СЕКЦИЯ 14

«СОВРЕМЕННЫЕ ТЕХНОЛОГИИ НАУКИ И ОБРАЗОВАНИЯ В СФЕРЕ ВООРУЖЕНИЯ И БЕЗОПАСНОСТИ»

СОДЕРЖАНИЕ

ВОПРОСЫ РЕАЛИЗАЦИИ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ «БОЕПРИПАСЫ И ВЗРЫВАТЕЛИ»

Акимов С.С., кандидат технических наук
Федеральное государственное бюджетное образовательное учреждение высшего образования «Оренбургский государственный университет»

Аннотация: описаны ключевые аспекты реализации образовательной программы «Боеприпасы и взрыватели», направленной на подготовку специалистов в области вооружения и военной техники. Освещено создание современной лаборатории, оснащенной макетами боеприпасов, специализированными стендами и технической документацией. Подчеркнуто внедрение передовых технологий 3D-моделирования и аддитивного производства для изучения конструкций и изготовления прототипов. Отмечена организация практических занятий по сборке и разборке образцов, обеспечивающих формирование профессиональных навыков. Программа интегрирует теоретическую подготовку с практикой с использованием современного оборудования.

Ключевые слова: боеприпасы и взрыватели, образовательная программа, лаборатория.

Образовательная программа «Боеприпасы и взрыватели» предназначена для подготовки специалистов, обладающих практическими навыками и теоретическими знаниями в области проектирования, производства, эксплуатации и обслуживания вооружения и военной техники. Реализация данной программы включает создание современных лабораторных условий, развитие практических навыков студентов и использование передовых технологий для моделирования и производства образцов боеприпасов. В рамках реализации данной программы сделан ряд значимых шагов, которые позволяют обеспечить высокий уровень подготовки будущих специалистов.

Одним из ключевых этапов развития образовательной программы стало открытие новой лаборатории, оборудованной современными средствами для проведения практических занятий и экспериментов. Лаборатория представляет собой специализированное пространство, оснащенное разнообразным оборудованием, необходимым для изучения конструкции, физических свойств и методов испытаний боеприпасов и взрывателей.

В рамках оснащения лаборатории приобретены макеты образцов боеприпасов и взрывателей различного назначения, их комплектующие элементы, а также набор технических описаний и плакатов. Макеты выполнены по реальным образцам и позволяют студентам наглядно изучать конструкцию, особенности сборки и взаимодействия элементов. Наличие разных типов

боеприпасов способствует расширению практических навыков и пониманию их функционирования в различных условиях.

Рисунок 1 – Модели боеприпасов

Для расширения возможностей учебного процесса в программе активно разрабатываются и создаются стенды для проведения лабораторных работ и натурных экспериментов. Эти стенды позволяют моделировать реальные процессы, а также исследовать поведение боеприпасов и взрывателей в различных условиях.

Рисунок 2 – Стенд для оценки правильности разбора боеприпасов

Самостоятельная разработка стендов осуществляется с учетом требований к безопасной эксплуатации, удобству использования и точности измерений. Стенды оснащены комплектами измерительной и регистрирующей аппаратуры,

которая позволяет фиксировать параметры процессов, такие как давление, температура, сила и другие важные характеристики.

В рамках развития программы активно внедряются современные технологии моделирования и производства. Это существенно повышает качество образовательного процесса и дает студентам навыки работы с передовыми инструментами и методами.

Использование программных комплексов для 3D моделирования позволяет создавать точные виртуальные копии боеприпасов и взрывателей. Студенты могут изучать конструкции, проводить компьютерные испытания и оптимизировать модели без затрат на физические материалы. Применение аддитивных технологий, таких как 3D-печать, позволяет получать прототипы и тестовые образцы сложных компонентов боеприпасов. Это ускоряет процесс проектирования, облегчает модификацию и позволяет экспериментировать с различными конфигурациями. В результате студенты приобретают навыки работы с современными производственными технологиями.

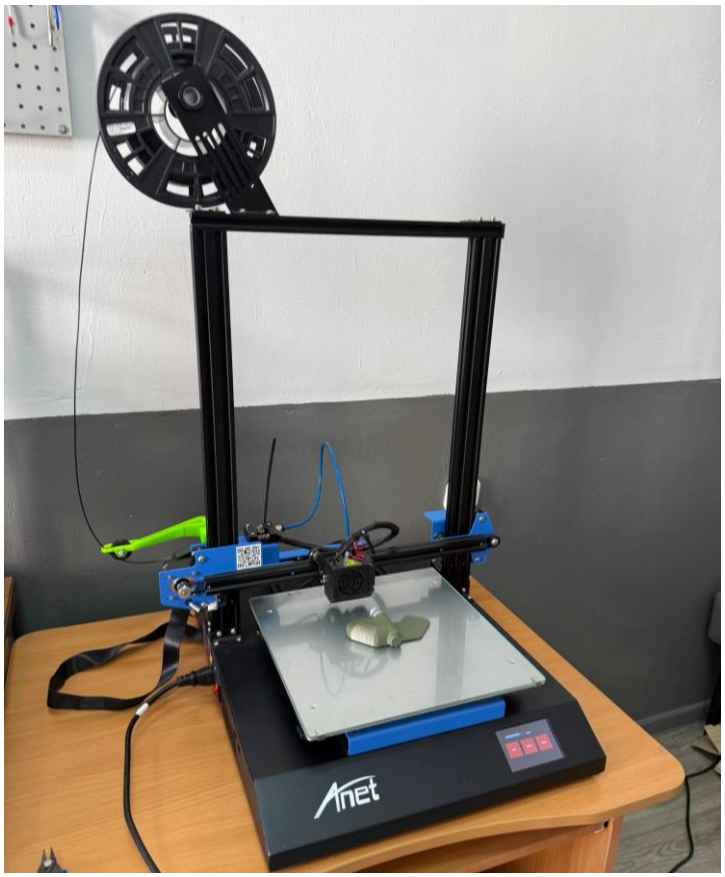


Рисунок 3 – 3D принтер

Для эффективного обучения необходимо современное оснащение рабочих мест. В рамках программы созданы рабочие зоны со столами и набором

инструментов для сборки, разборки и обслуживания боеприпасов. Это обеспечивает практический опыт, необходимый для формирования профессиональных навыков.

Были приобретены ручные инструменты для разборки и сборки, а также специализированное оборудование для техобслуживания. Столы и рабочие места организованы с учетом требований безопасности и эргономики, что позволяет студентам работать эффективно и без риска.

Практическая подготовка включает сборку и разборку реальных образцов, проведение профилактических осмотров, диагностику неисправностей и испытания готовых боеприпасов. Такой подход способствует закреплению теоретических знаний и развитию профессиональных умений.

Таким образом, реализация образовательной программы «Боеприпасы и взрыватели» достигла значимых результатов благодаря созданию современной материально-технической базы, внедрению передовых технологий и развитию практических навыков студентов. Открытие новой лаборатории и комплектование ее макетами образцов и технической документацией создали условия для углубленного обучения, а разработанные стенды и использование 3D моделирования существенно расширили возможности практических занятий. В дальнейшем предполагается развитие инфраструктуры и интеграция новых технологий для поддержания высокого качества подготовки специалистов в области вооружения и военной техники.

Список литературы

1 Шепель, В. Н. Модернизация метода гистограмм для выявления принадлежности неизвестного массива данных определенному закону распределения вероятностей / В. Н. Шепель, С. С. Акимов // Вестник Оренбургского государственного университета. – 2014. – № 9(170). – С. 179-181.

2 Трипкош, В. А. Особенности построения системы управления мехатронными модулями / В. А. Трипкош, С. С. Акимов // Компьютерная интеграция производства и ИПИ-технологии : Сборник материалов X Всероссийской конференции, Оренбург, 18–19 ноября 2021 года. – Оренбург: Оренбургский государственный университет, 2021. – С. 220-223.

3 Трипкош, В. А. Синтез алгоритма машинного распознавания ситуаций на основе составной байесовской процедуры принятия решений / В. А. Трипкош, С. С. Акимов // Научно-технический вестник Поволжья. – 2022. – № 6. – С. 91-95.

4 Трипкош, В. А. Алгоритмы принятия решений для комбинированных систем автоматического распознавания образов / В. А. Трипкош, С. С. Акимов //

Университетский комплекс как региональный центр образования, науки и культуры : Материалы Всероссийской научно-методической конференции (с международным участием), Оренбург, 23–25 января 2020 года. – Оренбург: Оренбургский государственный университет, 2020. – С. 741-745.

5 Ульянова Т.С. Способ определения измерительной сложности приборов и устройств для построения информационно-измерительной системы / Т. С. Ульянова, С. С. Акимов //Автоматизация. Современные технологии. – 2023. – Т. 77, № 11. – С. 523-527.

6 Трипкош, В. А. Программно-аппаратная система управления робото-техническим комплексом / В. А. Трипкош, С. С. Акимов // Университетский комплекс как региональный центр образования, науки и культуры : Сборник материалов Всероссийской научно-методической конференции, Оренбург, 26–27 января 2022 года. – Оренбург: Оренбургский государственный университет, 2022. – С. 1470-1474.

7 Трипкош, В. А. Применение инструментов бережливого производства на основе байесовского алгоритма распознавания / В. А. Трипкош, С. С. Акимов // Современные наукоемкие технологии. – 2023. – № 3. – С. 40-44.

ПРИМЕНЕНИЕ ИНТЕЛЛЕКТУАЛЬНЫХ ЦИФРОВЫХ ДВОЙНИКОВ В ВОЕННОМ ПРОИЗВОДСТВЕ

М.В. Архапчева, С.С. Акимов, кандидат технических наук
Федеральное государственное бюджетное образовательное учреждение высшего образования «Оренбургский государственный университет», г. Оренбург

Аннотация. Современное военное производство активно интегрирует цифровые двойники, обеспечивающие виртуальное моделирование объектов и процессов для повышения эффективности и прогнозирования. Анализ литературных источников подтверждает их роль в оптимизации управления, снижении рисков и трансформации оборонно-промышленного комплекса.

Ключевые слова: военное производство, цифровые двойники, моделирование, оптимизация, управление рисками, оборонно-промышленный комплекс.

Современное военное дело претерпевает глубокие изменения, становясь все более технологически углубленным, зависимым от новых, информационных технологий. Развитие таких технологий перекраивает понимание военного дела, предлагая различные варианты решения, от новых видов вооружения до интеллектуальных систем управления.

Среди новых, ключевых направлений развития военных технологий можно выделить следующие:

– новые автономные системы, такие как беспилотные летательные аппараты (БПЛА), автономные подводные аппараты (АПА), роботизированные наземные платформы;

– системы, оснащенные искусственным интеллектом, в том числе в вопросах анализа больших данных (Big Data), распознавания образов, построения прогностических моделей, способных имитировать ход ведения боевых действий;

– системы кибербезопасности, представленные защитными моделями от кибератак и способностями киберразведки.

Помимо перечисленных направлений, большими перспективами в военном деле обладают цифровые двойники. Цифровые двойники – виртуальные модели реальных объектов и систем – становятся ключевым инструментом для повышения эффективности, безопасности и боеспособности вооруженных сил.

Стоит отметить, что цифровой двойник – это не просто 3D-модель, а полная виртуальная реконструкция, которая включает в себя:

– физические характеристики объекта: масса, материалы изготовления, свойства;

– функциональные возможности, представленные типами и видами датчиков, возможностями связи, новыми системами вооружений;

– моделирование поведения, включающее в себя модели движения, взаимодействие с окружающей средой, динамику;

– работу с данными, включающими обработку больших цифровых массивов [1].

Современная научная мысль достаточно часто касается вопросов применения цифровых двойников в военном производстве. В работе [2] предлагается методический подход для оценки эффективности работы оборонно-промышленного комплекса в рамках внедрения цифровизации, что позволяет предопределить необходимые внутренние корректировки с целью достижения поставленных задач.

В статье [3] изучена цифровая трансформация процессов, проистекающих на промышленном производстве в результате внедрения цифровых двойников. Проведенный анализ выявил необходимость развития инструментов, методов и организации производственного процесса для проведения цифровой трансформации промышленного производства военного назначения. Среди перспектив развития рассматриваются также методы блокчейн-онтологии и смарт-контрактов.

Авторами работы [4] изучены вопросы диверсификации военного производства с учетом рисков невыполнения заказов и недостаточности финансового обеспечения. В качестве решения предложено использование цифровых двойников на различных этапах жизненного цикла с прогнозированием финансовой устойчивости на каждой стадии, с целью нивелирования риска финансовой нестабильности предприятия военного производства.

Таким образом, практика применения цифровых двойников в современном военном производстве является актуальной задачей, находящей свое отражение в трудах различных авторов.

Создание цифровых двойников является сложной задачей, поскольку необходимо переносить на цифровой носитель не только данные о процессе производства, но и модели, описывающие процесс динамичного развития. Строго говоря, процесс создания цифровых двойников представляет собой поэтапный ввод различных характеристик военного производства, а затем их взаимную интеграцию в единое целое, с возможностями дальнейшей обработки данных в отрыве от реального производства.

Среди моделей, вносимых в цифровой двойник можно выделить:

– организационную модель – описывающую взаимодействие межу отделами, определяющую иерархию взаимоподчинения и распределения задач на конкретные рабочие группы;

– структурную модель, определяющую состав, структуру и ключевые характеристики промышленных объектов, обеспечивающих работу военного производственного комплекса;

– функциональную модель, определяющую необходимые к выполнению функции, а также те отделы и цеха, где они должны быть реализованы;

– модель данных, характеризующую распределение потока информации необходимой для обеспечения работы предприятий военного производства;

– модель управления, обеспечивающую строгое распределение целей и задач по подразделениям, отелам и цехам, сбор обратной связи, анализ и итоговое принятие управленческих решений для повышения эффективности работы предприятий военного производства.

Совокупное взаимодействие перечисленных моделей отображено на рисунке 1.

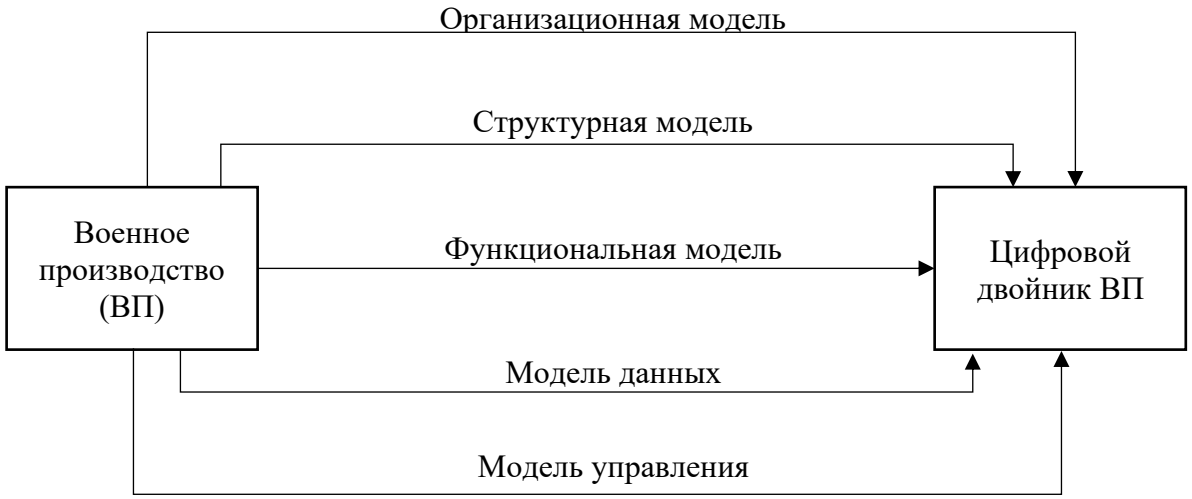


Рисунок 1 – Модели, формирующие цифровой двойник

Интеграция представленных моделей позволяет разработать цифровой двойник, способный не только характеризовать процесс военного производства, но и осуществлять прогнозирование развитие производственного процесса в будущем [5].

Среди преимуществ, которыми обладают цифровые двойники, можно выделить следующие:

– улучшение планирования за счет создания сценариев и моделирование военного производства;

– оптимизация эксплуатации, достигаемой за счет прогнозирования технического состояния, предупреждения о потенциальных отказах, снижения затрат на техническое обслуживание;

– создание эффективного обучения, за счет осуществления симуляции реальных производственных ситуаций, повышение навыков работы с оборудованием;

– модификация проектных работ, за счет моделирования новых систем вооружения и техники, оптимизации конструкции и характеристик.

Таким образом, несмотря на трудности, цифровые двойники имеют огромный потенциал для повышения эффективности и боеспособности вооруженных сил. Обзор литературы показывает как концепция цифровых двойников развивается, так и ее применение расширяется в различных областях. В будущем можно ожидать их широкого применения в различных военных задачах, от стратегического планирования до решения тактических и оперативных производственных задач.

Список литературы

1 Архапчева, М. В. Инфологическое моделирование базы данных для организации / М. В. Архапчева, В. А. Трипкош, С. С. Акимов // Вызовы современности и стратегии развития общества в условиях новой реальности : сборник материалов XX Международной научно-практической конференции, Москва, 10 октября 2023 года. – Москва: Алеф, 2023. – С. 259-262.

2 Кохно, П. А. Методический подход к оценке цифровых технологий в оборонной промышленности / П. А. Кохно // Социально-экономические и технические проблемы оборонно-промышленного комплекса России: история, реальность, инновации : Сборник статей по материалам IX Всероссийской научно-практической конференции, Арзамас, 11–12 апреля 2023 года. – Нижний Новгород: Нижегородский государственный технический университет им. Р.Е. Алексеева, 2023. – С. 53-59.

3 Гарина, И. О. методический подход к внедрению технологий агрегированных цифровых двойников в процессы производства машин арктического назначения / И. О. Гарина // Современные наукоемкие технологии. – 2021. – № 9. – С. 47-55.

4 Андреев, Д. А. Разработка организационных способов снижения накладных расходов на предприятиях ОПК / Д. А. Андреев, М. М. С. Абуева, А. А. Островская // Горизонты экономики. – 2022. – № 6(72). – С. 110-118.

5 Акимов, С. С. Разработка цифрового двойника биотехнической системы / С. С. Акимов, А. С. Боровский // Научно-технический вестник Поволжья. – 2024. – № 5. – С. 78-81.

ПЕРСПЕКТИВЫ И ЭФФЕКТИВНОСТЬ ПРИМЕНЕНИЯ БПЛА В ГРАЖДАНСКОЙ БЕЗОПАСНОСТИ

Богодухова А.С., Боровский А.С., доктор технических наук, профессор
Федеральное государственное бюджетное образовательное учреждение высшего образования «Оренбургский государственный университет», г. Оренбург

Аннотация. В статье исследуются актуальные области применения БПЛА, такие как поисково-спасательные операции, мониторинг чрезвычайных ситуаций, охрана объектов и границ, а также их сравнительная эффективность по сравнению с традиционными методами. Особое внимание уделяется ключевым преимуществам использования БПЛА, включая скорость, доступность, сбор данных в реальном времени и минимизацию рисков для персонала. В заключительной части статьи рассматриваются перспективы дальнейшего развития технологий БПЛА и их потенциал для укрепления систем гражданской безопасности.

Ключевые слова: беспилотные летательные аппараты, БПЛА, дроны, гражданская безопасность, чрезвычайные ситуации, спасательные операции, охрана границ, мониторинг, эффективность, перспективы, технологии, безопасность.

Современный мир сталкивается с множеством вызовов, требующих оперативного и эффективного реагирования. Природные катаклизмы, техногенные аварии, террористические угрозы и необходимость контроля над обширными территориями ставят перед службами гражданской безопасности сложные задачи. Традиционные методы реагирования, несмотря на свою значимость, часто оказываются недостаточно быстрыми, дорогостоящими или сопряженными с высоким риском для жизни и здоровья задействованного персонала. В этом контексте беспилотные летательные аппараты (БПЛА), также известные как дроны, становятся все более востребованным инструментом, демонстрируя выдающуюся эффективность и открывая новые перспективы для обеспечения гражданской безопасности [1].

БПЛА представляют собой летательные аппараты, управляемые дистанционно или действующие в автономном режиме. Их развитие за последние десятилетия было стремительным: от простых игрушек до сложных многофункциональных платформ, оснащенных передовыми сенсорами, камерами высокого разрешения, тепловизорами, лидарами и другими технологиями. Технологический прогретив позволил дронам совершить настоящий прорыв: из узкоспециализированного военного инструмента они превратились в универсальных помощников для решения множества

гражданских задач. Беспилотные системы становятся инструментом в сфере экологического контроля и природоохранной деятельности. Они обеспечивают оперативное отслеживание состояния лесных массивов, раннее обнаружение очагов возгорания, мониторинг загрязнения водных объектов и воздушного бассейна с беспрецедентной точностью и регулярностью. В строительной индустрии БПЛА применяют для высокоточных трехмерных моделей местности, непрерывного мониторинга хода строительных работ и инспектирования технического состояния объектов инфраструктуры. Данные технологии помогают кардинально оптимизировать временные и финансовые затраты.

Важно и то, что дроны берут на себя самый первоначальный, самый опасный риск. Они первыми отправляются в эпицентр катастрофы, чтобы передать картину происходящего, не подвергая опасности жизни спасателей. А в ситуациях, когда традиционные пути разрушены, даже небольшой дрон может стать единственной нитью, связывающей пострадавших с помощью, оперативно доставив в изолированный район аптечку или спутниковый телефон [2].

Дроны стали надежным инструментом для инспекции критически важных объектов — мостов, дамб, промышленных зон. Они помогают выявить малейшие дефекты и потенциальные угрозы до того, как те приведут к серьезной аварии. Эта же оперативность незаменима при ликвидации чрезвычайных ситуаций: дроны первыми прибывают на место разлива нефти или химикатов, чтобы точно оценить масштабы бедствия и направить усилия спасателей в нужное русло.

В сфере охраны дроны совершили настоящую революцию. Они патрулируют огромные территории − от периметра заводов до площадок массовых − делая это быстрее и дешевле, чем наземные группы. Современные системы наблюдения на их борту способны автоматически распознавать попытки проникновения, действуя как неутомимый часовой с идеальным зрением. Во время городских праздников, матчей или концертов дрон, зависший в небе, становится центральным звеном в системе безопасности: его обзор позволяет координировать действия служб, мгновенно обнаруживать давку или конфликт и предотвращать эскалацию еще до того, как ситуация выйдет из-под контроля.

Эффективность применения беспилотных летательных аппаратов (БПЛА) в сфере гражданской безопасности детерминирована рядом системообразующих факторов. Первостепенным критерием выступает временной показатель реагирования: беспилотные платформы обладают способностью к практически моментальному развертыванию и передаче данных в режиме, приближенном к реальному времени. Данная характеристика обеспечивает значительное сокращение временного интервала, необходимого службам безопасности для

принятия оперативных решений, по сравнению с традиционными методами наблюдения и разведки.

Существенным аспектом является экономическая составляющая эксплуатации БПЛА. Несмотря на наличие первоначальных капиталовложений, совокупная стоимость владения беспилотными комплексами в долгосрочной перспективе оказывается существенно ниже, чем содержание аналогичных по функционалу человеко-машинных систем или авиационной техники пилотируемого типа. Снижение эксплуатационных расходов достигается за счет минимальных затрат на энергоносители, техническое обслуживание и фонд оплаты труда.

Ключевым преимуществом является минимизация рисков для личного состава оперативных служб. Использование БПЛА позволяет исключить или значительно ограничить присутствие человека в зонах повышенной опасности, к которым относятся районы стихийных бедствий, техногенных катастроф, химического или радиационного заражения, а также локации с высокой вероятностью противоправных действий [3].

Дополнительным оперативно-тактическим преимуществом выступает способность беспилотных платформ осуществлять мониторинг и сбор данных в труднодоступных для наземной техники и человека районах: на пересеченной местности, в условиях плотной городской застройки, на разрушенных объектах инфраструктуры и в иных условиях, характеризующихся повышенным уровнем опасности или физической непроходимостью.

Перспективы развития беспилотных авиационных систем в сфере гражданской безопасности определяются поступательной эволюцией ключевых технологических направлений. Совершенствование алгоритмов искусственного интеллекта и машинного обучения создает предпосылки для реализации полностью автономных операций, включая сложное целеполагание и адаптацию к динамически изменяющимся условиям окружающей среды.

Параллельно наблюдается развитие сетевой интеграции беспилотных платформ в единые информационно-управляющие системы, обеспечивающие их взаимодействие с другими сенсорными комплексами и центрами обработки данных. Значимый прогресс ожидается в области энергетической эффективности, где разработка новых источников питания и двигательных установок направлена на увеличение продолжительности полета и грузоподъемности беспилотников.

Эволюция сенсорных технологий позволит осуществлять мониторинг расширенного спектра угроз, включая химическое и биологическое заражение, а развитие технологий группового взаимодействия откроет возможности координации гетерогенных групп БПЛА для решения масштабных оперативных

задач. Одновременно с техническим развитием происходит адаптация нормативно-правовой базы, направленная на обеспечение безопасной интеграции беспилотных систем в общее воздушное пространство и стандартизацию протоколов обмена данными.

Дальнейшая применение беспилотных авиационных систем представляется необходимым условием формирования устойчивого и защищенного общества, способного эффективно противостоять вызовам современности. Технологическая конвергенция перечисленных направлений создает предпосылки для качественного преобразования всей системы гражданской безопасности.

Список литературы

1. Ведерников, Ю. В. Основы теории структурной оптимизации систем контроля и управления беспилотными летательными аппаратами : учебное пособие / Ю. В. Ведерников. – 2-е изд. – Санкт-Петербург : Политехника, 2022. – 367 с.
2. Молоденков С.А., Пашкин М.С. Анализ современных беспилотных летательных аппаратов // Современные научные исследования и инновации. 2023. № 9 [Электронный ресурс]. URL: https://web.snauka.ru/issues/2023/09/100804 (дата обращения: 09.09.2025).
3. Павлов, Н. С. Применение беспилотных летательных аппаратов (БПЛА) в правоохранительных органах России / Н. С. Павлов, В. К. Тарыкин // Вестник науки. – 2024. – Т. 1, № 12 (81). – С. 1764 - 1770 – URL: https://cyberleninka.ru/article/n/primenenie-bespilotnyh-letatelnyh-apparatov-bpla-v-pravoohranitelnyh-organah-rossii (дата обращения: 10.09.2025).

ПРОЕКТИРОВАНИЕ И 3D МОДЕЛИРОВАНИЕ ТЕХНИЧЕСКИХ СРЕДСТВ ВОЕННОГО НАЗНАЧЕНИЯ

Виноградов К.А.,Акимов С.С., кандидат технических наук
Федеральное государственное бюджетное образовательное учреждение высшего образования «Оренбургский государственный университет»

Аннотация: в статье рассматриваются ключевые аспекты проектирования и 3D моделирования технических средств военного назначения. Описаны методы разработки виртуальных прототипов, использование современных программных средств для создания трехмерных моделей и их дальнейшую оптимизацию для испытаний и производства. Особое внимание уделяется вопросам повышения точности моделирования, эффективности проектных решений и интеграции 3D моделей в инженерные процессы для повышения надежности и боеспособности вооружения и военной техники.

Ключевые слова: проектирование, 3D моделирование, технические средства военного назначения, виртуальные прототипы, инженерное моделирование.

В современном мире безопасность и обороноспособность государства напрямую зависят от эффективности разработки и использования новых технических средств. Одним из ключевых направлений развития военной техники является использование передовых технологий проектирования и моделирования – в частности, 3D моделирования. Эти технологии позволяют создавать точные виртуальные модели боеприпасов и других элементов вооружения, что существенно ускоряет процессы разработки, тестирования и внедрения новых образцов, а также повышает их качество и безопасность.

Внедрение технологий 3D-моделирования и компьютерного инжиниринга предоставляет специалистам мощный инструментарий для сквозного проектирования. Оно позволяет проводить комплексную цифровую визуализацию, инженерный анализ и оптимизацию конструкций в условиях, максимально приближенных к реальным, полностью отказавшись от этапа изготовления полноценных физических прототипов [1].

Применительно к сфере высокоточных боеприпасов и взрывателей данная методология приобретает ключевое значение. Каждый компонент, будь то деталь силового механизма, элемент корпуса или узел системы наведения, должен быть верифицирован с помощью компьютерного расчета на прочность, динамику и термостойкость. Это гарантирует высочайший уровень надежности, безопасности и строгое соответствие изделия всем техническим регламентам.

Моделирование в виртуальной среде предоставляет возможность тестировать поведение изделий под различными условиями – вибрацией,

ударом, температурными режимами и др. Это значительно снижает затраты на производство опытных образцов и минимизирует риски ошибок при изготовлении настоящих боеприпасов [2]. Кроме того, современные программы позволяют вносить изменения и сразу видеть их влияние, что ускоряет цикл проектирования.

На рисунке 1 приведен процесс моделирования головной втулки взрывателя КТМ-2.

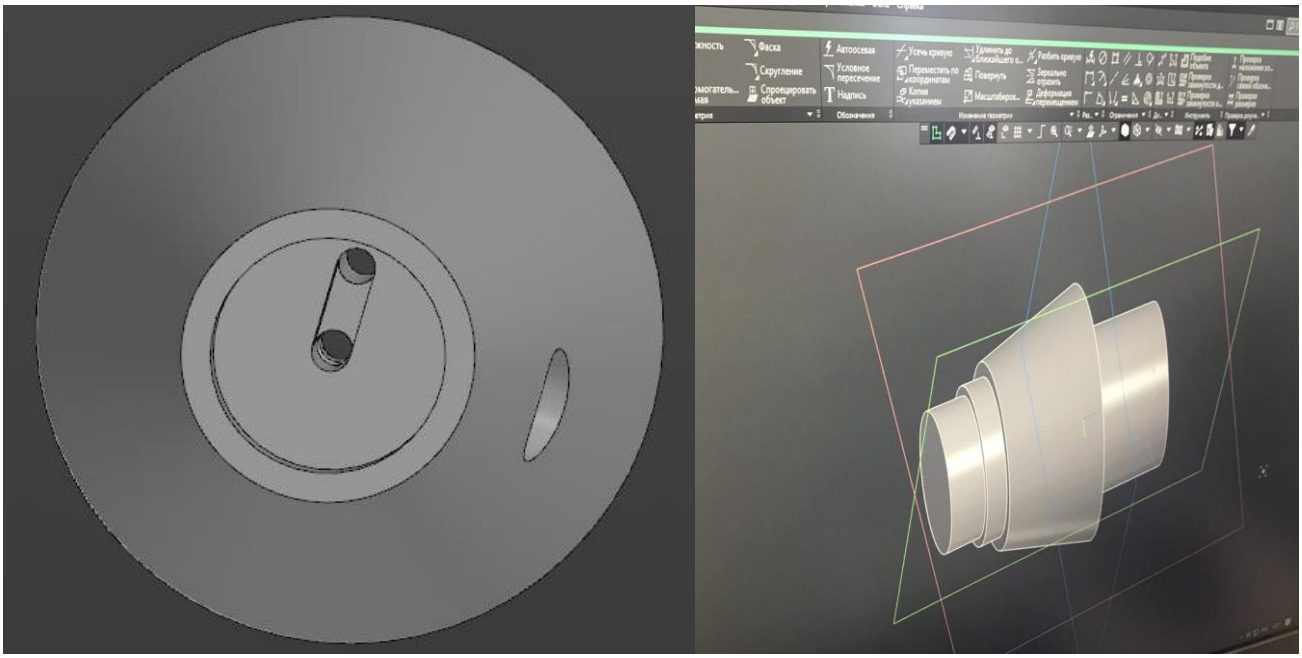


Рисунок 1 – Процесс моделирования головной втулки взрывателя КТМ-2

После завершения этапа моделирования производится его печать на 3D принтере. Это дает возможность создания физических прототипов, которые можно использовать для механических, тактильных и визуальных исследований. Быстрая печать моделей повышает мобильность и гибкость исследований, позволяет инженерам оперативно выявлять недостатки и вносить коррективы [3]. Особенно актуально это в условиях военного производства, где требуется часто обновлять модели или создавать индивидуальные решения.

Главное преимущество этого подхода в его исключительной оперативности и гибкости. Скорость, с которой цифровой проект превращается в физический образец, кардинально повышает мобильность всего исследовательского цикла. Это позволяет практически в режиме реального времени выявлять конструктивные недочеты и оперативно, с минимальными временными и финансовыми затратами, вносить необходимые коррективы в цифровую модель для последующей печати улучшенной версии [4].

3D печать также важна для изготовления мелких деталей, которые сложно или дорого производить обычными методами. Использование аддитивных технологий существенно сокращает сроки изготовления, снижает издержки и позволяет поддерживать высокий уровень точности для сложных форм и геометрий. В результате, полученные модели можно использовать не только для презентаций или учебных целей, но и для практических испытаний и демонстраций в боевых условиях.

На рисунок 2 показана головная втулка взрывателя КТМ-2 и его модель, выполненная на 3D-принтере.

Рисунок 2 – Головная втулка взрывателя КТМ-2 и его модель, выполненная на 3D-принтере

Продвижение технологий 3D моделирования и печати в военной сфере открывает новые возможности для разработки высокоточных, легких и надежных систем вооружения. Однако, одновременно с этим возникают и задачи по обеспечению кибербезопасности, защиты авторских прав и предотвращению утечек секретных данных. Также важно совершенствовать материалы для 3D печати, чтобы обеспечить их соответствие требованиям военного применения в части прочности и устойчивости к воздействию окружающей среды.

Стремительное развитие этих технологий одновременно порождает комплекс серьезных вызовов, которые требуют незамедлительного решения. Цифровая природа проектов превращает файлы моделей в уязвимые активы,

выдвигая на первый план острую необходимость в создании максимально защищенных экосистем для их хранения и передачи [5].

Таким образом, проектирование и 3D моделирование технических средств военного назначения – это современные инструменты, гарантирующие высокоточные, быстрые и экономичные разработки. Использование технологий виртуализации и аддитивного производства позволяет повысить уровень безопасности и эффективности вооруженных сил. В дальнейшем интеграция этих решений станет неотъемлемой частью развития современной военной промышленности.

Список литературы

8 Шулья, Д. В. Использование 3D-моделирования в военной сфере / Д. В. Шулья // Новые информационные технологии в телекоммуникациях и почтовой связи. – 2024. – № 1. – С. 221-222.

9 Акимов, С. С. Расчет вероятности дискретности для массива данных / С. С. Акимов // Научное обозрение. – 2013. – № 6. – С. 78-83.

10 Копосов, А. А. 3D технологии в военной сфере: особенности применения в развитии беспилотной авиации / А. А. Копосов, Т. В. Широкоград // ДОСТИЖЕНИЯ в НАУКЕ и ОБРАЗОВАНИИ 2024 : сборник статей Международного научно-исследовательского конкурса, Пенза, 05 июня 2024 года. – Пенза: Наука и Просвещение (ИП Гуляев Г.Ю.), 2024. – С. 345-348.

11 Трипкош, В. А. Алгоритмы принятия решений для комбинированных систем автоматического распознавания образов / В. А. Трипкош, С. С. Акимов // Университетский комплекс как региональный центр образования, науки и культуры : Материалы Всероссийской научно-методической конференции (с международным участием), Оренбург, 23–25 января 2020 года. – Оренбург: Оренбургский государственный университет, 2020. – С. 741-745.

5. Ульянова Т.С. Способ определения измерительной сложности приборов и устройств для построения информационно-измерительной системы / Т. С. Ульянова, С. С. Акимов //Автоматизация. Современные технологии. – 2023. – Т. 77, № 11. – С. 523-527.

ВОЕННАЯ НАУКА КАК ОСНОВА РАЗВИТИЯ ОБОРОННО-ПРОМЫШЛЕННОГО КОМПЛЕКСА

Вязьмин А.Г.
Федеральное государственное бюджетное образовательное учреждение высшего образования «Оренбургский государственный университет», г. Оренбург

Аннотация: Государство для защиты своих национальных интересов и укрепления обороноспособности вынуждено выделять часть интеллектуальных, организационно-управленческих, экономических, финансовых, социальных и иных ресурсов на военно-техническое развитие, на оснащение национальных Вооруженных Сил современными и перспективными системами и комплексами вооружений и военной техники. В результате формируется оборонно-промышленный комплекс страны.

Ключевые слова: военная наука, национальная безопасность, обороноспособность, перспективные технологии, разработка и модернизация образцов вооружения, диверсифицированность.

Наука о войне – это фундамент, на котором строится безопасность страны, восстанавливается роль науки и повышается её престиж в обществе.

Развитие теории оружия и военной техники, как части военной науки, требует улучшения продукции оборонно-промышленного комплекса. А если грамотно подойти к диверсификации, можно значительно увеличить потребность в отечественных товарах и услугах.

Это требует переосмысления роли и значимости военной науки в обеспечении национальной безопасности страны, особенно при разработке рациональной и эффективной военно-технической политики.

Для обороны страны важны результаты военной науки – конструкторские и технологические достижения, а также результаты интеллектуальной деятельности военного и двойного назначения.

В связи с этим, главные цели военной науки в обеспечении обороноспособности страны: подготовить проект оптимальной военно-технической политики на будущее, которая будет адекватно отвечать на вызовы и угрозы военной безопасности при финансовых и других ограничениях; поддерживать научно-технологический уровень развития вооружения и военной техники, чтобы гарантировать их эффективное и надёжное функционирование в мирное и военное время.

Среди основных задач военной науки можно выделить: прогноз развития вооружения и военной техники на перспективу; комплексный анализ и оценка научно-технических и производственно-технологических возможностей оборонно-промышленного комплекса и других структур, занимающихся

разработкой и производством вооружения и военной техники; подготовка проектов документов долгосрочного программно-целевого планирования развития вооружения и военной техники; обоснование и подготовка проекта перечня необходимых научно-исследовательских и опытно-конструкторских работ, обеспечивающих сбалансированное и асимметричное развитие системы вооружения Вооружённых Сил, других войск и воинских формирований.

Для военной науки ключевым моментом является достижение научно-технологической безопасности. Это означает, что необходимо обеспечить независимость от иностранных государств в создании и использовании перспективных технологий и комплектующих при разработке и модернизации образцов вооружения и военной техники.

Единое государственное управление военной наукой и межведомственная координация работ по её развитию. Приоритетность – сосредоточение усилий на военно-техническом обеспечении первостепенных задач строительства вооружённых сил и других войск и воинских формирований. Адекватное противодействие современным и перспективным системам вооружений с учётом их жизненного цикла. Сбалансированность между задачами, возлагаемыми на военную науку, и финансово-экономическими возможностями страны. Гибкость и способность к корректировке плановых заданий на разработку и модернизацию образцов вооружения и военной техники. Программно-целевое планирование развития образцов, комплексов и систем вооружения и военной техники. Реализуемость разработок вооружения и военной техники на основе обеспечения научно-технического и производственно-технологического потенциала предприятий оборонно-промышленного комплекса. Преемственность – разработка новых образцов вооружения и военной техники с учётом накопленного опыта создания вооружения. Военно-экономическая эффективность – оптимальное соответствие создаваемого вооружения и военной техники задачам, структуре и составу вооружённых сил. Системное обоснование и целенаправленное наращивание научно-технического задела для создания образцов вооружения и военной техники последующих поколений. Обеспечение адаптивности мобилизационной базы оборонно-промышленного комплекса к изменениям военно-политических и экономических условий. Соответствие требованиям научно-технической безопасности и сохранения окружающей среды в части обеспечения различных видов безопасности.

Диверсифицированность – рациональное использование научно-технического потенциала военной науки и производственно-технологического потенциала предприятий оборонно-промышленного комплекса при создании образцов вооружения и военной техники.

Эти принципы должны стать основой для дальнейшего развития вооружения и военной техники в Российской Федерации. Они позволят разработать взаимоувязанную систему требований к уровню развития систем, комплексов и образцов вооружения и военной техники на долгосрочный период.

При подготовке проекта основных направлений развития вооружения и военной техники необходимо выполнить большой объём работ, основанных на результатах исследований, проведённых или систематизированных военной наукой. В частности, необходимо: проанализировать условия и факторы, а также тенденции развития военных технологий и технологий двойного назначения в РФ и за рубежом. Оценить возможности выполнения задач группировками войск (сил) в вероятных военных конфликтах при различных вариантах их технического оснащения. Сформировать ведущие и второстепенные тенденции развития вооружения и военной техники на прогнозируемый период. Обосновать тактико-технические требования к перспективному вооружению, удовлетворяющему потребностям вооружённых сил и других силовых структур с учётом долгосрочной перспективы.

Учитывая эти принципы, необходимо уделять больше внимания планированию развития военной науки, так как это влияет на разработку новых современных образцов вооружения и военной техники в долгосрочной перспективе.

На данный момент недостаточное внимание к значимости науки в области военного искусства и военных технологий приводит к тому, что военная наука сводится к минимуму, который не позволяет не только создавать военные технологии, но и проводить эксперименты для проведения поисковых исследований.

Для того чтобы военная наука развивалась и играла более значимую роль в укреплении научного потенциала России, необходимо решить важную задачу – подготовить новые кадры. Эти специалисты, которые будут стремиться к получению знаний в области военного дела и технологий, станут движущей силой российской науки и будут способствовать её успеху в технологической сфере. Ведь именно оборонная промышленность всегда была движущей силой научных достижений развитых стран.

Поэтому необходимо увеличить количество талантливых и заинтересованных учёных, которые занимаются фундаментальными, прогнозирующими и прикладными исследованиями в научно-исследовательских организациях. Это позволит ускорить достижение приемлемого уровня развития базовых военных и промышленных технологий. Также важно расширять спектр исследований и разработок, чтобы создать научно-технический задел по всем перспективным направлениям.

Таким образом, создание конкурентной среды в области разработки вооружения и военной техники на предприятиях и в научно-исследовательских организациях оборонно-промышленного комплекса может повысить мотивацию и эффективность разрабатываемых образцов. А обеспечение вооружённых сил, других войск и воинских формирований материальными ресурсами, техникой и вооружением будет способствовать созданию взаимосвязанной системы развития военной науки и научно-технического задела для разработки новых образцов вооружения и военной техники.

Список литературы

1. Военная экономика: учеб. пособие/В. Г. Ольшевский,А. Н. Леонович, А. П. Хлебоказов [и др];под общ. ред. В.Г.Ольшевского.-Минск:ВА РБ, 2011.

2. Военно-экономическое обеспечение национальной безопасности России в много-полярном мире. Рук. Проекта -Р.А. Фарамазян.М. :ИМЭ-МО РАН,2009.

3. Государственная программа вооружения России на период 2011-2020 годов: комментарии/ А.Фролов. - Режим доступа: http://periscope2.ru/pdf/100628-frolov.pdf. - 27.11.2014.

4. Государственный оборонный заказ России: статья/А. Фролов. - Режим доступа: ://vpk.name/news/47577_gosudarstvennyii_oboronnyii_zakaz_rossii.html.- 27.11.2014. Горностаев, Г.А. Внешние военно-экономические связи России: проблемы развития и пути их решения. М.:ВНИ-ИВС, 2000.

5. Итоги размещения ГОЗ-2013 по номенклатуре Минобороны России: оффициальный сайт Рособоронпостави/ О.В.Князева. - Режим доступа: http://rosoboronpostavka.ru/osnovnye%20itogi%20razmesheniya%20goz%202013.php.-27.11.2014.

6. Кузык, Б.Н. Экономика военной сферы, Учебник. - М., МГФ: «Знание», 2006.

СИСТЕМНЫЙ АНАЛИЗ КАК МЕТОДОЛОГИЯ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ ВООРУЖЕНИЯ И ВОЕННОЙ ТЕХНИКИ: СОВРЕМЕННЫЕ ПОДХОДЫ И ПЕРСПЕКТИВЫ РАЗРАБОТКИ

Голуб А.А., Ульянова Т.С.
Федеральное государственное бюджетное образовательное учреждение высшего образования «Оренбургский государственный университет»

Аннотация: в данной статье исследуются современные методологические подходы к обеспечению безопасности вооружения и военной техники с позиций системного анализа. Рассмотрены ключевые принципы, методы и инструменты анализа безопасности сложных технических систем на всех этапах их жизненного цикла. Особое внимание уделено применению цифровых технологий (цифровых двойников, искусственного интеллекта, обработки больших данных) в системном анализе безопасности. Определены перспективные направления развития методологии, связанные с конвергентными и когнитивными технологиями.

Ключевые слова: системный анализ, безопасность вооружения, цифровые двойники, искусственный интеллект, когнитивные технологии, обработка больших данных, жизненный цикл военной техники, моделирование безопасности.

Современные системы вооружения и военной техники представляют собой сложные технические комплексы, функционирование которых требует комплексного подхода к обеспечению безопасности. Новые образцы вооружения и военной техники представляют собой интегрированные многоуровневые технические комплексы, включающие аппаратные, программные и организационные подсистемы и характеризующиеся высокой плотностью связей и динамическим поведением. Изучение их безопасности эффективно лишь при системном подходе: системный анализ обеспечивает формализацию структуры системы, моделирование взаимодействий между компонентами, выявление критических точек уязвимости и количественную оценку рисков. В результате он позволяет обосновывать проектные решения по снижению рисков на всех стадиях жизненного цикла – от эскизного проекта до утилизации. В данном контексте системный анализ выступает ключевой методологией, позволяющей исследовать и оптимизировать системы безопасности как на этапе проектирования, так и в процессе эксплуатации. Методологическая основа системного анализа безопасности включает несколько ключевых аспектов.

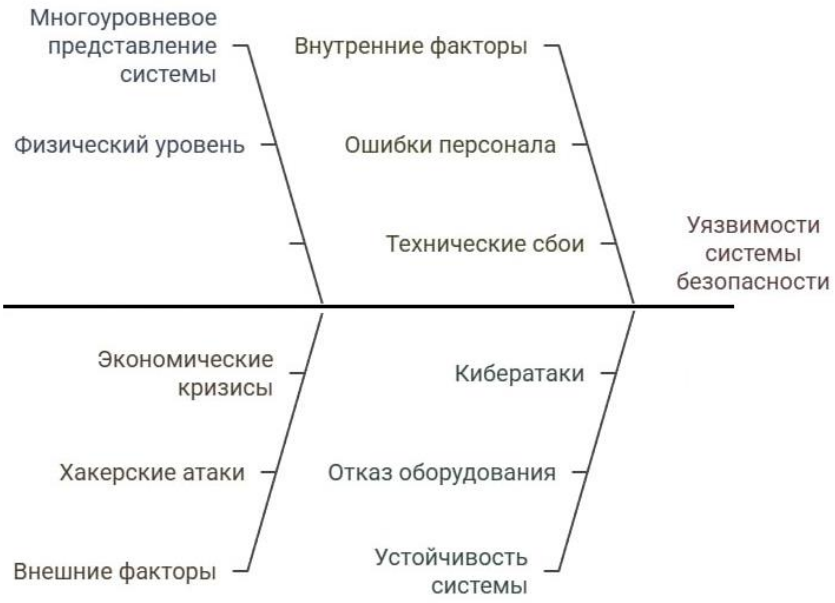


Рисунок 1 – Анализ рисков и угроз в системе безопасности

Методический аппарат системного анализа безопасности можно охарактеризовать как совокупность трёх направлений. Первое направление связано со структурно-качественными методами, в числе которых функционально-стоимостной анализ, декомпозиция функций, метод анализа иерархий, построение диаграмм влияния и моделирование на языке SysML. Второе направление охватывает математические и вычислительные методы, такие как теория надёжности и отказоустойчивости, вероятностный анализ, методы FTA и FMEA, стохастическое моделирование, теория катастроф, имитационные эксперименты и системная динамика. Третье направление относится к когнитивным и социотехническим методам и включает анализ надёжности деятельности оператора, когнитивный анализ задач, моделирование человеко-машинных интерфейсов и оценку ситуационной осведомлённости. Эти три группы применяются итеративно: структурный разбор и формализация требований дополняются количественными методами, а когнитивные аспекты учитываются параллельно для интеграции человеческого фактора. Особое значение имеют когнитивные технологии, позволяющие моделировать человеко-машинные интерфейсы, анализировать факторы человеческой ошибки и прогнозировать поведение оператора в критических ситуациях.

Применение системного анализа охватывает все этапы жизненного цикла вооружения и военной техники.

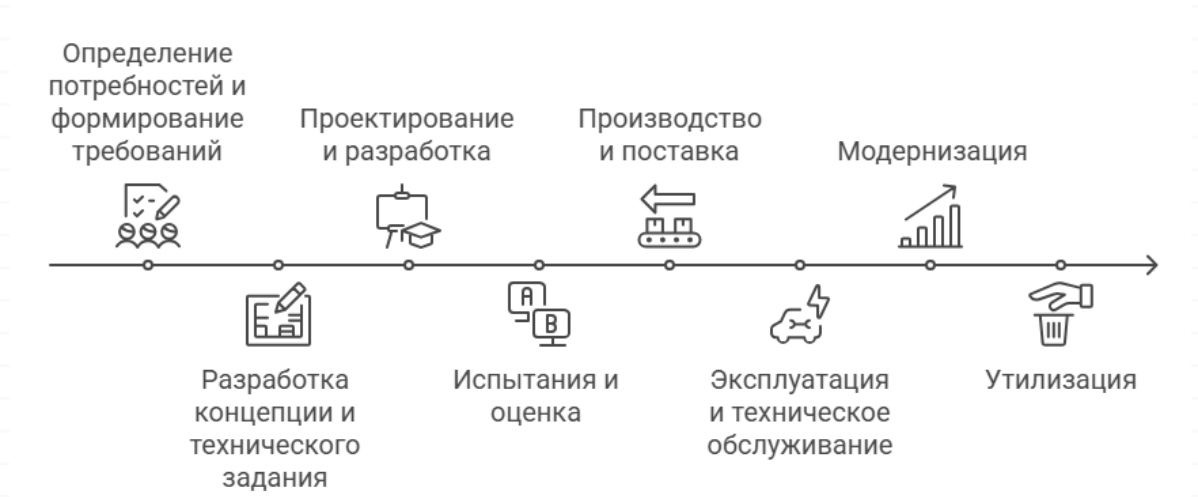


Рисунок 2 – Этапы жизненного цикла вооружения и военной техники

Системный анализ безопасности охватывает все стадии жизненного цикла вооружения и военной техники. Безопасность системы формируется на протяжении всего её жизненного цикла, начиная с этапа концепции и определения требований, когда осуществляется идентификация потенциальных угроз и формулирование базовых требований к защищённости. На стадиях предпроектного анализа и эскизного проектирования проводится оценка уязвимостей для различных архитектурных решений и моделирование сценариев отказов (FMEA). В процессе проектирования разрабатывается архитектура системы, оптимизированная по критериям безопасности, и определяются конкретные механизмы и меры защиты. Этап разработки и верификации, организованный в соответствии с V-моделью, включает тестирование и валидацию соответствия системы всем заявленным требованиям безопасности.

Ввод в эксплуатацию и последующее сопровождение предусматривают непрерывный мониторинг метрик безопасности, прогнозирование остаточного ресурса защитных механизмов и использование цифрового двойника для уточнения и калибровки моделей. Любая последующая модернизация требует проведения оценки воздействия на безопасность (Impact Analysis) и управления возникающими сопутствующими рисками.

На завершающей стадии, утилизации, уделяется внимание анализу опасностей, связанных с демонтажом, и обеспечению сохранности конфиденциальной информации на протяжении всего процесса.На этапе проектирования он позволяет оценивать уязвимости на стадии технического предложения, оптимизировать архитектуру системы по критериям безопасности и формировать требования к системе защиты.

В процессе эксплуатации системный анализ используется для мониторинга деградационных процессов, прогнозирования остаточного ресурса безопасности и анализа данных телеметрии. При модернизации военной техники методы системного анализа помогают оценивать эффективность предлагаемых усовершенствований, балансировать характеристики системы и минимизировать риски при внедрении изменений.

Современный этап развития системного анализа безопасности характеризуется активным внедрением информационных технологий. Особое значение приобретают средства моделирования, включающие программные комплексы для многофизического моделирования (ANSYS, COMSOL), средства виртуального прототипирования и цифровые двойники критических систем [1].

Цифровые технологии радикально расширяют возможности системного анализа безопасности. Цифровые двойники обеспечивают непрерывную синхронизацию виртуальной модели и реального объекта, что позволяет выполнять предиктивную аналитику, раннее обнаружение деградации и оптимизацию технического обслуживания. Методы обработки больших данных и машинного обучения дают возможность выявлять скрытые закономерности в телеметрии и строить адаптивные системы поддержки принятия решений. Когнитивные технологии и объяснимый искусственный интеллект способствуют интерпретации прогнозов и обоснованному выбору мер реагирования. При этом требуется учитывать риски, связанные с кибербезопасностью и целостностью данных цифровых моделей.

Методы обработки больших данных позволяют анализировать временные ряды параметров работы, выявлять скрытые зависимость и аномалии, а также реализовывать предиктивную аналитику отказов. Интеллектуальные системы поддержки решений, включающие экспертные системы диагностики, нейросетевые алгоритмы распознавания угроз и адаптивные системы управления рисками, становятся неотъемлемой частью современной методологии обеспечения безопасности. Перспективные направления развития системного анализа безопасности связаны с конвергентными технологиями, включающими системы безопасности на основе квантовых вычислений, бионические подходы к защите критически важных узлов и нанотехнологии в создании защитных систем [2]. Особый интерес представляют когнитивные системы нового поколения с самообучающимися алгоритмами анализа угроз, элементами искусственного сознания и адаптивными интерфейсами «человек-машина».

В заключении следует подчеркнуть, что системный анализ как методологическая основа обеспечения безопасности вооружения и военной техники продолжает динамично развиваться, интегрируя достижения цифровых

технологий и искусственного интеллекта. Для специалистов в области системного анализа и управления особую важность приобретает освоение междисциплинарных методов анализа, современных инструментов моделирования, подходов к обработке больших массивов данных и инновационных решений в области когнитивных технологий.

Эти компетенции становятся критически важными для эффективного решения сложных задач обеспечения безопасности современных и перспективных образцов вооружения в условиях цифровой трансформации оборонно-промышленного комплекса. Развитие методологии системного анализа безопасности требует продолжения исследований в области интеграции искусственного интеллекта, квантовых вычислений и нейрокогнитивных технологий, что открывает новые перспективы для создания принципиально новых систем защиты вооружения и военной техники.

Список литературы

1 Иванов А.В. Цифровые двойники в военной технике / А.В. Иванов. – М.: Воениздат, 2022.

2 Петрова С.И. Искусственный интеллект для систем безопасности / С.И. Петрова. – СПб.: Политехника, 2023.

3 ГОСТ Р 56734-2021 «Цифровое моделирование сложных технических систем».

4 Разумов, О.С. Системные знания: концепция, методология, практика / О. С. Разумов, В. А. Благодатских. – М. : Финансы и статистика, 2006. – 400 с.

СИАМСКИЕ НЕЙРОННЫЕ СЕТИ В ЗАДАЧАХ СОПОСТАВЛЕНИЯ ВЫБОРОК

Греков М.В., Боровский А.С., д-р техн. наук, профессор
Федеральное государственное бюджетное образовательное учреждение высшего образования «Оренбургский государственный университет», г. Оренбург

Аннотация: в статье рассматриваются особенности медицинской информации как объекта защиты, выявляются характерные угрозы и юридические неопределенности в сфере защиты данных, а также предлагается многоуровневая архитектура обеспечения безопасности медицинских информационных систем.

Ключевые слова: Сиамские нейронные сети, сравнение выборок, ограниченные данные, относительные метки, классификация, устойчивость к дисбалансу данных, обучение с малыми выборками, поддержка принятия решений.

При разработке систем поддержки принятия решений нередко возникает необходимость сравнивать две выборки между собой или с заранее известной парой. Такая ситуация может возникать, например, при анализе результатов или при сопоставлении содержимого различных наборов данных, когда стандартные алгоритмы оказываются недостаточными, поскольку требуется учитывать контекст, определяющий, каким образом выборки должны быть соотнесены. Дополнительную сложность создаёт наличие заранее заданных условий сопоставления: далеко не всегда существующего контекста достаточно для корректной работы алгоритма, и тогда возникает необходимость привлекать экспертов или вручную оценивать выборки, чтобы сформировать примеры положительных и отрицательных соответствий.

При этом процесс ручной разметки больших массивов данных часто оказывается либо чрезвычайно трудоёмким, либо требует слишком много времени, что делает его практически неприменимым в реальных задачах. В таких ситуациях особую ценность приобретают методы, способные создавать контекст автоматически или работать с ограниченными объёмами данных, при этом улучшая итоговую модель за счёт аккумулирования информации из существующих выборок с приемлемой точностью.

Одним из наиболее эффективных подходов для подобных задач являются сиамские нейронные сети. В отличие от традиционных моделей, ориентированных на классификацию объектов, они обучаются выявлять степень сходства между парами образцов. Такой принцип работы позволяет обходиться ограниченными наборами данных, поскольку даже из небольшого числа

примеров можно получить значительно больше пар для обучения, расширяя вариативность выборки без необходимости в дополнительной разметке.

Результаты, представленные в работе «Classification and Comparison via Neural Networks» авторов İlkay Yıldız, Peng Tian и Jennifer Dy, показывают, что сиамская архитектура сохраняет высокую точность даже при существенном сокращении числа положительных примеров, что подчёркивает её устойчивость к дисбалансу данных. Авторы отмечают, что при уменьшении α, то есть при переходе от абсолютных меток к относительным сравнениям, модель способна лучше адаптироваться к условиям, где полный набор аннотированных данных недоступен.

Таким образом, продемонстрированные в работе результаты показывают, что сиамские нейронные сети могут эффективно использовать как ограниченные наборы данных, так и относительные метки, достигая при этом высокой точности и устойчивости к вариативности исходных условий.

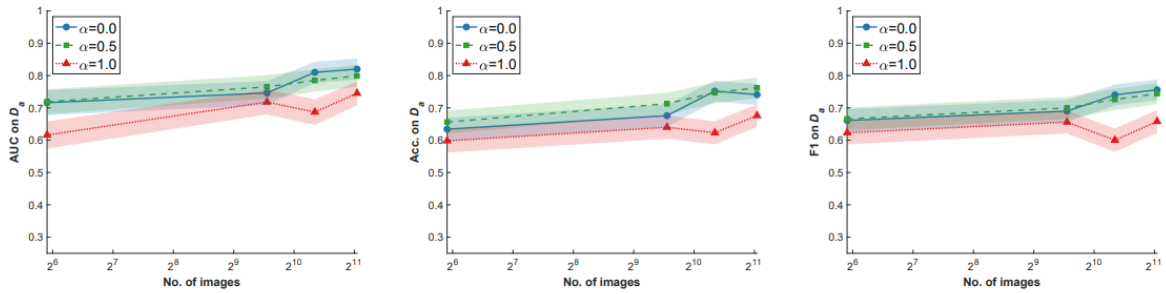
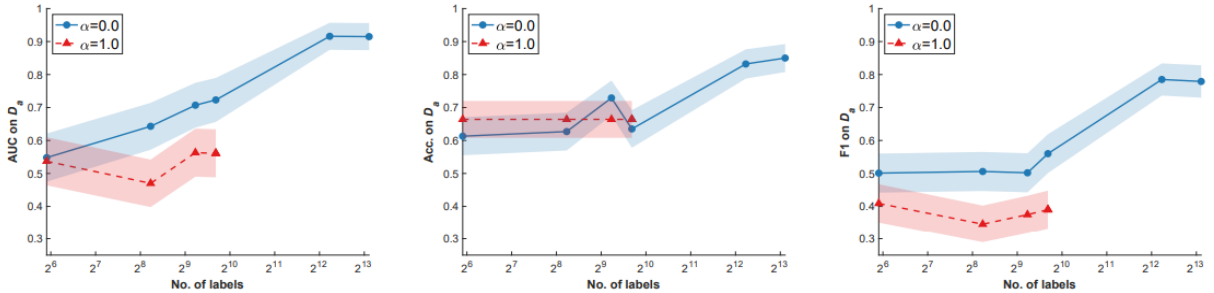


Рисунок 1 – Метрики точности при снижении выборок исследуемого класса

После этого авторы приводят сравнение эффективности применения относительных и абсолютных меток. На рисунке 2 представлено сравнение в виде графиков для 3 наборов данных и 3 метрик: Accuracy, F1 и ROC-AUC.



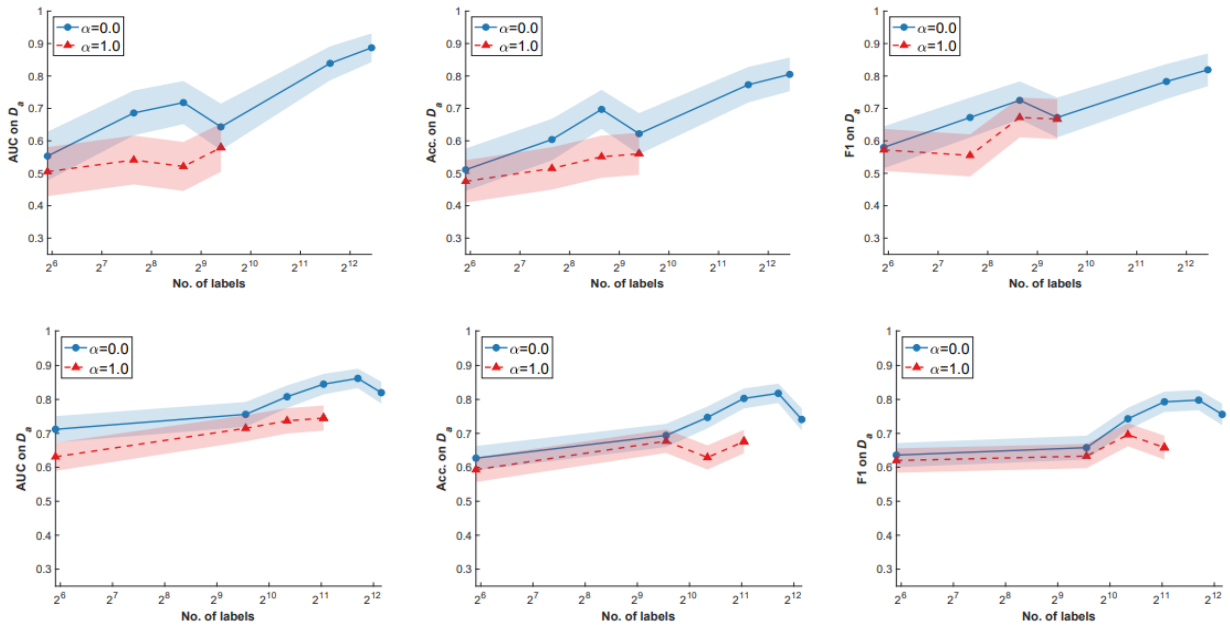


Рисунок 2 – Метрики Accuracy, F1 и ROC-AUC для наборов данных GIFGIF Happiness, GIFGIF Pleasure и FAC

Исходя из результатов, полученных авторами, можно сделать вывод, что сиамские нейронные сети достаточно эффективно снижают требования к исходному набору данных, а также могут повысить точность результатов.

Таким образом, сиамские нейронные сети можно эффективно использовать для сравнения нескольких выборок при этом имея малый набор исходных размеченных данных, которые могут быть использованы для обучения модели.

Более того, при использовании сиамских нейронных сетей можно добиться более качественного результата, чем при использовании классических нейронных сетей, которые сравнивают результат с общим контекстом.

Список литературы

1. Reasat, T. Data efficient contrastive learning in histopathology using active sampling / T. Reasat, A. Sushmit, D. S. Smith // Machine Learning with Applications. – 2024. – Vol. 17. – 100577. – ISSN 2666-8270. – DOI: https://doi.org/10.1016/j.mlwa.2024.100577.

ИННОВАЦИОННЫЕ ТЕХНОЛОГИИ НАУКИ И ОБРАЗОВАНИЯ В ОБОРОННОЙ СФЕРЕ И БЕЗОПАСНОСТИ: МИРОВОЙ ОПЫТ

Гылыджов Г.
Туркменский сельскохозяйственный институт, г. Дашогуз, Туркменистан

Аннотация. Статья посвящена анализу современных технологий, применяемых в науке и образовательных системах в сфере вооружения и безопасности на глобальном уровне. Рассматриваются инновационные методы подготовки кадров для оборонной промышленности, кибербезопасности и управления безопасностью, а также роль научных исследований в развитии современных вооружений и технологий защиты. Особое внимание уделяется интеграции информационных технологий, моделирования, систем искусственного интеллекта и направленный на подготовку специалистов в области безопасности.

Ключевые слова: современные технологии, безопасность, кибербезопасность, моделирование, подготовка кадров, оборонная промышленность, международное сотрудничество.

Современный мир характеризуется высокой динамикой технологических изменений, которые оказывают существенное влияние на сферу вооружения, национальной и международной безопасности. В условиях глобальной конкуренции, роста киберугроз, распространения автономных систем и робототехники стратегическое превосходство государств во многом определяется уровнем научных исследований, технологических инноваций и качеством подготовки кадров в оборонной и безопасностной сферах. Наука и образование становятся ключевыми факторами формирования компетентных специалистов, способных разрабатывать, внедрять и эксплуатировать сложные системы вооружений, а также обеспечивать защиту критической инфраструктуры и киберпространства.

Развитие современных вооружений и систем безопасности требует интеграции множества научных дисциплин: физики, материаловедения, механики, электроники, информатики, искусственного интеллекта и кибернетики. Подготовка кадров для этих областей становится крайне сложной задачей, требующей междисциплинарного подхода. В образовательном процессе активно используются информационные технологии, симуляционные платформы, виртуальная и дополненная реальность, позволяющие создавать условия, максимально приближенные к реальным, для обучения специалистов и тестирования сложных систем. На глобальном уровне ведущие страны, включая США, Великобританию, Китай, Израиль, Южную Корею и Японию, создают высокотехнологичную инфраструктуру для исследований и образования в

оборонной сфере. Университеты, научные центры и оборонные корпорации тесно взаимодействуют, внедряя инновационные методы обучения, такие как цифровые симуляторы, робототехнические лаборатории, системы искусственного интеллекта для анализа и прогнозирования угроз. Международное сотрудничество, обмен опытом и участие в совместных проектах позволяют странам ускорять внедрение инноваций и сокращать технологический разрыв. Особое внимание уделяется подготовке специалистов нового поколения, способных интегрировать знания из разных областей науки, технологий и инженерии. Образовательные программы включают курсы по кибербезопасности, управлению системами вооружений, робототехнике, аналитике больших данных, моделированию и стратегическому планированию. Постоянное обновление содержания программ и внедрение современных цифровых платформ обеспечивает высокую адаптивность подготовки к быстро меняющимся технологическим и стратегическим требованиям [1].

Актуальность данной темы определяется не только необходимостью обеспечения национальной и международной безопасности, но и стратегической задачей формирования кадрового и технологического потенциала, способного поддерживать конкурентоспособность страны на мировом уровне. Интеграция науки, образования и технологий в сфере вооружения и безопасности является ключевым условием достижения технологического превосходства, эффективного управления рисками и защиты критической инфраструктуры, а также развития инновационного оборонного сектора в долгосрочной перспективе.

1. Научные исследования в сфере вооружения и безопасности. Научные исследования в области вооружения и безопасности охватывают широкий спектр направлений: разработку современных систем вооружений, роботизированных комплексов, средств киберзащиты, интеллектуальных систем управления и аналитики данных. Информационные технологии, включая искусственный интеллект и большие данные, позволяют моделировать боевые сценарии, прогнозировать угрозы и оптимизировать процессы управления безопасностью. Современные исследования включают разработку новых материалов для защиты и повышения эффективности вооружений, внедрение автономных систем, применение машинного обучения для анализа разведывательных данных и прогнозирования потенциальных угроз. Также особое внимание уделяется интеграции теоретических моделей и практических экспериментов для обеспечения достоверности и надежности систем безопасности [2].

2. Практическое применение технологий в вооружении и безопасности. Практическое применение современных технологий охватывает оборонную промышленность, кибербезопасность, управление безопасностью на

стратегическом и тактическом уровнях. Использование симуляторов и виртуальных полигонов позволяет проводить обучение специалистов в условиях, максимально приближенных к реальности, что сокращает риски и затраты на подготовку кадров. В области кибербезопасности применяются методы анализа больших данных, моделирования атак, создания систем обнаружения вторжений и защиты критической инфраструктуры. Роботизированные и автономные комплексы, системы искусственного интеллекта и беспилотные летательные аппараты находят широкое применение как в оборонной сфере, так и в обеспечении безопасности на гражданском уровне.

3. Подготовка кадров для сферы вооружения и безопасности. Ключевым аспектом развития оборонной и безопасностной инфраструктуры является подготовка специалистов, способных интегрировать знания в области науки, инженерии и информационных технологий. Университеты, военные академии и исследовательские центры создают междисциплинарные образовательные программы, включающие курсы по системам вооружений, кибербезопасности, робототехнике, моделированию и аналитике данных. Международное сотрудничество и обмен опытом играют важную роль в повышении квалификации кадров, внедрении инновационных методик обучения и создании глобальных стандартов подготовки специалистов. Постоянное обновление образовательных программ и использование цифровых технологий обеспечивают подготовку кадров, способных эффективно реагировать на современные вызовы и угрозы.

4. Перспективы развития. Перспективы развития в сфере науки и образования для вооружения и безопасности включают интеграцию технологий искусственного интеллекта, робототехники и виртуальной реальности в образовательные и исследовательские процессы. Расширение дистанционного обучения и цифровых симуляционных платформ позволит готовить специалистов на международном уровне, обеспечивая доступ к передовым знаниям и методикам. Долгосрочная цель заключается в создании устойчивой системы подготовки кадров, способной поддерживать технологическое превосходство, обеспечивать кибербезопасность и эффективно реагировать на новые угрозы в глобальной сфере безопасности [4].

Таблица 1 – Применение технологий в сфере вооружения и безопасности

№	Направление	Применяемые технологии	Основные задачи	Примеры применения

1.	Образование	Виртуальные лаборатории, симуляторы, VR/AR	Подготовка специалистов, тренировки, моделирование	Военные академии, центры киберподготовки
2.	Вооружение	Робототехника, автономные системы, ИИ	Разработка и модернизация вооружений	Беспилотные летательные аппараты, роботы
3.	Кибербезопасность	Анализ больших данных, системы обнаружения вторжений	Защита критической инфраструктуры, прогноз угроз	Государственные и частные системы защиты
4.	Управление безопасностью	Системы поддержки принятия решений, аналитика данных	Оптимизация процессов, стратегическое планирование	Военные штабы, центры управления кризисами

Современные технологии науки и образования играют ключевую роль в развитии сферы вооружения и обеспечения безопасности. Интеграция информационных технологий, искусственного интеллекта, робототехники и симуляционных платформ позволяет создавать эффективные системы подготовки специалистов и разрабатывать современные вооружения. Международный опыт показывает, что страны с развитой научной и образовательной инфраструктурой получают стратегические преимущества, обеспечивая технологическое превосходство и высокий уровень безопасности. Развитие междисциплинарного образования, цифровых платформ и международного сотрудничества способствует формированию квалифицированных кадров, способных эффективно реагировать на современные угрозы и вызовы. В долгосрочной перспективе это обеспечивает устойчивое развитие оборонной промышленности, повышение национальной безопасности и технологическое лидерство на глобальном уровне [5].

Список литературы

1. Иванов И.И., Петров П.П. Современные технологии в оборонной промышленности // Вестник военной науки. – 2020. – №4. – С. 12–24.
2. Сидоров А.А., Кузнецова Е.В. Информационные технологии в сфере безопасности: теория и практика // Журнал прикладной информатики. – 2019. – Т. 15, №3. – С. 45–59.
3. Zhang Y., Li H. Education and training in defense technologies: global trends // International Journal of Security Studies. – 2021. – Vol. 8, №2. – P. 101–118.

4. Smith J., Brown R. Artificial intelligence and robotics in military applications // Defense Technology Review. – 2022. – Vol. 12, №1. – P. 33–50.

5. Ковалев С.В. Кибербезопасность и защита критической инфраструктуры // Информационная безопасность. – 2021. – №2. – С. 5–17.

СОВЕРШЕНСТВОВАНИЕ АВТОМАТИЗИРОВАННЫХ СИСТЕМ УПРАВЛЕНИЯ ПРОЦЕССАМИ ПОДГОТОВКИ НЕФТИ ЗА СЧЕТ ПРИМЕНЕНИЯ ПРЕДИТКИВНОГО АНАЛИЗА

Евдокимов Д.Д., Тугов В.В., доктор технических наук, доцент
Федеральное государственное бюджетное образовательное учреждение высшего образования «Оренбургский государственный университет»

Аннотация: в статье рассматривается возможность совершенствования автоматизированных систем управления технологическими процессами (АСУ ТП) на этапе подготовки нефти за счёт внедрения методов предиктивного анализа. Авторы обосновывают актуальность использования прогнозных моделей, основанных на машинном обучении и статистическом анализе, для повышения точности управления, предотвращения аварийных ситуаций и снижения эксплуатационных затрат. Описана архитектура типовой АСУ ТП, а также предложен алгоритм интеграции предиктивной аналитики с SCADA- и MES-системами. Подчёркивается, что применение данных технологий способствует увеличению надёжности оборудования, оптимизации производственных циклов и созданию основ для внедрения цифровых двойников.

Ключевые слова: предиктивный анализ, автоматизированные системы управления, подготовка нефти, машинное обучение, SCADA, большие данные, цифровизация, прогнозное моделирование, оптимизация процессов.

Нефтегазовая отрасль сегодня находится в условиях, где повышение операционной эффективности, качества конечного продукта и сокращение затрат на обслуживание становятся ключевыми факторами конкурентоспособности. Особенно это касается этапа подготовки нефти, где требуется максимальный уровень автоматизации и точности управления. Растущая сложность современных технологических систем делает традиционные подходы к контролю неэффективными, что ведет к нестабильности производства. В этой связи все более актуальным становится внедрение цифровых решений, основанных на компьютерном моделировании и аналитике, позволяющих осуществлять достоверный прогноз критически важных параметров технологического режима [1].

В числе ключевых инновационных направлений выделяется методология предиктивного анализа. Ее основное достоинство заключается в способности не просто фиксировать текущие операционные параметры, но и заблаговременно вычислять вероятные нештатные ситуации, предотвращая тем самым серьезные поломки и сводя к минимуму время простоя технических средств.

Внедрение предиктивных моделей ведет к усовершенствованию производственных циклов и увеличению отказоустойчивости агрегатов, поскольку обеспечивает раннее обнаружение скрытых дефектов. Повсеместное

внедрение цифровых решений и возможность работать с большими массивами информации формируют идеальную среду для адаптации данной методологии в действующих контурах регулирования, что подчеркивает ее высокую рентабельность и стратегическую значимость.

Автоматизированные системы управления технологическими процессами (АСУ ТП), применяемые на установках подготовки нефти, являются сложными иерархическими комплексами. Их задача — поддержание в заданных пределах критически важных технологических переменных, включая уровень температуры, величину давления и концентрацию сторонних веществ. На рисунке 1 приведена структуру типовой АСУ ТП подготовки нефти, включающей датчики, контроллеры и систему диспетчерского управления [2].

Архитектурно такие комплексы базируются на трех ключевых компонентах: полевых приборах, программируемых логических контроллерах (ПЛК) и SCADA-системах. Первичные датчики, устанавливаемые непосредственно на объекте, непрерывно снимают информацию о ходе процесса. Полученные сигналы обрабатываются ПЛК, которые формируют управляющие воздействия на исполнительные устройства (клапаны, заслонки). Верхний уровень, представленный SCADA, решает задачи наглядного отображения информации, архивирования данных и оперативного контроля в режиме реального времени. Совместная работа всех компонентов гарантирует постоянное наблюдение и автономное поддержание параметров, что значительно снижает роль субъективного человеческого фактора и обеспечивает исключительную точность выполнения операций [3].

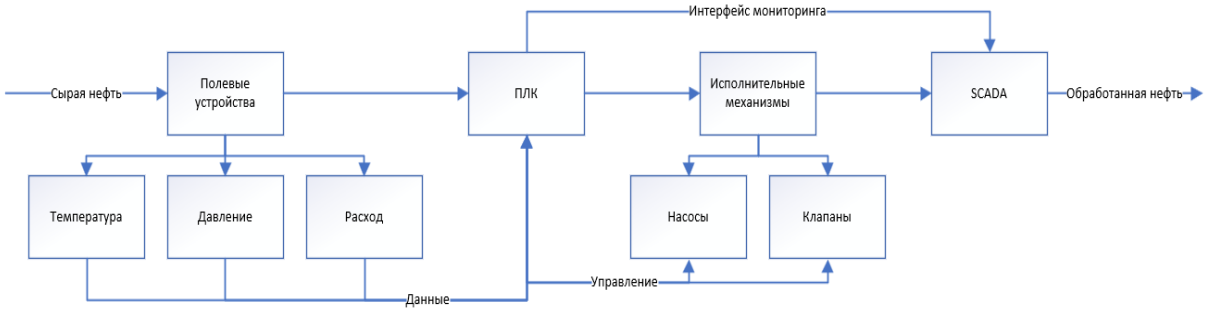


Рисунок 1 – Структура типовой АСУ ТП подготовки нефти

Объединение предиктивной аналитики и АСУ ТП приводит к качественному расширению их совокупных возможностей. На рисунке 2 представлен алгоритм предиктивного анализа, охватывающий этапы сбора данных, предварительной обработки, обучения модели, прогнозирования и корректирующих действий.

Современные методы обработки больших данных дают возможность распознавать сложные, неочевидные закономерности и отклонения от

нормального режима работы. Этот потенциал обеспечивает возможность не просто реагировать, а заблаговременно устранять риски возникновения неполадок, что ведет к существенному сокращению продолжительности внеплановых остановок и повышению общей производительности.

В основе прогнозной аналитики лежит использование методов машинного обучения и статистического моделирования. Наиболее широко применяются регрессионный анализ для построения количественных прогнозов, алгоритмы на основе деревьев решений, а также комбинированные подходы, включая метод случайного леса и градиентный бустинг, которые демонстрируют повышенную достоверность при классификации событий и оценке вероятностей. Отдельную категорию составляют нейросетевые модели, эффективно выявляющие сложные нелинейные взаимосвязи в данных. Перечисленные инструменты дают возможность обрабатывать значительные массивы информации в режиме онлайн и динамически подстраиваться под новые условия [4].

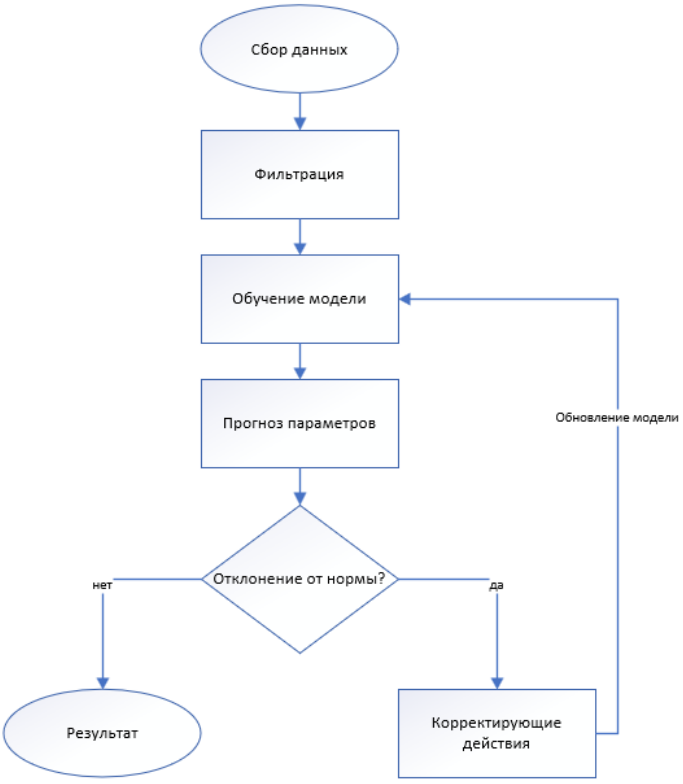


Рисунок 2 – Алгоритм предиктивного анализа для управления процессом подготовки нефти

Реализация предиктивного подхода состоит из последовательности взаимосвязанных стадий. Первичный этап предполагает накопление информации от контрольно-измерительных приборов и датчиков, формируя тем самым детальную исходную базу. Далее выполняется очистка и подготовка данных, в рамках которой устраняются помехи, а также приводится масштабирование

величин для повышения качества последующего анализа. Следующий шаг — построение и обучение модели, которая использует ранее собранные данные для формирования предсказательной способности. Обученная модель используется для расчета будущих значений параметров и анализа отклонений от нормального состояния. Завершающим этапом является принятие корректирующих решений, что замыкает цикл и обеспечивает постоянное повышение точности предсказаний.

Совместное использование прогнозных моделей с SCADA-системами и MES-комплексами создает основу для автоматической настройки технологических режимов и быстрого ответа на возникающие отклонения. Рисунок 3 демонстрирует схему связи между предиктивной аналитической моделью, датчиками и системой управления, включая обратную связь для улучшения точности прогнозов [5].

Модели предиктивного анализа дают возможность формировать управленческие решения на основе объективных данных, что способствует повышению производительности, улучшению качества продукции и снижению эксплуатационных затрат. В условиях растущей цифровизации промышленности такие технологии становятся неотъемлемым элементом стратегического управления.

Рисунок 3 – Интеграция предиктивного анализа с системами SCADA

Внедрение прогнозной аналитики дает ряд существенных выгод, ключевыми из которых являются продление ресурса эксплуатации активов, сокращение расходов на восстановительные работы и плановое сервисное обслуживание, а также стабилизация основных производственных операций. Помимо этого, применение инструментов работы с большими данными и алгоритмов ИИ открывает перспективы для создания виртуальных копий физических объектов (цифровых двойников). Такие модели дают возможность имитировать реальное функционирование установок и находить оптимальные режимы их работы. Дальнейшее развитие технологий связано с усилением кибербезопасности и созданием адаптивных систем, способных самостоятельно корректировать параметры управления в реальном времени [6].

Таким образом, предиктивный анализ является ключевым элементом модернизации нефтеподготовки на основе цифровых решений. Его практическая реализация способствует не только совершенствованию контроля над ключевыми технологическими переменными, но и росту общей рентабельности предприятия. Указанные факторы определяют статус предиктивных систем в качестве неотъемлемого компонента для достижения долгосрочной устойчивости и укрепления рыночных позиций компаний топливно-энергетического комплекса.

Список литературы

1 Шитова, Т.Ф. ERP-система – эффективный инструмент развития цифровой экономики / Т.Ф. Шитова // Муниципалитет: экономика и управление. - 2021. – № 2(35). С. 27-39. DOI: 10.22394/2304-3385-2021-2-27-39.

2 Тугов, В.В. Автоматизация процессов дегазации нефти: монография / В.В. Тугов, Н.И. Жежера, А.И. Сердюк. – Оренбург: ОГУ, 2003. -168 с.

3 Кульга, К.С. Особенности внедрения на машиностроительных предприятиях CAD/CAM/PDM/CAE/PLM и ERP-систем и методы их интеграции / К.С. Кульга // Нефтяное хозяйство. - 2008. – № 2. С. 112-115.

4 Акимов, С.С. Оптимизация производственных потоков на основе алгоритма распознавания производственных ситуаций / С.С. Акимов, В.А. Трипкош // Современные наукоемкие технологии. - 2024. – № 5-1. С. 10-15. DOI: 10.17513/snt.39553.

5 Тугов, В.В. Оптимальное управление готовностью системы сбора и подготовки нефти к использованию / В.В. Тугов, А.М. Пищухин, А.В. Трибунский // Автоматизация и современные технологии. - 2010. - № 3. С. 3-5.

6 Трипкош, В.А. Применение инструментов бережливого производства на основе байесовского алгоритма распознавания / В.А. Трипкош, С.С. Акимов // Современные наукоемкие технологии. - 2023. – № 3. С. 40-44. DOI: 10.17513/snt.39553.

ОРГАНИЗАЦИОННЫЕ МЕРЫ ЗАЩИТЫ КОНФИДЕНЦИАЛЬНОЙ ИНФОРМАЦИИ ПРИ РАБОТЕ С ОБЛАЧНЫМИ СЕРВИСАМИ В УЧЕБНОМ ЗАВЕДЕНИИ

Жумабаев Ж.К.
Федеральное государственное бюджетное образовательное учреждение высшего образования «Оренбургский государственный университет», г. Оренбург

Аннотация. В статье рассматриваются ключевые организационные меры защиты конфиденциальной информации, которые необходимы при использовании облачных сервисов в образовательных учреждениях. Анализируются особенности обеспечения информационной безопасности в учебной среде, выделяются основные угрозы и риски, а также рекомендации по построению эффективной системы защиты, включающей нормативно-правовые, административные и кадровые аспекты.

Ключевые слова: конфиденциальная информация, информационная безопасность, облачные сервисы, кибербезопасность, ИТ-инфроструктура, фишинг, аудит, персональные данные.

Образовательная среда оперирует с конфиденциальными данными несовершеннолетних, что предъявляет повышенные требования к информационной безопасности и защите от деструктивного контента в соответствии с Федеральным законом «О защите прав ребёнка». В связи с этим система информационной безопасности в учебных заведениях должна выполнять две ключевые функции. Во-первых, она обязана защищать базы данных и конфиденциальные сведения от несанкционированного доступа. Во-вторых, необходимо полностью исключить проникновение в образовательные учреждения какого-либо деструктивного контента, независимо от их характера – будь то противоправное влияние или внешне безобидные, но целенаправленно воздействующие на сознание обучающихся материалы. Это касается как школ, так и вузов.

Первые случаи целенаправленных атак на информационные системы образовательных учреждений были зафиксированы в первые годы XXI века. По данным исследований, цели злоумышленников могут быть самыми разными – от хищения персональной информации учащихся и сотрудников до совершения мошеннических операций с использованием полученных данных. С каждым годом киберпреступники разрабатывают всё более изощрённые схемы несанкционированного доступа к конфиденциальной информации.

В современных образовательных учреждениях все чаще применяют облачные сервисы для организации коммуникации с обучающимися и

распределения учебных материалов. Подобный подход приводит к тому, что персональные данные участников образовательного процесса, финансовая информация и другие конфиденциальные сведения размещаются не на локальных серверах учебного заведения, а передаются на хранение внешним поставщикам услуг. Отдельную проблему представляет использование "умных" устройств, работающих совместно с облачными решениями - каждое такое устройство создает новые потенциально уязвимые точки в системе информационной безопасности.

Фишинговые атаки остаются серьезной угрозой информационной безопасности, поскольку способны обходить многоуровневые защитные системы. Особую опасность в образовательной среде представляют случаи, когда преступники фальсифицируют электронные адреса, имитируя официальные рассылки. Неосведомленные учащиеся, переходя по таким ссылкам, невольно предоставляют злоумышленникам доступ к корпоративным данным. Эффективное противодействие фишингу требует комплексного подхода, сочетающего регулярное обучение преподавателей и студентов основам кибергигиены с внедрением специализированных программных решений, способных детектировать поддельные письма и предупреждать пользователей о потенциально опасной корреспонденции [1].

В рамках проверки состояния информационной безопасности учебного заведения необходимо оценить несколько ключевых аспектов. К ним относится характер взаимодействия с облачными сервисами, методы организации хранения данных, проверка корпоративной и учебной почтовой переписки. Также подлежат аудиту специализированные образовательные порталы и иные внутренние системы. В ситуации, когда в школе или вузе отсутствует современная ИТ-инфраструктура, средства киберзащиты и квалифицированные специалисты, оптимальным решением становится привлечение сторонних экспертов для проведения независимого аудита.

Борьба с различными видами угроз информационной безопасности должна вестись на пяти уровнях, причем работа должна носить комплексный характер:

- нормативно-правовой способ защиты информационной безопасности;
- морально-этические средства обеспечения информационной безопасности;
- административно-организационные меры;
- физические меры;
- технические меры.

В России принята «Национальная стратегия действий в интересах детей», определяющая степень угроз и меры защиты их безопасности. Действия по ограничению агрессивного воздействия на сознание ребенка должны стать

основными. На втором месте должно оказаться обеспечение безопасности баз данных.

Защита информации опирается на действующие в этой сфере законы, определяющие отдельные ее массивы как подлежащие защите. Они выделяют те сведения, которые должны быть недоступны третьим лицам по разным причинам (конфиденциальная информация, персональные данные, коммерческая, служебная или профессиональная тайна). Порядок защиты персональных данных определяется в том числе федеральным законом «Об информации», Трудовым кодексом. Они и Гражданский кодекс помогают разработать методику для обеспечения защиты сведений, относящихся к коммерческой тайне. Кроме законов необходимо выделить действующие в этой сфере ГОСТы, определяющие порядок защиты данных, и применяемые в этих целях методики и аппаратные средства [2].

Фундаментальное значение в образовательном процессе имеет комплекс морально-нравственных принципов. Данная система формирует базис для создания эффективных средств защиты, ограждающих несовершеннолетних от влияния деструктивного, противозаконного и аморального контента. Правовой основой для противодействия опасной пропаганде выступают положения Федерального закона «О защите прав ребёнка», которые закрепляют право каждого подростка на ограждение от материалов, наносящих ущерб его нравственному развитию. В этой связи особую актуальность приобретает задача по формированию перечней учебных пособий, литературных произведений и иных ресурсов, представляющих потенциальную угрозу для психики учащихся, с целью их исключения из образовательного пространства. Реализация указанных мер составляет неотъемлемый компонент обеспечения информационной безопасности в учебных заведениях.

Административно-организационные мероприятия охватывают политику информационной безопасности. Основу данной политики составляет комплекс нормативных требований, методических пособий и инструктивных материалов, детализирующих все аспекты обработки информации. Существенным является её внутрикорпоративный статус: положения документа действуют в рамках учреждения и являются закрытыми для внешних лиц.

Составной частью политики выступают также обновления, вносимые в должностные регламенты преподавательского и административного корпуса. Принятие единой системы предписаний обеспечивает руководству возможность эффективного администрирования процессов информационного обмена.

Дополнительным разделом в политике информационной безопасности должен являться порядок доступа к сети Интернет. Раздел должен регламентировать работу учащихся на сторонних сайтах и доступ к внутренним

программам. В дополнение, Политика может содержать рекомендации для родителей по организации безопасного доступа в интернет дома [3].

Отвечать за разработку и реализацию системы мер информационной безопасности обязаны руководители образовательных организаций совместно с сотрудниками ИТ-служб. Недопустимо возлагать обеспечение физической защиты компьютерных сетей и устройств хранения данных на сотрудников частных охранных предприятий. Физические меры защиты предполагают введение строгого режима пропуска в помещения, содержащие важные данные, контроль над доступом посторонних лиц и распределение уровней допуска. К таким мерам относятся также обязательные резервные копии важной информации на компьютерах, изолированных от Интернета. Помимо установки паролей, необходимо регулярно обновлять их [4].

Для обнаружения и устранения различных рисков существуют специальные программы, среди которых выделяются DLP- и SIEM-системы. Эти инструменты позволяют учебному заведению создать многоуровневую защиту данных от несанкционированных действий. Тем не менее, многие образовательные организации сталкиваются с проблемой нехватки финансирования, не позволяющей приобрести дорогостоящее программное обеспечение. В таком случае рекомендуется хотя бы установить лицензионные антивирусные решения. Вместе с тем, важно понимать, что использование лишь антивирусов не обеспечит полноценную безопасность

Важно осуществлять мониторинг электронной почты работников и учеников, устанавливая эффективные фильтры против нежелательной рассылки. Руководству рекомендуется ограничивать доступ к файлам, хранящимся на жёстких дисках рабочих машин. Дополнительно образовательное учреждение вправе внедрить специальное программное обеспечение, предотвращающее посещение веб-ресурсов определённого содержания, включая сайты с агрессивной пропагандой и экстремистскими материалами.

Синергия этих мер позволит защитить компьютерные системы организации не только от намеренных действий злоумышленников, но и от случайных действий учащихся. Дополнительный мониторинг могут осуществлять обученные специалисты, которые будут контролировать работу существующих средств защиты и пополнять этот список [5].

Организационные меры играют ключевую роль в обеспечении эффективной защиты конфиденциальной информации учебного заведения при использовании облачных сервисов. Проведенное исследование позволило выявить наиболее значимые угрозы информационной безопасности и предложить комплекс мер, направленных на минимизацию рисков утечки, несанкционированного доступа и потери данных.

Для успешного внедрения разработанных рекомендаций предлагается создать рабочую группу, включающую представителей администрации учебного заведения, ИТ-подразделения и службы информационной безопасности. Эта группа должна осуществлять координацию мероприятий по внедрению организационных мер, контролировать выполнение установленных процедур и своевременно вносить изменения в систему защиты.

Таким образом, внедрение комплекса рассмотренных организационных мер позволит значительно повысить уровень защищенности конфиденциальной информации учебных заведений при работе с облачными сервисами, обеспечить надежную защиту данных и минимизировать риски нарушений информационной безопасности.

Список литературы

1. Козлов А.Ю. «Риски и угрозы при использовании облачных технологий в образовательных учреждениях» // Информационные технологии в образовании. – 2021. – № 3. – С. 12-20.

2. Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации».

3. Иванов А.В., Смирнов Д.О. «Методы защиты данных в облачных образовательных платформах» // Вопросы кибербезопасности. – 2022. – № 4. – С. 45-52.

4. Вострецова, Е. В. Основы информационной безопасности: учебное пособие для студентов вузов / Е. В. Вострецова. – Екатеринбург: Изд-во Урал. ун-та, 2019. – 204 с.

5. Петренко, С. А. Политики безопасности компании при работе в Интернет / С. А. Петренко, В. А. Курбатов. – 3-е изд. – Москва : ДМК Пресс, 2018. – 396 с

АРХИТЕКТУРА ИНТЕЛЛЕКТУАЛЬНОЙ СИСТЕМЫ АДАПТИВНОГО УПРАВЛЕНИЯ ПАРАМЕТРАМИ МИКРОКЛИМАТА ДЛЯ ТРАНСПОРТИРОВКИ СПЕЦИАЛЬНЫХ ГРУЗОВ

К.С. Жумашев, В.В. Тугов, доктор технических наук, доцент
Федеральное государственное бюджетное образовательное учреждение высшего образования «Оренбургский государственный университет», г. Оренбург

Аннотация. Предложена архитектура интеллектуальной системы адаптивного управления микроклиматом для транспортировки специальных грузов, основанная на использовании цифрового двойника, LSTM-сетей и обучения с подкреплением. Система обеспечивает отказоустойчивый контроль параметров в реальном времени и автономный режим работы в условиях нарушения связи.

Ключевые слова: адаптивное управление, микроклимат, цифровой двойник, LSTM-сети, обучение с подкреплением, отказоустойчивость, специальные грузы, IoT.

Обеспечение стабильности параметров микроклимата (температура, относительная влажность, концентрация диоксида углерода, освещенность) в процессе транспортировки специальной и чувствительной продукции военного и двойного назначения, в том числе фармацевтической продукции, представляет собой критическую задачу, обусловленную жёсткими требованиями технических регламентов и тактико-технических заданий (ТТЗ) и высокой чувствительностью грузов к внешним воздействиям. Разработка структуры интеллектуальной системы адаптивного управления микроклиматом при транспортировке фармацевтической продукции является комплексным процессом, требующим тщательного проектирования архитектурных решений и компонентного состава. Такая система создается для обеспечения строгого контроля температурных и влажностных параметров в режиме реального времени, что особенно критично для термочувствительных препаратов, таких как вакцины, биологические материалы и гормональные средства [1].

Основой системы является многоуровневая архитектура, которая представлена на рисунке 1, объединяющая физические датчики, сетевые компоненты, модули обработки данных и интерфейсы взаимодействия с пользователем. На физическом уровне используются высокоточные сенсоры температуры, влажности, давления и концентрации CO_2, а также GPS-трекеры для мониторинга местоположения. Данные с датчиков передаются через шлюзы с использованием современных IoT-протоколов, таких как MQTT и LoRaWAN, обеспечивающих надежную связь даже в условиях ограниченного покрытия

сетей. Центральным элементом системы является облачная платформа, где происходит обработка и анализ данных.

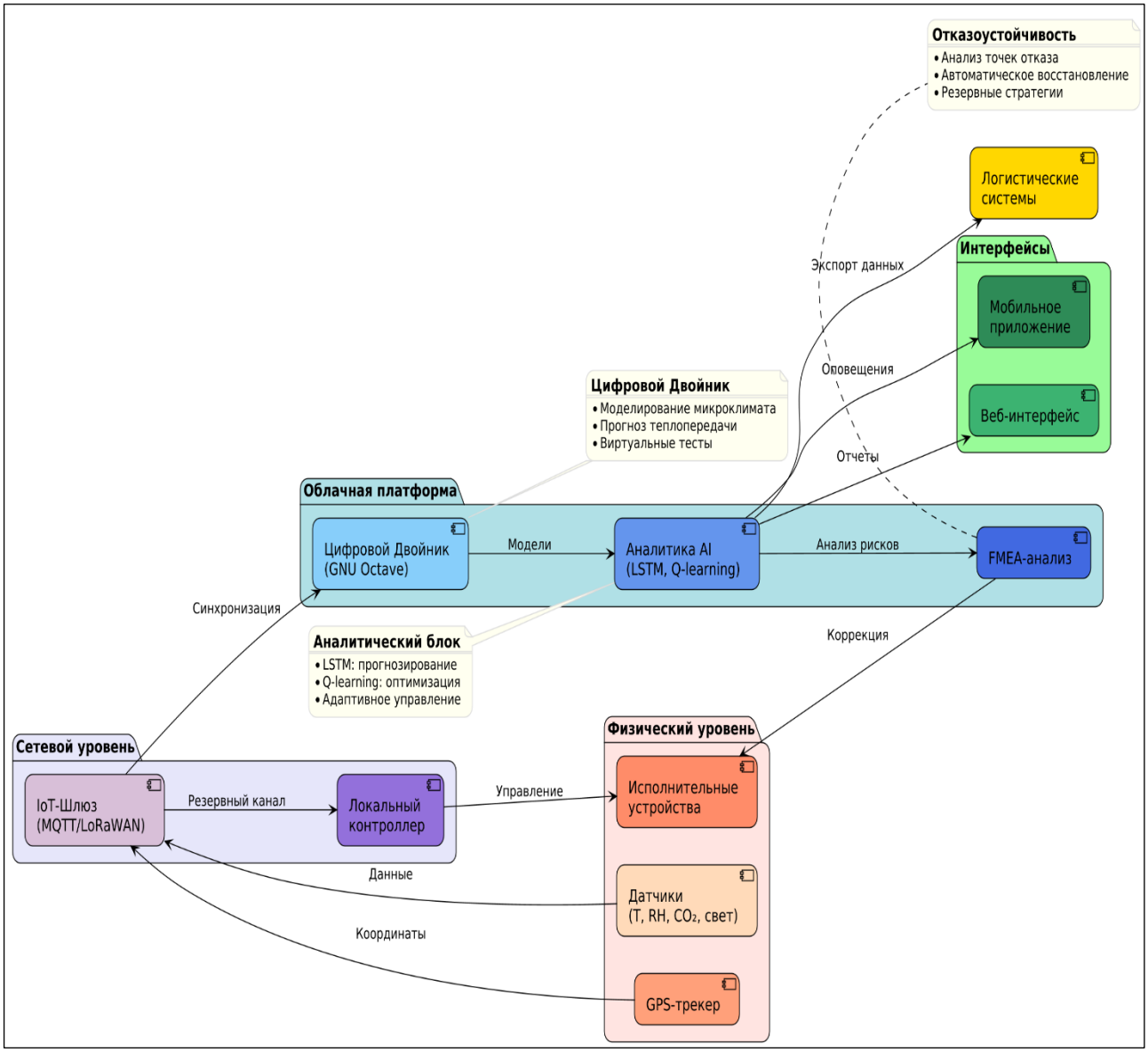


Рисунок 1 – Архитектура интеллектуальной системы адаптивного управления параметрами микроклимата при транспортировке фармацевтической продукции

Описание динамики микроклимата внутри разрабатываемого термоконтейнера требует использования не одного, а нескольких дифференциальных уравнений, учитывая сложность процесса [2]. Метод математического моделирования на основе цифрового двойника, который в дальнейшем будет реализован в среде GNUOctave, служит основой для создания виртуального представления транспортной среды и процессов теплопередачи, что позволяет моделировать реакцию системы на различные управляющие

воздействия и внешние факторы. Метод прогнозирования отклонений параметров на основе обработки временных рядов с использованием LSTM-сетей применяется для предсказания динамики температуры и влажности, выявления потенциально опасных трендов и заблаговременного формирования корректирующих сигналов.

На основе комплексного анализа данных, включая прогнозы LSTM и состояние цифрового двойника, метод оптимизации управляющих воздействий на основе обучения с подкреплением (Q-learning) определяет наиболее эффективные команды для исполнительных устройств (систем охлаждения, вентиляции, подогрева и осушения) с целью минимизации энергопотребления при гарантированном поддержании заданных параметров микроклимата.

Ключевым требованием к системе в контексте безопасности является возможность работы в автономном режиме при потере связи с облаком или в условиях действия помех, что обеспечивает непрерывный контроль параметров и устойчивость функционирования в нестандартных ситуациях [3], при этом локальные алгоритмы управления, основанные на упрощенных моделях и правилах, активируются для поддержания критических условий до восстановления связи.

Метод обеспечения отказоустойчивости и реального времени на основе адаптивного управления и FMEA-анализа интегрирован на всех уровнях системы: FMEA-анализ используется для выявления потенциальных точек отказа аппаратных и программных компонентов и разработки стратегий их парирования, а адаптивные алгоритмы управления позволяют динамически перестраивать логику работы системы при обнаружении сбоев датчиков или исполнительных механизмов, обеспечивая отказоустойчивость и выполнение требований реального времени. Для взаимодействия с пользователем разработан веб-интерфейс и мобильное приложение, предоставляющие оперативную визуализацию данных, оповещения о критических отклонениях и инструменты для формирования отчетов.

Система интегрируется с логистическими платформами, что позволяет учитывать тип перевозимой продукции, длительность и условия маршрута при принятии управленческих решений. Компонентный состав системы включает как аппаратные (датчики, контроллеры для локальной обработки данных, исполнительные механизмы), так и программные модули (сбор и предобработка данных, аналитический блок с алгоритмами машинного обучения, включая LSTM и Q-learning, система управления на основе адаптивных стратегий и цифрового двойника, пользовательский интерфейс). Особое внимание уделено безопасности данных – реализовано шифрование передаваемой информации, аутентификация устройств и разграничение прав доступа.

Таким образом, предлагаемая архитектура интеллектуальной системы обеспечивает комплексный подход к управлению микроклиматом при транспортировке специальной продукции, повышая надёжность логистических цепочек и сохранность критически важных грузов, сочетая современные технологии IoT, машинного обучения (включая LSTM-сети и Q-learning), облачных вычислений, математического моделирования (цифровой двойник) и методы обеспечения надежности (FMEA-анализ, адаптивное управление). Это позволяет минимизировать риски порчи груза за счет оперативного выявления отклонений, точного прогнозирования и автоматической корректировки условий перевозки с учетом отказоустойчивости.

Список литературы

1. Кувшинов, Ю. Я. Интеллектуализация управления системами формирования микроклимата помещений / Ю. Я. Кувшинов, Р. Ш. Мансуров // Известия КБНЦ РАН. – 2012. – № 2-2. – С. 200-206. – URL: https://cyberleninka.ru/article/n/intellektualizatsiya-upravleniya-sistemami-formirovaniya-mikroklimata-pomescheniy (дата обращения: 03.09.2025).

2. Жумашев, К. С. Моделирование процесса поддержания микроклимата в транспортировочном термоконтейнере / К. С. Жумашев, В. В. Тугов // Школа-семинар молодых ученых и специалистов в области компьютерной интеграции производства : Материалы Школы-семинара, Оренбург, 14 ноября 2024 года. – Оренбург: Оренбургский государственный университет, 2024. – С. 185-188

3. Бутаков Р. А. Разработка Архитектуры энергоэффективной системы управления микроклиматом для многозонных складских комплексов / Р. А. Бутаков, Ю. Е. Каюмова // ИНТЕР – Информационные технологии и радиоэлектроника : сборник тезисов студенческой конференции (Екатеринбург, 12-13 мая 2025 г.). – Екатеринбург : Издательский Дом «Ажур», 2025. – С. 73-78.

ИСПОЛЬЗОВАНИЕ ТЕХНОЛОГИЙ БЕРЕЖЛИВОГО ПРОИЗВОДСТВА ДЛЯ СОЗДАНИЯ ПРОДУКЦИИ В ОБЛАСТИ БЕЗОПАСНОСТИ

Жумашева Б.К., Акимов С.С., канд. техн. наук
Федеральное государственное бюджетное образовательное учреждение высшего образования «Оренбургский государственный университет»

Аннотация: Статья посвящена анализу специфики производства военной продукции и возможностям повышения его эффективности за счет внедрения принципов бережливого производства. Особый акцент делается на необходимости количественной оценки выявленных резервов и особенностях построения карт потоков на военных предприятиях, где минимизируется взаимодействие с внешней средой. Автор отмечает, что устранение потерь позволяет высвободить временной резерв для увеличения количества производственных циклов, а также повысить управляемость и контроль над процессами.

Ключевые слова: бережливое производство, карта потока создания ценности, военная продукция

Производство военной продукции представляет собой сложный и многогранный процесс, требующий высочайшего уровня технологического мастерства, точности и надежности. Это не просто фабрика, штампующая оружие, а комплекс взаимосвязанных отраслей, отвечающих за создание сложных систем, способных защитить страну и ее интересы, обеспечивающие безопасность граждан в беспрерывном режиме. Особенную важность в нестабильных международных условиях приобретает точность и четкость исполнения всех производственных задач, связанных с исполнением государственного оборонного заказа.

Путь военной продукции от идеи до ее появления на поле боя начинается с разработки. В специальных конструкторских бюро и исследовательских центрах ведут интенсивные работы по созданию новых видов вооружения и техники, а также по улучшению уже существующих боевых систем. Процесс разработки включает в себя моделирование, прототипирование, испытания и доводку.

После завершения разработки начинается массовое производство военной продукции. Огромные заводы и предприятия преобразуют разработанные ранее чертежи и спецификации в реальные образцы военной техники. Процесс включает в себя металлообработку, сварку, сборку, тестирование.

Производство военной продукции отличается от гражданского производства рядом особенностей, среди которых можно выделить:

– высокие стандарты качества, поскольку военная техника должна быть надежной и безотказной, способной выдержать экстремальные условия боевых действий;

– высокая точность: оружие и оборудование должны быть изготовлены с максимальной точностью, чтобы обеспечить их эффективность и безопасность эксплуатации;

– безопасность: производственный процесс должен быть строго регулируемым, чтобы исключить риск утечки технологий и информации.

Контроль качества играет ключевую роль в производстве военной продукции. Он включает в себя регулярные проверки и тестирования на каждом этапе производственного цикла, чтобы обеспечить соответствие изделий заданным параметрам и требованиям.

Реализация всех поставленных требований возможна лишь с применением передовых производственных технологий. Одной из наиболее перспективных технологий на сегодня является концепция бережливого производства.

Бережливое производство – это философия производственного менеджмента, направленная на оптимизацию производственных процессов путем устранения потерь и повышения эффективности.

Основные принципы бережливого производства базируются на устранении потерь, создании потока ценности, постоянном совершенствовании производственной стратегии, непрерывном взаимодействии с поставщиками и персональным подходом к сотрудникам предприятия. Преимущества бережливого производства заключаются в повышении производительности за счет сокращения потерь и оптимизации процессов; снижении затрат в результате устранения ненужных действий; улучшении качества путем устранения дефектов и несоответствий; снижение нерегламентированных запасов, ввиду более глубокого контроля за потоками и повышение гибкости, позволяющей быстрее реагировать на различные изменения рынка.

Ключевым этапом бережливого производства является создание потока ценности в виде карты такого потока. Карта потока создания ценности представляет собой визуальную модель производства, с отмеченными на нем единицами оборудования и потоками, связующими производственный процесс в единое целое.

Главная цель карты потока заключается в визуализации промышленных потоков таким образом, чтобы создать возможность для поиска потерь, простоев, излишков запасов и определения альтернатив производственных процессов для повышения эффективности производства в целом.

Хотя карта потока создания ценности является достаточно универсальным инструментом бережливого производства, при ее оценке необходимо

использовать различные количественные методы, позволяющие получить численную оценку качества производственного цикла, количества потерь и пр. Потери, обнаруженные в каждом цехе и на каждом месте, структурируются, с целью получения дальнейшей количественной характеристики. Потоки, протекающие на военном предприятии, строятся отдельно, при этом проектировщики карт стараются ограничить количество взаимодействий с внешней средой – исключением является только сообщение со складскими помещениями.

Пример карты потока ценности для некоего производственного участка представлен на рисунке 1.

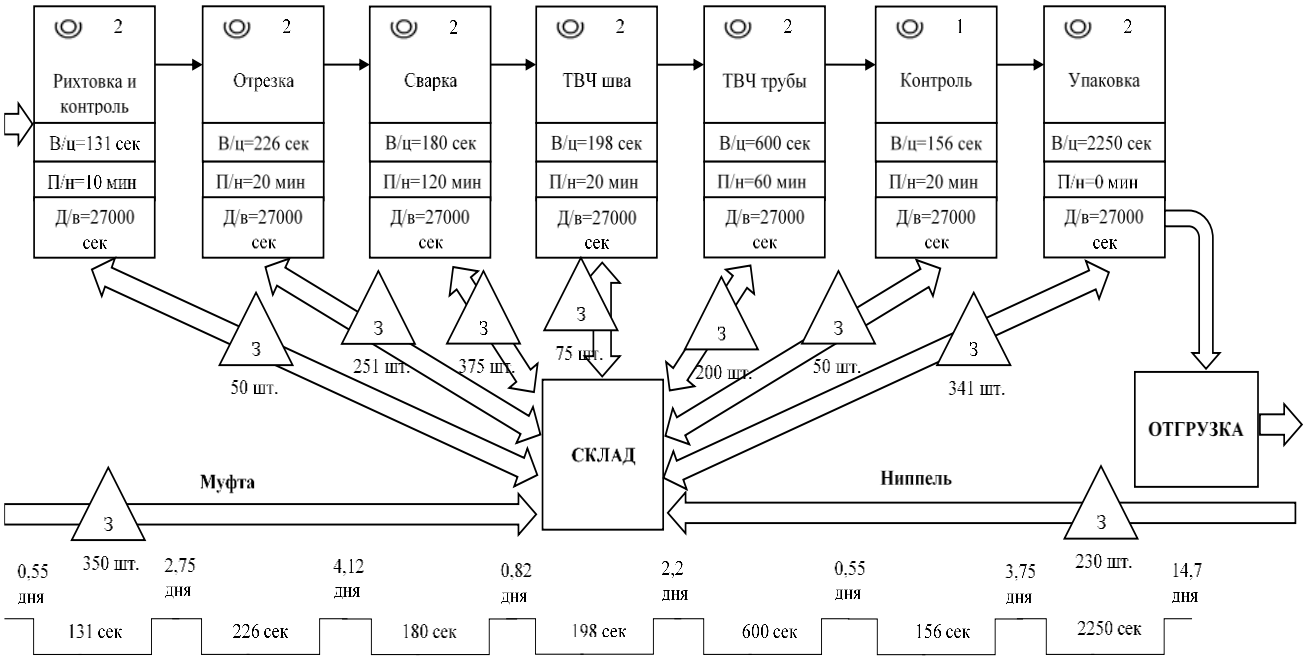


Рисунок 1 – Пример карты потока создания ценности производственного участка

Выявленные потери представляют собой резерв времени, который военное предприятие может использовать для повышения своей эффективности за счет большего числа производственных циклов. Отработанные схемы движения более четко исполняются, что дает возможность осуществлять контроль по определенным точкам, не давая разрастаться второстепенным отделам и департаментам, не священным непосредственно с производственными функциями.

Особенно необходимо отметить, что процесс реализации карты потока создания ценности требует точного учета и контроля, что позволяет обеспечивать высокое качество продукции, так необходимого в военном деле.

Отдельная составляющая – переобучение персонала для работы в новых условиях. Не секрет, что больше всего простоев в работе предприятия связано с человеческим фактором. Наиболее существенные простои связаны с выходом из строя оборудования, чему причиной, как правило, ненадлежащий уход за ним.

Таким образом, производство военной продукции – это сложный и ответственный процесс, требующий высокой квалификации работников, современного оборудования и строгого контроля качества. От его эффективности зависит безопасность страны и ее военная мощь. В современном мире этот сектор продолжает развиваться, интегрируя новые технологии, чтобы создавать более эффективное, надежное и современное оружие и оборудование. Бережливое производство представляет собой философию управления, которая помогает предприятиям достигать новых высот эффективности. Внедрение бережливого производства требует от сотрудников готовности к изменениям, взаимодействию и постоянному совершенствованию процессов. Однако результаты могут превзойти все ожидания, повышая конкурентоспособность предприятия и открывая новые возможности для роста.

Список литературы

1 Акимов, С. С. Производственные процессы в карте потока создания ценностей / С. С. Акимов, В. А. Трипкош // Актуальные проблемы экономической деятельности и образования в современных условиях : Сборник научных трудов Тринадцатой Международной научно-практической конференции, Оренбург, 25 апреля 2018 года. – Оренбург: Общество с ограниченной ответственностью "Научно-инновационный центр", 2018. – С. 235-239.

2 Гуньков, С. А. Построение карты потока создания ценностей в системе бережливого производства предприятия / С. А. Гуньков, С. С. Акимов // Университетский комплекс как региональный центр образования, науки и культуры : материалы Всероссийской научно-методической конференции, Оренбург, 31 января – 02 2018 года / Министерство образования и науки РФ, ФГБОУ ВО "Оренбургский государственный университет". – Оренбург: Оренбургский государственный университет, 2018. – С. 654-657.

3 Шепель, В. Н. Проблемы извлечения знаний / В. Н. Шепель, С. С. Акимов // Университетский комплекс как региональный центр образования, науки и культуры : Материалы Всероссийской научно-методической конференции (с международным участием), Оренбург, 04–06 февраля 2015 года. – Оренбург: Оренбургский государственный университет, 2015. – С. 1562-1565.

4 Акимов, С. С. Минимизация временных потерь на производстве при построении карт потока создания ценности / С. С. Акимов, Б. К. Жумашева // Научно-технический вестник Поволжья. – 2021. – № 6. – С. 83-85.

5 Жумашева, Б. К. Механизм подбора инструментов бережливого производства / Б. К. Жумашева, А. С. Боровский, С. С. Акимов // Компьютерная интеграция производства и ИПИ-технологии : Материалы XI Всероссийской конференции, Оренбург, 16 ноября 2023 года. – Оренбург: Оренбургский государственный университет, 2023. – С. 195-198.

РАЗВИТИЕ ОТЕЧЕСТВЕННЫХ ВООРУЖЕНИЙ НА НОВЫХ ФИЗИЧЕСКИХ ПРИНЦИПАХ

Захаренков Я.Г.
Федеральное государственное бюджетное образовательное учреждение высшего образования «Оренбургский государственный университет», г. Оренбург

Аннотация: **оружие на новых физических принципах –** оружие, в основу создания которого положены физические процессы и явления, не использовавшиеся ранее в оружие обычном (холодном, огнестрельном) или в оружие массового поражения (ядерном, химическом, бактериологическом). Термин носит условный характер, так как в большинстве случаев в образцах ОНФП используются известные физические принципы, а новым является их применение в оружии. В зависимости от принципа действия выделяются следующие виды ОНФП: лазерное, радиочастотное, пучковое, кинетическое оружие и иные виды оружия.

Ключевые слова: оружие на новых физических принципах, лазерные комплексы, оптико-электронные системы, беспилотные летательные аппараты, гиперзвуковые системы, робототехника, высокоточное оружие, электромагнитное оружие, машина дистанционного разминирования.

Ведущие государства активно ищут технологии для разработки принципиально новых видов оружия. В нашей стране также ведутся работы над созданием таких систем, которые получили название «оружие на новых физических принципах» (ОНФП). Один из таких образцов уже принят на вооружение и находится на боевом дежурстве. В ближайшем будущем ожидается появление новых систем подобного типа или аналогичных им.

Разработка ОНФП ведётся в условиях строжайшей секретности. Официальные сведения о таких разработках появляются крайне редко и в ограниченном объёме. Однако все эти новости вызывают большой интерес.

В марте 2018 года было объявлено о начале разработки мобильного боевого лазерного комплекса. Впоследствии он получил название «Пересвет» и был принят на вооружение. В конце 2019 года комплексы нового типа были введены в эксплуатацию. Подробности об их использовании не разглашались.

В декабре прошлого года заместитель министра обороны Алексей Криворучко в интервью для газеты «Красная Звезда» рассказал о ходе работ. Он сообщил, что ведутся разработки новых лазерных комплексов, которые будут использоваться для поражения оптико-электронных систем и беспилотных летательных аппаратов противника. Боевые лазеры будут интегрированы с системами вооружения бронетехники.

В настоящее время ведётся работа над созданием перспективного радиочастотного комплекса, который будет предназначен для нейтрализации беспилотных летательных аппаратов противника. Этот комплекс будет способен наносить «функциональное поражение», что подразумевает не только использование средств радиоэлектронной борьбы, но и создание полноценной «электромагнитной пушки».

В военном ведомстве осознают потенциал и преимущества ОНФП и предлагают уделить этому направлению особое внимание. В начале мая вице-премьер Юрий Борисов в интервью для «Интерфакса» заявил, что в ближайшем будущем оружие на новых принципах станет одним из ключевых направлений развития, наряду с гиперзвуковыми системами, робототехникой и высокоточным оружием. Разработка ОНФП будет включена в будущую Государственную программу вооружений, которая начнёт действовать в 2024 году и продлится до 2033 года.

В настоящее время среди всех типов оружия направленной энергии наиболее впечатляющих результатов достигли боевые лазеры. Эти системы разрабатывались ещё в СССР, и в последнее время были созданы новые образцы. Один из них уже был представлен широкой публике, а другие пока лишь упоминаются в общих чертах.

С 2017 года в некоторые подразделения вооружённых сил для испытаний начали поступать комплексы «Пересвет». Позже они были приняты на полноценное боевое дежурство.

Официально не сообщалось о развёртывании боевых лазеров, их принадлежности и задачах, которые они выполняют. Однако, по оценкам экспертов, эти комплексы могут быть использованы для противодействия авиации, высокоточному оружию или спутникам потенциального противника. В зависимости от типа цели, лазер может разрушить её конструкцию или вывести из строя оптические устройства.

По данным зарубежных СМИ, ранее «Пересветы» находились только на территории России. В прошлом году отечественные СМИ сообщили, что в мае 2020 года такая техника была развёрнута в Сирии. Подробности этой операции не уточнялись. Если эта информация соответствует действительности, это может подтвердить одну из версий о предназначении комплекса.

Возможности «Пересвета» в противовоздушной обороне пока остаются неясными, в то время как цели и задачи других разрабатываемых систем уже определены. В настоящее время проектируются новые лазерные комплексы ПВО, способные бороться, как минимум, с беспилотными летательными аппаратами. Вероятно, после завершения разработки они также будут представлены общественности.

К настоящему времени отечественная промышленность достигла значительных успехов в разработке средств радиоэлектронной борьбы, способных подавлять аппаратуру противника. Также известно о работе над электромагнитным оружием, которое может оказывать на электронику самое серьёзное воздействие.

Несколько лет назад активно обсуждался проект под кодовым названием «Алабуга». По имеющейся информации, это было научно-исследовательское исследование, направленное на поиск основных решений и концепций в области электромагнитного оружия. Позже сообщалось о разработке полноценного импульсного взрывомагнитного генератора, который можно было бы использовать на различных носителях.

По некоторым данным, электромагнитное оружие системы «Алабуга» будет устанавливаться на ракетах с подходящими характеристиками. Их задача — доставить генератор в заданный район, где он будет взорван, создавая импульс, который поразит радиоэлектронное оборудование противника. Однако эта информация не подтверждена, и даже не было объявлено о переходе от научно-исследовательской работы к опытно-конструкторской.

С 2015 года испытывается электромагнитная «пушка» — устройство, предназначенное для поражения электроники противника. В прошлом году сообщалось, что опытный образец этого устройства успешно выводит из строя наземные и воздушные цели на расстоянии до 10 километров. Также были продемонстрированы высокие характеристики устройства.

В настоящее время проект электромагнитного оружия (ЭМИ-пушки) переходит от стадии экспериментов к созданию реального образца вооружения. Хотя проект не раскрывают полностью, уже известно, что он существует.

Вероятно, информация об испытаниях, которые проводились в прошлом году, позволяет предположить, каким будет новое боевое электромагнитное оружие и какие функции оно будет выполнять.

Стоит отметить, что один из образцов электромагнитного оружия уже находится на вооружении. Ракетные войска стратегического назначения используют машину дистанционного разминирования «Листва». На её борту есть устройство, которое называется «микроволновая пушка». Оно предназначено для поражения электроники взрывных устройств.

Практика показывает, что машина дистанционного разминирования «Листва» полностью соответствует требованиям, но её оборудование может действовать на расстоянии не более нескольких десятков метров.

Несколько лет назад стало известно о существовании экспериментальной рельсовой пушки, созданной в нашей стране. Это устройство успешно прошло испытания и позволило собрать необходимые данные.

По неподтверждённым сведениям, исследования продолжаются, но о результатах пока ничего не известно. Однако длительное отсутствие информации может свидетельствовать о продолжении исследований и разработок — результаты могут появиться в любой момент.

В сферу ОНФП также входят технологии, основанные на использовании звуковых колебаний, геофизических, генетических и прочих видов оружия. Эти разработки пока не получают должного признания ни в России, ни за её пределами. Вероятно, в будущем они будут реализованы, но до их практического применения ещё далеко.

Для того чтобы вооружённые силы могли лучше выполнять свои задачи, необходимо улучшать существующие виды оружия и техники, а также разрабатывать новые системы. Именно это происходит в настоящее время во всех ведущих странах.

В области оружия на новых физических принципах разрабатывается несколько направлений, при этом в каждой стране приоритеты и акценты определяются в соответствии с её потребностями и возможностями.

В нашей стране особое внимание уделяется боевым лазерам. Оружие этого типа уже находится на боевом дежурстве, а также разрабатываются новые образцы. Кроме того, активно развиваются все виды радиоэлектронных систем, включая те, которые поражают цель импульсом. Работы в других направлениях ведутся, но не так активно.

При этом очевидно, что российская армия и промышленность в целом проявляют большой интерес к теме оружия на новых физических принципах. Наиболее перспективные проекты и предложения получают поддержку и развиваются. Это создаёт серьёзную научно-техническую базу для будущего перевооружения и повышения боеспособности.

Список литературы

1. Владимиров В.А., Черных Г.С. Состояние и основные направления развития оружия нелетального действия, средств и способов защиты от него. Стретегия гражданской защиты: проблемы и исследования. 2012 г. Т. 2. №1. С. 13-22.

2. Черных Г.С., Старостин А.С. Оружие на новых физических принципах, проблемы защиты населения и территорий от его поражающих факторов.

3. Лютикас П.Л. Анализ современного состояния и основные пути развития разработок оружия основанного на новых физических принципах. «Инновационная наука». 2021 г. № 4, С. 59–63.

НАУЧНО-ТЕХНИЧЕСКАЯ БЕЗОПАСНОСТЬ: ПОНЯТИЕ, ЭЛЕМЕНТЫ, ОСНОВНЫЕ УГРОЗЫ Исхаков Р.З.

Федеральное государственное бюджетное образовательное учреждение высшего образования «Оренбургский государственный университет», г. Оренбург

Аннотация: В статье рассмотрены подходы к определению понятия «научно-технологическая безопасность». Раскрыты цели и задачи обеспечения научно-технологической безопасности, а также интересы государства в научно-технологической сфере. Определены угрозы научно-технологической безопасности. Рассмотрен опыт обеспечения научно-технологической безопасности зарубежных стран. В статье проанализированы нормативные правовые акты, программные документы (стратегии, концепции и т. д.) зарубежных стран в области обеспечения научно-технологической безопасности. 68 Определены ключевые направления, инструменты и механизмы обеспечения научно-технологической безопасности в исследуемых странах.

Ключевые слова: научно-техническая безопасность, научно-техническая сфера, военная безопасность страны, научный потенциал, конкурентоспособность науки и техники, международное научное и техническое сотрудничество.

В основе интенсивного развития экономики лежит научно-техническая сфера. Её ключевая функция — быть связующим звеном между наукой и производством. Она помогает довести результаты фундаментальных и прикладных исследований до стадии практического применения через опытно-конструкторские работы.

Научно-техническая сфера оказывает влияние на экономику, стимулируя научные исследования в перспективных направлениях. Это способствует динамичному развитию экономики и повышению конкурентоспособности товаров и услуг. В свою очередь, наука стимулирует отрасли экономики, где можно реализовать результаты перспективных исследований.

Среди основных национальных интересов России в научно-технической сфере можно выделить следующие: преодоление кризиса в науке, сохранение ведущих научных школ и научно-технических комплексов, особенно в области фундаментальных наук и военно-научных исследований на мировом уровне; сохранение достигнутого мирового уровня и научного превосходства, особенно в отраслях, важных для обеспечения экономического и научно-технического прогресса и военной безопасности страны; сохранение кадрового потенциала науки, противодействие интеллектуальной миграции научных кадров за

границу, систематическое воспроизводство научных кадров и создание условий для их жизни, соответствующих научной квалификации, а также повышение престижа научной деятельности; развитие материально-технической базы отечественной науки до уровня, соответствующего мировым стандартам; создание механизма финансирования науки, который сочетает целевые государственные расходы с растущей долей частного финансирования прикладных исследований; обеспечение нового уровня интеграции российской науки и техники в мировой научно-технический процесс для наращивания научно-технического и экономического потенциала страны, а также решения глобальных экологических и других проблем; развитие научно-технических связей России с другими странами.

Научно-техническая безопасность – это один из видов безопасности, который тесно связан с научной и экономической сферами. Она зависит от государственной научно-технической политики, а также от других важных компонентов, таких как правовая система, подготовка специалистов и внешние связи.

Научно-техническая безопасность обеспечивает специальную систему защиты, которая позволяет поддерживать её в устойчивом состоянии и развивать в интересах страны. Она также способствует повышению национального научного потенциала и интеллектуальной конкурентоспособности.

Внешние факторы, которые могут негативно повлиять на научно-техническую безопасность, включают в себя зависимость от другой страны в стратегически важной отрасли экономики и отставание в научном и техническом развитии.

Внутренние факторы, которые могут негативно повлиять на научно-техническую безопасность, включают в себя отсутствие единой правительственной политики в области научного и технического развития, утрату проверенной временем технологии и недостаточную защиту конкретных технологий, исследований и информации о генофонде.

Также научно-техническая безопасность может пострадать из-за неспособности внедрить передовые мировые технологии из-за отсутствия благоприятных экономических и юридических условий, утраты конкурентоспособности национальной техники и технологии из-за не внедрения современных достижений науки и техники, а также из-за отсутствия условий для использования новых и инновационных технологий в производстве.

Научно-техническая сфера имеет тесную связь с другими сферами, такими как научная и экономическая. Она зависит от государственной научно-технической политики и других важных компонентов, таких как правовая система, подготовка специалистов и внешние связи.

Научно-техническая безопасность обеспечивает защиту и развитие научно-технической сферы в интересах страны. Она способствует повышению национального научного потенциала и интеллектуальной конкурентоспособности.

Внешние факторы, которые могут негативно повлиять на научно-техническую безопасность, включают в себя зависимость от другой страны в стратегически важной отрасли экономики и отставание в научном и техническом развитии.

Внутренние факторы, которые могут негативно повлиять на научно-техническую безопасность, включают в себя отсутствие единой правительственной политики в области научного и технического развития, утрату проверенной временем технологии и недостаточную защиту конкретных технологий, исследований и информации о генофонде.

Научно-техническая безопасность также может пострадать из-за неспособности внедрить передовые мировые технологии из-за отсутствия благоприятных экономических и юридических условий, утраты конкурентоспособности национальной техники и технологии из-за не внедрения современных достижений науки и техники, а также из-за отсутствия условий для использования новых и инновационных технологий в производстве.

Стратегическими целями и задачами государственной политики в области промышленной науки и технологий должны стать:

– возвращение к стабильному экономическому развитию;

– обеспечение необходимого научно-технического задела, гарантирующего технологическую независимость и военную безопасность страны;

– выход на мировые рынки технологий и научно-технической продукции.

Существенную роль должно сыграть осуществление государственного регулирования в области международного технологического сотрудничества и трансфера технологий.

Это регулирование должно быть нацелено на повышение технологического уровня отечественной промышленности, обеспечение конкурентоспособности российских научных и технологических достижений на мировом рынке.

Конкретное регулирование технологии обмена может основываться на следующих принципах:

1) невозможность сделок, предусматривающих, предусматривающие утрату российской стороной прав на технологии отечественной разработки;

2) строгое соблюдение принципа взаимности (признается недействительным любой контракт, предусматривающий ограничения прав российской стороны);

3) заключение контрактов, связанных с передачей новейшей технологии, имеющей общенациональное экономическое значение (список таких технологий должен быть выработан), только по лицензиям.

Пути и средства обеспечения научной и технической безопасности, могут быть достигнуты при выполнении следующих условий:

1) определить единообразную научную и техническую политику и ее приоритетные задачи, выделять не менее 3% национального дохода на финансирование научной деятельности;

2) поощрять исследования, обеспечить научные открытия и интеллектуальные продукты, создать юридические гарантии для внедрения иностранных технологий, адаптированных к российским условиям;

3) развивать и внедрять технологии, подходящие для российских условий, в области использования природных ресурсов, продовольствия и сельскохозяйственного сырья;

4) создать интегрированную национальную научную и техническую информационную сеть, и базу данных и поместить их под защиту государства;

5) поощрять честную конкуренцию за внедрение научных и технических достижений в промышленность и за развитие промышленных технологий. Применять принцип предоставления налоговых послаблений и мягких кредитов на приоритетной основе частным предприятиям и организациям, которые достигли успеха в нахождении научных и технических решений национальной важности и в использовании их результатов в производстве и практической работе;

6) укреплять конкурентоспособность науки и техники, их потенциал развития посредством вовлечения частного сектора в научное и техническое развитие;

7) создать техническую инфраструктуру и благоприятные условия для научного и технического развития, ввести систему должной оценки содержания, потенциала и статуса национальной технологии;

8) концентрировать интеллектуальный потенциал науки и техники и доступные средства, и ресурсы главным образом на реализации национально важных исследовательских проектов;

9) постоянно повышать качество системы образования, поощрять и развивать таланты людей;

10) содействовать специальному обучению высококвалифицированных специалистов в передовых технических областях, создавать интеллектуальные и

материальные предпосылки и условия, чтобы ученые страны могли работать и процветать в собственной стране;

11) ввести практику отбора подающих надежду детей с уровня средней школы для последующей работы в области научных и технических исследований, а также в перерабатывающих и промышленных производствах, обеспечить их условиями для индивидуального обучения и профессиональной подготовки;

12) обеспечить приоритетное развитие искусственного разума, технологии менеджмента и биотехнологии. Уделяя особое внимание приобретению технологий по сборке компьютеров и другого электронного оборудования, использованию солнечной энергии и энергии ветра, а также интегрированной телекоммуникационной сети, основанной на современной технологии, расширить работу по развитию наукоемких новых материалов;

13) развивать международное научное и техническое сотрудничество и обеспечить место страны в международной и региональной интеграции;

14) сохранять национальные научные и технические традиции и методы, приспосабливать их к современным условиям.

Список литературы

1. Сакович, В. А. Инновационная безопасность: основные понятия, сущность / В. А. Сакович, Г. М. Бровка // Наука и техника. – 2016. – Т. 15, № 2. – С. 144–153.

2. Гапонюк, Н. А. Инновационные направления регионального развития / Гапонюк Н. А., Буряченко А. Е. // Вестник ВГУ. Сер. Экономика и управление. – 2014. – № 1. – С. 40–47.

3. Научно-технологическая безопасность регионов России: методические подходы и результаты диагностирования / А. И. Татаркин [и др.] ; под ред. А. И. Татаркина, А. А. Куклина. – Екатеринбург, 2000. – 416 с.

4. Худяков, А. В. Научно-технологическая безопасность Республики Беларусь / А. В. Худяков // Национальная безопасность и стратегическое планирование. – 2016. – № 4. – С. 123–128.

СПЕЦИАЛЬНАЯ ВОЕННАЯ ОПЕРАЦИЯ И РЕВОЛЮЦИЯ ВОЕННОГО ДЕЛА

Ишмуратов И.Р.
Федеральное государственное бюджетное образовательное учреждение высшего образования «Оренбургский государственный университет», г. Оренбург

Аннотация: Специальная военная операция на Украине перевернула представление о тактике и стратегии современных боевых действий. На поле боя начали активно применяться абсолютно новые виды оружия, а также полностью изменился подход к использованию традиционных средств вооруженной борьбы. Воздушные беспилотники в ходе СВО навсегда поменяли концепцию вооруженного противостояния на суше, однако аналогичные изменения произошли и на море. Морские дроны и без экипажные катера в разы дешевле, чем те корабли, которые они атакуют. Кроме того, такие беспилотники представляют серьезную угрозу объектам портовой инфраструктуры.

Ключевые слова: специальная военная операция, стратегия, оперативное искусство, тактика, беспилотная авиация, FPV-дроны, робототехника, высокоточное оружие.

Специальная военная операция, которая началась в феврале 2022 года, уже не ограничивается рамками обычного вооружённого конфликта. Она стала настоящим испытанием для всех аспектов военного дела и военного строительства.

Центр анализа стратегий и технологий (ЦАСТ) одним из первых начал анализировать события, происходящие в зоне СВО, и выявлять новые тенденции в области вооружённой борьбы. Результатом этой работы стал сборник военно-научных статей «Алгоритмы огня и стали», посвящённый специальной военной операции и военным конфликтам последних лет.

СВО стала проверкой всех аспектов военного дела и военного строительства, от тактики и стратегии до организационной структуры войск и испытаний различных видов вооружения и военной техники. Опыт, полученный в ходе СВО, ещё предстоит осмыслить военным учёным. Но уже сейчас ясно, что СВО показала несостоятельность многих прогнозов развития военного дела и потребовала переоценки роли и места различных видов оружия.

В развитии боевых действий и применении сил и средств важно увидеть тенденции и закономерности, которые позволят преодолеть кризис и позиционный тупик так называемого «прозрачного поля боя».

Какие же открытия принесла СВО в военное дело?

Во-первых, современные армии, которые раньше были высокоманевренными, теперь перешли к позиционной окопной войне, где продвижение на поле боя происходит медленно даже по меркам Первой мировой войны.

Артиллерия, особенно дальнобойная и высокоточная, снова стала главным оружием на поле боя. Количество выпущенных снарядов стало одним из определяющих факторов успеха в бою и операции.

Пехота, которая после Второй мировой войны не была готова к такому бою, снова стала важным элементом военных действий.

ПВО неожиданно превзошла военную авиацию, которая не только потеряла способность массово действовать над территорией противника, но и вынуждена летать и базироваться с осторожностью над своей территорией.

Беспилотная авиация стремительно и безоговорочно захватила воздушное пространство. Небо наполнилось множеством микроаппаратов — коптеров и FPV-дронов, которые следят за каждым пехотинцем. Беспилотная революция сделала поле боя прозрачным и начала вытеснять артиллерию.

Это новый облик войны, который во многом противоречит прежним представлениям. Его основные черты — высокая рассредоточенность и низкая плотность войск, а также резко возросшие возможности разведки и высокоточного поражения целей в реальном времени.

В результате значительно увеличилась уязвимость группировок войск, включая тактические подразделения и даже отдельные боевые машины, и бойцов на поле боя.

Чем обеспечивается беспрецедентная прозрачность поля боя? Огромным количеством постоянно используемых средств разведки и целеуказания, особенно беспилотных и спутниковых. Но не только. Наблюдается качественный скачок в объёме и скорости получаемых и передаваемых данных разведки.

Изобилие беспилотных средств разведки позволяет организовать почти непрерывное наблюдение за полем боя на всех уровнях, вплоть до отдельного солдата.

В ближайшие годы ожидается взрывной рост коммерческих спутниковых систем разведки и наблюдения, что приведёт к созданию огромных спутниковых сетей наблюдения с доступом в любой точке планеты.

Радиотехническая разведка, методы киберразведки и слежения за информационными сетями противника также активно развиваются.

Это фактически устраняет «туман войны» и значительно ускоряет процессы определения целей и принятия решений в связке «выстрел — поражение».

Более того, прозрачность становится реальностью не только на тактическом уровне, но и на оперативном и стратегическом. Теперь можно наносить высокоточные удары на любую глубину, включая стратегическую.

Онлайн-целеуказание и гиперзвуковые ракеты позволяют бороться с войсками противника в глубине его территории. В арсенале средств поражения появились относительно небольшие и недорогие барражирующие боеприпасы с дальностью полёта в тысячи километров.

Все эти технологии делают устаревшими учебники по скрытному перемещению, развёртыванию и применению крупных группировок войск. Любое сосредоточение войск становится целью для немедленного удара.

Огромная уязвимость сил тылового обеспечения этих группировок усугубляет проблему.

Это вынуждает пересмотреть основы военного дела. Например, теперь приходится вести боевые действия небольшими подразделениями и отдельными боевыми машинами. А это требует кардинального изменения подходов ко всем аспектам боевого, тылового и технического обеспечения, организации войск и сил и развития всех систем вооружения и военной техники.

В числе систем вооружения, чья роль на поле боя радикально меняется в ходе специальной военной операции, оказались танки. Они стали одной из главных жертв опыта боевых действий последних лет. Символ ударной силы и боевой мощи оказался легко обнаруживаемой и легко поражаемой целью. Кроме того, танк оказался очень уязвим для мин.

В связи с этим возникает ряд вопросов, на которые пока нет ответов. Могут ли танки применяться массированно? Обладают ли они необходимой защитой? Есть ли у них эффективное оружие для ведения огня в условиях прямой видимости? И главный вопрос: утратил ли танк своё значение как главная ударная сила, средство прорыва и манёвра, основа современной войны?

Эксперты считают, что перспективному танку необходимо продемонстрировать сохранение мощного огня прямой наводкой на поле боя по сравнению с другими средствами огневого поражения.

С другой стороны, необходимо решить проблемы, связанные с защитой от мин и минных полей, а также с защитой от барражирующих боеприпасов и FPV-дронов. Один из возможных путей — создание новых комплексов активной защиты, основанных на инновационных технологиях.

Также стоит обратить внимание на роль полевой артиллерии. В этой области наблюдается тенденция к увеличению дальности стрельбы и использованию высокоточных боеприпасов. Развитие артиллерии также влияет на принципы контрбатарейной борьбы, где всё большую роль играют беспилотные разведывательные и наводящие устройства.

Современные системы разведки и огня позволяют быстро обнаруживать цели и точно поражать их. В перспективе ожидается полный переход артиллерии на использование высокоточных боеприпасов.

Ещё одна инновация в тактике — рассредоточение орудийных расчётов. Отдельные орудия, а не батареи и дивизионы, становятся высокоточным оружием и могут использоваться независимо друг от друга. Это можно наблюдать в ходе боевых действий на Украине.

К сожалению, российские разработчики артиллерийских систем пока отстают от своих западных коллег. НАТО демонстрирует качественное превосходство благодаря переходу на 155-мм орудия с длиной ствола 52-го калибра и разработке 155-мм снарядов сверхбольшой дальности. Специальная военная операция выявила значительное отставание российской артиллерии и ракетных систем и требует их кардинального перевооружения в ближайшие годы.

Неожиданным результатом специальной военной операции стало противостояние между системами противовоздушной обороны и военной авиацией. В итоге такие традиционные формы применения боевой авиации, как воздушные наступательные операции или массированные авиационные удары, потеряли свою актуальность.

Подавление систем противовоздушной обороны противника оказалось практически неразрешимой задачей. А ведь её решение определяет дальнейший ход и исход борьбы в воздухе и не только.

Для эффективного противодействия системам противовоздушной обороны противника необходимо создать комплексную систему. Она должна включать в себя системы разведки, обнаружения и вскрытия систем противовоздушной обороны, специальные средства радиоэлектронной борьбы и радиоподавления, средства огневого поражения, специальные авиационные комплексы постановки помех и радиоподавления, ложные цели, комплексы бортовой защиты боевых самолётов и специальные боевые самолёты подавления и поражения систем противовоздушной обороны.

Все эти элементы должны быть интегрированы в единую систему управления и проходить совместное обучение и боевую подготовку для выполнения поставленных задач.

Стремительное развитие беспилотных военных технологий и методов их применения стали проблемой для систем противовоздушной обороны, которые не были готовы к борьбе с такими небольшими объектами. Однако дроны различных классов и назначений, вероятно, стали главной проблемой для средств ПВО и серьёзным вызовом для любой системы противовоздушной обороны.

Следует признать, что столь значительное влияние дронов на современные военные действия не было предсказано военными теоретиками. Хотя намёки на новую тенденцию можно было заметить ещё во время второй карабахской войны 2020 года.

Произошло кардинальное изменение в использовании беспилотников обеими сторонами конфликта. Вместо применения дронов самолётного типа большой, средней и малой дальности, продолжительности полёта и размера, теперь массово используются небольшие коммерческие коптеры. Они применяются как для разведки и наблюдения, так и в качестве ударных средств, включая FPV-дроны и барражирующие боеприпасы.

Это привело к значительному расширению их использования, фактически сделав их одним из основных видов вооружения в боевых действиях.

FPV-дроны могут поражать практически все виды военной техники на передовой, обеспечивая беспрецедентное соотношение «стоимость — эффективность», которое ранее было недоступно для любого управляемого оружия.

Беспилотники, которые революционизировали боевые действия в ходе специальной военной операции, — это небольшие барражирующие боеприпасы, в том числе российские «Ланцеты». Они становятся доступным и эффективным тактическим средством поражения, а также одним из основных средств борьбы с артиллерией противника.

Можно предположить, что в будущем развитие «ланцетоподобных» аппаратов в качестве летающих артиллерийских систем приведёт к их частичной трансформации в малогабаритные тактические ракеты. По его словам, широкое распространение FPV-дронов и барражирующих боеприпасов приведёт к их эволюции вплоть до индивидуального оружия солдата. Это означает, что в ближайшие годы на поле боя будут задействованы десятки и сотни тысяч небольших беспилотных летательных аппаратов. Соответственно, перед системами ПВО встанет задача борьбы с ними на уровне отдельных подразделений, экипажей и расчётов.

В заключение приведем высказывание известного военного теоретика А.А. Свечина из его книги «Стратегия», написанной в 1926 году: «В стратегии пророчество может быть только шарлатанством; и гений не в силах предусмотреть, как фактически развернется война. Но он должен составить себе перспективу, в которой он и будет оценивать явления войны».

Список литературы

1. Половинкин В.Н. Специальная операция на Украине. СПб.: Крыловский гос. науч. центр, 2023. 140 с.

2. Небренчин С.М. Специальная военная операция на Украине – 2022: война с коллективным Западом // Большая Евразия: развитие, безопасность, сотрудничество: материалы Пятой междунар. науч.-практ. конф. Т.6. Ч.1. М.: ИНИОН РАН, 2023. С. 287-290.

3. Дульнев П.А., Колесниченко А.П., Котов А.В. К вопросу об интеллектуализации управления общевойсковыми формированиями тактического звена // Военная мысль. 2024. №7. С. 87-97.

4. Мажуга С.Н., Вдовин А.В., Гончаров О.В. Превосходство в управлении – перспективная область вооруженного противоборства // Военная мысль. 2024. №6. С. 67-75.

5. Баканеев С.А., Сильников М.В., Карпович А.В., Орлов С.А., Чернышев Ю.М. Применение беспилотных летательных аппаратов при управлении огнем артиллерии. СПб.: Первый ИПХ, 2023. 112 с.

СОВРЕМЕННЫЕ ВЫЗОВЫ И НАПРАВЛЕНИЯ ИНТЕЛЛЕКТУАЛЬНОГО УПРАВЛЕНИЯ ИНФОРМАЦИОННЫМИ ПОТОКАМИ В РАСПРЕДЕЛЕННЫХ СИСТЕМАХ СПЕЦИАЛЬНОГО НАЗНАЧЕНИЯ

А.А. Колонюк, А.С. Боровский, доктор технических наук, профессор
Федеральное государственное бюджетное образовательное учреждение высшего образования «Оренбургский государственный университет», г. Оренбург

Аннотация: Рассматриваются проблемы управления информационными потоками в распределенных системах специального назначения, функционирующих в условиях неопределенности и противодействия. Обосновывается необходимость перехода к интеллектуальному управлению на основе методов AI/ML для обеспечения киберустойчивости и эффективности.

Ключевые слова: распределенные системы, информационные потоки, интеллектуальное управление, киберустойчивость, искусственный интеллект, машинное обучение, беспилотные рои, РЭБ, критическая инфраструктура.

Распределенная система – это набор компьютерных программ, использующих вычислительные ресурсы нескольких отдельных вычислительных узлов для достижения одной общей цели. Ее также называют распределенными вычислениями или распределенной базой данных. Распределенная система основывается на отдельных узлах, которые обмениваются данными и выполняют синхронизацию в общей сети. Обычно узлы представляют собой отдельные физические аппаратные устройства, но это могут быть и отдельные программные процессы или другие рекурсивные инкапсулированные системы. Распределенные системы направлены на устранение узких мест или единых точек отказа в системе.

Эволюция распределенных систем специального назначения – управляющих комплексов беспилотных роев, систем радиоэлектронной борьбы (РЭБ) и мониторинга критической инфраструктуры – формирует новый класс задач в области управления информационными потоками. Эти системы функционируют в агрессивных и динамически изменяющихся средах, где ключевыми параметрами являются не только скорость и объем обрабатываемых данных, но и их предельная актуальность, достоверность и своевременность доставки.

Информационные потоки в таких системах характеризуются крайней гетерогенностью – от телеметрии и сигналов сенсоров до разведывательных данных и команд управления. Они отличаются высокой интенсивностью и подвержены резким, зачастую непредсказуемым всплескам нагрузки,

вызванным изменениями оперативной обстановки. Жесткие временные ограничения и требования к отказоустойчивости делают классические, детерминированные алгоритмы управления трафиком неэффективными и даже опасными, так как они не способны к оперативной адаптации в условиях неполной информации и целенаправленного противодействия.

Центральной проблемой становится обеспечение киберустойчивости архитектуры, способности обрабатывать данные в условиях неопределенности и сохранять функциональность при частичной деградации. Традиционные подходы, основанные на статических моделях и заранее предопределенных правилах, исчерпали свой потенциал. Назрела объективная необходимость в применении методов интеллектуального управления, использующих алгоритмы искусственного интеллекта и машинного обучения (AI/ML). Эти методы позволяют реализовать адаптивное, прогнозирующее и самоорганизующееся управление информационными потоками, что является критически важным для выполнения поставленных задач в современных условиях.

Распределенные системы специального назначения представляют собой сложные киберфизические комплексы, объединяющие разнородные вычислительные ресурсы, сенсоры и исполнительные устройства, рассредоточенные в пространстве. Их работа направлена на достижение единой оперативной цели. К таким системам относят, к примеру, системы управления группами беспилотных летательных аппаратов, требующие координации множества агентов в реальном времени на основе данных лидаров, видеопотоков и телеметрии. Или комплексы радиоэлектронной борьбы, обрабатывающие широкополосные радиосигналы для обнаружения и оперативного противодействия. Сюда же входят системы мониторинга критической инфраструктуры, агрегирующие данные с тысяч датчиков для предупреждения аварий.

Информационные потоки в таких системах обладают особыми свойствами, отличающими их от стандартного сетевого трафика. Прежде всего, это жесткие временные ограничения. Для многих задач, таких как уклонение от препятствия или подавление канала связи, задержка передачи является не метрикой качества, а детерминированным требованием к жизнеспособности системы. Запаздывание команды на миллисекунды может привести к катастрофическим последствиям.

Другой характеристикой служит высокая динамика и нестационарность. Интенсивность и маршруты потоков данных не являются заранее предопределенными. Они резко меняются в зависимости от оперативной обстановки: появление новой цели, выход из строя узла, изменение режима работы. Это требует мгновенного перераспределения сетевых ресурсов, что невозможно при статической настройке.

Кроме того, наблюдается ярко выраженная гетерогенность данных. Система одновременно обрабатывает принципиально разную информацию: критичные по времени, но небольшие по объему команды управления; широкополосные потоки данных от сенсоров, такие как RAW-видео или радиозахват; а также служебную информацию для поддержания работы самой сети. Ко всему этому добавляются повышенные требования к достоверности и целостности критических данных, передача которых часто происходит по зашумленным и неустойчивым каналам связи.

Именно эта совокупность характеристик – детерминированные задержки, динамичность, гетерогенность и работа в условиях противодействия — и приводит к несостоятельности классических методов управления трафиком. Традиционные подходы, основанные на статических конфигурациях и протоколах, таких как QoS с жестким приоритизированием или статическая маршрутизация, не справляются.

Их главный недостаток – отсутствие подлинной адаптивности. Заранее заложенные правила не могут адекватно реагировать на непредвиденные изменения в сетевой топологии или характере трафика. Конфигурация просто не успевает за динамикой оперативной обстановки. Эти методы работают по факту возникновения проблем, то есть реактивно, а не проактивно. Они начинают бороться с перегрузкой канала только после того, как она уже возникла и привела к потере пакетов. Такая модель является хрупкой: жестко заданные политики часто оказываются неработоспособными при частичном отказе элементов сети или появлении новых, не предусмотренных типов трафика. В условиях зашумленных каналов стандартные протоколы, например TCP, начинают деградировать, бесконечно повторяя попытки передачи, что лишь усугубляет ситуацию с задержками.

Интеллектуальное управление информационными потоками предполагает создание когнитивной управляющей системы, способной в автоматическом режиме решать задачи адаптивной маршрутизации, прогнозного управления ресурсами, оптимизации трафика и обеспечения киберустойчивости. Это не просто еще один инструмент, а смена фундаментального подхода: сеть из пассивной «труб»" для передачи данных превращается в активный, самонастраивающийся и самовосстанавливающийся организм.

Основу для этой трансформации составляют методы искусственного интеллекта и машинного обучения. Например, обучение с подкреплением позволяет создать агента, который методом проб и ошибок в симуляционной среде вырабатывает оптимальную стратегию управления – выбора маршрута или приоритета пакета. Критерием успеха служит не соблюдение абстрактного правила, а максимизация конкретного вознаграждения, которое формулируется

как совокупность целевых метрик: минимальная задержка, отсутствие потерь, максимальная пропускная способность для критичного трафика.

Глубокие нейронные сети находят применение для классификации трафика и выявления аномалий на основе анализа паттернов сетевого потока, что является ключевым для обнаружения кибератак. Они же могут использоваться для прогнозирования состояния каналов связи и нагрузки на сеть, позволяя действовать на опережение, а не реагировать постфактум.

Внедрение таких технологий знаменует переход от управления к настоящему оркестрованию информационными потоками, где решения принимаются на основе анализа текущего состояния, прогноза его изменения и понимания оперативных целей. Это уже не просто техническая задача, а создание нового качества управления, адекватного современным вызовам.

Список литературы

1. Горяинов, Р. И. Метод распределения информационных потоков в автоматизированных системах специального назначения / Р. И. Горяинов, И. В. Левко, Н. А. Шуваев // Известия ТулГУ. Технические науки. – 2022. – № 10. – URL: https://cyberleninka.ru/article/n/metod-raspredeleniya-informatsionnyh-potokov-v-avtomatizirovannyh-sistemah-spetsialnogo-naznacheniya (дата обращения: 05.09.2025)

2. Моряков, В. Е. Внедрение технологий виртуальной реальности в процесс обучения личного состава в военной учебной среде / В. Е. Моряков, Н. В. Серищев, Е. А. Жидко // Молодой ученый. – 2024. – № 49 (548). – С. 306-308. – URL: https://moluch.ru/archive/548/119943 (дата обращения: 05.09.2025).

3. Караван, Ф. Э. Возможности применения интеллектуальных систем управления и поддержки принятия решений при организации обслуживания и ремонта в специальных организационно-технических системах [Электронный ресурс] / Ф. Э. Караван, А. С. Боровский // Компьютерная интеграция производства и ИПИ-технологии : материалы XI Всерос. конф., Оренбург, нояб. 2023 г. / Оренбург. гос. ун-т ; гл. ред. А. И. Сергеев. - Оренбург : ОГУ,2023. - . - С. 230-232

ПОДГОТОВКА ПЕДАГОГОВ ПО ДЕЙСТВИЯМ ПРИ ПОЛУЧЕНИИ СИГНАЛОВ И ИНФОРМАЦИИ ОПОВЕЩЕНИЯ НАСЕЛЕНИЯ

Леонова А.Н.
Всероссийский научно-исследовательский институт по проблемам гражданской обороны и чрезвычайных ситуаций МЧС России, г. Москва

В свете современных вызовов и угроз, таких как теракты, природные катастрофы и техногенные аварии, значительное внимание уделяется подготовке педагогов к действиям при получении сигналов и информации оповещения населения. В статье рассматриваются сигналы ГО и предлагает рекомендации по обучению педагогов.

Ключевые слова: оповещение населения, система оповещение населения, сигнал оповещения, операторы связи, оконечные средства оповещения.

Сигналы оповещения доводятся до населения по специально создаваемых для этой цели системам оповещения, которые в современном виде она начали формироваться в 30-х годах прошлого века одновременно с образованием системы местной противовоздушной обороны, а затем гражданской обороны. Сначала системы оповещения строились на базе сетей уличной радиотрансляции, а также сирен, размещенных на крупных промышленных предприятиях. Запуск сирен осуществлялся вручную. Всему населению было известно, что если звучит сирена, то это сигнал «Воздушная тревога», который предупреждал о нападении противника с воздуха, а в годы холодной войны - о ракетно-ядерном нападении. По этому сигналу население должно было немедленно покинуть свои дома, квартиры, рабочие места, транспортные средства и укрыться в защитных сооружениях (убежищах, подвалах, погребах, укрытиях простейшего типа). Сигнал оповещения передавался не только сиренами, но и гудками промышленных предприятий.

Перед началом Второй мировой войны в нашей стране были установлены следующие сигналы оповещения: «Воздушная тревога», «Отбой воздушной тревоги», «Химическая опасность» [1, 2].

После окончания войны с появлением оружия массового поражения количество сигналов оповещения, называвшихся в те времена «сигналами гражданской обороны» увеличилось. Так, к шестидесятым годам прошлого века их стало десять: «Воздушная тревога», «Закрыть защитные сооружения», «Угроза радиоактивного заражения», «Химическое нападение», «Бактериальное заражение», «Угроза затопления», «Отбой воздушной тревоги», «Отбой радиоактивного заражения», «Отбой химического нападения». Тогда же планировалось ввести еще один сигнал «Внезапное нападение», но поскольку аппаратура оповещения позволяет передавать только два сигнала звучания сирены (постоянное и прерывистое завывание), а население исторически привыкло к сигналу «Воздушная тревога», данное решение принято не было.

В конце семидесятых годов количество сигналов оповещения было сокращено до четырех: «Воздушная тревога», «Отбой воздушной тревоги», «Радиационная опасность», «Химическая тревога» [1, 2].

Сигнал «Воздушная тревога» передавался прерывистым завыванием электрических и ручных сирен, а также записанный на пластинке по радиотрансляционной сети в течение двух-трех минут. Все остальные сигналы передавались по радиотрансляционной сети речевыми сообщениями. При этом должны были сообщаться границы действия данного сигнала и правила поведения населения при каждой конкретной опасности.

Впоследствии в начале 80 годов прошлого века рассматривался вопрос о введении сигнала «Воздушное предупреждение», который должен был предварять сигнал «Воздушная тревога». Для его звучания предполагалось включать электросирены при постоянном звучании, но поскольку подлетное время ракет было минимальным, и население, прослушав два сигнала не успело бы принять меры защиты, данный сигнал также не был введен.

Сигналы оповещения изменились после трагедии на Чернобыльской АЭС, последствия аварии, а затем и землетрясение в городе Спитак Армянской ССР, поставили перед системой гражданской обороной новые задачи, в том числе оповещение населения в мирное время при угрозе или возникновении техногенных аварий и природных катастроф [3].

1986 год стал переломным для Гражданской обороны СССР в целом, в том числе для оповещения населения. В октябре1988 года директивой Штаба ГО СССР был изменен порядок оповещения населения и со 2 января 1989 года был введен новый универсальный сигнал «Внимание Всем!». Подача сигнала должна осуществляться путем включения сетей электрических, электронных сирен и мощных акустических систем длительностью до 3 минут с последующей передачей по сетям связи, в том числе сетям связи телерадиовещания, через радиовещательные и телевизионные передающие станции операторов связи и организаций телерадиовещания с перерывом вещательных программ.

За годы, прошедшие с введения сигнала «Внимание всем!», электросирены включались неоднократно, два раза в год системы оповещения населения проводятся проверки систем оповещения населения с задействованием оконечных средств оповещения [4].

При неизменности сигнала оповещения, увеличивается количество операторов связи и редакций средств массовой информации, передающих сигнал и экстренную информацию оповещения [5]. Введен порядок передачи информации оповещения. Так, для сетей связи подвижной радиотелефонной связи - сообщений объемом не более 134 символов русского алфавита, включая цифры, пробелы и знаки препинания). Допускается трехкратное повторение этих сообщений (для сетей подвижной радиотелефонной связи - повтор передачи сообщения осуществляется не ранее, чем закончится передача предыдущего сообщения).

Типовые аудио- и аудиовизуальные, а также текстовые и графические сообщения населению о фактических и прогнозируемых чрезвычайных ситуациях готовятся заблаговременно постоянно действующими органами управления РСЧС совместно с органами повседневного управления РСЧС. Услышав звук электросирены или звуковой сигнал «Внимание всем!», население должно немедленно включить приемник радиовещания на любой программе или телевизионный приемник на любой местный новостной канал и окончании звукового сигнала «Внимание всем!» по каналам телевидения и по радио будет передаваться речевая информация о сложившейся обстановке и порядке действия населения.

При получении сигналов оповещения населения, учителям необходимо среагировать немедленно и организовать действия в соответствии с инструкциями общеобязательного укрытия или эвакуации. Вот перечень обязательных действий при получении сигналов оповещения:

– оперативно перейти к выполнению указаний в исполнение сигнала оповещения;

– быстро и спокойно вывести всех учащихся из здания школы и направить их к местам укрытия или местам стояния для эвакуации;

– следовать указаниям руководства школы и сотрудничать с другими учителями и сотрудниками для осуществления эвакуации или укрытия;

– проверить, что все учащиеся находятся в безопасности и помочь им, если им потребуется помощь;

– следовать инструкциям руководства и соблюдать порядок и дисциплину в процессе эвакуации или укрытия;

– сообщать о своем местоположении и состоянии учащихся руководству школы и службам спасения, если это потребуется.

Главная задача учителя - обеспечить безопасность учащихся, поэтому следуйте инструкциям и действуйте профессионально в любой чрезвычайной ситуации.

С этой целью необходимо:

– изучить инструкции по действиям при получении различных сигналов оповещения населения, так, например, знание правил эвакуации и поведения в чрезвычайных ситуациях помогут правильно реагировать на сигналы оповещения;

– проводить тренировки с педагогическим коллективом для получения практики реагирования на сигналы оповещения в случае чрезвычайной ситуации, что поможет всем педагогам и учащимся быть готовыми к действиям в случае необходимости;

– изучить план эвакуации всеми сотрудниками учебного заведения, чтобы убедиться, что каждый знает, как действовать в различных ситуациях и где находятся пути эвакуации и места укрытия;

– проводить практическую подготовку учащихся действиям в чрезвычайных ситуациях;

– проводить уроки по безопасности, практикуя эвакуационные упражнения; это поможет знать, что делать, если возникнет чрезвычайная ситуация на территории учебного заведения.

Самое главное: оставаться спокойными и решительными в случае получения сигнала оповещения, чтобы ваши действия были образцовыми для учеников и коллег. Помните, что ваша безопасность и безопасность учеников - главный приоритет во время чрезвычайных ситуаций.

В заключение необходимо отметить, что только таким образом можно обеспечить эффективное реагирование на угрозы и обеспечить безопасность обучающихся и персонала в школах и других учреждениях образования.

Список литературы

1. Гражданская оборона. Под редакцией генерала армии А. Т. Алтунина – М.: Воениздат, 2005–252 с.

2. От МПВО к гражданской защите. Страницы из истории МПВО-ГО-РСЧС субъектов Российской Федерации. Владимиров В.А., Долгин Н.Н., Маланичев Ф.Г. -М.: МЧС России, 2004. Режим доступа: https://fireman.club/literature/ot-mpvo-k-grazhdanskoy-zashhite-2004/, дата обращения 03.09.2025.

3.Постановление Совета Министров СССР от 23 октября 1989 года № 882 «О мерах по обеспечению защиты персонала атомных станций и населения в случае радиационно опасных аварий на этих станциях» [Электронный ресурс] Режим доступа: Технорма.RU (tehnorma.ru), дата обращения: 03.09.2025.

4. Положение о системах оповещения населения [Электронный ресурс] Режим доступа: docs.cntd.ru дата обращения 03.09.2025.

5. Постановление Правительства РФ от 28.12.2020 № 2322 «О порядке взаимодействия федеральных органов исполнительной власти, органов исполнительной власти субъектов Российской Федерации, органов местного самоуправления с операторами связи и редакциями средств массовой информации в целях оповещения населения о возникших 03.09.2025.

ЦИФРОВАЯ ТАМОЖНЯ: СИСТЕМА УПРАВЛЕНИЯ РИСКАМИ И ИСКУССТВЕННЫЙ ИНТЕЛЛЕКТ

Матияс Е.Ю.
Учреждения образования «Гродненский государственный университет имени Я. Купалы»,
г. Гродно

Аннотация: В статье рассматриваются современные подходы к минимизации незаконного вывоза товаров через внедрение системы управления рисками и технологий искусственного интеллекта в деятельность таможенных органов Республики Беларусь. Анализируются организационные и правовые условия эффективной реализации данных технологий.

Ключевые слова: *искусственный интеллект, система управления рисками, участники внешнеэкономической деятельности, пост-таможенный контроль.*

В современном мире необходимо постоянно улучшать таможенный контроль, ведь международная торговля растет, и появляется все больше способов незаконно вывозить товары. Сегодня в торговле между странами государство в основном использует экономические способы регулирования. Таможня становится все более современной и цифровой. Вместо бумаг и долгого досмотра, теперь есть компьютерные программы и искусственный интеллект. Это помогает быстрее пропускать товары и выявлять даже потенциальные правонарушения. Одним из мощнейших инструментов современной таможни является система управления рисками. Данная система представляет собой современный метод таможенного контроля, основанный на выборочном подходе к проверке товаров. Благодаря системе управления рисками, таможенные органы тратят меньше сил и времени, уделяя внимание объектам, находящимся в зоне риска.

Опыт других стран также доказывает эффективность данного инструмента. В Европе, например, управление рисками помогает таможне следить за товарами даже после того, как они прошли контроль. Следовательно, система управления рисками внедрена в таможенное администрирование. Стоит отметить, что в европейских странах акцент делается на пост-таможенный контроль и взаимодействие с уполномоченными экономическими операторами. Согласно стратегии развития до 2030 года, разработанной таможенными органами Республики Беларусь, были разработаны и утверждены ориентиры уменьшения контрольной нагрузки на участников внешнеэкономической деятельности. Но есть и проблемы. На данный момент еще не все процессы автоматизированы, а также не доработан институт уполномоченных экономических операторов. Для сравнения: в Республике Беларусь насчитывается около 400 уполномоченных экономических операторов, в то

время как европейских странах в среднем 17 тысяч [3]. Именно поэтому информации не всегда достаточно.

Использование пост-таможенного контроля на основе системы управления рисками создаст необходимый баланс между упрощением процедур и сохранением важных функций. В таком случае, таможенные органы смогут в первую очередь оптимизировать ресурсы и проводить часть проверок на этап уже после выпуска, и, что немало важно, ускорить таможенное оформление для добросовестных участников внешнеэкономической деятельности.

Необходимо также отметить, что за последние несколько лет в мире начали активно изучать и внедрять во многие сферы искусственный интеллект. К сожалению, современное таможенное законодательство не в полной мере учитывает специфику применения искусственного интеллекта. Существует множество рисков, а также сложно внедрять новые технологии. Но искусственный интеллект может помочь таможне работать лучше. Например, в Нигерии есть программа, которая была разработана с участием группы анализа таможенных данных Всемирной Таможенной Организации. Система анализирует оценки вероятности нарушений таможенного законодательства и обеспечивает максимизацию уплату таможенных платежей в результате выявления таких нарушений. Искусственный интеллект может быстро анализировать много данных, находить связи и определять потенциальные угрозы и правонарушения [1].

1 марта 2024 года глава ФТС России Руслан Давыдов в своем выступлении по итогам заседания объединенной коллегии таможенных служб ЕАЭС отметил, что в государствах-членах уже применяют системы управления рисками в ходе таможенных проверок. При этом он подчеркнул, что использование средств искусственного интеллекта позволит ускорить принятие решений по результатам [2].

Таким образом, можно сделать вывод, что современное таможенное администрирование стоит на пороге цифровой трансформации. Необходимо грамотно сочетать упрощение процедур для добросовестных участников внешнеэкономической деятельности и ужесточение борьбы с правонарушениями. Искусственный интеллект и усовершенствованная система управления рисками, безусловно, являются важными и эффективными инструментами современной таможни. Но их успешное применение напрямую зависит от готовности сотрудников применять их на практике. Специалисты должны не только использовать их, но и критически оценивать данные, принимать взвешенные управленческие решения. Интеграция системы управления рисками в пост-таможенный контроль, углубление партнерства с уполномоченными экономическими операторами и точечное применение анализа данных позволит оптимизировать ресурсы и ускорить таможенное оформление. Результатом такой комплексной модернизации станет не только повышение конкурентоспособности национальной экономики, но и укрепление

научно-практической базы отечественного таможенного администрирования, а также содействие в дальнейших исследованиях в данной области.

Список литературы

1. WCO BACUDA experts develop and share a neural network model to assist Customs to detect potential fraudulent transactions [Electronic resource] : World Customs Organization. – Mode of access: https://www.wcoomd.org/en/media/newsroom/2020/may/wco-bacuda-experts-develop-and-share-a-neural-network-model.aspx. – Date of access: 10.09.2025.

2. Глава ФТС заявил, что таможни ЕАЭС перешли на риск ориентированный подход при проверках [Электронный ресурс]. – https://tass.ru/ekonomika/20130819 – Дата доступа: 05.09.2025.

3. Официальный сайт таможенных органов Республики Беларусь [Электронный ресурс] – Режим доступа: https://www.customs.gov.by/ – Дата доступа: 09.09.2025.

ЗАЩИТА ДАННЫХ И ПОЛИТИКА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В МЕДИЦИНСКИХ СИСТЕМАХ

Махметова К.М., Боровский А.С., д-р техн. наук, профессор
Федеральное государственное бюджетное образовательное учреждение высшего образования «Оренбургский государственный университет», г. Оренбург

Аннотация: в статье рассматриваются особенности медицинской информации как объекта защиты, выявляются характерные угрозы и юридические неопределенности в сфере защиты данных, а также предлагается многоуровневая архитектура обеспечения безопасности медицинских информационных систем.

Ключевые слова: информационная безопасность, защита данных, информационная система, медицинские данные, конфиденциальность, несанкционированный доступ.

Современное развитие цифровых технологий привело к широкому внедрению медицинских информационных систем (МИС), которые обеспечивают хранение, обработку и передачу больших объемов данных о пациентах, медицинских услугах и организационных процессах здравоохранения. Одной из главных проблем при разработке МИС выступает задача обеспечения их информационной безопасности. Речь идет не только о защите сведений о состоянии здоровья пациентов, результатах обследований и лечении, но и о сохранности самой структуры системы: программных модулей, механизмов хранения и обработки информации и т.д.

Под информационной безопасностью понимается комплекс мер, направленных на предотвращение несанкционированного доступа, утечек, искажения или полной потери данных. В условиях цифровизации медицины это приобретает особое значение, поскольку сбои в защите могут повлечь не только утрату ценных данных, но и прямой риск для жизни и здоровья пациентов [1].

Медицинская информация имеет особый статус, поскольку напрямую связана с личной жизнью человека и требует строгой конфиденциальности. Сведения о факте обращения к врачу, диагнозах, назначениях и результатах обследований относятся к персональным данным и могут составлять врачебную тайну. Их защита регулируется рядом действующих нормативных актов. В первую очередь это Федеральный закон «О персональных данных» № 152-ФЗ от 27.07.2006, который устанавливает правила обработки и хранения персональных сведений, а также Федеральный закон «Об информации, информационных технологиях и о защите информации» № 149-ФЗ от 27.07.2006, определяющий порядок обеспечения информационной безопасности. Дополнительно вопросы

сохранения тайны при оказании медицинской помощи отражены в законодательстве о здравоохранении, где закреплены права пациента на неразглашение информации о его состоянии здоровья.

В контексте медицинских информационных систем это означает, что любая база данных или программный модуль, где содержатся сведения о пациентах, должен соответствовать установленным требованиям: обеспечивать защиту от несанкционированного доступа, исключать возможность утечки, искажения или утраты данных. Помимо технических средств защиты важную роль играет организационная составляющая – регламенты доступа, обучение персонала и контроль за соблюдением правил обработки медицинской информации.

Формирование необходимого уровня информационной безопасности медицинских информационных систем опирается на три фундаментальных принципа:

1) конфиденциальность;

2) целостность;

3) доступность данных [2].

Эти параметры находятся в тесной взаимосвязи и зачастую вступают в противоречие. Например, обеспечение быстрого и удобного доступа пользователей к требуемой информации может снижать уровень защиты и создавать риски утраты или искажения данных. В противоположность этому, строгий контроль конфиденциальности и целостности информации усложняет процесс ее получения и обработки.

Возникает своеобразный баланс: повышение одного показателя безопасности нередко сопровождается ограничением другого. Более того, чрезмерное усиление всех трех направлений одновременно может привести к перегрузке системы, снижению ее производительности и надежности, что особенно критично при работе с электронными медицинскими картами и оперативной диагностической информацией.

Поэтому подход к информационной безопасности в медицинских организациях должен строиться на компромиссе, т.е. с одной стороны – обеспечении должной защиты персональных данных и врачебной тайны, а с другой — сохранении удобства и скорости работы врачей и медицинского персонала. С учетом того, что лечебно-профилактические учреждения функционируют как системы массового обслуживания, концепция безопасности медицинских информационных систем должна учитывать как специфику их деятельности, так и реальные потребности медицинской практики.

Для того чтобы определить оптимальный уровень информационной безопасности в медицинских информационных системах, важно внимательно

изучить специфику медицинской информации, ее состав и идентифицировать всех участников процесса обработки данных.

Исследователи выделяют несколько характерных особенностей медицинской информации как сведений ограниченного распространения:

1. Медицинская информация тесно связана с личной тайной пациента и формально находится под его контролем. Пациент вправе самостоятельно распоряжаться этими сведениями, включая возможность предоставления их третьим лицам по собственному усмотрению. Однако в реальной практике такая свобода ограничена законодательством о врачебной тайне и защите персональных данных: пациент может делиться информацией, но учреждения и специалисты обязаны соблюдать установленные правила конфиденциальности.

2. Медицинские документы подчинены строгим временным рамкам, которые определяют скорость и эффективность оказания медицинской помощи. Такие регламенты направлены на сокращение времени пребывания пациента в учреждении, повышение его удовлетворенности качеством обслуживания, оптимизацию использования коечного фонда и эффективное применение дорогостоящего медицинского оборудования.

Слишком жесткое соблюдение конфиденциальности, которое ограничивает доступ медицинских специалистов к необходимой информации, может негативно сказаться на этих показателях. В частности, замедление доступа к данным может привести к задержкам в диагностике и лечении, создавая прямую угрозу здоровью и даже жизни пациентов. Кроме того, такие ситуации могут повлечь значительные финансовые потери для лечебно-профилактического учреждения, рост юридических рисков и претензий со стороны пациентов и их родственников.

3. Структура медицинской информации позволяет рассматривать ее отдельными фрагментами. К таким фрагментам относятся: персональные данные пациента (имя, дата рождения и т. д.), сведения о состоянии здоровья, рекомендации и назначения врача, информация о проведенном лечении, а также агрегированные статистические данные.

Конфиденциальной является только совокупность нескольких фрагментов, которая позволяет идентифицировать конкретного пациента. По отдельности отдельные данные обычно не подпадают под режим врачебной тайны.

Агрегированные сведения о заболеваемости, количестве обращений, уровне нетрудоспособности и характеристиках групп пациентов (регион проживания, возрастная группа, пол и т. д.) формируют статистическую информацию, которая также не относится к сведениям ограниченного доступа. Такой подход позволяет сочетать защиту персональных данных с возможностью анализа медицинских процессов и планирования здравоохранения.

4. Обработка отдельных фрагментов медицинской информации часто распределена между разными сотрудниками лечебно-профилактического учреждения. В работу с данными вовлечены регистраторы, врачи, медсестры, диагностические специалисты, лаборанты, статистики и другие специалисты. При этом многие фрагменты обрабатываются отдельно и не позволяют однозначно идентифицировать пациента.

Например, лабораторный материал и результаты анализов могут привязываться к уникальному номеру медицинской карты (штрих-коду или другому ключу), при этом личность пациента не раскрывается. Такой подход важен в случаях, когда требуется повышенная анонимность или конфиденциальность.

В рамках медицинской информационной системы эта концепция может быть реализована более эффективно: МИС позволяет гибко настраивать права доступа пользователей, предоставляя каждому специалисту доступ только к тем фрагментам медкарты, которые необходимы для выполнения его функций. Это обеспечивает соблюдение принципов конфиденциальности и минимизирует риски утечки данных, при этом не снижая оперативность работы и качество медицинской помощи.

5. При работе с медицинской информацией возможны три основных типа угроз: несанкционированный доступ, утрата информации и искажение данных. Нарушения могут привести к утечкам, задержкам в лечении или ошибочным назначениям.

6. Взаимоотношения между медицинским персоналом, пациентами и их доверенными лицами/родственниками остаются юридически неурегулированными. На сегодняшний день законодательство не дает однозначного ответа на принципиальный вопрос: следует ли сообщать сведения о состоянии здоровья пациента самому пациенту или его доверенным лицам (даже без согласия пациента) в случаях тяжелых заболеваний, когда такая информация может ухудшить здоровье или вызвать психологический стресс.

Вероятно, что формальное законодательное регулирование этих вопросов в обозримом будущем маловероятно, поскольку каждая ситуация отличается высокой индивидуальностью и требует профессиональной оценки конкретного врача. Универсальные правила здесь могут оказаться неэффективными или даже вредными.

Все перечисленные особенности формируют основу политики информационной безопасности медицинской информационной системы.

На основании анализа результатов исследований была разработана комплексная схема защиты данных (рисунок 1). Надежная защита медицинских

данных строится на принципе многоуровневой безопасности, где каждый слой выполняет собственные задачи и дополняет другие.

Рисунок 1 – Комплексная схема защиты данных

Первый уровень – это пользователь. Уже на этапе работы с интерфейсом важно ограничивать действия в зависимости от роли и обучать персонал основам кибергигиены. Второй уровень – многофакторная аутентификация, позволяющая значительно снизить риск несанкционированного доступа при компрометации пароля. Третий уровень связан с ролевым доступом: врач, медсестра, администратор или пациент получают лишь те права, которые необходимы для их задач. На четвертом уровне применяется шифрование: TLS защищает передаваемые данные, а AES обеспечивает надежное хранение информации в базе. Пятый уровень включает систему логирования и аудита, позволяющую фиксировать каждое действие и своевременно выявлять нарушения. И наконец, шестой уровень – это физическая защита серверов и дата-центров: строгий контроль доступа, резервирование и инженерная защита инфраструктуры.

Таким образом, такая архитектура обеспечивает комплексную безопасность медицинской информации и минимизирует риски утечек и несанкционированного доступа.

Список литературы

1. Бетин, А. В. Разработка методики автоматизированного аудита безопасности персональных данных в медицинских информационных системах / А. В. Бетин // Информационные технологии : Сборник тезисов XIII Конгресса молодых ученых, Санкт-Петербург, 09–11 апреля 2024 года. – Санкт-Петербург: федеральное государственное автономное образовательное учреждение высшего образования "Национальный исследовательский университет ИТМО", 2024. – С. 45.

2. Горбунов, Н. А. Моделирование угроз информационной безопасности медицинских информационных систем / Н. А. Горбунов // Информационные технологии : Сборник тезисов XIII Конгресса молодых ученых, Санкт-

Петербург, 09–11 апреля 2024 года. – Санкт-Петербург: федеральное государственное автономное образовательное учреждение высшего образования "Национальный исследовательский университет ИТМО", 2024. – С. 97-98.

ПРИМЕНЕНИЕ СОВРЕМЕННЫХ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ В ПРОЦЕССЕ ОБУЧЕНИЯ СТУДЕНТОВ В ВОЕННОМ УЧЕБНОМ ЦЕНТРЕ

Милин А.И.
Федеральное государственное бюджетное образовательное учреждение высшего образования «Оренбургский государственный университет», г. Оренбург

Аннотация: Одной из важных задач, стоящих перед военными институтами, является обучение и воспитание будущих офицеров, то есть их профессиональная подготовка к выполнению своего воинского долга по защите Родины. Чтобы реализовать эту задачу, необходимо качественно организовать военно-педагогический процесс, опираясь при этом на теоретические основы и практический опыт.

Ключевые слова: информационные технологии, виртуальный мир, интерактивные электронные игры, автоматизированная обучающая система, электронная литература, мультимедийное сопровождение.

Информационные технологии становятся неотъемлемой частью жизни современного человека. В России наблюдается стремительный рост уровня компьютеризации населения, что делает информационные технологии ключевым элементом развития общества. Порой трудно представить себе жизнь без них.

В некоторых российских вузах студенты проходят военную подготовку в специальных учебных центрах. Для повышения качества обучения необходимо пересмотреть традиционные подходы к образовательному процессу. Это позволит улучшить качество и доступность образования, а также снизить количество студентов, не освоивших программу обучения.

Информационные технологии эффективно используют информационные ресурсы общества, которые сегодня являются ключевым стратегическим фактором развития. Опыт показывает, что использование информационных ресурсов позволяет значительно сократить расход других видов ресурсов: материалов, оборудования, человеческих и социальных.

Информационные технологии обучения — это педагогические методы, которые используют специальные инструменты, программное обеспечение и технические средства для работы с информацией.

Применение современных информационных технологий является необходимым условием для разработки более эффективных подходов к обучению и совершенствования методов обучения. Использование ИТ

способствует повышению мотивации учащихся, экономии времени и более наглядному представлению учебного материала.

Приобщение студентов к информационным технологиям является важным шагом в решении задачи информатизации в учебных центрах. Важно отметить, что виртуальное обучение не должно заменять реальное, а должно расширять и ускорять его.

В настоящее время существует множество инструментов информационных технологий, которые могут быть использованы в обучении студентов. Например, визуализация материала с помощью технологий AR и VR позволяет создать виртуальный мир, который передаётся человеку через его ощущения. Чаще всего это реализуется с помощью очков виртуальной реальности и наушников.

Интерактивные электронные игры — это форма обучения, которая воссоздаёт и усваивает опыт в различных ситуациях. Они направлены на передачу знаний, навыков и умений. Это форма обучения без принуждения, которая включает в себя элементы развлечения.

Виртуальные наглядные учебные пособия — это учебные материалы, которые создаются с помощью технологий виртуальной или дополненной реальности, а также с помощью веб-ресурсов и образовательных программ. Основной принцип — это перенос модели исследуемого объекта в информационное пространство с отображением всех необходимых свойств для его изучения.

Контроль и тестирование — это информационная система, которая используется для оценки успеваемости студентов. Она основана на анализе результатов обучения, включая предварительные результаты.

Кейс-методика — это метод конкретных ситуаций, который использует описание реальных ситуаций для обучения.

Автоматизированная обучающая система — это комплекс технических, учебно-методических, программных и организационных ресурсов, которые используются для индивидуализации обучения.

Работа с прикладным учебным программным обеспечением — это использование специализированных программ для обучения.

Электронная литература — это электронные учебники и пособия, которые используются в образовательном процессе.

Рассмотрим инструменты, которые могут значительно улучшить процесс обучения. Среди них: визуализация материала, тестирование и использование электронных ресурсов.

В настоящее время одним из наиболее популярных методов является мультимедийное сопровождение. Этот способ представления информации делает процесс обучения более эффективным.

Однако, использование виртуальной и дополненной реальности может значительно повысить эффективность обучения и улучшить практические навыки по сравнению с традиционными методами. Важно обеспечить плавный переход от традиционных методов к новым технологиям.

Внедрение информационных технологий в обучение военнослужащих уже происходит в некоторых странах, таких как Россия, США, Германия, Великобритания, Канада и Китай.

В Китае исследования в области информационных технологий в военной сфере проводятся в Командной академии связи. Также Академия военных наук, Китайский университет национальной обороны, Университет информационной техники и Военно-морское инженерное училище активно работают над внедрением информационных технологий в систему военного образования. Эти центры занимаются подготовкой офицеров к ведению информационной войны, проводят кибертренировки и другие исследования, а также разрабатывают новую технику.

В Китае концепция «информационной войны» приходит на смену концепции «народной войны в современных условиях». В соответствии с новой концепцией, армия должна перейти к сетевой архитектуре управления, координируя действия всех родов войск с помощью системы C4ISR2 (Command, Control, Communications, Computers, Intelligence, Surveillance, Reconnaissance — контроль, оперативное управление, коммуникации, компьютеры, разведка, наблюдение, зондирование).

Вторым по значимости элементом военной стратегии Китая после ядерного оружия является способность создавать информационные угрозы.

Компания Microsoft поставляет американской армии прототипы систем дополненной реальности, в частности, модификацию устройств Microsoft Hololens IVAS (Integrated Visual Augmentation System — «интегрированная система визуального дополнения»). Предполагается, что они предоставят войскам более подробную информацию для принятия решений и позволят отработать действия во время сложных операций. Армия получит 100 тысяч голографических гарнитур, а стоимость сделки составит 480 миллионов долларов США.

В США армейская исследовательская лаборатория активно работает над усовершенствованием синтетической среды обучения (STE — Synthetic Training Environments), которая использует VR/AR технологии. В новой версии STE военнослужащие различных подразделений смогут проводить масштабные

совместные учения и взаимодействовать, не выходя из дома или в любом другом месте. Это позволяет нивелировать географический фактор и обеспечить одновременное обучение большого числа участников виртуальных миссий.

Вся экипировка представляет собой готовую коммерческую продукцию, а военные создают свои программы и сценарии для имитации военных миссий в виртуальной реальности. Это соответствует концепции развития армии будущего «Сила 2025» (F2025B — Force 2015 and beyond), где VR/AR занимают особое место.

Фонд оборонных инноваций Великобритании также заключил контракт на обучение военнослужащих с использованием VR технологий. Контракт был подписан в феврале 2019 года с компанией Bohemia на сумму 1 миллион фунтов стерлингов.

В России также активно рассматривается вопрос о внедрении информационных технологий в обучение военнослужащих. Уже есть примеры использования этой технологии. Например, в 2016 году в Санкт-Петербургском государственном университете на военной кафедре начали подготовку офицеров с использованием технологии виртуальной реальности. Очки HOMiDO VR с подключённым смартфоном позволяют студентам не только получать знания по истории, но и ощущать себя участниками событий, связанных с их профессиональной деятельностью. Например, с помощью виртуальной реальности студенты могут побывать в блокадном Ленинграде и на Дороге жизни. Стоимость устройства HOMiDO варьируется от 4500 до 5000 рублей.

В 2019 году госкорпорация Ростех представила на форуме «Армия2019» комплекс учебно-тренировочных средств, включающий в себя первые очки виртуальной реальности для военных.

Это устройство является частью системы обучения военных в виртуальной среде. Благодаря ему военнослужащие могут практиковаться в условиях, максимально приближенных к реальным, и развивать навыки, необходимые для работы с техникой.

Комплекс разработан российскими специалистами на основе отечественных технологий. Он может использоваться не только в виртуальной, но и в дополненной и смешанной реальности.

Однако стоит отметить, что некоторые современные ИТ-решения могут быть дорогостоящими, что может повлиять на стоимость обучения. Тем не менее, рынок устройств предлагает продукты, которые можно использовать вместе со смартфонами. Это более доступный вариант, но он всё ещё может быть полезен для обучения студентов.

В настоящее время у большинства студентов есть доступ к интернету через смартфоны, что упрощает использование VR-технологий.

Анализ мировых тенденций в области информационных технологий, обучения иностранных военнослужащих и рынка устройств виртуальной и дополненной реальности показывает необходимость внедрения VR-технологий в систему обучения студентов военных учебных центров. Это позволит вывести процесс обучения на новый уровень и предоставить новые возможности для студентов.

Кроме того, опыт гражданских университетов показывает, что внедрение таких технологий может увеличить число студентов, успешно освоивших программу обучения.

Исследование, проведённое в 2015 году в Петрозаводском государственном университете, показало эффективность использования виртуальной реальности для обучения. В ходе исследования было создано пять обучающих программ, которые адаптировали для демонстрации через шлемы Z800 и Oculus Rift Development Kit 2.

Студенты, которые ранее показывали результаты ниже среднего, после изучения материала с помощью виртуальной реальности давали на 40-50% больше правильных ответов по сравнению с контрольной группой. А студенты с высокими результатами показали абсолютные результаты тестирования в 100%.

Другое исследование, проведённое в Китае, показало, что использование VR-технологий влияет на академическую успеваемость, эффективность усвоения материала и долговременную память студентов.

Испытуемые были разделены на четыре группы по 10 человек в каждой. Первые две группы изучали материал с помощью VR-технологий, а вторые — традиционным способом.

После обучения группа, которая использовала VR-технологии, продемонстрировала результаты на 27% выше, чем группа, которая изучала материал традиционным способом. Повторные тесты также показали преимущество VR-группы.

Таким образом, использование информационных технологий в обучении способствует более эффективному усвоению материала, делает процесс обучения более наглядным и доступным. Кроме того, это позволяет использовать тренажёры, которые ранее были недоступны из-за высокой стоимости учебных пособий и военной техники.

Внедрение VR-технологий в обучение также поможет подготовить для военной службы профессионалов, которые будут хорошо разбираться в современных информационных технологиях. Это особенно важно в условиях развития военного потенциала России в современном мире.

Список литературы

1. Зимина О.В. Дидактические аспекты информатизации образования // Вестник Московского университета. Серия 20. – 2005. – № 1. – С. 17-66.

2. Вилотиевич М. От традиционной к информационной дидактике // Вестник Московского университета. Серия 20. Педагогическое образование. – 2003. – № 1. – С. 46-48

3. Сиренко С.Н. Качество университетского образования в контексте междисциплинарного диалога естественно-математических и гуманитарных наук // «Университетское образование: опыт тысячелетия, проблемы, перспективы развития: тезисы докладов II международного Конгресса, 14-16 мая 2008 г. В 2 т. Т.2 / отв. ред. Р.С. Пионова. – Минск, МГЛУ, 2008. С. 88-91

4. Приказ Министра Обороны РФ от 15 сентября 2014 г. № 670 «О мерах по реализации отдельных положений статьи 81 Федерального закона от 29 декабря 2012 г. № 273-ФЗ “Об образовании в Российской Федерации”»

5. Санжаева Р.Д. Готовность и ее психологические механизмы // Вестн. Бурятского гос. ун-та. 2016.№ 2. С. 6-16.

ОСОБЕННОСТИ ПРИМЕНЕНИЯ ОБРАЗОВАТЕЛЬНЫХ ТЕХНОЛОГИЙ XXI ВЕКА В ВОЕННОМ ВУЗЕ: АКТУАЛЬНОСТЬ И ПЕРСПЕКТИВЫ

Мисюрин И.В.
Федеральное государственное бюджетное образовательное учреждение высшего образования «Оренбургский государственный университет», г. Оренбург

Аннотация: В статье рассматриваются актуальные вопросы, связанные с использованием современных технологий в военном обучении. В современном мире военная подготовка требует постоянного совершенствования и современные технологии играют ключевую роль в этом процессе. Статья фокусируется на выявлении вызовов и возможностей, которые эти технологии предоставляют для улучшения военной подготовки.

Ключевые слова: образовательные технологии, технология развития критического мышления, проектная технология, технология интегрированного обучения, методы дифференцированного обучения, военно-профессиональная среда.

Процесс обучения в высшем учебном заведении занимает особое место в системе образования. Цель любого вуза — подготовка высококвалифицированных специалистов, настоящих профессионалов своего дела.

Особое внимание следует уделить военным вузам, поскольку в современном мире от качества подготовки специалистов зависит будущее страны.

Методы и подходы к обучению играют ключевую роль в подготовке кадров, военных специалистов и инженеров.

В условиях современного мира, включая проведение специальной военной операции, государство нуждается в высококвалифицированных специалистах, которые соответствуют требованиям теории и практики вооружённого конфликта. Эти специалисты должны быть готовы постоянно учиться и развиваться на протяжении всей своей карьеры.

Они должны уметь управлять войсками в бою и в мирное время, а также обучать, воспитывать и психологически подготавливать личный состав. Кроме того, они должны быть способны изучать, эксплуатировать и применять сложные системы вооружения и военной техники.

Каждый курсант, обучающийся в военном учебном заведении, должен развивать свои исследовательские навыки и уметь быстро адаптироваться к изменяющимся условиям жизни и службы. Также важно, чтобы они могли эффективно выполнять задачи различной сложности.

Для достижения этих целей в военных вузах необходимо использовать современные образовательные технологии. Эти технологии позволяют формировать у обучающихся знания, умения и навыки, характерные для выбранной профессии и направления деятельности.

При выборе педагогических технологий для высших учебных заведений необходимо учитывать особенности каждой образовательной организации. Однако, независимо от специфики вуза, существуют определённые технологии, которые обеспечивают качественное обучение по различным направлениям и специальностям.

Среди основных современных педагогических технологий можно выделить:

1. Технология развития критического мышления.
2. Проектная технология.

В контексте образовательных методов, используемых в военных учебных заведениях, можно выделить несколько ключевых направлений:

1. Метод развивающего обучения.
2. Методы, направленные на поддержание здоровья.
3. Игровые методы.
4. Модульный метод.
5. Метод мастерских.
6. Кейс-метод.
7. Метод интегрированного обучения.
8. Педагогика сотрудничества.
9. Методы дифференцированного обучения.
10. Групповые методы.
11. Традиционные методы.

Среди многообразия образовательных методов, применяемых в военных учебных заведениях, особое внимание стоит уделить тем, которые активно используются в процессе обучения.

Метод развития критического мышления — это подход, который позволяет студентам самостоятельно анализировать информацию, выявлять закономерности и развивать критическое мышление.

Применение этого метода особенно важно для будущих военных специалистов, так как им необходимо уметь критически оценивать информацию и выделять главное из большого объёма данных.

Метод проектов – это подход, который играет важную роль в подготовке высококвалифицированных специалистов в технических и военных учебных заведениях.

В основе метода проектов лежат следующие принципы:

1. Акцент на студенте.
2. Обучение через деятельность, которая имеет личный смысл для ученика.
3. Сбалансированное развитие основных функций студента.
4. Глубокое усвоение базовых знаний за счёт их применения в различных ситуациях.

С точки зрения образовательной методологии, метод проектов включает в себя исследовательские, поисковые и проблемные методы, которые сами по себе являются творческими.

Применение метода проектов позволяет студентам самостоятельно конструировать свои знания, ориентироваться в информационном пространстве, развивать критическое мышление и прогнозировать результаты.

В военном учебном заведении метод проектов тесно связан с военно-научным обществом, в котором состоит большое количество студентов. Благодаря методу проектов студенты могут наглядно увидеть применение теоретических знаний на практике. Каждый проект представляет собой научную работу, в которой будущие военные инженеры рассматривают реальные примеры.

Среди всех перечисленных методов особое место занимает метод интегрированного обучения. Название «интегрированный» связано с тем, что процесс интеграции (от лат. Integratio — соединение, восстановление) предполагает объединение различных элементов в единую систему на основе их взаимозависимости и взаимодополняемости.

Интеграция содержания в обучении — это процесс установления связей между различными элементами содержания в рамках образовательной системы с целью формирования целостного представления о мире и развития личности.

Уникальность применения метода интегрированного обучения в военном учебном заведении заключается в том, что каждая дисциплина, преподаваемая обще академическими кафедрами, тесно связана с военными дисциплинами, которые изучаются на старших курсах.

Интегрированное обучение предоставляет возможности для развития и служит мотивацией для активизации процесса обучения.

Специфика военного учебного заведения диктует особые условия и требования к организации и проведению занятий, которые меняются в зависимости от курса обучения. Чем выше курс, тем сложнее применять традиционные подходы и методы обучения.

Благодаря разнообразию подходов к образовательному процессу, в военном учебном заведении можно применять и адаптировать основные

педагогические технологии, которые не противоречат основным принципам дидактики и педагогики.

Анализируя некоторые из используемых педагогических технологий, можно сделать вывод, что все они направлены на подготовку высококвалифицированных специалистов. Учитывая растущие требования к выпускникам военных учебных заведений, становится очевидным необходимость разработки новой стратегии высшего военного образования. Эта стратегия должна использовать педагогические технологии в воспитательно-образовательном процессе, чтобы восстановить баланс в работе механизмов самоорганизации участников процесса.

Таким образом, в современном мире, где знания быстро устаревают, а военные специалисты должны непрерывно повышать свою квалификацию, применение образовательных технологий XXI века в военном вузе становится всё более актуальным. Это связано с необходимостью адаптации к новым условиям военно-профессиональной среды и быстрым освоением новейших информационных технологий.

Перспективы применения образовательных технологий XXI века в военном вузе включают:

1. Повышение уровня профессиональной и личностной подготовки курсантов. Технологии помогают не только получить знания, но и развить логическое мышление, коммуникативные навыки и компетентность.
2. Построение индивидуальных образовательных траекторий для каждого курсанта. Это позволяет учитывать индивидуальные особенности каждого обучающегося и создавать персонализированный учебный процесс.
3. Подготовка будущих офицеров к выполнению служебно-боевых задач в условиях постоянных изменений. Курсанты учатся самостоятельно осваивать новую информацию, овладевать высокотехнологичными видами вооружения и техники, а также развивают навыки, необходимые для выполнения служебных задач.

Список литературы

1. Зимина О.В. Дидактические аспекты информатизации образования // Вестник Московского университета. Серия 20. – 2005. – № 1. – С. 17-66.

2. Вилотиевич М. От традиционной к информационной дидактике // Вестник Московского университета. Серия 20. Педагогическое образование. – 2003. – № 1. – С. 46-48

3.Сиренко С.Н. Качество университетского образования в контексте междисциплинарного диалога естественно-математических и гуманитарных

наук // «Университетское образование: опыт тысячелетия, проблемы, перспективы развития: тезисы докладов II международного Конгресса, 14-16 мая 2008 г. В 2 т. Т.2 / отв. ред. Р.С. Пионова. – Минск, МГЛУ, 2008. С. 88-91

4.. Приказ Министра Обороны РФ от 15 сентября 2014 г. № 670 «О мерах по реализации отдельных положений статьи 81 Федерального закона от 29 декабря 2012 г. № 273-ФЗ “Об образовании в Российской Федерации”»

5. Санжаева Р.Д. Готовность и ее психологические механизмы // Вестн. Бурятского гос. ун-та. 2016.№ 2. С. 6-16.

ВЛИЯНИЕ НОВЕЙШИХ ТЕНДЕНЦИЙ В РАЗВИТИИ ТЕХНОЛОГИЙ И СРЕДСТВ ВООРУЖЕННОЙ БОРЬБЫ НА ВОЕННОЕ ИСКУССТВО

Невзоров С.Г., к.и.н., доцент
Федеральное государственное бюджетное образовательное учреждение высшего образования «Оренбургский государственный университет», г. Оренбург

Аннотация: научно-технический прогресс в сфере создания нового и более эффективного вооружения и военной техники не стоит на месте. Исторический анализ показывает, что развитие вооружения, военной техники, боеприпасов происходило в тесной связи с общим прогрессом цивилизации.

В свою очередь развитие средств вооруженной борьбы в конечном итоге приводит к изменениям в тактике и оперативном искусстве. Методы и способы ведения войн за всю историю человечества претерпели сильные изменения. Все большее развитие получают системы дистанционного поражения противника, такие как баллистические ракеты, системы и комплексы ВТО. Дальность поражения все больше увеличивается, заставляя также совершенствовать средства защиты. Кроме того, современная геополитическая обстановка в мире не дает вести войны исключительно военными средствами.

Ключевые слова: военное искусство, глобализация, революция в военном деле, стратегия, оперативное искусство, тактика, информационно-коммуникационные технологии, робототехника, мобильность, избирательность, высокоточное оружие, ядерное оружие.

В современном мире происходит трансформация международных отношений под влиянием масштабных изменений в различных сферах жизни общества. Это касается не только политики, экономики и социальной сферы, но и науки, технологий и инноваций.

В последние десятилетия наблюдается стремительное развитие информационно-коммуникационных и биотехнологий, а также совершенствование микроэлектроники и робототехники. Это не только меняет повседневную жизнь людей, но и оказывает значительное воздействие на военное дело.

Современные военные теоретики пытаются осмыслить эти изменения, но влияние новых технологий на соотношение различных компонентов военного искусства, таких как стратегия и тактика, всё ещё недостаточно изучено.

В современных условиях военная сила остаётся важным инструментом внешней политики многих государств, особенно тех, которые занимают ведущее

положение на международной арене. Применение военной силы становится всё более многомерным и многоплановым.

В международных отношениях всё большую роль играет угроза военных конфликтов на всех уровнях военного искусства: стратегическом, оперативном и тактическом.

Вооружённая борьба в войнах, операциях по принуждению к миру и миротворческих операциях тесно связана с активными действиями в информационно-пропагандистской сфере, включая «психологическую войну», дипломатией и различными экономическими мерами.

Всё большее значение приобретает противостояние в киберпространстве, включая проведение боевых кибероперациий и нанесение кибераударов. Это усложняет процессы стратегического управления и распределения усилий, связанных с применением военной силы для достижения политических целей.

Многие страны становятся более чувствительными к внешним воздействиям из-за своей экономической взаимозависимости. Одной из новых черт мировой экономики в условиях глобализации является резко возросшая скорость возникновения и распространения кризисов на финансовых рынках, которые могут быть вызваны военными действиями различного масштаба и интенсивности в разных регионах мира.

Глобализация — это долговременный процесс, который начался в конце XIX века и ярко проявился в двух мировых войнах XX века. Военные действия развернулись в глобальном масштабе, охватив все континенты и ведущие государства того времени.

В современной системе мировой политики важным вопросом является избирательность или неизбирательность применения тех или иных сил и средств. Использование военной силы с значительным «сопутствующим ущербом» может привести к дополнительному осуждению таких действий во многих странах. В некоторых случаях наличие значительного «сопутствующего ущерба» может вызвать обратный политический эффект.

Среди актуальных тенденций в области вооружённых конфликтов стоит выделить значительное усиление роли информационно-коммуникационных технологий, новые возможности радиоэлектронной борьбы, а также автоматизацию ударных и вспомогательных систем. Наиболее заметными примерами этого являются растущее использование беспилотных разведывательно-ударных комплексов и средств стратегической, оперативной и тактической мобильности. Эта тенденция наблюдается уже несколько десятилетий и, вероятно, сохранится в будущем.

Современные технологии играют важную роль в обработке информации и разведданных из различных источников, включая данные, полученные от

спецслужб разных ведомств и находящиеся в открытом доступе. Они также используются для целеуказания, контроля обстановки и деятельности собственных соединений, частей и подразделений.

В последние годы всё более актуальным становится вопрос о проведении научно-исследовательских и опытно-конструкторских работ по созданию квантовых компьютеров в некоторых странах. Эти машины будут основаны на принципиально новой научно-технической основе и станут важным инструментом в будущем.

Многие российские эксперты, справедливо отмечают, что боевые действия войск остаются основной формой ведения войны.

В современных условиях становится возможным комплексное воздействие на противника одновременно в воздушно-космическом пространстве, на суше и на море, а также в информационной сфере. Это позволяет атаковать противника на всю глубину его территории или оперативную структуру его сил с разных направлений.

Для успешного проведения операции требуется высокий уровень профессионализма и способность сочетать различные компоненты. Одним из ключевых условий эффективности операций является их логическая и временная структура — чёткое определение последовательности этапов, упорядоченных по степени важности.

В то же время растёт потребность в многовариантном планировании операций и гибкости реализации планов в зависимости от меняющейся ситуации.

В современных условиях операции могут проводиться с привлечением меньшего количества войск, чем это было во время Великой Отечественной войны и предполагалось военной теорией в послевоенные годы.

Анализируя тенденции развития современного оперативного искусства, можно отметить, что в нём наблюдается постепенный отказ от использования традиционных группировок войск, состоящих из фронтов, армий и армейских корпусов. Вместо этого наметился переход к смешанным (комбинированным) группировкам, включающим в себя силы и средства всех правоохранительных органов страны как на стратегических континентальных направлениях, так и на стратегических и оперативных направлениях.

В современных условиях операции должны быть не просто результатом творческой деятельности полководца, но и результатом тщательного анализа и планирования, основанного на научных знаниях.

В условиях многомерных политических, экономических, информационных и социокультурных реалий применение военной силы требует не только стратегического, но и оперативного управления.

В настоящее время и военная стратегия, и политика могут ставить задачи по проведению операций, даже с использованием небольших контингентов войск (сил), таких как несколько батальонов и сопоставимое количество ударных авиационных средств, средств ПВО и военно-морских сил.

В современных условиях действия отдельной группы специального назначения, роты или батальона могут оказаться в центре внимания высшего руководства страны. Их успех или неудача могут привести к значительным политическим результатам — как положительным, так и отрицательным. В этой связи важно снова обратить внимание на контроль как на важный компонент управления.

В Соединённых Штатах Америки в последнее время всё большую популярность среди военных приобретает концепция «операций на основе эффектов». Эти операции должны проводиться объединёнными группами войск.

Использование информационных технологий для ускорения разведки, адекватного планирования сил на удалённом театре военных действий, сокращения времени переброски войск и планирования операций позволяет значительно изменить характер современного военного искусства.

Сегодня мобильность становится преобладающим принципом ведения войны. Этот принцип проявляется в действиях вооружённых сил разных стран. Мобильность важнее, чем заблаговременное сосредоточение сил на направлении главного удара, а в некоторых случаях даже заменяет его.

В современной войне без сплошных линий фронта и с многоочаговостью боевых действий возрастает роль сил и средств специальных операций. Эти силы берут на себя задачи, которые раньше выполняли сухопутные войска. В частях спецназа особенно ценится каждый боец, что является важной характеристикой современного военного дела. В связи с этим необходимо ввести в наставления и боевые уставы понятие специальных операций как нового вида боевых действий.

В последнее время значительно возросла роль различных средств ведения боя и операций. Это связано с использованием беспилотных летательных аппаратов для разведки и нанесения ударов, а также с применением космических и воздушных средств разведки, связи и целеуказания. Кроме того, вертолёты и самолёты используются для переброски войск и десантирования.

Высококачественный «человеческий капитал» также необходим для разведки — как военной, так и политической. Последняя играет важную роль в обеспечении обороноспособности и национальной безопасности страны.

Особое внимание следует уделить роли космического пространства в вооружённой борьбе. Многие аспекты этой борьбы требуют детального изучения с учётом не только военно-технических, но и политических и правовых факторов. Необходимо учитывать долгосрочные тенденции в развитии

противоспутниковых средств, которые актуальны с конца 1950-х годов и до сих пор не получили однозначной оценки.

В современных условиях, как и на предыдущих этапах развития военного дела, новейшие технологии сосуществуют с традиционными, характерными для «дореволюционного периода», но с существенным добавлением современных технологий. Это касается, в частности, танков и других боевых бронированных машин, авианосцев и т.д.

Всё более важным аспектом последней революции в военном деле стало активное развитие разнообразных нелетальных видов оружия, которое используется в самых разных невоенных действиях армии и других силовых структур. Это оружие имеет большой потенциал применения в военных конфликтах, когда возникает угроза дестабилизации тыла со стороны различных организаций без применения боевого оружия.

Прорывные достижения в области информационных технологий позволили обнаруживать противника и избирательно уничтожать его с помощью высокоточного оружия с неядерными боеприпасами. При этом боевые платформы — корабли и самолёты — могут находиться на расстоянии сотен и даже тысяч километров от места боевых действий.

Для современного и перспективного военного искусства характерен возврат к избирательному применению сил и средств. Это не означает полного отказа от сопутствующего ущерба. Одновременно наблюдается стремление максимально защитить свои войска, снизить собственные потери и обеспечить более благоприятные условия для применения военной силы на всех уровнях — стратегическом, оперативном и тактическом.

Для России вопрос об использовании военной силы как напрямую, так и косвенно остаётся крайне актуальным. Речь идёт о предотвращении различных видов агрессии против Российской Федерации или её союзников, а также о надёжном ядерном и неядерном (пред ядерном) стратегическом сдерживании. Для этого необходимо тщательно определять политические цели военной стратегии и задачи на оперативном уровне.

Ядерное сдерживание остаётся наиболее заметной формой невоенного применения военной силы, а для России оно играет особую роль. Не менее важным для обеспечения национальной безопасности нашей страны является стратегическое неядерное сдерживание, особенно с использованием обычных высокоточных дальнобойных средств поражения. Тезис о неядерном стратегическом сдерживании был обоснованно включён в новую редакцию Военной доктрины Российской Федерации, опубликованную в декабре 2014 года.

Нельзя не упомянуть весь комплекс проблем надёжного и стабильного управления. Это одно из ключевых требований современного военного искусства, в частности, эффективного политического управления (включая контроль) на всех уровнях использования военной силы.

Сегодня связь и системы управления (включая контроль) должны быть непрерывными, а не дискретными, от высшего политического уровня до уровня исполнителей. Это сложная, трудоёмкая и ресурсоёмкая задача, требующая больших средств, новых технических решений и, самое главное, изменения мышления и психологии значительной части командования. Всё это справедливо и в отношении политического управления применением военной силы на различных уровнях военного искусства.

Список литературы

1. Балахонцев Н., Мединн А. Развитие форм и способов ведения военных действий в начале XXI века // Зарубежное военное обозрение. 2003. № 4. С. 25–26.

2. Буренок В.М. Технологические и технические основы развития вооружения и военной техники. М.: Граница, 2010.

3. Буренок В.М., Гладышевский В.Л. Информатика и вычислительная техника: перспективы развития и применения в военном деле // Вооружение и экономика. 2015. № 3. С. 17–32.

4. Буренок В.М., Ивлев А.А, Корчак В.Ю. Развитие военных технологий XXI века: проблемы, планирование, реализация. Тверь: Купол, 2009.

5. Велихов Е.П., Кокошин А.А., Сагдеев Р.З. Космическое оружие: дилемма безопасности. М.: Мир, 1986.

6. Воробьев И.Н., Киселев В.А. Отечественная военная теория: история и современность // Военная мысль. 2010. № 3. С. 43–49.

7. Воробьев И.Н., Киселев В.А. Эволюция принципов военного искусства // Военная мысль. 2008. № 8. С. 2–8.

АКТУАЛЬНЫЕ ПРОБЛЕМЫ БЕЗОПАСНОСТЬ БЕСПИЛОТНЫХ АВИАЦИОННЫХ СИСТЕМ: АНАЛИЗ УГРОЗ И ЗАЩИТА

Парфёнов Д.И., к.т.н., Парфенов А.И.
Федеральное государственное бюджетное образовательное учреждение высшего образования «Оренбургский государственный университет», г. Оренбург

Аннотация: настоящая работа посвящена исследованию проблем информационной безопасности в сетях беспилотных летательных аппаратов. Особое внимание уделено двум основным категориям угроз: атакам на конфиденциальность и атакам на целостность данных. Проведён сравнительный анализ известных моделей угроз, адаптированных к условиям функционирования сетей БПЛА, выделены ключевые особенности и ограничения существующих методик моделирования безопасности. Представленная в статье модель угроз направлена на выявление слабых мест и потенциальных уязвимостей систем управления БПЛА, определение вероятных способов осуществления атак и разработка рекомендаций по повышению устойчивости сети к внешним воздействиям.

Ключевые слова: беспилотный летательный аппарат, угрозы, безопасность

Технологии продвинулись вперед, и в результате в современном мире произошел ряд новаторских разработок. Было продемонстрировано, что эти результаты более надежны, доступны и экономичны в нашей повседневной жизни. Кроме того, беспилотные летательные аппараты (БПЛА) используются как в коммерческих, так и в личных целях, в дополнение к тому, что они широко используются в военном контексте. По оценкам индустрии В 2025 году российский рынок беспилотных авиационных систем (БАС) продолжает активный рост до 35,9 млрд рублей в 2025 году.

Наиболее распространенными типами дронов являются мультикоптеры и беспилотные вертолеты, применяемые преимущественно для мониторинга и сбора данных. Использование дронов растет из-за их ценности в различных работах, в том числе для прямой трансляции событий, съемки видео с воздуха, мобильности для перемещения посылок из одного места в другое и простой навигации. Эти дроны обычно используются в транспортных целях из-за их дешевых требований к обслуживанию, способности взлетать и приземляться вертикально, способности зависать и высокой степени мобильности [1]. Эти дроны часто оснащаются компьютерным зрением и функциями, подобными Интернету вещей (IoT), особенно для роя дронов, и они оказались эффективным выбором для миссий, связанных с наблюдением и спасением [2]. Однако есть

несколько важных элементов, которые связаны с проблемами безопасности БПЛА. Основным вопросом безопасности является контроль сигналов управления и навигации. Использование дронов быстро расширяется, и в то же время вопросы безопасности и конфиденциальности стали более сложными и серьезными.

Большинство существующих исследований в области моделирования безопасности и угроз ориентированы на низкоуровневую системную перспективу и главным образом сосредотачиваются на факторах возникновения и способах предотвращения компьютерных атак. Однако основной недостаток такого подхода заключается в однотипности задаваемых вопросов: какими являются слабые места исследуемой системы, каким образом возможно избежать атакующих воздействий и насколько эффективно можно минимизировать угрозу [3]. Между тем, гораздо продуктивнее представляется использование метода причинно-следственного анализа, позволяющего выявить глубинные причины снижения производительности или сбоев функционирования отдельных подсистем и оценить последствия потенциальных нападений на способность всей системы успешно исполнять возложенные на нее миссии и задачи.

Типичные сети БПЛА характеризуются наличием трёх основных типов коммуникационных каналов, различающихся типом передаваемой информации. Они включают радиосвязь, временные интервалы которой варьируются от двух до пяти минут. В указанный промежуток времени ракеты способны покинуть зону покрытия датчиков БПЛА, особенно если траектория их полёта направлена противоположно курсу движения беспилотника. Именно поэтому передача данных в сетях слежения за баллистическими ракетами реализуется посредством гибридных беспроводных сенсорных сетей, соответствующих высоким стандартам доступности и защищённости.

Приведенный пример наглядно иллюстрирует критичность временных ограничений для приложений, связанных с БПЛА, подчеркивая значимость надёжности и безопасности каналов связи. Вопрос габаритов и мобильности оборудования также заслуживает внимания: миниатюрные БПЛА, сопоставимые размерами с колибри, были созданы и введены в эксплуатацию [4]. Такие компактные устройства обладают уникальными возможностями, открывающими новые горизонты в области исследования и эксплуатации воздушных пространств.

Несмотря на значительный объём научных трудов, посвящённых вопросам моделирования безопасности в различных типах беспроводных сетей, включая сенсорные и мобильные ad hoc сети, предложенные модели оказываются неприменимыми к классическим сетям БПЛА. Их сложность обусловлена

множеством факторов, отсутствующих в традиционных системах связи. Отличительными особенностями сетей БПЛА являются наличие разнородных каналов коммуникации, значительные различия в дистанции передачи сигнала (краткосрочная/долгосрочная связь), разнообразные требования к источникам питания, разнообразие форматов передаваемых данных (командные сигналы, видео-, аудиопотоки, изображения), строгие условия к обеспечению конфиденциальности и целостности информации. Эти характеристики существенно усложняют разработку эффективных методов обеспечения информационной безопасности в сетях БПЛА по сравнению с иными существующими сетевыми структурами.

Следует отметить, что особое внимание к вопросам безопасности коммуникаций не являлось центральным элементом большинства исследовательских проектов, посвящённых сетям беспилотных летательных аппаратов. Тем не менее, анализ рисков и угроз представляет собой значимый компонент общей стратегии обеспечения безопасности системы, так как помогает своевременно выявлять её уязвимые звенья. Предпринимаются усилия по разработке модели угроз, характерных для систем БПЛА, а также определению путей реализации потенциально возможных атак, исходящих от этих угроз. Такой подход направлен на создание комплексного представления о рисках, возникающих в процессе эксплуатации сетей БПЛА, и выработку мер противодействия таким угрозам.

В рамках настоящего исследования разработана модель угроз кибербезопасности беспилотных летательных аппаратов. Безопасность сетей БПЛА обеспечивается путём идентификации и устранения потенциальных угроз. Предлагаемая модель угроз состоит из двух крупных категорий: атака на конфиденциальность и атака на целостность. Рассмотрим их более подробно.

1. Атаки на конфиденциальность

Атаки на конфиденциальность связаны с несанкционированным доступом к информации и перехватом данных. Основными компонентами системы, подверженными этому типу атак, являются: беспилотный аппарат; система управления полётом (СУП); канал связи; человеческие субъекты.

Определим угрозы, характерные для СУП: компьютерные вирусы; троянские программы; кейлоггеры; другое вредоносное программное обеспечение. Злоумышленники могут внедрить вредоносный код в программное обеспечение СУП, получив доступ к командам управления и полетным параметрам БПЛА. Важно учитывать, что угроза программного характера распространяется и на саму конструкцию аппарата, однако степень воздействия ниже, чем на СУП.

Определим угрозы, характерные для каналов связи: взлом, подслушивание, Спуфинг (подмена личности), межуровневые атаки, многопротокольные атаки. Эти атаки специфичны для конкретных каналов связи и представляют серьёзную опасность для безопасности передачи данных. Например, в канале радиосвязи возможно прослушивание или фальсификации сообщений. Необходим тщательный анализ риска каждой возможной атаки для выбора адекватных защитных мер.

Современные социальные и деловые сети порождают дополнительные опасности, связанные с социальной инженерией, фишингом, манипуляциями поведением пользователей и целенаправленным воздействием на персонал.

2. Атаки на целостность

Цель атак на целостность – внесение изменений в существующий поток данных либо подделка нового потока информации. Целостность системы нарушается двумя путями:

– изменение данных во время передачи или хранения;

– добавление ложных данных.

Возможные источники угроз целостности:

– природные явления (например, молнии, солнечная активность);

– внешние угрозы воздушным средствам связи (глушение сигналов, искажение, перехват и анализ сигнала).

Природные события редко вызывают потерю целостности, и современные протоколы и оборудование хорошо справляются с такими ситуациями. Гораздо большую опасность представляют умышленные атаки, направленные на разрушение сигнала или получение несанкционированного доступа к нему.

Атаки на целостность включают:

– глушение: создаёт препятствия для нормального приема сигналов;

– нарушение целостности сигнала: намеренное снижение соотношения сигнал-шум, приводящее к снижению качества сигнала;

– перехват сигнала: подразумевает глубокое понимание структуры передаваемого сигнала, частоты и диапазонов.

Особое внимание уделяется классу атак, связанным с модификацией данных внутри самой системы, включая использование эксплойтов (использования уязвимостей в программном обеспечении). Вероятность успешной атаки на систему беспилотных летательных аппаратов снижается при введении необходимых мер безопасности, тогда как последствия атаки остаются стабильными независимо от наличия защит. Результаты анализа рисков представлен в таблице 1.

Таблица 1 – Результаты анализа рисков

Угроза	Алгоритм	Вероятность	Влияние	Риск
Глушение		3	1	3
Шифрование/Искажение		2	1	2
Подслушивание		3	2	6
Атаки между уровнями		2	1	2
Многопротокольная атака		2	1	2
Социальная инженерия		3	2	4
Спуфинг	Список устройств	3	3	9
	X.509	2	3	6
Управление и контроль	Без MAC	3	3	9
	SHA-1 MAC	3	3	6
	AES MAC	1	3	3
Модификация трафика данных	Без AES	3	1	3
	С AES	1	1	1
DoS на БПЛА	EAP/SHA-1/AES/MAC	3	3	9
Целостность сигнала		3	2	6
Эксплойт подпрограмм		1	3	3
Вирусы, вредоносное ПО		3	2	6

Результаты проведенного анализа показали следующую градацию уровней риска:

– значения риска менее 3: контрмеры не обязательны;

– значения риска 3 или 4: необходимо серьёзно отнестись к угрозе;

– значения риска 6 или 9: угроза признана критической и подлежит устранению в первоочередном порядке.

Стоит подчеркнуть, что подобная классификация носит субъективный характер и зависит от конкретного анализа и имеющихся сведений о состоянии системы. Из приведённой таблицы ясно, что уменьшение вероятности наступления инцидента автоматически ведет к уменьшению общего показателя риска.

Список литературы

1. Li Y. et al. Performance analysis for covert communications under faster-than-Nyquist signaling //IEEE Communications Letters. – 2022. – Т. 26. – №. 6. – С. 1240-1244.

2. Zhang W. et al. Unknown input observer-based appointed-time funnel control for quadrotors //Aerospace Science and Technology. – 2022. – Т. 126. – С. 107351.

3. Challita U. et al. Machine learning for wireless connectivity and security of cellular-connected UAVs //IEEE Wireless Communications. – 2019. – Т. 26. – №. 1. – С. 28-35.

4. Gaspar J. et al. Capture of UAVs through GPS spoofing using low-cost SDR platforms //Wireless Personal Communications. – 2020. – Т. 115. – №. 4. – С. 2729-2754.

ИНТЕГРИРОВАННЫЕ ИНФОРМАЦИОННЫЕ СИСТЕМЫ – ОСНОВА УПРАВЛЕНИЯ СТРОИТЕЛЬНЫМ ПРОИЗВОДСТВОМ

Турамуратова Н.К., Пищухин А.М., д-р техн. наук, профессор
Федеральное государственное бюджетное образовательное учреждение высшего образования «Оренбургский государственный университет»

Аннотация: В статье исследуется роль интегрированных информационных систем в повышении эффективности управления строительным производством. Рассматривается многоуровневая архитектура управления, включающая стратегический, тактический и оперативный уровни. Особое внимание уделяется механизмам интеграции BIM, ERP, MES и систем управления проектами, обеспечивающим сквозной поток данных от стадии проектирования до непосредственного выполнения строительно-монтажных работ. Анализируются практические аспекты внедрения таких систем и их влияние на производительность труда, сокращение сроков строительства.

Ключевые слова: информационные системы, технологический процесс, механизмам интеграции, управление проектами

Современное строительное производство характеризуется высокой сложностью технологических процессов, необходимостью координации множества участников и жёсткими требованиями к срокам и качеству работ. Методы управления, основанные на разобщенных данных и бумажном документообороте, не обеспечивают необходимой эффективности производства, приводя к простоям техники, несвоевременной поставке материалов и низкой производительности труда.

Основным вопросом организации строительного производства является разрыв между стратегическим планированием, тактическим управлением и оперативной деятельностью на площадке. Решение этой проблемы видится в создании интегрированной информационной среды, объединяющей системы различных классов - ERP, BIM, MES и системы управления проектами [0].

Временные горизонты планирования включают в себя: стратегический, тактический и оперативный уровни.

Стратегический уровень ориентирован на долгосрочное планирование с временным диапазоном от 3 до 10 лет, здесь определяются генеральные направления развития, утверждаются инвестиционные программы и формируются целевые показатели деятельности строительного предприятия. Ключевыми инструментами данного уровня выступают корпоративные системы класса ERP (Enterprise Resource Planning), такие как SAP S/4HANA и 1C:ERP, которые обеспечивают консолидацию финансовой отчетности и оптимизацию ресурсного потенциала компании [0].

Тактический уровень охватывает средний по срокам период планирования, ограниченный временными рамками от 1 месяца до 3 лет. Основная задача данного уровня заключается в быстрой реализации стратегических установок через разработку детализированных проектных решений, формирование календарных графиков и обеспечение координации взаимодействия всех участников строительного процесса [3]. Для решения этих задач применяются специализированные системы проектного управления (Oracle Primavera P6, Microsoft Project) и платформы информационного моделирования (Autodesk Revit, Navisworks), которые обеспечивают интеграцию проектных данных и управление жизненным циклом объекта.

Оперативный уровень функционирует в краткосрочном временном горизонте, составляющем от одной рабочей смены до одного месяца. Деятельность на этом уровне сосредоточена на непосредственной организации строительно-монтажных работ, оперативном учете выполнения производственных заданий и управлении материально-техническими ресурсами в реальном времени. Технологическую основу данного уровня составляют системы MES (Manufacturing Execution Systems) и мобильные решения для автоматизации документооборота и контроля выполнения работ на строительной площадке.

Данная многоуровневая архитектура, которая обеспечивает согласованность управленческих решений на всех стадиях строительного производства, создавая условия для эффективного достижения стратегических, тактических и оперативных целей предприятия, представлена на рисунке 1 [1].

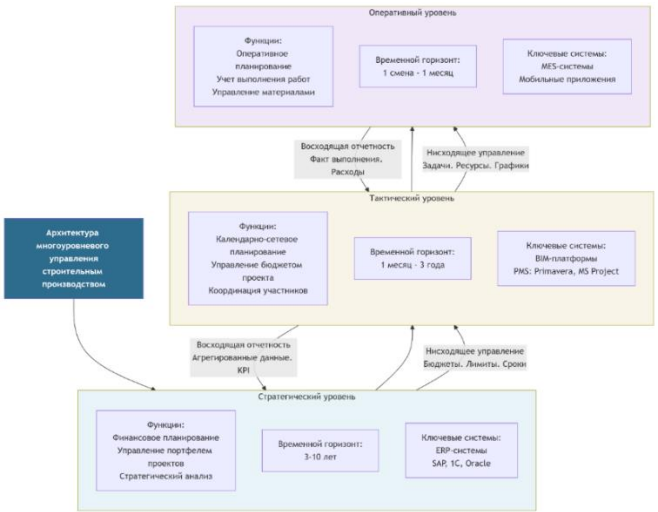


Рисунок 1 – Архитектура многоуровневого управления строительным производством

Эффективное взаимодействие между различными уровнями управления обеспечивается через систему интеграционных механизмов и технологий.

Облачные платформы CDE (Common Data Environment) выступают центральным хабом для хранения и обмена данными проекта. Такие платформы, как Autodesk Construction Cloud или Bentley SYNCHRO, обеспечивают единое пространство для работы всех участников проекта с актуальными версиями документов и моделей. Платформа CDE реализует принцип «единого источника истины», исключая возможность работы с устаревшими или противоречивыми данными.

Открытые стандарты данных играют основную роль в обеспечении совместимости между различными системами. Стандарт IFC (Industry Foundation Classes) позволяет передавать данные между различными BIM-приложениями, а формат COBie (Construction Operations Building information exchange) обеспечивает обмен информацией на этапе эксплуатации объекта. Использование открытых стандартов устраняет проблему технологической замкнутости отдельных систем.

Программные интерфейсы (API) обеспечивают автоматический обмен данными между системами в реальном времени. Современные API позволяют настраивать сложные сценарии взаимодействия, например, автоматическую передачу данных о выполнении работ из полевого приложения в систему управления проектами и далее в ERP-систему для учета затрат. Схема интеграции информационных систем представлена на рисунке 2 [4].

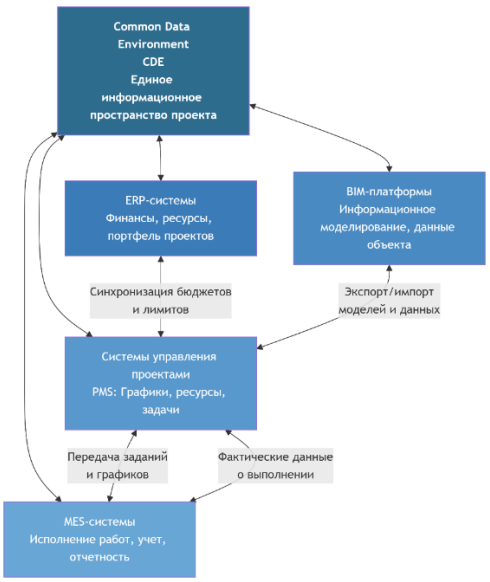


Рисунок 2 – Схема интеграции информационных систем через единую среду данных CDE

Специалистами компании «Проект-Центр» применялись российская BIM-платформа Renga в сочетании с программами Autodesk Revit и Allplan для разработки конструкций фундамента.

В рамках проекта была разработана информационная модель торгового комплекса, объединяющая архитектурные, конструктивные и инженерно-технические решения. Модель включала детализированные данные о применяемых материалах, технических спецификациях и объемах строительно-монтажных работ. Применение международного формата IFC обеспечило беспрепятственный обмен данными между различными программными средами. Информация от информационной модели (BIM) последовательно интегрировалась в систему управления проектами Oracle Primavera P6 и корпоративную ERP-систему SAP.

На основании полученных данных осуществлялось формирование заявок на материально-техническое обеспечение, заключались договоры с контрагентами и обеспечивалось целевое резервирование денежных активов. Согласованные бюджетные лимиты и графики поставок возвращались в систему управления проектами для последующего контроля. В рамках реализации проекта была обеспечена эффективная интеграция между платформой Renga и другими программами (Allplan, Navisworks), что позволило автоматизировать процесс бюджетного планирования и минимизировать вероятность ошибок.Информация о планируемых поставках материалов передавалась в систему MES, где производители работ посредством мобильных приложений осуществляли мониторинг графиков поставок и документальную фиксацию приемки материалов. Данные о ходе выполнения работ обновлялись в режиме реального времени.

В процессе возведения торгового комплекса применялось оборудование виртуальной реальности для трехмерной визуализации строительных процессов и заблаговременного выявления основных проблем, что способствовало недопущению срывов сроков выполнения работ. Фактические данные о выполнении строительных операций передавались в системы Primavera P6 и SAP, где руководители проектного отдела и финансовые менеджеры осуществляли мониторинг соответствия плановым показателям. При обнаружении расхождений система автоматически инициировала оповещения ответственных лиц. В реализации проекта компании «Проект-Центр» применение BIM-моделирования позволило сократить временные затраты на координацию и согласование на 90%, одновременно снизив количество ошибок в проектной документации на 40%. В простейшем случае рассмотренную методику можно свести к алгоритму, представленному на рисунке 3.

Интегрированные системы управления значительно повышают операционную эффективность. Руководители всех уровней получают доступ к актуальным данным в режиме реального времени, что обеспечивает полную прозрачность процессов. Автоматизация сбора и обработки информации сокращает время принятия решений на 40-60%. Цифровые платформы минимизируют ошибки, вызванные человеческим фактором, снижая их количество на 70-85%. Интеллектуальные алгоритмы аналитики выявляют отклонения на ранних стадиях, позволяя предотвращать сбои до их возникновения. Внедрение интегрированных систем сталкивается с многоуровневыми сложностями. Помимо существенных затрат на лицензии и внедрение, ключевыми барьерами становятся нежелание сотрудников осваивать новые процессуальные модели работы [5] и технические противоречия между различными платформами. Централизация данных требует усиления киберзащиты для блокирования потенциальных угроз.

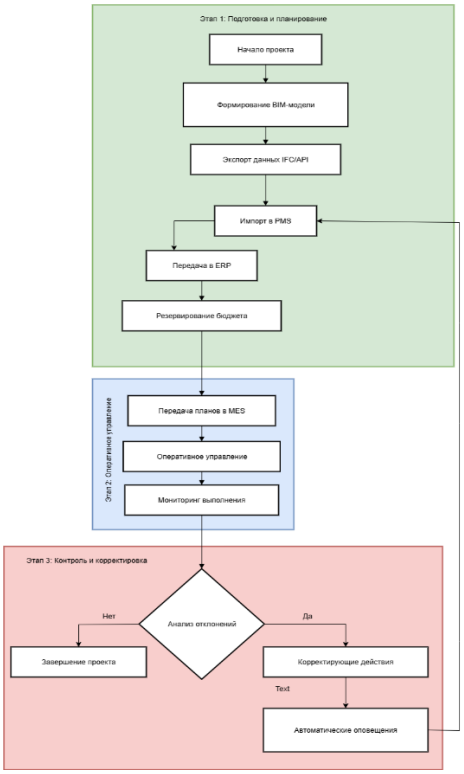


Рисунок 3 – Алгоритм управления строительным производством на основе интегрированных систем

Таким образом, современное строительное производство требует интеграции информационных систем (ERP, BIM, MES) для эффективного управления. Формирование единого информационного пространства обеспечивает сквозную передачу данных от стратегического планирования до

операционной деятельности на объекте. Несмотря на существенные инвестиции и организационно-технические сложности внедрения, преимущества интеграции демонстрируют многократную окупаемость. Ключевые эффекты включают повышение прозрачности процессов, ускорение принятия решений и улучшение качества управления, что непосредственно влияет на общую производительность строительства. Перспективы развития связаны с внедрением технологий искусственного интеллекта для прогнозной аналитики и использованием IoT-устройств для автоматизированного сбора данных. Данные направления позволяют создавать цифровые двойники объектов и реализовывать концепцию "Индустрии 4.0" в строительной отрасли.

Список литературы

1. Рязанов А.А. Управление проектами в строительстве / А.А. Рязанов // Молодой ученый. – 2020. – № 15(119). – С. 27-29.

2. Бадиков Д. Информационные системы управления строительным комплексом / Д. Бадиков, М. Кантарович//Строительная орбита, 2008. – № 5(12). – С. 14-17.

3. Кулешов И.В. Согласование процессов по вероятностным критериям качества с проектной симметризацией / И.В. Кулешов, Г.Ф. Ахмедьянова, А.М. Пищухин//Моделирование, оптимизация и информационные технологии, 2024. – Т. 12, № 1 (44). – С. 33.

4. Материалы по инвестиционному проекту строительства 6-ти этажного жилого дома в г. Оренбург : отчетная документация. – 2023. – 45 с. – Место хранения: Проектная организация «Проект-Центр», ООО СЗ «Ваш Дом» – Режим доступа: https://pro-center.pro/projects/kompleks-apartamentov-po-ul-9-yanvarya/

5. Моделирование процессов : монография / Г.Ф. Ахмедьянова, Т.А. Пищухина, А.М. Пищухин – Оренбург : ОГУ, 2024. – 162 с. – ISBN 978-5-7410-3332-6.

ИНФОРМАЦИОННАЯ ОБЕСПЕЧЕНИЕ УПРАВЛЕНИЯ ДЕЙСТВИЯМИ ПОЛЕВОГО ПЕРСОНАЛА ДОБЫВАЮЩЕГО ПРОМЫСЛА

Ломухин И.А., СПБГУ Пищухин А.М., д-р техн. наук, профессор
Федеральное государственное бюджетное образовательное учреждение высшего образования «Оренбургский государственный университет»

Аннотация: Представлена информационная система управления действиями полевого персонала добывающего промысла, позволяющая оптимизировать ресурсы, затрачиваемых на выполнение операционных задач по поддержке процесса добычи углеводородов на промысле добывающего предприятия.
Ключевые слова: добывающий промысел, система управления действиями персонала, оптимизация ресурсов, полевой персонал.

Сложившаяся в настоящий момент ситуация в добывающей отрасли характеризуется падающим качеством углеводородных запасов, высокой волатильностью цен и ростом непроизводительных потерь персонала предприятий, что приводит к непрерывному поиску дополнительных рычагов увеличения эффективности внутренних управленческих процессов. С другой стороны, наблюдается расширение географии и количества добывающих скважин, что непосредственно увеличивает риски снижения качества контроля за оборудованием и приводит к снижению уровня добычи углеводородов. Таким образом, отрасль испытывает потребность в применении высокотехнологичных инструментов для повышения эффективности добычи углеводородов на разрабатываемых месторождениях [1]. На текущий момент добывающий промысел должен представлять из себя высокотехнологичный комплекс программно-технических средств, включающий как элементы так называемой индустрии (или технологии) 4.0, так и специфические инструменты для выполнения производственных задач на опасном производстве [2]. На рисунке 1 проиллюстрирована концепция высокотехнологичного комплекса программно-технических средств для управления процессом добычи углеводородов.

Управление добывающим предприятием связано с решением множества нетривиальных задач [3-5]. Одной из таких задач является поиск оптимального набора действий сотрудника полевой службы при контроле добывающих скважин. Предлагаемый подход к решению такой задачи оптимизации использования трудовых и материальных ресурсов [6], затрачиваемых на выполнение

Рисунок 1 – Концепция высокотехнологичного комплекса программно-технических средств для интеллектуального управления процессом углеводородов УВС.

операционных задач по поддержке процесса добычи углеводородов на промысле добывающего предприятия основан на создании цифрового инструментов для планирования [7], диспетчеризации и управления действиями полевого персонала. Образ предлагаемой информационной системы представлен на рисунке 2.

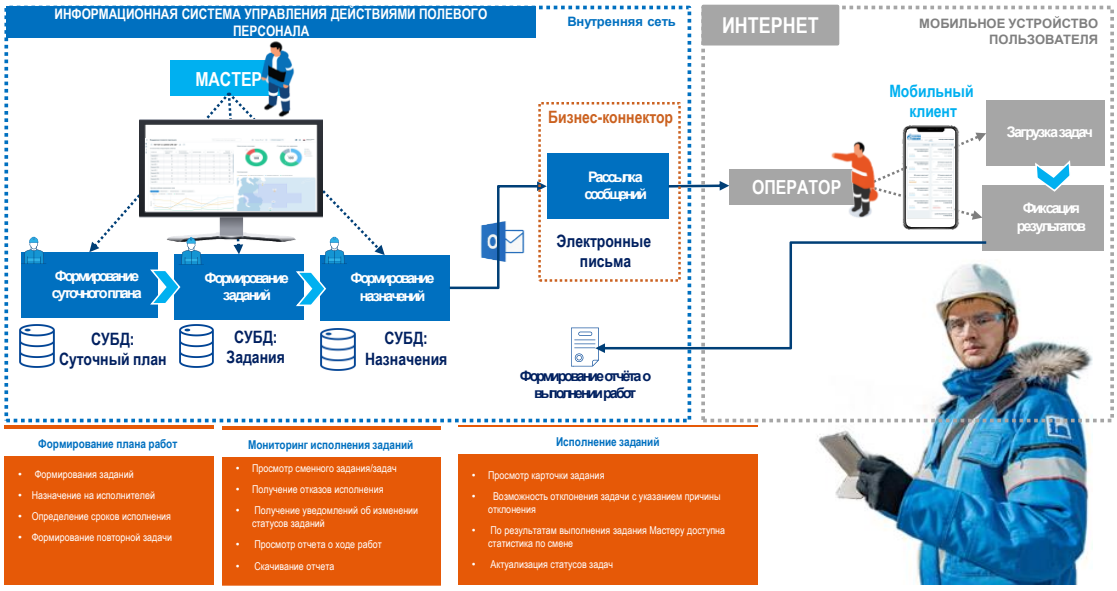


Рисунок 2 – Образ предлагаемой информационной системы для управления действиями полевого персонала добывающего промысла.

Разрабатываемая информационная система для управления действиями полевого персонала добывающего промысла позволяет автоматизировать процессы формирования, мониторинга и контроля [8] выполнения списка оперативных задач полевого персонала добывающего предприятия, а также оптимизировать использование ресурсов и обеспечить оперативное информирование о

происшествиях при проведении работ, соблюдении технологической дисциплины и безопасности проведения запланированных работ. Каждая порученная сотруднику задача описывается исчерпывающим набором атрибутов, что позволяет дополнительно решать аналитические задачи для поиска дополнительных способов минимизации непроизводительных потерь рабочего времени. Схематично набор атрибутов представлен на рисунке 3.

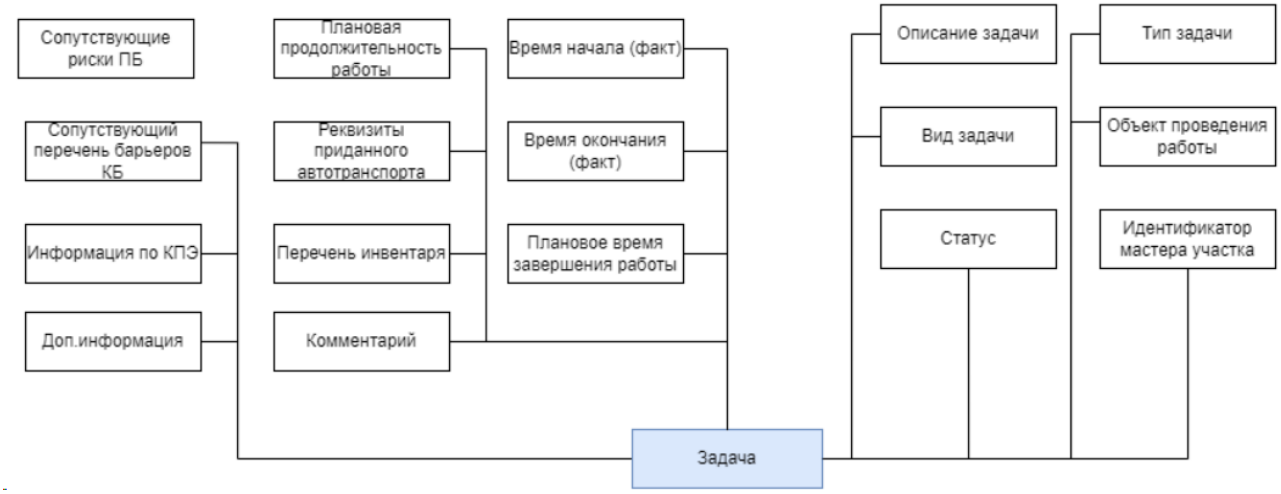


Рисунок 3 – Схема атрибутов сущности «Задача» внутренней базы данных

Процесс работы информационной системы для управления действиями полевого персонала добывающего промысла включает следующие шаги: сбор и анализ исходных данных о текущем состоянии промысла; набору плановых регламентных работ; набору оперативных задач для корректировки работы оборудования имеющихся ресурсах по полевому персоналу; задачах, переходящих с предыдущего периода; погодных условиях и других факторах. На основании собранной информации происходит верификация параметров и расчет, основанный на встроенных алгоритмах, с применением методов оптимизации, машинного обучения, графовых моделей для принятия эффективных решений при планировании работы полевого персонала. Конечный результат – оптимальные планы работы, учитывающие потребности добывающего предприятия, доступные ресурсы и внешние ограничения. Экранные формы информационной системы представлены на рисунке 4.

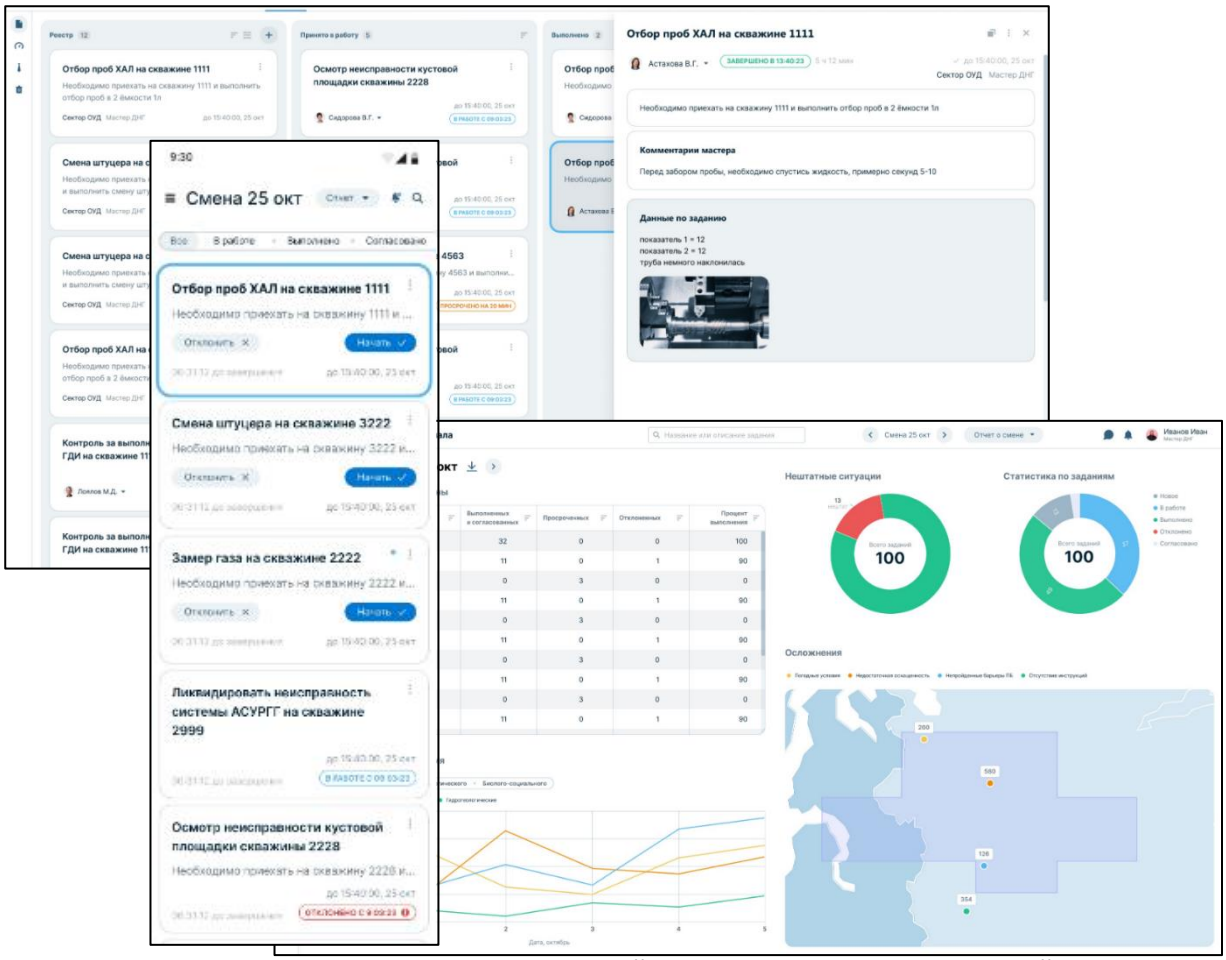


Рисунок 4 – Экранные формы информационной системы для управления действиями полевого персонала добывающего промысла.

Информационная система для управления действиями полевого персонала добывающего промысла была разработана с целью оптимизации ресурсов, затрачиваемых на выполнение операционных задач по поддержке процесса добычи углеводородов на промысле добывающего предприятия. Апробирование разработанной системы позволило сократить 14782 чел/часов за год, а также значительно повысить эффективность процессов ресурсного планирования и улучшить работу полевого персонала.

Список литературы

1. Process quality assessment/ Pishchukhin A.M./ В сборнике: IOP Conference Series: Materials Science and Engineering. Сер. 4 2020 International Conference on Modern Trends in Manufacturing Technologies and Equipment, ICMTMTE 2020. BRISTOL, ENGLAND, 2020. С. 042066.
2. Технологизация и автоматизация - два аспекта совершенствования техники Пищухин А.М., Ахмедьянова Г.Ф. Оренбург, 2019.
3. Автоматизированная система управления эксплуатацией месторождения углеводородов/ Ломухин И.А., Киян А.И., Пищухин А.М., Ахмедьянова Г.Ф.// Автоматизация. Современные технологии. 2023. Т. 77. № 3. С. 99-103.
4. Многоуровневое управление разработкой месторождения углеводородов/Ломухин И.А., Ахмедьянова Г.Ф., Пищухин А.М.// Нефтяное хозяйство. 2023. № 4. С. 80-85.

5. Новые подходы к управлению потенциалом добычи скважин механизированного фонда / Е.В. Юдин, Р.А. Хабибуллин, Н.А. Смирнов [и др.] // Нефтяное хозяйство. – 2021. – № 6. – С. 67-73. – https://doi.org/10.24887/0028-2448-2021-6-67-73. – EDN: JCOFAR.
6. Оптимальное распределение ресурсов в системе защиты информации в организации Мурзаханова Е.В., Пищухин А.М. Вопросы защиты информации. 2019. № 2 (125). С. 36-40.
7. Цифровые двойники нефтедобывающего предприятия/ Пищухин А.М., Ломухин И.А., Ахмедьянова Г.Ф./ В сборнике: XIV Всероссийское совещание по проблемам управления. сборник научных трудов. Москва, 2024. С. 2617-2621.
8. Автоматизация мониторинга и факторного анализа отклонений по добыче Власов Д.Ю., Занчаров А.А., Юдин Е.В., Мосягин Г.А. Нефтяное хозяйство. 2023. № 6. С. 78-82.

ОСОБЕННОСТИ СПЕЦИАЛИЗАЦИИ ОРГАНИЗАЦИОННО-ТЕХНИЧЕСКИХ СИСТЕМ

А.М. Пищухин, д.т.н., профессор, Г.Ф. Ахмедьянова, к.п.н., доцент
Федеральное государственное бюджетное образовательное учреждение высшего образования «Оренбургский государственный университет», г. Оренбург

Аннотация: работа посвящена системному исследованию признаков, по которым организационная система становится специальной. Основой при этом выбран состав и системные связи: персонал, технологическое оборудование и связи обеспечивающие взаимодействие составляющих при реализации деятельности или технологии. В результате отмечено, что к специализации ведет повышенная секретность используемой при функционировании системы информации и уникальность используемых технологий. По этим двум признакам также проедена классификация.

Ключевые слова: специализация, организационно-техническая система, персонал, техника, технология, уникальность, секретность.

Обычно классификация организационно-технических систем (ОТС) проводится по системным признакам [1]. В этом случае выбираются признаки в виде: характера взаимоотношений со средой (открытые, закрытые системы), причинной обусловленности (детерминированные, стохастические), степени подчиненности (простые, иерархические), по отношению к времени (статические, динамические), по степени к сложности (простые, сложные, большие). Однако такая классификация не объясняет почему система считается специальной, ведь специализация обуславливается назначением ОТС, а также малой распространенностью, то есть имеются часто встречающиеся ОТС и малораспространенные – последние и относят к специальным.

Специализация ОТС означает сосредоточение функционирования на конкретных задачах, процессах или областях деятельности организации. Следовательно, необходимо провести системный анализ специализации, с точки зрения специфики системных составляющих [2]. По-крупному ОТС включает персонал и искусственно созданную часть – технику. Связи между этими составляющими обусловливают внутрисистемную деятельность и применяемые технологии. Кроме того, ОТС может иметь различное назначение, определяемое взаимодействием с внешней средой. На рисунке 1 представлен возможный вариант классификации специальных ОТС.

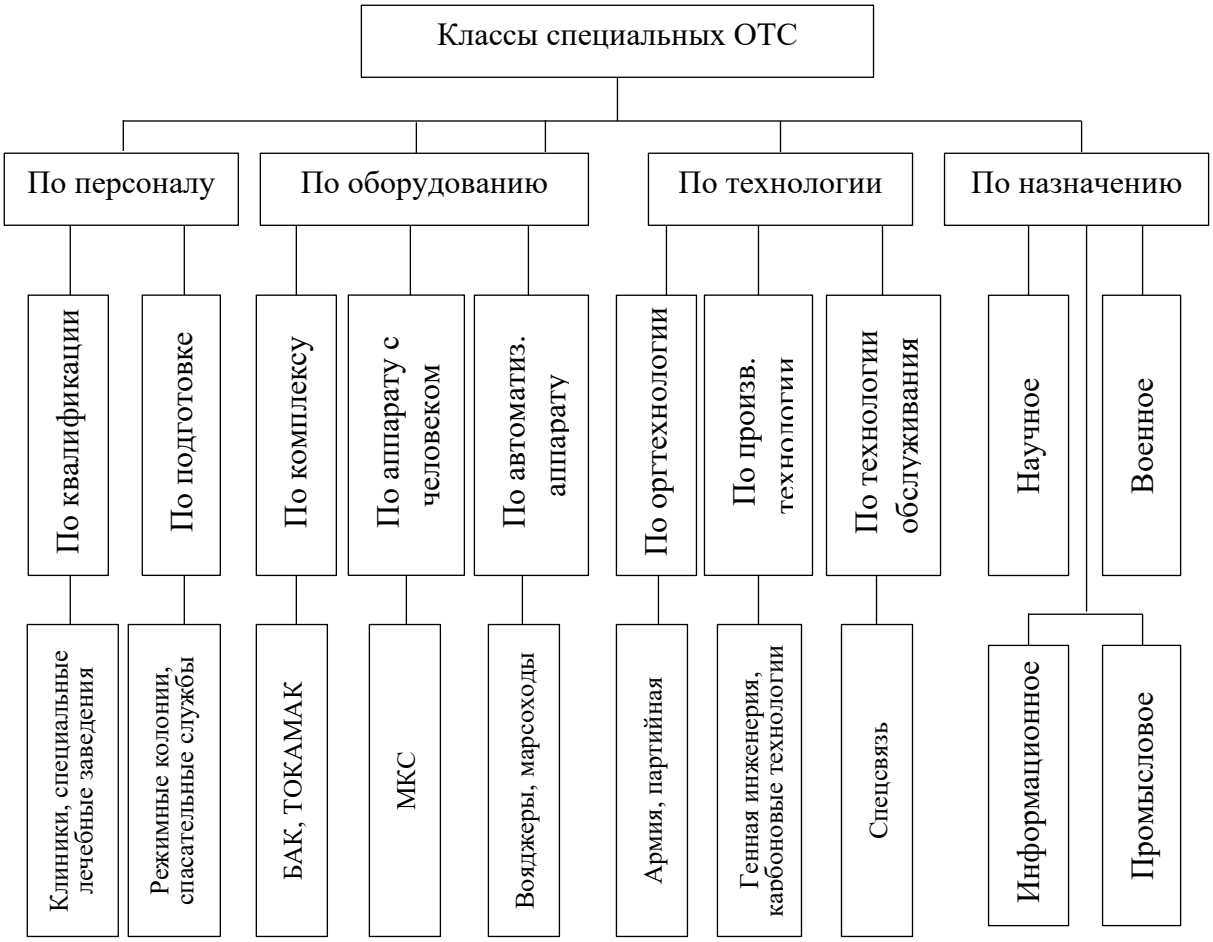


Рисунок 1 – Классификация специальных ОТС (с примерами)

В зависимости от квалификации персонала ОТС можно выделить несколько классов специальных систем. Это могут быть различные спец-предприятия и организации. Например, в специальных клиниках должна быть особая медицинская квалификация. Это же относится к специальным школам, к школам специальной подготовки и некоторым другим социальным заведениям.

Организационно-техническая система может стать специальной из-за уникальности используемой техники. Например, большой андронный коллайдер (БАК) требует особого рода специалистов, в первую очередь, физиков. То же самое относится к исследовательскому прибору в области термоядерных реакций - ТОКАМАКу, специальному инфракрасному телескопу Джеймса Уэбба, международной космической станции, космической станции «Новые горизонты» и так далее.

Уникальность используемой в ОТС технологии также может специализировать ОТС. Это могут быть, например, карбоновые технологии, технологии генной

инженерии, технологии обработки материалов взрывом, космические технологии и тому подобное.

Большим разнообразием отличается множество внешних назначений ОТС. Например, специализация может быть производственной, но тогда продукция должна быть уникальной – например, производство денежных знаков или чеканка монет.

Научное назначение имеют специальные ОТС в виде научно-исследовательских институтов по новым материалам, гиперзвуку, генной инженерии и многим другим направлениям исследований в науке, которые именуются прорывными.

Сфера услуг также может порождать специальные ОТС, если оказываемые услуги уникальны, например, в системе правосудия колонии строгого режима, спецавтохозяйства, специальные племенные хозяйства.

В современном мире практически ни одна деятельность не реализуется без применения компьютерной техники, поэтому любые организации становятся организационно-техническими [3]. Кроме упомянутых образовательных, исправительных и лечебных, даже такая организация как партия может пониматься как специальная ОТС.

Активно развиваются различные космические технологии от прогноза погоды до выращивания кристаллов в условиях космического вакуума, для чего, естественно создаются специальные ОТС.

Многие специальные ОТС связаны с военным назначением. Внутри этого назначения - изготовление спец-боеприпасов и спец-техники. Специальная военная операция внесла серьезные коррективы в отношении применяемых средств и сегодня много усилий направляется на изготовление новых моделей дронов и беспилотных летательных аппаратов.

Специальные ОТС связываются с ядерным оружием, как при его изготовлении, так и изготовлении и эксплуатации его носителей: стратегических подводных лодок, стратегической авиации, ракетно-космических систем.

Особый класс составляют природо-пользовательские ОТС. Сюда можно отнести предприятия по добыче алмазов, драгоценных и полудрагоценных камней. Другим подклассом являются промысловые предприятия такие как рыболовные и охотничьи хозяйства, предприятия по сбору лекарственных трав, грибов и лесных ягод, кедровых орешков.

ОТС в области ИТ-технологий специализируются закрытостью информации. Например, издательства журналов с секретностью или для служебного

пользования. Кроме того, ИТ-фирмы специализируются по разрабатываемому программному обеспечению, например, фирма, занимающаяся написанием антивирусных программ.

ОТС других назначений, например, энергетического становятся специальными при обслуживании закрытых объектов.

Из вышеприведенного системного анализа [4] сразу следует, что уникальность квалификации персонала, применяемого оборудования, технологии или назначения ОТС сопровождается повышенной секретностью и превращает систему в специальную. По уникальности и секретности также можно классифицировать специальные ОТС. Так по уникальности можно выделить три класса: с новизной в мировом масштабе, в масштабе страны и в масштабе региона.

С другой стороны, в настоящее время существует три уровня секретности используемой в специальных ОТС информации и соответствующие им грифы секретности: секретные, совершенно секретные, особой важности. Ограниченный доступ (потенциально конфиденциальная), но не секретная информация классифицируется как ДСП (для служебного пользования).

Отметим, в связи с этим, тот важный момент, что функционирование специальных ОТС предъявляет строгие требования прежде всего к системе управления.

Подобный подход к специализации организационно-технических систем применим при обеспечении образовательного процесса в Оренбургском государственном университете по специальности 27.05.01 Специальные организационно-технические системы.

Список литературы

1. Никоноров В.М. Классификации систем для управления // НК. 2016. №5 (38). URL: https://cyberleninka.ru/article/n/klassifikatsii-sistem-dlya-upravleniya (дата обращения: 01.09.2025).

2. Волкова В.Н. Теория систем и системный анализ : учебник для вузов / В. Н. Волкова, А. А. Денисов. – 3-е изд. – Москва : Издательство Юрайт, 2025. – 562 с. ISBN 978-5-534-14945-6. URL: https://urait.ru/bcode/559633 (дата обращения: 01.09.2025).

3. Ахмедьянова Г.Ф., Пищухин А.М. Основы многоуровневого управления в организационно-технических системах: монография. – Оренбург: ОГУ. – 2020. – 162 с. – ISBN: 978-5-7410-2488-1

4. Пищухин, А.М., Ахмедьянова Г.Ф. Общая теория систем. Метасистемы: учебное пособие. – Оренбург: ОГУ, 2019. – 163 с. – ISBN: 978-5-7410-2396-9

РАЗВИТИЕ КОМПЕТЕНТНОСТИ В АСПЕКТАХ УНИКАЛЬНОСТИ И СЕКРЕТНОСТИ НА ОСНОВЕ ГРАФА КОМПЕТЕНТНОСТИ

Ахмедьянова Г.Ф., к.п.н., доцент Пищухин А.М., д-р техн. наук, профессор
Федеральное государственное бюджетное образовательное учреждение высшего образования «Оренбургский государственный университет»

Аннотация: в статье исследуется отличия образовательного процесса по специальным организационно-техническим системам. Выявлены особенности в отношении уникальности квалификации персонала, технологического оборудования или используемой технологии, а также в отношении внешних объектов, на которые направлено ее функционирование. Для внесения соответствующей специфики в образовательный процесс разработан граф компетенций. Аналогичное исследование проведено в отношении аспекта секретности, используемой в специальной организационно-технической систем информации.

Ключевые слова: специальные организационно-технические системы, уникальность квалификации, уникальность технологии, граф компетентности, секретность.

В чем отличие обучения по программе 27.05.01 Специальные организационно-технические системы от курсов по организационно-техническим системам (ОТС) [1]? Очевидно, в том, что они специальные. Это влечет за собой наличие уникальности, особенности в таких системах, что требует в свою очередь засекречивания в той или иной степени, связанной с этой системой информации.

С точки зрения системного анализа, уникальность может быть связана с одной из составляющих специальной организационно-технической системы, а именно: с персоналом, технологическим оборудованием или с используемыми технологиями. Кроме того, специализация может быть обусловлена внешним для системы объектом, на который направлено ее функционирование.

В качестве примера специализации ОТС по персоналу можно рассмотреть процесс формирования отдела по оценке правдивости людей на полиграфе. Здесь применяется стандартное медицинское оборудование для измерения давления, частоты пульса, влажности кожи и тому подобное. С другой стороны, подготовка вопросов, форма их подачи и анализ результатов проводятся специально подготовленным персоналом, что и превращает эту ОТС в специальную.

Применение особого оборудования в виде уникального научного прибора, например, большого телескопа также требует внешнего проектирования специальной ОТС.

Такое же требование возникает, когда проводят внешнее проектирование специальной ОТС по используемой технологии, например, при создании консультирующей фирмы по PR-технологиям.

Наконец, внешнее назначение, например, по изготовлению документов государственного образца, также требует функционирования специально для этого созданной ОТС.

Даже краткий анализ, проведенный выше подсказывает, что в преподавании дисциплин по данной специальности необходимо подчеркивать значимость уникальности, умение отделить особенное от общего, понимание того факта, что оно, это особенное, требует особых же подходов, методов, моделей, критериев, алгоритмов и так далее. С другой стороны, необходимо учить проектированию таких систем, так называемому внешнему проектированию.

Уникальность напрямую связана с изобретательским делом. Если удается получить патент на изобретение какого-то устройства, способа, придумать необычное применение известных способа или устройства по новому назначению, а также комбинацию этих объектов, может возникнуть необходимость во внешнем проектировании специальной ОТС, например, в форме стартапа. Понятно, что необходимо обучить студентов во всех курсовых работах, проектах, индивидуальных заданиях обращаться к патентному поиску.

Инструментом, помогающим решить поставленные педагогические задачи, может служить граф компетенций [3]. Применим его в многоуровневом виде[4,5], тогда в корне графа находится умение проводить внешнее проектирование ОТС, от него расходятся лучи с названиями обеспечивающих компетенций, которыми нужно владеть, чтобы грамотно его осуществлять. От каждого узла с компетенцией расходятся ещё лучи, которые описывают, что нужно знать и уметь, чтобы считать, что обучающийся владеет обеспечивающей технологией. Граф можно продолжить дальше, детализируя каждый узел каким-то знанием или навыком и разбивая их на более элементарные знания или навыки. В каждом узле есть ссылки на материалы по данной теме и вопросы, чтобы сразу можно было изучить тему и проверить себя. Такой подход детализирует как педагогические средства, так и методы оценки достигаемого уровня компетенций [6,7].

Граф, построенный для обучения умению проводить внешнее проектирование представлен на рисунке 1. Из стандарта [2] выбрано соответственно: ОПК-3 - способен самостоятельно решать задачи управления в специальных организационно-технических системах на базе последних достижений науки и техники; ОПК-4 - способен определять критерии и применять методы оценки эффективности полученных результатов разработки в области специальных организационно-технических систем; ОПК-5 - способен определять формы и методы правовой охраны и защиты прав на результаты интеллектуальной деятельности, распоряжаться правами на них для решения задач специальных организационно-технических систем.

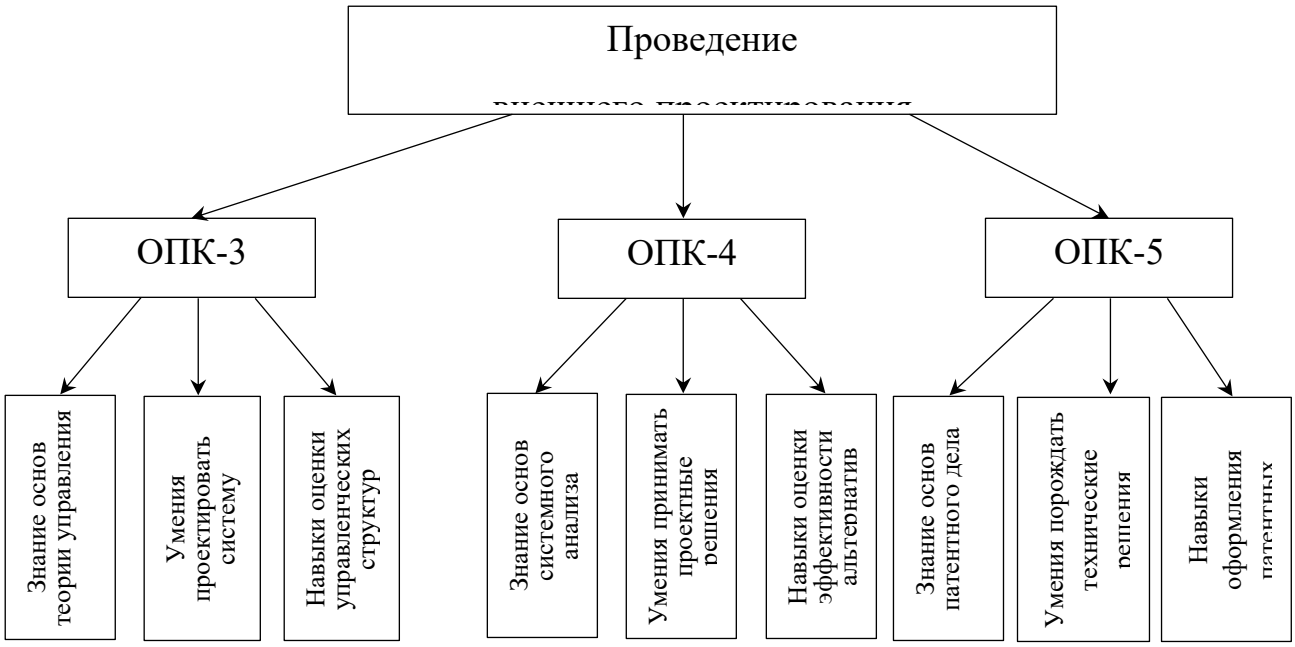


Рисунок 1 – Граф компетенций по внешнему проектированию

Другим отличием в данной специальности является повышенная секретность используемой информации. В России стандартом введены три уровня секретности: секретно, совершенно секретно и государственная важность. Иногда используют гриф для служебного пользования (ДСП), но он только ограничивает доступ, не делая информацию секретной.

Граф, построенный для развития компетенций по секретности представлен на рисунке 2. Из стандарта [2] выбрано соответственно: ОПК-6. Способен осуществлять сбор и анализ научно-технической информации, обобщать

отечественный и зарубежный опыт в области средств автоматизации и управления; ОПК-7. Способен аргументированно выбирать и обосновывать, а также разрабатывать схемотехнические, системотехнические и аппаратно-программные решения управления сложными техническими объектами и технологическими процессами и реализовывать их на практике; ОПК-10. Способен понимать принципы работы современных информационных технологий и использовать их для решения задач профессиональной деятельности. Добавим, что отличия, связанные с рассматриваемыми системами, влекут определенную психологическую нагрузку на персонал в отношении нужности дела, которым специалист занимается, поэтому необходимо чаще напоминать об этой «нужности».

Рисунок 2 – Граф компетенций по обеспечению секретности

Здесь уместны слова, что физику-ядерщику необходимо иногда колоть дрова, чтобы видеть результаты своего труда. Это подчеркивает важность разбиения больших целей на маленькие шаги с осязаемыми результатами, чтобы каждый день видеть прогресс и не терять мотивацию.

Таким образом, развитие компетентности в аспектах уникальности и секретности на основе графа компетентности рассмотрено на примере образовательной программы 27.05.01 Специальные организационно-

технические системы. Такой подход позволяет обучающимся, с одной стороны понять сущность специальности, а с другой стороны развивает инструменты углубления компетентности по ключевым направлениям.

Список литературы

1. Соловьёв И.В. Проблемы исследования сложной организационно-технической системы//Вестник МГТУ МИРЭА, 2013, № 1 (1), С. 20-40

2. Федеральный государственный образовательный стандарт высшего образования (ФГОС ВО) по специальности 27.05.01 «Специальные организационно-технические системы» (уровень специалитета). Утверждён приказом Министерства науки и высшего образования Российской Федерации от 12 августа 2020 года №951. Режим доступа: https://fgos.ru/fgos/fgos-27-05-01-specialnye-organizacionno-tehnicheskie-sistemy-951

3. Оболенский Д.М., Шевченко В.И. Построение и анализ графа компетенций на основе данных вакансий с порталов поиска работы//Экономика. Информатика. – 2023. – Т. 50, № 1 (1 91-202). DOI 10.52575/2687-0932-2023-50-1-191-202

4. Ахмедьянова, Г.Ф. Основы многоуровневого управления в организационно-технических системах : монография / Г.Ф. Ахмедьянова, А.М. Пищухин - Оренбург : ОГУ, 2020. – 162 с. – ISBN 978-5-7410-2488-1.

5. Ахмедьянова, Г.Ф. Многоуровневая модель оценки инженерных компетенций / Г.Ф. Ахмедьянова, А.М. Пищухин // Университетский комплекс как региональный центр образования, науки и культуры : материалы Всерос. науч.-метод. конф., посвящ. 70-летию Оренбург. гос. ун-та, Оренбург : ОГУ, 2025. – С. 20-23.

6. Ахмедьянова, Г.Ф. Формирование профессиональной компетентности на основе педагогического проектирования и организации учебной деятельности /Г.Ф. Ахмедьянова //Вестник Оренбургского государственного университета. – 2012. – №2. – С. 16-20.

7. Пищухин А.М., Методика оценки эффективности педагогических средств. /А.М. Пищухин, Г.Ф. Ахмедьянова // Модернизация педагогического образования в контексте глобальной образовательной повестки: Всерос. науч. практ. конф. /Нижегородский государственный педагогический университет им. К. Минина. – 2015. – С. 105-108.

УМНЫЕ СИСТЕМЫ ГАЗОВОГО МОНИТОРИНГА КАК ОСНОВА БЕЗОПАСНОСТИ СОВРЕМЕННЫХ ГОРОДОВ

С.В. Портнов, М.В. Архапчева
Федеральное государственное бюджетное образовательное учреждение высшего образования «Оренбургский государственный университет», г. Оренбург

Аннотация. Интеллектуальные системы газового мониторинга, основанные на многоуровневой сенсорной платформе и беспроводной связи, являются ключевым элементом безопасной городской среды, обеспечивая автономное обнаружение угроз и комплексное автоматическое реагирование. Их интеграция в городскую цифровую экосистему позволяет оперативно локализовать инциденты, минимизируя риски аварий и повышая устойчивость инфраструктуры «умного города».

Ключевые слова: умный город, системы газового мониторинга, безопасность, беспроводная связь, LPWAN, автоматическое реагирование.

Умные системы газового мониторинга играют ключевую роль в построении безопасной и устойчивой городской среды. В условиях стремительного роста городов и повышения плотности населения такие решения становятся неотъемлемой частью инфраструктуры «умного города», обеспечивая защиту как частных, так и общественных объектов. Сжиженный газ, состоящий из пропана и бутана, является легковоспламеняющимся и без запаха. Для обнаружения газа при утечке добавляется этантиол с сильным запахом. В одном устройстве объединены счетчик учета газа и датчики утечки, температуры (в случае пожара) и дыма [1].

При срабатывании любого датчика система блокирует подачу газа, посылает уведомление на телефон, личный кабинет пользователя и пульт оператора с информацией о месте происшествия (улица, дом, квартира). После короткой задержки включается вентилятор вытяжки для удаления газа. Система работает автономно на аккумуляторах и использует беспроводной LPWAN-радиомодем для передачи данных на расстояние до 10 км в городе и до 50 км на открытой местности.

Современная жизнь практически невозможна без использования газа и соответствующего оборудования. Газ применяется для готовки, отопления жилища и нагрева воды. Однако все газовые приборы представляют собой потенциальную опасность, и их эксплуатация требует строгого соблюдения правил безопасности. Несмотря на это, случаи взрывов и аварий, связанных с газом, являются не редкостью. Обычно причиной таких происшествий становится утечка газа. Даже ответственные потребители, соблюдающие все

меры предосторожности, могут столкнуться с несчастными случаями из-за износа оборудования или его периодического выхода из строя.

Причины взрыва бытового газа:

- неисправность газового оборудования;
- неквалифицированное подключение газового оборудования;
- нарушения правил эксплуатации оборудования.

Интеллектуальная система безопасности, обеспечивающая комплексное реагирование на потенциально опасные ситуации, включая утечку горючих газов, возникновение пожара и взрывоопасные состояния. В основе системы лежит многоуровневая сенсорная платформа, где газоанализаторы непрерывно контролируют состав воздушной среды, а высокочувствительные детекторы пламени мгновенно распознают термические аномалии.

Для оперативного устранения угроз реализован автоматизированный механизм защиты, включающий принудительную вентиляцию для рассеивания газовых скоплений и модуль пожаротушения с интеллектуальным управлением подачи огнетушащих веществ. При срабатывании любого из детекторов активируется многоуровневая система оповещения: визуальная индикация на графическом интерфейсе сопровождается звуковой сигнализацией, одновременно данные о чрезвычайной ситуации передаются через встроенный GSM-шлюз на мобильные устройства ответственных лиц, что гарантирует своевременное реагирование вне зависимости от присутствия персонала на охраняемом объекте.

Данная архитектура решения обеспечивает надежную защиту объектов различного назначения за счет превентивного выявления и автоматической нейтрализации широкого спектра техногенных угроз [2].

Такая система является недорогой и эффективной в спасении жизней, помогая защитить людей от опасных ситуаций, включая возможное гибель от ожогов. Основными причинами аварий являются утечка бытового газа, износ оборудования и нарушение правил его использования, что обусловлено использованием устаревших устройств и пренебрежением мерами безопасности. Даже при тщательных проверках невозможно полностью исключить риск утечки газа. Для предотвращения тяжелых последствий применяются газосигнализаторы − устройства, контролирующие уровень горючих газов в помещении. При превышении допустимой концентрации они активируют звуковое и световое оповещение, позволяя своевременно реагировать и предотвращать аварии. Некоторые модели дополнительно автоматически закрывают подачу газа.

Газосигнализаторы находят широкое применение на промышленных объектах, в котельных, общественных зданиях и жилых домах. Современные

устройства способны не только обнаруживать превышение концентрации газа, но и автоматически передавать данные на единый диспетчерский центр города, используя IoT-платформы. Это позволяет муниципальным службам ЖКХ, операторам газовых сетей и службам экстренного реагирования своевременно выявлять инциденты и локализовать угрозы. Таким образом, системы газового мониторинга становятся частью городской цифровой экосистемы.

Сигнализатор загазованности служат для непрерывного контроля воздушной среды в зонах потенциального скопления горючих газов. При превышении допустимых концентраций опасных веществ срабатывает светозвуковая сигнализация, одновременно активируя защитные механизмы газовой магистрали. Современные модели оснащены функцией аварийного отсечения топливоподачи при критических показателях или нарушениях в работе оборудования. Важной конструктивной особенностью является автономное срабатывание запорной арматуры даже при полном обесточивании системы. Встроенные диагностические модули постоянно проверяют целостность соединений между контрольными датчиками и управляющими блоками. Такие устройства обеспечивают круглосуточную защиту объектов, использующих газовое оборудование, без необходимости постоянного человеческого контроля. Интегрированные схемы защиты гарантируют предотвращение аварийных ситуаций при любых внештатных обстоятельствах [3].

Принцип работы сигнализатора основан на преобразовании уровня концентрации газа в электрическое напряжение с помощью датчика. Полученное значение сравнивается с установленным пороговым уровнем, заданным при калибровке. Если концентрация превышает этот порог, устройство генерирует звуковые, световые и управляющие сигналы согласно заданной логике работы. В случае обнаружения загазованности сигнал поступает на блок управления, который активирует электромагнитный запорный клапан и включает световую и звуковую индикацию. После этого микроконтроллер отправляет команду для оповещения пользователя о ситуации.

Эти функциональные возможности создают основу для единой экосистемы мониторинга в рамках концепции «умного города». В такой системе каждое подключенное устройство функционирует как интеллектуальный узел, непрерывно передающий оперативные данные в централизованную аналитическую платформу для обработки и принятия решений.

Для организации эффективных систем оповещения используются современные энергосберегающие технологии беспроводной связи, в частности LPWAN-решения. Наиболее значимым преимуществом рассматриваемых систем выступает минимальный уровень энергопотребления в сочетании с

поддержанием стабильного обмена данными на протяженных трассах (до десятков километров). Указанные свойства обуславливают их высокую востребованность в сфере городской инфраструктуры, для которой характерна острая потребность в оборудовании с длительным жизненным циклом и пониженными требованиями к техническому сопровождению.

Технологии LPWAN, обладая исключительными характеристиками, идеально подходят для развертывания масштабируемых сетей мониторинга. Их архитектура как нельзя лучше отвечает запросам концепции «умный город», обеспечивая связь для огромного количества распределенных датчиков.

Эволюция в области конструирования радиоэлектронных компонентов (антенн, приемопередающих модулей) обусловила существенный прогресс в средствах контроля газовой атмосферы. Внедрение данных разработок способствует повышению уровня безопасности в урбанистической среде, поскольку они позволяют диспетчеризировать утечки в режиме реального времени и сокращают период до начала аварийно-восстановительных работ, интегрируясь таким образом в концепцию умной инфраструктуры.

Список литературы

1. Важдаев К. В., Ураксеев М. Б., Мартяшева В. А. Автоматизированная многофункциональная система контроля утечки газа с использованием беспроводной технологии // Электротехнические и информационные комплексы и системы. 2020. № 1. URL: https://cyberleninka.ru/article/n/avtomatizirovannaya-mnogofunktsionalnaya-sistema-kontrolya-utechki-gaza-s-ispolzovaniem-bespro-vodnoy-tehnologii (дата обращения: 01.07.2025).

2. Архапчева, М. В. Применение автоматизированных систем интеллектуальной поддержки в управлении газораспределительной сетью / М. В. Архапчева, В. А. Трипкош, Н. А. Бочарова // Университетский комплекс как региональный центр образования, науки и культуры : материалы Всероссийской научно-методической конференции, посвященной 70-летию Оренбургского государственного университета, Оренбург, 30 января – 01 2025 года. – Оренбург: Оренбургский государственный университет, 2025. – С. 1739-1742.

3. Ульянова, Т. С. Разработка модели размещения ключевых датчиков газопровода / Т. С. Ульянова, М. В. Архапчева, А. С. Боровский // Школа-семинар молодых ученых и специалистов в области компьютерной интеграции производства : Материалы Школы-семинара, Оренбург, 14 ноября 2024 года. – Оренбург: Оренбургский государственный университет, 2024. – С. 256-258.

АНАЛИЗ ТИПОВЫХ УЯЗВИМОСТЕЙ ОРГАНИЗАЦИОННЫХ ПРОЦЕССОВ, ВЫЗВАННЫХ ЧЕЛОВЕЧЕСКИМ ФАКТОРОМ

М.А. Савина
Федеральное государственное бюджетное образовательное учреждение высшего образования «Оренбургский государственный университет», г. Оренбург

Аннотация. В статье проведены анализ уязвимостей корпоративных информационных систем и систематизация ключевых угроз информационной безопасности, возникающих по причине человеческого фактора. Установлено, что большинство индигенатов связано с ошибками персонала, нарушение регламента, а также некорректное исполнение обязанностей, что приводит к утечкам информации.

Ключевые слова: человеческий фактор, корпоративные информационные системы, реляционные СУБД, организационные уязвимости, когнитивное управление, достоверность данных, информационная безопасность.

В условиях современном мире корпоративные базы данных становятся основой для хранения и обработки важных данных. Однако совершенствование технических условий не исключает угрозу, связанную с человеческим фактором, который остается причиной рисков для информационной безопасности. Проблема уязвимости организационных процессов охватывает технические, организационные и экономические уровни функционирования предприятия, что определяет ее актуальность в данное время.

Человеческий фактор является одним из ключевых аспектов информационной безопасности. Под ним понимается совокупности поведенческих, когнитивных и психологических особенностей сотрудников, которые могут привести к нарушению целостности и конфиденциальности данных [1].

Основными угрозами, связанными с человеческим фактором, является [2]:

– непреднамеренные действия сотрудников организации, такие как несоблюдение правил по защите по паролю, нарушение правил безопасностей, ненадлежащее использование общих ресурсов и т.д. Например, использовать распространенные пароли или хранение в общедоступном доступе, что значительно повышает риск к несанкционированному доступу информации;

– злоупотребление полномочиями в лице сотрудников. Использование своих привилегий для несанкционированного доступа к конфиденциальной информации человека, такие как изменение информации, кража данных или установку вредоносных программ;

– малая осведомленность среди сотрудников о базовые принципы информационной безопасности. Незнание данных правил может привести к уязвимости фишинговых атак, а также социальной инженерии;

– психологическое воздействие на сотрудников или физических лиц для снижения концентрации внимания и принятия неверного решения. К подобным методам относят: создание стрессовой ситуации, использование в разговоре давление, угрозы;

– эмоциональная перегрузка и хроническая усталость снижает внимательность и осторожность, что значительно снижает соблюдение правил по работе с данными и их защите.

В современном мире в сфере информационной безопасности мы видим, что ни один из существующих подходов в отдельности не способен обеспечить должный уровень защиты. Поэтому для улучшения целостности информации стоит принимать комплексное решение, основанное на интеграции технических, организационных и человеческих аспектов.

Технический компонент включает в себя применение специализированных средств защиты данных. Среди них особое внимание заслуживают новые поколения защищённых носителей информации, построенных по принципу многоуровневой аутентификации и поддерживающих «прозрачное» шифрование. Эти устройства сочетают хранение ключей на самом носителе, защиту от физического доступа и возможность интеграции в существующую корпоративную инфраструктуру. В отличие от традиционных флеш-накопителей они позволяют существенно снизить риск утечек через съёмные носители, а также соответствуют требованиям регуляторов и могут быть сертифицированы для применения в государственных структурах. Наряду с этим важную роль продолжают играть системы мониторинга и контроля, включающие антивирусные решения, механизмы защиты от распределённых атак отказа в обслуживании, специализированные средства обнаружения целевых атак и программные комплексы для анализа сетевой активности. [3]

Однако даже самые совершенные технические средства не принесут результата без чёткой организации процессов внутри предприятия. Организационные меры включают создание продуманной системы мотивации персонала, которая ориентирована не только на наказания, но и на поощрения. Положительный эффект достигается за счёт премирования сотрудников за отсутствие инцидентов, компенсации расходов на приобретение защитного программного обеспечения для личных устройств, а также предоставления дополнительных выходных за ответственное отношение к политике безопасности. Существенным направлением является и повышение уровня осведомлённости работников: регулярные тренинги по распознаванию угроз,

курсы повышения квалификации и обязательное подписание соглашений о неразглашении информации формируют у персонала культуру ответственности.

Отдельная категория проблем связана с психологическим аспектом. Человеческий фактор в информационной безопасности традиционно считается самым уязвимым звеном. Эмоциональное выгорание, стресс и усталость способны снижать концентрацию внимания и увеличивать вероятность ошибок. Поэтому в современных условиях важно формировать культуру безопасности, которая воспринимается не как дополнительная нагрузка, а как естественная часть профессиональной деятельности. Позитивное отношение к мерам защиты, развитие внутренней ответственности и поощрение активного поведения сотрудников позволяют существенно повысить эффективность всей системы [4].

Таким образом, человеческий фактор может оказывать существенное негативное влияние на информационную безопасность. Несоблюдение правил техники безопасности, усталость, психологическое воздействие или злоумышленные действия со стороны сотрудников способны привести к утечке информации или финансовых потерь.

Список литературы

1. Дубинина Н.А. Подходы к оценке сбалансированности развития предприятий / Н.А. Дубинина, В.В. Усков // Вестник Астраханского государственного технического университета. Серия: Экономика. – 2019. – №1. – С. 164–172.

2. Моденов А.К. Оценка риска в экономической безопасности предприятия: учебное пособие / А.К. Моденов, М.П. Власов, Т.Н. Орловская [и др.]. – в 2 ч. – СПб.: Санкт-Петербургский политехнический университет Петра Великого, 2022. – 257 с. – ISBN 978–5-7422–7795–8. – EDN BVGUMW.

3. Кошелев С.О. Информационная безопасность и человеческий фактор / С.О. Кошелев, А.И. Яцкевич // Молодой ученый. – 2016. – № 7 (111). – С. 17-19. – URL: https://moluch.ru/archive/111/27330/.

4. Литвинов С. И. Социальная инженерия как фактор угрозы информационной безопасности // Вестник РУДН. Серия: Информатика. – 2021. – № 3. – С. 66–74. 5. Моденов А. К., Власов М. П., Орловская Т. Н. Оценка риска в экономической безопасности предприятия: учебное пособие. – СПб.: СПбПУ Петра Великого, 2022. – 257 с.

БЕЗОПАСНАЯ ДЕСЕРИАЛИЗАЦИЯ И КОНТРОЛЬ ЦЕЛОСТНОСТИ В ЦЕПОЧКАХ ПОСТАВОК МОДЕЛЕЙ МАШИННОГО ОБУЧЕНИЯ

Ситдиков Д.С., Лещинский Б.С.
Федеральное Государственное Казенное Военное Образовательное Учреждение Высшего Образования «Военная Орденов Жукова и Ленина Краснознаменная Академия Связи Имени Маршала Советского Союза С.М.Буденного»
Министерства Обороны Российской Федерации,
г. Санкт-Петербург

Аннотация: работа посвящена практической проверке целостности ML-моделей в контексте безопасности цепочки поставок. На одинаковой MLP-архитектуре демонстрируются процедуры сохранения и загрузки моделей в PyTorch (через state_dict) и TensorFlow/Keras 3.x (формат. keras), после чего вычисляются SHA-256 хэши файлов до и после перезагрузки и сопоставляются предсказания исходной и восстановленной моделей. Совпадение хэшей и идентичность предсказаний подтверждают неизменность весов и функционального поведения. Обсуждаются практики снижения рисков при десериализации (использование weights_only=True в PyTorch, «безопасного режима» загрузки в Keras) и интеграция криптографической подписи моделей в CI/CD как надстройки над базовой проверкой хэша.

Ключевые слова: безопасность цепочки поставок ML; проверка целостности; SHA-256; PyTorch state_dict; TensorFlow/Keras .keras; подпись моделей (CI/CD).

Современные практики CI/CD и безопасность цепочки поставок программного обеспечения распространяются и на сферу машинного обучения. Появились специальные инициативы по подписи ML-моделей и верификации их целостности – например, проект Model Signing от OpenSSF, предлагающий библиотеку и утилиты для криптографической подписи моделей любого формата и размера [1]. Модели часто передаются между различными командами (разработчики, команда деплоя), и важно убедиться, что файл модели не был подделан или повреждён по пути. Один из простых способов проверки целостности – вычисление криптографического хэша содержимого файла (например, SHA-256) и его сравнение при загрузке модели. SHA-256 широко применяется для таких целей: даже малейшее изменение данных приводит к совершенно иной хеш-сумме, что позволяет обнаружить любую попытку внести изменения, а сам алгоритм обладает высокой стойкостью к коллизиям (практически исключая вероятность совпадения хеша у разных входных данных) [2].

В данной работе рассматривается задача надёжного сохранения и загрузки ML-моделей в двух популярных фреймворках – PyTorch и TensorFlow – анализируется, как они справляются с сохранением весов модели и обеспечивают сохранение интерфейса модели. TensorFlow поддерживает стандартный формат SavedModel, который сохраняет структуру модели, значения всех весовых параметров и «сигнатуры» – именованные функции, определяющие ожидаемые входы и выходы модели [3]. Кроме того, начиная с версии Keras 2.13 (TensorFlow), был введён параметр safe_mode, призванный предотвратить десериализацию потенциально опасных слоёв Lambda, содержащих исполняемый код [3]. Однако исследования показывают, что данный «безопасный режим» лишь частично защищает от атак: злоумышленники всё ещё могут создать вредоносный файл модели, обходящий это ограничение, поэтому safe_mode должен дополняться другими мерами безопасности [4].

В свою очередь, PyTorch использует более прямолинейный механизм сохранения: модель хранит обученные параметры в виде словаря состояний (state_dict), который можно сериализовать с помощью функции torch.save. Загрузка осуществляется путём создания экземпляра той же модели и применения load_state_dict(). Специального «безопасного» режима при загрузке PyTorch-моделей не предусмотрено – фреймворк полагается на доверие к исходному коду модели. Поэтому разработчикам рекомендуется сохранять именно веса (state_dict), а не весь объект модели, и при загрузке при необходимости ограничивать выполняемые при десериализации функции [5].

Цель эксперимента – сравнить механизмы проверки целостности при экспорте и импорте одной и той же MLP-модели в PyTorch и TensorFlow. Модель в каждом фреймворке сохраняется, для соответствующих файлов весов до и после перезагрузки вычисляются SHA-256 хэши и проверяется их совпадение. Дополнительно сравниваются предсказания исходной и загруженной моделей на одном и том же входном примере, чтобы подтвердить неизменность функционального поведения. Такой подход иллюстрирует аспекты доверенного выполнения в ML-фреймворках и позволяет оценить влияние специальных опций (например, безопасного режима загрузки) на надёжность процесса сохранения моделей.

В качестве исходных данных используется встроенный датасет классификации опухолей груди. Датасет содержит числовые признаки, характеризующие опухоль, и бинарную целевую переменную (злокачественная или доброкачественная опухоль). Набор данных предварительно разделяется на обучающую и тестовую выборки (с сохранением соотношения классов,

используя стратифицированное разбиение). Для улучшения обучения все признаки масштабируются.

Архитектура модели в обоих фреймворках выбрана идентичной: полносвязная нейронная сеть с двумя скрытыми слоями по 64 нейрона с активацией ReLU и выходным слоем из одного нейрона с сигмоидной активацией (для предсказания вероятности положительного класса. Использование одинаковой архитектуры и данных в PyTorch и TensorFlow позволяет корректно сравнить результаты сохранения и загрузки моделей.

Эксперимент состоит из следующих этапов:

1. Загрузка и подготовка данных. Выполняется разделение на обучающую и тестовую выборки. Выполняется масштабирование признаков.

2. Определение модели в PyTorch. Создаётся класс MLP_PT, реализующий описанную выше архитектуру.

3. Обучение модели в PyTorch. Инициализируется объект модели и оптимизатор Adam. Модель обучается в течение 5 эпох (batch size = 32) с функцией потерь бинарной перекрёстной энтропии (nn.BCELoss).

4. Сохранение PyTorch-модели. После обучения вызывается torch.save(model_pt.state_dict(), "model_pt.pth"), что сохраняет на диск файл с расширением .pth, содержащий сериализованный словарь параметров модели (веса и смещения каждого слоя).

5. Определение модели в TensorFlow. Создаётся аналогичная модель model_tf с помощью tf.keras.Sequential.

6. Обучение модели в TensorFlow. Модель model_tf обучается на тех же обучающих данных (5 эпох, batch size = 32).

7. Сохранение TensorFlow-модели. После обучения Keras-модель сохраняется вызовом model_tf.save("model_tf.keras").

8. Вычисление SHA-256 после сохранения. С помощью модуля hashlib вычисляются криптографические хеш-суммы SHA-256 для каждого сохранённого файла: для PyTorch это model_pt.pth, для TensorFlow – файл model_tf.keras.

9. Загрузка моделей и проверка хешей. Загружаем модели из файлов. После загрузки повторно вычисляем SHA-256 соответствующих файлов модели (файлы на диске при этом не изменились). Сравниваем пары хеш-сумм.

10. Сравнение предсказаний моделей. Дополнительно убеждаемся, что загруженные модели выдают тот же результат, что и исходные обученные модели. Для этого берём небольшую выборку примеров и прогоняем через исходную PyTorch-модель model_pt и загруженную model_pt2, сравнивая полученные значения выхода (вероятности). Аналогично проверяем выводы model_tf и model_tf2 на этих же примерах. Все соответствующие пары выходов

должны совпадать с высокой точностью, что подтверждает идентичность поведения модели до сохранения и после загрузки.

Результаты эксперимента показали, что вычисленные SHA-256 для файлов весов до и после загрузки совпадают как для модели PyTorch, так и для модели TensorFlow. На рисунке 1 представлены соответствующие значения хэшей.

framework	sha_before	sha_after	test_accuracy
PyTorch	38acac9f1ade1da865d360fa5326a55a cdafa0cc8858a93df3726d09848cabce	38acac9f1ade1da865d360fa5326a55a cdafa0cc8858a93df3726d09848cabce	0.958580
TensorFlow (Keras 3.x)	dc63f2d1d8b4a2ceecbbbc05ca5666ee 393ff5a68a3d23ca515756042f80606d	dc63f2d1d8b4a2ceecbbbc05ca5666ee 393ff5a68a3d23ca515756042f80606d	0.970414

Рисунок 1 – Сводка хэш-сумм (SHA-256) и accuracy для PyTorch и TensorFlow (Keras 3.x)

Совпадение хеш-сумм свидетельствует о том, что файлы с весами не изменились в процессе сохранения и загрузки – веса модели полностью сохранили свою целостность. Также проверка на нескольких тестовых примерах показала, что загруженные модели выдают точно такие же предсказания, как и модели до сохранения (для обеих реализаций). Это означает, что функциональное поведение и параметры модели были сохранены без каких-либо искажений. В случае TensorFlow использование формата .keras гарантировало сохранение архитектуры модели и её параметров в одном файле; при загрузке эта информация восстановилась, и модель ожидаемо имеет тот же интерфейс, что и исходная (те же входные размеры и один выход с sigmoid-активацией). Таким образом, можно сказать, что в проведенном эксперименте оба фреймворка успешно прошли проверку: сохраняемая нейросеть после перезагрузки полностью эквивалентна исходной.

Аспекты безопасности сериализации требуют отдельного внимания. В TensorFlow/Keras по умолчанию действует safe_mode=True, блокирующий исполнение произвольного кода при загрузке, в частности через пользовательские слои Lambda [4]. Рассматриваемый пример таких слоёв не содержит, поэтому загрузка выполняется в стандартном режиме. Однако исследования по безопасности показывают, что даже при включённом safe-mode сохраняются обходные пути для запуска вредоносного кода при десериализации, что подчёркивает необходимость дополнительных мер предосторожности, особенно при работе с моделями из непроверенных источников. В PyTorch сериализация опирается на механизм pickle, который при сохранении целого объекта модели теоретически позволяет встроить и выполнить код при загрузке. По этой причине официальная документация рекомендует сохранять именно state_dict, а начиная с PyTorch 2.0 применять при загрузке режим

weights_only=True, ограничивающий выполняемые в процессе десериализации операции загрузкой одних лишь параметров модели [5]. Указанные практики существенно снижают риски, связанные с обработкой потенциально опасных модельных артефактов.

Проверка SHA-256 – простой и действенный контроль целостности, совпадение хешей до/после загрузки указывает на отсутствие модификаций, а криптографическая стойкость делает коллизии практически нереалистичными [2]. Однако хеш лишь один слой защиты, на практике следует применять цифровые подписи и проверять их на каждом этапе переноса модели (инициативы OpenSSF Model Signing) [1], что обеспечивает не только целостность, но и подтверждённое происхождение.

Проведённая проверка целостности MLP-модели при сохранении и загрузке в PyTorch и TensorFlow показывает, что при соблюдении надлежащих процедур оба фреймворка обеспечивают неизменность весов: вычисленные SHA-256 совпадают до и после загрузки, а идентичность предсказаний свидетельствует о сохранении функционального интерфейса. Следовательно, механизмы сериализации обоих фреймворков надёжны при корректном использовании. Однако практическое обеспечение доверия к модели не может ограничиваться одной проверкой хеша: следует учитывать более сложные угрозы (вплоть до исполнения произвольного кода и атак на процессы загрузки). Для комплексной защиты целесообразно комбинировать цифровую подпись моделей и её верификацию на каждом этапе, базовые проверки целостности (как в данном эксперименте) и рекомендации фреймворков (безопасная загрузка, сохранение state_dict), формируя полную доверенную цепочку поставок ML-моделей.

Список литературы

1. Marusheak M., Wickens E. Launch of Model Signing v1.0: OpenSSF AI/ML Working Group Secures the Machine Learning Supply Chain OpenSSF Blog. 2025-04-04. URL: https://openssf.org/blog/2025/04/04/launch-of-model-signing-v1-0-openssf-ai-ml-working-group-secures-the-machine-learning-supply-chain/ (дата обращения: 10.08.2025).

2. Saini K. Hashing in Cyber Security: Understanding the Best Practices // Simplilearn. 2025-06-27. URL: https://www.simplilearn.com/hashing-in-cybersecurity-article (дата обращения: 10.08.2025).

3. TensorFlow Team. SavedModel // TensorFlow Core Guide. URL: https://www.tensorflow.org/guide/saved_model (дата обращения: 10.08.2025).

4. Polkovnichenko A. Is TensorFlow Keras “Safe Mode” Actually Safe? Bypassing safe_mode Mitigation to Achieve Arbitrary Code Execution // JFrog Blog. 12.03.2025. URL: https://jfrog.com/blog/keras-safe_mode-bypass-vulnerability/ (дата обращения: 10.08.2025).

5. PyTorch Team. Saving and Loading Models — PyTorch Tutorials // PyTorch.org. URL: https://docs.pytorch.org/tutorials/beginner/basics/saveloadrun_tutorial.html (дата обращения: 10.08.2025).

ПОВЫШЕНИЕ НАДЁЖНОСТИ МОДЕЛЕЙ КОМПЬЮТЕРНОГО ЗРЕНИЯ: ОБНАРУЖЕНИЕ ШУМНЫХ МЕТОК МЕТОДОМ CONFIDENT LEARNING

Ситдиков Д.С., Лещинский Б.С.
Федеральное Государственное Казенное Военное Образовательное Учреждение Высшего Образования «Военная Орденов Жукова и Ленина Краснознаменная Академия Связи Имени Маршала Советского Союза С.М.Буденного» Министерства Обороны Российской Федерации, г. Санкт-Петербург

Аннотация: Работа посвящена автоматическому выявлению шумных меток в задачах классификации изображений с использованием подхода confident learning. На подмножестве датасета Animals-10 формируются out-of-sample вероятности классов посредством 5-кратной кросс-валидации CNN-классификатора; далее библиотека Cleanlab ранжирует объекты по вероятности ошибочной разметки. Анализ выявленных кандидатов показывает, что значительная часть выявленных случаев совпадает с преднамеренно внесёнными ошибками меток, а оставшаяся доля отражает пограничные и неоднозначные примеры. Подход позволяет оперативно приоритизировать ручной аудит данных и служит эффективным средством повышения качества обучающих выборок.

Ключевые слова: confident learning, качество данных, шумные метки, CNN, Cleanlab, валидация.

Аномалия в данных – это наблюдение, которое существенно отклоняется от типичного поведения системы [1]. В классических задачах обнаружения аномалий она часто связана с неразмеченными данными (например, выбросы во временных рядах, сбои датчиков). В задачах обучения с учителем одной из разновидностей «аномалий» можно считать шумную (ошибочную) метку, то есть неправильно проставленный класс. Шумные метки практически неизбежны при сборе реальных данных и оказывают серьёзный негативный эффект на обучение моделей: глубокие нейросети обладают большой ёмкостью и способны запоминать даже случайные или ошибочные метки, что приводит к переобучению и потере обобщающей способности модели [2]. Эта проблема привлекает всё больше внимания в русле концепции data-centric AI, фокусирующейся на качестве данных. Даже небольшое количество неправильно размеченных примеров может существенно снизить качество предсказаний и привести к неверным выводам при модели на продакшене.

Для решения проблемы качества разметки разрабатываются методы confident learning – алгоритмы «уверенного обучения», которые автоматически выявляют и помогают исправлять ошибки разметки без привлечения человека [3]. Библиотека Cleanlab – одна из популярных реализаций таких методов –

автоматически находит и устраняет ошибки разметки в наборах данных, тем самым снижая затраты ручного труда на очистку данных. Базовая идея заключается в том, что метка считается «подозрительной», если модель, обученная на остальной части данных, низко оценивает вероятность принадлежности объекта к его текущему классу и, напротив, высоко уверена в альтернативном классе. Чтобы такая оценка была честной, для каждого объекта необходимо получить out-of-sample вероятности классов – предсказания модели, которая никогда не видела этот объект при обучении. Практически это достигается через k-fold кросс-валидацию: на каждом фолде модель обучается на $(k-1)/k$ части данных и предсказывает вероятности для оставшейся $1/k$ части. Затем все эти «отложенные» предсказания собираются в единую матрицу.

В эксперименте использовался датасет Animals10 (28 тысяч RGB-изображений, 10 классов). Для обеспечения воспроизводимости и приемлемого времени вычислений из каждого класса было отобрано по 1400 изображений, все изображения были приведены к размеру 128×128 и нормированы. Далее в разметку целенаправленно был внесён контролируемый синтетический шум: в каждом классе небольшое фиксированное число объектов было переназначено в случайные ошибочные классы.

В качестве базовой модели применялась компактная CNN с двумя свёрточными и двумя полносвязными слоями, выдающая вероятностные предсказания по всем 10 классам. На каждом из 5 фолдов кросс-валидации сеть обучалась на тренировочной подвыборке (включая зашумлённые метки), а на валидационной формировались out-of-sample вероятности. После агрегации по всем фолдам была получена матрица pred_probs размера размера $N \times K$ (где N – число изображений, K – число классов).

Далее применялась библиотека Cleanlab [4]. Функция find_label_issues принимала пару (y_noisy, pred_probs) и вычисляла для каждого объекта оценку качества метки (label quality score). Для интерпретации использовалось ранжирование по метрике self-confidence — вероятности, которую модель приписывает текущему (аннотированному) классу объекта: чем она ниже, тем выше вероятность ошибочной разметки. В анализ включались топ-5 % наихудших по self-confidence примеров (frac_noise=0.05) как кандидаты на ручной аудит или автоматическую корректировку.

Полученный список «подозрительных» объектов, сформированный Cleanlab, был сопоставлен с множеством заранее искажённых меток (noisy_indices). Зафиксировано, что значительная часть выявленных библиотекой изображений действительно принадлежит к примерам с преднамеренной подменой класса. Для количественной оценки использовались метрики recall – доля обнаруженных ошибок среди всех внесённых шумов, и precision – доля истинных ошибок среди всех помеченных алгоритмом примеров.

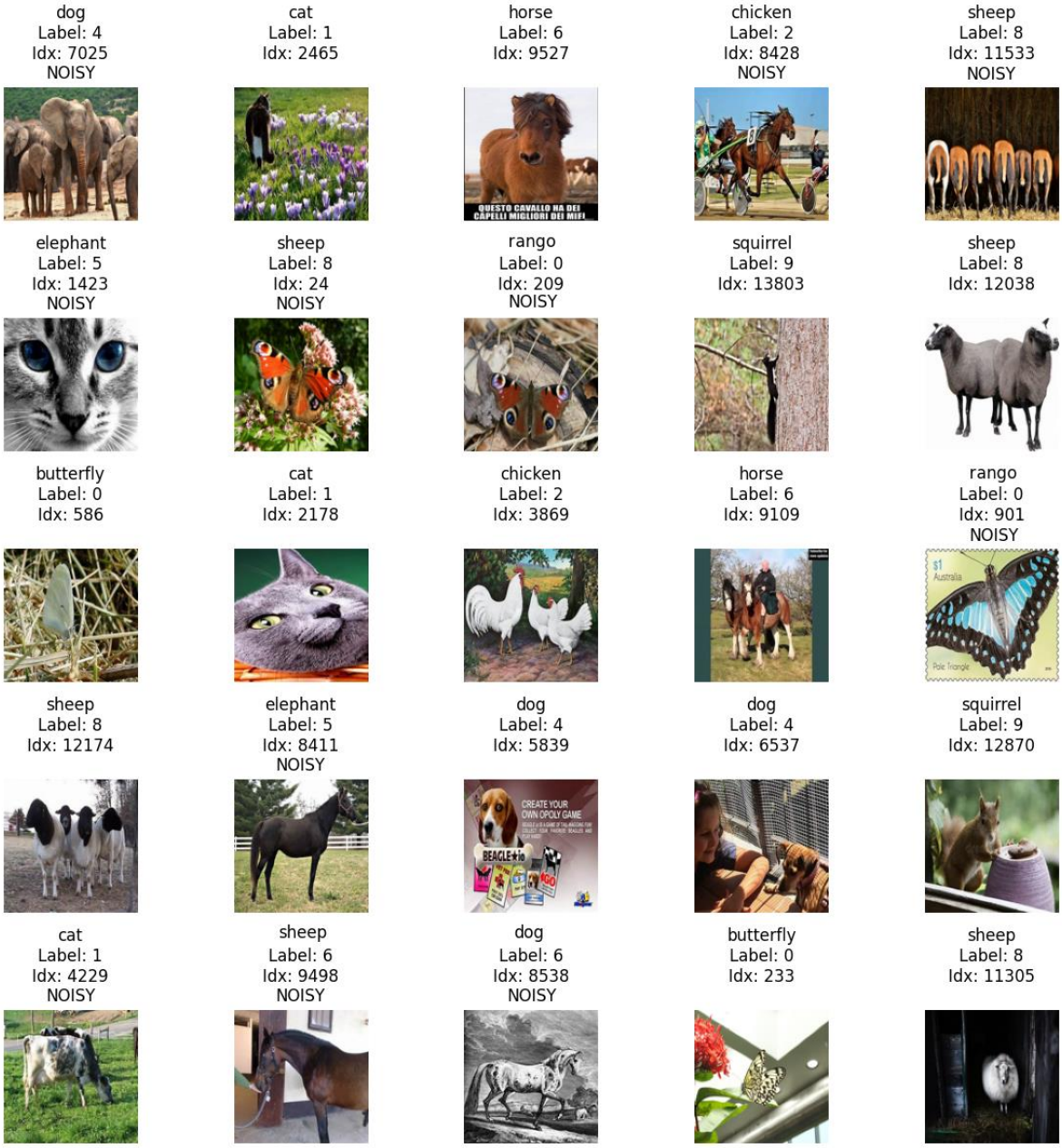


Рисунок 1 – Список объектов, сформированных Cleanlab

На рисунке 1 представлена набор изображений, отобранных для демонстрации поведения алгоритма. Половина изображений из этого списка имеют очевидные несоответствия между изображением и аннотированным классом (например, «бабочка» с меткой «овца», «кот» с меткой «слона»). Подобные очевидные ошибки легко выявляются, поскольку модель уверенно предсказывает для них правильный класс, резко не совпадающий с заданной меткой.

Помимо заведомых ошибок, Cleanlab выявил изображения, которые не входили в перечень noisy_indices, но получили низкий score self-confidence. При

просмотре выяснилось, что эти случаи представляют собой либо неоднозначные экземпляры, либо потенциальные выбросы датасета. Например, среди них были сильно размытые фотографии и изображения животных в необычном ракурсе, затрудняющие распознавание. Модель не была уверена в их принадлежности к заявленному классу, поэтому алгоритм отметил их как возможные проблемы разметки. Такие случаи не являются ошибкой разметки в прямом смысле, однако их выявление тоже ценно: они указывают на сложные для модели образцы, которые желательно пересмотреть вручную или исключить из обучающей выборки для повышения качества обучения.

Хотя в выборке 14 тысяч изображений относительное число шумных меток невелико (мы намеренно внесли ошибку примерно в 2% данных), Cleanlab находит несколько сотен кандидатов на ошибки. На практике даже в «чистых» наборах данных встречаются десятки ошибочно размеченных или спорных образцов – исследования показывают, что в эталонных датасетах может содержаться в среднем около 3% ошибок разметки (до 6–10% на отдельных наборах) [5]. Наш эксперимент подтверждает эту тенденцию и демонстрирует, что автоматический анализ качества меток способен эффективно подсветить подобные скрытые проблемы в данных.

Проведённое исследование демонстрирует практическую применимость confident learning для обнаружения проблемной разметки в наборах изображений. Использование 5-кратной кросс-валидации CNN для получения out-of-sample вероятностей и последующей фильтрации Cleanlab позволило выделить компактный «топ-лист» подозрительных объектов. Визуальный разбор подтверждает, что большинство из этих объектов действительно содержат ошибки меток; оставшиеся случаи представляют собой трудно интерпретируемые или нетипичные изображения, что объясняет ложные срабатывания. Таким образом, метод обеспечивает высокую чувствительность к шуму в данных и существенно снижает объём ручной проверки за счёт приоритизации наиболее вероятных ошибок.

При этом confident learning не заменяет экспертную валидацию, помеченные объекты рекомендуется просматривать вручную перед удалением или правкой. Наилучшей практикой является включение данного шага в конвейер подготовки данных (data-centric AI): периодический запуск пайплайна CNN – out-of-sample вероятности – Cleanlab с последующим адресным аудитом улучшает состав обучающей выборки и повышает надёжность итоговых моделей.

Список литературы

6. Karimi D. et al. Deep learning with noisy labels: Exploring techniques and remedies in medical image analysis //Medical image analysis. – 2020. – Т. 65. – С. 101759.Saini K. Hashing in Cyber Security: Understanding the Best Practices // Simplilearn. 2025-06-27. URL: https://www.simplilearn.com/hashing-in-cybersecurity-article (дата обращения: 10.07.2025).

7. Bai Y. et al. Understanding and improving early stopping for learning with noisy labels //Advances in Neural Information Processing Systems. – 2021. – Т. 34. – С. 24392-24403.

8. Lin T. et al. Efficiency and safety of automated label cleaning on multimodal retinal images //npj Digital Medicine. – 2025. – Т. 8. – №. 1. – С. 10.

9. Cleanlab Team. cleanlab Documentation (v2.3.1) // cleanlab.ai. URL: https://docs.cleanlab.ai/v2.3.1/ (дата обращения: 25.07.2025).

10. Northcutt C. G., Athalye A., Mueller J. Pervasive label errors in test sets destabilize machine learning benchmarks //arXiv preprint arXiv:2103.14749. – 2021.

МЕТОДЫ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ ПРИ ФУНКЦИОНИРОВАНИИ КОЛЛЕКТОРНО-ЛУЧЕВЫХ СИСТЕМ НЕФТЕГАЗОВЫХ СКВАЖИН

Ульянова Т.С., Акимов С.С., кандидат технических наук
Федеральное государственное бюджетное образовательное учреждение высшего образования «Оренбургский государственный университет»

Аннотация: в данной статье рассматриваются современные методы обеспечения безопасности при эксплуатации коллекторно-лучевых систем в нефтегазовой промышленности и практические решения в области обеспечения безопасности. Представленные материалы способствуют повышению надежности и безопасности процессов добычи нефти и газа, а также обеспечивают рекомендации по внедрению современных технологий в промышленную практику.

Ключевые слова: безопасность нефтегазовых скважин, коллекторно-лучевые системы, системы автоматической защиты, мониторинг и диагностика, предотвращение аварий, надежность систем, технологические методы безопасности.

Обеспечение безопасной эксплуатации коллекторно-лучевых систем (КЛС) нефтегазовых скважин является актуальной задачей, от решения которой зависит как безопасность персонала, так и сохранность технологического оборудования и окружающей среды. Современные методы и системы основаны на комплексных подходах, включающих автоматизацию, интеллектуальные системы контроля, диагностики и противоаварийной защиты, использование современных информационных технологий и математических моделей.

Можно выделить основные современные методы и технологии обеспечения безопасности, которые рассматриваются в научных работах:

1. Автоматизированные системы мониторинга и контроля. Развитие автоматизированных систем мониторинга позволяет непрерывно отслеживать технологические параметры скважин и их составляющих элементов (давление, температуру, вибрацию). Например, системы «точка к точке» и концентраторы данных обеспечивают интеграцию разрозненных компонентов в единую сеть, что повышает оперативность выявления аварийных ситуаций [1, 2]. Внедрение беспроводных устройств и автономных датчиков на устьях скважин и внутри коллектора позволяет своевременно получать критические данные и формировать централизованные базы данных для анализа.

Разработаны практические рекомендации для расстановки датчиков утечки газа в процессе эксплуатации газодобывающих объектов. Схема оптимального расположения датчиков приведена на рисунке 1.

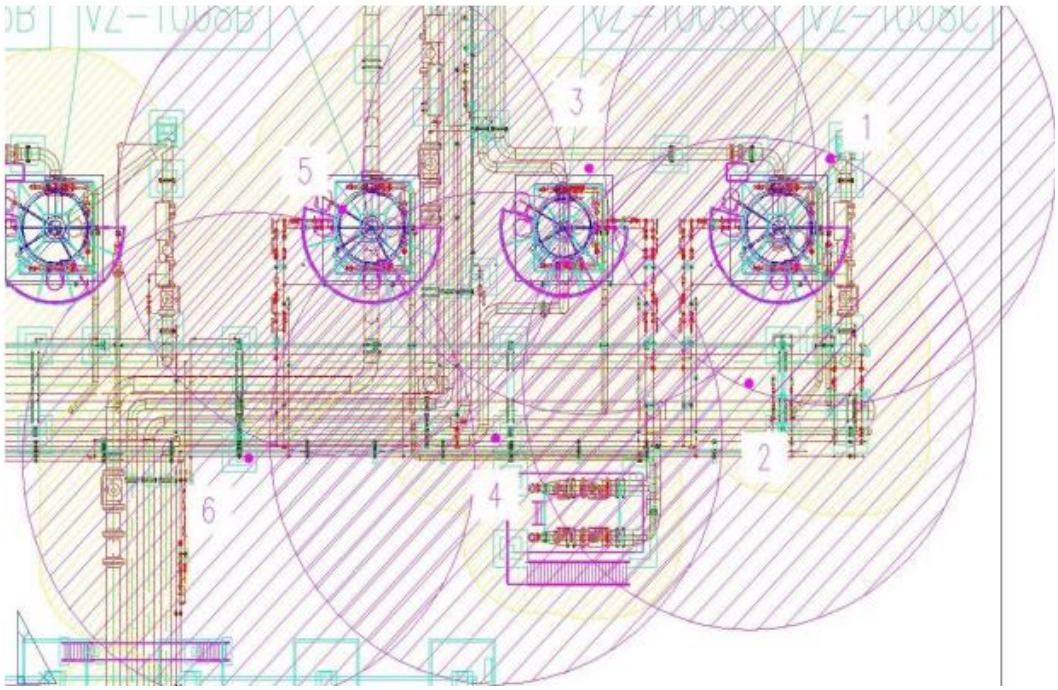


Рисунок 1 – Оптимальная расстановка датчиков утечки газа на объектах нефтегазовой промышленности

2. Интеллектуальные системы анализа и диагностики. Использование методов интеллектуальной обработки данных (ИАД), таких как нейросети, алгоритмы машинного обучения и статистические методы, значительно повышает точность и скорость обнаружения потенциальных отказов и аварийных ситуаций [3, 4]. Например, нейросетевые модели позволяют оценивать остаточный ресурс компонентов, прогнозировать их износ и предсказывать вероятные отказные режимы.

3. Диагностика и контроль аварийных факторов. Ключевые параметры системы постоянно контролируются с помощью специальных датчиков и систем вибродиагностики. В частности, контроль вибраций газокомпрессорных установок позволяет выявлять ранние признаки износа, а системы визуальной диагностики осуществляют мониторинг состояния металлических конструкций, выявляя нарушения в работе трубопроводов и насосных агрегатов.

4. Противоаварийные системы (ПАЗ). Создание систем противоаварийной защиты включает как автоматическое отключение или регулировку параметров для предотвращения аварийных условий, так и системы быстрого реагирования. Например, внедрение автоматических регуляторов давления, основанных на модели гидравлических сопротивлений, позволяет регулировать давление в коллекторах и снижать риск аварийных выбросов [5].

5. Оптимизация расположения датчиков и автоматизация реагирования. Для повышения надежности обнаружения утечек и аварий используют схемы оптимального расположения датчиков утечки газа, обеспечивает перекрытие зон и дублирование показаний. В дополнение, автоматизированные системы формирования управляющих воздействий быстро реагируют на сигналы датчиков, снижая вероятность ложных срабатываний и увеличивая оперативность реагирования [6].

6. Использование математических моделей и алгоритмов. Разработка математических моделей, отражающих отказные процессы, взаимодействие элементов системы, а также моделирование аварийных ситуаций и анализ рисков, позволяет проектировать более надежные системы защиты и принимать своевременные управленческие решения [7].

В настоящее время существует множество подходов к созданию систем противоаварийной защиты на объектах газодобывающих систем. Они имеют как концептуальное различие, так и разнообразие в вопросах реализации конкретных систем защиты.

В ходе исследования был определен критерий качества информации, как совокупность ее составляющих: точность, оперативность, достоверность, полнота, понятность. Каждый из этих составляющих находит свое соответствие с этапом реализации информационной системы. Связующим звеном выступает алгоритмическое обеспечение, позволяющее реализовать все критерии в комплексной информационной системе. Критерий качества информации представлен на рисунке 2.

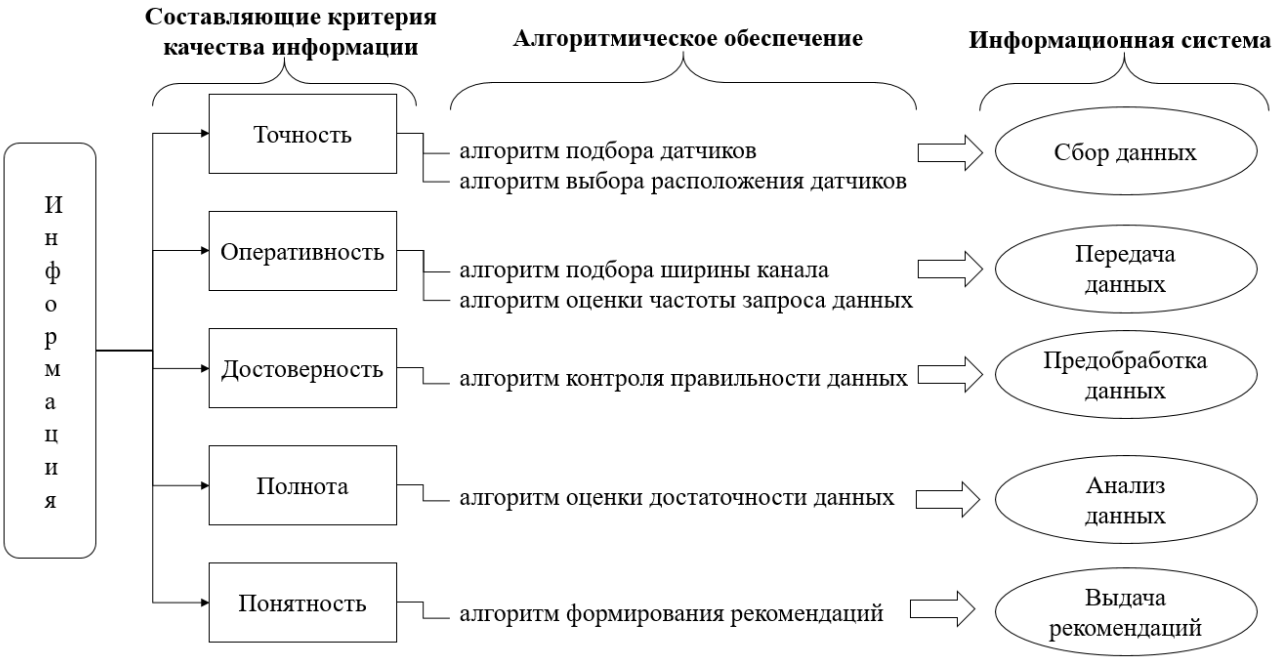


Рисунок 2 – Концептуальная схема взаимодействия параметров информации и этапов реализации информационной системы

Таким образом, обеспечение безопасности коллекторно-лучевых систем нефтегазовых скважин предполагает использование комплекса технологий, включающих автоматизированное и интеллектуальное управление, системы диагностики и мониторинга, математическое моделирование и системы противоаварийной защиты. Ключевым направлением является интеграция информационных технологий и автоматизированных систем, позволяющих быстро обнаруживать и реагировать на угрозы, что обеспечивает устойчивую и безопасную работу газодобывающих систем.

Список литературы

12 Телюк А.С. Синтез систем противоаварийной защиты для процессов подготовки продукции нефтегазовых скважин: диссертация ... кандидата технических наук: 05.13.06 / Телюк Антон Сергеевич; [Место защиты: Российский государственный университет нефти и газа имени И. М. Губкина]. – Москва, 2015. – 111 с.

13 Корниенко, В. Г. Оптимизация расстановки датчиков контроля воздушной среды, содержащей сероводород, на объектах нефтегазовой промышленности / В. Г. Корниенко, Р. С. Карабицин // Электронный сетевой политематический журнал "Научные труды КубГТУ". – 2014. – № 3. – С. 50-54.

14 Коптев, Н. П. Обеспечение безопасности технологических установок нефтепереработки с использованием систем противоаварийной защиты (на примере установки ЭЛОУ-АВТ-6) : специальность 05.02.21 : диссертация на соискание ученой степени кандидата технических наук / Коптев Николай Павлович. – Уфа, 2000. – 105 с.

15 Рогов, С. Л. Подсистемы противоаварийной защиты опасных производственных объектов в составе информационно-измерительных и управляющих систем : специальность 05.11.16 "Информационно-измерительные и управляющие системы (по отраслям)" : диссертация на соискание ученой степени кандидата технических наук / Рогов Сергей Львович. – Пенза, 2012. – 173 с.

5. Ульянова Т.С. Способ определения измерительной сложности приборов и устройств для построения информационно-измерительной системы / Т. С. Ульянова, С. С. Акимов //Автоматизация. Современные технологии. – 2023. – Т. 77, № 11. – С. 523-527.

6. Евсюткин, И. В. Интеллектуальная информационная система для управления фондом скважин нефтегазодобывающего предприятия : диссертация на соискание учёной степени кандидата технических наук : спец. 05.13.01 / И. В. Евсюткин ; Национальный исследовательский Томский политехнический университет ; науч. рук. Н. Г. Марков. – Томск, 2021. – 201 с.

7. Ульянова, Т. С. Определение точек контроля для обеспечения мониторинга работы системы сбора и транспортировки газа [Электронный ресурс] / Т. С. Ульянова, А. С. Боровский // Автоматизация и информатизация ТЭК, 2024. - № 9 (614). - С. 27-32. - 6 с.

ТРЕБОВАНИЯ К ЗАЩИТНЫМ КОНСТРУКЦИЯМ НА ОИАЭ В КОНТЕКСТЕ ПОВЫШЕНИЯ АНТИТЕРРОРИСТИЧЕСКОЙ ЗАЩИЩЕННОСТИ

Швец Г.К.
Санкт-Петербургский государственный электротехнический университет «ЛЭТИ» им. В.И. Ульянова (Ленина), г. Санкт-Петербург, Россия
Прищенко А.В., ассистент Балтийский государственный технический университет «ВОЕНМЕХ» им. Д.Ф. Устинова г. Санкт-Петербург, Россия

Аннотация: В статье рассматривается необходимость пересмотра требований к защитным конструкциям объектов использования атомной энергии (далее – ОИАЭ) в условиях повышения ядерной террористической угрозы. Анализируются параметры прочности, безопасности, конструктивного устройства и надежности, которыми должны обладать современные комплексные инженерные средства, установленные на режимных объектах.

Ключевые слова: защитные металлоконструкции, антитеррористическая защищенность, терроризм, ОИАЭ, режимные объекты.

Сегодняшняя глобальная геополитическая обстановка характеризуется повышенным уровнем угрозы террористических атак. Терроризм стал рычагом давления в руках ряда стран, добивающихся этим жестоким методом национальных, религиозных, политических и экономических целей. По данным Прокуратуры РФ за последние годы количество совершенных террористических актов выросло в 3 раза [1]. Резкое увеличение динамики диверсий вкупе с поступлением на вооружение террористических группировок современных типов вооружения, таких как БПЛА, БВУ, высокоточного оружия, требует незамедлительной реакции по защите гражданского населения и стратегически важной инфраструктуры.

Повышение антитеррористической защищенности объектов специального назначения имеет ключевое значение не только в силу материальных причин. Обеспечение безопасности режимных объектов является индикатором обороноспособности государства и поднимает уровень доверия к действиям власти. Поскольку промышленная и военная инфраструктура обладает статусом стратегически важных объектов, она наиболее часто подвергается атакам террористических группировок. Особое внимание следует уделить объектам использования атомной энергетики, ставшими целью международного ядерного терроризма, элементами которого являются незаконное использование атомной энергии, разработка ядерных взрывных устройств, захват или уничтожение атомных объектов [2]. На сегодняшний момент российскому обществу

малоизвестны случаи ядерных террористических актов, в связи с чем население не осознает потенциальные риски и масштаб последствий таких атак.

Выделим несколько причин необходимости разработки и внедрения предупредительных мер по борьбе с ядерным терроризмом. В первую очередь, ядерные теракты характеризуются непредсказуемостью последствий разрушений и большим материальным уроном независимо от масштаба утечек радиации. Даже при минимальных дозах радиоактивного вещества, попавшего в окружающую среду, необходимо осуществлять комплексную проверку на месте происшествия и ликвидировать зараженные территории. Приоритетной целью террористов могут стать атомные электростанции (далее – АЭС), которые станут мощнейшим источником техногенной катастрофы в случае осуществления ядерного теракта. Терроризм ставит своей главной задачей запугивание гражданского населения и подрыв доверия к действующей власти. В результате проведения террористической атаки на ОИАЭ общество начнет ощущать уязвимость и бессилие, а уверенность в действующей власти снизится [3]. Ситуация может усугубиться низким уровнем осведомленности населения об особенностях ядерных катастроф и радиофобией, проявляющейся через призму негативного отношения к применению ионизирующего излучения в любой сфере деятельности [2]. Захват ОИАЭ открывает для террористов возможность собственного производства ядерных взрывных устройств из высокообогащенного ядерного топлива, которые, в свою очередь, могут использоваться как инструмент шантажа органов государственной власти или привлечения внимания мирового сообщества [4].

Таким образом, угроза международного ядерного терроризма сформировала потребность разработки ряда предупредительных мер по обеспечению антитеррористической защищенности ОИАЭ. Это требует фундаментального пересмотра существующих требований к защитным конструкциям, особенно, к их наиболее уязвимым частям, которые подвергаются атакам террористов в первую очередь. К ним относятся защитно-герметические и противопожарные двери и ворота, укрытия бассейнов выдержки, хранилищ свежего топлива (ХСТ) и хранилищ отработанного ядерного топлива (ХОЯТ), ставни, люки, шлюзы-тамбуры и др. Взлом данных защитных металлоконструкций позволяет террористам беспрепятственно проникнуть на ОИАЭ, в закрытые служебные помещения, на склады радиоактивных веществ. Пересмотр конструкционных требований к защитным средствам, внедрение композитных материалов и повышение классов безопасности обеспечит максимальную устойчивость и значительно снизит риск проникновения террористов на ОИАЭ.

В сложившейся ситуации требуется разработка универсальных инженерных средств, обладающих комплексом необходимых параметров. Далее будут рассмотрены группы параметров, наличие которых у защитных металлоконструкций существенно уменьшит вероятность успешного исхода террористической атаки.

1) Параметры прочности. Прочность – это способность материала сопротивляться разрушению под действием установленного напряжения, возникающего в результате влияния внешних сил. Металлоконструкции в соответствии с НП-031-01 делятся на категории сейсмостойкости и должны обеспечивать прочность и сохранять работоспособность при возникновении различных факторов, действующих не единовременно. Системы и элементы атомных станций подразделяются на 3 категории: к I категории относятся все системы и элементы, выход из строя которых приводит к утечке радиоактивного вещества в производственные помещения и окружающую среду в объеме, который превышает установленные нормы [5]; ко II категории относятся все системы и элементы, выход из строя которых приводит к выходу из строя процессов электроэнергии и тепла; к III категории относятся все системы и элементы, не относящиеся к I и II категориям сейсмостойкости.

Универсальные защитные металлоконструкции должны быть устойчивы к колебаниям стен и перегородок зданий в чрезвычайных ситуациях, которые при разработке моделируются как сейсмические воздействия силой до максимального расчетного землетрясения (МРЗ – моделируемое землетрясение с периодичностью 1 раз в 10000 лет); воздействия силой планового землетрясения (ПЗ – моделируемое землетрясение с периодичностью 1 раз в 100 лет); воздействия импульса, возникающего от падения самолета на здание; воздействия импульса, возникающего от воздушной ударной волны на здания в результате подрыва изнутри и снаружи здания или запуска высокоточного боеприпаса. Для подтверждения способности сохранения прочности и герметичности во время и после прохождения различных сейсмических воздействий осуществляется расчет прочности. В рамках расчета обобщенные спектры ответов от сейсмических воздействий переводятся в баллы по балльной шкале интенсивности землетрясений MSK-64 [6]. Таким образом, можно наглядно увидеть, землетрясение какой мощности может выдержать рассматриваемая металлоконструкция.

2) Параметры безопасности. Не менее важными параметрами, задаваемыми при конструировании защитных инженерных средств, являются взломостойкость и пулестойкость, определяемые классом взломостойкости и классом защитной конструкции соответственно. Выделяют 4 класса устойчивости к взлому – чем выше класс, тем выше устойчивость

металлоконструкции к вскрытию. С увеличением класса растет число и класс замков, а, соответственно, и потенциальное среднее время взлома. Так, например, взлом двери I класса составляет 30-50 минут, в то время как нарушение устойчивости металлоконструкции IV класса займет у злоумышленника свыше 3 часов [7].

Кроме того, к защитным конструкциям предъявляются требования по пулестойкости в соответствии с разделением на 6 классов защитной структуры. Так, например, инженерные средства класса Бр 1 способны выдерживать расстрел пистолетным патроном с пулей калибра 9 мм; Бр 4 – патроном с пулей со стальным сердечником калибра 5,45 мм; Бр 5 – патроном с пулей со стальным сердечником калибра 7,62 мм; Бр 6 – патроном с пулей калибра 12,7 мм [7]. Класс пулестойкости имеет большое значение для металлоконструкций, толщина которых не превышает 20-30 мм, поскольку снайперская винтовка ОСВ-96 способна пробить лист стали толщиной 20 мм. В подобных случаях, защитная конструкция усиливается дополнительным бронеэлементов. Когда же толщина конструкции превышает 50 мм, класс пулестойкости имеет меньшее значение, поскольку из автоматического и снайперского оружия ее невозможно пробить.

3) Параметры конструктивного устройства. Антитеррористическая защищенность ОИАЭ должна также подразумевать устойчивость металлоконструкций к возникновению пожара, задымления или разгерметизации охраняемого объекта. Даже в случае, если защитная конструкция выдержит обстрел и атаку БПЛА, террористы могут устроить поджог или применить высокоточное оружие. В этой связи, металлоконструкции должны сохранять способность ограничивать в заданных пределах фильтрацию продуктов горения (предел дымогазонепроницаемости) и сохранять прежние свойства со времени нагрева и нагружения избыточным давлением (предел огнестойкости) [8]. Особенностью металлоконструкций на ОИАЭ являются повышенные требования к герметичности и радиационной защищенности помещений в условиях угрозы утечки радиоактивных веществ.

Помимо вышеописанных требований к параметрам металлоконструкций следует выделить повышенные требования к надежности: общий срок службы, превышающий 50 лет, вероятность отказа, не превышающая 0,1%, средний срок службы до проведения капитального ремонта, не менее 20% от общего срока службы. Несмотря на повышенную необходимость в антитеррористической защищенности ОИАЭ металлоконструкции должны быть удобны в эксплуатации, должны подвергаться монтажу и ремонту при среднем времени восстановления до работоспособного состояния, не превышающего 1 сутки. При наличии всех вышеописанных параметров руководство ОИАЭ должно определить целесообразность одинаковой степени усиления помещений,

хранилищ и складов, исходя из экономических причин – необходимо ли выделять денежные средства на усиление малозначительного элемента режимного объекта?

На сегодняшний момент крайне актуальным остается вопрос антитеррористической защищенности объектов специального назначения, в частности ОИАЭ. Соблюдение комплекса требований, предъявляемым к защитным конструкциям в условиях применения современных типов вооружения, позволит значительно снизить риск проникновения террористических группировок на закрытые объекты.

Список литературы

1. 588 заседание Совета Федерации / [Электронный ресурс] // Совет Федерации Федерального Собрания Российской Федерации : [сайт]. — URL: http://council.gov.ru/activity/meetings/165293/results/ (дата обращения: 08.09.2025).
2. Кобец, П. Н. Опыт и проблемы противодействия международному терроризму на объектах атомной энергетики / П. Н. Кобец // Научный портал МВД России. – 2019. – № 2(46). – С. 29-39.
3. Ениколопов, С. Н. Психологические последствия терроризма и роль СМИ в процессе их формирования / С. Н. Ениколопов, А. А. Мкртчян // Национальный психологический журнал. – 2010. – № 2(4). – С. 41-46.
4. Арбатов, А. Ядерный терроризм: политические, правовые, стратегические и технические аспекты / А. Арбатов, А. Пикаев, В. Дворкин // Мировая экономика и международные отношения. – 2006. – № 11. – С. 3-16.
5. НП-031-01. Нормы проектирование сейсмостойких атомных станций / утв. Постановлением Госатомнадзора России от 19 октября 2001 г. N 9. – М.: Госатомнадзор, 2001. – 30 с.
6. Нормы расчета на прочность оборудования и трубопроводных атомных энергетических установок. ПНАЭ Г-7-002-86. – М.: Энергоатомиздат, 1989.
7. ГОСТ Р 51072. Двери защитные. Общие технические требования и методы испытаний на устойчивость к взлому, пулестойкость и огнестойкость [Текст]. – Введ. 2007-01-01. – М. : Стандартинформ, 2007. – 9 с.
8. ГОСТ Р 53303. Конструкции строительные. Противопожарные двери и ворота. Метод испытаний на дымогазонепроницаемость [Текст]. – Введ. 2009-02-18. – М. : Стандартинформ, 2009. – 11 с.