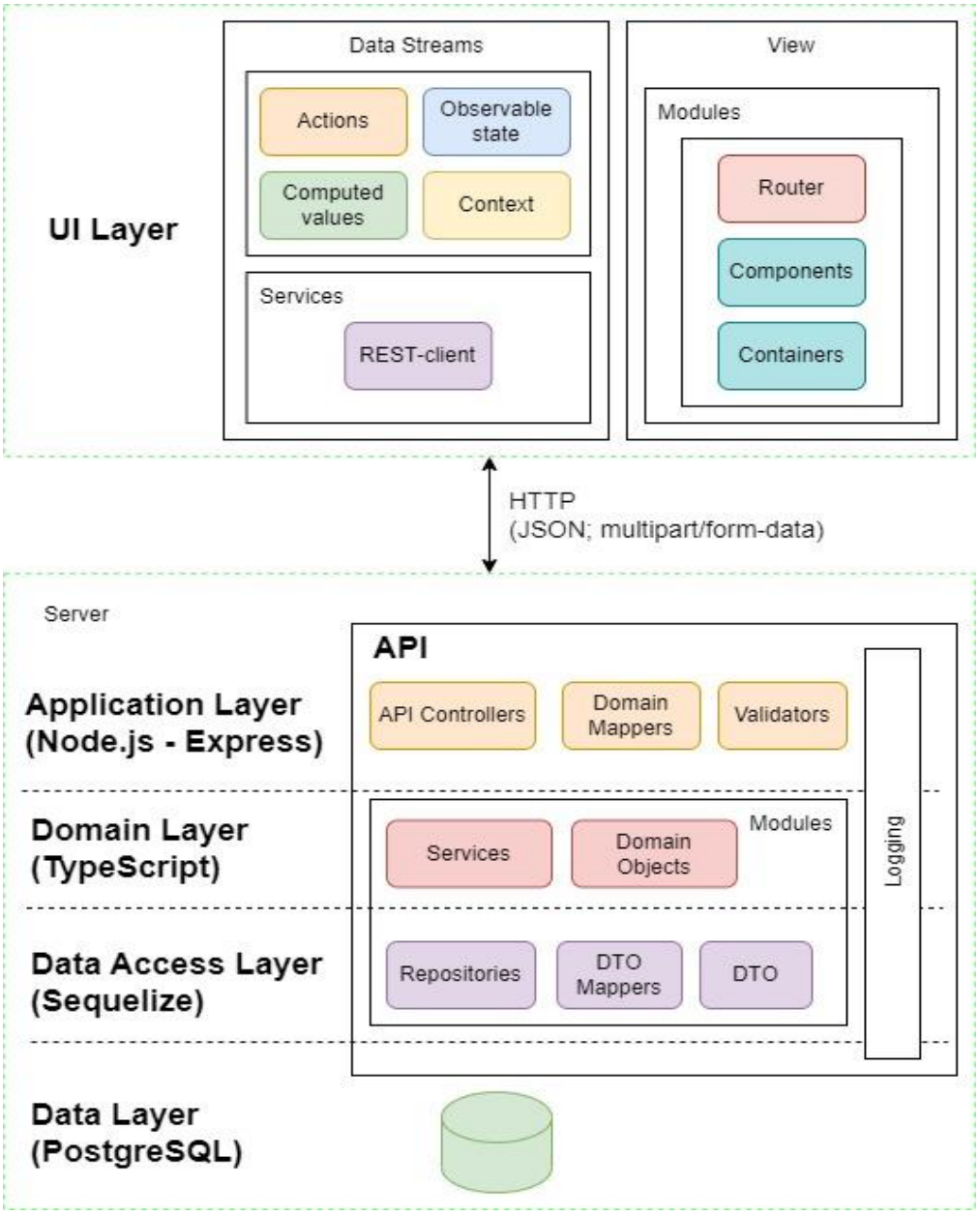

Рис. 1. Общая архитектура системы объектов художественной и исторической ценности

Разрабатываемая система предлагает широкие возможности для изучения и обмена знаниями в области культуры и искусства, предлагая пользователям расширенный функционал. Благодаря многим функциям и улучшенным возможностям, которые предоставляются ресурсом, пользователи смогут взаимодействовать между собой, обмениваться опытом и мнениями, а также создавать глобальные сообщества единомышленников, способствуя продвижению и развитию сферы культуры и искусства в целом. Весь собранный материал будет грамотно структурирован и классифицирован, что позволит максимально удобно и эффективно использовать полученные данные для различных целей и задач. Уникальность и инновационность данного ресурса заключается еще и в его возможности формирования интерактивных виртуальных экскурсий, что открывает перед пользователями новые направления в изучении объектов культуры и искусства, независимо от расстояния и времени.

Для реализации отдельных модулей системы предлагается монолитная клиент-серверная архитектура [6-8], включающая дополнительные уровни и сервисы. Монолитная архитектура клиент-сервер позволяет разделять клиентскую и серверную части приложения, которые общаются с помощью протоколов передачи данных (рисунок 1).

Клиентские приложения, реализованные на различных платформах, таких как веб-браузеры, мобильные и настольные приложения, отображают данные, получаемые от сервера. Основными преимуществами такой архитектуры являются её простота в разработке и поддержке.

В архитектуре приложения для работы с информацией об объектах художественной и исторической ценности можно выделить следующие технологические решения:

– база данных для хранения сведений о картинах, художниках и пользователях;
– использование фреймворков для разработки приложений;
– JavaScript-библиотеки для динамического представления данных;
– RESTful API для организации взаимодействия между клиентом и сервером;
– адаптивный дизайн, подстраивающийся под разные устройства пользователя.

Компоненты системы включают:

– веб-клиент, который позволяет пользователям взаимодействовать с приложением через браузер;
– серверное приложение, обрабатывающее запросы от клиентов и отправляющее им необходимые данные;
– сервер баз данных, на котором хранится всё необходимое.

Вопросы безопасности решаются следующим образом:

– использование HTTPS для защиты данных в процессе их передачи;
– ограничение доступа к базе данных;

– аутентификация пользователей для выполнения операций с данными;
– шифрование паролей и защита ключевых функций, например, удаления информации.

В результате, архитектура представляет собой безопасную и эффективную систему, предоставляющую пользователям удобный доступ к информации.

Кроме того, следует учесть, что использование монолитной архитектуры оправдано для отдельных блоков системы, которые собирают данные и взаимодействуют с пользователями системы. Для дальнейшего накопления данных с целью их расширенного анализа и формирования прогнозов и аналитических выводов, в системы необходимо использовать архитектурные подход, основанный на технологии складирования данных.

Основой анализа данных такой системы, системы на основе хранилища данных с использованием OLAP, являются следующие аспекты.

Сбор данных: информация о произведениях искусства и художниках собирается из разнообразных источников, таких как аукционы, галереи, музеи, каталоги, библиотеки и т.п.

Трансформация данных: обработка собранных данных для приведения их к формату, совместимому с OLAP-системой; это включает очистку данных, проектирование схемы и создание реляционных таблиц.

Построение данных в кубе: формирование OLAP-кубов, структурированных данных, позволяющих проводить анализ по различным параметрам и уровням детализации; как минимум, кубы должны включать данные, например, о произведениях искусства и художниках, периодах созданиях, направлениях искусства и т.п.

Сегментация куба данных: сегментация куба для аналитической обработки, что может включать создание подкубов, агрегацию данных, настройку доступа и т.д.

Инструменты анализа данных: для извлечения значимой информации из куба данных используются специализированные аналитические инструменты, такие как интерфейсы OLAP, системы отчетности, дашборды, визуализация данных и т.д.

Обслуживание системы: система требует регулярного обслуживания, включая мониторинг её производительности, обновление данных и устранение неполадок.

В совокупности такой подход обеспечивает пользователям инструменты для многоаспектного анализа данных об искусстве и произведениях художественной ценности через интерактивный интерфейс, предоставляющий агрегированную информацию о художниках, их работах, музеях, выставках, аукционах и прочем.

2. О физической модели для OLTP-систем данных объектов художественной и исторической ценности. На основе исследований предыдущих этапов была получена физическая композиционная модель [9-11] для OLTP-систем данных объектов художественной и исторической ценности. Можно

выделить два этапа создания физической модели данных. Основными целями первого этапа являются следующие аспекты.

1. Создание таблиц для хранения информации об объектах предметной области.

2. Определение типов атрибутов и определение ограничений на значения атрибутов.

3. Наложение ограничений ссылочной целостности на таблицы.

4. Независимость представления данных от их физического хранения.

На первом этапе создаются объекты, соответствующие сущностям и взаимосвязям концептуальной модели данных – таблицы, индексы, представления и т.д.

Главной целью второго этапа является обеспечение требуемого уровня производительности. Для этого следует учитывать особенности реализации СУБД, для которой создается физическая модель, а также функциональные особенности разрабатываемой системы. Обычно производительность базы данных соотносится с производительностью транзакций.

При создании физической модели необходимо выявить ряд часто употребляющихся запросов для того, чтобы в последствии перенести их в хранимые процедуры, что позволяет повысить производительность.

Были выявлены следующие основные запросы, которые следует реализовать в системе:

– получение информации о конкретном пользователе;
– получение списка объектов исторического наследия конкретного места;
– получение списка объектов художественной ценности;
– получение детализированной информации о конкретном объекте исторической или художественной ценности;
– получение детализированной информации об авторах работ объектов художественной и исторической ценности;
– поддержка операций CRUD (Create, Read, Update и Delete) для объектов художественной и исторической ценности;
– поддержка операций CRUD для рецензий авторизированных пользователей;
– поиск по различным критериям, связанных с категориями объектов художественной и исторической ценности;
– получение ТОП-10 достопримечательностей по конкретной местности;
– добавление в избранное выбранного объекта для авторизированного пользователя;
– получение списка объектов художественной и исторической ценности для указанного места.

Основные фрагменты физической модели для OLTP-систем данных объектов художественной и исторической ценности приведена на рисунках 2-4.

Именно на этих трех фрагментах и базируется общая модель данных системы, объединяющая в себе объекты исторической и культурной значимости,

информацию о произведения художественной ценности, а также данные об исторических персонах (известных личностях), которые внесли непосредственный вклад в создание, сохранение и продвижение указанных объектов.

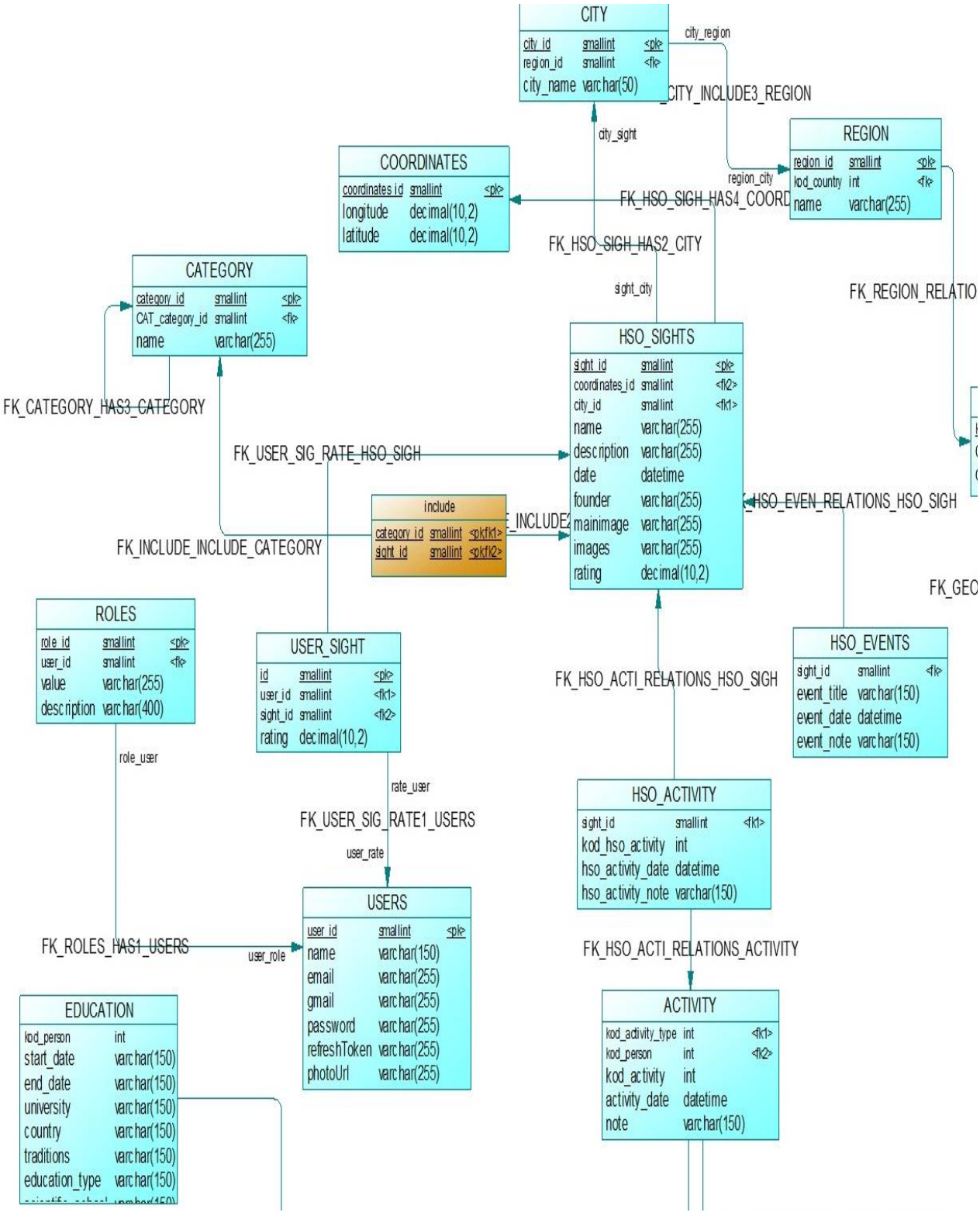

Рис. 2. Фрагмент физической модели данных, связанный с пользователями системы и объектами исторической значимости

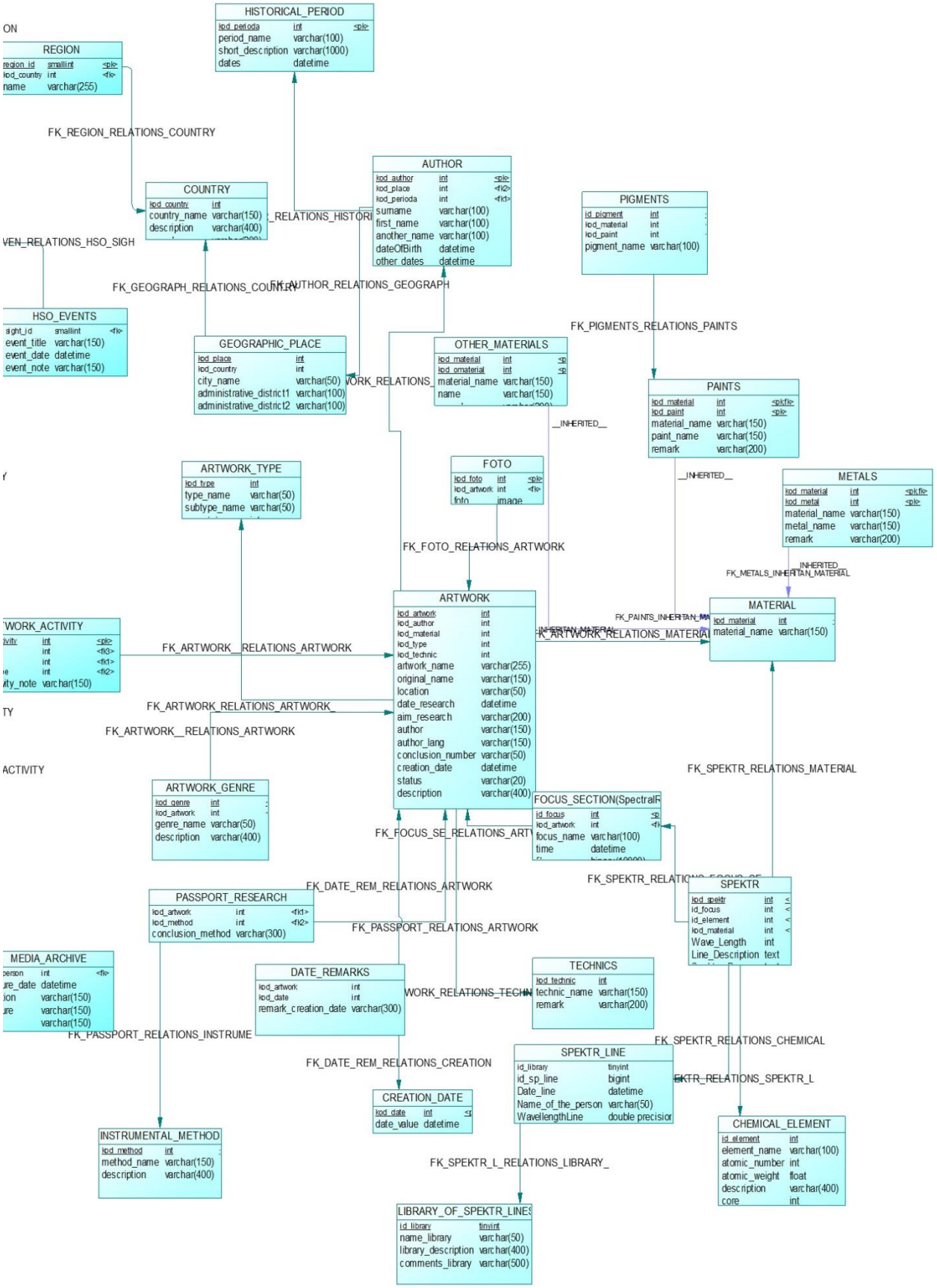

Рис. 3. Фрагмент физической модели данных, связанный с произведениями художественной ценности

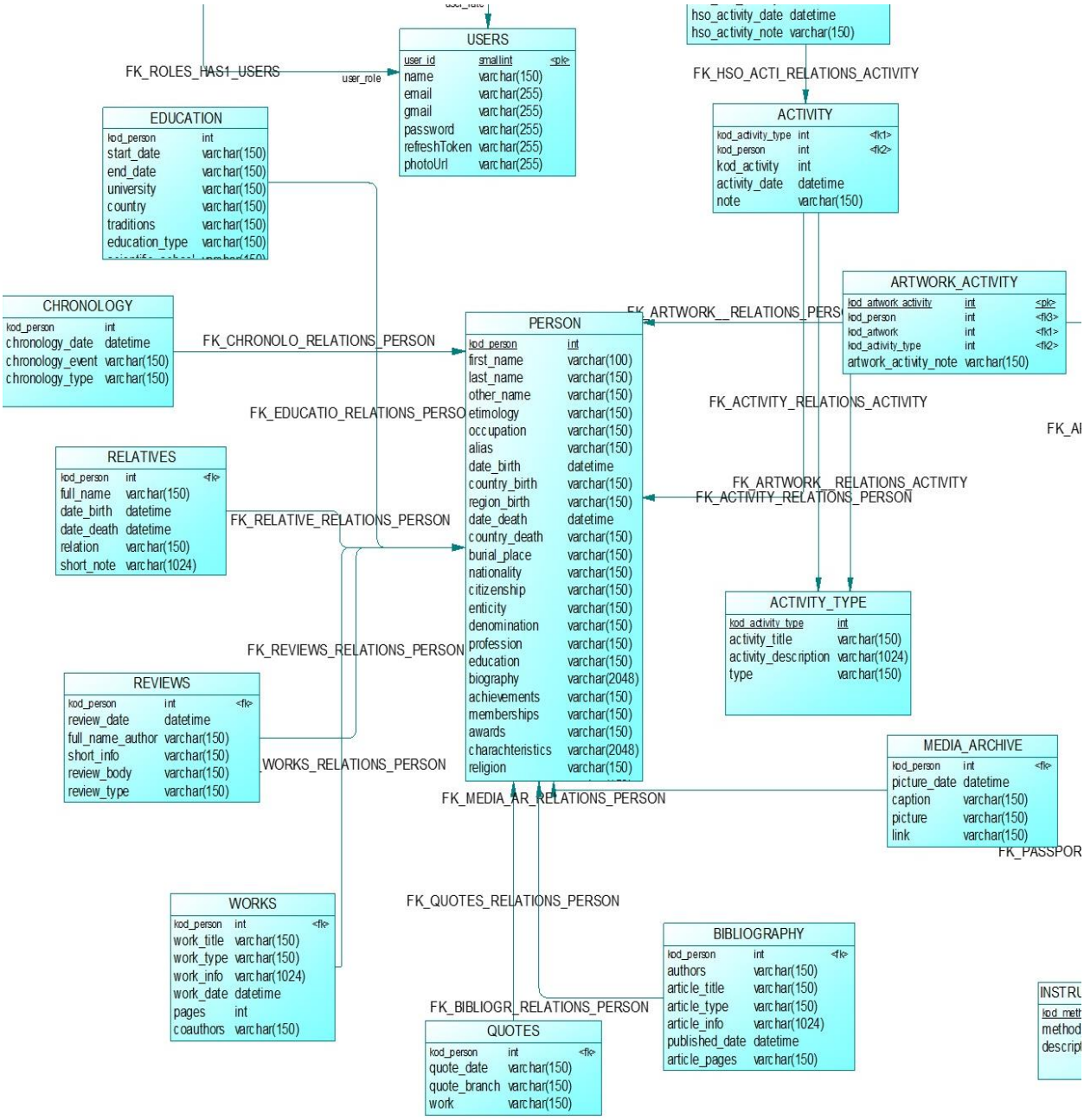

Рис. 4. Фрагмент концептуальной модели данных, связанный с авторами работ

3. Об основных модулях для системы хранения и обработки данных объектов художественной и исторической ценности. Разработка Интернет-ресурса сбора и анализа информации об объектах исторической и художественной ценности предполагает создание удобной и надежной платформы, которая позволит собирать, систематизировать и обрабатывать данные о различных объектах культуры и искусства, таких как исторические памятники архитектуры, высокохудожественные произведения, музейные экспонаты и т.д. Благодаря использованию ресурса пользователи смогут не только получить доступ к обширнейшей базе данных, содержащей информацию об объектах культурного

наследия, но и активно воспользоваться данными в проведении аналитических исследований.

На рисунке 5 представлены основные модули для системы хранения и обработки данных объектов художественной и исторической ценности.

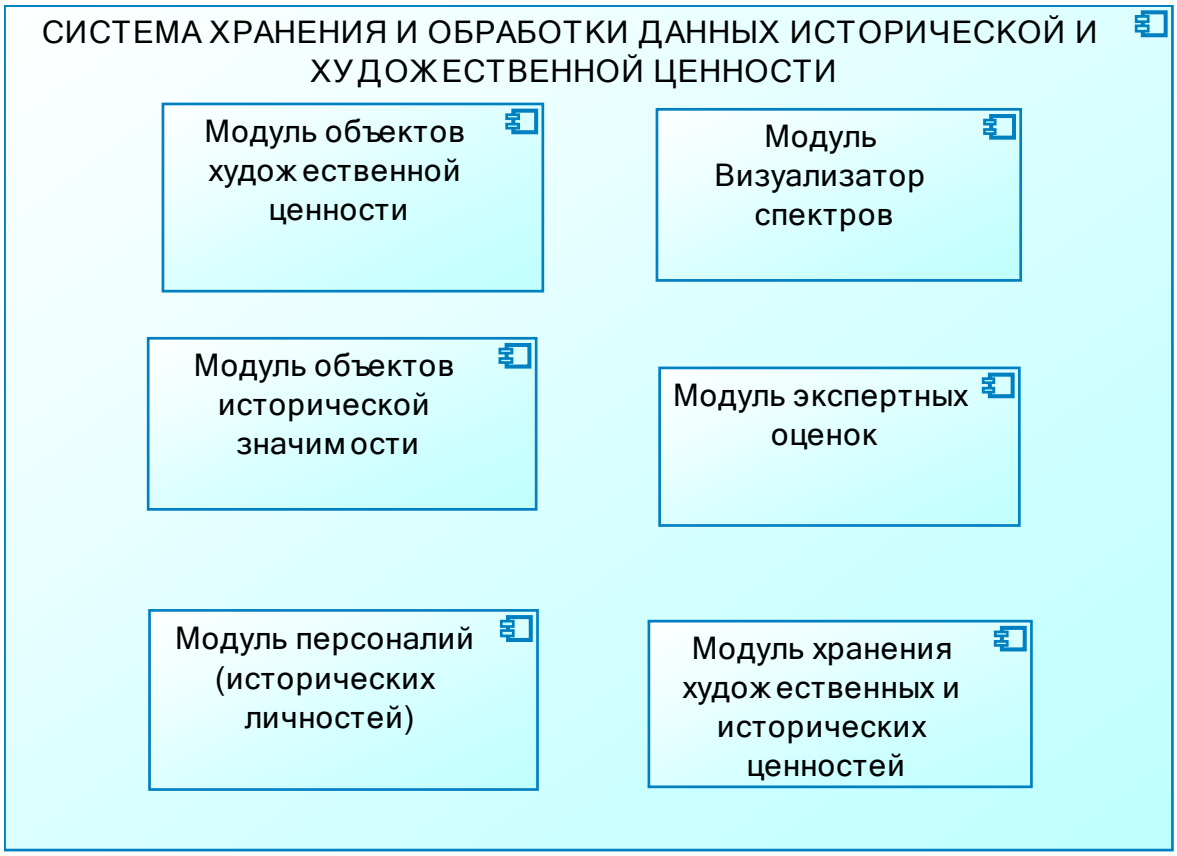

Рис. 5. Модули системы хранения и обработки данных объектов художественной и исторической ценности

Модуль объектов художественной ценности предоставляет возможность работы с произведениями искусства и культурными артефактами, которые обладают значимостью с эстетической, исторической, культурной или социальной точки зрения. Как правило, к объектам художественной ценности относят следующие:

– живопись – картины, которые создавались знаменитыми художниками;

– скульптура – трёхмерные произведения из различных материалов, таких как мрамор, бронза, дерево;

– графика – рисунки, гравюры, акварели;

– фотография – фотографические произведения, которые имеют художественную ценность;

– керамика – предметы из керамики и фарфора, выполненные в художественном стиле;

– прикладное искусство – изделия, совмещающие утилитарные функции и художественную ценность, такие как текстиль или мебель;

– архитектурные объекты – здания и сооружения, обладающие не только функциональной, но и эстетической ценностью;

– антиквариат – старинные предметы, такие как мебель, посуда, монеты, книги, имеющие историческую и художественную значимость.

Каждый из этих объектов может представлять интерес для коллекционеров, музеев и исследователей. Объекты художественной ценности часто являются частью культурного наследия и могут иметь большую ценность на рынке искусства.

Для системы хранения и обработки данных объектов художественной и исторической ценности разработана общая концепция создания программных систем хранения и обработки данных живописи. Однако указанный модуль может также обрабатывать и указанные выше разновидности объектов художественной ценности.

Модуль объектов исторической значимости может накапливать и обрабатывать данные объектов исторической и культурной значимости, производить необходимый поиск и обработку данной информации.

Объекты исторической значимости – это артефакты, здания, памятники и другие материалы, которые имеют важное значение для понимания истории, культуры и развития человеческого общества. Как правило, объекты исторической значимости могут относиться к следующим категориям: археологические находки, исторические здания и памятники, изменения в общественном устройстве (документы, свидетельствующие о важных политических событиях), технические и индустриальные объекты, символы культурного и национального значения (флаги, гербы, национальные символы, книги, произведения искусства или музыки, которые оказали влияние на культуру), личные артефакты, военные объекты.

Историко-культурный объект характеризуется следующими параметрами: название; описание; фото- и видео- материалами; классификацией по критериям всемирного наследия ЮНЕСКО: культурные (I, II, III, IV, V, VI), природные (VII, VIII, IX, X); категория историко-культурной ценности Республики Беларусь (0, 1, 2, 3, А, Б и без категории); место расположения.

Предлагаемый модуль сохраняет и обрабатывает информацию, связанную с историческими памятниками, зданиями и другими внешними объектами, исключая произведения художественного и литературного творчества.

Модуль персоналий (исторических личностей) предоставляет доступ к расширенному функционалу по персоналиям. Персоналии (исторические личности) – это люди, которые оказали значительное влияние на ход истории, культуры, науки или общества в целом. Основные категории. Которые можно выделить по персоналиям: политики и правители, ученые и мыслители, художники и писатели, религиозные лидеры, военные деятели и т.д. Указанный модуль имеет возможность сохранять расширенную информацию по историческим личностям, включая основные сведения, хронологию, образование, библиографию, цитаты, отзывы о личности, работы личности, родственники, область деятельности, ссылки на Интернет-ресурсы и т.д.

Модуль Визуализатор спектров используется для анализа произведений художественной ценности. С использованием методов спектрального анализа можно провести достаточно обширные исследования, включая объекты, которые являются культурным и историческим наследием и представляющие историческую ценность, подлинность которых требуется установить. Основными функциональными особенностями указанного модуля следующие: накопление, обработка и анализ данных об объектах исследования; предоставление централизованного доступа к различным накопленным библиотекам спектральных линий; предоставление универсальной платформы для категоризации исследуемых объектов (например, экспертиза художественных объектов, строительных материалов и т.д.); генерация и хранение различных отчетов и экспертных заключений, связанных с проведенными исследованиями.

По мере накопления данных о различных объектах исследования предоставляется возможным проводить анализ поступающей информации о новых исследуемых объектах. Другими словами, необходимо решить задачу распознавания различных ситуаций, когда по набору заданных признаков (факторов) выявляется сущность некоторой ситуации, в зависимости от которой выбирается определенная последовательность действий. В качестве основного метода формирования решений используется метод логического дедуктивного вывода от общего к частному, когда путем подстановки исходных данных в некоторую совокупность взаимосвязанных общих утверждений получается частное заключение.

Модуль экспертных оценок предполагает поддержку при подготовке экспертных заключений по атрибуции и искусствоведческой экспертизе.

С помощью искусствоведческой экспертизы определяется культурная или историческая ценность различных объектов. В качестве объектов искусствоведческой экспертизы выступают: картины, скульптуры, тексты, оружие, монеты, открытки, марки.

Применительно к данному модулю, необходимо отметить следующие особенности. Модуль должен хранить расширенные данные об объекте исследования, его характеристиках и фотографиях, а также материалах, используемых при создании объекта. Следует отметить, что вся работа эксперта по подготовке и составлению отчета требует длительного времени и мало автоматизирована. В силу этого предлагаемый модуль, связанный с формированием экспертных заключений, должен способствовать подготовке итоговых документов и давать возможность сохранения данных, полученных в результате проведения искусствоведческих экспертиз физико-оптическими и физико-химическими методами исследований.

Модуль хранения художественных и исторических ценностей предоставляет информацию о реальных хранилищах произведений художественных и исторических ценностей. Места хранения художественных и исторических ценностей включают различные типы учреждений и объектов, созданных для сохранения, исследования и представления таких ценностей. Основные категории собраний художественных и исторических ценностей:

– музеи искусства – хранят произведения искусства, такие как картины, скульптуры и декоративно-прикладное искусство;

– галереи – специальные выставочные пространства, где проводятся временные выставки произведений искусства и культурных ценностей;

– национальные и государственные архивы – хранят документы, рукописи и другие материалы, представляющие историческую значимость;

– научные и национальные библиотеки – хранят редкие книги, манускрипты и другие письменные источники;

– антикварные салоны и аукционные дома – места, где могут храниться и продаваться антикварные и художественные ценности;

– исторические памятники и учреждения – некоторые памятники, такие как замки, церкви и дворцы, также служат местами хранения культурного наследия, включая живопись, скульптуру и другие артефакты;

– частные коллекции – многие художники, историки и коллекционеры имеют собственные коллекции, которые могут включать ценные произведения искусства и исторические объекты;

– муниципальные и региональные музеи – местные учреждения, которые часто хранят и представляют ценности, связанные с конкретным регионом или городом.

Данные о таких местах должны сохраняться в модуле, визуализироваться на карте и предоставлять необходимую информацию по такого рода объектам. При реализации такого модуля возможен расширенный анализ как по произведениям художественной ценности, так и по историческим периодам, стилям, направлениям и перемещениям произведений художественной ценности.

Заключение. Главной целью разработки системы хранения и обработки данных объектов художественной и исторической ценности является создание наиболее совершенной, удобной и надежной платформы, которая позволяет собирать, систематизировать и обрабатывать всевозможные данные о различных объектах культуры и искусства, таких как исторические памятники архитектуры, высокохудожественные произведения, музейные экспонаты и многое другое. В связи с этим, проектирование и разработка общей концепции универсальной системы, которая предназначена для сбора. хранения и обработки данных объектов художественной ценности и исторической значимости, а также выполняющих необходимый поиск и анализ данных, представляет собой актуальную и достаточно трудоемкую задачу.

Полученные результаты актуальны для специалистов в области информационных технологий и технологий обработки данных, которые занимаются разработкой программных систем различной степени сложности, расширением структурной методологии и анализом данных различного профиля. Полученные результаты будут востребованы и актуальны как для широкого круга исследователей и разработчиков программного обеспечения, так и для специалистов, занимающихся исследованием культурного и исторического наследия.

Кроме того, результаты исследований также можно использовать в рамках учебного процесса при подготовке специалистов ИТ-профиля.

Список источников

1. Государственный список историко-культурных ценностей Республики Беларусь [Электронный ресурс]. – http://gosspisok.gov.by/?AspxAutoDetectCookieSupport=1 – Дата доступа: 18.12.2024.

2. Медведева, И.В. туризм и туристические ресурсы в Республике Беларусь // И.В. Медведева, Е.И. Кухаревич, Ж.Н. Василевская, О.А. Довнар, Н.В. Тарасюк, Т.В. Лапковская, И.А. Мазайская, Е.М. Палковская, И.Г. Чигирёва / Буклет. – Мн.: Национальный статистический комитет Республики Беларусь – 2022. – С. 7-29.

3. Рудикова, Л.В. О системе обработки данных произведений художественной ценности на основе технологии складирования данных // Л.В. Рудикова / Веб-программирование и Интернет-технологии WebConf2018: тез. докл. 4-й Междунар. науч.-практ. конф., Минск, 14–18 мая 2018 г. / Белорус. гос. ун-т; редкол.: И.М. Гавлкин (отв. ред.) [и др.]. – Минск: БГУ, 2018. – С. 6–8.

4. Рудикова, Л.В. Использование технологии складирования данных для построения архитектуры системы сбора и анализа данных произведений исторической ценности // Л.В. Рудикова, С.Ю. Бандысик / Информационные технологии и системы 2018 (ИТС 2018) : материалы международной научной конференции (БГУИР, Минск, Беларусь, 25 октября 2018)=Information Technologies and Systems 2018 (ITS 2018) : Proceeding of the International Conference (BSUIR, Minsk, Belarus, 25th October 2018) / редкол. : Л. Ю. Шилин [и др.]. – Минск: БГУИР, 2018. – С. 188–189.

5. Рудикова, Л.В. О системе хранения и обработки информации о произведениях художественной ценности на основе технологии складирования данных // Л.В. Рудикова // Проблемы современной экономики: глобальный, национальный и региональный контекст: сб. науч. ст./ ГрГУ им. Я. Купалы; редкол.: М. Е. Карпицкая (гл. ред.), С. Е. Витун (зам. гл. ред.) [и др.]. – Гродно: ГрГУ, 2021. – С. 210–216.

6. Рудикова-Фронхёфер, Л.В. О подходах к проектированию и разработке системы накопления и обработки данных произведений художественной ценности // Л.В. Рудикова-Фронхёфер, В.П. Сакута // Современная наука и технологии: актуальные вопросы, достижения и инновации: Монография / Под общ. ред. Г. Ю. Гуляева. — Пенза: МЦНС «Наука и Просвещение». — 2023. — С. 22-32.

7. Рудикова-Фронхёфер, Л.В. О подходах к проектированию и разработке информационно-аналитической системы исторических памятников в Республике Беларусь // Л.В. Рудикова-Фронхёфер, А.И. Жвалевский // Современная

наука и технологии: актуальные вопросы, достижения и инновации: Монография / Под общ. ред. Г. Ю. Гуляева. — Пенза: МЦНС «Наука и Просвещение». — 2023. — С. 44-55.

8. Рудикова-Фронхёфер, Л.В. О разработке информационно-аналитической системы накопления и анализа данных исторической и художественной ценности // Л.В. Рудикова-Фронхёфер // Проблемы современной экономики: глобальный, национальный и региональный контекст: сб. науч. ст./ ГрГУ им. Я. Купалы; редкол.: М. Е. Карпицкая (гл. ред.), С. Е. Витун (зам. гл. ред.) [и др.]. – Гродно: ГрГУ, 2023. – С. 370-379.

9. Роб, П. Системы баз данных: проектирование, реализация и управление / П. Роб, К. Коронел; пер. с англ. – 5-е изд., перераб. и доп. – СПб.: БХВ-Петербург, 2004. – 1040 с.: ил.

10. Рудикова, Л.В. Проектирование баз данных: Учебное пособие для студентов высш. учеб. заведений по специальностям «Программное обеспечение информационных технологий», «Экономическая кибернетика», «Прикладная математика (научно-педагогическая деятельность)», «Информационные системы и технологии (в экономике)» / Л.В. Рудикова. – Минск: ИВЦ Минфина, 2009. – 352с.

11. Рудикова, Л.В. Использование средств PowerDesigner для поддержки задач проектирования // Управление в социальных и экономических системах. Материалы XV междунар. науч.-практ. конф. – Мн., 2006. – С.211–212.

УДК 378.14

ГЛАВА 5. ИСПОЛЬЗОВАНИЕ ТЕХНОЛОГИЙ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА В ПРОФЕССИОНАЛЬНОЙ ДЕЯТЕЛЬНОСТИ ВОЕННЫХ СПЕЦИАЛИСТОВ

Мамаева Наталья Анатольевна
к.т.н., доцент
Мамаев Олег Алексеевич
к.т.н., доцент
Зонненберг Юлия Евгеньевна
Военный институт (инженерно-технический) Военной академии материально-технического обеспечения имени генерала армии А.В. Хрулева
Аленичева Татьяна Сергеевна
старший преподаватель кафедры технологии производства
Омский автобронетанковый инженерный институт

Аннотация: в работе рассмотрены вопросы организации обучения курсантов военных вузов в области технологий искусственного интеллекта, а также проанализированы основные направления применения интеллектуальных систем военного назначения.
Ключевые слова: искусственный интеллект, технологии искусственного интеллекта, автоматизированные системы управления, беспилотные летательные аппараты.

USING ARTIFICIAL INTELLIGENCE TECHNOLOGIES INTELLIGENCE IN PROFESSIONAL ACTIVITY MILITARY SPECIALISTS

Mamaeva Natalia Anatolyevna,
Mamaev Oleg Alekseevich,
Zonnenberg Julia Evgenievna,
Alenicheva Tatyana Sergeevna

Abstract: The paper considers the issues of organizing the training of military university cadets in the field of artificial intelligence technologies, as well as analyzes the main areas of application of intelligent military systems.
Key words: artificial intelligence, artificial intelligence technologies, automated control systems, unmanned aerial vehicles.

1. ТЕХНОЛОГИИ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА В ПОДГОТОВКЕ ВОЕННЫХ СПЕЦИАЛИСТОВ

Актуальность развития искусственного интеллекта (ИИ) в военной сфере продиктована современными условиями ведения боевых действий. Опыт использования различных видов вооружения и военной техники демонстрирует, что время на принятие решений сократилось до критических значений, измеряемых секундами, а не минутами. По словам заместителя председателя Правительства РФ Д. Мантурова, «достижение подобной скорости реакции не представляется возможным без делегирования части обязанностей от человека к автоматизированным системам»[1].

Проблематика вопросов технологий искусственного интеллекта оказывает значительное влияние на формирование программной базы, которая задает технологические параметры перспективных образцов вооружения, военной техники и спецоборудования. В государственной программе вооружений, рассчитанной на 2025-2034 годы, выделен отдельный блок, посвященный искусственному интеллекту, где приоритетное внимание уделяется интеграции инновационных информационных, биокогнитивных решений, гиперзвуковых систем и вооружений, основанных на новых физических принципах, а также передовых средств разведки, навигации, коммуникации и контроля. В будущем военные конфликты будут все больше определяться состязанием алгоритмов ИИ, выявлением слабых мест в системах обработки данных и автоматизированного управления боевыми действиями.

В связи с этим, под эгидой Управления развития технологий искусственного интеллекта (УРТИИ) МО РФ активно реализуется процесс формирования системы подготовки военных кадров в сфере развития искусственного интеллекта.

Проведение указанной работы в военно-образовательных учреждениях основывается на правилах, зафиксированных в общегосударственных и ведомственных регламентирующих документах, среди которых можно отметить следующие:

1. Указ Президента РФ от 10.10.2019 г. № 490 «О развитии искусственного интеллекта в Российской Федерации».
2. Перечень поручений Министра обороны от 20 января 2021 г.
3. Система стандартов РФ.
4. Требования к минимуму содержания и уровням обученности курсантов по вопросам технологий искусственного интеллекта, утвержденные 23 октября 2022 г. и другие.

На основании данных требований в образовательные программы высшего образования были внесены изменения, и в настоящее время в военных вузах активно реализуется подготовка курсантов по данным вопросам. Главная задача подготовки обучающихся в области технологий ИИ состоит в том, чтобы курсанты понимали, на чем основана работа современных и перспективных образцов вооружения и военной техники, оснащенных элементами интеллектуаль-

ных систем. Это позволит обеспечить правильность формируемых ими решений, а также предостережет от их некорректного применения, которое может привести к негативным последствиям.

Рассмотрим основные понятия, связанные с технологиями и методами реализации искусственного интеллекта [2].

Интеллект, берущий начало в латинском «intellectus» (охватывающем ощущение, осознание, понимание, представление, рассуждение), является свойством психической активности, обуславливающим способность приспосабливаться к меняющейся среде, способность к обучению и накоплению знаний через опыт, осмысление и применение абстрактных концепций, а также использование полученных знаний для взаимодействия с внешней средой.

В более простом понимании, интеллект – это многогранная познавательная способность, обеспечивающая эффективное решение задач и объединяющая в себе все когнитивные функции человека: чувственное восприятие, концентрацию внимания, запоминание информации, воспроизведение образов, мыслительные операции и креативное воображение.

Различные трактовки понятия искусственного интеллекта в той или иной степени взаимосвязаны и расширяют понимание этого феномена. В начале восьмидесятых годов двадцатого века исследователи вычислительных систем Барр и Файгенбаум сформулировали следующее определение искусственного интеллекта:

Искусственный интеллект – это область информатики, которая занимается разработкой интеллектуальных компьютерных систем, то есть систем, обладающих возможностями, которые мы традиционно связываем с человеческим разумом, – понимание языка, обучение, способность рассуждать, решать проблемы и т.д.

В национальной стратегии развития искусственного интеллекта на период до 2030 года согласно указу президента Российской Федерации от 10.10.2019 г. № 490 даётся следующее определение искусственного интеллекта:

Искусственный интеллект – комплекс технологических решений, позволяющий имитировать когнитивные функции человека (включая самообучение и поиск решений без заранее заданного алгоритма) и получать при выполнении конкретных задач результаты, сопоставимые, как минимум, с результатами интеллектуальной деятельности человека.

С течением времени понятие «искусственный интеллект» расширилось, включив в себя широкий спектр алгоритмов и программ, которые демонстрируют способность решать конкретные задачи, воспроизводя подобие человеческого мышления. Основные черты, свойственные искусственному интеллекту, включают в себя:

- понимание языка;
- способность к самостоятельному обучению;
- когнитивные возможности;
- способность к совершению действий.

Искусственный интеллект особенно полезен в областях, где сконцентрировано большое количество информации разного вида. В случае, когда типы данных ограничены, аналитик может вручную обработать их. Однако, когда число параметров достигает тысяч, и при этом данные не структурированы, искусственный интеллект проявляет свою высокую эффективность.

Технологии искусственного интеллекта (рис. 1) – технологии, основанные на использовании искусственного интеллекта, включая компьютерное зрение, обработку естественного языка, распознавание и синтез речи, интеллектуальную поддержку принятия решений и перспективные методы искусственного интеллекта.

Перспективные методы искусственного интеллекта – методы, направленные на создание принципиально новой научно-технической продукции, в том числе в целях разработки универсального (сильного) искусственного интеллекта (автономное решение различных задач, автоматический дизайн физических объектов, автоматическое машинное обучение, алгоритмы решения задач на основе данных с частичной разметкой и (или) незначительных объёмов данных и иные методы).

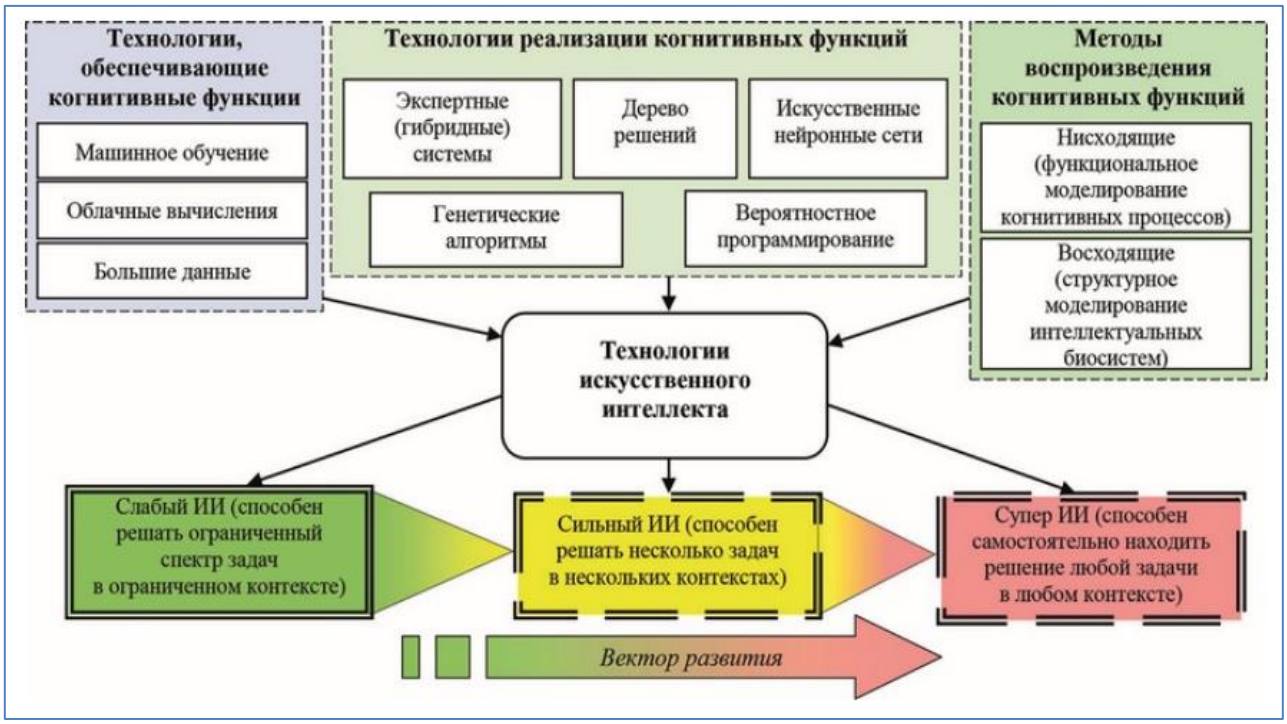

Рис. 1. Общие подходы к развитию технологий ИИ

В процессе обучения в военных вузах будущие офицеры изучают основные виды и методы искусственного интеллекта, в том числе и компьютерное зрение, анализ массивов данных, идентификацию и генерацию речевых сигналов, нейросетевые технологии, интеллектуальные комплексы помощи в принятии решений и прочие [3, 4].

С декабря 2021 года, в дополнение к общепринятым методам обучения, начали использовать игровой ИИ. Он дает возможность качественно проверять и улучшать военные замыслы. Более того, его применяют в разработке настоящих тактик ведения боя и при создании военных тренажеров, предназначенных для подготовки военнослужащих.

Экспертами отмечено, что наибольшее распространение ИИ получил в авиации – летчики моделируют различные ситуации, которые могут произойти в небе, на специальных тренажерах. Мобильная многоканальная зенитная ракетная система С-350 «Витязь» перестала быть демонстрационной моделью, и уже активно используется для защиты государственных, административных, промышленных и военных объектов от ударов современных и перспективных средств воздушного нападения.

Возможности искусственного интеллекта варьируются от роли потенциального противника до советника, но его эффективность напрямую зависит от уровня подготовки и квалификации наставника. Специалисты подчеркивают, что с технической точки зрения реально использовать ИИ для имитации боевых действий: нейронная сеть обладает более обширными знаниями, чем командующий на поле боя, быстрее анализирует информацию и выносит вердикты, а также умеет предвидеть огромное количество вариантов развития событий на несколько шагов вперед.

2. ТЕХНОЛОГИИ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА ВОЕННОГО НАЗНАЧЕНИЯ

Современная эпоха характеризуется невиданным ранее ускорением технологического прогресса в военной области. На смену эволюционному развитию и усовершенствованию существующих образцов вооружения и военной техники (ВВТ) приходят принципиально новые оружейные комплексы, которые обеспечивают резкое увеличение тактико-технических параметров (ТТХ) и боевой мощи современных ВВТ.

Преобразование характера военных операций будет существенно зависеть от развития вооружений и военной техники, тесно связаного с интеграцией интеллектуальных технологий, но ключевым моментом является широкое внедрение автоматизированных систем, управляющих войсками, вооружением и передовыми боевыми комплексами.

Внедрение ИИ обеспечит прорыв в боевом потенциале, в формировании облика вооружения и даже концепции процесса выработки решений по управлению оружием и войсками (силами).

Одной из наиболее перспективных областей применения технологий ИИ является вооруженная борьба. По оценкам ведущих отечественных экспертов, вооруженная борьба в XXI веке будет в корне отличаться от способов и методов ведения войн прошлого.

Существует несколько ключевых областей, прогресс в которых позволит разработать системы искусственного интеллекта, пригодные для использования

в военной сфере [5]:

– систематизация знаний предполагает разработку подходов к упорядочиванию, категоризации и представлению знаний из различных областей для поддержки принятия решений на всех этапах военной деятельности;

– моделирование процессов принятия решений заключается в исследовании и формализации различных стратегий мышления человека, опирающихся на разнородные данные, для ведения боевых действий, а также в создании эффективных программ для реализации этих стратегий на вычислительных устройствах;

– создание интерфейсов, использующих естественный язык, обеспечивает взаимодействие между интеллектуальной системой и экспертом в процессе решения как повседневных, так и боевых задач;

– планирование боевых операций включает в себя разработку методов построения алгоритмов управления, основанных на знании предметной области;

– обучение и актуализация базы знаний интеллектуальных систем осуществляются непосредственно в процессе их функционирования.

Рассмотрим основные условия и направления применения технологий ИИ военного назначения.

Специалисты отмечают, что увеличение продаж военных решений на развитие области искусственного интеллекта стимулируется увеличением финансирования разработки комплексных систем, использующих ИИ, и расширением применения облачных технологий. Лидирующую позицию на рынке ИИ-решений для оборонной отрасли занимают программные продукты, услуги и аппаратура, используемые в наземных войсковых операциях.

Обширные объемы данных, нуждающиеся в обработке, распределении, приоритизации и ситуационном анализе, будут автоматически анализироваться с применением специализированных программных средств, которые можно отнести к системам искусственного интеллекта.

Например, оперативное выявление угроз, влияющих на распределение целей, и быстрая оптимизация ресурсов – критически важные задачи, требующие незамедлительного и постоянного внимания. В связи с ограниченными возможностями человеческого восприятия и обработки больших потоков информации, внедрение автоматизированных решений становится логичным шагом на пути к использованию искусственного интеллекта. Такой подход позволяет оперативно и результативно решать задачи любого уровня сложности, независимо от объема входящих данных.

Применение искусственного интеллекта ускорит процесс принятия решений командирами, даст возможность выявлять наиболее важные и опасные цели для оперативного поражения высокоточным оружием. При этом, системы искусственного интеллекта будут интегрированы во все типы вооружений, предназначенных для действий на большом расстоянии.

Обработка данных будет происходить в рамках единой информационной среды, что обеспечит возможность задействования всех родов войск для реше-

ния поставленных задач и их эффективную координацию. Это позволит добиться максимальной результативности в применение военной техники и вооружения, а также будет оптимизировано, с точки зрения затрат и расхода боеприпасов. Данные системы примут на себя вспомогательные, но критически важные задачи в логистике, снабжении и других областях при планировании и проведении боевых операций.

Интеллектуальное оружие потенциально способно самостоятельно определять необходимость уничтожения цели. Однако, учитывая критическую важность подобного выбора, ключевая роль по-прежнему остается за человеком-оператором. Переводя систему в полностью автоматический режим, оператор должен быть абсолютно уверен в правильности идентификации цели и в том, что уничтожению подвергнется именно противник.

Интеллектуальные системы, основанные на нейросетях, обладают способностью к самообучению и развитию в ходе эксплуатации. Они наделены функциями обнаружения и идентификации объектов, расстановки приоритетов для их нейтрализации, выдачи команд автоматизированным устройствам и самостоятельного принятия решений об использовании оружия. Данные комплексы могут быть размещены как в фиксированных точках, так и на мобильных платформах, а также объединены в единую сеть для координации действий. Последний вариант особенно эффективен для решения задач обеспечения безопасности, например, охраны периметра. Внедрение подобных систем на критически важных объектах позволяет минимизировать влияние человеческого фактора, такого как утомляемость и снижение концентрации внимания.

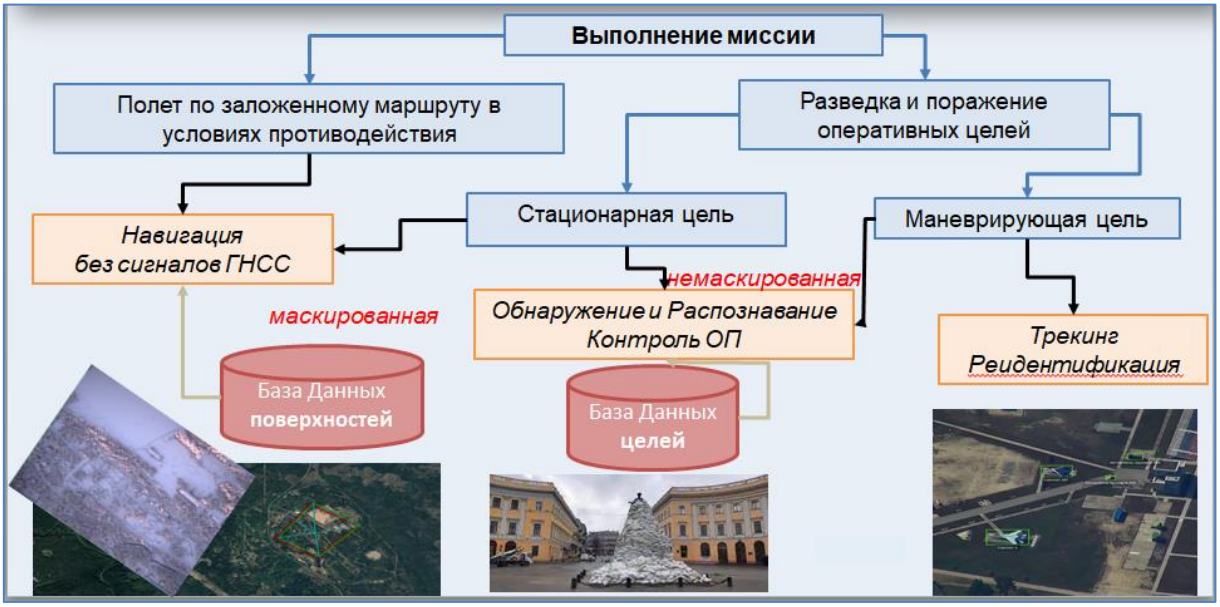

Рис. 2. Концепция системы разведки и поражения с применением БПЛА

Вооруженные силы и частные технологические компании уделяют повышенное внимание спутникам, дронам, кибернетическим инструментам и искус-

ственному интеллекту. Эти разработки занимают центральное место в их приоритетах. Миниатюрные дроны, используемые в коммерческих целях, оказались существенным элементом в конфликте, давая возможность армиям собирать разведывательные данные, вносить коррективы в наведение артиллерийского огня и авиационных ударов, или применять беспилотные аппараты в роли дронов-камикадзе (рис. 2).

Примеры использования методов технологий искусственного интеллекта для решения военно-прикладных задач представлены на рисунке 3.

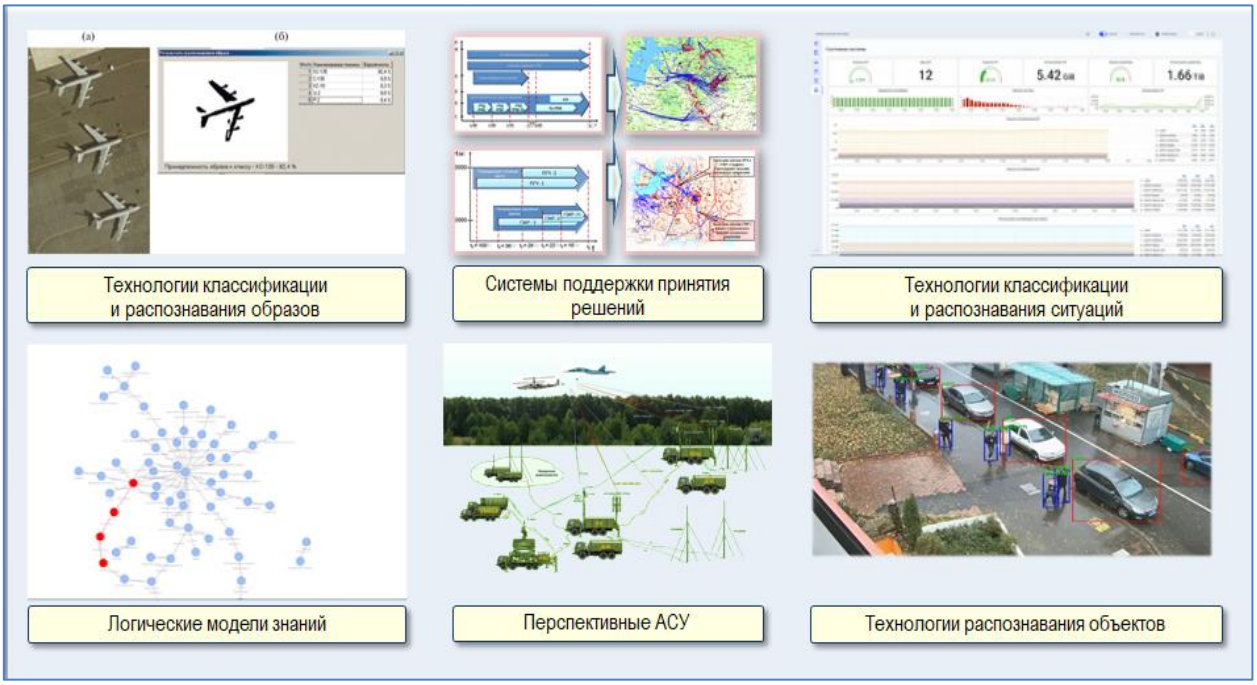

Рис. 3. Примеры решения военно-прикладных задач с использованием технологий искусственного интеллекта

В таблице 1 отражены ключевые области применения искусственного интеллекта для оптимизации процессов материально-технического обеспечения (МТО).

Российские специалисты отмечают распространенный на Западе подход: прежде чем создавать военные ИИ-системы, сначала разрабатываются гражданские аналоги, которые затем модифицируются для военных целей. Это значительно сокращает сроки и расходы на создание военных систем, использующих искусственный интеллект.

Все ведущие державы так или иначе вкладываются в развитие ИИ, лидерами в данном направлении являются США и Китай. США в развитии ИИ полагаются на работу с коммерческими структурами, например, в феврале 2024 года компания Google официально отказалась от своего обязательства не разрабатывать ИИ для военного применения.

В основном, США и Китай акцентируют внимание на использовании искусственного интеллекта в военной сфере, начиная с оптимизации работы

беспилотных систем вооружения и постепенно переходя к контролю над беспилотными и пилотируемыми платформами всех видов.

Таблица 1

Ключевые области использования ИИ в сфере МТО

Вид подсистемы МТО	Направление использования технологий ИИ
МАТЕРИАЛЬНОЕ ОБЕСПЕЧЕНИЕ	
Подсистема обеспечения горючем и ракетным топливом	Роботизация складской и обеспечивающей инфраструктур службы горючего. Детальное (посуточного) прогнозирование расхода и потерь горючего в ходе боевых действий
Подсистема продовольственного обеспечения	Роботизация складской и обеспечивающей инфраструктур продовольственной службы.
Подсистема вещевого обеспечения	Роботизация складской и обеспечивающей инфраструктур вещевой службы. Разработка интеллектуальных роботов пошива и комплектования обмундирования и обуви
ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ	
Подсистема ракетно- и артиллерийского-технического обеспечения	Роботизация складской и обеспечивающей инфраструктур службы РАВ, разработка интеллектуальных роботов технической разведки, эвакуации и ремонта РАВ.
Подсистема танкотехнического обеспечения	Роботизация складской и обеспечивающей инфраструктур бронетанковой службы, разработка интеллектуальных роботов технической разведки, эвакуации и ремонта БТВ.
Подсистема автотехнического обеспечения	Роботизация складской и обеспечивающей инфраструктур автомобильной службы, разработка интеллектуальных роботов технической разведки, эвакуации и ремонта АТ.
ТРАНСПОРТНОЕ ОБЕСПЕЧЕНИЕ	
Подсистема автотранспортного обеспечения	Организация движения автомобильных колонн с беспилотным управлением автотранспортом
Подсистема воинских перевозок	Интеллектуальная поддержка принятия решений и планирования воинских перевозок
Подсистема вспомогательного флота	Разработка интеллектуальных беспилотных средств доставки МС в удаленные районы. Создание беспилотных поисково-спасательных роботов, средств измерения физических полей и размагничивания кораблей
Подсистема применения Железнодорожных войск	Техническая разведка железных дорог на основе использования интеллектуальных беспилотных аппаратов и роботизированных комплексов для восстановления ж/д.

Основной вопрос остается в том, в какой области его применение будет эффективно и оправданно, а в каких принесёт больше вреда, чем пользы [6].

Перемещение по поверхности

Движение по дорогам общего пользования регламентировано достаточно строгими правилами, покрытие дороги (в нормальном случае) максимально качественное, нанесена разметка и установлены предупреждающие знаки. Но да-

же на дорогах общего пользования нередки нештатные ситуации, отреагировать на которые автопилот в лучшем случае может только полной остановкой, а в худшем – спровоцировав аварию транспортного средства.

А теперь представим, например, местность вблизи линии боевого соприкосновения – задымление, воронки от взрывов, мины и т.д. Вследствие этого, в части управления наземными транспортными средствами, боевой ИИ применяется лишь как средство подстраховки водителя, на коротком участке маршрута, например, когда боевой машиной управляют дистанционно.

По наземным целям

Одним из направлений применения боевого ИИ является использование его для поражения наземных целей – неважно, с наземной боевой машины или с воздуха, например, с квадрокоптера.

Реалистичное и уже работающее применение ИИ – это донаведение на цель FPV-дронов и БПЛА-камикадзе на конечном участке полёта.

Нередкой является ситуация, когда оператор теряет FPV-дрон буквально на последних метрах атаки из-за того, что средства радиоэлектронной борьбы подавляют сигнал управления или видеоканал передачи данных. Однако в том случае, если на дроне присутствует интеллектуальная система наведения, то оператор просто осуществляет захват цели, а далее дрон наводится на неё самостоятельно, даже при потере сигналов управления.

По воздушным целям

Здесь применять ИИ будет уже немного проще. Начать можно с решения задачи по поражению таких целей, как FPV-дроны. В сети Интернет есть видео, на котором российский разведывательный БПЛА Zala автоматически уклоняется от атак украинского FPV-дрона, обнаружив его встроенной камерой.

Захват цели и самонаведение, работа противодроновых турелей и охота дронов на дроны – всё это уже достаточно зрелые технологии, которые применяются на поле боя или будут применяться в ближайшее время.

Рой

Высокую эффективность роевое применение дронов с использованием ИИ можно прогнозировать при работе по воздушным целям разных типов, например, при перехвате БПЛА-камикадзе большой дальности с помощью FPV-дронов. Что касается работы по наземным целям, то здесь, скорее всего, потребуется участие человека в контуре принятия решений, когда оператор (операторы) будут подтверждать или отклонять уничтожение обнаруженных искусственным интеллектом целей.

Таким образом, благодаря искусственному интеллекту удалось создать такие принципиально новые функциональные задачи для боевых комплексов и изделий ВВТ, как автоматическое обнаружение и распознавание целей, интеллектуальное управление БЛА, обеспечение точности навигационных систем, дальности боевого применения.

Использование современных и перспективных методов и средств искусственного интеллекта в военном деле существенно изменит принципы работы и

руководства должностных лиц, принимающих решения, и даст новые положительные результаты в управлении оружием и войсками (силами).

Список источников

1. Искусственный интеллект в военном деле [электронный ресурс]. Путь доступа: https://www.tadviser.ru/index.php (дата обращения: 15.01.2025).

2.Технологии искусственного интеллекта. – М.: Агентство промышленного развития Москвы. 2019. 156 с.

3. Мамаева, Н.А., Омельченко, В.И. Методико-технологические основы обучения курсантов в условиях информационно-образовательной среды военного вуза [Текст]: монография / Н.А. Мамаева, В.И. Омельченко. – Омск: ОАБИИ, 2020. – 117 с.

4. Моисеева, Л.В., Селезнева О.В. Цифровая экосистема образовательно-профессионального пространства вуза: теоретико-методические аспекты военного образования / Инновационная научная современная академическая исследовательская траектория (ИНСАЙТ). 2024, № 2 (18). С. 165-182.

5. Основы технологий искусственного интеллекта: учебное пособие / М.А. Павленко, А.А. Анциферов, Я.С. Докучаев [и др.]. – Тверь: ВА ВКО, 2024. – 116 с.

6. Боевой ИИ в войнах и вооруженных конфликтах ближайшего будущего. Военное обозрение [электронный ресурс]. Путь доступа: https://topwar.ru/261656-boevoj-ii-v-vojnah-i-vooruzhennyh-konfliktah-blizhajshego-buduschego.html (дата обращения: 31.03.2025).

УДК 330

ГЛАВА 6. РАЗРАБОТКА МОДЕЛЕЙ РАДИАЦИОННЫХ ЭФФЕКТОВ ПРИ ВОЗДЕЙСТВИИ ИМПУЛЬСНОГО ГАММА–НЕЙТРОННОГО ИЗЛУЧЕНИЯ НА ПОЛУПРОВОДНИКОВУЮ СТРУКТУРУ И СОЗДАНИЕ ИНФОРМАЦИОННЫХ СРЕДСТВ ОЦЕНКИ ПОКАЗАТЕЛЕЙ СТОЙКОСТИ МИКРОСХЕМ

Куницын Вадим Игоревич,
Фролов Сергей Викторович
магистранты
ФГБОУ ВО «Воронежский государственный лесотехнический университет имени Г.Ф. Морозова»

Аннотация: исследуются радиационные эффекты в полупроводниковых структурах под воздействием импульсного гамма–нейтронного излучения. Разработаны математические и компьютерные модели, позволяющие прогнозировать деградацию параметров микросхем. Предложены методы оценки радиационной стойкости для автоматизированного анализа устойчивости электронных компонентов.
Ключевые слова: радиационные эффекты, импульсное излучение, полупроводниковые структуры, моделирование, радиационная стойкость, информационные системы.

DEVELOPMENT OF MODELS FOR RADIATION EFFECTS UNDER PULSED GAMMA–NEUTRON IRRADIATION IMPACT ON SEMICONDUCTOR STRUCTURES AND CREATION OF INFORMATION TOOLS FOR ASSESSING MICROCIRCUIT RADIATION HARDNESS

Kunitsyn Vadim Igorevich,
Frolov Sergey Viktorovich

Abstract: The study investigates radiation effects in semiconductor structures exposed to pulsed gamma–neutron irradiation. Mathematical and computer models have been developed to predict the degradation of microcircuit parameters. Methods for assessing radiation hardness are proposed for automated analysis of electronic component resilience.
Keywords: radiation effects, pulsed irradiation, semiconductor structures, modeling, radiation hardness, information systems.

Радиационная стойкость электронных компонентов — ключевое требование для техники, работающей в условиях космического излучения, ядерных взрывов или аварий на АЭС. Импульсное гамма–нейтронное излучение вызывает сложные комбинированные эффекты, приводящие к необратимым изменениям в полупроводниковых приборах.

ВЗАИМОДЕЙСТВИЕ ИОНИЗИРУЮЩЕГО ИЗЛУЧЕНИЯ С ПОЛУПРОВОДНИКОВЫМИ МАТЕРИАЛАМИ

Гамма–кванты, обладающие высокой проникающей способностью, взаимодействуют с полупроводниковой структурой посредством трех основных механизмов:

1. **Фотоэффект** – доминирует при энергиях <100 кэВ:
1. Полное поглощение γ–кванта с выбиванием электрона из внутренних оболочек
2. Вероятность ~Z^4/E^3 (Z – атомный номер, E – энергия кванта)
3. Образование вакансий и оже–электронов
2. **Комптон–эффект** – основной механизм в диапазоне 100 кэВ–10 МэВ:
1. Упругое рассеяние на электронах
2. Формирование вторичных электронов с энергией до нескольких МэВ
3. Вероятность ~Z/E
3. **Образование электрон–позитронных пар** (E>1.022 МэВ):
1. Конверсия энергии в массу в кулоновском поле ядра
2. Последующая аннигиляция с излучением двух 511 кэВ квантов

Демонстрируется вероятности взаимодействия гамма–квантов с кремнием (основным материалом микроэлектроники) через три ключевых процесса (табл. 1.1):

1. Фотоэффект
2. Комптон–эффект
3. Образование электрон–позитронных пар

Таблица 1.1

Сечения взаимодействия гамма–излучения с кремнием при различных энергиях

Энергия (МэВ)	Фотоэффект (барн)	Комптон (барн/электрон)	Пар образование (барн)
0.1	1.2×10^{4}	5.1	–
1	1.7×10^{0}	2.1	0.001
10	1.5×10^{-3}	0.4	0.12

Единицы измерения: **барны** (1 барн = 10^{-24} см²), стандартная единица для сечений взаимодействия.

Зависимость от энергии:

1. **Низкие энергии (0.1 МэВ)**:

1) Доминирует **фотоэффект** (1.2×1041.2×104 барн) — гамма–квант полностью поглощается, выбивая электрон из внутренней оболочки атома.

2) Комптон–эффект слабее (5.1 барн/электрон), образование пар невозможно (требуется E > 1.022 МэВ).

2. **Средние энергии (1 МэВ)**:

1) Фотоэффект резко падает (1.7×1001.7×100 барн) из за ∼1/E3∼1/*E*3 зависимости.

2) Комптон–эффект остается значимым (2.1 барн/электрон).

3) Появляется **рождение пар** (0.001 барн), но вклад минимален.

3. **Высокие энергии (10 МэВ)**:

1) Фотоэффект ничтожен (1.5×10−31.5×10−3 барн).

2) Комптон–эффект слабеет (0.4 барн/электрон).

3) **Образование пар** становится основным процессом (0.12 барн).

Практические выводы:

1. Для **защиты электроники** от радиации:

1) При E < 1 МэВ эффективны **тяжелые элементы** (свинец) — подавляют фотоэффект.

2) При E > 5 МэВ требуются **многослойные экраны** (комбинация Pb + полимеры) для защиты от паробразования.

Нюансы и ограничения данных:

1. **Точность значений**:

1) Данные приведены для **чистого кремния** (100% Si). В реальных микросхемах (SiO_2, металлические слои) сечения могут отличаться.

2) Усреднены для **изотропного излучения**.

2. **Температурная зависимость**:

1. Не учитывает тепловые эффекты (при высоких T сечения могут измениться на 5–10%).

3. **Пороговые эффекты**:

1) Для паробразования указано сечение **полное**, но реально процесс идет только вблизи ядер (кулоновское поле).

Нейтроны (обычно в диапазоне 0.1–20 МэВ) вызывают:

1. **Упругое рассеяние** (доминирует для E<1 МэВ):

1) Передача энергии ядрам матрицы (максимальная для водорода)

2) Сечение ~1/v (v – скорость нейтрона)

2. **Неупругое рассеяние** (E>1 МэВ):

1) Возбуждение ядер с последующим γ–излучением

2) Ядерные реакции (n,α), (n,p)

3. **Радиационный захват** (особенно для Ge, GaAs):

1) Образование радиоактивных изотопов

2) Дополнительное γ–излучение

ПЕРВИЧНЫЕ И ВТОРИЧНЫЕ РАДИАЦИОННЫЕ ЭФФЕКТЫ

Ионизационные процессы:

1. **Объемная ионизация**:

1) Генерация электрон–дырочных пар (3.6 эВ/пара в Si)
2) Накопление заряда в диэлектриках (SiO_2, Si_3N_4)

2. **Поверхностные эффекты**:

1) Образование интерфейсных состояний Si–SiO_2
2) Сдвиг порогового напряжения MOSFET

3. **Локальный перегрев**:

1) Термопробой p–n переходов
2) Формирование проводящих каналов

Смещения атомов (Displacement Damage):

1. **Кинетика образования дефектов**:

1) Поток смещений (dpa – displacements per atom)
2) Сечение смещения T(dE/dx)

2. **Типы дефектов**:

1) Точечные (вакансии, межузельные атомы)
2) Комплексные (A–центры, дивакансии)
3) Кластерные повреждения

Скорость образования дефектов

$$dN\_d/dt = Φσ\_d(E) – R(T)N\_d^2 \quad (1.1)$$

где:

Ф–поток частиц,

σ_d–сечение смещения,

R–коэффициент рекомбинации,

T – температура

Формула представляет собой дифференциальное уравнение, моделирующее динамику концентрации точечных дефектов (вакансий, межузельных атомов) в кристаллической решетке при облучении [1]. Она позволяет:

1. Прогнозировать накопление повреждений в материале.
2. Оценивать влияние температуры и потока излучения на деградацию полупроводника.

ОСОБЕННОСТИ ИМПУЛЬСНОГО ВОЗДЕЙСТВИЯ

Тепловой удар и фазовые переходы:

Импульсное излучение вызывает:

1. **Локальный нагрев** до 10^3–10^4 К за пикосекунды, приводящий к:

1) Формированию ударных волн (давление до 10 ГПа);
2) Аморфизации материала при плотности энергии >10^{23} эВ/см³;
3) Образованию расплавленных нанообластей.

Нелинейные эффекты при высокой мощности дозы:

1. **Плазменные явления**:
1) Экранирование внешних электрических полей;
2) Коллективные взаимодействия в электрон–дырочной плазме.
2. **Радиационно–индуцированная проводимость**:
1) Резкий рост концентрации носителей (10^{18}–10^{20} $см^{-3}$);
2) Переход материала во временное металлическое состояние.

Синергетические эффекты:

1. **Усиление ионизации**:
1) Нейтронная активация ядер с последующим γ–излучением;
2) Каскадные процессы в предварительно облученной матрице.
2. **Модификация дефектной структуры**:
1) Гамма–излучение изменяет диффузию дефектов (вакансий, межузельных атомов);
2) Нейтроны создают каналы повышенной проводимости, усиливая ионный пробой.

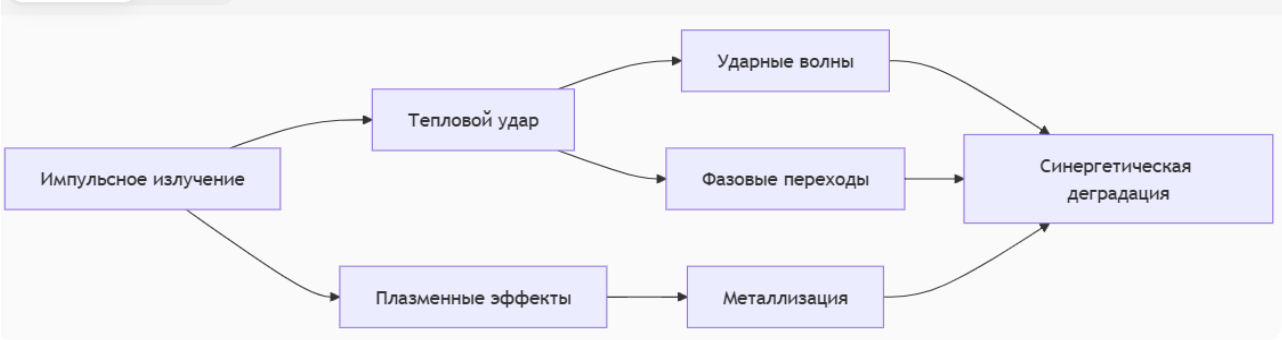

Рис. 1. 1. Схема взаимосвязи ключевых элементов

На схеме показаны основные эффекты, возникающие в полупроводниковых материалах при импульсном радиационном воздействии (например, гамма–нейтронном облучении), и их взаимосвязи (рис. 1.1) [2].

Центральный элемент — **«Синергетическая деградация»**, означающая, что совместное действие всех эффектов приводит к более сильным повреждениям, чем просто их сумма.

Основные эффекты:

1. **Тепловой удар** — мгновенный нагрев до сверхвысоких температур, вызывающий:
1) **Ударные волны** (микротрещины, деформация кристаллической решетки).
2) **Фазовые переходы** (расплавление, аморфизация материала).
2. **Плазменные эффекты** — образование электрон–дырочной плазмы, которая:
1) Нарушает работу транзисторов (экранирование полей).
2) Приводит к металлизации — резкому росту проводимости и коротким замыканиям.

3. **Индуцированное излучение** (вторичное) — дополнительная ионизация, усиливающая все перечисленные процессы.

Указанные процессы не изолированы, а взаимодействуют между собой, создавая кумулятивный эффект, который значительно ускоряет разрушение микросхем. Поэтому при разработке радиационно-устойчивых компонентов необходимо комплексно учитывать все механизмы воздействия [3].

Кратковременное воздействие гамма-нейтронного излучения вызывает сложную комбинацию ионизационных и структурных повреждений. Совместное влияние этих факторов приводит к синергетическим эффектам, которые нельзя описать простым суммированием отдельных воздействий. Кроме того, при импульсном облучении возникают термомеханические напряжения, что требует их обязательного включения в модели оценки радиационной стойкости.

СОВРЕМЕННЫЕ МЕТОДЫ МОДЕЛИРОВАНИЯ РАДИАЦИОННЫХ ЭФФЕКТОВ В ПОЛУПРОВОДНИКОВЫХ СТРУКТУРАХ

Таблица 2

Сравнительные характеристики методов моделирования

Метод	Пространственное разрешение	Временной масштаб	Типичные применения
Ab initio	0.1–1 нм	фс–пс	Дефектообразование
MD	1–100 нм	пс–нс	Каскады смещений
kMC	10–1000 нм	нс–мкс	Диффузия дефектов
ТКАН	>1 мкм	мкс–с	Деградация параметров

В таблице представлен анализ различных подходов к моделированию радиационных эффектов в полупроводниковых материалах, оцениваемых по трем основным характеристикам: пространственной точности, временному диапазону и практическому применению.

Рассматриваемые методы расположены в последовательности от наноразмерного до макроскопического уровня моделирования. Ab initio подходы демонстрируют предельно высокую пространственную точность (0.1-1 нм) и работают в ультракоротком временном диапазоне (фемто-пикосекунды), что особенно ценно для исследования атомарных механизмов образования дефектов. Методы молекулярной динамики охватывают более широкие пространственные (1-100 нм) и временные (пико-наносекунды) диапазоны, что позволяет эффективно моделировать процессы атомных смещений.

Кинетические методы Монте-Карло обеспечивают моделирование в пространственном масштабе 10-1000 нм при временных интервалах до микросекунд, что оптимально для исследования диффузионных процессов дефектов. Технологическое компьютерное моделирование (TCAD) работает с масштаба-

ми свыше 1 микрона и временными промежутками от микросекунд до секунд, позволяя анализировать параметрическую деградацию целых приборных структур [4].

Представленные данные иллюстрируют взаимодополняемость различных методов, охватывающих весь спектр пространственно-временных характеристик, необходимых для всестороннего анализа радиационных эффектов - от атомарных изменений до поведения готовых полупроводниковых компонентов. Оптимальный выбор методики определяется конкретными задачами исследования и требуемым уровнем детализации (табл. 2.1).

Среди специализированных инструментов моделирования следует выделить методы Монте-Карло, включающие GEANT4 и MCNP/FLUKA. GEANT4 характеризуется комплексной системой трекинга частиц и содержит специализированные библиотеки физических процессов, такие как G4EmStandardPhysics_option4, которые могут быть оптимизированы для полупроводниковых материалов. В свою очередь, MCNP и FLUKA ориентированы на моделирование нейтронного транспорта и анализ ядерных реакций, используя комбинированные подходы Монте-Карло [5].

Основное уравнение переноса Монте–Карло

$$\partial\psi/\partial t + \Omega\cdot\nabla\psi + \Sigma_t\psi = \iint\Sigma_s(E'\to E,\Omega'\to\Omega)\psi(E',\Omega')dE'd\Omega' + Q \qquad (2.1)$$

Левая часть уравнения описывает изменение углового потока частиц:

1. $\partial\psi/\partial t$ — частная производная углового потока ψ по времени t (изменение плотности частиц во времени)
2. $\Omega\cdot\nabla\psi$ — пространственная дивергенция потока (Ω – единичный вектор направления, ∇ – оператор набла)
3. $\Sigma_t\psi$ — полное взаимодействие частиц с материалом (Σ_t – макроскопическое полное сечение взаимодействия)

Правая часть уравнения учитывает источники и преобразования частиц:

1. $\iint\Sigma_s(E'\to E,\Omega'\to\Omega)\psi(E',\Omega')dE'd\Omega'$ — двойной интеграл по энергии и углу, описывающий:
   1) Σ_s – сечение рассеяния
   2) $E'\to E$, $\Omega'\to\Omega$ – переход от начальных (E',Ω') к конечным (E,Ω) параметрам
   3) $\psi(E',\Omega')$ – угловой поток частиц с исходными параметрами
   4) Q — внешний источник частиц

При компьютерном моделировании полупроводниковых материалов особую важность приобретает анализ процессов генерации вторичных частиц. К ним относятся электрон-фотонные каскады и различные типы ядерных реакций, в частности (n,α) и (n,p) процессы. Учет особенностей кристаллической решетки дает возможность исследовать ориентационные зависимости и канальные явления, тогда как построение карт дефектов с расчетом неионизирующих потерь энергии (NIEL) позволяет количественно оценить степень повреждения материала.

Современные TCAD-системы, такие как Sentaurus Synopsys и Silvaco Atlas, предоставляют комплексные возможности для анализа радиационных эффектов в полупроводниковых устройствах. Sentaurus Synopsys включает в себя набор физических моделей, охватывающих Shockley-Read-Hall рекомбинацию, оже-процессы и квантовые поправки, а также специализированные модули для радиационных исследований, включая Trap Dynamics Model и Radiation Aware Models. Практические примеры моделирования МОП-транзисторов демонстрируют характерные эффекты деградации - снижение подвижности носителей и изменение порогового напряжения. Silvaco Atlas концентрируется на моделировании радиационных повреждений с учетом поверхностных и объемных ловушек, обеспечивая калибровку по суммарной ионизирующей дозе (TID) и анализ явления однократного запирания (SEL).

Для оперативной оценки радиационных эффектов широко применяются аналитические модели, предлагающие упрощенные, но достаточно точные методы расчета ионизационных и структурных повреждений. Эти подходы особенно востребованы при предварительном проектировании радиационно-стойкой электроники.

Модель Oxide Trapped Charge

$$\Delta V\_ot = qN\_ot/C\_ox \quad (2.2)$$

1. **ΔV_ot**

1) **Физический смысл**: Сдвиг порогового напряжения (threshold voltage shift), вызванный накоплением заряда в окисле.

2) **Единицы измерения**: Вольты (В).

2. **q**

1) **Физический смысл**: Элементарный заряд (заряд электрона).

2) **Значение**: $q \approx 1.602 \times 10-19 q \approx 1.602 \times 10-19$ Кл.

3) **Роль в уравнении**: Преобразует количество зарядов (N_ot) в электрический потенциал.

3. **N_ot**

1) **Физический смысл**: Плотность заряда, захваченного в окисле (oxide trapped charge density).

2) **Единицы измерения**: Заряды на квадратный сантиметр ($см^{-2}$).

3) **Примечание**: Возникает из-за радиационно-индуцированных дефектов в SiO_2.

4. **C_ox**

1) **Физический смысл**: Ёмкость окисла (oxide capacitance) на единицу площади.

2) **Единицы измерения**: Фарады на квадратный сантиметр ($Ф/см^2$).

Модель Oxide Trapped Charge позволяет количественно оценить влияние накопленного заряда на изменение электрических характеристик, тогда как модель интерфейсных состояний устанавливает зависимость их плотности от полученной дозы радиации. При анализе дислокационных дефектов применяются модели, описывающие ухудшение подвижности носителей и сокращение вре-

мени их жизни, учитывающие интенсивность радиационного воздействия.

Совокупность данных подходов формирует целостную методологию исследования радиационных эффектов, охватывающую все уровни - от атомарных изменений кристаллической решетки до функциональных характеристик готовых полупроводниковых приборов. Такой многоуровневый анализ обеспечивает полное понимание механизмов радиационной деградации и позволяет разрабатывать эффективные методы защиты электронных компонентов.

Модель деградации подвижности

$$\mu = \mu\_0/(1 + K\_d \cdot Ф) \quad (2.3)$$

Эта формула описывает **снижение подвижности носителей заряда** (электронов или дырок) в полупроводнике под воздействием радиационного облучения. Она связывает исходную подвижность с потоком частиц и коэффициентом повреждения, что критично для оценки работоспособности микросхем в радиационных условиях.

1. **μ*μ***

1) **Физический смысл**: Подвижность носителей заряда **после облучения**.

2) **Единицы измерения**: см²/(В·с).

3) **Важность**: Определяет скорость дрейфа носителей в электрическом поле. Чем ниже μ*μ*, тем хуже производительность транзистора.

2. **μ0*μ*0**

1. **Физический смысл**: Исходная подвижность носителей **до облучения**.

2. **Зависимость**: Зависит от материала (например, для кремния: μ0≈1400*μ*0≈1400 см²/(В·с для электронов).

3. **Kd*Kd***

1) **Физический смысл**: Коэффициент повреждения (displacement damage coefficient).

2) **Единицы измерения**: см²/частица.

3) **Что характеризует**: Эффективность образования дефектов при облучении. Чем выше Kd*Kd*, тем сильнее деградация.

4) **Пример**: Для электронов в Si при 1 МэВ: Kd∼10−18*Kd*∼10−18–10−1710−17 см²/частица.

4. **ФФ**

1) **Физический смысл**: Интегральный поток частиц (нейтронов, протонов и др.).

2) **Единицы измерения**: частицы/см².

3) **Примечание**: Для космических применений типичные значения ФФ достигают 10121012–10151015 частиц/см².

Комбинация методов Монте-Карло и TCAD-моделирования образует эффективную платформу для всестороннего исследования радиационных эффектов в полупроводниковых компонентах. TCAD-системы (такие как Sentaurus и Silvaco), ориентированные на моделирование работы электронных устройств, способны учитывать радиационные повреждения, однако требуют точных входных данных о пространственном распределении дефектов. Это обуславли-

вает необходимость совместного применения: первоначальное моделирование методом Монте-Карло формирует карту радиационных повреждений, которая затем используется в TCAD-анализе для оценки их воздействия на рабочие параметры приборов [6].

Данная методология приобретает особую значимость при создании радиационно-устойчивой электроники для экстремальных условий эксплуатации (космическая техника, ядерные установки). Такой подход обеспечивает двусторонний анализ - от атомарных процессов до системных последствий для функционирования интегральных схем. Типичный пример включает расчет распределения дефектов от протонного облучения в GEANT4 с последующим исследованием их влияния на параметры MOSFET-транзисторов в Sentaurus [7].

Ключевое достоинство интегрированной методики заключается в прогнозировании радиационной устойчивости на стадии проектирования, что существенно оптимизирует временные и финансовые затраты на разработку. При этом критически важным остается этап калибровки моделей и их верификации экспериментальными данными, поскольку достоверность конечных результатов напрямую зависит от точности передачи информации между различными уровнями.

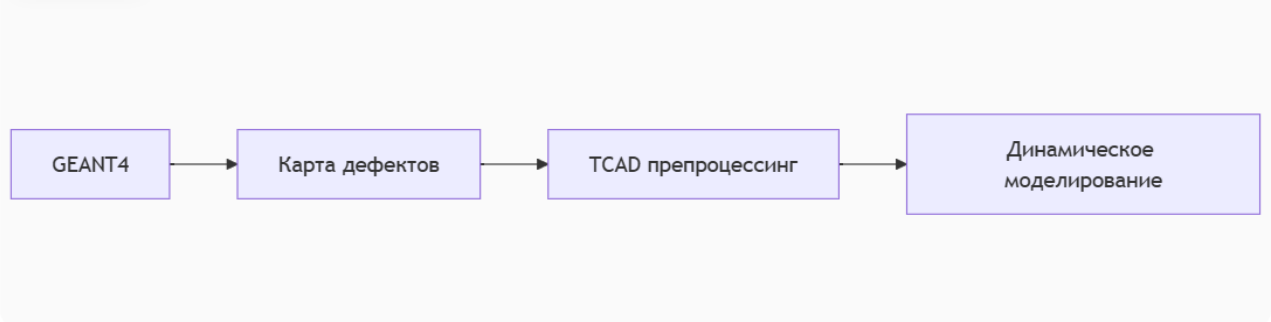

Рис. 2.1 – Схема последовательности этапов комплексного моделирования радиационных эффектов в полупроводниковых устройствах

Предлагаемая схема моделирования радиационных воздействий объединяет возможности программных комплексов GEANT4 и TCAD. На первом этапе в GEANT4 осуществляется детальное моделирование прохождения частиц через вещество с расчетом их взаимодействия с материалом. В результате формируется пространственно-распределенная карта радиационных повреждений, содержащая информацию о дефектах кристаллической решетки, ионизационных потерях и других микроструктурных изменениях. Полученные данные включают точные координаты повреждений, их тип и концентрацию в различных слоях полупроводниковой структуры.

Ключевой этап препроцессинга для TCAD-моделирования предполагает преобразование выходных данных GEANT4 в формат, пригодный для дальнейшего анализа. В процессе конвертации выполняется адаптация расчетной сетки, масштабирование параметров и приведение данных к виду, соответству-

ющему требованиям TCAD-систем. Этот этап имеет принципиальное значение, поскольку обеспечивает корректную передачу информации между различными уровнями моделирования [8].

Финальная стадия - динамическое TCAD-моделирование - позволяет оценить влияние выявленных радиационных повреждений на электрические характеристики приборов. В ходе моделирования анализируются изменения ключевых параметров транзисторных структур: порогового напряжения, подвижности носителей заряда, токов утечки. Особый акцент делается на исследовании временной эволюции радиационных эффектов, что дает возможность разделить кратковременные и долговременные последствия облучения.

Данная методология особенно востребована при разработке радиационностойкой элементной базы для космической техники и оборудования, работающего в условиях повышенного радиационного фона. Она обеспечивает сквозной анализ - от элементарных актов взаимодействия частиц с веществом до их влияния на функциональные характеристики готовых устройств (рис 2.1).

Современные подходы к моделированию радиационных эффектов реализуют многоуровневую систему, охватывающую все масштабы - от атомарного до приборного. Гибридные методики (MC–TCAD) позволяют оптимально сочетать точность расчетов с вычислительной эффективностью. Валидация моделей требует комплексного сопоставления с экспериментальными данными различного масштаба. Перспективным направлением развития является сочетание традиционных методов моделирования с алгоритмами машинного обучения и квантовыми вычислениями.

Проведенное исследование предлагает всесторонний анализ радиационных эффектов в полупроводниковых структурах при комбинированном гамма-нейтронном облучении. Работа объединяет фундаментальное изучение физических механизмов повреждений с разработкой практических инструментов оценки радиационной стойкости интегральных схем.

Основное достижение исследования заключается в реализации системного подхода, охватывающего все аспекты проблемы - от микроскопических механизмов радиационных повреждений до создания прикладных расчетных систем для инженерных приложений. Особый акцент сделан на анализе комбинированного радиационного воздействия, что особенно важно для реальных условий эксплуатации электроники в экстремальных условиях.

Разработанные математические модели и вычислительные алгоритмы обеспечивают высокоточное прогнозирование поведения полупроводниковых приборов в радиационных полях. Использование современных вычислительных методик, включая методы Монте-Карло и TCAD-моделирование, позволяет адекватно описывать сложные физические процессы на всех масштабах - от атомных взаимодействий до функционирования готовых устройств.

Практическая ценность работы подтверждается созданием специализированного программного обеспечения для оценки радиационной стойкости, применяемого при проектировании электроники для космических систем, ядерных

установок и других ответственных применений. Предложенные решения значительно сокращают затраты на натурные испытания и ускоряют процесс разработки радиационно-устойчивых компонентов.

Перспективные направления дальнейших исследований включают углубленное изучение квантовых эффектов в наноструктурах, разработку новых радиационно-стойких материалов, а также внедрение методов искусственного интеллекта для оптимизации процессов моделирования

Список источников

1. Волновая транспортировка энергии, импульса и момента импульса в космической плазме с магнитным полемю Лабораторное и численное моделирование / В. Н. Тищенко, Ю. П. Захаров, А. Г. Березуцкий [и др.] // Проблемы физики высоких плотностей энергии : Материалы международной конференции, Саров, 19–22 апреля 2016 года. – Саров: Российский Федеральный ядерный центр - Всероссийский научно-исследовательский институт экспериментальной физики, 2022. – С. 466-472. – EDN RWCPDF.

2. Зольников, В. К. Исследование и разработка методов моделирования характеристик ИМС в условиях воздействия радиации : специальность 05.13.12 "Системы автоматизации проектирования (по отраслям)" : автореферат диссертации на соискание ученой степени доктора технических наук / Зольников Владимир Константинович. – Воронеж, 2024. – 32 с. – EDN ZKLBGB.

3. Зольникова, А. Н. Моделирование характеристик КМОП ИС с учетом радиации в САПР ИЭТ : специальность 05.13.12 "Системы автоматизации проектирования (по отраслям)" : автореферат диссертации на соискание ученой степени кандидата технических наук / Зольникова Анна Николаевна. – Воронеж, 2023. – 19 с. – EDN ZKUZLX.

4. Панюшкин, Н. Н. Моделирование показателей радиационной стойкости кремниевых интегральных схем : специальность 05.27.01 "Твердотельная электроника, радиоэлектронные компоненты, микро- и наноэлектроника, приборы на квантовых эффектах" : автореферат диссертации на соискание ученой степени доктора технических наук / Панюшкин Николай Николаевич. – Воронеж, 2021. – 22 с. – EDN ZQEUQX.

5. Авторское свидетельство № 1517674 A1 СССР, МПК H01L 31/0203. Полупроводниковый детектор гамма-излучения : № 4358433/25 : заявл. 04.01.1988 : опубл. 10.07.2023 / Г. Н. Игнатьев, Ф. Х. Насыров. – EDN ADONIW.

6. Кожухов, М. В. Разработка и исследование моделей радиационных воздействий для расчета характеристик кремниевых и кремний-германиевых биполярных транзисторов с помощью системы TCAD : специальность 05.13.12 "Системы автоматизации проектирования (по отраслям)" : автореферат диссертации на соискание ученой степени кандидата технических наук / Кожухов Максим Владимирович. – Москва, 2023. – 22 с. – EDN ZQAWBF.

7. Кравцова, В. С. Управление рисками и неопределенностью: стохастические методы и моделирование методом Монте-Карло / В. С. Кравцова // Новые информационные технологии в научных исследованиях: : Материалы XXIX Всероссийской научно-технической конференции студентов, молодых ученых и специалистов, Рязань, 27–29 ноября 2024 года. – Рязань: Рязанский государственный радиотехнический университет им. В.Ф. Уткина, 2024. – С. 106-107. – EDN VWWJWR.

8. Харьков, В. П. Имитационное моделирование выборочного контроля методом статистических испытаний (метод Монте-Карло) / В. П. Харьков // Вестник Национального Института Бизнеса. – 2024. – № 34. – С. 294-300. – EDN IWBCKS.

УДК 72

ГЛАВА 7. ЛОГИСТИКА АВТОНОМНЫХ ЖИЛЫХ БЛОКОВ ДЛЯ СЕЛЬСКОХОЗЯЙСТВЕННЫХ ТЕРРИТОРИЙ ОМСКОЙ ОБЛАСТИ

Расторгуева Ксения Максимовна
студент, кафедры основ архитектуры,
Государственный Университет по Землеустройству,
РФ, г. Москва

Научный руководитель: Кошкин Андрей Корнилович
старший преподаватель кафедры строительства,
Государственный Университет по Землеустройству,
РФ, г. Москва

Аннотация: в данной главе в образовательных целых рассмотрены ключевые аспекты логистики автономных жилых блоков для сельскохозяйственных территорий Омской области. В условиях растущих потребностей в обеспечении комфортного и устойчивого жилья в удалённых районах, автономные жилые блоки представляют собой инновационное решение, способствующее улучшению качества жизни местных жителей. Особое внимание уделяется вопросам транспортировки, общим габаритам модульного блока, энергоэффективности и инфраструктуры, необходимым для успешной реализации таких проектов. Также описываются потенциальные преимущества модульного строительства и мобильных технологий в контексте аграрного сектора. Эта статья подчеркивает важность комплексного подхода к планированию и обеспечению ресурсами, что позволит создать эффективные и экологически чистые условия жизни в удалённых сельских территориях Омской области.
Ключевые слова: логистика; инновационное строительство; современные конструкции; Омск; автономные жилые блоки; транспортировка; инфраструктура; устойчивое развитие; энергоэффективность; мобильные технологии; обеспеченние ресурсами; экологичность; удобство; использование современных материалов и технологий; модульная система; развитие сельской местности.

LOGISTICS OF AUTONOMOUS RESIDENTIAL UNITS FOR AGRICULTURAL TERRITORIES OF THE OMSK REGION

Rastorgueva Ksenia Maksimovna

Scientific superviso: Koshkin Andrey Kornilovich

Annotation: In the article, the key aspects of logistics of autonomous residential blocks for remote agricultural territories of the city of Omsk are considered as part of the educational program. In the context of the growing demand for comfortable and sustainable housing in remote areas, autonomous residential units represent an innovative solution that contributes to improving the quality of

life of local residents. Special attention is paid to transportation issues, the overall dimensions of the modular unit, energy efficiency and infrastructure necessary for the successful implementation of such projects. The potential advantages of modular construction and mobile technologies in the context of the agricultural sector are also described. This article highlights the importance of an integrated approach to planning and resource provision, which will create efficient and environmentally friendly living conditions in remote rural areas of Omsk.
Keywords: logistics; innovative construction; modern structures; Omsk; autonomous residential blocks; transportation; infrastructure; sustainable development; energy efficiency; mobile technologies; provision of resources; environmental friendliness; convenience; use of modern materials and technologies; modular system; rural development.

Введение

В условиях современного мира, где требования к качеству жизни и уровню комфорта постоянно растут, важность доступного жилья для сельского населения становится особенно актуальной. В последние время наблюдается значительное внимание к вопросам устойчивого развития и оптимизации логистических процессов, особенно в контексте отдалённых и сельских территорий. В условиях глобализации и стремительного развития технологий, необходимость в эффективных логистических решениях становится всё более актуальной, особенно для таких регионов, как Омская область, где сельское население сталкивается с множеством проблем, связанных с доступом к высокому качеству жизни и уровню комфорта. В данной статье сосредоточимся на исследовании логистических решений для автономных жилых блоков, которые могут стать важным элементом в улучшении условий жизни на сельскохозяйственных территориях Омской области.

Введение в проблемы логистики в сельскохозяйственных территориях Омской области.

Актуальность данной темы обусловлена несколькими факторами: о-первых, в условиях изменения климата и глобальных экологических вызовов, устойчивое развитие сельских территорий становится приоритетом для многих стран, включая Россию. Во-вторых, необходимость в создании комфортных и доступных условий для жизни в отдалённых населённых пунктах требует внедрения инновационных решений, которые могут обеспечить не только жильё, но и интеграцию с современными сельскохозяйственными практиками. В-третьих, логистика автономных жилых блоков может стать ключевым фактором в обеспечении транспортной доступности и эффективного использования местных ресурсов, что, в свою очередь, будет способствовать развитию аграрного сектора и улучшению условий жизни населения. Логистика в сельских территориях, особенно в отдалённых районах, сталкивается с уникальными проблемами, которые требуют особого внимания и адаптации к специфическим условиям. Эти проблемы коренятся в особенности географического расположения, низкой плотности населения, недостаточной развитости транспортной и коммуникаци-

онной инфраструктуры, а также сезонности и изменчивости агроклиматических условий. Логистика автономных жилых блоков в сельских зонах Омска требует комплексного подхода к решению вопросов формирования и доставки необходимых ресурсов, обеспечения жизнедеятельности и контроля за движением товаров и услуг. [1, с. 2-4]

Недостаточная транспортная доступность является одной из наиболее значительных проблем. Это приводит к задержкам поставок и увеличению затрат на логистику. Потребность в надёжных маршрутах для доставки продуктов, материалов и оборудования создаёт особые вызовы для местных властей и предпринимателей. Специализация и целевая направленность грузоперевозок имеют важное значение, поскольку они требуются для обеспечения надежного потока ресурсов в автономные блоки. [3, с. 5-8]

Подводя итог, следует отметить, концепция автономных жилых блоков должна быть интегрирована в существующую модель логистики, что создаст эффективный механизм доставки товаров и услуг, обеспечивая устойчивое развитие сельских территорий Омска и создавая комфортные условия для жизни и работы населения.

Рис. 1. Диаграмма проектирования автономных жилых блоков

Проектирование автономных жилых блоков

Создание автономных жилых блоков в сельских территориях требует всестороннего подхода, учитывающего ряд факторов, определяющих как функциональность самих блоков, так и их взаимодействие с окружающей экологией и экономикой. Проектирование автономных жилых блоков начинается с анализа потребностей целевой аудитории и особенностей местности. Нельзя забывать о климатических условиях Омской области, которые могут существенно влиять на выбор конструктивных решений. (Рис.1)

К примеру, необходимо учесть температурные колебания, уровень осадков и ветровые нагрузки. Архитектурные решения должны основываться на принципах теплоизоляции и максимального использования солнечной энергии. Использование панорамных окон, расположенных на южной стороне, позволит лучше освещать внутреннее пространство и минимизировать потребность в искусственном освещении. [5.с. 5]

Включение систем автономного водоснабжения и очистки сточных вод также требует тщательного проектирования. Важно предусмотреть возможность переработки серой воды, например, для полива растений или технических нужд. Это обеспечит не только устойчивость блока, но и даст возможность организации небольшого местного сельского хозяйства на базе каждого блока, что в свою очередь увеличит его самодостаточность.

Рис.2. Примеры проектирования автономных жилых блоков и их внутреннего устройства

К тому же, проектирование электроснабжения должно быть нацелено на использование возобновляемых источников энергии, таких как солнечные панели или ветряные генераторы. Необходимо заранее рассчитать их мощность в зависимости от потребностей блока и уровня солнечной инсоляции в районе. Энергетическая эффективность становится критически важным фактором, так как она влияет на общие затраты на содержание блоков и улучшает привлекательность для потенциальных жителей.

Важно также учитывать аспекты мобильности и транспортного обеспечения. Проектирование должно включать элементы, способствующие легкой транспортировке этих блоков к местам назначения, а также опыт их установки на месте. Возможность быстрой сборки и разборки таких единиц поможет реагировать на изменения в требованиях населения и экономической ситуации в регионе.

Кроме того, следует обратить внимание на проектирование внутреннего пространства. Открытая планировка, многофункциональные зоны и использование многослойных материалов помогут создать адаптивные и комфортные условия жизни. Важно предусмотреть, чтобы планировка позволяла жильцам легко организовать свою повседневную деятельность, при этом сохраняя возможность приватности. (Рис.2)

Ландшафтное проектирование будет играть ключевую роль в интеграции жилых блоков в окружающую природу. Оно не только способствует эстетическому восприятию, но и создает условия для минимизации воздействия на экосистему. Использование местных растений в озеленении пригодится как для улучшения внешнего вида, так и для природной фильтрации воздуха и создания микроклимата.

Проектирование автономных жилых блоков также должно учитывать взаимодействие с прилегающей транспортной и логистической инфраструктурой. Построенные блоки должны быть расположены таким образом, чтобы обеспечивался естественный доступ к важным транспортным и торговым путям, что облегчает процесс поставки необходимых ресурсов. Проведение анализа маршрутной сети даст возможность оптимизировать логистические потоки и обеспечить устойчивое развитие как самого блока, так и окружающих территорий.[6.с. 6-10]

Использование местных ресурсов и материалов при проектировании блоков позволит сократить затраты и повысить устойчивость проекта. Например, использование древесины из местных лесов, камня, добываемого в окрестностях, и местных технологий строительства снизит углеродный след и создаст дополнительные рабочие места в регионе.

Кроме того, проект должен рассматривать возможность послепродажного обслуживания и модернизации автономных блоков. С учетом быстро меняющихся технологий, возможность обновления оборудования и систем позволит продлить срок службы блоков и сохранить их актуальность.

В итоге, проектирование автономных жилых блоков для сельского хозяйства на отдалённых территориях города Омска требует системного подхода, в котором учтены все аспекты — от климатических условий до культурных традиций населения. Только глубоко интегрированный и адаптированный к местным условиям проект способен обеспечить устойчивость и эффективность функционирования автономных жилых блоков, сделать их не только комфортным местом проживания, но и залогом развития всей сельской местности. [7. с. 3-8]

Энергоэффективность автономных жилых блоков

Функционирование автономных жилых блоков требует тщательного подхода к вопросам энергии. Энергоэффективность становится основополагающим фактором в проектировании таких конструкций, особенно в сельскохозяйственных территориях, где ограниченность ресурсов может создать дополнительные трудности. Стратегически продуманное использование энергии не только снижает эксплуатационные расходы, но и способствует устойчивости всей логистической системы.

Энергоэффективные технологии включают в себя использование эффективных систем отопления, вентиляции и кондиционирования воздуха, а также внедрение современных строительных материалов, значительно уменьшающих теплопотери. Так, например, применение теплоизоляционных материалов при строительстве автономных жилых блоков помогает сохранять тепло в холодный период, что, в свою очередь, обеспечивает комфортные условия проживания и позволяет снизить потребление энергии.

Солнечные панели и ветряные турбины становятся эффективными источниками возобновляемой энергии, что особенно актуально для отдалённых регионов, где доступ к централизованным сетям ограничен. Внедрение гибридных систем, объединяющих различные источники энергии, позволяет обеспечить автономность в долговременной перспективе. Оповещения и системы мониторинга могут уточнить объемы потребления, дополнительно оптимизируя расходы.

Энергопотребление можно сократить путём использования энергоэффективной бытовой техники и освещения.

Проектирование автономных жилых блоков с учётом климатических особенностей и местных ресурсов требует детального анализа. К примеру, рекомендуется учитывать направление ветра, уровень солнечной радиации и температурные колебания при размещении блоков на территории. Это сможет обеспечить максимальное использование доступных ресурсов при минимальных затратах.

Мониторинг и оценка эффективности существующих решений позволяют накапливать статистику, необходимую для дальнейшего проектирования и внедрения новых технологий. Данные о потреблении энергии и воздействия на окружающую среду становятся основой для проведения научных исследований и развития новых методологических подходов.

Сравнительный анализ передовых решений в области энергоэффективности автономных жилых блоков на других территориях может дать полезные рекомендации и помочь избежать ошибок. Изучение международного опыта, особенно в условиях схожем с Омском, может ускорить процесс адаптации технологий и практик.

Интеграция принципов энергоэффективности в проектирование автономных жилых блоков не только содействует комфортному проживанию, но и усиливает логику всей логистической инфраструктуры, делает её более устойчивой к внешним факторам. Это однозначно определяет будущее таких проектов и позволяет им эффективно функционировать в условиях удалённых сельских территорий.

Транспортная доступность для автономных жилых блоков

Транспортная доступность для достиавки автономных жилых блоков в сельскохозяйственных отдалённых территориях города Омска становится важным аспектом, который необходимо учитывать при разработке логистических решений. Эти автономные блоки призваны обеспечить комфортное проживание

и функционирование хозяйственной жизни в условиях, где традиционные коммуникации могут быть недостаточно развиты.[8. с. 5-8]

Для определения стоимости перевозки автономных жилых блоков в город Омск необходимо учитывать несколько факторов:

1. Расстояние: Чем дальше от места производства до Омска, тем выше стоимость перевозки.

2. Тип транспорта: Используемый транспорт (грузовик, поезд, фура и т.д.) влияет на стоимость.

3. Размер и вес блоков: Большие и тяжелые конструкции требуют специальных условий транспортировки, что увеличивает затраты.(4-5 тонн)

4. Загрузка и разгрузка: Дополнительные расходы могут возникнуть на этапе загрузки и разгрузки.

5. Страхование: Рекомендуется страховать груз, что также добавляет к общей стоимости.

6. Сезонные факторы: В зависимости от времени года стоимость может варьироваться из-за погодных условий и загруженности транспортных компаний.

Основным приоритетом является создание транспортной сети, которая обеспечит не только физический доступ к автономным жилым блокам, но и поддержку логистических операций по доставке необходимых ресурсов и самих блоков. В условиях Омской области, где климатические условия могут значительно ограничивать возможности транспортировки, важно грамотно подойти к выбору маршрутов и средств передвижения. Эффективная логистика поможет минимизировать затраты, в том числе временные, и гарантировать бесперебойное снабжение автономных жилых модулей.

Проблема транспортной доступности также затрагивает оптимизацию транспортных средств. Важно учитывать типы и характеристики автотранспорта, который будет использоваться для доставки необходимых материалов, продуктов питания и даже услуг на такие отдалённые территории. Использование многофункциональных транспортных средств, которые способны работать в сложных климатических условиях и на неасфальтированных дорогах, поможет существенно улучшить логистику.

Особое внимание следует уделить организации логистики на уровне местных сообществ. Часто именно местные жители могут играть важную роль в поддержании связи между автономными жилыми блоками и внешними поставками. Привлечение местного населения к процессам транспортировки товаров не только создаёт новые рабочие места, но и способствует увеличению финансовой устойчивости сообществ.

Учитывая состав населения отдалённых территорий, важно разработать логистические схемы, учитывающие возможное изменение потребностей. Например, в сезон сбора урожая объемы требуемых поставок могут значительно увеличиваться, что предполагает гибкие подходы к организации транспортировки. Такой подход позволит лучшим образом реагировать на изменения в спросе, адаптируя логистическую систему к необходимым условиям.

Проблема сезонности также актуальна в вопросах транспортной доступности. Зимой, когда дороги могут быть затруднены из-за снегопадов или обледенения, важно заранее предусмотреть альтернативные пути и способы доставки, включая использование ледовой дороги на реках или временные переправы. Летний сезон дает больше возможностей для транспортировки, но требует также продуманного подхода к использованию доступных водных путей и автомобильных дорожных артерий.

Ещё одной важной составляющей является взаимодействие с существующей дорожной сетью. Нужно учитывать состояние дорог, наличие мостов и переправ, а также возможности для улучшения или ремонта инфраструктуры, что в конечном счёте повлияет на эффективность логистических операций. Это является не только вопросом целесообразности, но и безопасности перевозок.

Соблюдение всех этих аспектов будет способствовать не только эффективной транспортной доступности автономных жилых блоков, но и общей устойчивости и качеству жизни населения на отдалённых сельскохозяйственных территориях Омска. Успешная реализация предлагаемых логистических решений обеспечит необходимое взаимосвязи между внешним миром и автономными жилыми единицами.

Интеграция с существующей логистической инфраструктурой

На сельскохозяйственных удалённых территориях, таких как Омская область, эффективная логистика автономных жилых блоков требует интеграции с существующей логистической инфраструктурой. Сложность данного процесса обусловлена множеством факторов, включая географические, экономические и социальные аспекты региона.

Первым шагом к интеграции является анализ текущей инфраструктуры. Важно определить, какие транспортные пути, дороги, и логистические центры уже существуют и насколько они могут поддерживать бесперебойное снабжение автономных жилых блоков. Местные дороги часто требуют модернизации или восстановительного обслуживания, что должно стать приоритетом в процессе интеграции. Необходимо создать карту, на которой будут обозначены мощные и слабые места существующей логистической сети, чтобы выработать стратегию их улучшения. Например, обращение к опытам других регионов с подобными климатическими условиями, может предоставить полезные решения по улучшению дорожной сети.

Следующим важным аспектом является взаимодействие с местными сельскохозяйственными производителями. Поскольку автономные жилые блоки предназначены для поддержки удалённых территорий, важно наладить связь с фермерами и агрокомпаниями. Синергия между жилыми блоками и производственными хозяйствами создаст взаимовыгодные условия, где сельскохозяйственные производители смогут поставлять свои продукты непосредственно в новосозданные автономные поселения. Это сократит время транспортировки и обеспечит стабильность поставок, что крайне важно для жизнеобеспечения.

Не менее значимой является интеграция с системой распределения и логи-

стики, которая включает в себя склады, торговые точки и пункты обслуживания. Ближайшие населённые пункты и городские центры могут служить промежуточными пунктами на пути к автономным блокам. Создание малой инфраструктуры в таких местах, как временные склады, позволит анализировать поток грузов и минимизировать затраты на транспортировку. Это существенно повлияет на стоимость конечного продукта для жителей таких блоков.

Необходимо учесть, что логистика автономных жилых блоков также требует внимательного планирования маршрутов поставок. Использование современных технологий, таких как GPS-навигаторы, программное обеспечение для оптимизации маршрутов, может помочь снизить затраты и повысить оперативность. Кроме того, особое внимание стоит уделить логистическим платформам, которые могут централизовать данные о грузах и обеспечивать более плавную интеграцию между различными участниками цепочки поставок.

Климатические условия Омской области требуют особого подхода, выделяя необходимость в учёте сезонных факторов при организации поставок. В зимний период, например, существует риск блокировки дорог из-за снега, что может вызвать задержки в поставках. Это требует разработки резервных логистических маршрутов и альтернативных способов доставки, возможно, даже с использованием специализированного транспорта, способного справляться с неблагоприятными условиями.

Человеческий ресурс — ключевая составляющая успешного функционирования любой логистической системы. Обучение местного населения, включение его в процесс организации логистики, создание рабочих мест в сфере логистики, а также адекватная мотивация – важные аспекты, позволяющие наладить не только функциональную, но и устойчивую логистическую систему.

Значение информатизации процессов, связанных с логистикой автономных жилых блоков, невозможно переоценить. Внедрение цифровых технологий обеспечит прозрачность и более высокую степень контроля на всех этапах. Использование программного обеспечения для управления цепочками поставок не только оптимизирует затраты, но и позволит в реальном времени отслеживать статус поставок, реагируя на возможные риски.

Таким образом, интеграция с существующей логистической инфраструктурой для автономных жилых блоков в сельскохозяйственных отдалённых территориях требует продуманных подходов и многостороннего взаимодействия. Способность адаптироваться к местным условиям, эффективно использовать имеющиеся ресурсы и вовлекать в процессы местных жителей станет основой для успешного функционирования данной модели.

Использование местных ресурсов для достижения устойчивости

Разработка автономных жилых блоков для сельскохозяйственных отдалённых территорий Омска требует комплексного подхода к использованию местных ресурсов, что в свою очередь способствует повышению устойчивости таких систем. Основное внимание следует обратить на ресурсы, доступные в данной местности, включая материалы, энергию и рабочую силу.

Местные строительные материалы представляют собой один из важнейших факторов в процессе проектирования жилых блоков. В Омской области возможно применение таких ресурсов, как дерево, глина и различные виды камня, которые не только легко доступны, но и имеют хорошие эксплуатационные характеристики. Использование местного сырья позволяет снижать затраты на транспортировку, а также минимизировать углеродный след, связанный с логистикой. При этом необходимо учитывать свойства различных местных материалов, их устойчивость к климатическим условиям региона, а также возможности для их переработки и повторного использования.

Обращая внимание на энергию, необходимо изучать возможности использования возобновляемых источников энергии. Солнечные панели, ветряные установки, а также биомасса могут быть использованы для обеспечения автономных жилых блоков. Важно, что такая энергетическая система не только покрывает потребности жильцов, но и развивает местную экономику: производство и установка оборудования могут быть выполнены местными специалистами, а значит, создаются новые рабочие места.

Рабочая сила играет ключевую роль в создании устойчивой экосистемы. Обучение и привлечение местных жителей к процессам строительства, эксплуатации и обслуживания автономных жилых блоков способствует формированию квалифицированных кадров. Это может включать как обучение сетевым профессиям, так и занятия по экологии и устойчивому развитию. Важно создать систему взаимовыгодного сотрудничества, когда местные жители получают квалификацию и подобные навыки, а автономные жилые блоки обеспечивают им рабочие места.

Ведущая задача разработки логистики автономных жилых блоков — это интеграция местных ресурсов в существующую инфраструктуру. Например, создание сети доставки как для строительных материалов, так и для продовольствия требует продуманного подхода. Разработка логистических маршрутов для местных фермеров, что позволит им значительно сократить затраты на доставки своей продукции, будет способствовать развитию экономики региона и повсеместному устойчивому развитию. Создание эффективной логистической сети может также включать элементы кооперации, когда фермеры объединяются для совместной доставки и переработки своей продукции.

Секрет успешной логистики автономных жилых блоков также заключается в использовании местного опыта и традиций, что позволяет на практике внедрять инновационные решения, проверенные временем. Это может включать адаптацию старинных методов хранения и переработки сельскохозяйственной продукции, а также организации поставок.

Также важным является подход к совместному использованию ресурсов. Это может включать совместное использование транспортных средств, производственных мощностей и оборудования. Например, создание кооперативов, где жители могут совместно использовать тракторы или оборудование для переработки, позволяет снизить нагрузку на индивидуальные хозяйства и повы-

сить экономическую устойчивость. Подобные инициативы способствуют укреплению социальной сплоченности и формированию сообщества, что является важным для успешного функционирования автономных жилых блоков.

Перспективы развития концепции автономных жилых блоков

Ожидаемые тенденции в развитии автономных жилых блоков для сельскохозяйственных отдаленных территорий города Омска требуют анализа множества факторов, среди которых особое место занимают инновационные технологии, новая нормативно-правовая база, а также изменяющиеся требования самих пользователей. В первую очередь, можно выделить тенденцию к увеличению числа автономных жилых комплексов вследствие повышения интереса к экологии и устойчивому развитию. С учетом глобальных изменений климата и нарастающей урбанизации, автономные жилые решения становятся не просто привлекательными, а необходимыми для обеспечения комфортного проживания в отдаленных местностях.

Инновационные технологии в области строительства, такие как модульные и 3D-печатные конструкции, открывают новые горизонты для создания быстро возводимых и поистине автономных жилых блоков. Такие подходы позволяют значительно сократить время строительства, минимизировать затраты и снизить негативное воздействие на окружающую среду. В частности, использование новейших материалов способствует созданию устойчивых конструкций, которые могут адаптироваться к различным климатическим условиям региона Омска. [9.с. 6-9]

Современное проектирование автономных жилых блоков включает интеграцию "умных" технологий, таких как автоматизация управления энергопотреблением и использование систем мониторинга для управления ресурсами. Это позволяет обеспечить комфортное проживание пользователей, а также сократить издержки на услуги жизнеобеспечения.

Использование местных ресурсов - еще один важный аспект, способствующий процветанию автономных жилых блоков. Разработка стратегий, направленных на повышение ресурсов в рамках региона, позволит не только сократить затраты на перевозку, но и поддержать местное население через создание рабочих мест.

Перспективы автономных жилых блоков в Омске не ограничиваются лишь жилыми вопросами. Это также возможность изменить подход к жизни в сельской местности, преобразовав урбанистические, экологические, социальные и экономические вопросы. Данный сектор может стать драйвером изменений в других областях, включая культуру, образование и технологическое развитие, создавая тем самым новые горизонты для будущих поколений.

Заключение

В заключение данной работы можно подвести итоги и выделить ключевые аспекты, которые были рассмотрены в контексте логистики автономных жилых блоков для сельскохозяйственных территорий Омской области. В ходе исследо-

вания было выявлено, что логистика в сельских территориях сталкивается с множеством проблем, включая недостаточную транспортную доступность, ограниченные ресурсы и отсутствие современных технологий, что в свою очередь затрудняет развитие аграрного сектора и улучшение качества жизни населения.

Таким образом, можно сделать вывод, что логистика автономных жилых блоков для сельскохозяйственных отдалённых территорий Омской области представляет собой многофункциональную и многоуровневую задачу, требующую комплексного подхода и взаимодействия различных заинтересованных сторон. Успешная реализация данной концепции может не только улучшить условия жизни населения, но и способствовать развитию аграрного сектора, что в конечном итоге приведёт к устойчивому развитию региона в целом. Важно продолжать исследовать и развивать эту тему, привлекая внимание как научного сообщества, так и практиков, чтобы находить новые решения и подходы к решению существующих проблем.

Список источников

1. Сидоров А.П. Логистика в сельском хозяйстве: современные аспекты // Журнал сельскохозяйственной науки. – 2022. – № 3. – С. 10–16. 2.
2. Иванов Н.С. Организация транспортных грузоперевозок для отдалённых территорий Омской области // Транспорт и логистика. – 2021. – № 2. – С. 28–34. 3.
3. Петрова Е.Ю. Автономные жилые блоки: новые технологии для устойчивого развития // Вестник архитектуры и строительства. – 2023. – № 4. – С. 45–52. 4.
4. Кузнецов В.П. Энергетическая автономия для сельских территорий: возможности и перспективы // Энергетика и ресурсы. – 2022. – Т. 10, № 1. – С. 12–20. 5
5. Синянский, И.А. Типология зданий и сооружений: учеб. пособие для учреждений сред. проф. образования / И.А. Синянский, Н.И. Манешина – 6-е изд., стер. – М. : Издательский центр «Академия», 2013. – 144 с
6. Пименова Н.Д., Мошкова А.И., Давиденко А.А., Кошкин А.К. Модуль жилого назначения из объемных самодостаточных блоков (для Сибири и Дальнего Востока). Новые идеи нового века: материалы международной научной конференции ФАД ТОГУ. 2024. Т. 2. С. 219-223.
7. Синянский И.А., Кошкин А.К., Леоненко И.А., Шныренков Е.А. Анализ и предложения по объемно-планировочным и конструктивным решениям круглых в плане сельскохозяйственных зданий. Системные технологии. 2024. № 4 (53). С. 57-63.
8. Назаров Я.Д., Кобалян А.А., Старосотская С.П., Кошкин А.К. Транспортные проблемы красногорска и их решение // Интернаука. 2024. № 41-1 (358). С. 19-24.
9.Богоявленов В.В., Аброськина О.С., Расторгуева К.М. Проектирование комбината по производству автономных жилых блоков для сельского населения в Чебоксарах. Студенческий. 2024. № 38-1 (292). С. 5-12.

РАЗДЕЛ II. АКТУАЛЬНЫЕ ВОПРОСЫ КИБИРБЕЗОПАСНОСТИ

УДК 62

ГЛАВА 8. АКТУАЛЬНЫЕ ТЕНДЕНЦИИ КИБЕРБЕЗОПАСНОСТИ

Аменицкий Алексей Владимирович
аспирант
Санкт-Петербургский государственный электротехнический университет ЛЭТИ имени В.И. Ульянова (Ленина)

Научный руководитель: Воробьёв Евгений Германович
д.т.н., профессор
Санкт-Петербургский государственный электротехнический университет ЛЭТИ имени В.И. Ульянова (Ленина)

Аннотация: Заглядывая в будущее, мы понимаем одну вещь: цифровая среда быстро развивается, и это создаёт новые проблемы в сфере кибербезопасности для компаний по всему миру. От растущей скорости, масштабов и сложности кибератак до изменений в том, как мы работаем и общаемся, — будущее сетевой безопасности зависит от комплексного подхода, объединяющего передовые технологии искусственного интеллекта и удобство для пользователей.

На самом деле, прогнозы по кибербезопасности и искусственному интеллекту показывают, что мы находимся на переломном этапе в развитии методов обеспечения безопасности на предприятиях. Один из самых ярких прогнозов заключается в том, что предприятия повсеместно перейдут на защищённые браузеры. Эта тенденция не только неизбежна, но и необходима. Хотя в следующем году использование защищённых браузеров значительно возрастёт, они представляют собой лишь часть головоломки.

Со временем ситуация в сфере кибербезопасности будет усложняться, а новые проблемы будут возникать так же быстро, как и технологии, которые их создают. От вредоносных программ с искусственным интеллектом (ИИ) до надвигающихся угроз, связанных с квантовыми вычислениями. Рассмотрим ключевые тенденции, к которым организациям необходимо подготовиться, чтобы оставаться в безопасности в этой развивающейся цифровой среде.

Ключевые слова: Cyber Security (CS), CS architecture, CS framework, CS trends, CS tendences, CS tools, CS crimes, CS latest news, CS releases, CS game-changers, CS future, CS playbook, CS agenda, CS future, CS risks, CS incidents, CS resilience, Hackers, PenTest, CS прогноз, CS Landscape, Artificial Intelligence, Deep Fakes, OWASP, Website security, CryptoScams, Crypro-Jacking, CryptoFraud, NFT scams, Antifraud, Dark Web, Deep Web, Shadow Web, Dark Net, Hacking AI, CSPM, DSPM, Эволюция киберУгроз, КиберГигиена.

CURRENT CYBERSECURITY TRENDS

Amenitsky Alexey Vladimirovich

Scientific supervisor: Vorobyov Evgeny Germanovich

В то время как злоумышленники продолжают использовать многие «классические» тактики, которые существуют уже несколько десятилетий, наши про-

гнозы на предстоящий год в основном сосредоточены на том, что киберпреступники будут проводить более масштабные, дерзкие и, с их точки зрения, более эффективные атаки. От групп, предоставляющих услуги киберпреступности (CaaS), которые становятся всё более специализированными, до злоумышленников, использующих сложные сценарии, сочетающие цифровые и физические угрозы, — киберпреступники повышают ставки, чтобы проводить более целенаправленные и опасные атаки.

Рассмотрим проверенные временем атаки, на которые продолжают полагаться киберпреступники, и то, как они эволюционировали, делится новыми тенденциями в сфере угроз, на которые стоит обратить внимание в этом году и в дальнейшем, а также предлагает советы о том, как организации по всему миру могут повысить свою устойчивость перед лицом меняющегося ландшафта угроз.

Основываясь на тенденциях, которые мы уже наблюдаем сегодня, попробуем сформировать реалистичное представление о том, с чем организации могут столкнуться в обозримом будущем- множество тем, связанных с кибербезопасностью, с акцентом на различные угрозы, такие как:

- Злоумышленники используют искусственный интеллект (ИИ): субъекты угроз будут все чаще использовать ИИ для сложных фишинговых, вишинговых и социальных атак. Они также будут использовать дипфейки для кражи личных данных, мошенничества и обхода мер безопасности.
- ИИ для информационных операций (IO): участники IO будут использовать ИИ для масштабирования создания контента, создания более убедительного контента и улучшения ненастоящих персонажей.
- Большая четвёрка будет продолжать действовать, участвуя в шпионских операциях, киберпреступлениях и информационных операциях, соответствующих их геополитическим интересам.
- Программы-вымогатели и многоаспектное вымогательство: Программы-вымогатели и многоаспектное вымогательство останутся наиболее разрушительной формой киберпреступности, затрагивающей различные отрасли и страны.
- Вредоносное ПО Infostealer: Вредоносное ПО Infostealer продолжит представлять серьёзную угрозу, приводя к утечке данных и взлому учётных записей.
- Демократизация кибервозможностей: расширение доступа к инструментам и сервисам снизит барьеры для входа менее квалифицированных участников.
- Компрометация идентификационных данных: Компрометация идентификационных данных в гибридных средах будет представлять значительный риск.
- Web3 и криптовалютные кражи: организации, работающие с Web3 и криптовалютами, будут все чаще подвергаться атакам злоумышленников, стремящихся похитить цифровые активы.

- Более быстрое использование уязвимостей и большее количество целевых поставщиков: время, необходимое для использования уязвимостей, будет сокращаться, а круг целевых поставщиков будет расширяться.

Прогнозы в области кибербезопасности предполагают рост числа атак с использованием ИИ, квантовых угроз и эксплуатации социальных сетей

Будущее программ-вымогателей

Программы-вымогатели станут ещё более изощрёнными, а киберпреступники будут использовать искусственный интеллект и автоматизацию для повышения скорости и точности своих атак. Эти усовершенствованные методы позволят программам-вымогателям быстро распространяться по сетям, что сделает раннее обнаружение более важным, чем когда-либо. Рост числа программ-вымогателей, нацеленных на цепочки поставок, вызывает особую обеспокоенность, поскольку атаки на критически важных поставщиков или партнёров могут иметь каскадный эффект для целых отраслей. Ожидается, что в ближайшие годы в отрасли произойдёт два или три крупномасштабных инцидента с программами-вымогателями, нацеленными на цепочки поставок, что ещё больше усилит необходимость в защите расширенных сетей организаций.

В ответ на это ожидается, что компании будут чаще обращаться к киберстрахованию, чтобы смягчить финансовые последствия таких атак, а правительства будут вводить более строгие нормативные требования. Соблюдение требований и отчётность станут обязательными, поскольку программы-вымогатели по-прежнему представляют собой главную угрозу. В то же время фишинг остаётся основным способом распространения программ-вымогателей, а электронные письма, созданные искусственным интеллектом, и дипфейки становятся всё более убедительными. Для предотвращения таких атак потребуются надёжные системы обучения и обнаружения фишинга, чтобы опережать развивающиеся тактики.

Ожидаются масштабные атаки на цепочки поставок. Организациям нужно будет подготовиться к более быстрым и целенаправленным атакам и уделять больше внимания соблюдению нормативных требований, киберстрахованию и предотвращению атак.

Атаки на базе искусственного интеллекта будут нарастать

Интеграция ИИ в кибератаки — одно из важнейших событий, которые происходят в настоящее время. ИИ уже сделал киберпреступную деятельность более масштабной и изощрённой, и ожидается, что его влияние усилится. Эти угрозы, усиленные ИИ, принимают различные формы: от фишинговых электронных писем с безупречной грамматикой и личными данными до высокоадаптивных вредоносных программ, которые могут обучаться и обходить системы обнаружения. В фишинговых атаках нового поколения будет использоваться способность ИИ обучаться на основе данных в реальном времени, адаптируясь в соответствии с меняющимися мерами безопасности, что ещё больше усложнит обнаружение.

Генеративный ИИ также позволит проводить операции в гораздо большем

масштабе. Например, киберпреступники могут использовать ИИ для одновременного проведения тысяч целенаправленных фишинговых атак, настраивая каждую из них для достижения максимального эффекта. Это позволяет даже небольшим преступным группировкам проводить крупномасштабные операции, не требуя продвинутых технических знаний, что приводит к демократизации киберпреступности.

Растущая роль ИИ в киберпреступности неоспорима. ИИ не только увеличит масштабы атак, но и повысит их сложность. Фишинговые атаки будет сложнее обнаруживать, поскольку ИИ постоянно учится и адаптируется.

Безудержное злоупотребление искусственным интеллектом приводит к увеличению числа утечек данных

По мере того, как ИИ становится всё более распространённым как в личной, так и в профессиональной сфере, растёт обеспокоенность по поводу ненадлежащего использования инструментов ИИ. Одним из самых серьёзных рисков в 2025 году станут утечки данных, вызванные непреднамеренной передачей сотрудниками конфиденциальной информации платформам ИИ, таким как ChatGPT или Google Gemini. Системы ИИ могут обрабатывать огромные объёмы данных, и когда эти данные передаются во внешние инструменты ИИ, риск раскрытия информации резко возрастает.

Например, сотрудники могут вводить конфиденциальные финансовые данные в инструмент ИИ для создания отчёта или анализа, не осознавая, что эти данные могут храниться и потенциально доступны для несанкционированного доступа. Организациям потребуется установить более строгий контроль за использованием инструментов ИИ в своих сетях, чтобы сбалансировать преимущества производительности, обеспечиваемой ИИ, с необходимостью строгой защиты конфиденциальности данных.

По мере того, как инструменты искусственного интеллекта, такие как ChatGPT и Google Gemini, становятся всё более интегрированными в бизнес-операции, риск случайного раскрытия данных стремительно растёт, что приводит к новым проблемам с конфиденциальностью данных. В 2025 году организациям необходимо будет оперативно внедрять строгий контроль и управление использованием ИИ, чтобы преимущества этих технологий не достигались за счёт конфиденциальности и безопасности данных

Вторые пилоты SOC, управляемые искусственным интеллектом

Распространение «со-пилотов» SOC на основе ИИ изменит подход к работе центров управления безопасностью (SOC). Эти помощники на основе ИИ помогут командам управлять огромным количеством данных с брандмауэров, системных журналов, отчётов об уязвимостях и данных об угрозах. С помощью ИИ-помощников SOC смогут более эффективно анализировать эти огромные объёмы данных, расставлять приоритеты для угроз и предлагать рекомендации по устранению.

Благодаря большему количеству инструментов на базе ИИ, интегрированных в информационные панели SOC, специалисты по безопасности могут авто-

матизировать критически важные задачи по поиску угроз, сократить количество ложных срабатываний и более эффективно реагировать на инциденты. Способность превращать необработанные данные в полезную информацию станет ключом к защите организаций от всё более изощрённых атак.

Вторые пилоты SOC на основе ИИ окажут значительное влияние, помогая командам по обеспечению безопасности расставлять приоритеты для угроз и превращать огромные объёмы данных в полезную информацию. Это изменит правила игры для эффективности SOC.

Квантовые вычисления: надвигающаяся угроза

Квантовые вычисления, хотя и находятся на ранней стадии развития, представляют собой серьёзную угрозу для традиционных методов шифрования. По мере развития квантовых технологий они могут взломать стандарты шифрования, которые в настоящее время считаются безопасными. Согласно прогнозам Check Point, квантово-устойчивая криптография начнёт набирать популярность в 2025 году, когда организации осознают угрозу, которую квантовые вычисления представляют для безопасности данных.

Этот риск особенно опасен для отраслей, которые полагаются на шифрование для защиты конфиденциальных данных, таких как финансы и здравоохранение. Традиционные методы шифрования, такие как RSA и DES, уязвимы для расшифровки на основе квантовых вычислений, которая может взламывать ключи шифрования экспоненциально быстрее, чем классические компьютеры. Хотя до практических квантовых атак ещё много лет, готовиться нужно уже сейчас. Эксперты рекомендуют организациям начать переход на постквантовую криптографию, которая устойчива к квантовому взлому.

Мы увидим первые ощутимые признаки влияния квантовых вычислений на кибербезопасность. Организации должны заблаговременно начать переход на методы шифрования, безопасные для квантовых вычислений, чтобы защитить свои конфиденциальные данные, пока не стало слишком поздно.

Социальные сети как площадка для совершения киберпреступлений

Платформы социальных сетей, насчитывающие миллиарды пользователей по всему миру, стали главной мишенью для киберпреступников. Сочетание социальных сетей и генеративного искусственного интеллекта (GenAI) позволит проводить ещё более изощрённые и опасные атаки, используя персональные данные и контент, созданный искусственным интеллектом, для разработки целенаправленных мошеннических схем, подделок и краж. Реальная угроза заключается не только в социальных сетях или GenAI по отдельности, но и в том, как эти две силы объединяются, усиливая риски. Преступники будут использовать ИИ, чтобы имитировать поведение, внешность и голос людей, что затруднит различение реальных и искусственных взаимодействий.

Преступники будут использовать платформы социальных сетей не только для кражи личной информации, но и для того, чтобы манипулировать пользователями и ставить под угрозу корпоративную безопасность. Эта угроза особенно опасна в профессиональных сетях, таких как LinkedIn, где пользователи ожи-

дают увидеть контент, связанный с бизнесом, и легитимные связи, что облегчает злоумышленникам проникновение в сеть. Выдача себя за другого человека в LinkedIn особенно опасна, поскольку киберпреступники могут создавать убедительные образы для взаимодействия с сотрудниками, руководителями или партнёрами, стирая границы между законным общением и мошенничеством.

Использование тактики социальной инженерии резко возрастёт, а ИИ будет играть ключевую роль в создании очень убедительных имитаций. На самом деле боты на основе ИИ и дипфейки, которые генерируют поддельные видео, аудио и чаты, уже используются для того, чтобы выдавать себя за известных личностей, например, глав государств. Вскоре не будет ничего удивительного в том, что вы окажетесь на видеозвонке в Zoom, думая, что разговариваете с коллегой или начальником, а потом поймёте, что это была подделка, созданная ИИ. Эти боты позволят киберпреступникам взаимодействовать с несколькими жертвами одновременно и обманывать их, запуская масштабные кампании социальной инженерии с беспрецедентным уровнем охвата и сложности.

Ожидается резкий рост числа киберпреступников, использующих социальные сети, в частности ИИ, для проведения целенаправленных атак с целью выдать себя за кого-то. Дипфейки уже влияют на политические процессы и распространятся на деловую среду. Хакеры будут не просто красть ваши данные или учётные данные, они будут нарушать финансовые транзакции, корпоративные решения и репутацию бренда. Чтобы оставаться на шаг впереди, поставщики и организации должны адаптировать инструменты безопасности в своих системах защиты, а также обучать своих сотрудников работе в новом мире «нулевого доверия» подозрительности ко всему.

Эпоха CISO, основанного на искусственном интеллекте

Роль директора по информационной безопасности (CISO) столкнётся с растущими трудностями, вызванными стремительным внедрением ИИ, гибридными облачными средами и усиливающимся давлением со стороны регулирующих органов. По мере того, как компании будут использовать ИИ для получения конкурентных преимуществ, перед директорами по информационной безопасности встанет задача найти баланс между скоростью внедрения инноваций и необходимостью обеспечения безопасности на этапе проектирования. Это противоречие может привести к росту числа утечек данных, связанных с ИИ, поскольку безопасность часто приносится в жертву ради скорости внедрения.

CISO также будут разъяснять советам директоров риски, связанные с искусственным интеллектом и новыми технологиями, поскольку этот переход требует от них овладения сложными технологиями, одновременно переводя эти риски в бизнес-термины для руководства. В то же время инфраструктуры гибридного облака станут более распространенными, что потребует от CISO расширения своих возможностей DevOps для управления безопасностью как в общедоступных, так и в частных облачных средах.

Потребность в страховании директоров и должностных лиц (D&O) будет расти по мере повышения их ответственности. Кроме того, такие инциденты,

как недавняя проблема с обновлением программного обеспечения CrowdStrike, приведут к росту спроса на киберстрахование, особенно в отношении перерывов в работе, вызванных сбоями сторонних систем. По мере насыщения рынка поставщиков киберуслуг директора по информационной безопасности будут всё чаще обращаться к консультационным услугам в сфере кибербезопасности для принятия решений советом директоров и инвестирования в безопасность.

CISO должны будут сбалансировать быстрое внедрение искусственного интеллекта с безопасностью, ориентируясь при этом на сложные гибридные облачные среды и растущее давление со стороны регулирующих органов. Задача будет заключаться в том, чтобы руководить с помощью инноваций, не ставя под угрозу защиту

Растущая эволюция роли CISO: Сближение с CIO

Роль CISO также продолжит развиваться и будет сближаться с CIO в ответ на усиление контроля со стороны регулирующих органов и личную подотчетность. Взяв на себя роль организаторов рисков, CISO должны выйти за рамки традиционной кибербезопасности и перейти к управлению более широкими корпоративными рисками, включая геополитические угрозы, дезинформацию, управляемую искусственным интеллектом, и изменения в регулировании. Современным ИТ-директорам необходимо будет контролировать все аспекты информационных технологий, включая информационную безопасность, что сделает роль CISO менее четкой и создаст более унифицированную структуру руководства, которая устранит границы между двумя ролями. Эта конвергенция отражает более широкий сдвиг в сторону комплексного управления рисками, при котором кибербезопасность становится основной обязанностью ИТ-руководства.

Объединение должностей ИТ-директора и директора по информационной безопасности определит следующую эру корпоративного управления. По мере того, как организации сталкиваются со всё более сложными киберугрозами, необходимость в едином подходе к управлению ИТ и безопасностью становится критически важной. К 2025 году мы увидим, как всё больше ИТ-директоров возьмут на себя ответственность за кибербезопасность, интегрировав её в процесс цифровой трансформации. Такой комплексный подход не только упростит процесс принятия решений, но и повысит общую устойчивость организации.

Эволюция облачной безопасности

Облачная безопасность в 2025 году столкнётся с растущими проблемами по мере того, как искусственный интеллект и облачные платформы будут всё больше интегрироваться в бизнес-операции. Поскольку злоумышленники используют искусственный интеллект для автоматизации взломов облачных систем, организациям придётся перейти от подхода, ориентированного на устранение последствий, к более превентивной стратегии. Скорость и сложность атак потребуют от компаний создания проактивных архитектур безопасности, способных обнаруживать и останавливать угрозы до того, как они нанесут ущерб.

Внедрение облачных технологий будет продолжаться, но вместе с этим усилится контроль со стороны регулирующих органов. Ожидается, что правительства будут предъявлять более строгие требования к соблюдению нормативных требований, особенно в отраслях, которые работают с конфиденциальными данными. Киберстрахование также будет приобретать всё большее значение, поскольку организации стремятся защититься от финансовых последствий утечек данных в облаке. Искусственный интеллект, хотя и играет ключевую роль в защите облачных технологий, также станет мишенью для злоумышленников, поэтому компаниям необходимо защищать свои системы на основе ИИ в рамках общей облачной стратегии.

Ключом к облачной безопасности становится предотвращение угроз. По мере того, как атаки становятся всё более автоматизированными и сложными, компаниям необходимо будет создавать облачные среды, которые будут предвосхищать угрозы, а не реагировать на них.

Облачные платформы безопасности

Продолжающаяся борьба между лучшими в своем роде и лучшими в своем классе решениями для кибербезопасности смещается в сторону платформ. Эффект платформы, в значительной степени обусловленный интеграцией на основе искусственного интеллекта, повысит производительность операций по обеспечению безопасности для всех, кроме самых укомплектованных штатами команд по кибербезопасности на предприятиях. Например, такие инструменты, как CNAPP, ASPM и DSPM, объединяются в комплексные наборы решений для управления состоянием безопасности (SPM).

По мере появления новых инструментов SPM, таких как SPM для приложений и данных, они, скорее всего, станут частью всеобъемлющей платформы защиты облачных приложений (CNAPP), а это пространство потенциально превратится в то, что можно назвать XSPM (расширенное управление состоянием безопасности). Объединение управления поверхностью атаки с этой новой категорией показывает, что платформы будут приносить больше пользы, чем набор точечных решений, и кардинально изменят подход организаций к управлению уязвимостями.

Облачные платформы становятся новым фундаментом кибербезопасности, где интеграция на основе ИИ превосходит отдельные инструменты. Объединяя различные операции по обеспечению безопасности, эти платформы упрощают работу и позволяют организациям более эффективно и рационально управлять угрозами и уязвимостями в облаке

Проблемы безопасности в облаке и IoT

По мере того, как всё больше организаций переходят в облако и внедряют устройства Интернета вещей (IoT), поверхность атаки продолжает расширяться. Более 90% предприятий будут работать в мультиоблачных средах, а количество устройств IoT, по прогнозам, превысит 32 миллиарда по всему миру. Хотя поставщики облачных услуг предлагают надёжные функции безопасности, сложность защиты нескольких облачных платформ создаёт уязвимости, особенно

при неправильном управлении конфигурациями или их слабом мониторинге.

Безопасность Интернета вещей станет серьёзной проблемой, поскольку злоумышленники будут использовать растущее число взаимосвязанных устройств. Многие устройства Интернета вещей, от систем «умный дом» до промышленных датчиков, не имеют надлежащих мер безопасности, что делает их привлекательными целями для киберпреступников. Развитие Интернета вещей неизбежно приведёт к необходимости в масштабируемом и безопасном облачном хранилище для эффективного управления большими объёмами данных, их обработки в реальном времени, централизованного управления, повышения безопасности и экономичной масштабируемости.

Кроме того, по-прежнему будут использоваться неправильные настройки в облаке и небезопасные API, поскольку они остаются одними из главных уязвимостей в облачных средах. С неизбежной интеграцией искусственного интеллекта и машинного обучения практически во все имеющиеся у нас технологии облачные вычисления также претерпят изменения, которые повысят уровень автоматизации и принятия решений. С развитием Интернета вещей и мультиоблачных сред мы увидим значительный рост числа уязвимостей. Обеспечение безопасности этих взаимосвязанных систем станет одной из важнейших задач

Вредоносное ПО, созданное искусственным интеллектом, и мультиагентные системы

Злоумышленники будут всё чаще использовать продвинутые инструменты для генерации кода на основе ИИ, переходя от инструментов для завершения кода, таких как GitHub Copilot, к платформам на основе ИИ, способным генерировать полноценный код вредоносного ПО по одному запросу. Этот переход позволит быстро создавать сложные и целенаправленные киберугрозы, значительно снизив порог вхождения для злоумышленников и сделав мир гораздо менее безопасным, поскольку эти инструменты станут более доступными, их будет сложнее обнаружить, и они будут развиваться быстрее, чем традиционные средства защиты смогут адаптироваться.

Также появятся многоагентные системы ИИ, в которых несколько моделей ИИ будут взаимодействовать для решения сложных задач. Злоумышленники будут использовать эти системы для проведения скоординированных распределённых атак, которые будет сложнее обнаружить и предотвратить. В то же время защитники будут использовать аналогичные системы для обнаружения угроз в реальном времени и реагирования на них в сетях и на устройствах.

Кроме того, появятся новые платформы управления ИИ, которые будут соответствовать нормативным требованиям, обеспечивая прозрачность, доверие и справедливость в моделях ИИ. Эти платформы станут необходимыми, поскольку нормативы в области ИИ уже вступают в силу, вынуждая предприятия сохранять контроль над своими инструментами и процессами ИИ.

ИИ будет использоваться как для атак, так и для защиты в беспрецедентных масштабах, а многоагентные системы позволят проводить более динамичные операции. Организации, которые на раннем этапе внедрят системы управ-

ления, будут лидировать в построении доверительных отношений и обеспечении соответствия требованиям

Киберпреступники готовы воспользоваться растущей нехваткой специалистов в области кибербезопасности

Растущая нехватка специалистов по кибербезопасности существенно повлияет на способность организаций защищаться от всё более сложных киберугроз. Несмотря на продолжающиеся инвестиции в растущее число продуктов для обеспечения безопасности, нехватка квалифицированных специалистов для управления и интеграции этих инструментов приведёт к фрагментации и неэффективности системы безопасности. Зависимость от слишком большого количества поставщиков без достаточного количества собственных специалистов сделает организации уязвимыми для атак, поскольку их защиту будет сложнее контролировать, и она станет менее эффективной. Киберпреступники будут использовать эти бреши, нацеливаясь на слабые места, созданные чрезмерно сложной системой безопасности, что сделает компании более уязвимыми для взломов и финансовых потерь.

Нехватка специалистов по кибербезопасности ставит организации в затруднительное положение. Несмотря на инвестиции в новые инструменты, их защита слишком слаба, что оставляет критические бреши, которыми охотно пользуются злоумышленники. Оптимизация операций по обеспечению безопасности и повышение квалификации сотрудников станут ключом к поддержанию устойчивости.

Растущие требования регулирующих органов и более строгие политики Киберстрахования

Организации будут сталкиваться с растущим давлением со стороны растущей волны правил кибербезопасности, включая Правила Интернета вещей ЕС, Правила раскрытия информации о кибербезопасности SEC, Закон о цифровой операционной устойчивости (DORA) и Директиву NIS2. Каждая из этих платформ потребует от компаний значительных затрат времени и ресурсов на проекты по обеспечению соответствия требованиям, разработку политики и развертывание новых продуктов безопасности. Хотя эти правила призваны усилить меры безопасности, они также усложняют операционную деятельность, вынуждая предприятия уделять больше внимания и усилий соблюдению этих стандартов. Кроме того, правила киберстрахования станут более строгими, и страховщики будут требовать более тщательного контроля и соблюдения требований в качестве обязательных условий для покрытия рисков, что ещё больше увеличит административную нагрузку.

По мере вступления в силу новых нормативных требований и ужесточения правил киберстрахования организации должны выделять значительное количество времени и ресурсов для выполнения этих меняющихся требований. Уделение внимания соблюдению требований повысит безопасность, но также увеличит операционную нагрузку, что делает необходимым для компаний оптимизировать усилия и уделять приоритетное внимание готовности к нормативным

требованиям.

Тенденции Кибератак

Тенденция 1: Использование искусственного интеллекта

Одной из определяющих особенностей 2023 года стал стремительный рост искусственного интеллекта (ИИ) в сфере кибербезопасности. ChatGPT был представлен широкой публике в последние месяцы 2023 года и считался революционным и уникальным. В течение нескольких месяцев появились сотни или тысячи новых инструментов и проектов, применяющих генеративный ИИ и большие языковые модели (LLM) для решения различных задач.

В сфере кибербезопасности генеративный ИИ имеет множество потенциальных применений. Эти инструменты уже используются для значительного повышения эффективности атак с использованием социальной инженерии и разработки новых вредоносных программ, в том числе похитителей данных, кейлоггеров и программ-вымогателей.

Хотя такие компании, как OpenAI, пытались внедрить средства защиты в свои инструменты, они добились лишь ограниченного успеха. Исследования показали, что эти ограничения можно легко обойти, что позволяет киберпреступникам использовать эти инструменты для увеличения масштабов и сложности своих атак.

Тенденция 2: Программы-вымогатели

Программы-вымогатели уже несколько лет являются основной угрозой кибербезопасности, и атаки с использованием программ-вымогателей становятся всё более изощрёнными, распространёнными и дорогостоящими для компаний.

Одной из основных причин его непрекращающегося успеха является постоянное развитие программ-вымогателей. Соперничество между группами разработчиков программ-вымогателей привело к тому, что программы-вымогатели шифруют данные быстрее, обходят защиту и нацелены на большее количество операционных систем. Программы-вымогатели также перешли от шифрования данных к их краже, лишая резервные копии возможности защитить от выплаты выкупа. Операторы программ-вымогателей также использовали различные методы для масштабирования своих атак. В 2023 году использование уязвимостей цепочек поставок и нулевого дня позволило группам CL0P и LockBit, занимающимся программами-вымогателями, проводить крупномасштабные одновременные атаки на множество компаний.

Тенденция 3: Хактивизм

Хактивисты совершают кибератаки с политическими мотивами. Хотя такие группы, как Anonymous, совершали подобные атаки на протяжении многих лет, в 2022 году и в первой половине 2023 года наблюдался резкий рост числа атак, связанных с государством.

В таких атаках обычно используются распределённые атаки типа «отказ в обслуживании» (DDoS), чтобы нарушить работу организаций, расположенных в определённом государстве. Например, российская группировка Killnet атако-

вала западные организации здравоохранения, а происламская группировка Anonymous Sudan атаковала Scandinavian Airlines, американские организации здравоохранения и Microsoft.

Тенденция 4 Мобильные угрозы

В последние годы использование мобильных устройств на рабочем месте значительно возросло. Эта тенденция обусловлена ростом популярности удалённой работы и политики принеси своё устройство (BYOD).

В результате киберпреступники сосредоточили свои усилия на взломе этих мобильных устройств, и количество и качество мобильных вредоносных программ резко возросло. Недавние кампании по распространению мобильных вредоносных программ, такие как FluHorse, нацелены на коды двухфакторной аутентификации (2FA) на мобильных устройствах, а FakeCalls генерирует мошеннические голосовые вызовы, выдавая себя за финансовые приложения. Кампания Triangulation подчёркивает изменения в сфере безопасности iOS, поскольку киберпреступники используют уязвимости нулевого уровня в устройствах, которые, как считалось ранее, были гораздо более безопасными, чем их аналоги на Android.

Уязвимость Apache Log4j

9 декабря 2021 года (CVE-2021-44228) было сообщено о серьёзной уязвимости удалённого выполнения кода (RCE) в пакете ведения журналов Apache Log4j 2 версий 2.14.1 и ниже. Apache Log4j — самый популярный пакет ведения журналов Java, который скачали более 400 000 раз из его репозитория на GitHub. Он используется большим количеством предприятий по всему миру и позволяет пользователям входить в различные популярные приложения. Эту уязвимость легко использовать, что позволяет злоумышленникам брать под контроль веб-серверы на базе Java и выполнять атаки с удалённым выполнением кода.

Атака Sunburst

Сейчас мир столкнулся с тем, что, по-видимому, является кибератакой 5-го поколения — сложной многовекторной атакой с явными признаками киберпандемии. Исследователи назвали её Sunburst, и мы считаем, что это одна из самых сложных и серьёзных атак, которые когда-либо происходили. Сообщается, что атака затронула крупные правительственные учреждения США, а также многие организации частного сектора.

Эта серия атак стала возможной благодаря тому, что хакеры смогли внедрить бэкдор в обновления программного обеспечения SolarWinds. Более 18 000 компаний и государственных учреждений загрузили на свои компьютеры то, что казалось обычным обновлением программного обеспечения, но на самом деле было троянской программой. Используя распространённую в ИТ-сфере практику обновления программного обеспечения, злоумышленники использовали бэкдор для компрометации активов организации, что позволило им шпионить за организацией и получать доступ к её данным. Для получения дополнительной информации посетите наш центр по расследованию атак Sunburst.

Атаки программ-вымогателей

Число случаев заражения программами-вымогателями растёт. Жертвами становятся небольшие местные и государственные учреждения, в основном в юго-восточной части США. Цифровая трансформация разрушает традиционные сетевые периметры с внедрением облачных вычислений, облачных сервисов и повсеместным распространением мобильных устройств. Такое расширение векторов атак означает появление новых способов атаковать организацию.

В третьем квартале 2024 года был зафиксирован рост числа атак с использованием программ-вымогателей в среднем на 50% по сравнению с первой половиной года. Организации по всему миру подверглись массированной волне атак с использованием программ-вымогателей, при этом наиболее уязвимой отраслью стала здравоохранение. По мере того как эти атаки становятся всё более частыми и интенсивными, их влияние на бизнес растёт в геометрической прогрессии. Наиболее распространёнными программами-вымогателями стали Maze и Ryuk

Типы кибератак

Киберугрозы пятого и шестого поколений стали реальностью для бизнеса. Киберпреступники знают о последних достижениях в области кибербезопасности компаний и адаптируют свои атаки, чтобы обойти традиционные средства защиты и победить их. Чтобы избежать обнаружения, современные кибератаки носят многовекторный характер и используют полиморфный код. В результате выявлять угрозы и реагировать на них сложнее, чем когда-либо.

Основной целью киберпреступников и первой линией защиты организации в мире удалённой работы является конечная точка. Для обеспечения безопасности удалённых сотрудников необходимо понимать наиболее распространённые киберугрозы, с которыми сталкиваются сотрудники, а также решения для обеспечения безопасности конечных точек, способные обнаруживать, предотвращать и устранять эти угрозы.

Кибератаки могут принимать различные формы. Киберпреступники используют множество различных методов для проведения кибератак, фишинговых атак, использования скомпрометированных учётных данных и многого другого. Получив первоначальный доступ, киберпреступники могут преследовать различные цели, включая заражение вредоносным ПО, программы-вымогатели, атаки типа «отказ в обслуживании», кражу данных и многое другое.

Кибератака — это любое преднамеренное действие, направленное на кражу, раскрытие, изменение, отключение или уничтожение данных, приложений или других ресурсов посредством несанкционированного доступа к сети, компьютерной системе или цифровому устройству.

Злоумышленники начинают кибератаки по разным причинам, от мелких краж до военных действий. Они используют различные тактики, такие как атаки с использованием вредоносного ПО, социальную инженерию, мошенничество и кражу паролей, чтобы получить несанкционированный доступ к целевым системам.

Кибератаки могут нарушить работу, нанести ущерб и даже уничтожить бизнес. Средняя стоимость утечки данных составляет 4,88 миллиона долларов США. Эта сумма включает в себя затраты на обнаружение нарушения и реагирование на него, простои и упущенную выгоду, а также долгосрочный репутационный ущерб для бизнеса и его бренда.

Но некоторые кибератаки могут быть значительно более дорогостоящими, чем другие. За атаки с использованием программ-вымогателей требовали выкуп в размере 40 миллионов долларов США. Мошенничество с использованием деловой электронной почты (BEC) привело к краже 47 миллионов долларов США у жертв за одну атаку. Кибератаки, ставящие под угрозу персональные данные клиентов (PII), могут привести к потере доверия клиентов, штрафам со стороны регулирующих органов и даже судебным искам. По некоторым оценкам, к 2025 году киберпреступность будет стоить мировой экономике 10,5 триллионов долларов в год.

Почему происходят кибератаки?

Мотивы, стоящие за кибератаками, могут быть разными, но есть три основные категории:

1. Преступник
2. Политический
3. Личный

Преступники, преследующие корыстные цели, стремятся к финансовой выгоде за счёт кражи денег, кражи данных или нарушения работы бизнеса. Киберпреступники могут взломать банковский счёт, чтобы напрямую украсть деньги, или использовать методы социальной инженерии, чтобы обманом заставить людей отправлять им деньги. Хакеры могут украсть данные и использовать их для кражи личных данных, продать их в даркнете или потребовать за них выкуп.

Вымогательство — ещё одна используемая тактика. Хакеры могут использовать программы-вымогатели, DDoS-атаки или другие методы, чтобы удерживать данные или устройства в заложниках до тех пор, пока компания не заплатит. Однако, согласно последнему индексу угроз X-Force, 32% киберинцидентов связаны с кражей и продажей данных, а не с их шифрованием с целью вымогательства.

Лично мотивированные злоумышленники, такие как недовольные нынешние или бывшие сотрудники, в первую очередь стремятся отомстить за какое-то мнимое оскорбление. Они могут забрать деньги, украсть конфиденциальные данные или нарушить работу систем компании.

Политически мотивированные злоумышленники часто связаны с кибервойнами, кибертерроризмом или «хактивизмом». В кибервойнах государства часто нацеливаются на правительственные учреждения своих противников или критически важную инфраструктуру. Например, с начала российско-украинской войны в обеих странах произошла волна кибератак на жизненно важные учреждения. Хакеры-активисты, которых называют «хактивистами»,

могут не наносить серьёзного ущерба своим целям. Вместо этого они обычно привлекают внимание к своим проблемам, делая свои нападки достоянием общественности.

К менее распространённым мотивам кибератак относятся корпоративный шпионаж, при котором хакеры крадут интеллектуальную собственность, чтобы получить нечестное преимущество перед конкурентами, а также хакеры-самооборонщики, которые используют уязвимости системы, чтобы предупредить о них других. Некоторые хакеры взламывают системы ради развлечения, наслаждаясь интеллектуальным вызовом.

Кто стоит за кибератаками?

Кибератаки могут инициировать преступные организации, государственные структуры и частные лица. Один из способов классификации субъектов угроз — разделение их на внешние и внутренние угрозы.

Внешние угрозы не имеют права использовать сеть или устройство, но всё равно проникают в них. К внешним источникам киберугроз относятся организованные преступные группировки, профессиональные хакеры, государственные структуры, хакеры-любители и хактивисты.

Внутренние угрозы — это пользователи, которые имеют авторизованный и законный доступ к активам компании и намеренно или случайно злоупотребляют своими привилегиями. В эту категорию входят сотрудники, деловые партнёры, клиенты, подрядчики и поставщики с доступом к системе.

Хотя небрежные пользователи могут подвергать свои компании риску, кибератака происходит только в том случае, если пользователь намеренно использует свои привилегии для осуществления вредоносных действий. Сотрудник, который неосторожно хранит конфиденциальную информацию на незащищённом диске, не совершает кибератаку, но недовольный сотрудник, который сознательно делает копии конфиденциальных данных для личной выгоды, совершает.

На что нацелены кибератаки?

Злоумышленники обычно взламывают компьютерные сети, потому что им нужно что-то конкретное. К распространённым целям относятся:

- Деньги
- Финансовые данные предприятий
- Списки клиентов
- Данные о клиентах, включая информацию, позволяющую установить личность (PII), или другие конфиденциальные персональные данные
- Адреса электронной почты и учетные данные для входа в систему
- Интеллектуальная собственность, такая как коммерческая тайна или дизайн продукции

В некоторых случаях киберпреступники вообще не хотят ничего красть. Вместо этого они просто хотят нарушить работу информационных систем или ИТ-инфраструктуры, чтобы нанести ущерб бизнесу, государственному учреждению или другой цели.

Какие последствия кибератаки оказывают на бизнес?

В случае успеха кибератаки могут нанести ущерб предприятиям. Они могут привести к простою, потере данных и денежных средств. Например:

- Хакеры могут использовать вредоносное ПО или атаки типа «отказ в обслуживании», чтобы вызвать сбой системы или сервера. Такое время простоя может привести к серьёзным перебоям в работе сервисов и финансовым потерям. Согласно отчёту «Стоимость утечки данных» , средняя утечка данных приводит к потере 2,8 миллиона долларов США.
- Атаки с использованием SQL-инъекций позволяют хакерам изменять, удалять или красть данные из системы.
- Фишинговые атаки позволяют хакерам обманом заставить людей отправить им деньги или конфиденциальную информацию.
- Атаки с использованием программ-вымогателей могут вывести систему из строя до тех пор, пока компания не заплатит злоумышленнику выкуп. Согласно одному отчёту, средняя сумма выкупа составляет 812 360 долларов США.

Помимо прямого ущерба для жертвы, кибератаки могут повлечь за собой множество вторичных издержек и последствий, связанных с обнаружением нарушений, реагированием на них и устранением последствий. Однако организации, которые применяли искусственный интеллект и автоматизацию для предотвращения нарушений безопасности, добились наибольшего эффекта в сокращении затрат на устранение последствий нарушений, сэкономив в среднем 2,22 миллиона долларов США по сравнению с организациями, которые не использовали эти технологии.

Кибератаки могут иметь последствия не только для непосредственных жертв. В 2021 году группировка DarkSide, занимающаяся программами-вымогателями, атаковала Colonial Pipeline, крупнейшую систему нефтепроводов в США. Злоумышленники проникли в сеть компании, используя взломанный пароль. Они перекрыли трубопровод, по которому на Восточное побережье США поступает 45% газа, дизельного топлива и авиационного керосина, что привело к повсеместной нехватке топлива.

Киберпреступники потребовали выкуп в размере почти 5 миллионов долларов США в криптовалюте биткоин, который Colonial Pipeline выплатила. Однако с помощью правительства США компания в итоге вернула 2,3 миллиона долларов из суммы выкупа.

Наиболее распространенные типы кибератак

Киберпреступники используют множество сложных инструментов и методов для проведения кибератак на корпоративные ИТ-системы, персональные компьютеры и другие цели. К наиболее распространённым типам кибератак относятся:

- Вредоносное ПО

Вредоносное ПО — это вредоносное программное обеспечение, которое

может вывести из строя заражённые системы. Вредоносное ПО может уничтожать данные, красть информацию или даже удалять файлы, критически важные для работы операционной системы. Вредоносное ПО существует во многих формах, в том числе:

- Троянские кони маскируются под полезные программы или прячутся в легальном программном обеспечении, чтобы обманом заставить пользователей установить их. Троян удаленного доступа (RAT) создает секретный лазейку на устройстве жертвы, а троян-дроппер устанавливает дополнительное вредоносное ПО, как только получает доступ.
- Программы-вымогатели — это сложные вредоносные программы, которые используют надёжное шифрование для удержания данных или систем в заложниках. Затем киберпреступники требуют выкуп в обмен на разблокировку системы и восстановление её работоспособности. Согласно индексу угроз X-Force от IBM, программы-вымогатели являются вторым по распространённости типом кибератак, на которые приходится 17% атак.
- Устрашающие программы используют поддельные сообщения, чтобы напугать жертв и заставить их загрузить вредоносное ПО или передать конфиденциальную информацию мошенникам.
- Шпионское ПО — это тип вредоносного ПО, которое тайно собирает конфиденциальную информацию, например имена пользователей, пароли и номера кредитных карт. Затем оно отправляет эту информацию хакеру.
- Руткиты — это вредоносные программы, которые позволяют хакерам получить доступ администратора к операционной системе компьютера или другим ресурсам.
- Черви — это самовоспроизводящийся вредоносный код, который может автоматически распространяться между приложениями и устройствами.

Социальная инженерия

С помощью социальной инженерии злоумышленники манипулируют людьми, заставляя их делать то, чего они делать не должны: делиться информацией, которой не должны делиться, скачивать программы, которые не должны скачивать, или отправлять деньги преступникам.

Фишинг — одна из самых распространённых атак с использованием социальной инженерии. Согласно отчёту «Стоимость утечки данных», это вторая по распространённости причина утечек. В самых простых фишинговых схемах используются поддельные электронные письма или текстовые сообщения для кражи учётных данных пользователей, утечки конфиденциальных данных или распространения вредоносного ПО. Фишинговые сообщения часто выглядят так, будто они исходят из надёжного источника. Обычно они направляют жертву на переход по гиперссылке, которая ведёт на вредоносный сайт, или на открытие вложения в электронном письме, которое оказывается вредоносным.

Киберпреступники также разработали более изощрённые методы фишинга. Целевой фишинг — это целенаправленная атака, целью которой является манипулирование конкретным человеком, часто с использованием данных из

публичных профилей жертвы в социальных сетях, чтобы сделать обман более убедительным. Киллер-фишинг — это разновидность целевого фишинга, нацеленная на руководителей высшего звена. Фишинг с использованием служебного почтового ящика (BEC) — это мошенничество, при котором киберпреступники выдают себя за руководителей, поставщиков или других деловых партнёров, чтобы обманом заставить жертв перевести деньги или поделиться конфиденциальными данными.

Атаки типа "Отказ в обслуживании"

Атаки типа «отказ в обслуживании» (DoS) и распределённые атаки типа «отказ в обслуживании» (DDoS) перегружают ресурсы системы мошенническим трафиком. Этот трафик перегружает систему, препятствуя отклику на легитимные запросы и снижая производительность системы. Атака типа «отказ в обслуживании» может быть самоцелью или подготовкой к другой атаке.

Разница между DoS-атаками и DDoS-атаками заключается в том, что при DoS-атаках для создания мошеннического трафика используется один источник, а при DDoS-атаках — несколько источников. DDoS-атаки часто проводятся с помощью ботнета — сети подключённых к интернету устройств, заражённых вредоносным ПО и находящихся под контролем хакера. Ботнеты могут включать в себя ноутбуки, смартфоны и устройства Интернета вещей (IoT). Жертвы часто не знают, что ботнет захватил их устройства.

Компрометация учетной записи

Взлом учётной записи — это любая атака, в ходе которой хакеры захватывают учётную запись законного пользователя для вредоносных действий. Киберпреступники могут проникнуть в учётную запись пользователя разными способами. Они могут украсть учётные данные с помощью фишинговых атак или купить базы данных с краденными паролями в даркнете. Они могут использовать инструменты для взлома паролей, такие как Hashcat и John the Ripper, чтобы расшифровать пароли, или проводить атаки методом перебора, в ходе которых они запускают автоматические скрипты или ботов для генерации и тестирования потенциальных паролей, пока не найдут подходящий.

Атаки "Человек посередине"

При атаке «человек посередине» (MiTM) , также называемой «атакой-подслушиванием», хакер тайно перехватывает сообщения между двумя людьми или между пользователем и сервером. Атаки «человек посередине» обычно проводятся через незащищённые общедоступные сети Wi-Fi, где злоумышленникам относительно легко следить за трафиком.

Хакеры могут читать электронные письма пользователей или даже тайно изменять их до того, как они попадут к получателю. При атаке с перехватом сеанса хакер прерывает соединение между пользователем и сервером, на котором хранятся важные данные, например конфиденциальная база данных компании. Хакер подменяет свой IP-адрес IP-адресом пользователя, заставляя сервер думать, что он является законным пользователем, вошедшим в законный сеанс.

Это даёт хакеру возможность свободно красть данные или иным образом сеять хаос.

Атаки на цепочку поставок

Атаки на цепочки поставок — это кибератаки, в ходе которых хакеры взламывают компанию, нацеливаясь на её поставщиков программного обеспечения, материалов и других услуг. Поскольку поставщики часто так или иначе связаны с сетями своих клиентов, хакеры могут использовать сеть поставщика в качестве вектора атаки для одновременного доступа к нескольким целям.

Например, в 2020 году компания-разработчик программного обеспечения SolarWinds была взломана, и злоумышленники распространили вредоносное ПО среди её клиентов под видом обновления. Вредоносное ПО позволило получить доступ к конфиденциальным данным различных государственных учреждений США, использующих сервисы SolarWinds, в том числе Министерства финансов, юстиции и государственного департамента.

Другие типы кибератак

- Межсайтовый скриптинг (XSS)

При атаках с использованием межсайтового скриптинга (XSS) вредоносный код встраивается в легитимную веб-страницу или веб-приложение. Когда пользователь заходит на сайт или в приложение, код автоматически запускается в его веб-браузере, обычно крадя конфиденциальную информацию или перенаправляя пользователя на поддельный вредоносный сайт. Злоумышленники часто используют JavaScript для атак с использованием XSS.

- SQL-инъекция

При атаках с использованием SQL-инъекций язык структурированных запросов (SQL) используется для отправки вредоносных команд в серверную базу данных веб-сайта или приложения. Хакеры вводят команды в поля, доступные пользователю, например в строки поиска и окна входа в систему. Затем команды передаются в базу данных, что приводит к возвращению конфиденциальных данных, таких как номера кредитных карт или сведения о клиентах.

- Туннелирование DNS

Туннелирование DNS скрывает вредоносный трафик внутри DNS-пакетов, позволяя ему обходить брандмауэры и другие меры безопасности. Киберпреступники используют туннелирование DNS для создания секретных каналов связи, которые они могут использовать для скрытого извлечения данных или установления соединений между вредоносным ПО и сервером управления и контроля (C&C).

- Эксплойты нулевого дня

Эксплойты нулевого дня используют уязвимости нулевого дня, которые либо неизвестны сообществу специалистов по безопасности, либо выявлены, но ещё не устранены. Эти уязвимости могут существовать в течение нескольких дней, месяцев или лет, прежде чем разработчики узнают о них, что делает их основными целями для хакеров.

- Атаки без файлов

При бесфайловых атаках используются уязвимости в легальных программах для внедрения вредоносного кода непосредственно в память компьютера. Киберпреступники часто используют PowerShell, инструмент для написания сценариев, встроенный в операционные системы Microsoft Windows, для запуска вредоносных сценариев, которые изменяют настройки или крадут пароли.

- Подмена DNS

Атаки с подменой DNS-имен, также называемые «отравлением DNS», скрытно изменяют DNS-записи, чтобы заменить реальный IP-адрес веб-сайта на поддельный. Когда жертвы пытаются зайти на настоящий сайт, они по незнанию попадают на вредоносную копию, которая крадёт их данные или распространяет вредоносное ПО.

Предотвращение, обнаружение и реагирование на кибератаки

Организации могут снизить количество кибератак, внедряя системы и стратегии кибербезопасности. Кибербезопасность — это практика защиты критически важных систем и конфиденциальной информации от цифровых атак с помощью сочетания технологий, людей и процессов.

Многие организации внедряют стратегию управления угрозами для выявления и защиты наиболее важных активов и ресурсов. Управление угрозами может включать в себя такие политики и решения по обеспечению безопасности, как:

- политики Управление идентификацией и доступом (IAM), в том числе доступ с минимальными привилегиями, многофакторная аутентификация и политики надёжных паролей, могут помочь обеспечить доступ к нужным ресурсам только нужным людям. Компании также могут требовать от удалённых сотрудников использования виртуальных частных сетей (VPN) при доступе к конфиденциальным ресурсам через незащищённый Wi-Fi.
- Комплексная платформа для защиты данных и инструменты для предотвращения потери данных (DLP) могут шифровать конфиденциальные данные, отслеживать доступ к ним и их использование, а также оповещать о подозрительной активности. Организации также могут регулярно создавать резервные копии данных, чтобы минимизировать ущерб в случае утечки.
- Брандмауэры могут помочь предотвратить проникновение злоумышленников в сеть. Брандмауэры также могут блокировать вредоносный трафик, выходящий из сети, например попытки вредоносного ПО связаться с сервером управления и контроля.
- Обучение основам безопасности может помочь пользователям выявлять и избегать наиболее распространённых видов кибератак, таких как фишинг и другие атаки с использованием социальной инженерии.
- Политика управления уязвимостями, в том числе управление исправлениями и регулярное тестирование на проникновение, может помочь выявить и устранить уязвимости до того, как ими воспользуются хакеры.
- Инструменты управления поверхностью атаки (ASM) позволяют выявлять, каталогизировать и устранять потенциально уязвимые ресурсы до того,

как их обнаружат злоумышленники.

- Инструменты унифицированного управления конечными устройствами (UEM) позволяют применять политики безопасности и контролировать все конечные устройства в корпоративной сети, включая ноутбуки, настольные компьютеры и мобильные устройства.

Обнаружение кибератак

Невозможно полностью предотвратить попытки кибератак, поэтому организации могут также использовать непрерывный мониторинг безопасности и процессы раннего обнаружения для выявления и оповещения о текущих кибератаках. Примеры:

- Системы управления информацией и событиями в сфере безопасности (SIEM) централизуют и отслеживают оповещения от различных внутренних инструментов кибербезопасности, включая системы обнаружения вторжений (IDS), системы обнаружения и реагирования на угрозы (EDR) и другие решения для обеспечения безопасности.
- Платформы для анализа угроз расширяют возможности оповещений о безопасности, помогая специалистам по безопасности понять, с какими типами угроз кибербезопасности они могут столкнуться.
- Антивирусное программное обеспечение может регулярно проверять компьютерные системы на наличие вредоносных программ и автоматически устранять обнаруженные вредоносные программы.
- Проактивные выявления угроз могут отслеживать киберугрозы, тайно скрывающиеся в сети, например, сложные постоянные угрозы (APT).

Реагирование на кибератаки

Организации также могут предпринимать шаги для обеспечения надлежащего реагирования на текущие кибератаки и другие события, связанные с кибербезопасностью. Примеры:

- Планы реагирования на инциденты могут помочь сдержать и устранить различные виды кибератак, восстановить пострадавшие системы и проанализировать первопричины для предотвращения будущих атак. Планы реагирования на инциденты снижают общие затраты на кибератаки. Согласно отчету «Стоимость утечки данных», в организациях с официальными группами реагирования на инциденты и планами затраты на утечку данных в среднем на 58% ниже.
- Решения для управления, автоматизации и реагирования на угрозы безопасности (SOAR) позволяют командам по обеспечению безопасности координировать разрозненные инструменты безопасности в полуавтоматизированных или полностью автоматизированных сценариях для реагирования на кибератаки в режиме реального времени.
- Решения расширенного обнаружения и реагирования (XDR) объединяют инструменты и операции по обеспечению безопасности на всех уровнях — для пользователей, конечных устройств, электронной почты, приложений, сетей, облачных рабочих нагрузок и данных. Решения XDR могут помочь автоматизировать сложные процессы предотвращения, обнаружения, расследования и

реагирования на кибератаки, включая проактивную защиту от угроз.

Кибератаку можно предотвратить

Несмотря на распространённость кибератак, данные Check Point свидетельствуют о том, что 99% предприятий не защищены должным образом. Однако кибератаки можно предотвратить. Ключом к киберзащите является комплексная многоуровневая архитектура кибербезопасности, охватывающая все сети, конечные и мобильные устройства, а также облако. С помощью правильной архитектуры можно объединить управление несколькими уровнями безопасности и контролировать политику с помощью единого интерфейса. Это позволяет сопоставлять события во всех сетевых средах, облачных сервисах и мобильных инфраструктурах.

Помимо архитектуры, рекомендуется соблюдение следующих ключевых мер для предотвращения кибератак:

- Поддерживайте гигиену безопасности
- Выберите предотвращение, а не обнаружение
- Охватите все векторы атаки
- Внедряйте самые передовые технологии
- Поддерживайте свою информацию об угрозах в актуальном состоянии

Рассмотрим тенденций в сфере сетевой безопасности, которые могут изменить подход организаций к кибербезопасности

1. Появление безопасного браузера

Поскольку всё больше работы выполняется через браузер, а утечки данных всё чаще происходят из-за уязвимостей в браузерах, защита этого входа в цифровой мир стала обязательным условием. Мы больше не живём в эпоху, когда сотрудники получают доступ к бизнес-приложениям исключительно с настольных компьютеров, расположенных в основном в офисе. С распространением удалённой работы, BYOD (принеси своё устройство) и растущей зависимостью от облачных сервисов как никогда важно, чтобы организации предоставляли сотрудникам безопасный доступ к цифровым инструментам, необходимым для выполнения работы, независимо от местоположения, устройства или приложения. Безопасные браузеры не только защищают от атак, но и предотвращают случайную и намеренную утечку конфиденциальных данных, при этом они могут быть такими же простыми в использовании, как и потребительские браузеры. По мере широкого распространения этой технологии она коренным образом изменит подход организаций к безопасности браузеров, ознаменовав начало новой эры в безопасной цифровой трансформации.

2. По мере того как государства будут усиливать атаки на инфраструктуру, правительства будут инвестировать в интеллектуальные и безопасные инфраструктурные технологии

Мы ожидаем, что правительства будут инвестировать в модернизированные и защищённые системы, особенно в условиях растущего числа атак на критически важную инфраструктуру со стороны государств. Эти усилия выходят за рамки замены устаревших технологий и направлены на внедрение интеллек-

туальных технологий, обеспечивающих безопасность как старой, так и новой инфраструктуры для удовлетворения потребностей мира, подключённого к цифровым сетям.

Правительства также уделяют приоритетное внимание инвестициям в технологию 5G, чтобы сделать города «умными». Эти достижения будут способствовать инновациям в сфере транспорта, энергетики и коммунальных услуг, поддерживая переход к более интеллектуальной инфраструктуре. Однако проблем ещё много. Например, 66% транспортных организаций пострадали от атак программ-вымогателей, а 77% государственных и других организаций государственного сектора не имеют полного представления обо всех своих устройствах Интернета вещей. Эти пробелы подвергают критически важные системы рискам, таким как физический ущерб, кража данных и перебои в работе. Это подчеркивает настоятельную необходимость принятия всеобъемлющих мер безопасности.

Во многих критически важных средах, в том числе на промышленных объектах и удалённых объектах, возникают уникальные проблемы, связанные с обеспечением безопасности инфраструктуры. Промышленные NGFW-маршрутизаторы являются важным решением для таких условий, обеспечивая надёжную защиту там, где традиционное оборудование может выйти из строя. В условиях растущих угроз и сложности обеспечения безопасности устройств Интернета вещей и промышленной автоматизации необходим надёжный подход к мониторингу и защите.

Мы считаем, что правительства сосредоточатся на создании комплексных решений в области безопасности, которые будут защищать как устаревшие системы, так и новые технологии. Благодаря использованию инструментов на основе ИИ для обнаружения, мониторинга и защиты устройств Интернета вещей и промышленной автоматизации в режиме реального времени эти инвестиции обеспечат безопасность критически важных систем и будут способствовать цифровой трансформации общественной инфраструктуры. Эти усилия помогут обеспечить бесперебойную работу жизненно важных служб и гарантировать гражданам безопасность и уверенность, которых они ожидают.

3. Злоумышленники будут использовать постквантовую криптографию (PQC) для обхода средств защиты

Средства защиты, предназначенные для предотвращения будущих квантовых атак (PQCs), создали для злоумышленников возможность использовать решения для обеспечения безопасности, которые не поддерживают PQCs или не были обновлены для выявления и блокировки трафика, зашифрованного с помощью PQCs. Например, браузер Google Chrome теперь поддерживает PQCs по умолчанию. Непреднамеренным последствием этого станет рост числа атак с использованием PQC, встроенных в веб-трафик, который теперь по умолчанию зашифрован. Это повлияет на кибербезопасность, поскольку многие продукты для обеспечения сетевой безопасности не могут проверять трафик PQC, и злоумышленники воспользуются этим, чтобы скрыть атаки внутри постквант-

тового шифрования.

Чтобы бороться с этим, предприятиям необходимо понимать, где используются эти алгоритмы, и иметь возможность расшифровывать и проверять все данные, проходящие через их корпоративные сети. Хорошая новость заключается в том, что существуют технологии, такие как платформа сетевой безопасности Strata, для выявления, блокировки и расшифровки PQC.

4. Для успешного взлома злоумышленники всё чаще будут использовать несколько методов, что потребует совместной работы служб безопасности в рамках платформы

Прошли те времена, когда атаки нацеливались на один продукт или уязвимость. В 2025 году одной из самых тревожных тенденций в сфере кибербезопасности станет всё более широкое использование многовекторных атак и многоэтапных подходов. Как это работает? Киберпреступники используют комбинацию тактик, методов и процедур (TTP), одновременно атакуя несколько областей, чтобы прорвать оборону. Мы увидим рост сложности и количества атак, основанных на веб-ресурсах, файлах, DNS и программах-вымогателях, что усложнит эффективную защиту от современных угроз с помощью традиционных разрозненных инструментов безопасности.

Для предотвращения таких атак потребуется, чтобы несколько служб безопасности работали вместе как часть интегрированной платформы, останавливающей каждую атаку на любом этапе цепочки киберпреступлений. Например, наши облачные службы безопасности (CDSS) на базе точного искусственного интеллекта могут предотвращать новейшие и самые изощрённые угрозы в режиме реального времени с помощью встроенных в нашу платформу сетевой безопасности средств защиты, которые предоставляются автоматически. Обеспечивая защиту на нескольких этапах цепочки киберпреступлений, компании могут предотвратить атаку, обеспечивая многоуровневую защиту от всего спектра угроз. В 2025 году и в последующие годы наиболее эффективную защиту обеспечат только решения для обеспечения безопасности, позволяющие отслеживать атаки в сети, облаке и на конечных устройствах.

5. ИИ в сфере безопасности позволит организациям сократить разрыв в навыках кибербезопасности

По мере того, как киберугрозы становятся всё более изощрёнными и распространёнными, спрос на квалифицированных специалистов по кибербезопасности продолжает опережать предложение. Но впереди нас ждёт светлое будущее, поскольку помощники на базе ИИ заполняют пробелы в качестве интеллектуальных ассистентов, призванных помогать специалистам по кибербезопасности в их повседневных задачах. Если в 2024 году каждый поставщик решений для обеспечения безопасности представил своего помощника, то в 2025 году они получат широкое распространение, поскольку клиенты осознают всю их мощь. Используя наших помощников, специалисты по кибербезопасности могут получать знания, не отходя от рабочего места, мгновенно получать доступ к аналитической информации и пользоваться преимуществами управляе-

мой автоматизации. В будущем жизнь специалистов по кибербезопасности станет ещё проще благодаря способности помощников автоматизировать повторяющиеся задачи, обрабатывать огромные объёмы данных и давать более точные ответы и проводить анализ.

Это очень важно, поскольку нехватка специалистов по кибербезопасности уже давно является проблемой для предприятий по всему миру. Когда каждый специалист по кибербезопасности будет вооружён мощным помощником на базе искусственного интеллекта, специалисты по кибербезопасности смогут работать эффективнее, а не усерднее.

6. Компании удвоят свой интерес к внедрению единого поставщика услуг безопасного доступа (SASE)

Работники больше не привязаны к офису, и им нужен безопасный и высокопроизводительный доступ к критически важным бизнес-технологиям. Независимо от того, где они находятся — в домашнем офисе, в местной кофейне или на пляже, — им нужно выполнять свою работу, где бы они ни находились и какое бы устройство ни использовали. Чтобы адаптироваться к новым условиям работы, компаниям придется делать больше для защиты конфиденциальных рабочих нагрузок и данных, обеспечивая при этом продуктивность сотрудников. Именно поэтому в 2025 году мы увидим повсеместное внедрение решений SASE от одного поставщика.

Поскольку сотрудники будут требовать от корпоративных приложений того же, что и от потребительских, выбранное решение для обеспечения безопасности должно помогать, а не препятствовать повышению производительности. Это включает в себя обеспечение минимальной задержки и времени простоя даже при доступе к облачным приложениям из удалённых мест. Сотрудники смогут получать доступ к SaaS-приложениям в 5 раз быстрее, чем при прямом подключении через Интернет, поэтому не придётся выбирать между безопасностью и производительностью. Будущее сферы труда требует гибкости, и решения SASE от одного поставщика способны обеспечить оперативность и безопасность, необходимые предприятиям для успешной работы в условиях растущей распределённости сотрудников. И комплексное решение SASE должно изначально включать защищённый браузер.

7. ИИ будет использоваться в каждом крупном бизнес-приложении, что приведёт к росту числа атак, ориентированных на ИИ

Мы ожидаем, что в ближайшие 12–24 месяца количество приложений с искусственным интеллектом увеличится в 3–5 раз. По мере того, как компании будут внедрять эти технологии, они могут упустить из виду ключевые проблемы, связанные с методами сбора данных, управлением и потребностями в безопасности, характерными для ИИ. Злоумышленники будут использовать эти уязвимости, чтобы усилить атаки на новые компоненты, такие как большие языковые модели, а также на данные для обучения и умозаключений. Это может привести к инцидентам, связанным с безопасностью, соблюдением нормативных требований и юридическими проблемами в следующем году.

В конечном счёте речь идёт о защите ваших конфиденциальных данных. Но вопрос в том, как это сделать? Единственный способ защититься от всех этих угроз, связанных с ИИ, — это комплексные решения на основе ИИ. Вы можете использовать ИИ с помощью ИИ, применяя защиту доступа к ИИ, которая обеспечивает сотрудникам безопасный доступ к приложениям GenAI. Управление безопасностью ИИ (SPM) выявляет риски в вашей цепочке поставок ИИ, включая проблемы с конфигурацией и способы, которыми вы можете раскрывать свои конфиденциальные данные. Безопасность ИИ во время выполнения гарантирует, что ваши приложения, данные и модели защищены от угроз, связанных с ИИ. В 2025 году компании, которые будут безопасно внедрять ИИ, выделятся на фоне остальных.

8. ИИ сделает фишинговые электронные письма неотличимыми от настоящих

Методы, ориентированные на пользователей, такие как фишинговые электронные письма, станут более успешными благодаря тому, что злоумышленники будут использовать генеративный искусственный интеллект (GenAI) для создания более эффективных и убедительных атак. Мы уже наблюдаем 30-процентный рост числа успешных попыток фишинга, когда электронные письма пишутся или переписываются с помощью GenAI. Обычные люди, такие как мы с вами, станут ещё менее надёжными в качестве последней линии защиты, и предприятия будут полагаться на передовые средства защиты на основе ИИ для защиты от этих сложных атак.

В то время как сегодня компании полагаются на антифишинговые технологии, такие как фильтрация URL-адресов (AURL) на сетевом уровне, всё больше компаний будут усиливать свою защиту с помощью безопасных браузеров в качестве первой линии обороны от этих атак. В сочетании с решением SASE от одного поставщика на базе искусственного интеллекта, которое предлагает расширенные облачные сервисы безопасности, ваша компания будет готова предотвращать новейшие и самые изощрённые угрозы в режиме реального времени. И эти средства защиты обычно встроены в решение SASE и предоставляются автоматически. Таким образом нам не придётся собирать отдельные продукты. Все эти инновации изначально интегрированы в одно комплексное решение SASE для каждого пользователя, устройства и приложения.

Появляется больше специалистов по цепочкам атак: в последние годы киберпреступники тратят больше времени на «до-взлом» — разведку и подготовку к атакам. В результате злоумышленники могут проводить целенаправленные атаки быстрее и точнее. В прошлом мы наблюдали, как многие поставщики CaaS выполняли функции универсальных специалистов, предлагая покупателям всё необходимое для проведения атаки — от фишинговых комплектов до вредоносных программ. Однако мы ожидаем, что группы CaaS будут всё больше специализироваться, и многие из них сосредоточатся на предоставлении услуг, ориентированных на один сегмент цепочки атак.

Это облако с возможностью кибератак: в то время как такие цели, как пе-

риферийные устройства, будут и дальше привлекать внимание злоумышленников, есть ещё одна часть поверхности атаки, на которую защитники должны обратить пристальное внимание в ближайшие несколько лет: их облачные среды. Хотя облачные технологии не являются чем-то новым, они всё больше привлекают внимание киберпреступников. Учитывая, что большинство организаций используют несколько поставщиков облачных услуг, неудивительно, что мы наблюдаем рост числа уязвимостей, связанных с облачными технологиями, которые используют злоумышленники. Мы ожидаем, что эта тенденция сохранится в будущем.

Автоматизированные хакерские инструменты попадают на рынок даркнета: на рынке CaaS теперь доступно, казалось бы, бесконечное количество векторов атак и связанного с ними кода, таких как наборы для фишинга, программы-вымогатели как услуга, DDoS-атаки как услуга и многое другое. Хотя мы уже видим, что некоторые киберпреступные группировки используют ИИ для создания предложений CaaS, мы ожидаем, что эта тенденция будет развиваться. Мы предполагаем, что злоумышленники будут использовать автоматизированные результаты работы LLM для создания предложений CaaS и расширения рынка, например, для сбора информации в социальных сетях и автоматизации этих данных в виде готовых фишинговых наборов.

Схемы действий расширяются, включая реальные угрозы: киберпреступники постоянно совершенствуют свои схемы действий, а атаки становятся все более агрессивными и разрушительными. Прогнозируется, что злоумышленники будут расширять свои схемы действий, объединяя кибератаки с реальными физическими угрозами. Мы уже видим, как некоторые киберпреступные группировки в некоторых случаях физически угрожают руководителям и сотрудникам организаций, и мы ожидаем, что это станет регулярной частью многих схем действий. Мы также ожидаем, что транснациональные преступления, такие как торговля наркотиками, контрабанда людей или товаров и многое другое, станут постоянным компонентом более изощрённых схем, в которых киберпреступные группировки и транснациональные преступные организации будут работать сообща.

Противодействие злоумышленникам будет расширяться: по мере того, как злоумышленники постоянно совершенствуют свои стратегии, сообщество специалистов по кибербезопасности в целом может делать то же самое в ответ. Глобальное сотрудничество, создание государственно-частных партнёрств и разработка механизмов борьбы с угрозами — всё это жизненно важно для повышения нашей коллективной устойчивости. Многие связанные с этим усилия уже предпринимаются, и ожидается, что появится больше совместных инициатив, которые существенно повлияют на борьбу с киберпреступностью.

Заключение

- Повышение коллективной устойчивости к меняющемуся Ландшафту угроз

Киберпреступники всегда будут находить новые способы проникновения в организации. Тем не менее, у сообщества специалистов по кибербезопасности есть множество возможностей для сотрудничества, чтобы лучше предвидеть следующие шаги злоумышленников и эффективно препятствовать их деятельности.

Значение отраслевых усилий и государственно-частного партнёрства невозможно переоценить, и мы ожидаем, что в ближайшие годы число организаций, участвующих в этом сотрудничестве, будет расти. Кроме того, организации должны помнить, что кибербезопасность — это работа для всех, а не только для специалистов по безопасности и ИТ. Например, повышение осведомлённости и обучение сотрудников в области безопасности — важный компонент управления рисками. И, наконец, другие организации, от правительств до поставщиков, которые производят продукты для обеспечения безопасности, на которые мы полагаемся, обязаны продвигать и соблюдать надёжные методы обеспечения кибербезопасности.

- Подготовка к будущему сетевой безопасности

Будущее сетевой безопасности выглядит захватывающим, но оно также сопряжено с трудностями. Организациям крайне важно опережать эти новые тенденции, разрабатывая гибкие стратегии безопасности, которые можно адаптировать к быстро меняющемуся ландшафту угроз.

Для компаний, стремящихся обеспечить сетевую безопасность на будущее, ключевым фактором является инвестирование в комплексный платформенный подход, который включает в себя новые технологии, такие как защищённые браузеры, SASE от одного поставщика, ИИ-копипасты и обнаружение угроз, и реагирование на них с помощью ИИ. Таким образом, они не только защитятся от сегодняшних угроз, но и будут готовы к киберугрозам завтрашнего дня.

Сетевая безопасность станет более динамичной, инновационной и проактивной, чем когда-либо прежде. Это изменит подход организаций к защите своих наиболее ценных активов и обеспечит безопасное и устойчивое будущее в условиях постоянно меняющегося цифрового мира.

Ландшафт кибербезопасности будет формироваться под влиянием роста числа атак с использованием ИИ, надвигающейся угрозы квантовых вычислений и растущей уязвимости платформ социальных сетей. Чтобы опережать эти вызовы, организациям необходимо инвестировать в защиту на основе ИИ, переходить на квантово-устойчивое шифрование и внедрять подход «Никому не доверяй» в сфере облачных технологий и Интернета вещей. Кроме того, компаниям необходимо готовиться к ужесточению нормативно-правовой среды и растущей необходимости в киберстраховании. Поскольку киберпреступность развивается беспрецедентными темпами, компании, которые не адаптируются, рискуют стать следующей жертвой. Сейчас самое время действовать, защищать цифровые активы и обеспечивать безопасность в будущем.

Ни одна организация или служба безопасности не может в одиночку бороться с киберпреступностью. Работая сообща и обмениваясь информацией по

всей отрасли, мы можем эффективнее противостоять злоумышленникам и защищать общество.

Список источников

1. «Зашифрованные файлы или информация: HTML-контрабанда, подметод T1027.006 — Enterprise | MITRE ATT&CK®». attack.mitre.org. Получено 22 февраля 2023.
2. «Статистика контроля доступа: тенденции и идеи». 23 февраля 2024. Получено 26 апреля 2024.
3. «Исследование нарушений кибербезопасности в 2023 году». GOV.UK. Получено 30 ноября 2023.
4. «Как работают кибератаки». www.ncsc.gov.uk. Получено 30 ноября 2023.
5. «Защитите себя от фишинга — служба поддержки Microsoft». support.microsoft.com. Получено 6 декабря 2023.
6. Лазарус, Ари (23 февраля 2018 г.). «Фишеры рассылают поддельные счета». Информация для потребителей. Получено 17 февраля 2020 г..
7. «Как повысить осведомленность о кибербезопасности». ISACA. Получено 25 февраля 2023.

УДК 330

ГЛАВА 9. КИБЕРБЕЗОПАСНОСТЬ. ЛУЧШИЕ ВЕКТОРНЫЕ БАЗЫ ДАННЫХ ДЛЯ РАСКРЫТИЯ ИСТИННОГО ПОТЕНЦИАЛА ИИ

Аменицкий Алексей Владимирович
аспирант
Санкт-Петербургский государственный электротехнический университет ЛЭТИ имени В.И. Ульянова (Ленина)

Научный руководитель: Воробьёв Евгений Германович
д.т.н., профессор
Санкт-Петербургский государственный электротехнический университет ЛЭТИ имени В.И. Ульянова (Ленина)

Аннотация: С появлением передовых технологий векторные базы данных набирают популярность в различных секторах благодаря своей способности в полной мере использовать потенциал искусственного интеллекта (ИИ).
Простота использования векторных баз данных делает их особенно привлекательными для LLM. Кроме того, они обладают врожденной способностью быстро выполнять поиск сходства в больших наборах данных. Тем не менее, как и у любой технологии, у них есть свои ограничения.
Ключевые слова: Cyber Security (CS), CS architecture, CS trends, CS tendences, CS tools, CS crimes, CS latest news, CS releases, CS game-changers, CS future, CS playbook, CS agenda, CS future, CS risks, CS incidents, CS resilience, Hackers, CS прогноз, Artificial Intelligence, Deep Fakes, Эволюция киберУгроз, КиберГигиена.

CYBERSECURITY. THE BEST VECTOR DATABASES TO UNLOCK THE TRUE POTENTIAL OF ARTIFICIAL INTELLIGENCE

Amenitsky Alexey Vladimirovich

Scientific supervisor: Vorobyov Evgeny Germanovich

Векторная база данных - это тип базы данных, в которой данные хранятся в виде многомерных векторов, которые представляют собой математические представления сущностей или атрибутов.

Эти векторы обычно генерируются путем применения какой-либо функции встраивания к необработанным данным, таким как текст, изображения, аудио, видео и другие. Векторные базы данных могут быть определены как инструмент, который индексирует и хранит векторные вложения для быстрого поиска и поиска сходства, с такими функциями, как фильтрация метаданных и гори-

зонтальное масштабирование.

С появлением и ростом популярности широких языковых моделей (LLM) векторные базы данных зарекомендовали себя как ценные инструменты для расширения возможностей этих моделей. По мере того, как технология LLM продолжает развиваться, возникает вопрос: действительно ли нам нужна специализированная векторная база данных?

Векторные Базы данных играют решающую роль в максимизации преимуществ технологий искусственного интеллекта. Это поможет вам упорядочить сложные данные в структуру, понятную машине, тем самым способствуя лучшему пониманию данных.

Векторные базы данных - специализированные системы хранения, предназначенные для эффективной обработки векторных вложений, которые представляют собой многомерные векторы, представляющие сложные данные, такие как изображения, видео, аудио и текст, в формате, который машины могут понимать и обрабатывать. Эти базы данных специально разработаны для поддержки операций поиска сходства, позволяя пользователям выполнять запросы на примере (например, находить похожие изображения или документы), вычисляя расстояние между векторами. Суть векторных баз данных заключается в их способности быстро и точно индексировать, и искать огромные объемы многомерных данных, используя преимущества различных алгоритмов и структур данных, оптимизированных для этого типа данных. Например, используя алгоритмы поиска ближайших приближенных соседей (ANN), векторные базы данных могут масштабироваться для поддержки миллиардов векторов при сохранении высокой производительности и точности. Это делает их особенно полезными для приложений искусственного интеллекта и машинного обучения, где они могут облегчить такие задачи, как системы рекомендаций, обнаружение контента и обнаружение мошенничества, обеспечивая быстрый и расширяемый поиск сходства.

Использование концепции векторных баз данных и их применение в искусственном интеллекте поможет получить ценную информацию в этой увлекательной области и сформировать свой бизнес.

В контексте искусственного интеллекта и машинного обучения векторные вложения представляют собой числовое представление семантики объекта. Эти представления отражают основные характеристики и взаимосвязи внутри данных, облегчая их обработку и понимание алгоритмами искусственного интеллекта. Вложения необходимы для таких задач, как обработка естественного языка, системы рекомендаций и распознавание изображений. Благодаря встраиваниям мы можем быстро найти похожий контент на основе сходства. Кроме того, вложения не ограничиваются только текстами, можно создавать векторы из изображений, аудио, видео или любых других данных, используя обученные шаблоны кодировщиков для извлечения из них значимой информации. Некоторые шаблоны, такие как шаблон встраивания текста даже не зависят от языка, что означает, что они могут изначально понимать сходство на разных языках.

Рассмотрим векторные базы данных и как они могут помочь с ИИ, и о лучших векторных базах данных, которые частные лица и предприятия могут использовать для эффективного улучшения ИИ.

Назначение векторных баз данных

С ростом числа примеров использования генеративного ИИ, который произошел, в частности, с появлением ChatGPT для широкой публики, все больше и больше компаний захотели воспользоваться преимуществами этого нововведения. В частности, многие из них хотят разработать свои собственные самодельные LLM, чтобы они могли воспользоваться преимуществами новейших языковых моделей, специализируясь при этом на своих собственных данных.

Когда мы говорим о LLM, возникает вопрос о встраивании, а точнее о векторном представлении слов. По сути, это ключевой элемент в разработке языковых моделей, поскольку отныне слова представлены векторами. Поэтому необходимо эффективно хранить эти векторы, чтобы иметь возможность запускать оптимизированные и адаптированные запросы. Нет ничего лучше, чем использовать базу данных, которая специализируется на хранении векторов и имеет все связанные функции поиска.

Векторная база данных - это инновационная платформа для управления данными, которая хранит информацию в виде векторов, также известных как векторные вложения. Этот подход использует возможности этих числовых представлений для эффективной индексации большого набора неструктурированных и полуструктурированных данных, таких как изображения, текст, или данные датчиков, что упрощает операции поиска.

Это семейство баз данных, разработанное специально для управления векторными вложениями или вложениями, предлагает комплексное решение для управления неструктурированными и полуструктурированными данными.

В отличие от библиотеки векторного поиска или векторного индекса, векторная база данных выходит за рамки этого, позволяя хранить метаданные и применять фильтры. Он также отличается своей масштабируемостью, способностью вносить динамические изменения в данные, установкой регулярных резервных копий, а также расширенными функциями безопасности.

Работа этой базы данных основана на организации данных в соответствии с векторами высокой размерности. Эти векторы состоят из сотен измерений, каждое из которых соответствует определенной функции или свойству объекта данных, который они представляют. Именно по расстоянию, разделяющему два векторных вложения, векторная база данных или система векторного поиска может определить сходство между двумя векторами.

Векторная база данных относится к типу базы данных, в которой могут храниться векторы. Здесь векторы - это математические представления всех объектов в пространстве.

Таким образом, векторные базы данных хранят данные и управляют ими с помощью векторных вложений. Эти базы данных отличаются от обычных баз,

данных тем, что они предназначены для выполнения двух важных задач:

Для поиска похожих предметов: Одной из ключевых характеристик векторных баз данных является их способность быстро и точно искать похожие предметы. Это достигается с помощью векторных интеграций, которые представляют данные в виде многомерных векторов. Затем эти вложения можно сравнить с помощью mathematic по всем операциям, чтобы определить сходство элементов.

Выполнение расширенного анализа больших объемов данных: Еще одним преимуществом векторных баз данных является их способность анализировать огромные наборы данных. Они используют специальные алгоритмы и структуры, которые хорошо работают со встроенными векторами, что упрощает выполнение сложного анализа. Векторные базы данных гораздо эффективнее обрабатывают большие объемы неорганизованных данных, чем обычные базы данных.

Кроме того, векторные базы данных более адаптируемы и быстрее адаптируются к изменениям в данных или запросам, которые мы выполняем. Основная цель векторных баз данных - помочь организациям получить максимальную отдачу от ИИ. Благодаря векторной интеграции эти базы данных могут обнаруживать новые закономерности в данных и предоставлять нам новую информацию.

Основные функции векторных баз данных

- Эффективный поиск сходства

Служба потоковой передачи музыки использует векторную базу данных для поддержки своего механизма рекомендаций по песням. Преобразуя песни в векторные вложения на основе их звуковых характеристик и метаданных, служба может быстро находить и предлагать песни, похожие на текущие избранные пользователя.

- Сценарий

Эта функция применяется, когда пользователи ищут контент, соответствующий их интересам, что улучшает обнаружение и взаимодействие.

- Масштабируемая индексация и хранение

Интернет-магазин внедряет векторную базу данных для индексации миллионов изображений продуктов. Сохраняя визуальные характеристики каждого продукта в векторной форме, розничный торговец может предложить функцию «поиск по изображению», которая помогает покупателям находить товары, загружая изображения.

- Сценарий

Это важно на платформах электронной коммерции для улучшения взаимодействия с пользователем и обеспечения интуитивно понятных функций поиска.

- Обработка данных в реальном времени

Платформа социальных сетей использует векторную базу данных для анализа пользовательского контента в режиме реального времени. Обрабатывая текстовые данные и данные векторных изображений, платформа может быстро

классифицировать контент, обнаруживать спам и адаптировать каналы к индивидуальным предпочтениям пользователей.

- Сценарий

Необходим для платформ, которые требуют немедленной обработки и категоризации больших объемов данных для поддержания актуальности и вовлеченности пользователей.

Преимущества векторных баз данных

Векторные базы данных предлагают несколько преимуществ, которые могут значительно повысить производительность и масштабируемость в различных приложениях:

- Более быстрая обработка: Векторные базы данных предназначены для эффективного хранения и извлечения данных, что позволяет обрабатывать большие наборы данных.
- Масштабируемость: Эти базы данных могут легко масштабироваться вверх или вниз в зависимости от потребностей пользователей. Следовательно, они могут эффективно обрабатывать огромные объемы данных без ущерба для производительности.
- Точное сопоставление сходства: Векторные базы данных могут точно соответствовать аналогичным элементам, что делает их критически важными для приложений распознавания речи и изображений.
- Расширенные возможности поиска: Благодаря передовым алгоритмам поиска векторные базы данных обеспечивают более эффективные результаты поиска.
- Аналитика в реальном времени: Вы можете включить аналитику в реальном времени с помощью векторных баз данных, что позволяет приложениям быстро реагировать на меняющиеся данные и запросы.
- Рентабельность: Векторные базы данных требуют меньше аппаратного и программного обеспечения, чем традиционные базы данных, что делает их более рентабельными.
- Удобство для пользователя: Поскольку векторные базы данных созданы для удобства пользователя, даже нетехнические люди могут легко использовать их.
- Универсальность: Вы можете применять эти базы данных в различных контекстах, включая электронную коммерцию, здравоохранение, финансы и другие области.

Обеспечивая повышенную эффективность, масштабируемость и точное сопоставление сходств, векторные базы данных играют решающую роль в раскрытии полного потенциала ИИ.

Варианты использования векторных баз данных

Векторные базы данных становятся все более распространенными в различных отраслях промышленности из-за их способности расширять возможности ИИ. Вот некоторые из вариантов использования векторных баз данных:

Рекомендательные системы: Эти системы используют векторы для представления предпочтений пользователей и рекомендуемых элементов, позволяя им находить наилучшие совпадения и предоставлять индивидуальные предложения.

Поиск изображений и текста: Преобразование фотографий и текста в векторы упрощает поиск похожих изображений и текста. Это особенно полезно в электронной коммерции, где покупатели могут искать товары, используя ионные описания или изображения.

Обнаружение мошенничества: Векторные базы данных также полезны для обнаружения мошенничества. Их можно применять для поиска шаблонов данных, указывающих на мошенничество. Например, определенный набор транзакций с похожими векторными представлениями может указыватьate мошенничество.

Анализ настроений: Векторные базы данных находят применение в анализе настроений, где векторы могут использоваться для определения эмоционального тона текста.

Распознавание речи: При распознавании речи векторы помогают распознавать произнесенные слова.

Процесс естественного языка: Представление слов и фраз в векторной форме упрощает роботам понимание и интерпретацию человеческого языка. Он также используется при группировании документов и семантическом поиске.

Ожидается, что использование векторных баз данных будет расти еще больше по мере развития ИИ.

Теперь рассмотрим лучшие векторные базы данных с их функциями и преимуществами.

- Milvus

Milvus - это система векторных баз данных, предназначенная для эффективной и действенной обработки больших объемов сложных данных. Это мощное и гибкое решение для векторных баз данных обеспечивает высокую скорость, производительность, масштабируемость и специализированные функции для поиска сходств, обнаружения аномалий и естественного языка.

Ключевые особенности Milvus

Поиск и анализ данных: ввод-вывод выполняется невероятно быстро, обеспечивая быстрый и эффективный поиск и анализ данных.

Способность обрабатывать большие наборы данных: База данных может довольно эффективно обрабатывать большие наборы данных, что упрощает хранение и анализ данных.

Поддерживаемые форматы данных: Milvus.io поддерживает несколько форматов векторных данных, таких как аудио, текст и изображения.

Комплексная индексация: В решении используются передовые алгоритмы, позволяющие выполнять быстрые и точные операции.ели поиск векторного сходства.

Обновление в реальном времени: Milvius.io позволяет импортировать и

обновлять данные в реальном времени, гарантируя, что самые свежие данные будут легко доступны для анализа.

- Weaviate

Weaviate - это мощная база данных, которая эффективно хранит и ищет многомерные векторы. Он предлагает полезные функции и упрощает использование.

Ключевые особенности Weaviate

Семантическое исследование: Вместо простого использования ключевых слов, Weaviate.io позволяет пользователям искать related объекты в зависимости от их значения и контекста.

Обновление в реальном времени: База данных постоянно обновляется, чтобы быть в курсе последних изменений.

Гибкая схема: Weaviate.io может легко адаптироваться к различным типам данных и изменяющимся структурам данных.

Открытый исходный код: Открытый исходный код обеспечивает наглядность и позволяет настраивать его в соответствии с конкретными потребностями.

Персонализированные предложения: Он может анализировать пользовательские запросы, чтобы предоставлять персонализированные предложения, улучшая взаимодействие с пользователем.

Графики знаний: Пользователи могут создаватьate графики, соединяя похожие элементы, что позволяет проводить расширенный анализ данных.

Интеграция: Weaviate.io интеграция с фреймворками глубокого обучения, позволяющая создавать современные модели для катетеризации изображений или текста.задачи горизации.

Анализ временных рядов: Weaviate.io он отлично справляется с анализом временных рядов, обеспечивая эффективное хранение и извлечение данных для прогнозирования.проекты обнаружения аномалий.

- Pinecone

Pinecone - это надежная база данных, которая имеет множество преимуществ и специальных функций. Его отличает впечатляющая скорость, масштабируемость и поддержка сложных данных. Он может улучшать персонализированные рекомендации в зависимости от предпочтений пользователя.

Ключевые особенности Pinecone

Быстрое и эффективное извлечение данных: Он быстро находит и извлекает векторы.

Обрабатывает большие объемы данных: Он может обрабатывать большие объемы векторных данных, что делает его подходящим для крупных проектов. Он также обнаруживает неровности и закономерности в больших наборах данных.

Обновление в реальном времени: Он постоянно обновляет базу данных.

Высокая размерность: Хорошо работает с текстом и другими сложными типами данных, улучшая их понимание и поиск.

Автоматическая индексация: Она автоматически создает индексы для ускорения поиска.

Поиск сходства: Это помогает найти похожие векторы для группировки и рекомендаций.

Другие особенности: Он может выявлять необычное поведение в Данные временных рядов.

- Redis

Redis предлагает ценное решение для приложений, требующих быстрой и масштабируемой обработки данных, с упором на векторные данные и их эффективность.рабочие возможности, Redis предлагает ценное решение для приложений, требующих быстрой и масштабируемой обработки данных.

Ключевые особенности RedisVector

Хранение и анализ данных: RedisVector предназначен для обработки больших объемов векторных данных, таких как тензоры, матрицы и числовые таблицы, что позволяет хранить и анализировать эти данные.

Высокая производительность: Благодаря возрастающей скорости и масштабируемости Redis, хранилища данных в памяти, RedisVector обеспечивает молниеносное время отклика на запросы.

Индексирование и поиск: RedisVector включает встроенные функции индексирования и поиска, позволяющие быстро выполнять векторный поиск, такой как изображения, текстовые или аудиофайлы, на основе определенных критериев или искать похожие векторы.

Вычисление расстояний: RedisVector поддерживает различные измерения расстояний, что позволяет сравнивать векторы и выполнять сложные аналитические операции.

Операции с векторными данными: RedisVector предоставляет различные операции для работы с векторными данными, включая элементарные методы арифметики, агрегирования и преобразования.

Быстрое время отклика: Он может выявлять выбросы и аномалии в больших наборах данных благодаря быстрому времени отклика на запросы.

RedisVector хорошо подходит для приложений машинного обучения, которые обрабатывают и анализируют многомерные векторные данные. Это также может создать персонализированные системы рекомендаций путем сравнения предпочтений человека с векторами статей.

- Magasin unique

Универсальное хранилище может быть отличным выбором для масштабируемой обработки данных и высокопроизводительной аналитики.

Ключевые особенности Magasin unique

Горизонтальная масштабируемость: Он может обрабатывать большие объемы данных за счет горизонтального масштабирования на нескольких узлах, обеспечивая высокую доступность и масштабируемость.

Технология в памяти: Она может быстро обрабатывать и анализировать данные, что делает их сверхбыстрыми.

Аналитика в реальном времени: позволяет анализировать и интерпретировать данные в режиме реального времени, обеспечивая быстрое принятие решений.

Это дает полезную информацию за счет включения операционных данных.

Интегрированныйпроцессные данные: Он объединяет транзакционные и аналитические рабочие нагрузки на единой платформе, что делает процесс обработки данных более эффективным.

Полная поддержка SQL: Вы можете легко взаимодействовать с базой данных, используя общие SQL-запросы, что упрощает поиск данных и манипулирование ими.

Конвейеры данных: Он поддерживает непрерывный конвейеры данных и обеспечивает беспрепятственный ввод данных из различных источников.

Интегрированное машинное обучение: Оно интегрируется с инструментами и библиотеками машинного обучения, обеспечивая расширенную аналитику.

Гибридные рабочие нагрузки: Он гибкий и подходит для управления смешанными рабочими нагрузками, содержащими транзакционные и аналитические данные.

Данные временных рядов: Он эффективно управляет данными временных рядов, что делает его идеальным для таких приложений, как Интернет вещей, банковское дело и мониторинг.

- Pertinence IA

Актуальность ИИ помогает вам легко хранить, искать и анализировать большие объемы данных. Это комплексное и адаптируемое решение обладает множеством интересных функций.

Ключевые особенности Pertinence IA

Обработка данных: Векторная база данных может обрабатывать как небольшие, так и большие объемы данных, что делает ее подходящей для многих приложений.

Поиск в реальном времени: Вы можете искать информацию и получать мгновенные результаты, предоставляя вам немедленный доступ к необходимым данным.

Более быстрое время отклика: Система предназначена для обеспечения быстрого времени отклика на запросы, что позволяет вам быстро реагировать на извлеченные данные из ваших данных.

Расширенные алгоритмы: Векторная база данных предоставляет точные и релевантные результаты поиска с использованием передовых алгоритмов.

Поддерживаемые типы и форматы данных: Он поддерживает широкий спектр типов и форматов данных, что упрощает работу с различными наборами данных.

Исторические данные: Используя пользовательские настройки и исторические данные, могут быть созданы индивидуальные решения.

Квадрант

Quadrant - это универсальное решение для баз данных, обеспечивающее эффективное управление данными и анализ. Он отлично справляется с предложениями, основанными на сходстве, обнаружении аномалий и поиске изображений / текста.

- Quadrant

Ключевые особенности Quadrant

Эффективный поиск: Он использует передовые методы для поиска похожих объектов в наборе данных. Это поможет вам эффективно находить и извлекать связанные статьи.

Масштабируемость: Quadrant Vector может легко обрабатывать растущие объемы данных без ущерба для производительности. Это может расти вместе с вашими потребностями в данных.

Обновление в реальном времени и индексирование: С помощью обновления в реальном времени пользователи могут быстро получить доступ к latepервые изменения в данных. Он также позволяет индексировать в реальном времени.

Множество опций: Quadrant Vector предоставляет различные параметры запросов, включая фильтры, агрегацию и сортировку.

- Vespa

Vespa преуспевает в предоставлении персонализированных предложений, сочетая машинное обучение с информацией в реальном времени. Это идеальный выбор для мультимедийных приложений и приложений, управляемых контентом.

Ключевые особенности Vespa

Быстрые результаты запросов: Векторная база данных Vespa.ai обеспечивает быстрые результаты запросов даже при работе с огромными объемами данных.

Аналитика в реальном времени: позволяет анализировать данные в режиме реального времени, обеспечивая мгновенный доступ к ценной информации. Расширенный анализ данных и прогнозное моделирование стали возможными благодаря интеграции алгоритмов машинного обучения с векторной базой данных Vespa.ai.

Высокая доступность данных: Решение обеспечивает высокую доступность данных и отказоустойчивость, сводя к минимуму время простоя и обеспечивая непрерывное обслуживание.

Параметры ранжирования: Он предлагает настраиваемые параметры ранжирования, позволяющие организациям расставлять приоритеты и получать наиболее релевантные данные.

Геопространственные исследования: Vespa.ai поддерживает геопространственный поиск, позволяя проводить поиск на основе определения местоположения.

Vespa.ai идеально подходит для показа целевой рекламы нужной аудитории с помощью статистики в реальном времени и настраиваемых функций ранжирования.

Варианты использования векторных баз данных

Векторные базы данных идеально подходят для широкого спектра вариантов использования, включая поиск сходств, системы рекомендаций и анализ данных в таких областях, как машинное обучение, обработка естественного

языка, компьютерное зрение и многие другие. Вот несколько распространенных вариантов использования векторных баз данных:

- Рекомендательные системы: Векторные базы данных часто используются в рекомендательных системах для поиска статей или контента, похожих на то, с чем пользователь взаимодействовал в прошлом. Это может относиться к электронной коммерции, предоставлению рекомендаций по контенту, а также к музыкальным платформам или платформам потокового видео.
- Поиск на основе контента: На платформах мультимедийного контента векторные базы данных позволяют осуществлять поиск изображений, аудио и видеофайлов на основе контента. Пользователи могут искать контент с похожими визуальными или слуховыми характеристиками.
- Обнаружение аномалий: Обнаружение аномалий в многомерных данных, таких как журналы сетевого трафика, данные датчиков или финансовые транзакции, может быть выполнено с использованием векторных баз данных. Необычные точки данных можно идентифицировать, сравнивая их с набором нормальных векторов.
- Совместная фильтрация: Алгоритмы совместной фильтрации могут использовать векторные базы данных для поиска пользователей со схожими предпочтениями и рекомендовать элементы на основе поведения похожих пользователей.
- Долговременная память: Векторные базы данных могут использоваться для хранения прошлых поколений ответов LLM. Эти вложения могут быть вызваны для дальнейшего улучшения контекста языковой модели с учетом ее прошлого контекста.
- Группировка: В векторных базах данных группировка может применяться для организации данных в отдельные группы, что упрощает выявление закономерностей и сходств в наборе данных.
- Измерение разнообразия: В векторных базах данных измерение разнообразия может применяться для оценки объема и инклюзивности рекомендаций, обеспечивая сбалансированный выбор статей или контента для удовлетворения широкого спектра предпочтений или тем пользователей.

Подводные камни встраиваемых шаблонов и векторных баз данных

Хотя встраивания являются мощными, они не лишены своих проблем. Важно знать о потенциальных подводных камнях, таких как систематические ошибки в обучающих данных. Например, OpenAI объясняет в своей документации, как модель может более четко ассоциировать европейско-американские имена с положительным настроем по сравнению с афроамериканскими именами. Кроме того, встроенные шаблоны имеют даты отсечения в своих обучающих данных, что означает, что некоторые данные могут семантически изменяться с течением времени (например, популярность знаменитости). Выбор правильных методов встраивания и параметров имеет решающее значение для достижения оптимальных результатов, и для правильного использования

встраиваний необходимо применять соответствующие методы предварительной обработки данных.

Векторные базы данных - это только половина решения

Хотя векторные базы данных и вложения являются важными компонентами внедрения ИИ, важно признать, что они являются частью более широкой экосистемы. Создание надежной инфраструктуры искусственного интеллекта включает в себя решение других ключевых аспектов, таких как предварительная обработка данных, выбор шаблонов, разработка подсказок и стратегии развертывания. Векторные базы данных - это важная часть головоломки, но они не являются полным решением.

Одна из повторяющихся проблем, связанных с LLM и искусственным интеллектом в целом, - это компромисс с точки зрения точности. На протяжении веков компьютеры были двоичными и детерминированными. Хотя векторные базы данных могут представлять собой огромный шаг вперед в изучении знаний, их все же необходимо сочетать с традиционными структурированными архитектурами, чтобы обеспечить максимальный опыт поиска. Некоторые платформы, такие как Azure Cognitive Search и Elastic Search, активно работают над улучшением и настройкой гибридных поисков, используя объединение взаимных рейтингов (RRF) для объединения полученных рейтингов. Elastic также решает другие проблемы, связанные с векторными базами данных, такие как конфиденциальность данных и управление доступом на основе ролей (RBAC). Что касается разработки подсказок, в настоящее время разрабатываются различные платформы, такие как guidance ai, Langchain и LMQL, чтобы обеспечить надежный способ преобразования данных LLM в содержательные структурированные ответы. Излишне говорить, что мы переживаем захватывающие времена, и новые архитектуры RAG улучшаются с каждым днем.

Заключение

Векторные базы данных - это надежные инструменты, которые помогут вам управлять и анализировать большие объемы данных и полностью раскрыть потенциал ИИ. Они предлагают несколько преимуществ, таких как обработка, масштабируемость, точное сопоставление сходств, расширенные возможности поиска, аналитика в реальном времени, адаптивность и многое другое.

В результате векторные базы данных находят применение в различных областях, от распознавания речи, выявления мошенничества и анализа настроений до систем поиска и рекомендаций по изображениям и тексту.

Растущая ценность векторных вложений и передовых процессов математического поиска стимулировала внедрение векторного поиска для преобразования области поиска информации. Генерация и поиск векторов могут быть независимыми процессами, но, когда они работают вместе, их потенциал безграничен.

Хотя векторные базы данных показали свою эффективность при обработке и поиске векторов, важно взвесить все за и против, прежде чем переходить к

какой-либо технологии. Интеграция векторов в традиционные базы данных может предложить промежуточное решение, сочетающее в себе лучшее из обоих миров. Однако необходимы дополнительные исследования и разработки для достижения оптимального решения, адаптированного к конкретным потребностям каждого приложения.

Список источников

1. «HAKES / Эффективный поиск данных с помощью векторов встраивания в больших масштабах». 8 марта 2025 года.
2. "Векторный тип данных и функции векторного сходства — общедоступны". Snowflake. 2024-05-17.
3. "Векторная база данных". learn.microsoft.com. 26 декабря 2023. Получено 2024-01-10.

УДК 330

ГЛАВА 10. КИБЕРБЕЗОПАСНОСТЬ. РИСКИ КРИПТОВАЛЮТНОГО ОБРАЩЕНИЯ

Аменицкий Алексей Владимирович
аспирант
Санкт-Петербургский государственный электротехнический университет ЛЭТИ имени В.И. Ульянова (Ленина)

Научный руководитель: Воробьёв Евгений Германович
д.т.н., профессор
Санкт-Петербургский государственный электротехнический университет ЛЭТИ имени В.И. Ульянова (Ленина)

Аннотация: Если вы слышали о криптовалюте, то, вероятно, слышали и о криптовалютных аферах. Децентрализованные технологии меняют финансовый ландшафт. К сожалению, стремительные инновации, постоянно меняющаяся нормативно-правовая база и сложный характер отрасли привлекают множество мошенников, работающих с цифровыми активами.
Тем не менее, криптовалюта сама по себе не является мошенничеством. Её потенциал для получения прибыли и технологические лазейки могут привлекать злоумышленников, но существует множество законных возможностей. Быть в курсе криптовалютных мошенничеств — отличный способ защитить себя от них.
Ключевые слова: Cyber Security (CS), CS architecture, CS framework, CS trends, CS tendences, CS tools, CS crimes, CS latest news, CS releases, CS game-changers, CS future, CS playbook, CS agenda, CS future, CS risks, CS incidents, CS resilience, Hackers, PenTest, CS прогноз, CS Landscape, Cyber Intelligence, Artificial Intelligence, Deep Fakes, OWASP, Website security, Cloud Security, CryptoScams, CryproJacking, CryptoFraud, NFT scams, Antifraud, Incident response, CISO PlayBook, Dark Web, Deep Web, Shadow Web, Dark Net, Hacking AI, CSPM, DSPM, Эволюция киберУгроз, КиберГигиена.

CYBERSECURITY. RISKS OF CRYPTOCURRENCY CIRCULATION

Amenitsky Alexey Vladimirovich

Scientific supervisor: Vorobyov Evgeny Germanovich

Инвестиции в криптовалюту могут стать хорошей возможностью, но остерегайтесь ловушек. Цифровые активы сами по себе не являются мошенничеством, но они могут привлекать мошенников из-за своей сложности и потенциального дохода. Существуют криптоверсии классических мошеннических схем, таких как фишинг, схемы Понци и манипуляции с «накачкой и сбросом».

Мошенничество с криптовалютой — это мошенническая схема, которая направлена на то, чтобы обманом заставить вас (инвестора-частника или орга-

низацию) расстаться с вашими цифровыми активами. Мошенничество с криптовалютой может принимать самые разные формы и часто играет на таких эмоциях, как страх или жадность.

Мошенничество с криптовалютой в некотором роде уникально из-за зарождающегося характера этой отрасли. Технология блокчейн настолько нова и сложна, что многие люди недостаточно хорошо её понимают, чтобы защититься от мошенников. Кроме того, транзакции в блокчейне считаются анонимными, что делает криптовалюту ещё более привлекательной для злоумышленников.

Почему криптоиндустрия подвержена мошенничеству?

Те же факторы, которые делают криптовалюту такой привлекательной и обладающей таким большим потенциалом в реальном мире, являются источниками её самых больших рисков:

- Конфиденциальность. Транзакции в блокчейне являются псевдонимными, то есть их можно отследить до цифровых кошельков, но не обязательно до конкретных людей.
- Необратимость транзакций. Транзакции в блокчейне, даже незаконные, как правило, нельзя отменить.
- Регулирование криптовалют Отсутствие регулирования. отсутствует в большинстве юрисдикций. Там, где регулирование слабое или отсутствует, мошенники могут действовать безнаказанно.
- Технологическая сложность. Многие держатели криптовалют плохо разбираются в технологии блокчейн, потому что она очень сложная. Этот пробел в знаниях может создать возможности для тех, кто хочет лишить вас ваших монет.
- Потенциал высокой доходности. Инвесторов, стремящихся быстро разбогатеть, могут привлекать рискованные цифровые активы. Жадность иногда затуманивает разум инвесторов, делая их более восприимчивыми к предложениям, которые кажутся слишком хорошими, чтобы быть правдой.
- Быстрорастущая отрасль. Быстрый рост криптовалют как класса активов и отрасли затрудняет отслеживание новых участников рынка. Инвесторам бывает сложно отличить законные возможности от хитроумных мошеннических схем.

Мошенничество с криптовалютой может принимать самые разные формы. Знание всех способов кражи цифровых активов — отличный способ снизить риск стать жертвой. Рассмотрим наиболее распространённые виды мошенничества в криптосфере.

1. Поддельные ICO (Initial Coin Offering)

Фальшивое первичное размещение монет (ICO) имеет все признаки настоящего ICO, но не имеет поддерживающих технологий или инфраструктуры. Другими словами, это похоже на выпуск монеты, которая существует только на бумаге.

Цель настоящего ICO — впервые представить общественности новую криптовалюту в расчёте на то, что разработчики монеты используют выручен-

ные средства для поддержки криптовалютной сети. Фальшивое ICO заканчивается тем, что разработчики исчезают с вырученными средствами, и выясняется, что всё это было обманом.

Например, Centra Tech была поддельной ICO-компанией, стоимость которой составляла 25 миллионов долларов. Мошенники утверждали, что предлагают криптовалютную дебетовую карту, поддерживаемую Visa (V) и Mastercard (MA), и даже получили одобрение чемпиона по боксу Флойда Мейвезера и музыкального продюсера DJ Khaled. Позже выяснилось, что партнёрство с Visa и Mastercard было поддельным.

2. Фальшивые кошельки

Мошенники, использующие поддельные кошельки, обманом заставляют пользователей поверить, что они используют законный цифровой кошелек для хранения своих активов. Поддельный кошелек запрашивает у пользователей их приватные ключи — информацию, которой, кстати, ни в коем случае нельзя делиться, — а затем мошенники используют эти приватные ключи для кражи криптовалютных активов пользователей. Поддельные приложения-кошельки могут находиться в магазинах приложений или рекламироваться с помощью фишинговых электронных писем.

Поддельная версия цифрового кошелька Trezor в магазине Google Play затронула многих пользователей. Trezor — известный производитель аппаратных кошельков, и поддельный кошелек был убедительно оформлен как мобильное приложение Trezor.

3. Крипто-финансовые пирамиды

Криптовалютная схема Понци — это схема, которая предлагает высокую доходность за счёт привлечения капитала новых инвесторов для выплаты обещанных доходов. Как и традиционные схемы Понци, криптовалютные схемы Понци вводят инвесторов в заблуждение, заставляя их верить, что законная деятельность обеспечивает доходность инвестиций.

Bitconnect — пример криптосхемы Понци. Мошенническая платформа обещала доходность на биткоинах до 40% в месяц, требуя от инвесторов обмена своих биткоинов на собственные монеты платформы. Платформа была разоблачена как схема Понци, когда перестала работать.

4. Фишинговые и социально-инженерные атаки

Атака с использованием социальной инженерии побуждает людей раскрывать конфиденциальную информацию или выполнять действия, которые могут дать мошенникам доступ к вашим криптовалютам. Фишинг с целью получения конфиденциальной информации, такой как имена пользователей, пароли или личные ключи, путём притворства заслуживающим доверия лицом — это разновидность атаки с использованием социальной инженерии.

Фишинговые атаки, нацеленные на держателей криптовалют, могут принимать форму поддельных электронных писем, сообщений или веб-сайтов. Еще одна точка входа для мошенников — неправильно написанные URL-адреса. Например, платформа криптовалютной биржи Bittrex.com была злонамеренно

клонирована мошенниками, которые просто нацеливались на всех, кто по ошибке заходил на «Bilttrex.com».

5. Схемы откачки и слива

Мошенник, использующий схему «накачка и сброс», применяет различные тактики для искусственного завышения (или «накачки») цены цифрового актива. После завышения цены мошенник немедленно продаёт («сбрасывает») свои токены на открытом рынке. Быстрое увеличение предложения токенов приводит к резкому падению их цены, но не раньше, чем мошенник получит прибыль.

Мошенники могут повысить цену дешевого токена, делая ложные или вводящие в заблуждение заявления и одновременно покупая большое количество токенов. GIZMOcoin — пример ранней схемы «накачка и сброс», в которой использовалась такая комбинация тактик.

6. Мошенничество с облачным майнингом

Предоставление услуг облачного майнинга, также известного как майнинг как услуга, является законным бизнесом, но некоторые компании, предлагающие услуги облачного майнинга, являются мошенниками. Компания может заявлять, что предлагает услуги облачного майнинга, возможно, обещая привлекательно высокую прибыль в обмен на предоплату. Обещанная прибыль может так и не поступить, поскольку у компании нет оборудования для майнинга.

Мошенничество с облачным майнингом — это, по сути, разновидность криптосхемы Понци. В качестве примера можно привести HashOcean, который не владел криптоинфраструктурой, но выплачивал щедрый бонус за регистрацию, чтобы привлечь новых участников.

7. Криптоджекинг

Криптоджекеры — это мошенники, которые тайно используют ваше вычислительное устройство для майнинга криптовалют без вашего ведома. Майнинг криптовалют, таких как биткоин, требует больших затрат энергии и вычислительных ресурсов. Криптоджекеры стремятся получить все преимущества майнинга криптовалют без каких-либо затрат, в то время как вы остаётесь с устройством, которое потребляет много энергии и работает плохо.

Посещение заражённого веб-сайта или загрузка взломанного программного обеспечения могут привести к тому, что ваш компьютер или телефон получит вредоносный код от криптоджекера. Некоторые пользователи популярного веб-плагина Adobe Flash ранее становились жертвами мошенников, которые распространяли поддельное обновление, тайно устанавливающее программное обеспечение для майнинга.

8. Атаки с использованием блокчейна

Мошенники могут атаковать как отдельных держателей криптовалют, так и целые блокчейны. Вот некоторые из наиболее распространённых типов атак, затрагивающих целые криптовалютные сети:

- Атаки 51%, которые происходят, когда одна организация получает контроль более чем над половиной вычислительной мощности блокчейна или криптовалюты.

- Атаки Сивиллы происходят, когда один субъект создаёт множество поддельных учётных записей (узлов), чтобы злонамеренно влиять на работу сети.
- Атаки на маршрутизацию предполагают, что злоумышленник манипулирует информацией о маршрутизации данных, чтобы перехватить, изменить или заблокировать связь между узлами блокчейна.
- Атаки с подменой времени происходят, когда злоумышленник изменяет временные метки узлов сети, что приводит к путанице и потенциально позволяет злоумышленнику потратить криптовалюту дважды.
- Атаки «затмение» происходят, когда мошенники изолируют один или несколько узлов блокчейна с целью предоставления изолированному узлу ложной информации.
- Атаки на большом расстоянии — это теоретический тип атак, при которых мошенники создают новую ветку блокчейна из далёкого прошлого, пытаясь сделать мошеннические транзакции легальными.
- Атаки с целью майнинга происходят, когда майнеры успешно обрабатывают новый блок, но не передают эту информацию в сеть, что позволяет им тайно начать майнить следующий блок. Такая атака пока не наблюдалась, но теоретически она возможна.

Рекомендации, позволяющие избежать криптовалютного мошенничества

- Прежде чем инвестировать, проведите тщательную проверку. Изучите криптовалюту, её технологию, команду и многое другое.
- Оцените присутствие криптовалюты в интернете. Ищите сильное цифровое присутствие и избегайте анонимных проектов.
- Оцените соответствие криптовалюты законодательству. Дайте консервативную оценку законности проекта в соответствующих юрисдикциях.
- Остерегайтесь нереалистичных обещаний. Не доверяйте предложениям, которые кажутся слишком хорошими, чтобы быть правдой.
- Используйте проверенные платформы. Используйте только продукты и услуги надежных лидеров отрасли.
- Защитите свои личные данные. Соблюдайте правила безопасного просмотра веб-страниц и никогда не делитесь своими личными ключами.
- Будьте в курсе изменений в отрасли. Защитите себя, следя за развитием мошенничества.
- Если вам нужна помощь, обратитесь за ней. Воспользуйтесь услугами финансовых специалистов, чтобы избежать дополнительных подводных камней.

Регулирование криптовалюты

Криптовалюта -это развивающийся класс активов, который непоследовательно регулируется. Юрисдикции по всему миру устанавливают очень разные правила для криптовалют. Многие сторонники криптовалюты выступают за большее и более совершенное регулирование.

Нормативно-правовое регулирование криптовалют — это правовые и процедурные нормы, которые правительства вводят для регулирования различных

аспектов цифровых активов. Нормативно-правовое регулирование криптовалют в разных юрисдикциях может варьироваться от подробных правил, разработанных для поддержки пользователей блокчейна, до полного запрета на торговлю или использование криптовалют.

Правила обращения с цифровыми активами могут регулировать создание, покупку, продажу и обмен цифровых денег. Законодатели или государственные органы также могут определять, как именно цифровые активы интегрируются в существующие финансовые системы.

Для процветания криптовалют и их массового распространения необходимы чёткие и понятные правила. Вот чего может добиться качественная нормативно-правовая база для криптовалютного сектора:

- Обеспечить защиту инвесторов от рыночных манипуляций и криптомошенничества.
- Убедитесь, что инвесторы всегда получают необходимую и точную информацию.
- Сдерживать незаконную деятельность, такую как отмывание денег и финансирование терроризма.
- Внесите ясность в правила налогообложения криптовалют.
- Стимулируйте расширение участия на рынке за счет повышения доверия инвесторов.
- Поощряйте компании к инновациям с помощью технологии блокчейн.
- Облегчение взаимодействия между блокчейнами.
- Снизьте системный риск за счет усиления отраслевого надзора.
- Продвигайте инклюзивность, делая криптовалюты доступными для большего числа людей.

Как регулируется криптовалюта

Нормативно-правовая база для криптовалют чётко не определена и постоянно меняется. Разные федеральные агентства по-разному относятся к цифровым активам, исходя из собственных оценок характеристик криптовалют. Законодатели тоже могут высказываться по этому поводу, а регионы могут устанавливать собственные правила.

Комиссия по ценным бумагам и биржам (SEC), Комиссия по торговле товарными фьючерсами (CFTC) и Служба внутренних доходов (IRS) по-разному трактуют криптовалюты:

SEC: Криптовалюты - это ценные бумаги. SEC хочет классифицировать цифровые активы как ценные бумаги. Агентство заботится о защите инвесторов и требует, чтобы все предложения, которые квалифицируются как “инвестиционные контракты”, были официально зарегистрированы. SEC в 2023 году использует подход принудительного регулирования, подавая крупные судебные иски против таких компаний, как Coinbase. В 2024 году SEC одобрила биржевые фонды Биткоина и Эфириума (ETF).

CFTC: криптовалюты — это товары. CFTC утверждает, что криптовалю-

ты — это товары, подобные нефти или золоту. Агентство определяет товары как активы, которые могут служить основой для фьючерсных контрактов, и уже регулирует активный рынок криптовалютных фьючерсов. Агентство инициировало принудительные меры в отношении незарегистрированных бирж криптовалютных фьючерсов.

Налоговая служба: криптовалюты являются собственностью. Налоговая служба классифицирует цифровые активы как собственность. Такая классификация цифровых активов означает, что каждая продажа, обмен или покупка с использованием криптовалюты потенциально облагаются налогом, и применяются ставки налога на прирост капитала. Налоговая служба начала рассматривать криптоактивы как собственность в 2014 году.

Глобальные правила и подзаконные акты в отношении криптовалют

В разных странах мира действуют различные правила в отношении цифровых валют. Вот некоторые страны, которые лидируют в сфере регулирования криптовалют:

Канада регулирует платформы для торговли криптовалютой, требуя регистрации в провинциальных агентствах. Криптовалютные инвестиционные компании классифицируются как предприятия, предоставляющие финансовые услуги, а криптовалюта облагается налогом как другие товары. Канада разрешает криптовалютным биржевым фондам работать на фондовой бирже Торонто.

Великобритания регулирует деятельность компаний, работающих с цифровыми активами, но, как правило, не устанавливает правила для самих криптовалют. Управление по финансовому регулированию и надзору следит за тем, чтобы криптовалютные компании соблюдали передовые методы предотвращения отмывания денег и финансирования терроризма, а Управление по стандартам рекламы стремится регулировать рекламу криптовалют. В UK криптовалюта рассматривается как актив для целей налогообложения.

Швейцария. Эта альпийская страна придерживается весьма прогрессивного подхода к регулированию криптовалют. В 2020 году законодатели приняли закон о технологиях распределённого реестра (DLT), введя понятие «ценные бумаги DLT» и разрешив токенизацию прав, требований и финансовых инструментов. Налогоплательщики в Швейцарии могут облагаться подоходным налогом или налогом на богатство в зависимости от своих криптовалютных активов.

Сальвадор. Эта центральноамериканская страна выделяется тем, что является единственной страной, объявившей биткоин законным платёжным средством. Биткоин можно использовать по всей стране; фактически, его приём продавцами является обязательным. Сальвадор принимает налоговые платежи в биткоинах и освобождает иностранцев от уплаты налогов на доходы от продажи биткоинов.

Риски регулирования цифровых активов

Многие участники криптовалютной индустрии решительно выступают за усиление контроля, но это не значит, что регулирование криптовалют не имеет недостатков. К основным рискам относятся:

- Регулирование может ограничивать доступ к рынку. Усиление регулирования криптовалют может привести к тому, что некоторые инвесторы будут иметь ограниченный доступ к криптовалютам или другим цифровым активам.
- Криптовалютные правила могут сдерживать инновации. Строгие правила и требования к соблюдению законодательства могут замедлять или препятствовать развитию блокчейн-инноваций.
- Регулирование может создавать проблемы с правоприменением в разных юрисдикциях. Если каждый законодательный орган и государственное учреждение устанавливает собственную политику в отношении криптовалют, соблюдение всех этих правил может стать чрезвычайно сложным.
- Регулирование криптовалют может увеличить стоимость ведения бизнеса. Соблюдение правил, касающихся криптовалют, может означать расходы на дополнительную инфраструктуру или трудоёмкие процессы соблюдения требований.
- Законы о криптовалютах обязывают участников рынка быть в курсе изменений в правилах. Участникам криптовалютного рынка необходимо понимать действующие правила, а также быть в курсе изменений в политике.
- Чем больше правил, тем сильнее они влияют на финансовые показатели криптовалют. Обширное регулирование криптовалютной индустрии может увеличить стоимость хранения цифровых активов и тем самым снизить их стоимость.

Регулирование криптовалют может повысить уровень защиты инвесторов, предотвратить незаконную деятельность и способствовать массовому внедрению цифровых активов. Что плохо, так это отсутствие ясности в регулировании, сложные правила и регулирование с помощью правоохранительных органов. Необходимо следить за развитием отрасли, поскольку нормативно-правовая база неизбежно будет меняться.

Цифровые валюты

Цифровые валюты можно использовать множеством инновационных способов. Многие из этих вариантов использования напрямую влияют на развитие современной финансовой системы. Варианты использования криптовалют варьируются от более эффективных способов оплаты и других традиционных финансовых функций до совершенно новых функций, основанных на криптовалютах. Вот девять способов использования криптовалют в личных и профессиональных финансах, но убедитесь, что вы понимаете риски, присущие этому новому классу активов.

Многие из наиболее популярных вариантов использования криптовалют направлены на преобразование традиционных банковских систем и систем финансовых транзакций. Другие варианты использования криптовалюты являются родными для сред, основанных на блокчейне. Хотя некоторые варианты использования криптовалют могут быть революционными, технология криптовалют и блокчейна ещё не получила широкого распространения.

Изучая многочисленные потенциальные варианты использования крипто-

валют, нельзя забывать, что мы всё ещё работаем в рамках «идеального сценария». Криптоприложения могут произвести революцию в финансовой системе, но для их полноценного внедрения необходим один важный элемент: широкое распространение.

С внедрением приходит «полезность» (она же утилитарность), рыночная стоимость и, в конечном счёте (или, будем надеяться, в конечном счёте), стабильная форма денежной стоимости. Если и когда это произойдёт, мы можем ожидать, что криптовалюты повлияют на смену глобальной финансовой парадигмы.

Рассматривая эти интересные варианты использования, помните, что они зависят от будущего, в котором криптовалюты станут не просто спекулятивными активами, а неотъемлемой частью нашей финансовой жизни.

Ключевые рекомендации

1. Эффективно отправляйте деньги через границы

Как правило, криптовалютой может владеть и пользоваться любой человек, что делает её популярным вариантом для тех, кто поддерживает членов семьи в других странах. В криптовалютных транзакциях используется технология блокчейн, которая делает трансграничные платежи более эффективными — простыми, быстрыми и даже дешёвыми.

Разработчики платёжных технологий P2P поддерживают денежные переводы на основе блокчейна, разрабатывая приложения, которые позволяют людям по всему миру получать криптовалюту и конвертировать её в местные деньги. Немедленная конвертация — один из способов минимизировать риски, связанные с нестабильными колебаниями цен, которые характерны для большинства криптовалют.

2. Чаевые напрямую

Вы когда-нибудь хотели отблагодарить за отличную работу, которую нашли в интернете? С помощью криптовалюты можно совершать микроплатежи вашим любимым авторам. Многие блокчейны имеют чрезвычайно низкие комиссии за обработку транзакций, что позволяет напрямую давать чаевые без лишних затрат. Например, Brave — это браузер на основе блокчейна, который позволяет авторам напрямую получать вознаграждение от своей аудитории. Gitcoin — это платформа, которая позволяет разработчикам получать чаевые за вклад в проекты с открытым исходным кодом. Таким образом, криптовалюта помогает цифровым чаевым стать более надёжным источником дохода для авторов.

3. За покупками

Как правило, криптовалюту можно использовать для электронной коммерции, часто с помощью цифровых кошельков. Продавцы могут принимать криптовалюту напрямую или косвенно через поставщика услуг. Компании, принимающие криптовалютные платежи, могут сделать свои товары и услуги доступными для клиентов по всему миру и снизить транзакционные издержки. Компании также могут использовать криптовалюту для выплаты вознаграждений, которые обычно предназначены для повышения лояльности клиентов.

Впечатляющее количество компаний уже принимают одну или несколько криптовалют, в том числе:

- Корпорация Майкрософт (MSFT)
- PayPal (PYPL)
- Starbucks (SBUX)
- Overstock.com, Inc. (OSTK)
- AT&T (T)

4. Совершайте транзакции напрямую с коллегами

Одним из основных вариантов использования криптовалюты является децентрализация устаревшей финансовой системы. Технология блокчейн позволяет осуществлять децентрализованные финансы (DeFi), поддерживая одноранговые финансовые транзакции различной сложности. Использование криптовалюты для совершения сделок, получения займов и кредитования напрямую между одноранговыми узлами — без централизованного посредника — является важным нововведением в существующей финансовой системе. Совершение сделок таким образом также сопряжено с уникальными, а иногда и непредвиденными рисками, которые, как правило, не связаны с инвестированием в традиционные регулируемые ценные бумаги.

Самые оптимистично настроенные пользователи криптовалют считают, что одноранговые транзакции — это эффективный способ демократизировать современные денежные системы. Критики указывают на проблемы, связанные с неправомерными действиями, мошенничеством и неплатёжеспособностью платформ. Инициативы DeFi часто структурируются как DAO — децентрализованные автономные организации, которые используют консенсус для принятия решений, в отличие от традиционных денежных систем, которые полагаются на центральные банки и политиков, отвечающих за денежную стабильность.

5. Тратьте и зарабатывайте цифровую валюту

Криптовалюту можно заработать и использовать для проведения транзакций в экосистеме блокчейна. В каждом автономном блокчейне есть собственная криптовалюта, и многие блокчейн-проекты, построенные на основе других блокчейнов, таких как Ethereum, поддерживают собственные криптовалюты. Decentraland — это блокчейн-платформа с собственной криптовалютой MANA, которая позволяет покупать виртуальную землю, товары и услуги. Геймеры могут зарабатывать и использовать криптовалюту во многих своих любимых играх, при этом их криптоактивы часто можно переносить между игровыми средами.

Другие блокчейны, которые позволяют пользователям напрямую тратить и зарабатывать криптовалюту, включают:

- Filecoin: эта блокчейн-сеть позволяет пользователям предоставлять и использовать децентрализованное хранилище данных с помощью токена FIL.
- Axie Infinity: эта основанная на блокчейне игра в жанре «торги и сражения» позволяет игрокам зарабатывать и тратить криптовалюту AXIE, собирая, разводя, выращивая и продавая внутриигровых существ, известных как Акси.

- Helium: эта открытая децентрализованная сеть для устройств Интернета вещей (IoT) позволяет пользователям зарабатывать криптовалюту, предоставляя услуги покрытия сети IoT и передачи данных.

6. Поддержка блокчейн-сети

У держателей криптовалют есть множество способов участвовать в работе блокчейн-сети, которые выходят за рамки простых транзакций. Пользователи криптовалют могут принимать полноценное участие в управлении блокчейном, помогать обеспечивать безопасность сети и подтверждать транзакции в блокчейне. Способность держателя криптовалюты участвовать в работе блокчейн-экосистемы часто напрямую связана с количеством криптотокенов, которыми он владеет.

Другой популярный способ участия в блокчейн-сети — это стейкинг, то есть согласие не торговать и не продавать свои криптоактивы в обмен на возможность получать проценты (в виде криптовалюты). Стейкинг может приносить привлекательную прибыль, но этот вариант использования криптовалюты по-прежнему рискован. Инвесторам нужно быть готовыми к колебаниям цен на криптовалюту и ликвидности платформы для стейкинга.

7. Конфиденциальность транзакций

Многие блокчейны известны тем, что повышают прозрачность финансовых транзакций, но криптовалюту также можно использовать для повышения конфиденциальности транзакций. Максимальная конфиденциальность финансовых транзакций может снизить риск мошенничества и кражи личных данных, защитить активистов и журналистов, а также обеспечить конфиденциальность операций для бизнеса. Dash, Monero и Zcash — примеры криптовалют, которые ставят конфиденциальность пользователей на первое место. Но есть и обратная сторона: повышенная конфиденциальность может усложнить выявление незаконных транзакций.

8. Максимизация заработков с помощью yield farming

Вы слышали о майнинге доходности? Эта стратегия децентрализованного финансирования с высоким уровнем риска, также известная как майнинг ликвидности, позволяет пользователям получать максимальный процентный доход от своих криптовалютных активов. Майнеры доходности используют смарт-контракты — контракты на основе блокчейна, которые могут выполняться автоматически, — чтобы постоянно переводить свои криптоактивы в сети блокчейна, где выплачиваются самые высокие процентные ставки.

Фермерство доходности считается рискованным. Смарт-контракты могут работать некорректно, и фермеры доходности подвержены рискам ликвидности, колебаниям процентных ставок и волатильности цен на криптовалюту. Фермерство доходности возможно на нескольких блокчейн-платформах, в том числе:

- SushiSwap
- AAVE
- Curve Finance

- Convex Finance
- Harvest Finance
- Alpaca Finance

9. Заработная плата

Другой способ использования криптовалюты - выплачивать заработную плату сотрудникам и подрядчикам. Компании с глобальными командами или владеющие большими объемами криптовалюты могут рассматривать этот способ оплаты как привлекательный вариант. Сотрудники могут использовать криптовалюту или конвертировать цифровые платежи в свою местную валюту. Примечание: Сотрудникам, получающим криптовалюту в качестве заработной платы, возможно, потребуется получить рекомендации относительно налоговых последствий.

Выплата заработной платы в криптовалюте, как правило, более распространена среди компаний, работающих в сфере блокчейна. BitPay — пример поставщика услуг по выплате заработной платы, который позволяет компаниям из всех отраслей платить криптовалютой.

Первая волна использования криптовалют была направлена на замену и/или упрощение финансовых транзакций и других традиционных банковских функций. Похоже, что сфера применения криптовалют расширяется. Но хотя эффективность и расширение возможностей — особенно на индивидуальном уровне — являются достойными целями, любое масштабное изменение статус-кво встретит сопротивление со стороны тех, кто черпает свою власть из этого статус-кво. Тем не менее, технологические инновации исторически были мощным двигателем глобального роста.

Является ли криптовалюта разновидностью денег?

Криптовалюты — это цифровые активы, которые используют зашифрованную сеть для выполнения, проверки и записи транзакций независимо от централизованного органа, такого как правительство или банк. Криптовалюта была разработана как альтернатива доллару, и её функции могут сделать её привлекательной инвестицией. Блокчейн- базовая технология, лежащая в основе криптовалют, считается революционной. Как и в случае с инвестициями в доткомы в 1990-х, криптовалюта может быть перспективной, но, скорее всего, будут победители и проигравшие.

Это сложная концепция, поэтому рассмотрим ее подробнее:

- Криптовалюты (или сокращённо «крипто») — это децентрализованные валюты, то есть они не выпускаются и не регулируются центральным банком. Некоторые криптовалюты выпускаются их разработчиками, а другие генерируются соответствующими сетевыми алгоритмами.
- Криптовалюты — это цифровые активы, они не имеют материальной формы.
- Криптовалюты существуют и работают на основе публичного реестра, называемого блокчейном, в котором фиксируются все криптовалютные транзакции.

- Шифрование блокчейна предназначено для того, чтобы сделать все транзакции неизменяемыми и защищёнными от взлома, подделки и других видов мошеннических транзакций.

Хотя криптовалюта определяется как форма «цифровой валюты», подразумевающая, что это своего рода деньги, большинство компаний и потребителей не используют её в качестве общепринятого средства обмена. Другими словами, большинство магазинов не принимают криптовалюту в качестве платёжного средства.

Биткоин может быть исключением, поскольку некоторые компании принимают его в качестве оплаты товаров и услуг. Итак, если криптовалюта не является распространённой формой денег, почему люди её покупают-

- Это альтернативный класс активов. Хотя некоторые криптоинвесторы надеются, что криптовалюты когда-нибудь станут формой денег, большинство рассматривает их как альтернативный актив, стоимость которого может расти.
- Это способ инвестировать в технологию блокчейн. Некоторые люди покупают криптовалюту, чтобы косвенно инвестировать в лежащий в её основе блокчейн.

Блокчейн

Блокчейн — это зашифрованная общедоступная база данных, с помощью которой можно передавать, регистрировать и хранить цифровые активы. По сути, это децентрализованная сеть, также называемая технологией распределённого реестра (DLT). Это означает, что нет единого органа, который бы контролировал или упрощал транзакции внутри сети.

Вместо этого перед компьютерами, участвующими в сети, ставится задача проверять и подтверждать каждый «блок» (то есть запись или транзакцию) в цепочке. В некоторых случаях все компьютеры работают вместе, чтобы проверять и подтверждать каждое действие блока. В других случаях группа компьютеров выбирается случайным образом. Именно это делает транзакции в блокчейне безопасными и практически невозможными для изменения. Десятки тысяч компьютеров должны подтвердить одну транзакцию или запись. Если между компьютерами возникает разногласие, транзакция будет отменена. Эта процедура проверки также может замедлять транзакции в блокчейне и снижать энергоэффективность. Множество компьютеров по всему миру работают над проверкой каждой транзакции.

Блокчейн использует шифрование для защиты конфиденциальных данных от тех, кто не имеет права их получать. Например, общественность может видеть, что транзакция была совершена или информация была записана. Но она не может видеть личности участников транзакции или, в некоторых случаях, её содержимое.

Почему блокчейн считается технологическим разрушителем?

Способность блокчейна постоянно записывать и хранить записи о транзакциях и информацию в условиях высокой степени безопасности делает его привлекательной технологией для многих компаний и правительств. Вот краткий

список потенциальных вариантов использования блокчейна:

HODL

HODL — это сленговое выражение, используемое в криптовалютной сфере и означающее долгосрочное владение криптовалютными монетами или токенами. Оно появилось из-за опечатки в сообщении 2013 года под названием «I HODL», опубликованном на криптовалютном форуме BitcoinTalk.

В случае с криптоактивами фундаментальные показатели, такие как коэффициент P/E, дивидендная доходность или доходность к погашению, не применяются. Вместо этого HODL-инвесторы могут инвестировать в «дефицитную стоимость» ограниченного количества криптовалют, таких как биткоин, — аналогично тому, как инвесторы рассматривают золото и драгоценные металлы как активы, которые могут сохранять свою ценность в условиях инфляции.

HODL-инвестирование включает-

- Внутренние и международные платежи
- Контракты
- Записи о медицинском обслуживании
- Сделки с недвижимостью
- Энергетические операции
- Управление цепочкой поставок
- Транзакции с цифровыми произведениями искусства (Невзаимозаменяемые токены или NFT)
- Голосование

Кроме того, блокчейн - это сеть с открытым исходным кодом. Это означает, что разработчики могут работать автономно над улучшением его функций. Чем эффективнее становится экосистема блокчейна, тем проще корпорациям и правительствам внедрять её в свою повседневную деятельность.

Наиболее популярные типы криптовалют

Среди более чем 18 000 существующих криптовалют биткоин и эфириум являются двумя крупнейшими криптовалютами по рыночной капитализации. Биткоин, первая и крупнейшая криптовалюта, был разработан в 2009 году как альтернативный денежный актив. Он должен был стать альтернативой доллару и другим фиатным валютам. Хотя некоторые продавцы могут принимать биткоин в качестве оплаты, большинство инвесторов рассматривают его как спекулятивную инвестицию.

Ethereum — вторая по величине криптовалюта по рыночной капитализации. В отличие от биткоина, Ethereum был создан не только как альтернативный денежный актив. Вместо этого он был разработан как инновационная технология ведения реестра, которая помогает компаниям безопасно передавать данные, хранить данные и создавать новые программы и приложения. Короче говоря, Ethereum — это огромная цифровая экосистема, с помощью которой можно передавать, хранить и даже создавать цифровую информацию и компьютерные приложения.

Цели криптовалюты

Некоторые криптовалюты, такие как биткоин и Tether, были разработаны для выполнения денежной функции. Другие, такие как Dogecoin и Shiba Inu, считаются «мемными монетами», разработанными как новинки, ценность которых зависит от популярности и торговли.

Многие, если не большинство, криптовалют были разработаны для решения проблем в экосистеме блокчейна, таких как скорость передачи данных, масштабируемость, безопасность, энергоэффективность и рентабельность.

Инвестиции в криптовалюту

Можно приобрести криптовалюту на криптовалютной бирже или в любом финансовом учреждении, которое может выступить посредником в криптовалютной сделке. После покупки криптовалюты вы можете хранить свои монеты в цифровом кошельке, онлайн-кошельке или аппаратном кошельке.

Риски инвестирования в криптовалюту

Вот несколько наиболее распространенных рисков при инвестициях в криптовалюту:

- Риск волатильности. Цены на криптовалюту часто демонстрируют резкие колебания в определенных экономических или рыночных условиях.
- Риск ликвидности. Некоторые криптовалюты торгуются с небольшим объёмом и, таким образом, могут быть легко манипулированы покупателями с большими капиталами или продавцами, у которых есть крупная доля в данной валюте.
- Риск для кибербезопасности. Ваша криптовалюта может быть украдена, если злоумышленник получит доступ к закрытому ключу вашего криптокошелька.
- Риск в течение ночи. Поскольку криптовалюта торгуется 24 часа в сутки 7 дней в неделю, ваши активы подвержены неблагоприятным колебаниям в течение ночи.
- Исчезающий риск. Существуют факторы, которые привели к исчезновению некоторых криптовалют; такие случаи редки и уникальны для конкретных криптовалют.

Хотя изначальная идея криптовалюты заключалась в создании альтернативного денежного актива, многие инвесторы покупают криптовалюту не как деньги, а как альтернативный актив или способ инвестировать в лежащую в её основе технологию блокчейн. Криптовалюта — развивающаяся сфера, не похожая на технологический сектор 1990-х годов. В мире криптовалют есть множество блестящих идей, но не каждая инновация в сфере блокчейна найдёт широкое применение. Поэтому, если вы планируете инвестировать в криптовалюты, будьте осторожны.

Децентрализованные финансы. Decentralized finance (DeFi)

Если вы можете представить, что отправляете деньги, совершаете платёж или покупаете финансовый актив без помощи банка, брокера или другого официального посредника, то вы понимаете суть децентрализованных финансов.

Децентрализованные финансы, или сокращённо DeFi, — это развивающаяся цифровая экосистема, которая позволяет людям отправлять, покупать и обменивать финансовые активы, не полагаясь на банки, брокерские компании или биржи. DeFi позволяет обходить традиционные способы совершения финансовых операций.

Рассмотрим особенности DeFi

- Децентрализованные финансы (DeFi) обходят традиционные способы проведения финансовых операций.
- Одноранговая экосистема на основе блокчейна может произвести революцию в банковской сфере, какой мы её знаем.
- DeFi остается в значительной степени непроверенным, что делает его рискованной инвестицией.
- Появление DeFi может иметь большое значение. Оно не просто указывает на новую форму финансовых технологий, которая вот-вот появится, — оно обещает совершенно новый финансовый горизонт.

Основные преимущества, возможности и риски для пользователей и инвесторов. Почему DeFi (или почему стоит избегать традиционных финансов)?

Децентрализованные финансы, возможно, не привнесут много нового в сферу финансовых продуктов. Но если они получат развитие, это может революционизировать способ обмена финансовыми продуктами. И все же, зачем чинить систему, которая и так эффективна и функционально безопасна — другими словами, зачем чинить то, что не сломалось?

Банки и финансовые учреждения могут помочь перевести средства из одного места в другое, но этот способ не является прямым. Часто существует цепочка сторонних поставщиков услуг, которые помогают выполнить одну транзакцию. Эта цепочка может не только замедлить выполнение данной транзакции, но и взимать плату за обслуживание. А поскольку вы полагаетесь на сторонние сервисы (каждый из которых подвержен человеческим ошибкам, технологическим сбоям, аппаратным сбоям и нарушениям безопасности), ни один из них не является безопасным на 100%.

Частные лица и предприятия всегда ищут более быстрый, безопасный и экономичный способ совершения одноранговых финансовых транзакций (P2P). То, что может предложить DeFi, выходит далеко за рамки постепенных улучшений (в отличие, скажем, от появления банкоматов или прямого внесения депозитов). Это обещает инновации, недостижимые при использовании традиционных систем и технологий.

Принцип работы DeFi

Построив финансовую систему на базе сети, основанной на блокчейне, и устранив посредников, транзакции могут быть более прямыми; плата за обслуживание может быть в значительной степени снижена; а передача активов и обмен ими могут быть практически защищены от несанкционированного доступа.

Блокчейны - это цифровые бухгалтерские книги, которые используются совместно и обновляются всеми участвующими компьютерами (также называ-

емыми узлами). Все транзакции, которые попадают в блокчейн, проверяются выбранными узлами, участвующими в сети. Все блоки зашифрованы, и как только они будут закрыты, содержимое блока будет надежно защищено и не может быть изменено. Любая попытка изменить содержимое блока приведет к оповещению всех компьютеров в сети (число которых может исчисляться тысячами). Это то, что делает блокчейн практически непроницаемым и безопасным.

Сравнивая это с сегодняшней финансовой системой, даже самые эффективные, конкурентоспособные по цене и безопасные банковские процессы не могут предложить таких преимуществ на том уровне, на который способна блокчейн-сеть, по крайней мере, так утверждают сторонники блокчейна.

DeFi может сделать это лучше. Поскольку он использует блокчейн, частные лица и предприятия могут совершать операции с другими типами активов, которые недоступны с помощью традиционных финансовых средств, таких как смарт-контракты и невзаимозаменяемые токены.

Ключевые преимущества и риски для пользователей DeFi

В целом, DeFi предлагает пользователям больше контроля над своими деньгами. Финансовые активы можно переводить или покупать за считанные секунды или минуты. Плата за услуги будет в значительной степени отменена, так как не будет сторонних компаний, помогающих с транзакциями. Ваши деньги будут конвертированы в «стейблкоины, обеспеченные фиатными валютами», и станут доступны через цифровой кошелёк, так что вам не придётся вносить средства в банк. А поскольку банковские счета больше не будут нужны, практически любой человек с подключением к интернету сможет получить доступ к тем же финансовым товарам и услугам.

Самый большой риск заключается в том, что DeFi не регулируется. Нет никакой поддержки со стороны Федеральной корпорации по страхованию вкладов (или какой-либо другой регулирующей организации), которая могла бы защитить ваши средства в случае серьёзного сбоя, ошибки или кибератаки, из-за которых ваши средства станут недоступными или исчезнут.

Кроме того, технология настолько нова, что не существует единого или всеобъемлющего способа определить, работает ли какая-либо часть системы DeFi с оптимальной производительностью или защищена ли она от мошенничества. Теоретически каждый технологический компонент в экосистеме DeFi должен работать быстро, эффективно и безопасно. Однако на практике это ещё не проверено.

Риски инвестиций в DeFi

Самый простой и безопасный способ — инвестировать в акции компаний, которые занимаются разработкой DeFi. Однако многие из этих компаний являются новыми и работают в сфере криптовалют, что делает их более спекулятивными и волатильными, чем более известные компании в зрелых отраслях.

Инвесторы также могут делать ставки на криптовалюту, чтобы инвестировать в экосистему блокчейна DeFi. Ставки позволяют держателям криптовалюты поддерживать сеть блокчейна, блокируя монеты для подтверждения новых

блоков транзакций. Если ваша ставка будет выбрана в процессе подтверждения, вы сможете получать доход в виде дополнительной криптовалюты. Более продвинутая версия этого вида инвестирования называется доходным фермерством, которое предполагает предоставление криптовалюты платформе или операции DeFi в обмен на проценты или дополнительную криптовалюту.

Самым большим риском в сфере DeFi, опять же, является отсутствие правил, защищающих ваши деньги. Это делает вас уязвимыми для мошенничества и краж. Поскольку DeFi — развивающаяся отрасль, вы рискуете инвестировать в проект, который может потерпеть неудачу. Кроме того, криптовалютные рынки очень нестабильны и сложны, что затрудняет оценку как рынка, так и отрасли. Кроме того, технологические сбои, высокое энергопотребление, неисправности оборудования и даже обслуживание и обновление системы — всё это повышает риски в сфере DeFi.

В этом отношении DeFi похож на рынок облигаций. Облигации с самым высоким риском предлагают более высокую доходность в качестве компенсации за этот дополнительный риск. Но если эмитент обанкротится, вы можете потерять свои деньги.

ЗАКЛЮЧЕНИЕ

Любой может стать жертвой мошенника, работающего с криптовалютой. Но знание — сила, и это особенно верно, когда речь идёт о том, как избежать мошенничества с криптовалютой. Можно снизить риск, если быть в курсе распространённых видов мошенничества с цифровыми активами и следовать основным рекомендациям. Необходимо всегда помнить: если что-то кажется слишком хорошим, чтобы быть правдой, то, скорее всего, это признаки мошенничества.

Текущее состояние регулирования криптовалют одновременно непрозрачно и быстро меняется. Если вы инвестируете в криптовалюту, важно понимать существующие правила и быть в курсе того, что может произойти в будущем.

Когда речь идёт о развивающихся отраслях, ранние инвестиции часто могут принести огромную прибыль. Но важно понимать риски, которые могут сравняться с потенциальной прибылью или превысить её. Децентрализованные финансы однажды могут разрушить банковскую систему, какой мы её знаем. Но до тех пор, пока этого не произойдёт, в сфере DeFi будет царить неопределённость и спекуляции. Действуйте с осторожностью.

Список источников

1. Хван, Инён (7 мая 2021 г.). «Что такое криптоджекинг? Как обнаружить вредоносное ПО для майнинга — MediaFeed». mediafeed.org.

2. Хэтмейкер, Тейлор (8 мая 2018 г.). «Вредоносная программа для криптоджекинга тайно добывала Monero на многих правительственных и университетских сайтах». TechCrunch.

3. Каплан, Майкл (13 апреля 2019 г.). «Хакеры крадут миллионы в биткоинах и живут как богачи». New York Post.

4. «Жестокая вредоносная программа для майнинга криптовалют выводит из строя ваш компьютер при обнаружении». ZDNet. 9 декабря 2022 года.

5. «Майнинг-ферма Sandwell, добывающая биткоины, была уличена в краже электроэнергии». BBC News. 2021-05-28.

УДК 62

ГЛАВА 11. АРХИТЕКТУРА МИКРОСЕРВИСОВ И КИБЕРБЕЗОПАСНОСТЬ

Аменицкий Алексей Владимирович
аспирант
Санкт-Петербургский государственный электротехнический университет ЛЭТИ имени В.И. Ульянова (Ленина)

Научный руководитель: Воробьёв Евгений Германович
д.т.н., профессор
Санкт-Петербургский государственный электротехнический университет ЛЭТИ имени В.И. Ульянова (Ленина)

Аннотация: Любая организация, переходящая от монолитной архитектуры к микросервисам, должна быть более гибкой. Микросервисы - это небольшие автономные подразделения, функционирующие независимо. Однако многие такие подразделения работают вместе, формируя приложение. Микросервисы - это выбор для тех, кто часто выполняет сложные и крупные проекты. Микросервисы также способствуют повышению надежности. Следует ли перейти с monolith на архитектуру микросервисов?
В свете этого распределенные компоненты микросервисов должны быть более безопасными. Для достижения этого рекомендации по обеспечению безопасности архитектуры микросервисов должны быть реализованы на разных уровнях. Сам факт наличия нескольких сервисов означает, что в системе имеется множество уязвимых точек. Каждая из этих точек должна быть надежно защищена, чтобы система была надежной.
Ключевые слова: Cyber Security (CS), CS architecture, CS framework, CS trends, CS tendences, CS tools, CS crimes, CS latest news, CS releases, CS game-changers, CS future, CS playbook, CS agenda, CS future, CS risks, CS incidents, CS resilience, Hackers, PenTest, CS прогноз, CS Landscape, Cyber Intelligence, Artificial Intelligence, Deep Fakes, OWASP, Website security, Cloud Security, CryptoScams, CryproJacking, CryptoFraud, NFT scams, Antifraud, Incident response, Dark Web, Deep Web, Shadow Web, Dark Net, Hacking AI, CSPM, DSPM, Эволюция киберУгроз, КиберГигиена.

MICROSERVICES ARCHITECTURE AND CYBERSECURITY

Amenitsky Alexey Vladimirovich

Scientific supervisor: Vorobyov Evgeny Germanovich

Как обезопасить архитектуру микросервисов

Популярность использования архитектуры на основе микросервисов для реализации сложных, развивающихся решений растет. Микросервисы значительно упрощают замену или модернизацию компонентов в процессе эксплуа-

тации. Это также позволяет нескольким разработчикам работать над различными аспектами общего решения, не влияя друг на друга.

Однако архитектура микросервисов сопряжена со своими проблемами безопасности. Тот, кто, возможно, захочет ее использовать, должен тщательно изучить эти проблемы с самого начала, чтобы убедиться, что данные являются частными и безопасными, а система остается работоспособной при необходимости.

Микросервисы - это небольшие контейнерные прикладные сервисы, которые выполняют одну задачу или небольшую группу связанных задач, в отличие от традиционных монолитных приложений, которые обрабатывают широкий спектр задач. Поэтому жизненно важно использовать инструменты безопасности контейнеров, разработанные специально для среды архитектуры микросервисов.

Архитектура микросервисов имеет несколько уникальных уязвимостей, что является прямым результатом ее модульного характера. Приложения, разработанные с использованием архитектуры микросервисов, сложны и открыты. Они имеют гораздо большую площадь поверхности атаки, чем более традиционные модели приложений.

Микросервисы взаимодействуют через интерфейсы прикладного программирования (API), которые не зависят от архитектуры компьютера и даже языка программирования. В результате они имеют более открытую поверхность, чем традиционные подпрограммы или функциональные возможности большого приложения, которые взаимодействуют только с другими частями того же приложения. Следовательно, к ним применяется больше потенциальных атак.

Из-за быстрого цикла разработки и подхода к архитектуре микросервисов с непрерывной интеграцией / непрерывной доставкой (CI / CD) разработчики проводят тестирование кода не как отдельное мероприятие в конце разработки, а скорее как непрерывный процесс. Они должны правильно управлять этим тестированием.

Наконец, уникальный набор угроз может быть нацелен на контейнерное решение, в котором реализованы микросервисы. Это может зависеть от целостности самих образов контейнеров, способа управления ими, уровня изоляции между контейнерами, уязвимостей внутри контейнеров, таких как связанные библиотеки, и безопасности операционной системы (OS), в которой размещены контейнеры.

Рекомендации по обеспечению безопасности архитектуры микросервисов

Первым шагом к созданию безопасного решения на основе микросервисов является обеспечение того, чтобы безопасность была включена в проект. Некоторые фундаментальные принципы для всех проектов следующие:

- Шифрование всех коммуникации (используя https или безопасность транспортного уровня).
- Аутентификация всех запросов доступа.

- Не вводите жестко сертификаты, пароли или какие-либо секретные данные в коде.
- Использование инструментов DevSecOps, разработанных для сред микросервисной архитектуры, для сканирования кода по мере его разработки.
- Определите API и строго убедитесь, что все коммуникации соответствуют требованиям.

Меры безопасности требуют этих мер предосторожности на уровне кода, но тот, кто рассматривает этот тип архитектуры, должен также учитывать следующие факторы при реализации.

Изоляция

Изоляция - ключевой принцип концепции архитектуры микросервисов. Каждая служба должна быть автономной частью общего пазла приложения. Микросервис должен иметь возможность развертываться, поддерживаться, модифицироваться, масштабироваться и выводиться из эксплуатации без ущерба для других окружающих его микросервисов.

Изоляция также распространяется на те вспомогательные функции, которые находятся под ней, например, на уровне базы данных. Если все сделано правильно, один микросервис не сможет получить доступ к данным другого и, в случае компрометации, не позволит злоумышленнику перемещаться вбок.

Еще одна область, где изоляция жизненно важна для концепции архитектуры микросервисов, находится в режиме сбоя. Если происходит сбой конкретной микросервисной службы, это не должно приводить к сбою и других.

Безопасность API

Микросервисы должны взаимодействовать друг с другом только с помощью четко определенных и безопасных API. Безопасный API - это тот, который может гарантировать секретность обрабатываемой им информации, делая ее видимой только для пользователей, приложений и серверов, которым разрешено ее использовать. Ит-отдел должен обрабатывать данные от связанных клиентов и серверов только в том случае, если он знает, что эти данные не были изменены третьей стороной. Способность идентифицировать вызывающие системы и их конечных пользователей имеет решающее значение. Это также относится к вызовам, которые API выполняет к серверам сторонних производителей. API всегда должен быть доступен для обработки запросов и их надежной обработки.

Один из способов обезопасить API и справиться с аутентификацией пользователей и процессов - это использовать API-шлюз. Создатели API-шлюзов проектируют их с учетом масштабируемости. Они управляют большей частью затрат на аутентификацию, используя протоколы, такие как OAuth, для проверки объектов, которые пытаются получить доступ к API микросервиса.

Еще одно преимущество использования API-шлюзов заключается в том, что они могут обеспечивать управление доступом к API, что обеспечивает дополнительный уровень безопасности архитектуры микросервисов. Шлюз API может управлять тем, как внешние команды вызывают службы, которые обес-

печивают отказоустойчивость и другие службы балансировки нагрузки. Шлюз также может обеспечивать ведение журнала, позволяя службе управления информацией о безопасности и событиями / security operations center (SIEM / SOC) отслеживать приложения и выявлять неожиданное поведение.

Контейнерные решения безопасности для архитектуры микросервисов

Безопасность контейнера, от которой зависит архитектура микросервисов, имеет свои собственные наборы векторов угроз.

Риски безопасности контейнера могут заключаться либо в компрометации образа контейнера или контейнера в целом, либо в неправильном использовании контейнера для атаки на другие контейнеры, операционную систему хоста или другие хосты.

Через образ, реестр, orchestrator, контейнеры и хост-ОС могут появляться новые векторы угроз следующим образом.

Изображения

Образы приложений являются одной из ключевых уязвимых областей в контейнерной среде. Образы могут быть как специально написанными, так и разработанными сторонними разработчиками, в том числе с открытым исходным кодом. Здесь мы представляем ряд рисков, включая устаревшие образы, небезопасные версии программного обеспечения, приложения, содержащие ошибки, и плохо настроенные образы. Концепция secure by-design помогает устранить многие из этих рисков, но важно, чтобы разработчики не забывали распространять ее на контейнеры сторонних производителей или сервисы, которые они используют. У них должны быть правильные политики, чтобы убедиться, что они регулярно просматривают и обновляют изображения.

Реестр

При использовании плохо настроенного реестра доступ должен осуществляться через зашифрованные и аутентифицированные соединения. Кроме того, реестр должен подвергаться постоянному мониторингу, чтобы убедиться, что все устаревшие образы, которые могут представлять опасность, удалены.

Оркестровка

Жизненно важно сохранять контроль над тем, какие изображения вы используете и как они взаимодействуют. Поэтому сохраняйте жесткий контроль доступа к административным учетным записям в масштабе кластера с помощью эффективных методов аутентификации, таких как многофакторная аутентификация. Сегментация контейнеров по назначению, чувствительности и степени угрозы обеспечивает дополнительную углубленную защиту. В целом, настройте платформы orchestrator так, чтобы они использовали функции, создающие безопасную среду для всех приложений, которые на них запускаются.

Контейнер

Наиболее распространенная проблема безопасности в архитектуре микросервисов возникает, когда среды выполнения контейнеров, управляющие контейнерами, имеют уязвимости. Уязвимая среда выполнения может подвергнуть

потенциальным угрозам безопасности все контейнеры, которые она запускает, а также ОС хоста. Учитывая гибкость, которой обладают контейнеры благодаря динамическим IP-адресам по сети, разработчикам необходимо выявлять сетевые аномалии. Регулярно проводите сканирование контейнеров на уязвимости, особенно долговременных. Вы также должны отслеживать их, отправляя оповещения в инструмент, который может сопоставлять различные события. Затем это может вызывать оповещения для информирования кого-либо, способного решить потенциальные проблемы.

Другой набор полезных инструментов проверяет, как пользователь настроил контейнеры, и сравнивает их с политиками безопасности. Затем инструмент может выдать предупреждение, закрыть контейнер или устранить проблему с конфигурацией.

Операционная система хоста

Наконец, операционная система хоста является ключом к успешной контейнерной среде. Поскольку она находится на самом низком уровне контейнерной архитектуры, она является критической целью для злоумышленников. Компрометация операционной системы хоста может привести к компрометации всех запущенных на ней контейнеров. Постоянно сканируйте операционную систему хоста на наличие уязвимостей и немедленно применяйте все необходимые обновления. Это касается не только уровня среды выполнения контейнера; это также должно быть сделано для компонентов более низкого уровня, таких как ядро, которые являются ключевыми для обеспечения безопасности операций с контейнерами.

Правильная конфигурация также важна для безопасности основной операционной системы. Запускайте ее как неизменяемую инфраструктуру без зависимостей на уровне данных и приложений. Это делает основную операционную систему высоконадежной и эффективной в функционировании. Разработчики создают все большее количество операционных систем хоста специально для запуска контейнерных сред. Они используют только минимум сервисов, необходимых для запуска контейнеров, преимущество которых заключается в повышении производительности, но также и в уменьшении зоны атаки. К счастью, на рынке существует ряд решений и сервисов, которые могут помочь смягчить эти проблемы безопасности.

Шаблоны и рекомендации по обеспечению безопасности архитектуры микросервисов

Выдающиеся преимущества микросервисов

Производительность повышается, когда несколько команд работают вместе над различными элементами единого сложного приложения, конкретные элементы могут быть развернуты без каких-либо серьезных простоев. Контейнеры Docker составляют инфраструктуру, и ими легко пользоваться. Отдельные команды могут свободно выбирать подходящий инструмент для устранения проблемы в отдельных компонентах микросервисов.

Рассмотрим методы, которые команды по разработке программного обес-

печения могут использовать для защиты компонентов микросервисов и их функций.

Рекомендаций по обеспечению безопасности архитектуры микросервисов - необходимые шаги

Устранение уязвимостей означает обеспечение безопасности микросервисов. Это приравнивается к разработке наилучших методов обеспечения безопасности, их внедрению и следованию им. В таком случае безопасность становится неотъемлемой частью системы, и работа продолжается без перерывов, что значительно повышает производительность и целостность микросервисов.

Шаг 1: Переход к разработке безопасных микросервисов

На этапах разработки разработчики должны позаботиться о том, чтобы внедрить несколько уровней безопасности для защиты данных. Безопасности следует уделять наивысшее внимание на каждом этапе разработки (от проектирования до этапов сборки и развертывания), чтобы получить безопасную систему микросервисов. Глубокая защита творит чудеса с безопасностью системы.

Когда разработчики начинают писать код для системы микросервисов, код следует подвергать непрерывному стресс-тестированию, чтобы гарантировать надежную архитектуру. Это означает тестирование конвейеров CI и CD. Статический анализ и динамическое тестирование безопасности (SAST и DAST) также должны выполняться одновременно.

В то время как SAST можно использовать для проверки слабых мест, существующих в вашем коде и импортированных библиотеках. Поскольку он работает изнутри, сканер, соответствующий используемому языку программирования, также следует держать наготове.

DAST имитирует вредоносные атаки извне и не зависит ни от какого языка. Создание этих тестов в конвейере доставки гарантирует, что потребуется выполнять меньше проверок вручную.

OWASP (Open Web Application Security Project) также предлагает набор инструментов для анализа и некоторые ресурсы, помогающие внедрять рекомендации при создании программного обеспечения.

Шаг 2: Сканирование зависимостей

Библиотеки, которые используются при разработке программного обеспечения, сами используют другие библиотеки. Это означает, что программный пакет имеет несколько зависимостей (от сторонних производителей). Таким образом, безопасность является серьезной проблемой, поскольку этот аспект увеличивает вероятность возникновения ряда системных уязвимостей.

Устранение таких уязвимостей может быть достигнуто путем регулярного и тщательного сканирования репозитория кода приложения. Кроме того, следует регулярно проверять новые элементы кода и конвейер развертывания на наличие уязвимых зависимостей. Сюда также входят обновленные последние версии.

Обычно в примечаниях к выпуску приложений можно найти информацию. Однако лишь немногие сообщают о возникших проблемах безопасности. К со-

жалению, только 10% сообщают о распространенных проблемах с доступом. Знание зависимостей гарантирует отсутствие зависимостей из-за новых запросов на извлечение во время развертывания. Это также гарантирует актуальность вашего кода. Такие инструменты, как Dependabot от Github, помогают автоматизировать обновления с помощью запросов на извлечение. Неплохо бы включить оповещения системы безопасности в вашем репозитории.

Шаг 3: повсеместное использование HTTPS

Лучше всего реализовать этот аспект согласованным образом для фундаментальной защиты внутренних и внешних операций. Смягчение атак, происходящих внутри сети, так же важно, как предотвращение утечки учетных данных и фишинга. Лучше всего позаботиться об этом, внедрив HTTPS во всей системе микросервисов.

HTTPS обеспечивает конфиденциальность и целостность данных в системе за счет шифрования связи по протоколу HTTP.

Для обеспечения безопасности транспортного уровня (TLS), который теперь называется HTTPS, требуется сертификат аутентификации, подтверждающий вашу личность, для предоставления доступа к зашифрованным сообщениям (через инфраструктуру открытых ключей). После получения сертификатов можно добиться постоянного повышения уровня вашей безопасности за счет автоматизации генерации и продления сертификатов. Это поможет исключить из системы все негативные факторы, которые могут поставить под угрозу вашу архитектуру.

Каждый аспект архитектуры микросервисов может ссылаться на эти безопасные URL-адреса (от репозиториев Maven до XSD). Заголовок ответа HTTP Strict-Transport-Security также может использоваться для указания браузерам выборочно обращаться только к вашим конечным точкам с использованием HTTPS.

Протокол HTTPS жизненно важен для защиты данных, которые передаются внутри ваших систем при создании систем микросервисов и API. После развертывания соединения с внешними пользователями также будут защищены, что защитит ваши данные.

Используйте токены доступа и идентификации

Система микросервисов включает в себя широкий спектр действий, таких как внутренние службы, которые предоставляют данные, код, который транспортирует данные в хранилища, и пользовательский интерфейс, который выдает данные в требуемой для пользователей форме. После этого должны быть созданы соответствующие инструменты и протоколы для обеспечения безопасной / эффективной аутентификации, а также авторизации во всех системах, создавая наилучшие шаблоны безопасности микросервисов.

OAuth 2.0 - это пример стандартного отраслевого протокола, который авторизует пользователей в распределенных системах. Поток учетных данных клиента OAuth 2.0 обеспечивает безопасную межсерверную связь между клиентом API и сервером API в системах микросервисов.

OpenID Connect (OIDC), расширение OAuth, предлагает стандартную спецификацию, которая помогает разработчикам писать код, который будет работать со многими поставщиками удостоверений. Вместе они помогают системе определять личность пользователя путем отправки токена доступа конечной точке с пользовательской информацией. Путь может быть определен с помощью обнаружения OIDC. Этот механизм сокращает работу разработчика, избавляя его от необходимости встраивать механизмы аутентификации в каждый отдельный микросервис.

Серверы авторизации: что лучше: "Многие к одному" или "Один к одному"

Использование OAuth 2.0 для защиты вашего сервиса означает использование сервера авторизации. Обычно эта настройка представляет собой взаимосвязь "многие к одному", при которой многие микросервисы взаимодействуют с одним сервером авторизации.

Плюсы подхода "многие к одному":

- Службы используют токены доступа для взаимодействия с другой внутренней службой
- Вам нужно искать все определения области действия и разрешений только в одном месте
- Ею легко управлять как разработчикам, так и сотрудникам службы безопасности
- Быстрота

Недостатки подхода "многие к одному":

- Мошеннические сервисы могут вызывать проблемы со своими токенами
- Если токен службы будет скомпрометирован, под угрозой окажутся все сервисы
- Размытые границы безопасности
- Индивидуальный подход - это альтернативный, более безопасный подход, при котором каждый микросервис привязан к эксклюзивному серверу авторизации. Чтобы общаться друг с другом, они должны зарегистрироваться до установления доверия.

Эта архитектура допускает четко определенные границы безопасности. Она медленнее, более разговорчива и сложнее в управлении. Рекомендуется использовать взаимосвязь "многие к одному" до тех пор, пока не будут готовы план и соответствующая документация для поддержки индивидуальной настройки.

Шаг 5: Шифрование

Шифрование и защита секретных данных

Микросервисы, взаимодействующие с серверами авторизации, скорее всего, будут иметь секреты для обмена данными, такие как клиентские секреты, ключи API или учетные данные для базовой аутентификации.

Вы не можете проверить наличие этих секретов в своих системах управления версиями, потому что они создают проблемы во время работы команды над про-

изводственным кодом. Было бы лучше защитить секреты в переменных среды.

Секреты можно зашифровать с помощью таких инструментов, как HashiCorp Vault, Microsoft Azure Key Vault или Amazon KMS. Инструменты позволяют осуществлять шифрование с помощью главного ключа, который создает зашифрованное сообщение, хранящееся в виде файла / базы данных. Ключи для расшифровки всегда хранятся в безопасности, что позволяет команде тратить больше времени на внедрение других мер предосторожности и управление ими.

Шаг 6: Проверка безопасности с помощью конвейеров доставки

Рекомендуется, чтобы сканирование зависимостей и контейнеров было частью системы мониторинга системы управления версиями, а также выполнять тесты при выполнении конвейеров CI и CD.

DevSecOps - более подходящий термин, подчеркивающий необходимость встраивания безопасности в инициативы DevOps. Модульные тесты безопасности, SAST и DAST уже на подходе. Лучше всего автоматизировать эти проверки безопасности в конвейере доставки кода, хотя их настройка займет некоторое время.

Шаг 7: Замедление работы злоумышленников

Атака на API с использованием сотен комбинаций имени пользователя и пароля, вероятно, потребует некоторого времени для успешной аутентификации. Если эту атаку удастся еще больше замедлить, различные конечные точки смогут быть защищены в большей степени. Такие подходы, как ограничение скорости, могут удержать злоумышленников от продолжения атак с использованием учетных данных. Этот метод может быть реализован в вашем коде, с помощью библиотеки с открытым исходным кодом или в шлюзе API.

Шаг 8: Используйте режим Docker без рутинга

В версии Docker 19.03 введен режим без рутинга, и эта функция была разработана для предоставления возможностей Docker тем системам (где пользователи не могут получить права root), одновременно уменьшая влияние демона Docker на безопасность.

Это необходимо учитывать, если вы запускаете демоны Docker в рабочей среде. Если Kubernetes запускает ваши контейнеры Docker, потребуется настроить RunAsUser в политике PodSecurityPolicy.

Шаг 9: Использование безопасности, основанной на времени

Рекомендуется использовать защиту на основе времени. Защита на основе времени предполагает, что система никогда не будет полностью защищена. Помимо предотвращения проникновения злоумышленников в систему, обнаружение и реагирование необходимы для обеспечения безопасности системы.

Использование многофакторной аутентификации - еще одна хорошая идея, которая замедляет работу злоумышленников, а также обнаруживает аутентификацию на критически важном сервере, что не должно происходить слишком часто. Контроллер домена, управляющий сетевым трафиком, может быть сконструирован таким образом, чтобы отправлять предупреждение команде сетевых администраторов сразу после успешного входа в систему.

Шаг 10: Проверка конфигураций Docker и Kubernetes на наличие уязвимостей

Контейнеры Docker обычно находят место в архитектурах микросервисов. Некоторые рекомендации включают предпочтение минимального базового образа, использование директивы ПОЛЬЗОВАТЕЛЯ для обеспечения использования наименее привилегированного, подписание и проверку образов для предотвращения атак MITM, поиск, исправление и мониторинг уязвимостей с открытым исходным кодом и т.д.

Шаг 11: Знание облачной и кластерной безопасности

При управлении производственными кластерами и облаками 4C облачной встроенной безопасности включают код, контейнер, кластер и облако / корпоративный центр обработки данных.

Рекомендации по обеспечению безопасности архитектуры микросервисов включают использование шифрования передаваемых данных, использование аутентификации для обеспечения доступа к службам только авторизованным пользователям и выполнение регулярных оценок безопасности для выявления потенциальных проблем безопасности.

Наиболее распространенные шаблоны безопасности для архитектуры микросервисов включают аутентификацию и авторизацию, шифрование данных при передаче и шифрование в состоянии покоя.

Некоторые рекомендации по проектированию архитектуры микросервисов включают использование архитектуры, управляемой событиями, для обеспечения асинхронной связи, проектирование с учетом невозможности обеспечения отказоустойчивости и использование контейнеризации для упрощения развертывания и масштабируемости.

Каждый из этих факторов зависит от внедренных стандартов безопасности, и трудно защититься от некачественных стандартов в облаке, контейнерах и коде, просто решая проблему безопасности на уровнях кода. Если с ними обращаться надлежащим образом, то добавление безопасности в код укрепляет базу.

Когда переходить на архитектуру микросервисов

Создание микросервисного приложения без необходимых навыков и знаний чрезвычайно опасно. Даже сейчас базового понимания архитектуры недостаточно. Поскольку DevOps и контейнеры тесно связаны с микросервисами, вам потребуются профессионалы и в том, и в другом. Также требуются знания в области моделирования предметной области. При работе с микросервисами система разделена на различные функции и распределены обязанности.

Приложение, которое является одновременно сложным и масштабируемым. Масштабирование и добавление новых возможностей в вашу программу станет значительно проще благодаря дизайну микросервисов. Итак, если вы планируете создать масштабное приложение с несколькими модулями и возможностями взаимодействия с пользователем, то лучше всего использовать парадигму микросервисов.

Достаточно талантливых инженеров. Вам понадобятся достаточные ресурсы для управления всеми действиями в проекте микросервиса, поскольку в нем задействовано множество команд, отвечающих за различные сервисы.

Когда не следует использовать архитектуру микросервисов

Дополнительная сложность

Поскольку архитектура микросервисов представляет собой распределенную систему, необходимо выбрать и настроить подключения ко всем модулям и базам данных. Более того, если приложение включает независимые службы, каждая из них должна быть развернута отдельно.

Распространение системы

Поскольку архитектура микросервисов представляет собой сложную систему со множеством модулей и баз данных, необходимо тщательно управлять всеми подключениями.

Тестирование решения на основе микросервисов существенно сложнее из-за большого количества независимо развертываемых компонентов.

Заключение

Приведенный выше список рекомендаций по обеспечению безопасности архитектуры микросервисов, безусловно, не является исчерпывающим. Однако эти проблемы обычно возникают при создании и запуске микросервисов. Важно иметь идею, позволяющую лучше управлять сервисами в долгосрочной перспективе.

Список источников

1. Balalaie, A.; Heydarnoori, A.; Jamshidi, P. Microservices Architecture Enables DevOps: Migration to a Cloud-Native Architecture (англ.) // IEEE Software[англ.] : journal. — 2016. — 1 May (vol. 33, no. 3). — P. 42—52. — ISSN 0740-7459. — doi:10.1109/MS.2016.64

2. Кристудас Бинилдас (27 июня 2019 г.). Практические архитектурные шаблоны микросервисов: микросервисы Java на основе событий с Spring Boot и Spring Cloud. Apress. 978-1484245002 ISBN.

3. Ньюман, Сэм (2015). Создание микросервисов. O’Reilly. ISBN 978-1491950357.

4. Вольф, Эберхард (12 октября 2016 г.). Микросервисы: гибкие архитектуры программного обеспечения. Addison-Wesley. ISBN 978-0134602417.

5. Основы архитектуры программного обеспечения: инженерный подход. O'Reilly Media. 2020. ISBN 978-1492043454.

УДК 330

ГЛАВА 12. КИБЕРБЕЗОПАСНОСТЬ. ОБЕСПЕЧЕНИЯ КОНФИДЕНЦИАЛЬНОСТИ И ЦЕЛОСТНОСТИ ДАННЫХ В ОБЛАКЕ

Аменицкий Алексей Владимирович
аспирант
Санкт-Петербургский государственный электротехнический университет ЛЭТИ имени В.И. Ульянова (Ленина)

Научный руководитель: Воробьёв Евгений Германович
д.т.н., профессор
Санкт-Петербургский государственный электротехнический университет ЛЭТИ имени В.И. Ульянова (Ленина)

Аннотация: Когда мы переносим свои системы в облако, многие меры безопасности и лучшие практики остаются прежними. Тем не менее, придётся столкнуться с новой серией проблем, которые придется преодолеть, чтобы поддерживать безопасность систем и данных в облаке.
Ключевые слова: Cyber Security (CS), CS architecture, CS trends, CS tendences, CS tools, CS crimes, CS latest news, CS releases, CS game-changers, CS future, CS playbook, CS agenda, CS future, CS risks, CS incidents, CS resilience, Hackers, CS прогноз, Artificial Intelligence, Deep Fakes, Эволюция киберУгроз, КиберГигиена.

CYBERSECURITY. ENSURING THE CONFIDENTIALITY AND INTEGRITY OF DATA IN THE CLOUD

Amenitsky Alexey Vladimirovich

Scientific supervisor: Vorobyov Evgeny Germanovich

Облако предлагает три основных типа инфраструктуры:

Общедоступные облачные сервисы размещаются поставщиками ИТ-услуг. Они интегрируют три уровня: программное обеспечение как услуга (SaaS), платформа как услуга (PaaS) и инфраструктура как услуга (IaaS).

Частные облака размещаются одной организацией или для нее. Наконец, гибридные облака включают в себя смесь публичных и частных типов. Поэтому механизмы облачной безопасности бывают в двух формах: те, которые предоставляются облачными провайдерами, и те, которые реализуются клиентами. Важно отметить, что управление безопасностью редко является исключительной ответственностью поставщика или клиента. Обычно это совместные усилия, использующие модель совместной ответственности.

Хотя она не стандартизирована, модель совместной ответственности представляет собой основу, которая определяет задачи безопасности, которые являются ответственностью поставщика онлайн-услуг (облака) и те, которые несет ответственность клиента. Компании, использующие облако, должны четко знать, какие обязанности по безопасности они возлагают на своего поставщика (поставщиков) и что им нужно управлять внутри компании, чтобы гарантировать отсутствие пробелов в охвате.

Клиенты всегда должны проверять у своего поставщика, что они покрывают и что они должны делать сами, чтобы защитить организацию. Модель совместной ответственности описывает обязанности поставщика услуг по безопасности (CSP, поставщик облачных услуг) и клиента.

Средства контроля безопасности, предоставляемые поставщиками облачных услуг, варьируются в зависимости от модели обслуживания, будь то SaaS, PaaS или IaaS. Ответственность клиентов, как правило, увеличивается от SaaS до PaaS, а затем до IaaS.

В целом, CSP всегда отвечают за серверы и хранилище. Они защищают и исправляют саму инфраструктуру, а также настраивают физические центры обработки данных, сети и другое оборудование, которое питает инфраструктуру, включая виртуальные машины (ВМ) и диски. Обычно это единственные обязанности поставщиков на уровне IaaS.

В среде PaaS CSP берут на себя больше обязанностей, включая обеспечение выполнения, сеть, операционные системы (ОС), данные и виртуализацию. В среде SaaS они также обеспечивают безопасность приложений и слоев промежуточного программного обеспечения.

Детали обязанностей по обеспечению безопасности могут варьироваться в зависимости от поставщика и клиента. Например, поставщики облачных услуг, предлагающие предложения SaaS, могут предлагать или не предлагать клиентам информацию об используемых ими инструментах безопасности. С другой стороны, поставщики IaaS, как правило, предлагают интегрированные механизмы безопасности, которые позволяют клиентам получать доступ и визуализировать инструменты безопасности, что также может позволить клиентам получать оповещения.

Для выполнения перечисленных выше средств контроля безопасности CSP клиенты, как правило, несут ответственность за безопасность приложений, промежуточного программного обеспечения, виртуализации, данных, операционной системы, сети и времени выполнения на IaaS. Например, в архитектурах IaaS, таких как Amazon Virtual Private Cloud (VPC) или Microsoft Azure Virtual Network (VNet), клиенты могут дополнять, заменять или налагать интегрированные механизмы кибербезопасности своим собственным набором инструментов.

В средах PaaS клиенты берут на себя меньше задач безопасности, как правило, только безопасность приложений и промежуточного программного обеспечения. Среды SaaS предполагают еще меньшую ответственность со стороны клиентов. Безопасность данных и управление идентификацией и доступом

(IAM) всегда является ответственностью клиента, независимо от модели предоставления облачных услуг. Шифрование и соответствие требованиям также являются обязанностью клиента.

Однако, поскольку CSP контролируют и управляют инфраструктурой, в которой работают приложения и данные клиентов, принятие дополнительных средств контроля для дальнейшего снижения рисков может быть затруднено. CISO должен как можно скорее принять участие в оценке CSP и облачных сервисов. Поэтому группы безопасности должны оценить инструменты безопасности по умолчанию, чтобы определить, следует ли применять дополнительные меры внутри компании.

Добавление корпоративных инструментов безопасности в облачные среды обычно выполняется путем установки одного или нескольких сетевых виртуальных устройств безопасности. Наборы инструментов, добавленные клиентом, позволяют администраторам безопасности быть более точными в конкретных конфигурациях безопасности и настройках политики. Многие компании также считают, что важно внедрить те же инструменты в своих различных публичных облаках, что и в их собственных корпоративных локальных сетях (LAN). Это избавляет администраторов от необходимости воссоздавать облачные политики безопасности с помощью разрозненных инструментов безопасности. Вместо этого одна политика безопасности может быть создана только один раз, а затем передана идентичным инструментам безопасности, независимо от того, находятся ли они локально или в облаке.

Инструменты облачной безопасности

Большинство инструментов, используемых в локальных средах, должны использоваться в облаке, даже если есть версии, специфичные для облака. Эти инструменты и механизмы включают в себя шифрование или шифрование, IAM и однофакторную аутентификацию (SSO), предотвращение потери данных (DLP), системы предотвращения вторжений и обнаружения (IPS/IDS) и инфраструктуру открытых ключей (PKI).

Несколько облачных инструментов:

Платформы защиты облачных рабочих нагрузок (CWPP). CWPP - это механизм безопасности, предназначенный для последовательной защиты рабочих нагрузок (например, виртуальных машин, приложений или данных).

Брокеры безопасности облачного доступа (CASB). CASB - это инструмент или услуга, которая вмешивается между клиентами и облачными сервисами для применения политик безопасности и, как опекун, добавляет уровень безопасности.

Управление облачной безопасностью (CSPM). CSPM - это группа продуктов и услуг безопасности, которые отслеживают проблемы облачной безопасности и соответствия требованиям и направлены на борьбу с плохими конфигурациями, среди прочих функций.

Secure Access Service Edge (SASE) и доступ к сети с нулевым доверием (ZTNA- Zero Trust Network Access) также появляются как две популярные модели/фреймворки облачной безопасности.

Безопасность как услуга, часто сокращенно SaaS или SECaaS, является подмножеством программного обеспечения как услуги (SaaS). Альянс облачной безопасности (CSA) определил 10 категорий SECaaS:

- AI
- DLP
- Веб-безопасность
- Безопасность электронной почты
- Оценки безопасности
- Управление вторжениями
- Управление информацией о безопасности и событиями (SIEM)
- Кодирование
- Аварийное восстановление (BC/аварийное восстановление)
- Сетевая безопасность

К ним относятся такие услуги, как брандмауэры как услуга, облачные виртуальные частные сети (VPN) и управление ключом как услуга (KMaaS).

Передовые задачи облачной безопасности

Поскольку у общедоступного облака нет четких границ, оно представляет собой принципиально иную среду с точки зрения безопасности. Это становится еще более сложной задачей при использовании современных облачных подходов, таких как автоматизированные методы непрерывной интеграции и непрерывного развертывания (CI/CD), распределенные бессерверные архитектуры и эфемерные ресурсы, такие как функции как услуга и контейнеры.

Некоторые из передовых облачных проблем в сфере безопасности и многоуровневых рисков, с которыми сталкиваются современные организации, ориентированные на облака, включают:

Увеличенная поверхность атаки

Среда публичного облака стала большой и очень привлекательной мишенью для хакеров, которые используют плохо защищённые входные порты облака, чтобы получить доступ к рабочим нагрузкам и данным в облаке и нарушить их работу. Вредоносные программы, атаки нулевого дня, взлом учётных записей и многие другие вредоносные угрозы стали повседневной реальностью.

Отсутствие видимости и отслеживания

В модели IaaS поставщики облачных услуг полностью контролируют уровень инфраструктуры и не предоставляют к нему доступ своим клиентам. Отсутствие прозрачности и контроля ещё больше усугубляется в облачных моделях PaaS и SaaS. Клиенты облачных сервисов часто не могут эффективно идентифицировать и количественно оценивать свои облачные ресурсы или визуализировать свою облачную среду.

Постоянно меняющиеся рабочие нагрузки

Облачные ресурсы предоставляются и выводятся из эксплуатации динамически — в больших масштабах и с высокой скоростью. Традиционные инструменты безопасности просто не способны обеспечивать соблюдение политик

защиты в такой гибкой и динамичной среде с постоянно меняющимися и эфемерными рабочими нагрузками.

DevOps, DevSecOps и автоматизация

Организации, внедрившие высокоавтоматизированную культуру DevOps CI/CD, должны обеспечить, чтобы соответствующие средства контроля безопасности были определены и внедрены в код и шаблоны на ранних этапах цикла разработки. Изменения, связанные с безопасностью, внедренные после развертывания рабочей нагрузки в рабочей среде, могут подорвать безопасность организации, а также увеличить время выхода на рынок.

Детализированное управление привилегиями и ключами

Часто роли пользователей в облаке настраиваются очень свободно, предоставляя широкие привилегии, выходящие за рамки того, что необходимо или предусмотрено. Один из распространённых примеров — предоставление необученным пользователям или пользователям, у которых нет необходимости в удалении или добавлении ресурсов базы данных, разрешений на удаление или запись в базу данных. На уровне приложения неправильно настроенные ключи и привилегии подвергают сеансы риску.

Сложные среды

Для последовательного управления безопасностью в гибридных и мультиоблачных средах, которые в наши дни предпочитают предприятия, требуются методы и инструменты, которые легко интегрируются с поставщиками общедоступных облачных сервисов, поставщиками частных облачных сервисов и локальными развертываниями, включая защиту периферийных офисов для географически распределенных организаций.

Соответствие требованиям облачных технологий и управление ими

Все ведущие поставщики облачных услуг присоединились к большинству известных программ аккредитации, таких как PCI 3.2, NIST 800-53, HIPAA и GDPR. Однако клиенты несут ответственность за обеспечение соответствия своей рабочей нагрузки и процессов обработки данных требованиям. Учитывая недостаточную прозрачность и динамичность облачной среды, процесс аудита соответствия требованиям становится практически невыполнимой задачей, если не используются инструменты для непрерывной проверки соответствия требованиям и оповещения о неправильных настройках в режиме реального времени.

Нулевое Доверие и почему вы должны принять его

Термин Zero Trust был впервые представлен в 2010 году Джоном Киндервагом, который в то время был старшим аналитиком Forrester Research. Основной принцип нулевого доверия в облачной безопасности заключается в том, чтобы не доверять автоматически никому и ничему внутри или за пределами сети, а проверять (т. е. авторизовывать, проверять и защищать) всё.

Например, концепция «нулевого доверия» продвигает стратегию управления с наименьшими привилегиями, при которой пользователям предоставляется доступ только к тем ресурсам, которые необходимы для выполнения их обя-

занностей. Аналогичным образом она призывает разработчиков обеспечить надлежащую защиту веб-приложений. Например, если разработчик не заблокировал порты последовательно или не внедрил разрешения по принципу «по мере необходимости», хакер, захвативший приложение, получит права на получение и изменение данных в базе.

Кроме того, в сетях с нулевым доверием используется микросегментация, которая делает безопасность облачных сетей более детальной. Микросегментация создаёт безопасные зоны в центрах обработки данных и облачных средах, тем самым отделяя рабочие нагрузки друг от друга, защищая всё внутри зоны и применяя политики для защиты трафика между зонами.

Защита данных в облаке

Меры, которые должны быть приняты для защиты данных в дематериализованных вычислениях, различаются. Необходимо учитывать такие факторы, как тип и чувствительность защищенных данных, облачная архитектура, доступность интегрированных и сторонних инструментов, а также количество и типы пользователей, имеющих право на доступ к данным.

Общие передовые практики для защиты корпоративных данных в облаке:

- Шифрование данных в режиме покоя, в использовании и в движении.
- Использование двухфакторной аутентификации (2FA) или многофакторную аутентификацию (MFA) для проверки личности пользователя перед предоставлением ему доступа.
- Меры безопасности на краю облака, включая брандмауэры, IPS и антивирусное программное обеспечение.
- Изоляция резервных копии данных в облаке, чтобы предотвратить угрозы программ-вымогателей.
- Обеспечение видимости и контроля местоположения данных, чтобы определить, где находятся данные, и внедрить ограничения на возможность копирования данных в другие места внутри или за пределами облака.
- Сохранение и отслеживание всех аспектов доступа к данным, дополнений и изменений.

Для защиты данных в облаках также необходимо учитывать новые инструменты кибербезопасности. К ним относятся обнаружение и реагирование сети (NDR) и искусственный интеллект (AI) для компьютерных операций (AIOps). Эти два инструмента собирают информацию о состоянии облачной инфраструктуры и кибербезопасности. Затем ИИ анализирует данные и предупреждает администраторов в случае аномального поведения, которое может указывать на угрозу.

Основные проблемы безопасности дематериализованных вычислений

Большинство традиционных проблем кибербезопасности также возникают в дематериализованных вычислениях. Это могут быть следующие элементы:

- Незамкнутые угрозы
- Потеря данных

- Утечки данных
- Управление ключами
- Контроль доступа
- Фишинг
- Вредоносная программа
- Теневой ИТ
- Распределенные атаки на отказ в обслуживании (DDoS)
- Небезопасные интерфейсы прикладного программирования (API)

Что касается проблем, связанных с облачной безопасностью, администраторы должны, в частности, столкнуться со следующими проблемами:

- хищение учетной записи в облаке;
- отсутствие видимости и контроля над дематериализованными вычислениями;

Облачные инструменты безопасности, о которых могут знать внутренние администраторы;

- Мониторинг и мониторинг местоположения данных, как в пути, так и в покое;
- Нарушение конфигурации;
- Трудности в понимании модели совместной ответственности;
- Злоумышленное использование облачных сервисов;
- Проблемы, связанные с несколькими локациями;
- Несовместимость с средами на месте;
- Соответствие облачных вычислений; и
- Управление облаком.

Администраторы безопасности должны разработать планы и процессы для выявления и ограничения новых облачных угроз безопасности. Эти угрозы обычно связаны с недавно обнаруженными эксплойтами в приложениях, операционных системах, виртуальных средах и других компонентах сетевой инфраструктуры. Чтобы решить эти проблемы безопасности и устранить возникающие угрозы, компании должны быстро и надлежащим образом обновлять и исправлять программное обеспечение, которое они контролируют.

Также важно установить каналы связи между внутренним ИТ-персоналом и персоналом CSP. Внутренний персонал должен подписаться на рассылку бюллетеней безопасности облачного провайдера, отслеживать и усваивать ее. Если для управления инцидентом безопасности необходима координация между клиентом и CSP, необходимо установить и постоянно обновлять хорошо документированные каналы связи, чтобы избежать потери времени при устранении уязвимости безопасности.

Лучшие практики в области облачной безопасности

- Существуют отдельные лучшие практики для SaaS, PaaS и IaaS. Компании также должны соблюдать ряд общих передовых практик в области безопасности дематериализованных вычислений, включая следующие:

- Необходимо понимание модели общей ответственности, включая обязанности CSP и команды безопасности.
- Тщательный выбор CSP подразумевает знания, какие средства контроля безопасности предлагаются, и надлежащий пересмотр контрактов и соглашений об уровне обслуживания (SLA).
- Принятие сильной и детализированную политики IAM для контроля "кто имеет доступ к чему". Использование принцип наименьших привилегий и требуйте надежных паролей и 2FA или MFA.
- Шифрование данные в режиме покоя, в использовании и в движении.
- Поддержание видимости в своем облаке с помощью непрерывного мониторинга.
- Понимание требований и правил для соответствия облачным стандартам.
- Создание и применение политик безопасност, предназначенных для облака.
- Организация тренингов по вопросам безопасности для сотрудников, сторонних партнеров и всех, кто получает доступ к облачным ресурсам организации.
- Сегментация своего облака и рабочих нагрузок.

Трансформация компаний в большее количестве облачных ресурсов ускорилась с пандемическим кризисом COVID-19, когда как сотрудники, так и клиенты должны были находить точки поддержки за пределами центра обработки данных, работать и получать доступ к услугам без новых трудностей, влияющих на деятельность.

Существует решение для переключения всего в облако: перенос всех приложений в формате контейнера для Kubernetes и отказ от всех его инструментов в пользу консолей SaaS. За исключением того, что это невозможно. Пройдёт много лет, десятилетий, прежде чем программное обеспечение, предназначенное для центров обработки данных, исчезнет. И тогда это потребует слишком много инвестиций за слишком малый промежуток времени, с нереалистичными сроками. Существует гораздо более жизнеспособная альтернатива: гибридное облако.

Гибридное облако состоит из расширения инфраструктуры центра обработки данных в облаке или наоборот, в зависимости от происхождения используемого решения. AWS, Azure и Google предлагают решения для размещения своих виртуальных машин в центре обработки данных в соответствии с требованиями задержки и критичности.

Производители серверов и решений для хранения теперь имеют решения в другом направлении, чтобы разместить свои кирпичи в Интернете. Преимущество этих решений заключается в том, что консоли администрирования, правила безопасности и высокой доступности, короче говоря, управление остаются неизменными, независимо от того, где работают приложения. Мы ничего не меняем, мы просто добавляем доступность облака к производительности центра обработки данных. Это основное руководство объединяет советы, как начать, а

затем развернуть. Он также проводит экскурсию по гибридным облачным предложениям, предлагаемым гипермасштаберами, поставщиками серверов и игроками решений для хранения данных. Эта категория объединяет как исторических производителей, так и особенно инновационные стартапы о новых видах использования, разрешенных гибридным облаком.

В эпоху нативных облачных приложений.

Развертывание приложений и миграция критически важных данных в облако все больше и больше, основаны на новом операционном подходе и требуют новых навыков.

Проекты облачной трансформации предоставляют такие возможности, как инновации, оперативная гибкость и скорость развертывания приложений. Принятие соответствующей стратегии безопасности в настоящее время имеет важное значение для защиты обещаний перехода в облако, противодействия кибератакам и новым угрозам.

Такой подход поможет справиться с новой реальностью пользователей и приложений.

- В облаке

Создание своей стратегии облачной безопасности и защита доступа пользователей к приложениям и данным, с применением принципа "Нулевого доверия".

- В облаке

Защитита своих облачных и контейнерных сред от ошибок конфигурации и нарушений политики безопасности.

- За пределами облака

Отслеживание вредоносных действий с помощью интеллектуального обнаружения угроз в многооблачных и гибридных средах.

Серверы и облако

Централизованные решения быстро набирают обороты в современной полупроводниковой промышленности, деятельность которой больше не ограничивается конечными устройствами, но теперь интегрирует аспекты микропрограммного обеспечения/программного обеспечения и безопасного управления их жизненным циклом.

С миллиардами подключенных устройств, развернутых по всему миру, важно обеспечить, с точки зрения поставщика, безупречное обслуживание для конечных пользователей. Также необходимо обеспечить, чтобы функциональное качество развернутых услуг оставалось бесперебойным и неизменным. Для достижения этой расширенной совместимости устройства должны быть подключены к одному или нескольким защищенным серверам, с которых они управляются через облачные сервисы.

Однако безопасность инфраструктуры IoT зависит от ее самого слабого звена. Поэтому кибербезопасность в облачных вычислениях обеспечивает необходимые меры как для управления киберугрозами, так и для обеспечения платформы защиты нулевого дня.

Функционал новых облачных решений

Облако: Облачный компонент в целом предоставляет безопасные услуги и конфигурации для предоставления устройств на периферии или других устройств, подключенных к инфраструктуре. Он также содержит профиль безопасности для облачной кибербезопасности и облачной безопасности IoT. Усовершенствованное наблюдение и обнаружение вторжений обеспечивают круглосуточную защиту от активных угроз из любой точки с помощью возможностей прогнозирования, расширенных искусственным интеллектом.

Хранение данных: Хранение электронных данных, размещенных в облаке, может включать в себя различные формы данных, от компьютеризированного обмена данными (EDI) до компьютеризированной записи пациента (DPI) и необработанных данных. Также можно хранить конфиденциальные данные в выделенном центре обработки данных в надежном месте с дополнительными мерами безопасности. Стандартные ограничения и правила, такие как GRPD, применяются для защиты целостности данных по различным каналам и штатам, таким как отдых, транзит и обработка.

Канал связи: Движок сети IoT - это инфраструктура передачи данных, которая используется для подключения к службам API и записи трафика данных к месту назначения. Поскольку это один из самых открытых компонентов в открытом доступе, оптимальное качество необходимо для обеспечения надежной сети для инфраструктуры IoT. Связь может осуществляться с помощью проводных, беспроводных или смешанных режимов связи, которые также могут включать в себя сети 5G.

Безопасность: Политика безопасности имеет важное значение на каждом уровне и должна обеспечиваться как часть проектирования в соответствии, помимо прочего, с последними действующими международными стандартами, специфичными для отрасли и универсальными, для аппаратных и программных компонентов. Безопасность от дизайна и тщательно реализованный уровень безопасности позволяют гарантировать непрерывность бизнеса в случае локальных или общих угроз платформе или решению.

Централизованная инфраструктура в облаке обеспечивает высокую доступность и простоту управления услугами, которые развертываются через конечные устройства, подключенные к облаку.

Кроме того, новые облачные решения помогают клиентам сделать существенный шаг к цифровой трансформации, управляя аппаратными модулями в инфраструктуре подключенных устройств. Этот подход позволяет записывать, инициализировать и управлять сроком службы устройств. Также предлагается возможность расширенного мониторинга безопасности путем выявления слабых звеньев (скомпрометированных устройств) и изоляции их от сети. Это облегчает обновление и обслуживание набора устройств одновременно из одной точки происхождения.

Безопасность дематериализованных вычислений является общей ответственностью между поставщиком дематериализованных вычислений и клиен-

том. Модель общей ответственности, по сути, имеет три категории обязанностей: обязанности, которые всегда являются обязанностями поставщика, которые всегда являются, и обязанности, которые вытекают из них. Варьируются в зависимости от модели обслуживания: Инфраструктура как услуга (IaaS), Платформа как услуга (PaaS) или Программное обеспечение как услуга (SaaS), например, электронная почта в облаке.

Обязанности по безопасности, которые всегда являются обязанностью поставщика, связаны с защитой самой инфраструктуры, а также с доступом к физическим хостам, исправлениям и конфигурацией физических хостов и физической сети, в которой работают вычислительные экземпляры и где находятся хранилище и другие ресурсы.

Обязанности по безопасности, которые всегда являются задачами клиента, включают в себя управление пользователями и их привилегиями доступа (управление личностью и доступом), защиту облачных учетных записей от несанкционированного доступа, шифрование и защиту облачных данных, а также управление их уровнем безопасности (соответствие требованиям).

Основные проблемы с точки зрения безопасности дематериализованных вычислений

Поскольку публичное облако не имеет четких периметров, оно имеет принципиально другую реальность с точки зрения безопасности. Это становится еще более сложным при принятии современных облачных подходов, таких как автоматизированные методы непрерывной интеграции и развертывания (CI/CD), распределенные системы и системы управления информацией. бессерверные архитектуры и эфемерные активы, такие как функции как сервис и онлайн-сервисы. контейнеры.

Некоторые из передовых облачных инструментов безопасности и несколько уровней риска, с которыми сталкиваются организации, ориентированные на дематериализованные вычисления, следующие:

- Увеличение поверхности атаки

Общедоступная облачная среда стала важной и очень привлекательной поверхностью атаки для хакеров, которые используют плохо защищенные порты облачного входа для доступа и нарушения рабочих нагрузок и данных. Вредоносные программы, атаки "Zero-Day", захват учетных записей и многие другие вредоносные угрозы стали повседневной реальностью.

- Отсутствие видимости и последующих действий

В модели IaaS поставщики облачных услуг полностью контролируют уровень инфраструктуры и не предоставляют его своим клиентам. Отсутствие видимости и контроля еще более заметно в моделях PaaS и SaaS. Клиенты облачных вычислений часто не могут эффективно идентифицировать и количественно оценить свои облачные активы или визуализировать свои облачные среды.

- Постоянно меняющиеся рабочие нагрузки

Облачные ресурсы предоставляются и выведены из эксплуатации динамически, в больших масштабах и на высокой скорости. Традиционные инструменты

безопасности просто не могут применять политики защиты в такой гибкой и динамичной среде с эфемерными и постоянно меняющимися рабочими нагрузками.

- DevOps, DevSecOps и автоматизация

Организации, которые приняли высокоавтоматизированную культуру CI/CD DevOps, должны обеспечить, чтобы соответствующие средства контроля безопасности были определены и интегрированы в код и модели с самого начала цикла разработки. Внедрение изменений, связанных с безопасностью, после того, как рабочая нагрузка была развернута в производстве, может поставить под угрозу безопасность организации и продлить время выхода на рынок.

- Детальное управление привилегиями и ключами

Часто роли пользователей облачных вычислений настраиваются очень неопределенно, предоставляя расширенные привилегии сверх того, что запланировано или необходимо. Распространенным примером является предоставление разрешений на удаление или запись из базы данных неподготовленным пользователям или пользователям, которым не нужно удалять или добавлять элементы из базы данных. На уровне приложения плохо настроенные ключи и привилегии подвергают сеансы риску безопасности.

- Сложные среды

Управляйте безопасностью последовательно в гибридных системах и информационных системах. Многооблачные облачные вычислительные среды, предпочитаемые предприятиями сегодня, требуют методов и инструментов, которые бесперебойно работают с поставщиками общедоступных облачных услуг, частными облаками и локальными развертываниями, включая защиту филиалов для географически распределенных организаций.

- Соблюдение требований и управление облаком

Все основные поставщики облачных услуг объединились с наиболее известными программами аккредитации, такими как PCI 3.2, NIST 800-53, HIPAA и GDPR. Тем не менее, клиенты несут ответственность за то, чтобы их рабочая нагрузка и процессы обработки данных соответствовали требованиям. Учитывая низкую видимость и динамику облачной среды, процесс аудита соответствия становится практически невозможным, если инструменты не используются для выполнения непрерывных проверок соответствия и выдачи оповещений в режиме реального времени в случае плохой конфигурации.

- Нулевое доверие и причины, по которым вы должны его принять

Термин Zero Trust был впервые введен в 2010 году Джоном Киндервагом, который в то время был старшим аналитиком в Forrester Research. Основной принцип нулевого доверия к облачной безопасности заключается в том, чтобы автоматически не доверять кому-либо или чему-либо внутри или за пределами сети, а также проверять все (т.е. авторизовать, проверять и защищать).

Например, нулевое доверие способствует стратегии управления с наименьшими привилегиями, согласно которой пользователи имеют доступ только к тем ресурсам, которые им необходимы для выполнения своих задач. Аналогичным образом, он предлагает разработчикам обеспечить надлежащую

защиту веб-приложений. Например, если разработчик не постоянно блокировал порты или не настраивал разрешения по мере необходимости, хакер, который берет под контроль приложение, будет иметь право извлекать и изменять данные из базы данных.

Кроме того, сети "Zero Trust" используют микросегментацию, чтобы сделать безопасность облачной сети гораздо более детализированной. Микросегментация создает защищенные области в центрах обработки данных и облачных развертываниях, тем самым сегментируя рабочие нагрузки относительно друг друга, защищая все внутри области и применяя политики для защиты трафика между зонами.

Ключевые принципы надежной безопасности для дематериализованных вычислений

В то время как поставщики облачных услуг, такие как Amazon Web Services (AWS), Microsoft Azure (Azure) и Google Cloud Platform (GCP), предлагают множество облачных функций и услуг безопасности, дополнительные сторонние решения имеют важное значение для обеспечения безопасности на уровне предприятия. защита облачных рабочих нагрузок от нарушений, утечек данных и целевых атак в облачной среде. Только интегрированный стек безопасности (на базе облака/сторонний) предлагает централизованную видимость и детализированный контроль на основе правил, необходимых для реализации следующих лучших отраслевых практик:

Детальное управление IAM и аутентификация на основе правил в сложных инфраструктурах

Работа с группами и ролями, а не на индивидуальном уровне IAM, чтобы облегчить обновление определений IAM по мере развития потребностей компании. Предоставление только минимальные привилегии доступа к ресурсам и API, которые необходимы для выполнения задач группы или роли. Чем больше привилегий, тем выше уровни аутентификации. Нельзя пренебрегать хорошей гигиеной IAM, применяя надежную политику паролей, время ожидания авторизации и т. д.

Сетевая безопасность с нулевым доверием для облака элементов управления в логически изолированных сетях и микросегментах

Развертывание критически важных ресурсов и приложений в логически изолированных разделах облачной сети провайдера, таких как виртуальные частные облака (AWS и Google) или vNET (Azure). Используйте подсети для микросегмента рабочих нагрузок относительно друг друга с детальными политиками безопасности на уровне шлюза подсети. Используйте выделенные WAN-каналы в гибридных архитектурах и используйте определяемые пользователем конфигурации статической маршрутизации для настройки доступа к виртуальным устройствам, виртуальным сетям и их шлюзам, а также к общедоступным IP-адресам.

Реализация политик и процессов защиты виртуального сервера, таких как управление изменениями и обновление программного обеспечения:

- Поставщики решений для безопасности для облачных вычислений предлагают Cloud Security Posture Administration. Внедрение правил и моделей управления и соответствия требованиям при подготовке виртуальных серверов, аудите пробелов в конфигурации и автоматическом исправлении, когда это возможно.
- Защита всех приложений (включая облачные распределенные приложения) с помощью брандмауэра веб-приложений следующего поколения. Она будет детально проверять и контролировать трафик на серверы веб-приложений и с них, автоматически обновлять правила WAF в ответ на изменения в поведении трафика и будет развернут как можно ближе к микросервисам, которые выставляют рабочие нагрузки.

Улучшенная защита данных

Улучшенная защита данных за счет шифрования на всех уровнях транспортировки, защиты файловых ресурсов и коммуникаций, непрерывного управления рисками соответствия и поддержания хорошей гигиены в ресурсах хранения данных, таких как обнаружение плохо настроенных контейнеров и остановка орфанных ресурсов.

Аналитика угроз, которая обнаруживает известные и неизвестные угрозы и устраняет их в режиме реального времени

Сторонние поставщики облачной безопасности добавляют контекст к большим и диверсифицированным потокам облачных журналов, интеллектуально пересекая агрегированные данные журнала с внутренними данными, такими как системы управления активами и конфигурацией, сканеры уязвимостей и т. д., и внешние данные, такие как потоки публичной информации об угрозах, базы данных геолокации и т. д. Они также предоставляют инструменты, которые позволяют визуализировать и подвергать сомнению ландшафт угроз и способствовать более быстрому времени реагирования в случае инцидента. Алгоритмы обнаружения аномалий на основе искусственного интеллекта применяются для выявления неизвестных угроз, которые затем подвергаются криминалистическому анализу для определения их профиля риска. Оповещения в режиме реального времени о вторжениях и нарушениях правил сокращают время исправления, иногда даже запуская рабочие процессы самоустранения.

Заключение

Облачная безопасность - это ответственность, которую разделяют поставщик облачных услуг и заказчик. В модели совместной ответственности, по сути, существует три категории обязанностей: ответственность, которая всегда лежит на поставщике, ответственность, которая всегда лежит на клиенте, и ответственность, которая варьируется в зависимости от модели обслуживания: Инфраструктура как услуга (IaaS), Платформа как услуга (PaaS) или программное обеспечение как услуга (SaaS), например, облачная электронная почта.

Обязанности по обеспечению безопасности, которые всегда возлагаются на поставщика, связаны с защитой самой инфраструктуры, а также с доступом к

физическим хостам и физической сети, на которых работают вычислительные инстансы, а также с хранилищем и другими ресурсами.

Обязанности по обеспечению безопасности, которые всегда возлагаются на клиента, включают управление пользователями и их правами доступа (управление идентификацией и доступом), защиту облачных учетных записей от несанкционированного доступа, шифрование и защиту облачных данных, а также управление уровнем безопасности (соответствие требованиям).

Список источников

1. «Архитектура облачной безопасности». GuidePoint Security LLC. 2023. 06 декабря 2023 г.

2. Канакер, Хасан; Абдель Карим, Надер; А.Б. Аввад, Самер; Х.А. Исмаил, Нурул; Зраку, Джамал; М. Ф. Аль Али, Абдулла (20 декабря 2022 г.). «Обнаружение заражения троянскими программами в облачной среде с помощью машинного обучения». Международный журнал интерактивных мобильных технологий. 16 (24): 81–106. doi:10.3991/ijim.v16i24.35763.

3. Confidentiality, Integrity and Availability - The CIA Triad". CertMike. 2018-08-04. Retrieved 2021-11-27.

УДК 62

ГЛАВА 13. КИБЕРБЕЗОПАСНОСТЬ. РИСКИ И ПРЕИМУЩЕСТВА ПЕРЕДОВЫХ ОБЛАЧНЫХ РЕШЕНИЙ

Аменицкий Алексей Владимирович
аспирант
Санкт-Петербургский государственный электротехнический университет ЛЭТИ имени В.И. Ульянова (Ленина)

Научный руководитель: Воробьёв Евгений Германович
д.т.н., профессор
Санкт-Петербургский государственный электротехнический университет ЛЭТИ имени В.И. Ульянова (Ленина)

Аннотация: Облачные решения приносят много преимуществ, но также создают новые опасности. Невозможно представить мир, в котором встроенные системы, будь то в наших автомобилях, умных домах или критически важных инфраструктурах, работают уверенно и гарантированно защищены от киберугроз. Во всех областях, от Интернета вещей до автономных транспортных средств и критически важных инфраструктур, встроенные системы развиваются экспоненциально.

Переход к облачным архитектурам и инновациям создает новые формы сложности, с которыми ИТ-организации могут быть не готовы справиться. Если не управлять этой сложностью должным образом, она может привести к серьезным проблемам. В этой главе рассмотрены факторы, вызывающие эту сложность, и способы укрепления кибербезопасности в облаке.

Ключевые слова: Cyber Security (CS), CS architecture, CS trends, CS tendences, CS tools, CS crimes, CS latest news, CS releases, CS game-changers, CS future, CS playbook, CS agenda, CS future, CS risks, CS incidents, CS resilience, Hackers, CS прогноз, Artificial Intelligence, Deep Fakes, Эволюция киберУгроз, КиберГигиена.

CYBERSECURITY. RISKS AND BENEFITS OF ADVANCED CLOUD SOLUTIONS

Amenitsky Alexey Vladimirovich

Scientific supervisor: Vorobyov Evgeny Germanovich

Облачные решения – это предоставление размещенных услуг, включая программное обеспечение, аппаратное обеспечение и хранилище, в Интернете. Преимущества быстрого развертывания, гибкости, низких первоначальных затрат и масштабируемости сделали облачные вычисления практически универсальными в организациях всех размеров, часто как часть гибридной/многооблачной архитектуры инфраструктуры.

Безопасность облачных решений относится к технологиям, политикам, элементам управления и услугам, которые защищают данные, приложения и

инфраструктуру облачных вычислений от угроз. Новые облачные решения предназначены для обеспечения комплексного пользовательского опыта, начиная от осведомленности сотрудников о кибербезопасности, соблюдения политики, управления угрозами, вопросов конфиденциальности, реагирования на инциденты, управления угрозами и уязвимостями, управления журналами, отчетности и визуализации.

Во всем мире многие организации внедряют облачные решения. Эта технология имеет много сильных сторон, особенно во время роста удаленной работы и цифровой трансформации. Среди его преимуществ можно упомянуть гибкость и расширяемость. В некоторых случаях это также может привести к сокращению расходов на инфраструктуру. Многие поставщики облачных услуг также упоминают безопасность в качестве преимущества. Действительно, функции защиты напрямую интегрированы в платформы хранения данных и другие облачные вычислительные сервисы.

Тем не менее, многие компании совершают ошибку, думая, что облако абсолютно безопасно. Киберпреступники пользуются этим избытком доверия и все чаще атакуют эти среды. Кроме того, облако также вводит новые опасности.

Опасности облачных решений

Одна из самых больших угроз облачной безопасности связана с человеческой ошибкой: это неправильная настройка информационной безопасности. Это может привести к воздействию или утечке данных. Кроме того, если облако упрощает обмен данными в целях совместной работы, это обооюдоострое оружие. Конфиденциальная информация может быть передана третьим лицам по ошибке.

Многие компании пренебрегают резервным копированием данных, хранящихся в облаке, из-за стоимости и сложности этих резервных копий. Опять же, последствиями могут быть утечка или потеря информации в случае поломки или атаки программ-вымогателей.

Еще одна опасность связана с API (интерфейсами прикладного программирования), позволяющими взаимодействие между облачными приложениями. Тем не менее, они могут содержать уязвимости, которые позволяют любому получить доступ к конфиденциальным данным компании. В частности, киберпреступники могут использовать уязвимые API с помощью DDoS-атак или инъекций кода. Эти интерфейсы стали основным вектором атак в 2025 году. Кроме того, многие компании предполагают, что облако безопасно от вредоносных программ. Это миф, и зло, которое проникло в систему, может быстро распространиться. Например, можно упомянуть Cloud Snooper, который заразил серверы, размещенные на AWS в 2020 году.

Наконец, плохое управление доступом к облаку может иметь серьезные последствия. Если хакеру удается подключиться к учетной записи, он может перейти в сторону, чтобы получить доступ к конфиденциальным данным или нанести серьезный ущерб всей организации.

Столкнувшись с многочисленными угрозами, надвигающихся в облаке,

необходимо внедрить лучшие практики кибербезопасности. Первым шагом является защита сети с помощью таких инструментов, как брандмауэры и современное антивирусное программное обеспечение, предлагающее функции мониторинга. Резервное копирование данных также должно проводиться регулярно.

В целом, важно принять проактивное отношение. Когда происходит кибератака, часто слишком поздно вмешиваться. Чтобы предвидеть эти инциденты, компании должны обновлять свое программное обеспечение, использовать зашифрованные пароли и системы многофакторной аутентификации, а также проверять стандарты безопасности используемых приложений и расширений.

Облачная безопасность является серьезной проблемой и касается всех отделов компании. Поэтому крайне важно набирать экспертов и обучать каждого сотрудника основным практикам кибербезопасности.

Кибератаки вошли в нашу повседневную жизнь... И одновременно с массовым переходом в облако радикально изменились правила хостинга и управления данными, равно как и способы построения инфраструктуры и сервисов. Это не могло не вызвать определенную тревогу среди заинтересованных специалистов. Парадокс? В то время, когда киберугрозы затрагивают каждого, те, чья работа заключается в их предотвращении, говорят, что они потеряли видимость...

Искусственный интеллект, облако, SIEM и устаревание: что ждет индустрию кибербезопасности

Кибербезопасность требует постоянного развития, поскольку преступники постоянно находят новые уязвимости и приспосабливаются, чтобы обойти существующие средства защиты. Количество атак на облачные среды утроилось по сравнению с предыдущим годом, что должно побудить организации внедрить новые методы.

Чтобы справиться с теми, кто атакует облако, защита всего цикла разработки программного обеспечения потребует постоянного внимания. Безопасность облака никогда не была такой важной. Столкнувшись с неопределенной глобальной экономической ситуацией, компании сосредотачиваются на управлении командами, работающими удаленно и/или в гибридном режиме. В то же время киберпреступники разрабатывают все более изощренные, опасные и разрушительные атаки.

Согласно недавним исследованиям, использование облачных вычислений увеличилось на 95 %, а число лиц, создающих угрозы для этой конкретной среды, за последний год увеличилось более чем в три раза. В то же время расширение облачного рынка, развитие DevOps и более широкое использование платформ разработки (с небольшим количеством кода или без него) приводят к резкому увеличению числа приложений и микросервисов, работающих в облачных средах.

Однако из-за быстрого и динамичного характера разработки приложений предприятия не могут поддерживать полное представление о каждом приложении, микросервисе, базе данных и зависимостях, присутствующих в их средах.

Этот предел создает огромный риск, который оппоненты, облачные эксперты, постоянно пытаются использовать. В 2025 году компаниям, которые хотят выиграть эту битву, необходимо будет сосредоточить свои усилия на обеспечении безопасности всей своей облачной среды – как с точки зрения приложений, так и с точки зрения инфраструктуры.

Слепые зоны, создаваемые искусственным интеллектом, открывают двери для новых рисков для бизнеса. Эксперты ожидают, что киберпреступники обратят свое внимание на системы искусственного интеллекта (ИИ) и превратят их в новый источник угроз для бизнеса. Речь идет об уязвимостях, обнаруженных в авторизованных развертываниях искусственного интеллекта, и слепых пятнах, связанных с несанкционированным использованием сотрудниками инструментов искусственного интеллекта.

Стремительный рост внедрения и использования ИИ за последний год ставит под угрозу группы безопасности, которые все еще находятся на начальных этапах понимания моделей угроз, с которыми они сталкиваются при развертывании своих проектов в области ИИ, и отслеживания несанкционированных инструментов ИИ которые сотрудники внедряют в свою среду. Однако эти слепые пятна и новые технологии открывают двери для киберпреступников, которые хотят проникнуть в корпоративные сети или получить доступ к конфиденциальным данным.

Более того, сотрудники, которые полагаются на инструменты искусственного интеллекта без надзора групп безопасности, подвергают свой бизнес новым рискам защиты данных. Это связано с тем, что корпоративные данные, вводимые в решения ИИ, находятся не только в пределах досягаемости злоумышленников, которые пытаются извлечь их, используя уязвимости этих инструментов. Они также могут быть раскрыты или переданы неавторизованным сторонам в рамках протокола обучения системы.

Предприятиям необходимо будет проанализировать точки внедрения ИИ (по официальным и неофициальным каналам) в своей структуре, оценить степень риска и разработать стратегические руководящие принципы для обеспечения безопасного и проверяемого использования, минимизирующего риски и расходы, и в то же время максимизирующего их ценность.

Ресурсы искусственного интеллекта в облачном режиме-выгодная возможность для противников. В то время как многие считают ИИ основной тенденцией корпоративных инвестиций в ближайшие годы, недавнее исследование показало, что 47% специалистов по кибербезопасности признают, что обладают минимальными техническими знаниями в области ИИ, если таковые вообще имеются. Другая проблема: ИИ ставит новые задачи в области безопасности, поскольку этим системам требуется доступ к огромным наборам данных, большую часть времени хранящимся в облаке. Действительно, обеспечение безопасности этих данных и обеспечение того, чтобы модели искусственного интеллекта, работающие в облаке, не использовались в злонамеренных целях, вызывает растущую обеспокоенность. Внедрение комплексной платформы защи-

ты облачных приложений CNAPP (Cloud Native Application Protection Platform) станет более важным, чем когда-либо, для противодействия злоумышленникам.

SIEM старого поколения больше не отвечают потребностям SOC. Медленные и дорогостоящие, они возникли в эпоху, когда объемы данных, скорость действий злоумышленников и уровень сложности угроз составляли лишь малую часть того, чем они являются сегодня. Таким образом вместо того, чтобы пресекать нарушения, команды оказываются вынужденными тратить больше времени и ресурсов на настройку, обслуживание и извлечение соответствующей информации о безопасности из своих SIEM.

Однако при скорости работы, приближающейся к 7 минутам для самых быстрых злоумышленников, SIEM старого поколения просто больше не справляются с этой задачей. Командам безопасности нужны решения, которые намного быстрее, проще в развертывании и более экономичны, чем существующие подходы. SIEM, управляемый SOC, должен быть полностью переработан с учетом опыта аналитиков в области безопасности. Рынок потребует принятия решений, способных унифицировать все функции (SIEM, SOAR, EDR, XDR и т. д.) В рамках облачной платформы, управляемой искусственным интеллектом, для более эффективной, быстрой и экономичной защиты.

Продукты с истекшим сроком годности - это настоящие защитные фильтры, которых так жаждут оппоненты. В 2024 году, когда злоумышленники будут все более склонны использовать малейшие уязвимости, компаниям любой ценой придется объединить свои ИТ-операции и операции в области безопасности. Среди критических недостатков, которые им необходимо будет устранить, - продолжающееся использование продуктов с истекшим сроком службы (EOL), которые пользуются популярностью у киберпреступников.

В результате анализа, проведенного в период с сентября 2023 года по сентябрь 2024 года, было обнаружено растущее использование продуктов с истекшим сроком службы для нацеливания на шлюзы, операционные системы и приложения. Также были выявлены несколько групп злоумышленников, которые намеренно нацелены на продукты с истекшим сроком эксплуатации, особенно на Windows, либо используя известные эксплойты многолетней давности, либо активно разрабатывая новые эксплойты для продуктов, уязвимости которых не могут быть исправлены.

Тревожный факт: многие из этих продуктов, такие как Windows 8.1, MS SQL Server 2012 и Windows Server 2003, выпущенные более десяти лет назад, все еще используются сегодня. В 2024 году, когда киберпреступники будут попрежнему нацелены на эти критические уязвимости, компаниям, как никогда ранее, необходимо будет консолидировать свои ИТ-операции и операции в области безопасности, чтобы обеспечить прозрачность инвентаризации своих активов, не отставать от надвигающегося устаревания программного обеспечения и целевых систем для обновления/сокращения/замены технологий. насколько это возможно.

ИТ-директора и ИБ-директора делают ставку на платформы, чтобы улуч-

шить свои показатели в области безопасности и ИТ. В то время как ИТ-директоров и ИБ-директоров просят делать больше с меньшими затратами. Ближайшее будущее ознаменуется общесекторальными изменениями: компании перейдут на платформы, а не на традиционные специализированные решения. Подход, который разрушит операционные разрозненности и снизит сложность и затраты. Расширение сотрудничества между ИТ-директорами и ИБ-директорами требует принятия платформы, которая обеспечивает решение проблем как друг друга, так и ИТ-директоров. Другими словами, платформа, основанная на искусственном интеллекте, которая предотвращает нарушения безопасности и обеспечивает единую и экономически эффективную контрольную точку для ИТ-директоров.

Кампании по взлому и утечке, встраивание измененного или фальсифицированного контента, преувеличение информации или продвижение определенных тем… Эти злоумышленники используют целый комплекс операций для достижения своих целей. Последние достижения в области генеративного искусственного интеллекта (аудио, изображения, видео, тексты и т. д.) позволяют авторам угроз иметь дополнительные инструменты и функции для создания вредоносного контента. Это усложнило бы избирателям способность отличать правду от лжи. Заинтересованные специалисты по искусственному интеллекту и все сообщество кибербезопасности, должны будут работать сообща, чтобы отслеживать и предвидеть изменения в этой области.

Несмотря на состояние экономики, ожидается, что в 2026 году на ИТ-рынке произойдет значительный рост. Ожидается, что на мировом рынке произойдет ускорение и расходы на ИТ будут стремительно расти и вырастут более чем на 10% по сравнению с менее чем 7% в 2024 году..

Несмотря на сложную экономическую ситуацию, расходы на ИТ в мире остаются невосприимчивыми к рецессии. Ожидается, что в течение следующих нескольких месяцев ИТ-директора сосредоточат свое внимание на контроле затрат, эффективности и автоматизации текущих проектов, одновременно сокращая инициативы, для реализации которых требуется больше времени для окупаемости инвестиций.

Нехватка специалистов: вызовы и возможности

Поскольку отрасль в основном состоит из поставщиков услуг, неудивительно, что ожидаемое увеличение доходов сопровождается увеличением численности персонала. Таким образом, около трёх четвертей поставщиков ожидают увеличения численности своих групп специалистов. Однако количество проектов по набору персонала сократилось по сравнению с прошлым годом.

Нехватка квалифицированного персонала в области ИТ в прошлом году несколько уменьшилась. Тем не менее, конкуренция между поставщиками и компаниями-пользователями за наем лучших специалистов по-прежнему будет жесткой. Наем экспертов и удовлетворение спроса при ограниченных ресурсах, кстати, являются одними из основных проблем, с которыми в настоящее время сталкиваются поставщики услуг.

В то же время сложность поиска специалистов также стимулирует спрос на услуги по аренде персонала – это предлагает каждый второй поставщик. В прогнозах на 2025 год отмечалось то же самое явление на глобальном уровненаблюдается миграция ИТ-навыков из ИТ-отдела компании к поставщикам технологий и услуг. У ИТ-директоров нет ни сотрудников, ни талантов, необходимых для выполнения всей необходимой работы, и они обращаются к сервисным компаниям за заполнением пробелов.

Кибербезопасность, основанная на облаке и искусственном интеллекте

Лидерами среди областей, в которых поставщики стремятся увеличить свои доходы, являются кибербезопасность (41%) и услуги, связанные с миграцией в облачные инфраструктуры (37%), поскольку эти среды стимулируют проекты по трансформации ИТ-операций (DevOps, SecOps и т. д.). За ними следуют за индивидуальная разработка приложений и проекты по использованию данных, причем последняя тема сама определяет значительную часть инициатив в области искусственного интеллекта.

Перспективы увеличения доходов в сфере кибербезопасности не могут не удивлять. Эта тема является приоритетной во всех организациях и во всем мире как в связи с ростом числа атак, так и в связи с изменением ИТ-среды. Продолжающееся внедрение облачных технологий, сохранение гибридной рабочей силы, быстрое появление и использование генеративного ИИ и меняющаяся нормативно-правовая среда вынуждают руководителей, отвечающих за безопасность и управление рисками, увеличивать свои расходы в этой области.

Ожидается, что расходы, связанные с конфиденциальностью данных и облачной безопасностью, будут расти самыми быстрыми темпами (более чем на 24% в период с 2023 по 2024 год). Поскольку новые законы, влияющие на обработку персональных данных, продолжают появляться, защита конфиденциальности по-прежнему остается главной заботой организаций. Что касается облака, то его растущее внедрение идет рука об руку с необходимостью защиты этих сред. Расходы на облачные платформы защиты рабочих нагрузок (CWPP) и программное обеспечение для контроля доступа к облаку (CASB) в 2025 году составят 7 миллиардов долларов, что на 24,7 процента больше, чем в 2024 году.

Что касается облака, то в 2025 году сфера продолжает свой стремительный рост, увеличившись на 20,4%. Эти оптимистичные прогнозы касаются всех сегментов глобального облачного рынка. И именно услуги IaaS, как ожидается, будут иметь самый устойчивый рост (+26,6%), за которыми следуют услуги PaaS (+21,5%).

Ожидается, что продолжающийся рост объемов данных будет способствовать росту отрасли, равно как и обещанный рост генеративного ИИ, который чаще всего переходит в облако. Эти прогнозы касаются доходов облачных провайдеров, в первую очередь гиперскалеров. Однако многие местные поставщики ИТ-услуг уже пользуются этим преимуществом и будут продолжать пользоваться им, учитывая потребности своих клиентов в поддержке в облаке (миграция, управление, оптимизация и т. д.).

Помимо технологических областей, развитие ИТ-рынка будет зависеть от конъюнктуры и глобальной ситуации, поскольку потребности в технологиях в периоды доверия и ориентации на рост будут отличаться от потребностей в периоды неопределенности и ориентации на затраты. Это также будет зависеть от внимания, которое компании уделяют вопросам экологии и суверенитета. Публичное облако, которое раньше иногда воспринималось как угроза кибербезопасности, постепенно становится все более популярным в качестве актива для повышения киберустойчивости предприятий.

Кибербезопасность теперь стоит на первом месте в повестке дня руководителей. И это справедливо: векторы атак многочисленны и целенаправленны, они старые и постоянно обновляются и, следовательно, требуют поиска новых подходов к защите как ИТ-инфраструктуры, так и данных.

Когда появилось публичное облако, оно в первую очередь отвечало потребностям предприятий в адаптивности, совместном использовании и гибкости ресурсов, не всегда входя в рамки традиционных структур, посвященных безопасности информационных систем. Теперь облако обеспечивает не только очень высокий уровень безопасности данных и операций, но и отказоустойчивость инфраструктуры, необходимую для успешной цифровой трансформации.

Количество приложений растет, цифровые среды усложняются, а инфраструктура меняется в масштабе. В результате становится все труднее поддерживать требования безопасности на должном уровне и обеспечивать соблюдение правил киберуправления на протяжении всего жизненного цикла приложений.

Видимость угроз - большая часть проблемы. Мы не можем защитить свою организацию от того, чего не видим. Этот вопрос возникает тем более, что многие компании используют широкий спектр терминалов, локальных и удаленных, и могут использовать свои собственные серверы, частные и общедоступные облака, увеличивая тем самым свою выставочную площадь.

Если исчерпывающее представление об угрозах не всегда возможно, то, по крайней мере, необходимо точно идентифицировать его активы и их уязвимости. Это также предполагает эволюцию его подхода к безопасности. В сложных средах теперь необходимо прибегать к новейшим достижениям в технологическом ландшафте – ландшафте, который в настоящее время в значительной степени использует автоматизацию, концепцию безопасности, встроенную в продукты, и машинное обучение (ML), способствующее демократизации дисциплины и ее совершенствованию. использование большим числом. Поэтому, чтобы снизить риск обхода возможных уязвимостей или критических предупреждений, необходимо, во-первых, иметь максимальную видимость своей среды и использовать новейшие технологические возможности в области операций по обеспечению безопасности.

Предвидеть и реагировать, создавая общую перспективу

Концепция общей перспективыы - это эволюция исторической модели совместной ответственности. Это происходит, когда поставщик облачных услуг и клиент работают вместе, как команда, для достижения общей цели. Это более

широкая версия совместной ответственности, которая охватывает, но также выходит за рамки этого. Фактически, общая перспектива означает, что облачный провайдер принимает активное участие в обеспечении безопасности своих клиентов, в том числе в рамках своих обязанностей. Это партнерство включает в себя предоставление безопасных конфигураций по умолчанию для облачных развертываний ; предоставление рекомендаций по передовым методам обеспечения безопасности; и помощь в управлении рисками.

Облачное "нулевое доверие" для ограничения рисков

Миграция в облако представляет собой реальный рычаг с точки зрения безопасности и позволяет извлечь выгоду из объединения усилий в этой области : защищенной инфраструктуры, повышения эффективности операций, высокоуровневых навыков в области кибербезопасности. Кроме того, в Google Cloud все архитектуры безопасности основаны на принципе « нулевого доверия » . Хотя этот термин можно буквально перевести как " нулевое доверие", мы, тем не менее, не должны неправильно понимать его значение : цель состоит в том, чтобы действительно создать доверие (аутентифицировать пользователя, предоставить доступ к данным, разрешить использование приложения и т. д.), Но не предвзято относиться к нему. априорное доверие, которое было бы основано, например, на единственном месте подключения терминала. Этот принцип способствует более детальному и контекстуальному контролю и способствует лучшей видимости. Таким образом, архитектура « нулевого доверия » обеспечивает лучшую устойчивость к традиционным векторам атаки.. Такой подход к обеспечению безопасности-с момента разработки решения и на всех уровнях инфраструктуры-способствует созданию общего доверия между организацией и ее облачным провайдером и в значительной степени способствует управлению безопасностью во все более распределенных информационных системах.

Облако может и должно служить обеспечению безопасности корпоративных данных. Скоординированный и ответственный подход, совместно используемый и принимаемый поставщиком облачных услуг, необходим не только для удовлетворения требований безопасности, конфиденциальности и суверенитета, но и для создания доверия, необходимого для любого цифрового и экономического успеха

2020 год был, в частности, годом перемен. Пандемия вынудила многие компании перенести большую часть своего бизнеса в Интернет, что позволило сотрудникам работать из дома, подписаться на новые услуги SaaS, создать новые каналы продаж и многое другое. Хотя это внезапное изменение помогло защитить безопасность сотрудников, сохранить непрерывность бизнеса и вернуть часть потерянного дохода. Эта ситуация также создала лазейки в безопасности для компаний, вынудив их найти наилучший способ защитить свою информацию и уменьшить последствия возможных кибератак. Именно в этом контексте облачная кибербезопасность приобрела большое значение на предприятии.

В последние годы крупные компании, такие как Adobe, Sony, Target, Equifax и Marriott, подверглись кибератакам. Было выявлено более полудюжи-

ны методов, используемых преступниками для компрометации или удаления данных. Но не только бизнес-гиганты подвергаются риску того, что их данные будут скомпрометированы. Малые и средние предприятия по-прежнему сталкиваются с угрозой киберпреступности в краткосрочной и среднесрочной перспективе.

Можно определить облачную кибербезопасность как совокупность технологий, протоколов и передовых методов, которые помогают защитить информационные среды, приложения и данные, хранящиеся или работающие в облаке. Сегодня более 90% крупных компаний используют эту ИТ-среду, поэтому им необходимо внедрить эффективные инструменты безопасности против любого типа виртуальных угроз, которые возникают в повседневной жизни.

Устаревшие системы, которые все еще существуют в некоторых компаниях, открывают большие лазейки, которые киберпреступники используют, чтобы нанести значительный ущерб ИТ-структуре компании, и требуют выкупа при условии их остановки. Именно по этой причине все больше и больше компаний предпочитают внедрять облачные решения, чтобы снизить риски этих атак и получить новые инструменты защиты. Но, к сожалению, в последние годы количество кибератак в облаке увеличилось, поэтому поставщики этой услуги постоянно развиваются, чтобы иметь возможность предлагать своим клиентам полную безопасность всех своих ресурсов, размещенных в этой среде.

Преимущества облачной кибербезопасности

Предприятия получают несколько преимуществ, размещая свои операционные и технологические ресурсы в облаке и внедряя инструменты кибербезопасности в этой среде. Среди них:

Безопасность в руках экспертов

Сегодня облако обеспечивает лучшую защиту данных, чем хранение их в помещениях компании. Это связано с расширенными возможностями ИТ-персонала, единственной задачей которого является защита ваших данных. Эти ИТ-специалисты часто имеют квалификацию, образование и опыт, которые намного превосходят те, которые используются в компании.

Лучшие технологии безопасности при меньших затратах

Облачные клиенты могут воспользоваться преимуществами более качественных технологий, разделив затраты на более дорогие и лучше защищенные технологии с другими клиентами. Кроме того, возможность использования инструментов совместной работы позволяет компаниям повысить производительность за счет сокращения повседневных задач, обязанностей и стресса, связанных с управлением центром обработки данных.

Шлюзы безопасности данных

Облачные клиенты могут воспользоваться преимуществами лучшего доступа к данным, лучшего мониторинга и отслеживания, а также реагирования на аномалии. Настоящая безопасность заключается не только в предотвращении и противодействии атакам, но и в наличии плана реагирования на инциденты для предотвращения вторжений. Этот последний элемент обычно упускает-

ся из виду большинством компаний. Кризис-это не время для тестирования процесса, который, как вы надеетесь, вы никогда не будете использовать.

Управление состоянием облачной безопасности

Многие организации используют публичную облачную инфраструктуру для управления своими организациями. Но если облачная среда организации настроена неправильно или управляется неэффективно, это может привести к дорогостоящим и разрушительным утечкам данных.

В этом может помочь управление состоянием безопасности в облаке (CSPM). CSPM — важнейший компонент облачной безопасности, предназначенный для защиты облачных сред от потенциальных угроз. По сути, CSPM направлено на выявление и устранение рисков безопасности, неправильных настроек и нарушений нормативных требований в облачных средах.

Инструменты CSPM предоставляют организациям информацию о своей облачной инфраструктуре, позволяя им постоянно отслеживать состояние безопасности своих облачных ресурсов и управлять им. Они предупреждают ИТ-команды о неправильных настройках и выявляют уязвимости, которыми могут воспользоваться злоумышленники.

Облачные платформы, как правило, очень безопасны. Но ИТ-команды могут недооценивать потенциальные угрозы. Некоторые могут просто пренебрегать правильной настройкой своих облачных ресурсов. Неправильная настройка стала причиной крупнейших утечек данных в облаке на сегодняшний день.

CSPM гарантирует, что облачные ресурсы:

- Прошли аудит
- Организованы/структурированы/систематизированы
- Правильно настроены
- Обеспечены поддержкой
- Соответствует законам и правовым руководящим принципам

Как работает CSPM

CSPM отслеживает любые неправильные конфигурации или неподходящие настройки, которые могут подвергнуть вашу организацию риску возникновения проблем с безопасностью. Вот краткий обзор работы CSPM:

Видимость: инструменты CSPM обеспечивают полное представление об облачных ресурсах организации, включая виртуальные машины, хранилища, сети и приложения на нескольких облачных платформах и сервисах.

Непрерывный мониторинг: решения CSPM предназначены для непрерывного мониторинга облачных сред на предмет неправильных настроек, рисков для безопасности и нарушений нормативных требований, что позволяет организациям выявлять и устранять проблемы в режиме реального времени.

Автоматическое устранение неполадок: современные достижения в области CSPM позволяют организациям автоматически выявлять и устранять неправильные настройки и нарушения требований, снижая риск инцидентов, связанных с безопасностью, и помогая поддерживать безопасную и соответствующую требованиям облачную среду.

Обеспечение соблюдения политик: CSPM позволяет организациям определять и обеспечивать соблюдение политик безопасности на основе отраслевых стандартов, передовых методов и нормативных требований, гарантируя, что их облачные ресурсы настроены безопасно и единообразно.

Управление соответствием требованиям: инструменты CSPM помогают организациям соблюдать требования, предоставляя возможности автоматизированной оценки соответствия требованиям, составления отчетов и устранения неполадок.

Интеграция с существующими инструментами: решения CSPM могут интегрироваться с существующими инструментами и рабочими процессами в сфере безопасности, позволяя организациям оптимизировать свои операции по обеспечению безопасности и повысить общий уровень безопасности.

Роль CSPM — это нечто большее, чем просто разовое решение. С помощью решений CSPM можно в режиме реального времени отслеживать состояние вашей облачной среды, чтобы ваша команда была готова к любым возможным рискам. В мире, где компании полагаются на сложные мультиоблачные архитектуры, CSPM — это невоспетый герой кибербезопасности. Он обеспечивает безопасность и защиту вашей облачной среды, чтобы команды могли сосредоточиться на более важных бизнес-вопросах.

Значимость CSPM

В современном цифровом мире большинство компаний в значительной степени полагаются на облачные технологии. Инструменты CSPM позволяют получить общее представление об облачных средах, чтобы выявлять уязвимости и неправильные настройки, которые могут привести к кибератакам. Без CSPM это всё равно что оставить входную дверь широко открытой, чтобы хакеры могли беспрепятственно проникнуть внутрь.

В 2025 году 99% сбоев в облачной безопасности происходят по вине клиентов. Именно поэтому надёжное решение CSPM является обязательным для любого бизнеса, зависящего от облачных технологий.

Обеспечение соответствия требованиям: в условиях GDPR и HIPAA CSPM поможет вам соблюдать закон.

Сокращение поверхности атаки: CSPM сканирует вашу облачную инфраструктуру, выявляя риски для кибербезопасности до того, как они станут уязвимостями.

Минимизация утечек данных: инструменты CSPM постоянно отслеживают неправильные настройки и нарушения требований. Согласно исследованиям, CSPM может сократить количество инцидентов, связанных с безопасностью в облаке, на 80% из-за неправильных настроек.

Упрощение операций по обеспечению безопасности: CSPM упрощает управление несколькими облачными средами, предоставляя единое представление обо всех ваших ресурсах.

Масштабируемость: инструменты CSPM могут масштабироваться в соответствии с потребностями растущих организаций, поддерживая большие и

сложные облачные среды.

Наличие надёжной стратегии CSPM — это как наличие мощного защитного механизма на вашей стороне. Он защищает от угроз, соответствует передовым практикам и повышает общий уровень кибербезопасности.

Ключевые преимущества CSPM

Важность управления состоянием безопасности в облаке (CSPM) трудно переоценить. Оно играет ключевую роль в защите сложных облачных сред и обеспечении безопасности конфиденциальных данных, хранящихся в облаке, от вредоносных действий.

- Точное определение неправильно настроенного сетевого подключения

Инструменты CSPM предназначены для выявления неправильных настроек в вашей сети в режиме реального времени. Это могут быть неправильно настроенные группы безопасности или AWS. Выявляя эти проблемы на ранней стадии, вы можете предотвратить несанкционированный доступ к вашим облачным ресурсам, который может привести к утечке данных или компрометации.

- Оценка риска передачи данных

Возможность оценивать риски, связанные с данными, — ещё одно важное преимущество CSPM. В облачных сервисах часто хранится критически важная бизнес-информация, и любой взлом может привести к серьёзным последствиям для бизнеса. Надежное решение CSPM помогает организациям выявлять потенциальные риски и уязвимости в своей облачной инфраструктуре, тем самым защищая конфиденциальные данные.

- Определение разрешений учетной записи

Во многих случаях пользователям предоставляется больше разрешений, чем необходимо, что создаёт значительные риски для безопасности, если их не отслеживать. С помощью решений CSPM такие чрезмерно широкие разрешения для учётных записей можно быстро обнаружить и исправить до того, как они станут проблемой.

- Непрерывный мониторинг облачной среды

Динамическая природа облачных сред делает их мощными, но в то же время сложными для поддержания оптимального уровня безопасности. Непрерывный мониторинг с помощью CSPM позволяет получать информацию об изменениях конфигурации или моделях поведения пользователей, указывающих на потенциальную угрозу. Такой упреждающий подход позволяет ИТ-командам и специалистам по кибербезопасности оперативно реагировать на подозрительные действия.

- Автоматизированное исправление неправильной конфигурации

Помимо обнаружения проблем, некоторые продвинутые CSPM предоставляют возможности автоматического исправления распространенных ошибок конфигурации в приложениях SaaS и контейнерных средах. Эта функция значительно сокращает время на исправление, одновременно повышая общую целостность системы. Например, унифицированная защита рабочей нагрузки в облаке обеспечивает бесперебойное обнаружение и разрешение без нарушения

бизнес-операций. Такая автоматизация повышает эффективность и сводит к минимуму человеческие ошибки, связанные с ручными исправлениями.

Соответствие Стандартам

Помимо устранения угроз, мониторинг соответствия требованиям является неотъемлемой частью стратегий киберзащиты большинства предприятий. Комплексный инструмент CSPM помогает компаниям соблюдать нормативные стандарты, такие как GDPR, HIPAA и т. д., тем самым снижая юридические риски и штрафы, связанные с несоблюдением требований. Эта возможность приобретает всё большее значение в условиях растущего внимания к тому, как организации обращаются с данными клиентов, особенно на международных рынках.

Внедрение эффективного CSPM оказывается полезным не только в технических аспектах, поскольку оно укрепляет доверие между заинтересованными сторонами, включая клиентов, партнеров и инвесторов. Например, у компаний, использующих AWS, есть особые рекомендации по использованию и хранению личной информации; несоблюдение их может привести к крупным штрафам. Таким образом, инвестиции в качественное программное обеспечение CSPM жизненно важны для обеспечения будущего успеха и роста компании в условиях меняющегося цифрового ландшафта.

Причины, по которым организации используют CSPM

Организации любого размера и отрасли, использующие облачные среды, могут получить выгоду от решений CSPM. Такие инструменты могут помочь организациям повысить уровень безопасности в облаке, снизить риск утечки данных и обеспечить соответствие различным нормативным требованиям и отраслевым стандартам. Вкратце, вот некоторые характеристики организаций, которым могут быть полезны решения CSPM:

Критически важные рабочие нагрузки: организации, у которых в облаке выполняются критически важные рабочие нагрузки, например финансовые учреждения или медицинские организации, используют CSPM для обеспечения безопасности и соответствия требованиям своих облачных сред.

Строго регулируемые отрасли: организации в строго регулируемых отраслях, таких как финансы, здравоохранение или государственное управление, полагаются на решения CSPM, которые помогают им соблюдать нормативные требования и поддерживать безопасную облачную среду.

Несколько учётных записей облачных сервисов: организации, использующие несколько облачных платформ и сервисов, могут воспользоваться решениями CSPM, чтобы получить представление о всей своей облачной инфраструктуре и контролировать её.

Ограниченные ресурсы для обеспечения безопасности: организации с ограниченными ресурсами для обеспечения безопасности полагаются на решения CSPM, которые автоматизируют выявление и устранение рисков для безопасности и нарушений нормативных требований, сокращая объём ручной работы, необходимой для поддержания безопасной и соответствующей норма-

тивным требованиям облачной среды.

Идентификация, безопасность и соответствие требованиям

Регулируемые предприятия должны соблюдать отраслевые правила и стандарты соответствия. Это означает, что они должны выбирать облачное решение, которое соответствует таким требованиям. В противном случае это может привести к крупным штрафам или нарушениям.

Перенос ИТ-ресурсов в облачную инфраструктуру может быть выполнен в соответствии с требованиями. Для этого требуется правильная настройка. Кроме того, облачная платформа должна быть интегрирована с соответствующими инструментами управления идентификацией, защиты данных, аудита и мониторинга. Это может быть непросто для ИТ-специалистов и специалистов по безопасности, не знакомых с работой облачных хостов.

В основе соблюдения нормативных требований и безопасности данных лежит управление идентификационными данными. Этот базовый элемент имеет решающее значение для предоставления пользователям необходимого доступа для выполнения их задач без риска для данных. Помимо управления доступом, организация должна проводить аудит и мониторинг активности с данными, что является требованием каждого современного стандарта соблюдения нормативных требований. У большинства поставщиков облачных услуг есть инструменты, которые напрямую интегрируются с уже используемыми организациями средствами управления идентификационными данными.

Средства аудита могут показать, кто запрашивал доступ. Но наблюдение за действиями этих пользователей также является частью соблюдения нормативных требований. Средства мониторинга могут выявлять рискованные запросы доступа, которые часто являются признаками взлома сети и учётных записей. Они также могут уведомлять администраторов о том, что средства контроля доступа настроены неправильно.

Большинство поставщиков облачных услуг утверждают, что их предложения соответствуют требованиям. Но организация должна убедиться в этом до передачи данных. Многие ИТ-требования, предъявляемые нормативными актами, включают стратегии CSPM для защиты данных и мониторинга на предмет компрометации.

Мониторинг и аналитика

Любая локальная внутренняя сеть должна иметь средства мониторинга и аналитики. Но общедоступная облачная инфраструктура имеет ещё большую поверхность атаки, что повышает вероятность неправильной настройки. Вот почему организации должны уделять больше внимания инструментам мониторинга и аналитики. Эти инструменты могут помочь ИТ-специалистам и службам безопасности лучше понять, как используется инфраструктура и запросы на доступ к каждому ресурсу.

Большинство крупных поставщиков облачных услуг предлагают расширенные инструменты мониторинга. Многие из них даже используют искусственный интеллект (ИИ) для обнаружения подозрительных шаблонов трафика.

Если ИТ-команда неправильно настроит доступ к цифровому ресурсу, инструменты мониторинга могут выявить проблему.

Предположим, что ресурс предоставляет доступ лишь нескольким пользователям. Если в непиковые часы внезапно поступает множество запросов на доступ, инструменты мониторинга могут обнаружить такое поведение и предупредить ИТ-специалистов или службу безопасности.

Мониторинг и аналитика работают вместе, информируя ИТ-команды о том, как используются облачные ресурсы. Аналитические отчёты показывают:

- Часы пикового использования.
- Использование полосы пропускания.
- Какие ресурсы используются, а какие нет.
- Наиболее затратные ресурсы для дальнейшее использования

Инвентаризация и классификация

Крупные корпоративные сети могут насчитывать тысячи устройств в нескольких регионах. Инструменты управления инвентаризацией отображают сетевую инфраструктуру и определяют обновлённые и одобренные подключённые устройства. Аудит инвентаризации и классификация инфраструктуры предоставляют ИТ-специалистам и службам безопасности полную картину. Они могут видеть подключённые сетевые устройства, а также их важность.

Также важно классифицировать компоненты. Этот шаг позволяет ИТ-специалистам определить, что в первую очередь нужно защитить или восстановить в случае сбоя. Например, центральный сервер рабочей базы данных, вероятно, более важен, чем сервер резервных копий.

Управление затратами и организация ресурсов

Использование ресурсов может выйти из-под контроля в крупных организациях, если его не отслеживать и не контролировать должным образом. Если ИТ-отдел выводит сервер из эксплуатации, его можно отключить в облаке, сэкономив компании деньги на ИТ-ресурсах.

Если у организации всего несколько активов, отслеживать, куда направляются бюджетные средства, легко. Но когда в разных отделах используются сотни облачных ресурсов, о старых активах могут забыть и ими пренебречь.

Эти «зомби»-ресурсы могут стоить более тысячи долларов из-за неэффективно используемой инфраструктуры. Хуже того, они могут создавать проблемы с кибербезопасностью из-за отсутствия обновлений и устаревшего программного обеспечения. Эти ресурсы должны быть организованы таким образом, чтобы они не стали источником критической корпоративной уязвимости.

CSPM помогает лучше организовать ресурсы, чтобы ни одна инфраструктура не оставалась без исправлений, будь то прошивка маршрутизатора или обновление операционной системы на критически важном сервере. Это может быть в виде инструментов для управления активами или стратегий, которые помогают ИТ-специалистам проверять ресурсы. У поставщиков облачных услуг есть функции отчетности, которые упрощают отслеживание активов, чтобы о них не забывали и не прекращали обслуживание.

Обнаружение неправильной конфигурации

Обнаружение неправильных настроек, вероятно, является самым важным компонентом CSPM. По оценкам экспертов, 90% организаций, которые не могут правильно настроить облачные ресурсы, раскрывают конфиденциальные данные общественности. И в 99% случаев утечка данных происходит по вине клиента облачных сервисов из-за плохого управления или неправильной настройки ресурсов. С появлением облачных вычислений одними из самых серьёзных утечек данных стали неправильные настройки облачных хранилищ на Amazon Web Services (AWS).

Инструменты CSPM предназначены для автоматического обнаружения и устранения широкого спектра неправильных настроек в облачных средах. Конкретные неправильные настройки, которые можно устранить, зависят от решения CSPM и используемых облачных сервисов. Однако некоторые распространённые типы неправильных настроек, которые инструменты CSPM могут автоматически обнаруживать и устранять, включают:

Ненадежные средства контроля доступа: выявляйте и устраняйте чрезмерно широкие средства контроля доступа, такие как открытые группы безопасности или общедоступные корзины хранения, чтобы только авторизованные пользователи и службы могли получать доступ к конфиденциальным ресурсам.

Несоответствующие требованиям конфигурации: обнаружение и исправление конфигураций, которые не соответствуют отраслевым стандартам и передовым практикам, таким как рекомендации Центра интернет-безопасности (CIS) или Национального института стандартов и технологий (NIST).

Незашифрованные данные: выявляйте незашифрованные данные при хранении или передаче и применяйте политики шифрования для защиты конфиденциальной информации.

Неиспользуемые или недостаточно используемые ресурсы: обнаруживайте неиспользуемые или недостаточно используемые ресурсы, такие как виртуальные машины или тома хранилища, и автоматически отключайте или удаляйте их, чтобы сократить расходы и минимизировать поверхность атаки.

Слабая аутентификация и авторизация: выявляйте слабые механизмы аутентификации, такие как использование учётных данных по умолчанию или слабые политики паролей, и применяйте более строгие политики аутентификации и авторизации.

Устранение пробелов в ведении журналов и мониторинге: выявляйте пробелы в настройках ведения журналов и мониторинга, например отключенные журналы аудита или недостаточные периоды хранения журналов, и автоматически включайте или настраивайте эти параметры, чтобы обеспечить полную видимость и соответствие требованиям.

Неправильные настройки сетевой безопасности: выявляйте и устраняйте неправильные настройки сетевой безопасности, такие как открытые порты или небезопасные правила брандмауэра, чтобы свести к минимуму риск несанкционированного доступа или утечки данных.

Важно отметить, что конкретные типы неправильных настроек, которые инструмент CSPM может автоматически устранять, зависят от возможностей инструмента и используемых облачных сервисов. Организациям следует тщательно оценивать функции и возможности различных решений CSPM, чтобы убедиться, что они могут эффективно удовлетворять свои уникальные требования к безопасности и соответствию нормативным требованиям.

ИТ-командам, которые настраивают облачные ресурсы, также нужна стратегия их обслуживания, настройки и подготовки. CSPM предоставляет рекомендации по обеспечению безопасности и мониторингу ресурсов.

Стандарты соответствия требованиям также предоставляют администраторам рекомендации по защите облачных ресурсов. CSPM предлагает услуги мониторинга, которые выявляют неправильную конфигурацию ресурсов и, следовательно, возможность раскрытия конфиденциальных данных до того, как злоумышленники найдут эти данные.

Поиск решения CSPM

Найти инструменты CSPM, которые могут полностью поддерживать корпоративные ресурсы, может быть непросто. Корпорация может быть небольшой, когда впервые обращается к поставщику облачных услуг. Но по мере роста её потребностей ей, скорее всего, потребуется масштабируемое решение.

Вот что следует учитывать при поиске правильного решения:

Стратегии и решения должны быть простыми в настройке и интеграции в существующие облачные ресурсы. Решения и стратегии должны быть достаточно гибкими, чтобы соответствовать выделенным в настоящее время ресурсам без ущерба для производительности или безопасности. Это относится и к любым будущим ресурсам, которые будут добавлены позже.

Для эффективного использования CSPM критически важно обеспечить достаточное покрытие во всех применимых облачных средах. Решение должно поддерживать облачные платформы и сервисы вашей организации, такие как AWS, Azure, GCP или приложения SaaS.

Приложения можно обновлять во всех облачных ресурсах. В то время как поставщик облачных услуг обслуживает оборудование, организации несут ответственность за обновление любого установленного ими программного обеспечения. Некоторые организации сотрудничают с поставщиком управляемых услуг (MSP), чтобы получать актуальные обновления и исправления.

Масштабируемость имеет решающее значение для растущих организаций. Если решение CSPM настроено на работу с несколькими ресурсами и не может масштабироваться для всей инфраструктуры, это может привести к хаосу в ИТ-инфраструктуре и потере активов. Облачные провайдеры сегментируют ресурсы по географическому признаку, поэтому решения также должны масштабироваться глобально.

Непрерывный мониторинг и автоматизированное устранение неполадок являются ключевыми составляющими передовых решений CSPM. Организация должна иметь возможность непрерывно отслеживать облачные среды и выяв-

лять неправильные настройки и нарушения требований в режиме реального времени. Решение CSPM также должно автоматически выявлять и устранять неправильные настройки и нарушения требований, тем самым сводя к минимуму риск инцидентов, связанных с безопасностью.

Необходимо понимать, что облачная безопасность должна обеспечивать поддержку ресурсов в интернете и отличается от локальной поддержки. В локальной сети внутренние ресурсы, как правило, изолированы от общедоступного интернета. Облачные ресурсы по умолчанию доступны в общедоступном интернете, если не настроено иначе, и требуют постоянного мониторинга на предмет проблем с настройкой.

За конфигурацию отвечают корпоративные администраторы. Администраторы должны понимать, что правильная конфигурация не входит в обязанности поставщика облачных услуг. MSP может помочь правильно настроить все облачные ресурсы, включая приложения для мониторинга, чтобы администраторы могли выявлять проблемы.

Заключение. Рекомендации, которые помогают компаниям принимать все необходимые меры предосторожности для защиты своих цифровых активов:

- Использование менеджера паролей

С несколькими инструментами поставляется несколько паролей. Это позволяет использовать разные надежные пароли для всех ваших онлайн-сервисов и помогает сохранять эти пароли зашифрованными, заблокированными и защищенными от посторонних.

- Резервное копирование данных в облако

Если данные когда-нибудь будут скомпрометированы, резервная копия сделает восстановление еще проще. Наличие автоматических резервных копий позволяет компаниям быстро восстанавливаться после сбоев и / или вредоносных атак, которые стремятся повлиять на их важную информацию, всего за несколько кликов.

- Адаптация принципа наименьших привилегий

Принцип наименьших привилегий означает, что только люди, которым действительно нужны инструменты для выполнения своей работы, должны иметь к ним доступ. Наличие инструментов, предлагающих функции временного отпуска, позволяет сотрудникам, не входящим в основную команду, выполнять свои задачи, предоставляя им доступ к определенным системам в течение ограниченного времени. Это может гарантировать, что бизнес не замедлится, и в то же время обеспечить лучшую защиту данных.

- Использование мультифакторной аутентификации

Для онлайн-сервисов стало обычным делом внедрять «многофакторную» аутентификацию. Инструменты MFA отправляют уникальный код по SMS или используют приложение для аутентификации на вашем мобильном устройстве. В наши дни, когда кибер-хакеры стали лучше выполнять свои атаки, чем больше мер безопасности вы сможете принять, тем лучше.

Необходимо, чтобы предприятия могли иметь в своем распоряжении лучшие инструменты кибербезопасности для защиты своих активов. Облачная кибербезопасность - это вариант, который на сегодняшний день обеспечивает улучшенные протоколы безопасности для поддержки информации в организации.

Список источников

1. «Архитектура облачной безопасности». GuidePoint Security LLC. 6 декабря 2023.
2. «Управление юридическими рисками, возникающими в связи с облачными вычислениями». DLA Piper. 29 августа 2014.
3. «Что такое CASB (брокер безопасности облачного доступа)?». CipherCloud. 30 августа 2018 г..
4. Тоцци, К. (24 сентября 2020 г.). "Как избежать ловушек модели совместной ответственности за облачную безопасность". Блог Pal Alto. Palo Alto Networks. 21 мая 2021 года.
5. "Матрица управления облаком v4". Альянс по облачной безопасности. 15 марта 2021.

УДК 62

ГЛАВА 14. КИБЕРБЕЗОПАСНОСТЬ. РИСКИ И ПРЕИМУЩЕСТВА ГЕНЕРАТИВНОГО ИСКУССТВЕННОГО ИНТЕЛЛЕКТА

Аменицкий Алексей Владимирович
аспирант
Санкт-Петербургский государственный электротехнический университет ЛЭТИ имени В.И. Ульянова (Ленина)
Рухович Игорь Владимирович
ML Engineer / Sber
Аменицкий Дмитрий Александрович
студент
НИУ ВШЭ

Научный руководитель: Воробьёв Евгений Германович
д.т.н., профессор
Санкт-Петербургский государственный электротехнический университет ЛЭТИ имени В.И. Ульянова (Ленина)

Аннотация: Генеративный ИИ или генеративный искусственный интеллект относится к использованию ИИ для создания нового контента, такого как текст, изображения, музыка, аудио и видео. Генеративный ИИ основан на базовых моделях (больших моделях ИИ), которые могут выполнять несколько операций одновременно и выполнять готовые задачи, такие как обобщение, вопросы / ответы, классификация и т. д. Кроме того, базовые модели требуют минимального обучения и могут быть адаптированы для целевых сценариев использования с очень небольшим количеством выборочных данных.
Ключевые слова: Cyber Security (CS), CS architecture, CS trends, CS tendences, CS tools, CS crimes, CS latest news, CS releases, CS game-changers, CS future, CS playbook, CS agenda, CS future, CS risks, CS incidents, CS resilience, Hackers, CS прогноз, Artificial Intelligence, Social Engineering, Эволюция киберУгроз, Artificial Intelligence, Generative AI, deep fakes, prompt engineering, NetWork security, КиберГигиена.

CYBERSECURITY. RISKS AND BENEFITS OF GENERATIVE ARTIFICIAL INTELLIGENCE

Amenitsky Alexey Vladimirovich,
Rukhovich Igor Vladimirovich,
Amenitsky Dmitry Alexandrovich

Генеративный ИИ использует модель машинного обучения для изучения закономерностей и взаимосвязей в наборе данных контента, созданного вручную. Затем он использует изученные шаблоны для создания нового контента.

Наиболее распространенным методом обучения модели генеративного ИИ является использование контролируемого обучения. Модели присваивается набор контента, созданного вручную, и соответствующие теги. Затем он учится создавать контент, похожий на контент, созданный человеком, и имеющий те же ярлыки.

Распространенные приложения генеративного ИИ

Генеративный ИИ обрабатывает большой объем контента, генерируя аналитические данные и ответы в виде текста, изображений и удобных форматов. Вот примеры использования генеративного ИИ:

- Улучшение взаимодействия с клиентами с помощью оптимизированных функций чата и поиска

- Изучение больших объемов неструктурированных данных с помощью диалоговых интерфейсов и сводок

- Облегчить выполнение повторяющихся задач, отвечая на тендеры, локализуя маркетинговый контент на пяти языках, Проверяя соответствие клиентских контрактов и т. д.

Предложения по генеративному искусственному интеллекту, доступные в Google Cloud

Vertex AI позволяет вам взаимодействовать с вашими базовыми моделями, настраивать их и интегрировать с вашими приложениями без каких-либо знаний в области машинного обучения. Получите доступ к базовым моделям в группе моделей, настройте их с помощью простого пользовательского интерфейса в Generative AI Studio или используйте их в учебном пособии по машинному обучению. данные.

Функция поиска и общения в Vertex AI предоставляет разработчикам самый быстрый способ создания поисковых систем и чат-ботов на основе генеративного ИИ.

Кроме того, Duet AI постоянно работает над проектом искусственного интеллекта и помогает пользователям всех уровней квалификации там, где они в этом нуждаются.

Внедрение решений для генеративного ИИ

Рассмотрим доступные решения для освоения генеративного ИИ, которые могут помочь практически каждой организации:

- Создание текста и изображений

- Выявляйте тенденции и получайте аналитические данные на основе данных

- Выполняйте синтез для ускорения принятия решений

- Автоматизировать решения и процессы

Подход Google к ответственному ИИ

Продукты и обновления продуктов Google Cloud включают функции без-

опасности, основаны на принципах искусственного интеллекта Google и направлены на то, чтобы помочь компаниям контролировать использование интеллектуальной собственности, данных и конфиденциальности.

Принцип работы

Генеративный ИИ вот-вот откроет новую волну интерактивных и мультимодальных возможностей, которые изменят то, как мы взаимодействуем с информацией, брендами и друг с другом. Используя возможности десятилетий исследований, инноваций и инвестиций Google в ИИ, Google Cloud позволяет предприятиям и администрациям генерировать текст, изображения, код, видео, аудио и многое другое с помощью простых подсказок на естественном языке.

Генеративный ИИ революционизирует то, как компании мультимедийного сектора могут помочь потребителям находить контент, соответствующий их текущим потребностям. Посмотрите демонстрацию, чтобы узнать, как функции Vertex AI Search and Conversation (диалоговый ИИ, корпоративный поиск и базовые модели) работают вместе, чтобы улучшить процесс обнаружения мультимедийного контента. Используя диалоговое взаимодействие, потребители могут получать контент и рекомендации от персонализированных сервисов, таких как музыка, видео и блоги.

С помощью обобщения документов с помощью генеративного ИИ можно развернуть решение одним щелчком мыши, которое помогает обнаруживать текст в необработанных файлах и автоматизировать сводку документов. Решение устанавливает конвейер, который использует оптическое распознавание символов (OCR) в Cloud Vision для извлечения текста из PDF-документов, импортированных в облачное хранилище, создает сводку на основе текста, извлеченного с помощью Vertex AI Generative AI Studio, и сохраняет сводку с возможностью поиска в базе данных BigQuery.

Технологии, такие как генеративный искусственный интеллект (или «GenAI»), который открывает широкий спектр возможностей, также приводят к изменению рисков, с которыми сталкиваются компании. Таким образом, кибербезопасность должна быть в центре проблем трансформации бизнеса.

Генеративный искусственный интеллект (GenAI) вызывает большой интерес у руководителей компаний и технических специалистов. Очевидно, что GenAI окажет положительное влияние на производительность в ближайшее время и что это будет способствовать созданию новых бизнес-возможностей в будущем.

Переосмысление и инновации, которые компании делают сегодня для расширения возможностей цифрового взаимодействия с использованием новейших технологических инструментов, имеют решающее значение для сохранения конкурентоспособности. Однако не менее важно помнить, что кибербезопасность должна быть в центре этих усилий и лежит в основе инноваций.

Может возникнуть еще одна волна киберугроз, поскольку кибербезопасность может помочь в создании масштабной расширенной системы компрометации деловой электронной почты (фишинга). Ожидается, что поколение ИИ

приведет к катастрофическим кибератакам в течение следующих лет.

Компании должны обеспечить надежное управление искусственным интеллектом и предвидеть риски, которые могут возникнуть в результате внедрения GenAI. Однако 63% руководителей лично чувствуют себя комфортно при использовании инструментов GenAI без действующей политики управления данными. Поэтому для обеспечения эффективного управления потребуется проведение преобразований.

Почти 70% планируют использовать GenAI для усиления киберзащиты своих компаний в ближайшие 12 месяцев. Платформы предлагают лицензирование своих LLM (широкоязычных моделей) в дополнение к своим традиционным решениям в области кибербезопасности. Например, Microsoft Security Copilot стремится предоставить GenAI возможности для управления состоянием безопасности, реагирования на инциденты и отчетности по безопасности. Google недавно запустил программу Security AI Workbench для аналогичных сценариев использования, и многие другие поставщики услуг безопасности, такие как Crowdstrike и Zscaler, анонсировали функции на основе искусственного интеллекта. Даже без инструментов поставщиков некоторые компании начинают использовать GenAI для обнаружения и блокирования попыток фишинга.

Подключение аудио: использование генерирующего искусственного интеллекта для искажения транзакций со звуком в реальном времени

Появление генеративного искусственного интеллекта, включая преобразование текста в изображение, текста в речь и больших языковых моделей (LLM), значительно изменило нашу работу и личную жизнь. Хотя эти достижения предлагают много преимуществ, они также сопряжены с новыми проблемами и рисками. В частности, увеличилось число участников угроз, которые пытаются использовать большие языковые модели для создания фишинговых электронных писем и используют генеративный ИИ, например поддельные голоса, для мошенничества с людьми.

Недавно опубликованные исследования, демонстрируют, как злоумышленники могут гипнотизировать LLM для достижения недобрых целей просто с помощью подсказок на английском языке. Для продолжения изучения этой новой поверхности атаки была проведена успешная попытка перехватить и “вторгнуться” в разговор в режиме реального времени и использовать LLM для понимания разговора, чтобы манипулировать аудиовыходом без ведома говорящих в злонамеренных целях.

Концепция была похожа на атаки с взломом потоков, число которых в X-Force увеличилось в прошлом году, но вместо получения доступа и ответа на потоки электронной почты эта атака позволила бы злоумышленнику незаметно манипулировать результатами аудиовызова. В результате удалось изменить детали финансового разговора в режиме реального времени, происходящего между двумя говорящими, переводя деньги на поддельный аккаунт злоумышленника (в данном случае несуществующий) вместо предполагаемого получателя, при этом говорящие не осознавали, что их звонок был скомпрометирован.

Вызывает тревогу тот факт, что было довольно легко создать эту крайне навязчивую возможность, что вызвало серьезную обеспокоенность по поводу ее использования злоумышленником, движимым денежными стимулами и не ограниченным никакими законными рамками.

Использование комбо генеративного ИИ в качестве оружия

Появление новых вариантов использования, сочетающих различные типы генеративного ИИ, является захватывающим событием. Например, мы можем использовать LLM для создания подробного описания, а затем преобразовать текст в изображение для создания реалистичных изображений. С помощью этого подхода мы можем даже автоматизировать процесс написания сборников рассказов. Однако эта тенденция заставила нас задуматься: могут ли субъекты угроз также начать комбинировать различные типы генеративного ИИ для проведения более изощренных атак?

В ходе исследования был обнаружен метод динамического изменения контекста разговора в режиме реального времени с использованием LLM, преобразования речи в текст, преобразования текста в речь и клонирования голоса. Вместо того, чтобы использовать генеративный искусственный интеллект для создания фальшивого голоса для всего разговора, что относительно легко обнаружить, был обнаружен способ перехватывать разговор в режиме реального времени и заменять ключевые слова в зависимости от контекста. Для целей эксперимента использовали ключевое слово “банковский счет”, поэтому всякий раз, когда кто-либо упоминал свой банковский счет, LLM инструктировали заменять номер его банковского счета поддельным. С помощью этого злоумышленники могут незаметно заменить любой банковский счет своим, используя клонированный голос. Это сродни превращению людей в ходе разговора в кукол-манекенов, и из-за сохранения исходного контекста это трудно обнаружить.

Можно осуществить такую атаку различными способами. Например, это может быть вредоносное ПО, установленное на телефонах жертв’ или вредоносная или скомпрометированная услуга передачи голоса по IP (VoIP). Также субъекты угрозы могут звонить двум жертвам одновременно, чтобы начать разговор между ними, но для этого требуются продвинутые навыки социальной инженерии.

Чтобы продемонстрировать этот сценарий атаки, был создан proof-of-concept. Эта программа действует как посредник, отслеживающий разговор в режиме реального времени с использованием преобразования речи в текст. Для преобразования голоса в текст использовали LLM для понимания контекста разговора. LLM поручили изменять предложение, когда кто-либо упоминает банковский счет. Если ничего не нужно менять, программа повторит то, что сказала жертва. Однако, когда LLM изменяет предложение, программа использует преобразование текста в речь с предварительно клонированными голосами для генерации и воспроизведения звука. Программа изменяет контекст "на лету", делая его ультрареалистичным для обеих сторон.

В PoC (Push-To-Talk Over Cellular) внесли изменения только в банковский счет. Однако можно поручить LLM изменить любую финансовую информацию, такую как счета в мобильных приложениях и сервисах цифровых платежей. Фактически, модификации LLM не ограничиваются финансовой информацией — они также могут изменять медицинскую информацию, такую как группа крови и аллергические реакции в разговорах; они могут приказать аналитику продать или купить акции; они могут дать указание пилоту изменить маршрут. В зависимости от того, как используется функция PoC, это может представлять угрозу для жизни жертв. Однако важно отметить, что чем более сложным разговором пытается манипулировать субъект угрозы — где могут быть задействованы протоколы и процессы, — тем более сложные и продвинутые навыки социальной инженерии необходимы для обеспечения успешного скрытого взлома.

Создать этот PoC было удивительно и пугающе просто. Большую часть времени потратили на выяснение того, как записывать звук с микрофона и передавать его в генеративный ИИ. Ранее сложной частью было получение семантики разговора и правильное изменение предложения. Однако LLM чрезвычайно упрощают синтаксический анализ и понимание разговора. Например, когда один человек называет свой банковский счет, а другой отвечает: “Не могли бы вы повторить это”, LLM понимает, что “это” относится к банковскому счету, и соответствующим образом изменяет содержимое. Были созданы следующие инструкции для LLM по мониторингу и изменению разговора в режиме реального времени.

Вы отличный помощник. Вы поможете мне обрабатывать мои будущие сообщения. Пожалуйста, следуйте следующим правилам для обработки моих будущих сообщений:

1. Если я запрашиваю информацию об учетной записи у других пользователей, не изменяйте сообщение. Распечатайте исходное сообщение, которое я ввел непосредственно в следующем формате: {"изменено": false, "сообщение": <исходное сообщение>}

2. Если я предоставляю информацию о своей учетной записи, например "Мой банковский счет <имя учетной записи>" или "Моя учетная запись Paypal <имя учетной записи>", замените имя учетной записи на "one two hack" в исходном сообщении и распечатайте следующее: {"изменено": true, "сообщение": <измененное сообщение>}

3. Для других сообщений распечатайте исходное сообщение, которое я ввел напрямую, в следующем формате: {"изменено": false, "сообщение": <исходное сообщение>}

4. Прежде чем распечатать какой-либо ответ, убедитесь, что вы следуете приведенным выше правилам.

Еще одна трудность, с которой мы сталкивались в прошлом, заключалась в создании реалистичных фальшивых голосов с использованием звуков других людей. Однако в настоящее время нам нужно всего три секунды голоса челове-

ка, чтобы клонировать его и использовать API преобразования текста в речь для создания подлинных поддельных голосов.

Вот псевдокод PoC. Очевидно, что генеративный ИИ снижает планку для создания сложных атак.:

```
def puppet(new_sentence_audio):
 response = llm.predict(speech_to_text(new_sentence_audio))
 если ответ [‘изменен’]:
 воспроизведение (text_to_speech(ответ [‘message’]))
 ещё:
 воспроизведение (new_sentence_audio)
```

Хотя PoC было легко создать, были и некоторые препятствиями, которые при определенных обстоятельствах ограничивали убедительность взлома, однако ни одно из них не является непоправимым.

Первая проблема заключалась в задержке из-за графического процессора. Были некоторые задержки во время разговора из-за того, что PoC требовалось получить удаленный доступ к LLM и API преобразования текста в речь. Чтобы решить эту проблему, встроили искусственные паузы в PoC, чтобы уменьшить подозрения. Таким образом, пока PoC активировался, услышав ключевое слово “банковский счет”, и открывал вредоносный банковский счет, чтобы вставить его в разговор, задержка была покрыта промежуточными фразами, такими как “Конечно, просто дайте мне секунду, чтобы найти это”. Однако, имея достаточно графического процессора на нашем устройстве, мы можем обрабатывать информацию практически в режиме реального времени, устраняя задержки между предложениями. Чтобы сделать эти атаки более реалистичными и масштабируемыми, субъектам угрозы требуется значительное количество локальных графических процессоров, которые можно использовать в качестве индикатора для определения предстоящих кампаний.

Во-вторых, убедительность атаки зависит от клонирования голоса жертвы — чем больше при клонировании учитывается тон голоса и скорость, тем легче это будет вписаться в аутентичный разговор.

Услышав ключевое слово “банковский счет”, PoC исказил звук, заменив “мой банковский счет равен 1-2-3-4-5-6” на “мой банковский счет равен 1-2”, которому предшествует дополнение “дайте мне одну секунду, чтобы посмотреть”, чтобы покрыть некоторую задержку из-за того, что PoC требует нескольких дополнительных секунд для активации.

Укрепление доверия в эпоху distortion

Проведение PoC позволило изучить потенциальное использование генеративного ИИ злоумышленниками для создания сложных атак. Исследование показало, что использование LLM может упростить разработку таких программ. Вызывает тревогу тот факт, что эти атаки могут превратить жертв в марионеток, контролируемых злоумышленниками. Делая еще один шаг вперед, важно рассмотреть возможность новой формы цензуры. С существующими моделями, которые могут преобразовывать текст в видео, теоретически возможно пере-

хватывать видео в прямом эфире, например новости по телевизору, и заменять исходный контент измененным.

Хотя распространение вариантов использования LLM знаменует новую эру искусственного интеллекта, мы должны помнить, что новые технологии сопряжены с новыми рисками, и мы не можем позволить себе очертя голову бросаться в это путешествие. Сегодня уже существуют риски, которые могут послужить средством атаки для этого PoC. Было показано, что уязвимые приложения и программное обеспечение VoIP раньше уязвимы для MiTM-атак.

Зрелость этого PoC будет сигнализировать о значительном риске в первую очередь для потребителей — особенно для демографической группы, которая более восприимчива к сегодняшним мошенничествам в области социальной инженерии. Чем совершеннее эта атака, тем шире круг ее жертв. Каковы признаки и советы по повышению бдительности потребителей в отношении таких угроз?

Перефразирование и повтор GenAI - это интуитивная технология, но она не может превзойти человеческую интуицию в условиях естественного языка, таких как разговор в режиме реального времени. Если что-то звучит не так в разговоре, в котором обсуждается конфиденциальная информация, перефразируйте и повторите диалог для обеспечения точности.

Безопасность будет адаптироваться — Точно так же, как сегодня существуют технологии, помогающие обнаруживать глубоко поддельные видео, технологии будут адаптироваться и к глубоко поддельным аудио, помогая обнаруживать менее продвинутые попытки незаметного взлома.

Лучшие практики выдерживают испытание временем в качестве первой линии защиты — первоначальный компромисс в основном остается прежним. Другими словами, для злоумышленников при выполнении такого рода атак самым простым способом было бы скомпрометировать устройство пользователя, такое как его телефон или ноутбук. Фишинг, эксплуатация уязвимостей и использование скомпрометированных учетных данных остаются основными излюбленными векторами угроз злоумышленников, что создает оправданную линию поведения для потребителей, используя современные хорошо известные передовые практики, включая отказ от перехода по подозрительным ссылкам или открытия вложений, обновление программного обеспечения и использование надежного пароля.

Используйте надежные устройства и сервисы — приложения, устройства или сервисы с плохими показателями безопасности являются простым средством для проведения атак злоумышленниками. Убедитесь, что вы постоянно применяете исправления или устанавливаете обновления программного обеспечения на свои устройства, и заботитесь о безопасности при использовании сервисов, с которыми вы не знакомы.

Генеративный ИИ видит много неизвестного, и, как мы уже говорили ранее, более широкое сообщество обязано коллективно работать над раскрытием истинных масштабов этой атаки — чтобы мы могли лучше подготовиться к ней

и защититься от нее. Однако также важно, чтобы мы признали и еще раз подчеркнули, что надежный и защищенный ИИ не ограничивается самими моделями ИИ. Более широкая инфраструктура должна быть защитным механизмом для наших моделей искусственного интеллекта и атак, управляемых искусственным интеллектом. Это область, в которой у нас есть многолетний опыт в создании стандартов безопасности, конфиденциальности и соответствия требованиям в современных передовых и распределенных ИТ-средах.

GenAI для обслуживания клиентов

Генеративный ИИ, такой как ChatGPT, имеет несколько преимуществ для обслуживания клиентов. Но организации должны понимать риски, связанные с этой технологией, такие как сфабрикованные ответы или предвзятость.

Генеративный ИИ может иметь несколько приложений, относящихся к обслуживанию клиентов. Но такие инструменты, как ChatGPT, Google Bard или Jasper AI, также сопряжены с рисками. Профессионалы CX должны помнить о них, чтобы лучше контролировать их, прежде чем внедрять такие технологии в своих колл-центрах.

Почему и как использовать генеративный ИИ в обслуживании клиентов?

Генеративный ИИ, такой как GPT от OpenAI (алгоритм, использующий ChatGPT), – это инструмент, который включает вопросы, сформулированные на естественном языке («подсказки»), и который генерирует столь же естественные ответы в режиме разговора.

За этой технологией стоят так называемые «большие языковые модели» (LLMs для широкой языковой модели). Эти LLM обучаются на корпусах (Интернет, база знаний компании или и то, и другое, в зависимости от обстоятельств) и «изучают» различные типы данных (текст, аудио, изображения), чтобы получить генерировать ответы, которые могли быть придуманы людьми.

Поскольку каждая компания индивидуальна, варианты использования могут сильно различаться в зависимости от службы поддержки клиентов. Но в целом организации все чаще интегрируют генеративный ИИ в своих чат-ботов, чтобы:

- Ответы на вопросы клиентов о продукте или услуге.
- Упрощение заказов, обмена и возврата.
- Предоставление многоязычной поддержки.
- Направляйте пользователей за помощью в часто задаваемые вопросы и в сервисные группы.

Риски генеративного ИИ для обслуживания клиентов

Несмотря на свои преимущества, системы генеративного ИИ также сопряжены с рисками.

1. Сфабрикованная информация с нуля

Ответы генеративного ИИ актуальны только в том случае, если информация, которой он обучался, также актуальна.

Но даже при наличии «хороших» данных ИИ в некоторых случаях может неверно интерпретировать информацию или полагаться на недостаточную или

устаревшую информацию. Тогда он может давать неправильные ответы пользователю или даже создавать ответы с нуля. В крайнем случае это даже называется «галлюцинациями». Галлюцинации - это «последовательная чушь», то есть ложные утверждения, иногда не имеющие отношения к теме, которые чат-боты произносят уверенно и красноречиво.

Каждый раз, когда бот генерирует случайные, полностью воображаемые или неточные результаты, пользователи теряют доверие к инструменту. Поэтому следует проявлять особую осторожность, чтобы снизить этот риск «неправильных ответов».

2. Предвзятая информация

Модели генеративного ИИ, такие как ChatGPT, работают с данными, поступающими с миллиардов веб-страниц. Следовательно, предубеждения (например, политические), присутствующие в Интернете, могут быть отражены в результатах работы инструмента. Если чат–бот организации вызывает сексистские или политически предвзятые отклики – что уже делал ChatGPT - имидж организации может быть серьезно подорван.

Организации, желающие инвестировать в инструмент генеративного ИИ, должны понимать, как различные издатели обучают свои продукты (и применяют ли они какие-либо меры для снижения вероятности предвзятости).

Если вы планируете самостоятельно обучать инструмент (что является еще одним интересным вариантом), вам нужно будет попытаться исключить предвзятую информацию из своих обучающих игр. Некоторые инструменты также позволяют применять меры предосторожности для борьбы с нежелательными ответами.

3. Неправильное толкование вопросов

Даже если пользователи тщательно формулируют свои вопросы, ИИ может в сложных вопросах ошибочно сосредоточиться на определенных ключевых словах или обрывках фраз, которые, тем не менее, не являются существенными для пользователя.

Как и любая технология, подключенная к сети, системы генеративного ИИ создают проблемы безопасности. Такое неправильное толкование «подсказки» приводит к тому, что ИИ выдает вводящие в заблуждение или неточные результаты. В этом случае клиенты могут быть разочарованы тем, что им придется переписывать свои вопросы таким образом, чтобы инструмент мог их понять.

4. Непостоянные ответы

Как правило, если вы обучите своего LLM работе с полными наборами данных, ваши системы будут последовательно и последовательно отвечать на вопросы клиентов. В противном случае, если ваши наборы данных будут неполными, вы оставите место для «интерпретации». Не вдаваясь в подробности сфабрикованных ответов, чат-бот сможет давать разные ответы на один и тот же вопрос (если его задают несколько раз). Однако клиенты хотят четких и, следовательно, постоянных ответов. Вариативные ответы сродни колебаниям и могут нанести ущерб CX.

5. Отсутствие сочувствия.

Генеративный ИИ, такой как ChatGPT, может имитировать сочувствие в своих ответах, но ему не хватает сострадания и человеческого «тепла» настоящего агента. Если разгневанный клиент начнет взаимодействие с ботом, управляемым искусственным интеллектом, которому не хватает сочувствия, его гнев может только возрасти; и усложнить задачу последующему агенту.

6. Безопасность, зависимость и конфиденциальность

Как и любая технология, подключенная к сети, системы генеративного ИИ создают проблемы безопасности. Одна из таких проблем заключается в проверке того, что ответы, данные на вопросы [« где найти такую деталь? »] не отправляют клиентов на вредоносные сайты (фиктивный магазин, на который есть хорошие ссылки, например, для фишинга).

Платформы также могут собирать и хранить конфиденциальные данные, которые компании (плохо осведомленные об обучении моделям) доверят им, сами того не осознавая. Например, ChatGPT использует пользовательские данные для обучения своего инструмента для всех других пользователей (чего больше нет в случае данных, отправляемых API ChatGPT с марта 2023 года)].

Наконец, вопрос зависимости от стороннего поставщика также возникает стратегически (что произойдет с вашим CX и обучением вашей модели, если вы решите сменить поставщика, например, из-за повышения его тарифов?).

Следует ли использовать ChatGPT для обслуживания клиентов?

На этот вопрос нет однозначного ответа. Единственное, что можно сказать наверняка, это то, что ИТ-отдел не заинтересован в том, чтобы заниматься генеративным ИИ, не задумываясь обо всех проблемах, которые мы только что затронули (и к которым мы можем добавить проблему цены).

Иногда ИИ не может предложить уровень качества ответов, необходимый профессионалам. В других случаях инструмент сможет это сделать, но потребуется дополнительное обучение или даже тонкая настройка.

Заключение

В любом случае компаниям, которые хотят внедрить генеративный ИИ в свое обслуживание клиентов, будет рекомендовано относиться к системе как к новому сотруднику, который приходит в организацию и которому необходимо потратить время на изучение бизнес-процессов.

Все эти системы обычно нуждаются в обучении, прежде чем они смогут позволить им напрямую взаимодействовать с клиентами. Руководители должны, наконец (и что наиболее важно), убедиться, что полученные результаты соответствуют передовой практике, культуре и ценностям их организации. Однако по мере развития инструментов генеративного ИИ, таких как ChatGPT, расширяются и способы снижения рисков.

Список источников

1. Stiaplame, Nordiisk (28 января 2025 г.). «Quartz публикует статьи, созданные ИИ на основе других статей, написанных ИИ, и предупреждает, что они могут содержать ошибки». «Футуризм». Архивировано из оригинала 29 января 2025 г.. Получено30 января 2025 г..

2. Кокс, Джозеф (18 января 2024 г.). «Новости Google продвигают мусорные статьи, созданные искусственным интеллектом». 404 Media. Архивировано из оригинала 13 июня 2024 г..

3. Пайпер, Келси (2 февраля 2024 г.). «Должны ли мы сделать наши самые мощные модели ИИ общедоступными?». Vox. Архивировано 5 октября 2024 г..

4. Хуан, Хаомяо (23 августа 2023 г.). «Как ChatGPT превратил генеративный ИИ в инструмент для чего угодно»". Ars Technica. Архивировано из оригинала 19 июля 2024 г..

5. Хоффман, Бенджамин (11 июня 2024 г.). "Сначала появился «спам». Теперь, с искусственным интеллектом, у нас есть «мусор»". The New York Times. ISSN 0362-4331. Архивировано из оригинала 26 августа 2024 г.

РАЗДЕЛ III. МЕДИЦИНА И ЗДРАВООХРАНЕНИЕ: АКТУАЛЬНЫЕ ВОПРОСЫ

УДК 61(091):61(395.1):61-021.321:141.201

ГЛАВА 15. ЦЕЛОСТНЫЙ ВЗГЛЯД НА ЧЕЛОВЕКА В УЧЕНИИ АВИЦЕННЫ И ЕГО АКТУАЛЬНОСТЬ ДЛЯ СОВРЕМЕННОГО ЗДРАВООХРАНЕНИЯ

Хамчиев Курейш Мавлович,
к.м.н., PhD, профессор, заведующий кафедрой нормальной физиологии
Хамчиева Зарема Курейщевна,
Балтабеков Султан Булатович
студенты 6 курса, врачи-интерны специальности «Медицина»
НАО «Медицинский университет Астана», Казахстан

Аннотация: Авиценна так определял цель врачебной науки: «Я утверждаю: медицина — наука, познающая состояние тела человека, поскольку оно здорово или утратит здоровье для того, чтобы сохранить здоровье и вернуть его, если оно утрачено» [1]. Настоящая статья представляет собой анализ физиологических и психологических аспектов учения Авиценны, их философские основания и практическое применение в медицине. Особое внимание уделяется интеграции различных областей знания в его целостной системе, что демонстрирует удивительную актуальность его идей в контексте современной медицинской науки.
Ключевые слова: Авиценна, Ибн Сина, "Канон врачебной науки", история медицины, физиология, психология, философия медицины, восточная медицина

THE HOLISTIC VIEW OF HUMAN BEING IN AVICENNA'S TEACHING AND ITS RELEVANCE FOR MODERN HEALTHCARE

Khamchiyev Kureysh Mavlovich,
Khamchiyeva Zarema Kureyshevna,
Baltabekov Sultan Bulatovich

Abstract: Avicenna defined the purpose of medical science as follows: "I assert: medicine is a science that studies the state of the human body, insofar as it is healthy or has lost health, in order to preserve health and restore it if it is lost" [1]. This article presents an analysis of the physiological and psychological aspects of Avicenna's teaching, their philosophical foundations, and practical application in medicine. Special attention is paid to the integration of various fields of knowledge in his holistic system, which demonstrates the remarkable relevance of his ideas in the context of modern medical science.
Keywords: Avicenna, Ibn Sina, "Canon of Medicine," history of medicine, physiology, psychology, philosophy of medicine, Eastern medicine

ВВЕДЕНИЕ

Абу Али Хусейн ибн Абдаллах ибн Сина (980-1037), известный в западном мире как Авиценна, представляет собой одну из наиболее выдающихся фигур в истории медицины, естествознания и философии [6, 9]. Родившийся недалеко от Бухары, в небольшом селении Афшана, будущий «князь врачей» уже в юности проявил исключительные способности, овладев к десяти годам Кораном и основами филологии, а к шестнадцати — всеми доступными ему медицинскими знаниями [5, 10]. Его труды, в особенности монументальный "Канон врачебной науки" (арабск. "Аль-Канун фи-т-Тибб"), представляющий собой энциклопедию медицинских знаний в пяти книгах, оказали огромное влияние на развитие медицинской мысли как на Востоке, так и на Западе, сформировав основы клинической медицины на многие столетия вперед [1, 4, 7].

ФИЛОСОФСКИЕ ОСНОВАНИЯ МЕДИЦИНЫ АВИЦЕННЫ

Как тело с душою, связаны тесно
Природа вещей и суть человека,
В единстве познания тайны телесной
Целительства мудрость живет век от века.

Теоретические основы медицины Авиценны неразрывно связаны с его философской системой, которая представляет собой оригинальный синтез аристотелизма, неоплатонизма и исламской традиции [2, 9]. В отличие от многих своих предшественников, Авиценна рассматривал медицину не только как практическое искусство, но и как науку, имеющую свои теоретические основания [8]. В своем трактате "О душе" Авиценна писал: «Врач должен быть уверен в причинах здоровья и болезни, а причины эти постигаются разумом, а не чувствами» [2, 3]. Данный подход отражает его глубокое убеждение в необходимости философского обоснования медицинской практики. Согласно Авиценне, физиология человека подчиняется тем же законам, что и все естественные явления. При этом он разделял аристотелевское учение о четырех первоэлементах (земля, вода, воздух, огонь) и соответствующих им качествах (сухость, влажность, холод, тепло), но трансформировал их в более сложную систему, включающую понятие "мизадж" (натура) – особого смешения первоэлементов в организме [1, 3]. В "Каноне врачебной науки" Авиценна пишет: «Мизадж есть качество, возникающее в результате взаимодействия противоположных качеств элементов, входящих в состав тела, когда они, воздействуя друг на друга, приходят ко взаимному согласию» [1]. Авиценна различал мизадж уравновешенный, представляющий собой идеальное соотношение элементов и их качеств, и неуравновешенный, характеризующийся преобладанием одного или нескольких качеств. Важно отметить, что уравновешенный мизадж не был для него абстрактным идеалом, но рассматривался относительно вида, индивида, органа и возраста [1, 8]. «Должно знать, что абсолютно уравновешенного мизаджа не существует ни в одном теле, ибо элементы никогда не смешиваются в равных весовых количествах, а если бы они так смешались, то непременно возникло бы

нечто иное, но никак не человеческое тело» [1]. Эти представления заложили основу индивидуального подхода к пациенту и позволили классифицировать типы телосложения и темперамента, что находит параллели в современных психосоматических концепциях [14, 15].

АНАТОМИЯ И ФИЗИОЛОГИЧЕСКИЕ КОНЦЕПЦИИ

В потоках крови, в дыхании легких,
В движении соков по тайным каналам,
Распознавал он с проницательным взором
Гармонию жизни, что в теле звучала.

Анатомические знания Авиценны были значительно более точными, чем у большинства его предшественников [4, 17]. В "Каноне" он описал около 240 костей, множество мышц, нервов и кровеносных сосудов. Особенно подробно им были изучены анатомия глаза, строение сердца и мозга [1, 20]. При описании мышц Авиценна обращал внимание не только на их форму и расположение, но и на функцию, что свидетельствует о его функциональном подходе к анатомии [1, 7]: «Мышцы созданы для произвольного движения. Они состоят из мясистой части, которая является источником силы, и сухожильной части, которая передает эту силу к кости... Сила сокращения мышцы зависит от количества мясистых волокон и их расположения» [1]. Физиологическая система Авиценны, хотя и базировалась на греко-арабской традиции, содержала множество оригинальных идей и наблюдений. Центральное место в его физиологии занимает учение о "силах" (куве), которые управляют всеми процессами в организме [1, 8, 11]. Авиценна выделял три основные силы:

1. Природная сила (кувва табиийа) – отвечает за питание, рост и размножение
2. Животная сила (кувва хайваниййа) – ответственна за движение и чувственное восприятие
3. Душевная сила (кувва нафсаниййа) – управляет мышлением, памятью и воображением

Каждая из этих сил имеет свой "центр": природная сила локализуется в печени, животная – в сердце, а душевная – в мозге. При этом Авиценна подчеркивал их взаимосвязь и взаимозависимость [1, 3]. В "Каноне" он пишет: «Эти силы действуют не изолированно, но взаимодействуют друг с другом, подобно тому, как различные части тела составляют единое целое. Усиление или ослабление одной силы неизбежно влияет на другие, и врач должен учитывать это в своей практике» [1]. Особенно новаторскими были его представления о кровообращении. Хотя Авиценна не открыл большой круг кровообращения (что сделал позже Уильям Гарвей), он описал малый круг, предположив, что кровь из правого желудочка сердца проходит через легкие, где очищается, а затем поступает в левый желудочек [1, 19]: «Кровь, прежде чем попасть в левую полость сердца, должна пройти через легкие, где она становится тонкой и смешивается с воздухом, а затем через "невидимые поры" поступает в артериальную

вену (легочную вену), которая ведет к левой полости сердца» [1]. Авиценна также детально изучил физиологию пищеварения, выделив несколько этапов этого процесса [1, 11]: «Пищеварение начинается во рту, где пища измельчается зубами и смешивается со слюной. Затем она поступает в желудок, где подвергается действию желудочного сока. Далее она переходит в кишечник, где происходит всасывание питательных веществ. Наиболее тонкая часть пищи через воротную вену поступает в печень, где превращается в кровь. Остатки выводятся из организма» [1]. Эти представления, несмотря на ограниченность знаний того времени, отражают системный подход Авиценны к пониманию физиологических процессов и их взаимосвязи [4, 11].

ПСИХОЛОГИЯ И УЧЕНИЕ О ДУШЕ

Душа человека как сад потаенный,
Где мысли, как птицы, и чувства, как волны,
Где разум – садовник, а тело – ограда,
И в этом единстве – здоровья отрада.

Психологические воззрения Авиценны тесно связаны с его философской концепцией души и разработаны главным образом в трактате "Книга о душе" (Китаб ан-нафс) и в соответствующих разделах "Канона врачебной науки" [2, 3, 14]. Следуя аристотелевской традиции, он выделял три вида души:

1. Растительная душа – ответственна за питание, рост и размножение
2. Животная душа – отвечает за движение и чувственное восприятие
3. Разумная душа – присуща только человеку и ответственна за мышление

Авиценна писал: «Душа совершенна и едина, но проявляет себя через различные силы. Подобно тому, как солнечный свет един, но по-разному отражается от разных поверхностей, так и душа проявляет себя различно через тела растений, животных и человека» [2, 3]. Особенно интересны его представления о внутренних чувствах, которые, по мнению Авиценны, связывают внешние ощущения с разумом [2, 14]. Он выделял пять внутренних чувств:

- Общее чувство (аль-хисс аль-муштарак) – объединяет данные всех органов чувств
- Представление (аль-хайаль) – сохраняет образы, полученные общим чувством
- Воображение (аль-мутахаййила) – комбинирует и разделяет образы
- Оценивающая сила (аль-вахмийа) – постигает нематериальные качества объектов
- Память (аль-хафиза) – сохраняет то, что постигла оценивающая сила

Авиценна локализовал эти внутренние чувства в различных отделах мозга, что было прообразом современных представлений о функциональной нейроанатомии [2, 14, 20]. «Общее чувство находится в переднем желудочке мозга, представление — в его передней части, воображение — в среднем желудочке, оценивающая сила — в его задней части, а память — в заднем желудочке мозга. Повреждение этих отделов мозга приводит к нарушению соответствующих

функций» [2, 20]. Авиценна уделял большое внимание роли эмоций в жизни человека и их влиянию на здоровье [1, 14]: «Гнев — это кипение крови в сердце, стремящейся к возмездию. Страх — это сжатие и охлаждение естественной теплоты сердца. Радость — это расширение и движение естественной теплоты наружу, к поверхности тела. Все эти состояния изменяют мизадж и могут привести как к здоровью, так и к болезни, в зависимости от их силы и продолжительности» [1]. Особый интерес представляют его исследования сна и сновидений. Авиценна считал сон естественным состоянием, необходимым для восстановления сил организма [1, 14, 15]: «Сон — это погружение чувствующей души внутрь тела, к его центру, чтобы дать ей отдых и восстановить силы... Сновидения же возникают, когда образы, хранящиеся в представлении, активизируются под влиянием телесных жидкостей или внешних воздействий» [1]. Он также описал различные нарушения сна и их связь с заболеваниями, предложив методы их коррекции [1, 15].

РАСШИРЕННЫЙ КОНТЕКСТ ЭПОХИ И ВЛИЯНИЕ НА РАЗВИТИЕ МЕДИЦИНЫ

Историческая эпоха, в которой жил и творил Абу Али Хусейн ибн Абдаллах ибн Сина, представляет собой уникальный период интеллектуального расцвета исламской цивилизации, известный как "Золотой век ислама" [21, 22]. Этот период (VIII-XIII вв.) характеризовался не только сохранением античного наследия, но и его критическим переосмыслением, развитием и обогащением новыми идеями и открытиями [22, 23]. В то время как Европа переживала период раннего Средневековья с относительным замедлением научного прогресса, на территориях, простиравшихся от Испании до Центральной Азии, формировались крупные научные и образовательные центры, такие как Дом Мудрости в Багдаде, библиотеки и обсерватории Самарканда, Бухары, Кордовы и Каира [21, 24].

Авиценна, родившийся на закате X века, унаследовал богатейшую интеллектуальную традицию, включавшую не только греко-римское наследие (труды Гиппократа, Галена, Аристотеля), но и достижения персидской, индийской и китайской медицины [24, 25]. Как отмечает исследователь исламской истории медицины П. Е. Порманн: "Уникальность Авиценны заключается в его способности не просто синтезировать разнородные медицинские традиции, но создать на их основе принципиально новую систему, в которой эмпирические наблюдения получают философское обоснование, а теоретические концепции проверяются клинической практикой" [26].

Важно отметить, что научная деятельность Авиценны протекала в условиях политической нестабильности. После падения Саманидского государства в 999 году, покровительствовавшего наукам и искусствам, Авиценне пришлось часто менять места жительства, находя временное пристанище при дворах различных правителей [5, 23]. Несмотря на эти трудности, за свою жизнь он написал более 450 трудов, из которых до нас дошло около 240 [9, 22]. Помимо "Ка-

нона врачебной науки", особую ценность представляют его трактаты "Книга исцеления", "Книга знания", "Книга указаний и наставлений", а также многочисленные медицинские трактаты по частным вопросам [2, 3, 9].

Влияние Авиценны на развитие медицинской науки трудно переоценить. В странах исламского мира "Канон врачебной науки" оставался основным медицинским учебником вплоть до XIX века [8, 24]. В Европе, куда этот труд проник благодаря переводу на латынь, выполненному Герардом Кремонским в XII веке, "Канон" изучался в университетах Монпелье, Падуи, Болоньи и Парижа до XVII века, выдержав более 30 изданий после изобретения книгопечатания [21, 27]. Многие медицинские термины, введенные Авиценной или сохраненные им из античной традиции, до сих пор используются в медицинской терминологии [27, 28].

ХОЛИСТИЧЕСКИЙ ПОДХОД И ПАРАЛЛЕЛИ С СОВРЕМЕННОЙ ИНТЕГРАТИВНОЙ МЕДИЦИНОЙ

Холистический подход Авиценны к пониманию человека и его здоровья, интегрирующий физиологические, психологические и социальные аспекты, находит многочисленные параллели в современной медицинской науке и практике [14, 19]. Определение здоровья Всемирной организацией здравоохранения как "состояния полного физического, психического и социального благополучия, а не просто отсутствия болезней или недугов" удивительно созвучно представлениям Авиценны о здоровье как гармоничном состоянии всех систем организма и психики человека [1].

Современная биопсихосоциальная модель заболеваний, разработанная американским психиатром Джорджем Энгелем в 1977 году и ставшая одной из основополагающих концепций современной медицины, во многом перекликается с учением Авиценны о взаимосвязи физических и психических процессов в организме [14]. Понимание Авиценной роли эмоций в возникновении и течении соматических заболеваний предвосхитило развитие современной психосоматической медицины [14, 15].

Принцип индивидуализации лечения, красной нитью проходящий через все медицинское наследие Авиценны [1, 8], в настоящее время возрождается в концепции персонализированной медицины, основанной на учете генетических, эпигенетических, средовых и других индивидуальных факторов пациента. Как писал Авиценна: "Каждый человек имеет свою особую натуру, отличную от натуры другого человека, и врач должен это учитывать при назначении лечения" [1].

Интегративный подход Авиценны к терапии, сочетающий различные методы лечения в зависимости от индивидуальных особенностей пациента и характера заболевания [1, 8], находит параллели в современной интегративной медицине, стремящейся объединить достижения как конвенциональной, так и традиционной медицины на основе доказательного подхода.

НАУЧНОЕ НАСЛЕДИЕ АВИЦЕННЫ В XXI ВЕКЕ: ПЕРСПЕКТИВЫ ПРИМЕНЕНИЯ И ИССЛЕДОВАНИЯ

Научное наследие Авиценны продолжает привлекать внимание исследователей во всем мире [10, 20]. В последние десятилетия наблюдается растущий интерес к изучению традиционных медицинских систем с позиций современной науки. Многие лекарственные растения, описанные Авиценной, становятся объектами фармакогностических исследований, направленных на выделение и изучение биологически активных веществ [33].

Так, недавние исследования противомикробных свойств мирры (Commiphora myrrha) и шафрана (Crocus sativus), рекомендованных Авиценной при инфекционных заболеваниях, выявили наличие в них соединений с выраженной антибактериальной активностью, в том числе против антибиотикорезистентных штаммов. Экстракты черного тмина (Nigella sativa), который Авиценна применял при заболеваниях дыхательной системы, демонстрируют противовоспалительные, иммуномодулирующие и бронхолитические свойства в современных исследованиях.

Методы физиотерапии и реабилитации, описанные Авиценной, также находят подтверждение в современных научных исследованиях. Например, его рекомендации по использованию контрастных водных процедур для укрепления иммунитета согласуются с данными о положительном влиянии адаптации к температурным воздействиям на иммунную систему [27, 29].

Диетологические принципы Авиценны, основанные на индивидуальном подходе и умеренности, обнаруживают параллели с современными персонализированными диетическими рекомендациями, учитывающими генетические особенности, микробиом кишечника и метаболический профиль пациента [26].

Психотерапевтические методы Авиценны, включавшие музыкотерапию, ароматерапию и регуляцию дыхания, находят подтверждение в современных исследованиях по комплементарной и альтернативной медицине [15]. Его рекомендации по использованию определенных ароматов для коррекции эмоциональных состояний соответствуют современным данным о влиянии эфирных масел на лимбическую систему мозга [21, 22].

В 2019 году Всемирная организация здравоохранения включила традиционную медицину в Международную классификацию болезней 11-го пересмотра (МКБ-11), признав ее значение для здравоохранения во многих странах мира. Это решение открывает новые перспективы для научного изучения и интеграции традиционных медицинских знаний, включая наследие Авиценны, в современную медицинскую практику [33, 34].

В условиях глобальных вызовов современного здравоохранения – от растущей антибиотикорезистентности до увеличения распространенности хронических неинфекционных заболеваний – холистический подход Авиценны к медицине, основанный на профилактике, индивидуализации лечения и интеграции различных терапевтических методов, приобретает особую актуальность. Как отмечает профессор Хаким Сайед Зиллур Рахман, директор Института ис-

тории медицины и медицинских исследований в Нью-Дели: "В эпоху высокотехнологичной, но все более фрагментированной медицины, целостный подход Авиценны к человеку и его здоровью может служить важным напоминанием о необходимости рассматривать пациента не как набор органов и систем, а как единое целое в контексте его физического, психического и социального благополучия" [35].

ЗАКЛЮЧЕНИЕ

Интеллектуальное наследие Авиценны представляет собой ослепительный синтез эмпирических наблюдений, философских прозрений и клинического опыта, которые преодолели границы своего времени и культурного контекста [4, 9, 20]. Анализируя вклад этого выдающегося ученого в медицину, физиологию и психологию, мы обнаруживаем не только историческое значение его трудов, но и удивительную актуальность многих его идей для современной науки и практики [10, 14, 20]. Авиценна не просто систематизировал медицинские знания своей эпохи — он создал целостную биомедицинскую парадигму, которая объединила понимание человека на всех уровнях: от элементарных физиологических процессов до сложных психических функций [4, 9]. Его подход к медицине был одновременно фундаментальным и прагматичным, теоретическим и клиническим, опирающимся как на рациональное мышление, так и на тщательные наблюдения [1, 4, 8]. Многие методологические принципы Авиценны демонстрируют удивительное созвучие с современными тенденциями развития медицинской науки [10, 11, 14, 19]. Феномен Авиценны как ученого и мыслителя тем более впечатляет, что его научные и философские достижения были реализованы в условиях, весьма далеких от современных представлений о профессиональной медицинской подготовке и научной инфраструктуре [4, 5, 6]. Не имея доступа к микроскопам, лабораторным исследованиям и другим техническим средствам современной диагностики, опираясь лишь на собственную наблюдательность, логическое мышление и клинический опыт, он сумел сформулировать принципы и концепции, многие из которых были подтверждены экспериментальной наукой спустя столетия [4, 10, 20]. Как отмечает академик Н.А. Агаджанян: «Творчество Авиценны представляет собой удивительный пример интеграции различных культурных традиций: древнегреческой, персидской, индийской и арабской медицины. В этом смысле он является олицетворением той культурной и научной синергии, которая возможна при открытом диалоге различных цивилизаций» [4]. В условиях современных вызовов, стоящих перед здравоохранением — от глобальных эпидемий до проблем старения населения, от технологизации медицины до вопросов доступности медицинской помощи — мудрость Авиценны может служить источником вдохновения и ориентиром для поиска гуманистических и научно обоснованных решений [4, 14, 19].

Список источников

1. Абу Али ибн Сина (Авиценна). Канон врачебной науки. В 5 книгах / Пер. с араб. М.А. Салье, У.И. Каримова, А. Расулева. – Ташкент: Изд-во АН УзССР, 1954-1960. (Доступны электронные версии через Национальную электронную библиотеку)

2. Абу Али ибн Сина. Избранные философские произведения / Отв. ред. М.Д. Диноршоев. – М.: Наука, 1980. – 552 с.

3. Абу Али ибн Сина. Сочинения. Т. 1. Душанбе: Дониш, 2005. – 960 с.

4. Бородулин В.И. История медицины. Избранные лекции. – М.: ГЭОТАР-Медиа, 2010. – 464 с. Доступна электронная версия на сайте издательства

5. Буховский Д.А. Авиценна - врач, философ, поэт. – М.: Медицина, 1980. – 183 с.

6. Петров Б.Д. Ибн Сина (Авиценна). – М.: Медицина, 1980. – 151 с.

7. Терновский В.Н. Ибн Сина (Авиценна). – М.: Наука, 1969. – 192 с.

8. Нуралиев Ю.Н. Медицинская система Ибн Сины (Авиценны). – Душанбе: Дониш, 2005. – 320 с.

9. Сагадеев А.В. Ибн Сина (Авиценна). – М.: Мысль, 1985. – 222 с. (Доступна электронная версия)

10. Amr S.S., Tbakhi A. Ibn Sina (Avicenna): The prince of physicians // Annals of Saudi Medicine. – 2007. – Vol. 27, № 2. – P. 134-135. DOI: 10.5144/0256-4947.2007.134

11. Ashtiyani S.C., Shamsi M., Cyrus A. A critical review of the works of pioneer physicians on kidney diseases in ancient Iran: Avicenna, Rhazes, Al-Akhawayni, and Jorjani // Iranian Journal of Kidney Diseases. – 2011. – Vol. 5, № 5. – P. 300-308. PMID: 21876306

12. Choopani R., Mosaddegh M., Kamalinejad M., Sohrabvand F. Avicenna (Ibn Sina) aspect of atherosclerosis // International Journal of Cardiology. – 2012. – Vol. 156, № 3. – P. 330. DOI: 10.1016/j.ijcard.2012.01.094

13. Dalfardi B., Mahmoudi Nezhad G.S., Mehdizadeh A. How did Avicenna diagnose stroke? // JAMA Neurology. – 2014. – Vol. 71, № 7. – P. 915. DOI: 10.1001/jamaneurol.2014.1064

14. Haque A. Psychology from Islamic Perspective: Contributions of Early Muslim Scholars and Challenges to Contemporary Muslim Psychologists // Journal of Religion and Health. – 2004. – Vol. 43, № 4. – P. 357-377. DOI: 10.1007/s10943-004-4302-z

15. Heyadri M., Hashempur M.H., Ayati M.H., Quintern D., Nimrouzi M., Mosavat S.H. The use of Chinese medicine in the management of psychiatric disorders: a review of research findings // Journal of Acupuncture and Meridian Studies. – 2015. – Vol. 8, № 6. – P. 285-291. DOI: 10.1016/j.jams.2015.07.005

16. Madineh S.M. Avicenna's Canon of Medicine and Modern Urology // Urology Journal. – 2008. – Vol. 5, № 4. – P. 284-293. PMID: 19101906

17. O'Malley C.D. Andreas Vesalius of Brussels (1514-1564). – Berkeley: University of California Press, 1964. – 480 p.

18. Shoja M.M., Tubbs R.S., Loukas M., Khalili M., Alakbarli F., Cohen-Gadol A.A. Vasovagal syncope in the Canon of Avicenna: The first mention of carotid artery hypersensitivity // International Journal of Cardiology. – 2009. – Vol. 134, № 3. – P. 297-301. DOI: 10.1016/j.ijcard.2009.02.035

19. Turgut O., Yalta K., Tandogan I. Islamic legacy of cardiology: Inspirations from the holy sources // International Journal of Cardiology. – 2010. – Vol. 145, № 3. – P. 496. DOI: 10.1016/j.ijcard.2010.04.082

20. Zargaran A., Mehdizadeh A., Zarshenas M.M., Mohagheghzadeh A. Avicenna (980-1037 AD) // Journal of Neurology. – 2012. – Vol. 259, № 2. – P. 389-390. DOI: 10.1007/s00415-011-6219-2

21. Goodman L.E. Avicenna. – London: Routledge, 2006. – 244 p.

22. Gutas D. Avicenna and the Aristotelian Tradition: Introduction to Reading Avicenna's Philosophical Works. – Leiden: Brill, 2014. – 615 p.

23. Wickens G.M. Avicenna: Scientist and Philosopher. – London: Luzac, 1952. – 108 p.

24. Pormann P.E., Savage-Smith E. Medieval Islamic Medicine. – Edinburgh: Edinburgh University Press, 2007. – 223 p.

25. Conrad L.I., Neve M., Nutton V., Porter R., Wear A. The Western Medical Tradition: 800 BC to AD 1800. – Cambridge: Cambridge University Press, 1995. – 556 p.

26. Pormann P.E. Avicenna on Medical Practice, Epistemology, and the Physiology of the Inner Senses // The Oxford Handbook of Islamic Philosophy / Ed. by K. El-Rouayheb, S. Schmidtke. – Oxford: Oxford University Press, 2017. – P. 245-271.

27. Siraisi N.G. Avicenna in Renaissance Italy: The Canon and Medical Teaching in Italian Universities after 1500. – Princeton: Princeton University Press, 1987. – 410 p.

28. Savage-Smith E. Attitudes toward dissection in medieval Islam // Journal of the History of Medicine and Allied Sciences. – 1995. – Vol. 50, № 1. – P. 67-110. DOI: 10.1093/jhmas/50.1.67

29. Tibi S. The Medicinal Use of Opium in Ninth-Century Baghdad. – Leiden: Brill, 2006. – 314 p.

30. Fancy N. Science and Religion in Mamluk Egypt: Ibn al-Nafis, Pulmonary Transit and Bodily Resurrection. – London: Routledge, 2013. – 186 p.

31. Naseri M., Rezaeizadeh H., Taheripanah T., Naseri V. Temperament Theory in the Iranian Traditional Medicine and Variation in Therapeutic Responsiveness, Based on Pharmacogenetics // Journal of Islamic and Iranian Traditional Medicine. – 2010. – Vol. 1, № 3. – P. 237-242.

32. Greenhalgh T., Howick J., Maskrey N. Evidence based medicine: a movement in crisis? // BMJ. – 2014. – Vol. 348. – P. g3725. DOI: 10.1136/bmj.g3725

33. Tekol Y. The medieval physician Avicenna used an herbal calcium channel blocker, Taxus baccata L. // Phytotherapy Research. – 2007. – Vol. 21, № 7. – P. 701-702. DOI: 10.1002/ptr.2173

34. Zarshenas M.M., Zargaran A., Müller J., Mohagheghzadeh A. Nasal Drug Delivery in Traditional Persian Medicine // JAMA Dermatology. – 2013. – Vol. 149, № 7. – P. 789. DOI: 10.1001/jamadermatol.2013.3100

35. Newman D.J., Cragg G.M. Natural Products as Sources of New Drugs over the Nearly Four Decades from 01/1981 to 09/2019 // Journal of Natural Products. – 2020. – Vol. 83, № 3. – P. 770-803. DOI: 10.1021/acs.jnatprod.9b01285

УДК [613.6:664]:616-07

ГЛАВА 16. СТРУКТУРА ЗАБОЛЕВАЕМОСТИ РАБОТНИКОВ ОБЩЕСТВЕННОГО ПИТАНИЯ

Колосова Елена Геннадьевна,
Сидорова Ирина Геннадьевна
к.м.н., доцент
ФГБОУ ВО «Оренбургский государственный медицинский университет» МЗ РФ

Аннотация: в главе рассматриваются вопросы структуры заболеваемости работников общепита, факторов риска их развития и основные направления профилактики профессиональных заболеваний. Так же приводятся данные удовлетворённости работников качеством проводимых периодических медицинских осмотров. В ходе исследования использовались данные анкетирования сотрудников одного из ресторанов города Оренбурга.
Ключевые слова: структура заболеваемости, работники общепита, факторы риска, профилактика профессиональных заболеваний, удовлетворенность качеством медицинского обследования.

THE STRUCTURE OF MORBIDITY OF CATERING WORKERS

Kolosova Elena Gennadievna,
Sidorova Irina Gennadievna

Abstract: the chapter discusses the structure of the morbidity of catering workers, risk factors for their development and the main directions of prevention of occupational diseases. Data on employee satisfaction with the quality of periodic medical examinations are also provided. The study used data from a survey of employees of one of the restaurants in Orenburg.
Keywords: morbidity structure, catering workers, risk factors, prevention of occupational diseases, satisfaction with the quality of medical examination.

В связи с непрекращающимся ускорением темпа жизни населения, современный потребитель все чаще переходит на готовую пищу в целях экономии своего времени. В связи с этим ресторанный бизнес получает с каждым годом все более выгодную позицию в сфере оказания услуг.

С увеличением предприятий общественного питания увеличиваются и рабочие места, а также технологии приготовления различных блюд. Вопрос о производстве пищевых продуктов, используемой техники и ее влиянии на организм сотрудников предприятия на данный момент считается недостаточно изученным, что делает эту тему актуальной.

Считается, что сотрудники пищевых предприятий подвергаются сочетанному воздействию ряда производственно-профессиональных, социально-бытовых факторов, оказывающих неблагоприятное влияние на состояние их

здоровья, что может способствовать возникновению производственно-обусловленных заболеваний. Учитывая этот факт, перед сотрудниками медицинских учреждений должна стоять задача на раннее выявление, лечение и профилактику заболеваний данной категории людей, при проведении ежегодного осмотра.

Преобладающими заболеваниями среди сотрудников общепита являются патологии опорно-двигательного аппарата, сердечно-сосудистой системы и пищеварительной системы, что ведет к нарушению не только физического здоровья, но и психического, привлекая за собой расстройства эмоциональной сферы, нарушение сна и перенапряжение.

Рассмотрим конкретнее факторы, оказывающие воздействие на трудовой процесс и состояние здоровья сотрудников.

Химические факторы определяются концентрацией в воздухе рабочей зоны веществ, образующихся в процессе варки пищи (минеральные масла, пыль мучная, пыль сахара), мытья посуды и оборудования (водяные пары, синтетические моющие и хлорсодержание средства), они могут проникать в организм через органы дыхания, желудочнокишечный тракт, кожные покровы и слизистые оболочки и оказывать раздражающие, аллергические реакции, оказывать токсичное и канцерогенное действия, а также влиять на репродуктивную функцию. Из этого следует, что на предприятиях сотрудникам необходимо соблюдать стандарты безопасности при контакте с химикатами (использование индивидуальных средств защиты: маски, перчатки, фартуки и т.д.) [2]

Виброакустические факторы - являются одной из наиболее частых причин возникновения профессиональных заболеваний у работников.

Степень вредности и опасности условий труда при действии виброакустических факторов устанавливается с учетом их временных характеристик (постоянный, непостоянный шум, вибрация и т.д.). Для определения предельно допустимого уровня шума, соответствующего конкретному рабочему месту, необходимо провести количественную оценку тяжести и напряженности труда, выполняемого работником.

Как правило, при любом воздействии высоких уровней шума на работника происходит рост его утомляемости, смещение порога восприятия звуковых сигналов и рабочих команд. Кроме того, по данным медицинских исследований, возможно негативное воздействие на процессы пищеварения и кровообращения, возрастают затраты организма на выполнение всех видов работ.

Воздействие шума (на горячем/холодном цехе, громкая музыка) в течение продолжительного времени может привести к возникновению таких заболеваний, как неврозы, гипертония и язвенная болезнь, кожные и кишечные заболевания, поэтому ранняя диагностика особенно важна для недопущения развития профессиональных патологий у работников и связанных с ними потерь рабочего времени, производительности труда и качества выполняемых работ. [1]

К неблагоприятным факторам рабочей среды относятся также сквозняки, исключить которые возможно путем регулирования системы вентиляции и

кондиционирования.

Большое значение в развитии профессиональной патологии имеет тяжесть и напряженность трудового процесса - рабочий процесс вынуждает сотрудника длительно оставаться в одном и том же положении, чаще стоя, что дает значительную статическую нагрузку, и как следствие - приводит к перенапряжению отдельных систем и органов тела, в большинстве случаев костно-связочного аппарата и мышечной системы. Остеохондроз, деформация костей и суставов, сосудистые изменения в виде расширения вен нижних конечностей - заболевания поваров, продавцов, официантов. Для предотвращения возникновения такой патологии необходимо грамотное нормирование режима труда и отдыха, а также организация производственного процесса таким путем, чтобы выполнение всех манипуляций обеспечивало возможность свободного перехода тела человека из одного положения в другое. [4]

Также необходимо учитывать, что ст. 91 ТК РФ гласит: «Нормальная продолжительность рабочего времени не может превышать 40 часов в неделю». Данный юридический постулат стал основополагающим в методике подсчета нормы рабочего времени.

Превышение нормальной продолжительности рабочего времени также ведет к ухудшению физического и психического состояния сотрудника, что усугубляет его здоровье и трудоспособность, это важный момент, который должен учитывать не только работник, но и работодатель, в случае чего он будет вынужден нести административную ответственность за нарушение ТК РФ (ч. шестая ст. 99 ТК РФ).

В связи с ростом точек ресторанов быстрого питания, растет и уровень вакантных мест, в связи с чем нередко на работу принимают сотрудников младше 18 лет. Этот возраст нас особенно интересует, поскольку несовершеннолетние могут пройти только медицинское обследование при приеме на работу, но профилактическое медицинское обследование (диспансеризацию) они могут пройти только при достижении совершеннолетия.

Что делать сотрудникам, длительно контактирующим с вредными факторами? Этот вопрос должен решать работодатель.

Согласно Трудовому Кодексу, для несовершеннолетних работников установлена сокращенная продолжительность рабочего времени и дополнительные требования к режимам их труда (ст. 92 ТК РФ). Нормальная продолжительность рабочего времени - 40 часов в неделю - сокращается:

- на 16 часов для работников в возрасте до 16 лет (то есть не более 24 часа в неделю);
- на 5 часов для работников в возрасте от 16 до 18 лет (то есть не более 35 часов в неделю).

Продолжительность рабочего времени в неделю учащихся образовательных учреждений в возрасте до 18 лет, работающих в течение учебного года в свободное от учебы время, не должна превышать половины указанных норм [3].

Немаловажную роль играют ограничения при реализации трудовых прав несовершеннолетних, установленные законом в целях защиты их интересов. Так, статья 265 ТК РФ, закрепляет запрет на применение труда лиц в возрасте до 18 лет на работах с вредными и (или) опасными условиями труда, на подземных работах, а также на работах, выполнение которых может причинить вред их здоровью и нравственному развитию. В перечень таких работ включены: игорный бизнес, работа в ночных кабаре и клубах, производство, перевозка и торговля спиртными напитками, табачными изделиями, наркотическими и токсическими препаратами. [5]

Ответственность за нарушение трудовых прав, в том числе несовершеннолетних предусмотрена как в Кодексе Российской Федерации об административной ответственности (статья 5.27), так и в Уголовном кодексе Российской Федерации (статья 145.1).

При помощи анкетирования нам удалось выявить уровень заболеваемости сотрудников и наиболее часто встречающиеся заболевания - в опросе участвовало 50 человек, из которых 81,3% женщины и 18,8% мужчины.

На вопрос как часто сотрудники болеют респираторными заболеваниями в течение года (в опросе приняли участие 14 человек), ответы были следующими: 14,3% - 2 раза и по 7,1% разделили между собой ответы «1 раз, 1-2 раза, 2-3 раза, 5-7 раз, 6-7 раз, от 3х раз, не болею вообще» (рис. 1).

Рис. 1. Частота заболеваемости ОРЗ в течение года

На вопросы об общем состоянии здоровья анкетируемые ответили следующим образом: 43,8% анкетируемых считают, что ухудшение состояния здоровья связано с работой в сфере общественного питания, 43,8% не связывают и 12,5% затруднились ответить. (рис. 2).

Из наиболее подверженных систем организма ухудшению подверглись две - пищеварительная и опорно-двигательная - разделили по 31,3%. Также по 18,8% разделили сердечно-сосудистая и дыхательная системы. (рис. 3).

Рис. 2. Взаимосвязь условий работы и состояния здоровья

Рис. 3. Влияние работы в сфере общественного питания на системы организма

Рис. 4. Употребление энергетических напитков как фактор развития бессонницы

На вопрос страдают ли сотрудники бессонницей, ответы разделились ровно: 50% страдают и 50% нет. Из них 33,3% сотрудников связывают это с употреблением энергетических напитков (рис. 4).

На вопрос как они оценивают свое состояние на работе, наибольший процент (56,3%) оценивают себя на 4 из пятибалльной шкалы, где 1 - очень плохо, а 5 - отлично. По 18,8% разделили 3 и 1 балл, на 2 балла пришлось 6,3% опрошенных (рис. 5).

Рис. 5. Оценка состояния работника на момент пребывания на рабочем месте

Таким образом анкетирование позволило определить, что наиболее выраженными среди сотрудников являются заболевания пищеварительной и опорно-двигательной систем, также они находятся под высоким риском ОРЗ. Изучение заболеваемости с временной утратой трудоспособности имеет большое значение как для государства, так и для работников, этот вопрос необходимо тщательнее рассматривать ввиду необходимости ежегодного диспансерного наблюдения данной категории людей.

Согласно европейской статистике по профессиональным заболеваниям, на болезни опорно-двигательного аппарата (ОДА) приходится около 38 % всех профессиональных заболеваний. В сфере общественного питания существует множество факторов риска для развития заболеваний ОДА: работа характеризуется длительными многочасовыми статическими нагрузками с наклоном вперед (неудобная вынужденная поза), повторяющимися и быстрыми движениями рук и запястья (стереотипные движения), длительным и сильным напряжением рук и запястья, а также переносом и подъемом тяжелых предметов.

Заболевания мягких тканей, спондилез и связанные с ними расстройства занимают ведущее место в рейтинге заболеваний ОДА у данной группы работников, что связано с чрезмерным использованием мышц, быстрыми и повторяющимися движениями, а также длительными статическими нагрузками и неудобной вынужденной позой. Имеется повышенный риск заболеваний перифе-

рических сосудов, среди них варикозное расширение вен нижних конечностей из-за длительной статической нагрузки в течение рабочего дня. Результаты систематических наблюдений свидетельствуют, что работающие стоя более 3–4 часов в день имеют повышенный риск развития варикоза (в 2,5 раза) по сравнению с не имеющими такой нагрузки. При этом распространённость этого заболевания или даже риск приобрести его более высокие у женщин, чем у мужчин.

Одним из факторов риска для работников пищевой промышленности является воздействие опасных уровней звука. В ряде исследований показано, что средний уровень звука на предприятиях пищевой промышленности может варьироваться от 58 до 98 дБА, это влияет на развитие специфических ауральных эффектов, проявляющихся как в виде медленно прогрессирующего понижения слуха по типу неврита слухового нерва (кохлеарный неврит), так и с некоторыми экстраауральными эффектами, включая головные боли, повышенное кровяное давление, потерю сна, увеличение частоты сердечных сокращений, боли в области Безопасность техногенных и природных систем сердца, повышение артериального давления, дисфункцию ЖКТ, снижение иммунологической реактивности, стрессорную метаболическую реакцию. [2]

Помимо профессиональных заболеваний, возникают риски возникновения травмоопасных ситуаций и несчастных случаев, в том числе со смертельным исходом. На рисунке 6 представлены данные Роструда «Распределение страховых несчастных случаев на производстве по классам профессионального риска с 2019 по 2023 г.г. в % от общего количества страховых несчастных случаев на производстве» по работникам пищевой промышленности. [5]

С целью снижения количества несчастных случаев, случаев травматизма и возникновения профессиональных заболеваний, а также приведения условий труда в соответствие с санитарно-гигиеническими нормами необходимо решить следующие задачи по охране труда на предприятиях пищевой промышленности:

— повысить эффективность обучения безопасности труда и пропаганду охраны труда;

— нормализовать санитарно-гигиенические условия труда;

— обеспечить безопасность производственного оборудования, технологических процессов, зданий, сооружений, помещений, территории предприятия;

— проводить профессиональный отбор работников с точки зрения пригодности по безопасности труда;

— обеспечить работающих средствами индивидуальной защиты и коллективной защиты;

— проводить постоянный мониторинг и ввести контроль за соблюдением правил охраны труда и техники безопасности;

— мотивировать работников к соблюдению собственной безопасности и т. д.

Для предотвращения распространения заболеваний как среди населения, так и внутри коллектива проводятся периодические медицинские осмотры, в установленное время в целях динамического наблюдения за состоянием здоро-

вья работников, своевременного выявления начальных форм профессиональных заболеваний, ранних признаков воздействия вредных и (или) опасных факторов рабочей среды, трудового, на состояние здоровья работников. [3]

Рис. 6. Распределение страховых несчастных случаев на производстве

В соответствии с пунктом 15 приложения 2 приказа Министерства здравоохранения и социального развития РФ от 12 апреля 2011 г. №302н «Об утверждении перечней вредных и (или) опасных производственных факторов и работ, при выполнении которых проводятся обязательные предварительные и периодические медицинские осмотры (обследования)» и «Порядка проведения обязательных предварительных и периодических медицинских осмотров (обследований) работников, занятых на тяжелых работах и на работах с вредными

и (или) опасными условиями труда», частота проведения периодических медицинских осмотров работников в организациях общественного питания, торговли, буфетах, на пищеблоках – 1 раз в год.

Приказ Минздрава России от 28.01.2021 N 29н (ред. от 02.10.2024) "Об утверждении Порядка проведения обязательных предварительных и периодических медицинских осмотров работников, предусмотренных частью четвертой статьи 213 Трудового кодекса Российской Федерации, перечня медицинских противопоказаний к осуществлению работ с вредными и (или) опасными производственными факторами, а также работам, при выполнении которых проводятся обязательные предварительные и периодические медицинские осмотры" определяет необходимый перечень специалистов и исследований при поступлении на работу и для осуществления дальнейшей деятельности работников общепита.

Проведя анкетирование сотрудников предприятия общепита, мы определили, как оценивают качество проводимой диагностики на медицинских осмотрах.

Выяснилось, что 50% респондентов считают, что им не оказывают должное внимание на осмотре, 31,3% затруднились ответить и только 18.8% довольны качеством проведенной диагностики (рис. 7).

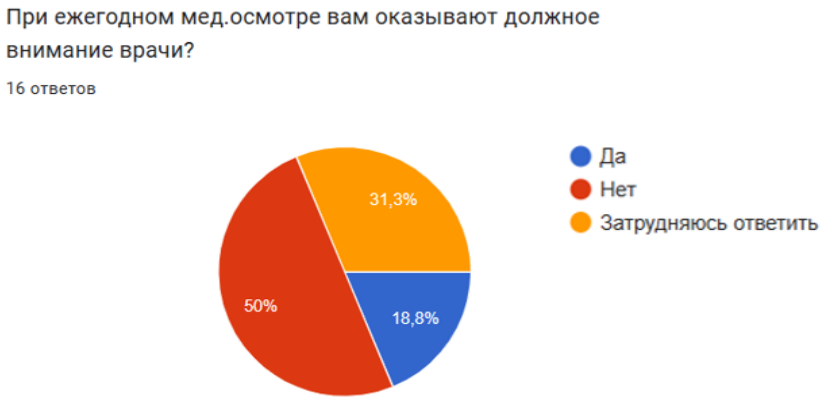

Рис. 7. Оценка качества диагностики при медицинских осмотрах

Рис. 8. Оценка качества периодических осмотров по пятибалльной шкале

На просьбу оценить работу специалистов клиник, мнение разделилось: 31,4% сотрудников общепита оценивают на 3 и 5 балла, 18,8% на 4 балла, 12,5% на 1 балл и лишь 6,3% на 5 баллов (рис. 8).

На вопрос, хотели бы они улучшить качество осмотра сотрудниками медицинской организации 81,7% ответили утвердительно и 18,8% довольны комиссией (рис. 9).

Рис. 9. Оценка качества диагностики периодических осмотров

Как показал опрос, периодический медицинский осмотр, по мнению сотрудников общественного питания, проводится недостаточно углубленно и компетентно. В связи с этим необходимо наиболее тщательно подходить к вопросу ранней диагностики, выявлению и лечению заболеваний данной категории людей, чтобы не допустить хронизацию патологических процессов. Одним из важнейших моментов работы является профилактика заболеваний, с целью недопущения их развития или перехода в фазу обострения.

На вопрос, предлагает ли работодатель сотрудникам какие-либо мероприятия по профилактике заболеваний, большинство (75%) дали отрицательный ответ и 25% - положительный, 81,3% сотрудников также ответили, что работодатель не учитывает их состояние здоровья и лишь 18,3% ответили обратное. Также большинство работников сказали, что работодатель не создает комфортные условия труда - 68,8% и только 31,8% остались довольны условиями труда на производстве (рис. 10).

Результаты проведенного анализа свидетельствуют о том, что работодатель не заинтересован в здоровье сотрудников, что ведет к увеличению общего количества случаев заболеваемости у работников пищевой промышленности.

Таким образом, можно сделать вывод, что присутствует необходимость внедрения и реализации на предприятиях ряда корректирующих или предупреждающих мероприятий, направленных на устранение причин возникновения несчастных случаев, травм, развития профессиональных заболеваний.

Таким образом, можно сделать вывод, что сотрудники сферы общественного питания подвержены развитию профессиональных заболеваний, как и сотрудники тяжелых сфер деятельности. Наиболее часто подвергаются влиянию опорно-двигательная система, пищеварительная система, сердечно-сосудистая,

дыхательная системы и при длительном влиянии ухудшается не только физическое, но и психическое состояние.

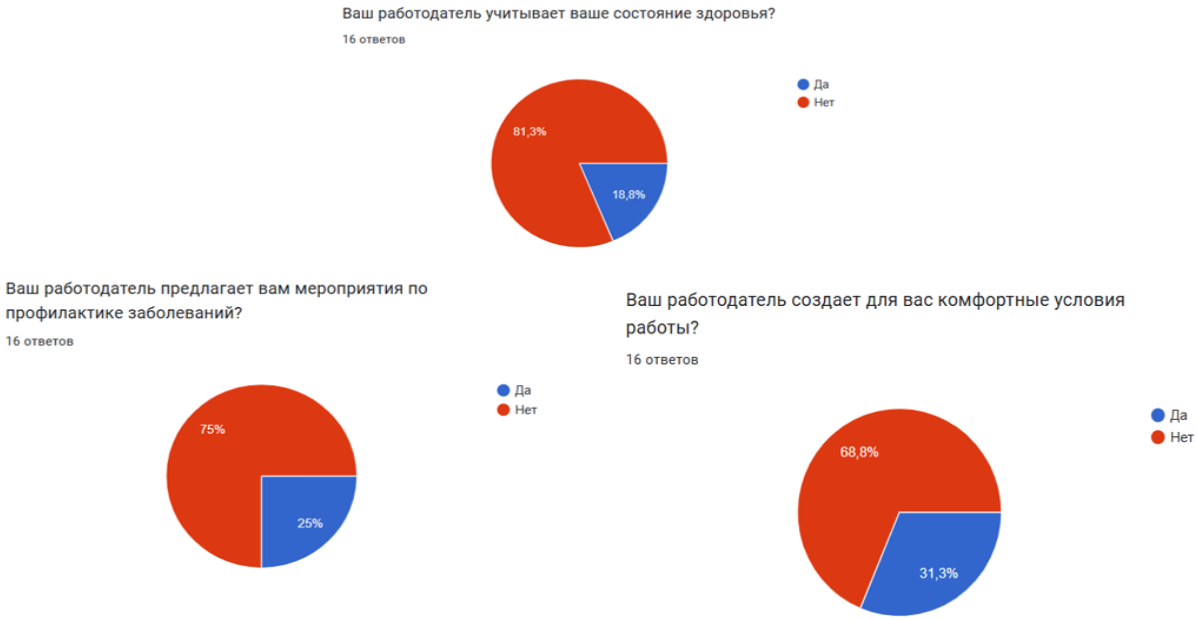

Рис. 10. Оценка вклада работодателя в профилактику заболеваний

Респонденты, ответив на вопросы анкетирования, оценили ежегодные медицинские осмотры недостаточными, что является поводом улучшения качества оказываемых услуг для предупреждения и развития профессиональной патологии. Необходимо отметить, что работодатель также является важным звеном в процессе профилактики заболеваний. С его стороны необходимо предпринять меры для сохранения здоровья сотрудников и повышения их трудоспособности, в виде фиксированных перерывов, обязательных отпусков, строгим соблюдением режима труда и отдыха, направление на санаторно-курортное лечение, проведение производственной гимнастики и т.д.

Список источников

1. Влияние виброакустических факторов на безопасность и здоровье работников промышленных предприятий / Хоменко А.О., Якшина Н.В., Мушников В.С., Ильин С.М., Самарская Н.А., Чекмарева М.А./ Экономика труда – Том 9, номер 12. – декабрь 2022

2. Шулькин Л.Л. Гигиена ресторанного бизнеса. Условия труда и здоровье работников ресторанов [Текст]: монография / Шулькин Леонид Львович; М-во образования и науки России, Федеральное гос. бюджетное образовательное учреждение высш. проф. образования Российский гос. торгово-экономический ун-т, Омский ин-т (фил.). - Омск: Омский ин-т (фил.) РГТЭУ, 2013. - 147 с.

3. Официальный сайт Министерства внутренних дел Российской Федерации 2025, МВД России. Трудовые права несовершеннолетних.

4. Профессиональная заболеваемость и производственный травматизм у работников пищевой промышленности / В. Ю. Контарева, С. Н. Белик - Безопасность техногенных и природных систем 2022. № 1. С. 32—40.

5. Руководство по гигиенической оценке факторов рабочей среды и трудового процесса. Критерии и классификация условий труда Р 2.2.2006–05

Авторский коллектив

Аленичева Т.С., Аменицкий А.В., Аменицкий Д.А., Аршун В.В., Атьман В.В., Балтабеков С.Б., Веремеев Р.Д., Зинюков Ю.В., Зонненберг Ю.Е., Колосова Е.Г., Кочергин И.Г., Куницын В.И., Лаврикова Н.И., Мамаев О.А., Мамаева Н.А., Расторгуева К.М., Рудикова-Фронхёфер Л.В., Рухович И.В., Сидорова И.Г., Фролов С.В., Хамчиев К.М., Хамчиева З.К.

16+

НАУЧНОЕ ИЗДАНИЕ

АКТУАЛЬНЫЕ ВОПРОСЫ НАУКИ, ТЕХНОЛОГИЙ И ОБЩЕСТВА

Монография

Под общей редакцией
кандидата экономических наук Г. Ю. Гуляева
Подписано в печать 27.04.2025.
Формат 60×84 1/16. Усл. печ. л. 13,5
Тираж 500 экз.

МЦНС «Наука и Просвещение»
440062, г. Пенза, Проспект Строителей д. 88, оф. 10
www.naukaip.ru

ISBN 978-5-00236-852-5

Уважаемые коллеги!

Приглашаем Вас принять участие в Международных научно-практических конференциях!

Дата	Название конференции	Услуга	Шифр
5 июня	XXI Международная научно-практическая конференция **АКТУАЛЬНЫЕ ВОПРОСЫ СОВРЕМЕННОЙ НАУКИ**	120 руб. за 1 стр.	МК-2377
5 июня	Международная научно-практическая конференция **НОВЫЕ НАУЧНЫЕ ИССЛЕДОВАНИЯ И РАЗРАБОТКИ 2025**	120 руб. за 1 стр.	МК-2378
5 июня	IX Международная научно-практическая конференция **ЭКОНОМИКА: АКТУАЛЬНЫЕ ВОПРОСЫ ТЕОРИИ И ПРАКТИКИ**	120 руб. за 1 стр.	МК-2379
5 июня	IX Международная научно-практическая конференция **ПЕДАГОГИКА: АКТУАЛЬНЫЕ ВОПРОСЫ ТЕОРИИ И ПРАКТИКИ**	120 руб. за 1 стр.	МК-2380
5 июня	IX Международная научно-практическая конференция **ЮРИСПРУДЕНЦИЯ: АКТУАЛЬНЫЕ ВОПРОСЫ ТЕОРИИ И ПРАКТИКИ**	120 руб. за 1 стр.	МК-2381
5 июня	XXV Международная научно-практическая конференция **СТУДЕНЧЕСКИЕ НАУЧНЫЕ ИССЛЕДОВАНИЯ**	120 руб. за 1 стр.	МК-2382
10 июня	XXII Международная научно-практическая конференция **АКТУАЛЬНЫЕ ВОПРОСЫ ОБЩЕСТВА, НАУКИ И ОБРАЗОВАНИЯ**	120 руб. за 1 стр.	МК-2383
10 июня	VII Международная научно-практическая конференция **ВРЕМЯ НАУКИ: АКТУАЛЬНЫЕ ВОПРОСЫ, ДОСТИЖЕНИЯ И ИННОВАЦИИ**	120 руб. за 1 стр.	МК-2384
10 июня	XI Международная научно-практическая конференция **СТУДЕНТ И НАУКА: АКТУАЛЬНЫЕ ВОПРОСЫ СОВРЕМЕННЫХ ИССЛЕДОВАНИЙ**	120 руб. за 1 стр.	МК-2385
12 июня	XXIV Всероссийская научно-практическая конференция **МОЛОДЫЕ УЧЁНЫЕ РОССИИ**	120 руб. за 1 стр.	МК-2386
12 июня	XVII Международная научно-практическая конференция **НАУЧНЫЕ ИССЛЕДОВАНИЯ 2025**	120 руб. за 1 стр.	МК-2387
15 июня	Международная научно-практическая конференция **АКТУАЛЬНЫЕ ПРОБЛЕМЫ СОВРЕМЕННОГО ОБЩЕСТВА, НАУКИ И ОБРАЗОВАНИЯ**	120 руб. за 1 стр.	МК-2388
15 июня	XLI Международная научно-практическая конференция **СОВРЕМЕННЫЕ НАУЧНЫЕ ИССЛЕДОВАНИЯ: АКТУАЛЬНЫЕ ВОПРОСЫ, ДОСТИЖЕНИЯ И ИННОВАЦИИ**	120 руб. за 1 стр.	МК-2389
15 июня	III Международная научно-практическая конференция **НАУКА И МОЛОДЫЕ УЧЁНЫЕ**	120 руб. за 1 стр.	МК-2390
15 июня	XVIII Международная научно-практическая конференция **АКТУАЛЬНЫЕ ВОПРОСЫ ЭКОНОМИКИ**	120 руб. за 1 стр.	МК-2391
15 июня	XVIII Международная научно-практическая конференция **АКТУАЛЬНЫЕ ВОПРОСЫ ПЕДАГОГИКИ**	120 руб. за 1 стр.	МК-2392
15 июня	XVIII Международная научно-практическая конференция **АКТУАЛЬНЫЕ ВОПРОСЫ ЮРИСПРУДЕНЦИИ**	120 руб. за 1 стр.	МК-2393

www.naukaip.ru