АКТУАЛЬНЫЕ ИССЛЕДОВАНИЯ

МЕЖДУНАРОДНЫЙ НАУЧНЫЙ ЖУРНАЛ

ISSN 2713-1513

#14 (249), 2025

ЧАСТЬ I

Актуальные исследования

Международный научный журнал
2025 • № 14 (249)
Часть I

Издается с ноября 2019 года Выходит еженедельно

ISSN 2713-1513

РЕДАКЦИОННАЯ КОЛЛЕГИЯ

Кузнецов Игорь Анатольевич, кандидат медицинских наук, доцент, академик международной академии фундаментального образования (МАФО), доктор медицинских наук РАГПН, профессор, почетный доктор наук РАЕ, член-корр. Российской академии медико-технических наук (РАМТН) (Астраханский государственный технический университет)

Литвинова Жанна Борисовна, кандидат педагогических наук (Кубанский государственный университет)

Мамедова Наталья Александровна, кандидат экономических наук, доцент (Российский экономический университет им. Г.В. Плеханова)

Мукий Юлия Викторовна, кандидат биологических наук, доцент (Санкт-Петербургская академия ветеринарной медицины)

Никова Марина Александровна, кандидат социологических наук, доцент (Московский государственный областной университет (МГОУ))

Насакаева Бакыт Ермекбайкызы, кандидат экономических наук, доцент, член экспертного Совета МОН РК (Карагандинский государственный технический университет)

Олешкевич Кирилл Игоревич, кандидат педагогических наук, доцент (Московский государственный институт культуры)

Попов Дмитрий Владимирович, доктор филологических наук (DSc), доцент (Андижанский государственный институт иностранных языков)

Пятаева Ольга Алексеевна, кандидат экономических наук, доцент (Российская государственная академия интеллектуальной собственности)

Редкоус Владимир Михайлович, доктор юридических наук, профессор (Институт государства и права РАН)

Самович Александр Леонидович, доктор исторических наук, доцент (ОО «Белорусское общество архивистов»)

Сидикова Тахира Далиевна, PhD, доцент (Ташкентский государственный транспортный университет)

Таджибоев Шарифджон Гайбуллоевич, кандидат филологических наук, доцент (Худжандский государственный университет им. академика Бободжона Гафурова)

Тихомирова Евгения Ивановна, доктор педагогических наук, профессор, Почётный работник ВПО РФ, академик МААН, академик РАЕ (Самарский государственный социально-педагогический университет)

Хаитова Олмахон Саидовна, кандидат исторических наук, доцент, Почетный академик Академии наук «Турон» (Навоийский государственный горный институт)

Цуриков Александр Николаевич, кандидат технических наук, доцент (Ростовский государственный университет путей сообщения (РГУПС)

Чернышев Виктор Петрович, кандидат педагогических наук, профессор, Заслуженный тренер РФ (Тихоокеанский государственный университет)

Шаповал Жанна Александровна, кандидат социологических наук, доцент (Белгородский государственный национальный исследовательский университет)

Шошин Сергей Владимирович, кандидат юридических наук, доцент (Саратовский национальный исследовательский государственный университет имени Н.Г. Чернышевского)

Эшонкулова Нуржахон Абдужабборовна, PhD по философским наукам, доцент (Навоийский государственный горный институт)

Яхшиева Зухра Зиятовна, доктор химических наук, доцент (Джиззакский государственный педагогический институт)

СОДЕРЖАНИЕ

ТЕХНИЧЕСКИЕ НАУКИ

ВОЕННОЕ ДЕЛО

ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ

АРХИТЕКТУРА, СТРОИТЕЛЬСТВО

СЕЛЬСКОЕ ХОЗЯЙСТВО

ФИЛОЛОГИЯ, ИНОСТРАННЫЕ ЯЗЫКИ, ЖУРНАЛИСТИКА

СОЦИОЛОГИЯ

ТЕХНИЧЕСКИЕ НАУКИ

БАГМАНОВ Магомед Махир оглы
магистрант, Азербайджанский государственный университет нефти и промышленности, Азербайджан, г. Баку

ОБЗОР СОСТОЯНИЯ ПРОБЛЕМЫ ПАРАЛЛЕЛЬНЫХ ВЫЧИСЛЕНИЙ

Аннотация. *В этой статье показана актуальность проблемы высокопроизводительных вычислительных систем, которые необходимы в различных областях таких как: обработка изображений, видео потоков, больших данных и другие. Дан анализ основных технологий параллелизации вычислений. Показаны основные преимущества и недостатки указанных подходов.*

Ключевые слова: *параллельные вычисления, параллельность данных, параллельность задач, OpenMP, MPI, Cuda.*

Введение

Сегодня системы высокопроизводительных вычислений являются чрезвычайно актуальными, Многие задачи такие как обработка изображений в ограниченное время, работа с большими данными и другие возможны только при использовании высокопроизводительных вычислительных систем. Повышение производительности в первую очередь возможно за счет модернизации технических ресурсов, использования новых физических принципов. К сожалению, здесь имеются физические ограничения. Другой подход – это параллелизация, которая в принципе не ограничена.

Рассмотрим основные механизмы реализации параллельных вычислений на разных уровнях.

Одновременное выполнение многих задач или процессов с использованием различных вычислительных ресурсов, таких как несколько процессоров или компьютерных узлов, для решения вычислительной задачи называется параллельными вычислениями. Это метод повышения производительности и эффективности вычислений путем разделения сложной задачи на более мелкие подзадачи, которые могут быть выполнены одновременно.

Задачи разбиваются на более мелкие компоненты в параллельных вычислениях, причем каждый компонент выполняется одновременно на отдельном ресурсе компьютера. Эти ресурсы могут состоять из отдельных процессорных ядер в одном компьютере, сети компьютеров или специализированных высокопроизводительных вычислительных платформ.

Методы обеспечения параллельных вычислений

Были созданы различные фреймворки и модели программирования. Проектирование и реализация параллельных алгоритмов облегчаются абстракциями и инструментами этих моделей. Часто используемые модели программирования включают:

1. **Интерфейс передачи сообщений (MPI):** Интерфейс передачи сообщений (MPI) – популярный подход к разработке параллельных вычислительных систем, особенно в ситуациях с распределенной памятью. Благодаря передаче сообщений он обеспечивает связь и сотрудничество между различными процессами.

2. **CUDA:** NVIDIA разработала CUDA, платформу для параллельных вычислений и язык программирования. Она дает программистам возможность использовать параллельные вычисления общего назначения в полном объеме с помощью графических процессоров NVIDIA.

3. **OpenMP:** Для параллельного программирования с общей памятью. OpenMP является популярным подходом. Он позволяет программистам определять параллельные части в своем коде, которые затем обрабатываются

несколькими потоками, работающими на разных процессорах.

Существует 4 типа параллельных вычислений, и каждый тип параллельных вычислений описан ниже.

1. Параллелизм на уровне битов: Одновременное выполнение операций над несколькими битами или двоичными цифрами элемента данных называется параллелизмом на уровне битов в параллельных вычислениях. Это тип параллелизма, который использует возможности параллельной обработки аппаратных архитектур для одновременной работы с несколькими битами.

Параллелизм на уровне битов очень эффективен для операций с двоичными данными, таких как сложение, вычитание, умножение и логические операции. Время выполнения может быть значительно сокращено путем выполнения этих действий над несколькими битами одновременно, что приводит к повышению производительности.

Например, рассмотрим сложение двух двоичных чисел: 1101 и 1010. В рамках последовательной обработки сложение будет выполняться побитно, начиная с младшего бита (LSB) и перемещая все биты переноса в следующий бит. Сложение может выполняться одновременно для каждой пары связанных битов, когда используется параллелизм на уровне битов, используя возможности параллельной обработки. В результате возможно более быстрое выполнение, и производительность в целом повышается.

Специализированные аппаратные элементы, которые могут работать с несколькими битами одновременно, такие как параллельные сумматоры, умножители или логические вентили, часто используются для реализации параллелизма на уровне битов. Современные процессоры также могут иметь инструкции SIMD (Single Instruction, Multiple Data) или векторные процессоры, которые позволяют выполнять операции с несколькими компонентами данных, включая несколько битов, параллельно.

2. Параллелизм на уровне инструкций: ILP, или параллелизм на уровне инструкций, – это концепция параллельных вычислений, которая фокусируется на выполнении нескольких инструкций одновременно на одном процессоре. Вместо того чтобы полагаться на многочисленные процессоры или вычислительные ресурсы, она стремится использовать естественный параллелизм, присутствующий в программе на уровне инструкций.

Инструкции выполняются последовательно традиционными процессорами, одна за другой. Тем не менее, многие программы содержат независимые инструкции, которые могут выполняться одновременно, не мешая друг другу. Для повышения производительности параллелизм на уровне инструкций стремится распознавать и использовать эти отдельные инструкции.

Параллелизм на уровне инструкций может быть достигнут различными методами:

- **Конвейеризация:** Конвейеризация делит процесс выполнения инструкций на несколько шагов, каждый из которых может выполнять более одной команды одновременно. Это позволяет перекрывать выполнение многих инструкций, пока они находятся на разных стадиях выполнения. Каждый шаг выполняет отдельную задачу, например, выборку, декодирование, выполнение и обратную запись инструкций.
- **Выполнение вне очереди:** в зависимости от доступности входных данных и ресурсов выполнения процессор динамически перестраивает инструкции во время выполнения вне очереди. Это повышает эффективность использования исполнительных блоков и сокращает время простоя, позволяя выполнять независимые инструкции вне того порядка, в котором они были изначально закодированы.

3. Параллелизм задач

Идея параллелизма задач в параллельных вычислениях относится к разделению программы или вычисления на множество задач, которые могут выполняться одновременно. Каждая задача является автономной и может выполняться на отдельном процессорном блоке, например, на нескольких ядрах в многоядерном ЦП или узлах в распределенной вычислительной системе.

Разделение работы на отдельные задачи, а не разделение данных, является основным фокусом параллелизма задач. При одновременном выполнении задания могут использовать доступные возможности параллельной обработки и часто работают с различными подмножествами входных данных. Эта стратегия особенно полезна, когда задачи автономны или просто слабо зависят друг от друга.

Основная цель параллелизма задач – максимально использовать доступные вычислительные ресурсы и повысить общую

производительность программы или вычислений. По сравнению с последовательным выполнением, время выполнения может быть значительно сокращено путем одновременного запуска множества процессов.

Параллелизм задач может быть реализован различными способами, некоторые из которых описаны ниже:

- **Параллелизм на основе потоков:** это подразумевает разбиение одной программы на несколько потоков выполнения. При одновременном запуске на разных ядрах или процессорах каждый поток отвечает за отдельную задачу. Обычно разделяемая память системы основана на потоке параллелизма.
- **Параллелизм на основе задач:** В этой модели задачи явно определены и запланированы для выполнения. Планировщик задач динамически назначает задачи доступным ресурсам обработки, принимая во внимание зависимости и баланс нагрузки. Параллелизм на основе задач – это универсальный и эффективный метод выражения параллелизма, который может использоваться с другими парадигмами параллельного программирования.
- **Параллелизм на основе процессов:** этот метод подразумевает разделение программы на множество процессов, каждый из которых представляет отдельную задачу. В распределенной вычислительной системе процессы могут работать на разных вычислительных узлах одновременно. В системах с распределенной памятью часто используется параллелизм на основе процессов.

4. Параллелизм на уровне супер слов

Параллелизм на уровне супер слова – это концепция параллельных вычислений, которая концентрируется на использовании параллелизма на уровне слова или вектора для повышения производительности вычислений. Архитектуры, которые поддерживают SIMD (Single Instruction, Multiple Data) или векторные операции, особенно подходят для их использования.

Поиск и классификация действий с данными в векторные или массивные операции является основной концепцией параллелизма на уровне суперслов. Параллелизм, встроенный в данные, может быть полностью использован путем проведения вычислений над несколькими фрагментами данных в одной инструкции.

На уровне супер слов особенно полезен для приложений с предсказуемыми шаблонами доступа к данным и легко параллелизуемыми вычислениями. Он часто используется в приложениях, где много данных могут обрабатываться одновременно, например, при научном моделировании, обработке изображений и видео, обработке сигналов и анализе данных.

Применение параллельных вычислений

Параллельные вычисления широко применяются в различных областях, и некоторые из их приложений упомянуты ниже:

1. **Финансовое моделирование и анализ рисков:** В финансовом моделировании и анализе рисков параллельные вычисления используются для выполнения сложных вычислений и моделирования, необходимых в таких областях, как анализ рисков, оптимизация портфеля, ценообразование опционов и моделирование Монте-Карло. В финансовых приложениях параллельные алгоритмы способствуют более быстрому анализу и принятию решений.
2. **Аналитика данных и обработка больших данных:** для эффективной обработки и анализа больших наборов данных в современную эпоху больших данных параллельные вычисления стали решающими. Для ускорения обработки данных, машинного обучения и добычи данных параллельные фреймворки, такие, как Apache Hadoop и Apache Spark, распределяют данные и вычисления по кластеру компьютеров.
3. **Параллельные системы баз данных:** Для быстрой обработки запросов и управления большими объемами данных параллельные системы баз данных используют параллельные вычисления. Для повышения производительности базы данных и обеспечения одновременного доступа к данным используются методы параллелизации, такие как параллелизм запросов и секционирование данных.

Преимущества параллельных вычислительных систем:

- **Эффективность затрат:** Параллельные вычисления могут помочь вам сэкономить деньги, используя обычное оборудование с несколькими процессорами или ядрами вместо дорогостоящего специализированного оборудования. Это делает параллельные вычисления более доступными и экономически эффективными для различных приложений.

- **Отказоустойчивость:** Системы для параллельных вычислений часто могут быть построены так, чтобы быть отказоустойчивыми. Система может продолжать функционировать и быть надежной, даже если процессор или ядро выходят из строя, поскольку она может продолжать выполнять вычисления на других процессорах.
- **Эффективность ресурсов:** Параллельные вычисления используют ресурсы более эффективно, разделяя рабочую нагрузку между несколькими процессорами или ядрами. Параллельные вычисления могут максимизировать использование ресурсов и минимизировать время простоя вместо того, чтобы полагаться исключительно на один процессор, который может оставаться недоиспользованным для некоторых задач.
- **Решение крупномасштабных задач:** крупномасштабные задачи, которые невозможно эффективно решить на одной машине, лучше всего решать с помощью параллельных вычислений. Это позволяет разделить задачу на более мелкие части, распределить эти части по нескольким процессорам.
- **Масштабируемость:** добавляя больше процессоров или ядер, параллельные вычислительные системы могут увеличить свою вычислительную мощность. Эта масштабируемость позволяет успешно решать более крупные и сложные проблемы. Параллельные вычисления могут предложить ресурсы, необходимые для эффективного решения проблемы по мере ее роста.

Недостатки параллельных вычислительных систем:

- **Повышенные требования к памяти:** репликация данных на нескольких процессорах, которая часто происходит при параллельных вычислениях, может привести к более высоким требованиям к памяти. Объем памяти, необходимый крупномасштабным параллельным системам для хранения и управления реплицированными данными, может повлиять на стоимость и использование ресурсов.
- **Отладка и тестирование:** Отладка параллельных программ может быть сложнее, чем отладка последовательных. Состояния гонки, взаимоблокировки и проблемы неправильной синхронизации могут быть сложными и требующими много времени для выявления и устранения. Также сложнее тщательно тестировать параллельные программы, чтобы гарантировать надежность и точность.
- **Сложность:** Программирование параллельных систем, а также разработка параллельных алгоритмов может быть намного сложнее последовательного программирования. Зависимости данных, балансировка нагрузки, синхронизация и связь между процессорами должны быть тщательно учтены при использовании параллельных алгоритмов.

Заключение

Высокопроизводительные вычислительные системы сегодня являются одним из стратегических направлений развития прикладной науки. Именно параллелизация задач позволяет сегодня решать задачи, которые были недоступны ранее. Специалист, решающий прикладную задачу, должен владеть знаниями о различных технологиях организации параллельных вычислений. В этом контексте системное рассмотрение различных аспектов параллельных вычислений имеет важное значение.

Литература

1. Comparing traditional grids with high-performance computing. IBM. Jun 13, 2006. http://mcslp.com/gridpdfs/gr-tradhp.pdf
2. Dietz, Hank. "Linux Parallel Processing HOWTO." Aggregate.org. Jan. 5, 1998 Retrieved March 29, 2008. http://aggregate.org/LDP/19980105/pphowto.htm
3. Parallel processing. Search Data Center. March 27, 2007. Retrieved March 29, 2008. http://searchdatacenter.techtarget.com
4. Programming Models. Tommesani. Retrieved March 29, 2008. http://www.tommesani.com/ProgrammingModels.html

BAGMANOV Magomed Mahir oglu
Master's Student, Azerbaijan State University of Petroleum and Industry,
Azerbaijan, Baku

OVERVIEW OF THE STATE OF THE PROBLEM OF PARALLEL COMPUTING

Abstract. *This article shows the relevance of the problem of high-performance computing systems, which are necessary in various fields such as image processing, video streams, big data, and others. The analysis of the main technologies of computing parallelization is given. The main advantages and disadvantages of these approaches are shown.*

Keywords: *parallel computing, data parallelism, task parallelism, OpenMP, MPI, Cuda.*

ГЮЛЬАХМЕДОВА Наргиз Зейдулла гызы
магистрантка, Азербайджанский государственный университет нефти и промышленности, Азербайджан, г. Баку

СРАВНИТЕЛЬНЫЙ АНАЛИЗ ТРАДИЦИОННЫХ МЕТОДОВ ПРОГНОЗИРОВАНИЯ И МЕТОДОВ МАШИННОГО ОБУЧЕНИЯ

Аннотация. *В этой статье показана актуальность проблемы прогнозирования в различных областях экономики: образования, медицины. Дан анализ основных традиционных методов прогнозирования: скользящее среднее, экспоненциальное сглаживание, модель авторегрессии, модель ARİMA. Выявлены основные недостатки указанных методов. Показаны основные преимущества методов машинного обучения.*

Ключевые слова: *прогнозирование, дерево регрессии, машинное обучение.*

Введение

Прогнозирование с помощью машинного обучения – это процесс, который использует специальные алгоритмы для обучения на основе данных и составления прогнозов о будущих событиях.

Такие компании, как Walmart, IBM и другие используют прогнозирование для всего: от прогнозирования спроса до прогнозирования ценовых тенденций. Модели машинного обучения, такие как нейронные сети, могут учитывать гораздо больше данных, что позволяет создавать более точные предиктивные модели.

В этой статье мы рассмотрим основные причины, по которым машинное обучение является лучшим предсказателем, чем традиционные методы.

Машинное обучение – это подмножество искусственного интеллекта, которое определяется как процесс обучения компьютера обучению на основе данных. Он делает это путем выявления закономерностей и взаимосвязей в обучающих данных, чтобы компьютер мог делать прогнозы о будущих значениях и событиях. В то время как традиционные методы используют набор предопределенных правил для составления прогнозов, машинное обучение способно учиться и адаптироваться на основе любого объема данных.

Машинное обучение может использоваться для различных целей, таких как прогнозирование поведения потребителей, понимание рыночных тенденций, прогнозирование продаж или даже прогнозирование того, когда сервер может выйти из строя. Фактически, его можно использовать для любой проблемы, где есть данные временного ряда и цель предсказать будущее.

Традиционные методы прогнозирования

Чтобы понять, почему машинное обучение лучше подходит для прогнозирования, сначала рассмотрим некоторые традиционные методы прогнозирования временных рядов, такие как скользящее среднее, экспоненциальное сглаживание и ARIMA.

Скользящая средняя

Скользящее среднее – это способ сглаживания данных путем вычисления средневзвешенного значения прошлых значений. Это может быть полезно для устранения шума из данных и выявления тенденций. Однако оно также может быть восприимчиво к выбросам и не может учитывать сезонность.

Предположим, у нас есть данные о продажах за 5-летний период:

- 2020 $3 млн.
- 2021: $6 млн.
- 2022: $7 млн.
- 2023: $8 млн.
- 2024: $11 млн.

Прогноз на 2025 год составляет $7,2 млн, полученный из простого среднего значения за последние пять лет. Однако это не учитывает тот факт, что продажи растут с каждым годом.

Скользящая средняя обычно используется для сглаживания ряда данных. Существует несколько различных типов скользящих средних, в том числе:

- Простое Скользящее Среднее (SMA).
- Сглаженное Скользящее Среднее (SMMA).

- Взвешенное Скользящее Среднее (WMA).
- Экспоненциальное Скользящее Среднее (EMA).

Самый базовый тип скользящей средней – это простая скользящая средняя (SMA), которая рассчитывается путем взятия среднего значения заданного количества точек данных, прошлых и настоящих. Взвешенная скользящая средняя (WMA) учитывает относительную важность каждой точки данных, придавая большее значение недавним точкам данных.

Они обычно используются на финансовых рынках для сглаживания колебаний цен и получения более четкой картины тренда.

Экспоненциальное сглаживание

Экспоненциальное сглаживание – это метод прогнозирования, который учитывает как прошлые данные, так и недавние тенденции. Он использует средневзвешенное значение для расчета прогноза, при этом больше веса придается недавним данным. Это называется экспоненциальным сглаживанием, поскольку оно присваивает экспоненциально меньшие веса более старым наблюдениям. Это может помочь устранить эффекты выбросов.

Обычно это используется для прогнозирования ближайшего будущего, и существует также несколько типов экспоненциального сглаживания, в том числе:

- Простое Экспоненциальное Сглаживание (SES).
- Двойное Экспоненциальное Сглаживание (DES).
- Тройное Экспоненциальное Сглаживание (TES).

ARIMA

ARIMA (Autoregressive Integrated Moving Average) – еще одна модель, которая использует прошлые данные для прогнозирования будущих событий. Это более сложный метод, который включает в себя выполнение внутренней регрессии в пределах того же временного ряда вместо прогнозирования другого временного ряда.

Эти традиционные методы требуют длительной ручной работы и инженерии данных, что может быть сложным и дорогим. Машинное обучение, с другой стороны, способно автоматически учиться на данных и делать прогнозы без какого-либо вмешательства человека.

Оно может легко обрабатывать большие объемы данных и может определять закономерности и взаимосвязи, которые люди никогда не смогут найти. Расширение ARIMA, называемое SARIMA (или Seasonal ARIMA), поддерживает одномерные временные ряды данных с сезонным компонентом.

Методы машинного обучения

Давайте рассмотрим основные причины, по которым машинное обучение является лучшим предсказателем, чем традиционные методы.

1. Машинное обучение может выявлять закономерности, которые слишком сложны для наблюдения человеком

Одним из ключевых преимуществ машинного обучения является то, что оно может выявлять закономерности, которые слишком сложны для наблюдения человеком. Традиционные методы прогнозирования ограничены объемом данных, которые могут быть обработаны и проанализированы человеком.

Например, предположим, что мы хотим спрогнозировать цены на фондовом рынке. Традиционные методы полагаются на аналитиков, которые выявляют закономерности на рынке и делают прогнозы на основе исследований. Однако людям часто сложно определить все факторы, влияющие на цены акций. Машинное обучение может очень быстро анализировать большие объемы данных и выявлять закономерности, которые не видны людям. Это может привести к более точным прогнозам, чем традиционные методы.

2. Машинное обучение может делать прогнозы на основе гораздо большего набора данных, чем традиционные методы

Машинное обучение также может делать прогнозы на основе гораздо большего набора данных, чем традиционные методы.

Рассмотрим задачу прогнозирования продаж. Традиционный метод, такой как анализ тенденций, может учитывать только прошлые данные о продажах для составления прогноза. С другой стороны, машинное обучение может анализировать данные из социальных сетей, отзывов клиентов и других источников для составления более точного прогноза.

В дополнение к данным временных рядов модели машинного обучения могут учитывать данные о цепочке поставок и другие реальные показатели, обеспечивая большую точность прогнозирования спроса. Традиционное прогнозирование временных рядов не оправдывает ожиданий, когда дело касается больших данных.

3. Машинное обучение не так подвержено влиянию человеческих эмоций или субъективных мнений

Одним из самых больших недостатков традиционных методов прогнозирования является то, что они предвзяты из-за человеческих эмоций и субъективных мнений. Это может привести к неточным прогнозам, поскольку люди часто находятся под влиянием своих личных предубеждений и эмоций. Машинное обучение не так предвзято из-за человеческих эмоций или субъективных мнений, что приводит к более точным прогнозам.

Рассмотрим пример компании, которая рассматривает возможность открытия нового магазина. Традиционные методы прогнозирования могут быть предвзятыми из-за личных предубеждений людей, делающих прогнозы.

Например, они могут с большей вероятностью предсказать, что магазин будет успешным, если они лично в него вложились, независимо от доказательств. Машинное обучение, с другой стороны, не будет подвержено влиянию этих личных предубеждений и будет делать более точные прогнозы

Конечно, модели МО также могут быть предвзятыми, если данные, используемые для обучения моделей, имеют предвзятость. Однако, убедившись, что вы используете непредвзятые данные, вы можете положиться на перекрестную проверку, чтобы узнать, является ли модель, которую вы создаете, точной.

4. Машинное обучение может быстро адаптироваться к изменениям

Машинное обучение также может адаптироваться к изменениям в наборе данных, тогда как традиционные методы могут со временем стать менее точными. По мере изменения набора данных машинное обучение соответствующим образом адаптирует свои прогнозы. Это гарантирует, что прогнозы всегда будут точными и актуальными. Традиционные методы, с другой стороны, могут со временем стать менее точными по мере изменения набора данных.

Например, предположим, что у вас есть набор данных, состоящий из данных о покупках клиентов. Со временем клиенты в этом наборе данных могут измениться. Традиционный подход заключается в перестройке прогноза с новым набором данных, что затем даст новые предсказания. Однако, если вы используете машинное обучение, модель может автоматически адаптироваться к новому набору данных.

5. Машинное обучение не так легко поддается манипуляциям, как традиционные методы

Машинное обучение также менее легко поддается манипуляциям, чем традиционные методы. Поскольку машинное обучение опирается на алгоритмы для составления прогнозов, манипулировать прогнозами гораздо сложнее, чем манипулировать прогнозами, сделанными традиционными методами. Это приводит к более точным прогнозам.

6. Машинное обучение – более эффективное использование ресурсов

Машинное обучение – более эффективное использование ресурсов, чем традиционные методы. Традиционные методы часто требуют большого объема ручной работы, которая может быть трудоемкой и дорогостоящей. Современный руководитель понимает, что для сохранения конкурентоспособности ему необходимо сосредоточиться на использовании технологий для получения конкурентного преимущества. Машинное обучение может автоматизировать процесс составления прогнозов, что является более эффективным использованием ресурсов.

7. Машинное обучение более доступно, чем традиционные методы

Машинное обучение также более доступно, чем традиционные методы. Традиционные методы часто требуют специальных знаний и обучения. Машинное обучение, с другой стороны, становится более доступным по мере развития технологий. Сейчас существует множество программных платформ, которые позволяют любому человеку создавать модели машинного обучения без каких-либо предварительных знаний или опыта.

Процесс прогнозирования с помощью машинного обучения состоит из четырех основных этапов: сбор данных, предварительная обработка данных, обучение модели и оценка модели.

Естественно, первым шагом является сбор данных, поскольку данные питают все модели машинного обучения. Добыча данных относится к процессу сбора и анализа исторических данных из различных источников, будь то scraping в Интернете, извлечение информации из форм или просто соответствующих таблиц Excel. Модели временных рядов требовательны

к форматированию данных, поэтому в данных должны быть четкие «временные шаги».

Предварительная обработка данных очищает и подготавливает данные для использования в алгоритме машинного обучения. Этот шаг включает в себя такие вещи, как удаление шумных данных, стандартизация данных, проектирование признаков и преобразование данных в формат, который может понять алгоритм. Даже традиционные статистические методы требуют предварительной обработки данных.

Традиционно для выполнения предварительной обработки данных с помощью таких инструментов, как Python, требовались технические таланты. Однако с появлением платформ самообслуживания, бизнес-пользователи теперь могут легко очищать и подготавливать свои данные без помощи ИТ-отдела. Это увеличило внедрение прогнозирования машинного обучения в бизнес-средах.

Как только данные готовы, алгоритм машинного обучения обучается на них. Это включает выбор типа модели и настройку ее параметров. После обучения модель используется для прогнозирования будущих событий. Затем производительность модели оценивается путем сравнения ее прогнозов с фактическими результатами.

Современные системы создают ряд моделей машинного обучения в фоновом режиме для любой заданной проблемы, чтобы максимизировать точность. В зависимости от набора данных это включает деревья решений, модели ARIMA, сети с долговременной краткосрочной памятью, рекуррентные нейронные сети (RNN), LSTM и другие методы глубокого обучения. Различные методы оптимизации используются в этих методах машинного обучения, обеспечивая большую точность, чем при использовании только одной модели.

Раньше компаниям приходилось нанимать специалистов по данным, чтобы использовать такие инструменты, как TensorFlow и Keras для создания этих моделей, но теперь любой нетехнический бизнес-профессионал может создавать и развертывать модели в несколько кликов.

Предположим, мы хотим спрогнозировать доход компании. Этап предварительной обработки данных будет включать удаление любых шумных данных, таких как ошибки в данных о продажах, и стандартизацию данных, чтобы все значения имели одинаковую шкалу. Этап обучения модели будет включать поиск закономерностей в данных для построения модели, которая может предсказывать будущий доход. Этап оценки модели будет включать сравнение прогнозов модели с фактическими результатами по доходу.

Машинное обучение становится все более важным инструментом прогнозирования. Понимая, как оно работает, вы можете воспользоваться его возможностями для более точных прогнозов для вашего бизнеса.

Заключение

Прогнозирование с помощью машинного обучения может делать прогнозы о будущих событиях, которые гораздо точнее, чем прогнозы, сделанные людьми. Ключ к этой точности – способность машины учиться на огромных объемах данных.

Машинное обучение может предсказывать тенденции фондового рынка, погодные условия или даже распространение заболеваний. Алгоритмы машинного обучения могут анализировать данные из социальных сетей и других источников для выявления закономерностей передачи заболеваний. Это позволяет должностным лицам здравоохранения разрабатывать подробные планы по смягчению распространения заболеваний.

Различные предприятия также могут использовать машинное обучение для улучшения прогнозирования. Например, розничный бизнес может использовать машинное обучение для прогнозирования того, сколько запасов ему понадобится для удовлетворения спроса клиентов. Это позволит предприятию избежать дефицита и упущенных продаж.

Литература

1. Ahmed N.K., Atiya A.F., Gayar N.E., El-Shishiny H. An empirical comparison of machine learning models for time series forecasting. Econometric Reviews, (2010).

2. Mohit Gurnani et al. “Forecasting of sales by using fusion of machine learning techniques”. In: 2017 International Conference on Data Management, Analytics and Innovation (ICDMAI). (2017).

3. Montgomery D.C., Jennings C.L., Kulahci M. Introduction to time series analysis and forecasting. John Wiley & Sons. (2015).

4. Negnevitsky M., Mandal P., Srivastava A.K. "An overview of forecasting problems and techniques in power systems," in Proc. IEEE Power and Energy Soc.General Meeting, P. 1-4, (2009).

5. Mitchell R., Michalski J., Carbonell T. An artificial intelligence approach Berlin: Springer, (2013).

6. Taieb S.B. Machine learning strategies for multi-step-ahead time series forecasting. Universit Libre de Bruxelles, Belgium, P. 75-86, (2014).

7. Paliyawan P. Stock market direction prediction using data mining Classification. future, 5, 6, (2006).

GULAKHMEDOVA Nargiz Zeidulla gizi
Graduate Student, Azerbaijan State University of Petroleum and Industry,
Baku, Azerbaijan

COMPARATIVE ANALYSIS OF TRADITIONAL FORECASTING METHODS AND MACHINE LEARNING METHODS

Abstract. *This article shows the relevance of the forecasting problem in various fields of economics: education, medicine. The analysis of the main traditional forecasting methods is given: moving average, exponential smoothing, autoregression model, ARIMA model. The main disadvantages of these methods have been identified. The main advantages of machine learning methods are shown.*

Keywords: *forecasting, regression tree, machine learning.*

ИВАНОВ Илья Андреевич
курсант, Военный учебно-научный центр Военно-воздушных сил «Военно-воздушная Академия имени профессора Н. Е. Жуковского и Ю. А. Гагарина», Россия, г. Воронеж

Научный руководитель – начальник факультета летательных аппаратов Военного учебно-научного центра Военно-воздушных сил «Военно-воздушной Академии имени профессора Н. Е. Жуковского и Ю. А. Гагарина», кандидат технических наук, доцент Маяцкий Сергей Александрович

НЕЙРОННАЯ СЕТЬ НА ЯЗЫКЕ ПРОГРАММИРОВАНИЯ C++

Аннотация. *В статье представлены общие сведения об архитектуре нейронных сетей, написанных языке программирования C++. Нейронная сеть, написанная на C++, показывает в полной мере ее обучение тем или иным действиям.*

Ключевые слова: *нейронная сеть, обучение, C++.*

Нейронная сеть (также искусственная нейронная сеть, ИНС, или просто нейросеть) – математическая модель, а также её программное или аппаратное воплощение, построенная по принципу организации биологических нейронных сетей – сетей нервных клеток живого организма.

Нейронная сеть состоит из большого числа нейронов, способных выполнять различного рода и сложности задачи. Так, на рисунке 1, представлена простейшая архитектура ИНС, состоящей одного нейрона входного слоя, трех нейронов скрытого слоя, а также нейрона выходного слоя.

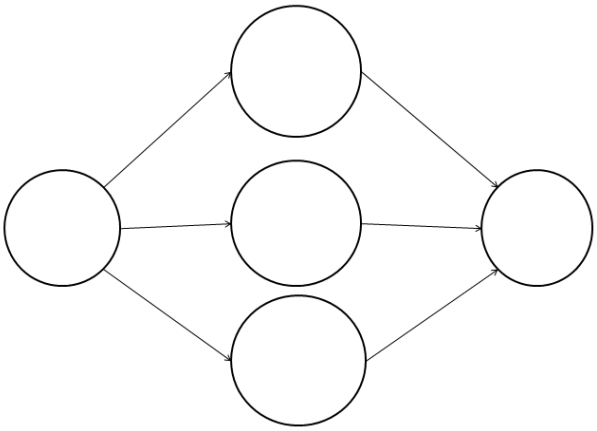


Рис. 1. Архитектура простейшей нейронной сети

Один нейрон может выполнять простейшие вычисления, но основные функции нейросети обеспечиваются не отдельными нейронами, а соединениями между ними. Однослойный перцептрон представляет собой простейшую сеть, которая состоит из группы нейронов, образующих слой. Входные данные кодируются вектором значений, каждый элемент подается на соответствующий вход каждого нейрона в слое. В свою очередь, нейроны вычисляют выход независимо друг от друга. Размерность выхода (то есть количество элементов) равна количеству нейронов, а количество синапсов у всех нейронов должно быть одинаково и совпадать с размерностью входного сигнала.

Обучение нейронной сети – это процесс, в котором параметры нейронной сети настраиваются посредством моделирования среды, в которую эта сеть встроена. Тип обучения определяется способом подстройки параметров. Различают алгоритмы обучения с учителем и без учителя. Процесс обучения с учителем представляет собой предъявление сети выборки обучающих примеров. Каждый образец

подается на входы сети, затем проходит обработку внутри структуры НС, вычисляется выходной сигнал сети, который сравнивается с соответствующим значением целевого вектора, представляющего собой требуемый выход сети. Данная схема обучения представлена на рисунке 2.

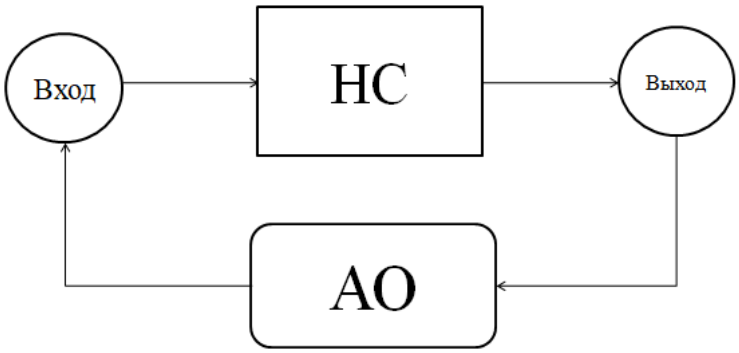


Рис. 2. Схема обучения нейронной сети, где НС – нейронная сеть, АО – анализатор ошибок

Основным методом обучения является градиентный спуск, который используется для минимизации ошибки, скорость которой задается непосредственно вручную (обозначают ее α).

Чтобы нейронная сеть начала свое обучение для этого необходима функция активации.

Функция активации в нейронных сетях – **это математическая модель, заданная в виде функции, применяемая к выходному сигналу нейрона.** Ее цель – внести нелинейность в модель, что позволяет сети обучаться и представлять сложные закономерности в данных. Без нелинейности нейронная сеть вела бы себя как линейная функция, независимо от количества слоев.

Функция активации решает, следует ли активировать нейрон или нет, путём вычисления взвешенной суммы и дальнейшего добавления к ней смещения. Существуют различные варианты функции активации, например: сигмовидная функция sigmoid, функция гиперболического тангенса tanh, функция максимизации значений ReLU.

Веса w_i и смещения b в нейронной сети – это регулируемые параметры, которые определяют, как сеть обрабатывает данные. **Веса** определяют силу связей между нейронами и фиксируют взаимосвязи между входными характеристиками и целевыми выходными значениями. **Смещения** обеспечивают гибкость заданной функции, что позволяет нейронам активироваться в ответ на различные входные условия. Таким образом, зная входные значения x_i, можно составить формулу для определения выходного значения yдля нейронной сети, состоящей из n количества нейронов.

$$y = \sum_{i=0}^{n} x_i w_i + b, \quad (1)$$

C++ является классикой программирования, без которой ни один профессиональный программист не может выполнять задачи программирования. На ней также возможно написание простейшей нейронной сети, которая представлена ниже.

Для работы нейронной сети, написанной на C++ Builder, требуется подключение нужных библиотек, а именно: math.h, ctime, fstream, iostream (рис. 3).

```
//---------------------------------------------------------------------------
#include "math.h"
#include "ctime"
#include "fstream"
#include "iostream"
#include <vcl.h>
#pragma hdrstop

#include "Unit1.h"
//---------------------------------------------------------------------------
#pragma package(smart_init)
#pragma resource "*.dfm"
TForm1 *Form1;
using namespace std;
```

Рис. 3. Подключаемые библиотеки C++

Далее, вводятся значения, необходимые для программирования и обучения нейронной сети (рис. 4).

```
float nin, n[100], nout;
float w12[100], w23[100];
float b[100], bout;
float alph;
float y[100], x[100];
float grnin, grnout[100];
float  outt, out[100];
int i;
bool l1=true;
bool flag=true;
```

Рис. 4. Значения, необходимые для работы нейронной сети

За nin обозначается нейрон входного слоя, n[100] – 100 нейронов скрытого слоя, nout – нейрон выходного слоя, w12[100] – инициализируемые 100 весов связи между входным и скрытым слоями нейронов, w23[100] – инициализируемые 100 весов связи между скрытым и выходным слоями нейронов, b – инициализируемые 100 смещения весов связи между входным и скрытым слоями нейронов, bout – смещение весов между скрытым и выходным слоем, alph – скорость (шаг) обучения.

Далее, пишется безразмерная функция readF(), позволяющая считывать значения с некоторого файла iksiki.txt, являющиеся входными x[i] и выходными значениями y[i], которым должна обучиться нейронная сеть (рис. 5).

```
void readF()
        {
ifstream X ("C:\\Users\\Admin329\\Desktop\\IskIntel\\iksiki.txt");
        if(X.is_open())
        {
        int i=0;
         for(i=0; i<100; i++)
                {
                  X>>x[i]>>y[i];
                }
        }

        X.close();
        }
```

Рис. 5. Функция для считывания текста с файла

Сама нейронная сеть представлена в виде функции десятичных чисел, рассчитываемая значения nin, n[100] и nout, рассчитываемая через функцию активации типа tanh, так как является самой оптимальной среди всех представленных выше функций и может охватывать больший диапазон значений. Функция выводит значение nout (рис. 6).

```
float network (float x1)
   {
   nin=tanh(x1);
   for (i = 0; i < 100; i++)
                {
                n[i]=tanh(nin*w12[i]+b[i]);
                }
   for (i = 0; i < 100; i++)
                {
                nout=tanh(n[i]*w23[i]);
                }
   nout=tanh(nout+bout);
   return nout;
   }
```

Рис. 6. Функция нейронной сети

Для наиболее качественного обучения, требуется инициализация весов. Инициализация представлена на рисунке 7 через функцию rand(), генерируя «случайные» числа, в безразмерной функции ini().

```
void ini()
        {
        srand(time(0));
        for (i = 0; i < 100; i++)
                {
                w12[i]=rand()%200-100;
                w23[i]=rand()%200-100;
                b[i]=rand()%100-50;
                w12[i]=w12[i]/100;
                w23[i]=w23[i]/100;
                b[i]=b[i]/100;
                }

        }
```

Рис. 7. Функция инициализации весов

Обучение нейронной сети представлено через функцию десятичных чисел teach(floaty_ns, floaty_zad) в виде градиентного спуска. Данная функция также обновляет веса, если значения, посчитанные нейросетью, не совпадают с заданными выходными значениями. Для обновления весов требуется производная функции активации, которая рассчитывается по следующей формуле:

$$f(x)' = 1 - f(x)^2, (2)$$

Зная производную функции активации каждого слоя и задав скорость обучения alph, функция обновляет и инициализирует новые веса (рис. 8).

```
float teach(float y_ns, float y_zad)
        {
        int i=0;
                        grnin=(y_zad-y_ns)*(1-pow(nout,2));

        for( i=0; i<100; i++)
                {
                grnout[i]=1-pow(nout,2)*grnin*w23[i] ;
                }
        for (i = 0; i < 100; i++)
                {
                w12[i]=w12[i]+grnout[i]*nin*alph;
                w23[i]=w23[i]+grnin*n[i]*alph;
                }
        }
```

Рис. 8. Функция обучения ИНС методом градиентного спуска

После создания кнопки Button1, в нее закладывается расчет и построение графиков, выверенные через те функции, которые находятся вне данной кнопки. Для вывода значения функции network добавляется переменная out[i]. Через нее строится график Series1, который определяется нейронной сетью, когда Series2 строится по переменной y[i], являющейся заданной функцией (рис. 9).

```
//---------------------------------------------------------------------------
__fastcall TForm1::TForm1(TComponent* Owner)
        : TForm(Owner)
{
}
//---------------------------------------------------------------------------
void __fastcall TForm1::Button1Click(TObject *Sender)
{
flag=true;
        int i=0;
        l1=true;
        alph=StrToFloat(LabeledEdit1->Text);
        readF();
        ini ();
        while(flag==true)
        {
         Series1->Clear();
         Series2->Clear();
                for (i = 0; i < 100; i++)
                {
                out[i]=network(x[i]);
                Series1->AddXY(x[i],out[i]);
                Series2->AddXY(x[i],y[i]);
                }
        srand(time(0));
        int r=rand()%50;
        float outt=network(x[r]);
        teach (outt,y[r]);
        Application->ProcessMessages();
        }


}
//---------------------------------------------------------------------------
```

Рис. 9. Код для построения графиков

Для того чтобы стереть графики в приложении, добавляется кнопка Button2, и пишется логическое равенство flag=false (рис. 10).

```
//---------------------------------------------------------------------------

void __fastcall TForm1::Button2Click(TObject *Sender)
{
flag=false;
}
//---------------------------------------------------------------------------
```

Рис. 10. Код для стирания графиков с приложения

Результатом будет являться построение функции в приложении. Таким образом, нейронная сеть, написанная на языке программирования C++ в полной мере, выполняет поставленные ей задачи и строит график, максимально приближенный к графику с исходными значениями, взятыми из файла.

Литература

1. https://ru.wikipedia.org/wiki/Нейронная_сеть.
2. https://sky.pro/wiki/python/kak-rabotaet-nejronnaya-set/.
3. https://ru.wikipedia.org/wiki/Функция_активации.
4. Гафаров Ф.М., Галимянов А.Ф. Искусственные нейронные сети и их приложения. – Казань: Изд-во Казан. ун-та, 2018. – 121 с.
5. Программирование на C++ в примерах и задачах / А. Васильев. – Москва: Эксмо, 2023. – 368 с. – (Российский компьютерный бестселлер).
6. Основы глубокого обучения. Создание алгоритмов для искусственного интеллекта следующего поколения / Н. Будума, Н. Локашо: пер. с англ. А. Коробейникова; [науч. ред. А. Созыкин]. – М.: Манн, Иванов и Фербер, 2020.
7. Нейронные сети: полный курс, 2-е изд.: Пер. с англ. – М.: ООО «И.Д. Вильямс», 2016. – 1104 с.: ил. – Парал. тит. англ.
8. https://msu.ai/neural_networks_notebook.
9. https://www.geeksforgeeks.org/activation-functions-neural-networks/.

IVANOV Ilya Andreevich
Cadet, Military Training and Research Center of the Air Force "Military Air Academy named after Professor N. E. Zhukovsky and Yu. A. Gagarin", Russia, Voronezh

Scientific Advisor – Head of the Faculty of Aircraft of the Military Training and Scientific Center of the Air Force "Air Force Academy named after Professor N. E. Zhukovsky and Yu. A. Gagarin", Candidate of Technical Sciences, Associate Professor Mayatsky Sergey Aleksandrovich

NEURAL NETWORKS IN C++ PROGRAMMING LANGUAGE

Abstract. *The article provides general information about the architecture of neural networks written in the C++ programming language. A neural network written in C++ fully demonstrates its learning of certain actions.*

Keywords: *neural network, learning, C++.*

ВОЕННОЕ ДЕЛО

ТЕЛЕГИН Алексей Андреевич
слушатель,
Военная академия материально-технического обеспечения
имени генерала армии А. В. Хрулева, Россия, г. Санкт-Петербург

ТУКАЛО Евгений Борисович
слушатель,
Военная академия материально-технического обеспечения
имени генерала армии А. В. Хрулева, Россия, г. Санкт-Петербург

САФОНОВ Дмитрий Александрович
преподаватель,
Военная академия материально-технического обеспечения
имени генерала армии А. В. Хрулева, Россия, г. Санкт-Петербург

ЧЕРНЕНКО Александр Николаевич
преподаватель,
Военная академия материально-технического обеспечения
имени генерала армии А. В. Хрулева, Россия, г. Санкт-Петербург

БЕЛЯЕВ Валентин Юрьевич
преподаватель,
Военная академия материально-технического обеспечения
имени генерала армии А. В. Хрулева, Россия, г. Санкт-Петербург

ПОВЫШЕНИЕ ЭФФЕКТИВНОСТИ ДИАГНОСТИРОВАНИЯ СИЛОВЫХ УСТАНОВОК АВТОМОБИЛЬНОЙ ТЕХНИКИ В СПЕЦИАЛЬНОЙ ВОЕННОЙ ОПЕРАЦИИ

Аннотация. *В статье рассматривается применение автомобильной техники войск национальной гвардии Российской Федерации в зоне проведения специальной военной операции, мероприятия по поддержанию ее исправного состояния, внедрение новых метода и средства технического диагностирования, которые позволили бы в кратчайшие сроки установить техническое состояние цилиндропоршневой группы двигателя автомобильной техники.*

Ключевые слова: *автомобиль многоцелевого назначения, автомобиль специального назначения, цилиндропоршневая группа, средства технического диагностирования, техническое диагностирование техники.*

В настоящее время в ходе специальной военной операции в войсках национальной гвардии Российской Федерации (ВНГ РФ) основным средством перевозки воинских грузов являются бортовые автомобили многоцелевого и общетранспортного назначения унифицированных семейств «Мустанг-М» и «Мотовоз-1». Так же широко используются бронированные автомобили ГАЗ-233014, АМН 233114 и АСН 233115 «Тигр-М», в основном применяются для

перевозки личного состава при выполнении боевых задач, сопровождения колонн, обеспечения мобильности разведывательных подразделений и подразделений специального назначения.

Автомобили с грузовой платформой повышенной проходимости (автомобили многоцелевого назначения с бортовой платформой и автомобильные базовые шасси) применяются в основном для выполнения задач материально-технического обеспечения и других видов обеспечения, перевозки личного состава и воинских грузов, монтажа и транспортирования вооружения, военной и специальной техники. В ходе специальной военной операции автомобили многоцелевого назначения эксплуатируются на дорогах всех категорий, в том числе грунтовых, в отдельных случаях местности, а автомобили общетранспортного назначения эксплуатируются в основном по дорогам с твердым покрытием.

Регулярно совершенствуется комплекс мероприятий по поддержанию автомобильной техники (АТ) в состоянии, обеспечивающем её умелое боевое применение [1, с. 26-31]. Своевременное применение АТ по назначению возможно при условии поддержания исправного (работоспособного) состояния силовой установки, в том числе цилиндропоршневой группы (ЦПГ) двигателя АТ. Важной составляющей комплекса мер по поддержанию постоянной боевой готовности образцов ВВСТ является разработка и внедрение новых методов и средств технического диагностирования техники ВНГ РФ, которые позволили бы в кратчайшие сроки установить её техническое состояние, а при наличии неисправности на более ранней стадии определить и локализовать её.

Техническое диагностирование обеспечивает целенаправленное проведение работ по поддержанию технического состояния АТ с целью их эффективного использования при выполнении задач по прямому предназначению. Система технического диагностирования (контроля технического состояния) – это совокупность средств, объекта и исполнителей, необходимая для проведения диагностирования (контроля) по правилам, установленным в технической документации. Задачами технического диагностирования являются: контроль технического состояния, поиск места и определение причин отказа, прогнозирование технического состояния [2, с. 54-59]. Повышение достоверности и полноты технического диагностирования позволяет установить объективно необходимый объем работ по техническому обслуживанию и ремонту, а также сократить трудоёмкость и время, отводимое на их выполнение, снизить расход запасных частей.

Эксплуатационная надежность техники в значительной степени определяется техническим состоянием двигателя внутреннего сгорания (ДВС), непосредственно состоянием ЦПГ. Большое количество существующих методов контроля технического состояния ДВС требуют значительных трудозатрат, использования дорогостоящего диагностического оборудования и могут быть реализованы только в стационарных условиях. Как правило, эти методы и средства технического диагностирования (СТД) основаны на необходимости пуска двигателя, выполнении работ по демонтажу отдельных его деталей с последующей их установкой на штатное место. Выполнение этих условий не всегда приемлемо. Так, при ведении боевых действий, при нахождении автомобильной техники в прифронтовой зоне, пуск двигателя для диагностирования неизбежно приведет к обязательному инфракрасному излучению и, как следствие, демаскировке мест сосредоточения техники и огневому поражению противником. В случае если двигатель не пускается из-за неисправности либо по другим причинам, то определить техническое состояние ЦПГ двигателя существующими методами и техническими средствами практически невозможно. Эти факты указывают на несовершенство системы технического диагностирования.

Исходя из чего возникает необходимость в совершенствовании системы технического диагностирования по средствам разработки и внедрения метода и средства технического диагностирования состояния ЦПГ, которые исключили бы из перечня выполняемых работ пуск двигателя и демонтаж отдельных его приборов (узлов) при диагностировании.

Средство должно содержать:

- элементы контроля;
- элементы устройства, в которых будет находиться подаваемый под давлением воздух;
- соединительные элементы.

Средство технического диагностирования позволит выполнить работы по

диагностированию деталей цилиндропоршневой группы двигателя [3, с. 80-85].

При использовании предлагаемого метода полностью исключена необходимость обязательного пуска двигателя, его прогрев и работа на холостом ходу. Также из перечня работ исключена необходимость демонтажа деталей систем двигателя. Это позволит сократить трудоёмкость и время, отводимое на диагностирование двигателя, повысит экономические показатели, исключит износ резьбовых и электрических соединений.

Предлагаемый Метод диагностирования цилиндропоршневой группы двигателя найдет применение как в стационарных, парковых условиях, так и при выполнении служебно-боевых задач при развертывании сборного пункта поврежденных машин (участка по ремонту вооружения, военной и специальной техники). В данном случае кроме снижения временных, экономических показателей и трудозатрат при выполнении работ по диагностированию будет исключена возможность создания инфракрасного излучения, которое приведет к демаскировке и как итог обнаружения разведывательными средствами противника.

Метод обладает, кроме всех перечисленных преимуществ, способностью выполнять прогнозирование остаточного ресурса двигателя, что позволит применять решение на использование отдельно взятой единицы техники для выполнения конкретной задачи.

Литература

1. Анализ существующих методов диагностирования цилиндропоршневой группы двигателей внутреннего сгорания. Разработка метода диагностирования цилиндропоршневой группы многоцилиндрового двигателя специального колесного шасси без инициализации рабочего процесса / А.А. Телегин, В.И. Никорчук, А.С. Рыжовцев [и др.] // Наука и военная безопасность. – 2024. – № 1(36). – С. 26-31. – EDN CBEDYF.

2. Анализ причин, вызывающих изменения технического состояния двигателей специальных колесных шасси, зависимость изменения основных технических показателей двигателя от величины износа деталей цилиндропоршневой группы / А.А. Телегин, С.С. Барсуков, Д.В. Селюк [и др.] // Наука и военная безопасность. – 2024. – № 4(39). – С. 54-59. – EDN DJLHEG.

3. Нечаев В.В. Определение технического состояния цилиндропоршневой группы двигателя при холодной, пусковой прокрутке коленчатого вала / В.В. Нечаев, К.В. Головко // Проблемы развития технологий создания, сервисного обслуживания и использования технических средств в агропромышленном комплексе: Материалы международной научно-практической конференции, ВОРОНЕЖ, 15-16 ноября 2017 года / Под общей редакцией Н.И. Бухтоярова, В.И. Оробинского. Том Часть I. – ВОРОНЕЖ: Воронежский государственный аграрный университет им. Императора Петра I, 2017. – С. 80-85. – EDN XOOXPN.

TELEGIN Alexey Andreevich
Listener, Military Academy of Logistics named after General of the Army A. V. Khrulev,
Russia, St. Petersburg

TUKALO Evgeny Borisovich
Listener, Military Academy of Logistics named after General of the Army A. V. Khrulev,
Russia, St. Petersburg

SAFONOV Dmitry Alexandrovich
Teacher, Military Academy of Logistics named after General of the Army A. V. Khrulev,
Russia, St. Petersburg

CHERNENKO Alexander Nikolaevich
Teacher, Military Academy of Logistics named after General of the Army A. V. Khrulev,
Russia, St. Petersburg

BELYAEV Valentin Yurievich
Teacher, Military Academy of Logistics named after General of the Army A. V. Khrulev,
Russia, St. Petersburg

IMPROVING THE EFFICIENCY OF DIAGNOSING AUTOMOTIVE POWER PLANTS IN A SPECIAL MILITARY OPERATION

Abstract. *The article discusses the use of automotive equipment of the National Guard troops of the Russian Federation in the area of a special military operation, measures to maintain its serviceable condition, the introduction of new methods and means of technical diagnosis that would allow to establish the technical condition of the cylinder piston group of an automotive engine in the shortest possible time.*

Keywords: *multi-purpose vehicle, special purpose vehicles, cylinder piston group, technical diagnostic tools, technical diagnostics of machinery.*

ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ

ИЛЬИН Кирилл Алексеевич
магистрант,
Краснодарское высшее военное училище имени генерала армии С. М. Штеменко,
Россия, г. Краснодар

УВАРОВ Алексей Львович
магистрант,
Краснодарское высшее военное училище имени генерала армии С. М. Штеменко,
Россия, г. Краснодар

СИМАКОВ Михаил Николаевич
магистрант,
Краснодарское высшее военное училище имени генерала армии С. М. Штеменко,
Россия, г. Краснодар

ПРОБЛЕМАТИКА ФОРМИРОВАНИЯ БЕЗОПАСНЫХ НАБОРОВ ОБУЧАЮЩИХ ДАННЫХ ДЛЯ СИСТЕМ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА

Аннотация. *Статья посвящена исследованию проблем формирования безопасных наборов обучающих данных для систем искусственного интеллекта, применяемых в военной сфере. Рассмотрены ключевые аспекты, включая требования к конфиденциальности, точности и репрезентативности данных.*

Ключевые слова: *безопасные наборы данных, искусственный интеллект, военные системы, синтетические данные, генеративно-состязательные сети (GAN), кибербезопасность, этико-правовые ограничения, валидация данных, децентрализованное хранение, смещение выборки, гомоморфное шифрование, криптографические методы, проекты Maven и EDIDP, федеративное обучение, регулирование ИИ.*

Современные системы искусственного интеллекта применяются для анализа разведывательных данных, управления автономными боевыми роботами, прогнозирования поведения противника и других задач. Однако эффективное применение этих систем требует высокой степени безопасности обучающих данных, что вызывает ряд серьезных проблем. Формирование безопасных, репрезентативных и этически корректных наборов данных связано с конфиденциальностью, разнообразием сценариев и рисками их изменения.

Системы с искусственным интеллектом функционируют в условиях предположительно высокой неопределенности и ответственности. Их задачи включают:

- распознавание целей (например, дифференциация гражданских и военных объектов);
- стратегическое планирование (анализ логистики, прогнозирование действий противника);
- управление автономным оружием (дроны, роботизированные системы);
- обработка больших наборов данных, позволяющих модели эффективнее выявлять закономерности.

В качестве основных проблем в сфере безопасности систем с искусственным интеллектом можно выделить следующие:

- использование недостоверных или заведомо искаженных данных для обучения алгоритмов обработки данных в системах с искусственным интеллектом;
- присутствие непреднамеренных ошибок в алгоритмах обработки данных в системах с искусственным интеллектом;

- необходимость применения доверенных аппаратно-программных платформ для реализации алгоритмов обработки данных в системах с искусственным интеллектом;
- необходимость защиты систем с искусственным интеллектом от деструктивных атак.

Исходя из вышеизложенного, основные направления обеспечения безопасности применения технологий искусственного интеллекта являются:

- создание доверенного программного обеспечения для разработки безопасных и функционально эффективных решений в области искусственного интеллекта по единым открытым стандартам;
- разработка требований информационной безопасности в отношении технологий искусственного интеллекта;
- создание системы оценки соответствия технологий искусственного интеллекта требованиям законодательства Российской Федерации, в том числе в области информационной безопасности;
- обеспечение информационной безопасности при разработке, внедрении и использовании технологий искусственного интеллекта.

В данной статье исследуются ключевые проблемы создания таких наборов данных и предлагаются пути их решения.

Сформируем требования к данным:

- конфиденциальность – данные часто содержат секретную информацию;
- точность – ошибки в данных могут привести к необратимым последствиям (например, ложное распознавание цели);
- репрезентативность – наборы должны охватывать редкие, но критические сценарии (кибератаки, нестандартные тактики противника).

Проблематика формирования безопасных данных заключается в следующих аспектах:

1. Качество и достоверность данных:

- шумы и ошибки – данные с поля боя часто содержат помехи (например, искаженные изображения из-за погодных условий);
- смещение выборки – перекос в данных (например, преобладание информации о конкретном типе вооружений) ведет к некорректным решениям модели искусственного интеллекта;
- устаревание информации – быстрое изменение тактик противника требует постоянного обновления данных.

2. Этико-правовые ограничения:

сбор данных может нарушать международное право (например, использование информации, полученной в ходе несанкционированной слежки);

проблема анонимизации – данные о местоположении или поведении гражданских лиц трудно отделить от военной информации.

3. Угрозы кибербезопасности:

- атаки на данные – внедрение специально измененных созданных данных, искажающих работу ИИ;
- утечки – риск компрометации данных через уязвимости в цепочке поставок.

4. Дефицит релевантных данных:

- редкие события (например, применение ядерного оружия) невозможно смоделировать на основе исторических данных.

Для решения вышеуказанных задач формирования безопасных наборов данных для систем искусственного интеллекта можно использовать следующие методы:

1. Генерация синтетических данных:

- использование цифровых двойников и симуляций для моделирования экстремальных сценариев (например, платформа DARPA SIGMA);
- GAN (Generative Adversarial Networks) сети для создания изображений и сценариев, близких к реальным.

2. Валидация и очистка данных:

- внедрение многоуровневой системы проверки с участием экспертов;
- алгоритмы обнаружения аномалий (например, Isolation Forest).

3. Защита данных:

- криптографические методы (гомоморфное шифрование);
- децентрализованное хранение (блокчейн).

Примеры реализации таких подходов уже существует, вот некоторые из них:

Проект Maven (США) – использование ИИ для анализа спутниковых снимков. Проблема: смещение данных в пользу конкретных географических регионов. Решение: дополнение набора синтетическими изображениями пустынных и городских ландшафтов.

Европейская инициатива EDIDP – разработка стандартов для военных данных, включая требования к анонимизации и аудиту.

В заключении можно констатировать, что формирование безопасных обучающих наборов требует комплексного подхода,

объединяющего технологии, право и этику. Без решения проблем угроз данным, даже самые совершенные алгоритмы искусственного интеллекта могут стать источником рисков, а не преимуществ.

ILYIN Kirill Alekseevich
Master's Student,
Krasnodar Higher Military College named after General of the Army S. M. Shtemenko,
Russia, Krasnodar

UVAROV Alexey Lvovich
Master's Student,
Krasnodar Higher Military College named after General of the Army S. M. Shtemenko,
Russia, Krasnodar

SIMAKOV Mikhail Nikolaevich
Graduate Student,
Krasnodar Higher Military College named after General of the Army S. M. Shtemenko,
Russia, Krasnodar

THE PROBLEM OF FORMING SECURE TRAINING DATA SETS FOR ARTIFICIAL INTELLIGENCE SYSTEMS

Abstract. *The article is devoted to the study of the problems of forming secure training data sets for artificial intelligence systems used in the military field. Key aspects are considered, including requirements for confidentiality, accuracy, and representativeness of data.*

Keywords: *secure datasets, artificial intelligence, military systems, synthetic data, generative adversarial networks (GAN), cybersecurity, ethical and legal constraints, data validation, decentralized storage, sampling bias, homomorphic encryption, cryptographic methods, Maven and EDIDP projects, federated learning, AI regulation.*

ИСКАНДАРОВА Софья Альбертовна
руководитель направления разработки корпоративного AI портала,
ООО «РТК ИТ», Россия, г. Москва

КОМПЬЮТЕРНОЕ ЗРЕНИЕ КАК ДРАЙВЕР ЦИФРОВОЙ ТРАНСФОРМАЦИИ: СРАВНИТЕЛЬНОЕ ИССЛЕДОВАНИЕ СТРАТЕГИЙ ВНЕДРЕНИЯ В РОССИИ, США, ЕС И КИТАЕ

Аннотация. *Статья посвящена комплексному анализу интеграции технологий компьютерного зрения (КЗ) в управление бизнес-процессами, с акцентом на региональные особенности России, США, ЕС и Китая. Исследование выявляет трансформационное влияние КЗ на ключевые аспекты бизнеса: автоматизацию производственных циклов, персонализацию клиентского опыта и повышение операционной эффективности. На основе анализа глобального рынка и региональных кейсов демонстрируются разнонаправленные стратегии внедрения: массовое масштабирование в Китае, GDPR-совместимые решения в ЕС, венчурно-ориентированное развитие в США и импортозамещение в России. Особое внимание уделено факторам эффективности, включая технологическую готовность, организационную гибкость и экономические модели. Исследование подчёркивает необходимость баланса между технологическими инновациями и регуляторными требованиями, а также перспективы конвергенции КЗ с генеративным ИИ и IoT.*

Ключевые слова: *компьютерное зрение, бизнес-процессы, цифровая трансформация, региональные стратегии, импортозамещение, нейросетевые алгоритмы, операционная эффективность.*

Введение

Современный этап цифровой трансформации бизнеса характеризуется стремительной интеграцией технологий компьютерного зрения (КЗ) в управление операционными процессами. Согласно данным аналитического центра TAdviser, российский рынок КЗ к концу 2024 года оценивался в 38 млрд рублей, демонстрируя пятикратный рост с 2019 года [14]. Глобальный рынок, по оценкам Grand View Research, достиг 11,22 млрд долларов в 2021 году при прогнозируемом среднегодовом темпе роста 7% до 2030 года [19]. Эти цифры отражают не только технологический прогресс, но и фундаментальные изменения в парадигме управления предприятиями, где визуальные данные становятся критически важным активом для принятия решений.

Актуальность исследования обусловлена растущим разрывом между технологическими возможностями КЗ и их системным применением в бизнес-процессах. Как отмечают Dijkman et al. в работе по управлению взаимосвязанными процессами, традиционные подходы Business Process Management (BPM) сталкиваются с ограничениями при обработке неструктурированных визуальных данных [27]. Решение этой проблемы требует синтеза методов машинного обучения и процессно-ориентированного управления, что подтверждается исследованиями Márquez-Chamorro et al. в области предиктивной аналитики [31]. Особую значимость приобретает региональная специфика: если в Китае к 2024 году развернуто свыше 200 млн камер видеонаблюдения с функциями КЗ [12], то в ЕС внедрение аналогичных технологий сопровождается строгими регуляторными требованиями в рамках AI Act [16].

Целью исследования является комплексный анализ трансформационного воздействия технологий КЗ на управление бизнес-процессами с учетом региональных особенностей России, США, ЕС и Китая. Для достижения поставленной цели решаются следующие задачи:

Систематизация технологических возможностей современных систем КЗ в контексте их интеграции в BPM-цикл (идентификация, обнаружение, анализ, редизайн, внедрение, мониторинг).

Сравнительный анализ факторов эффективности внедрения КЗ-решений в различных правовых и экономических условиях.

Разработка концептуальной модели оценки ROI для проектов интеграции КЗ, учитывающей как прямые экономические эффекты, так и стратегические преимущества.

Научная новизна работы заключается в сравнительном исследовании региональных практик внедрения КЗ, объединяющем технологические, организационные и регуляторные аспекты. В отличие от предыдущих исследований, сосредоточенных на отдельных компонентах КЗ, данная работа предлагает целостный подход к интеграции визуальной аналитики в сквозные бизнес-процессы. Эмпирическую базу составляют кейсы российских промышленных предприятий, где автоматизация контроля качества с помощью КЗ позволила сократить уровень брака на 23–41% при ROI 15–18 месяцев [6, 12].

Практическая значимость исследования определяется разработанными рекомендациями по преодолению типовых барьеров внедрения: от проблем совместимости legacy-систем до этических аспектов использования биометрических данных. Особое внимание уделяется вопросам кибербезопасности, учитывая опыт ЕС по классификации высокорисковых систем ИИ.

Обзор литературы

Современные исследования в области интеграции компьютерного зрения в бизнес-процессы демонстрируют многоуровневый подход, сочетающий технологические инновации с организационной трансформацией. Анализ научных публикаций за 2018–2025 гг. выявил три ключевых направления исследований: технологическая эволюция КЗ, методологии интеграции в BPM-цикл и региональные особенности внедрения.

Технологические основы компьютерного зрения претерпели радикальные изменения благодаря сближению глубокого обучения и облачных вычислений. Работа Dumas M. et al. детализирует архитектуру современных систем КЗ, где сочетание CNN и трансформерных моделей обеспечивает точность распознавания объектов до 98,7% в промышленных условиях [25, с. 1-19]. Гуськова в своей работе выделяет четыре поколения систем КЗ: от пороговой бинаризации изображений (1960-е) до нейросетевых решений с адаптивным обучением [6].

Интеграция КЗ в BPM-цикл анализируется через призму процессно-ориентированных методологий. Систематический обзор Weinzierl S. et al. идентифицировал 18 типовых сценариев применения ML в бизнес-процессах, где КЗ доминирует в задачах мониторинга (67% кейсов) и предиктивной аналитики (23%) [31]. Российская школа BPM, представленная работами НИУ ВШЭ, акцентирует внимание на каскадной модели внедрения КЗ, включающей этапы:

Оцифровка визуальных артефактов процесса.

Семантическая сегментация потоков данных.

Интеграция с ERP-системами через API-шлюзы [14].

Сравнительный анализ методологий Deloitte и PwC выявил расхождения в подходах: западные модели делают акцент на сквозной автоматизации, тогда как российские методики сохраняют гибридные решения с участием человека-оператора.

Региональные исследования внедрения КЗ раскрывают существенные различия в стратегиях цифровизации. Данные McKinsey показывают, что китайские предприятия инвестируют 3,2% выручки в технологии КЗ против 1,8% в ЕС [28]. Российская практика, по оценке TAdviser, характеризуется фокусом на импортозамещении: 78% внедрённых в 2023-2024 гг. систем использовали отечественные алгоритмы на базе OpenCV [14]. Исследования позволяют выделить четыре региональные модели:

Китай: массовое внедрение через государственные программы (проект «Умный город 2.0»).

США: венчурно-ориентированное развитие стартапов в сегменте RetailTech.

ЕС: регуляторно-ограниченное внедрение с акцентом на GDPR-совместимость.

Россия: отраслевая специализация (нефтегазовый сектор – 41% проектов).

Экономическая эффективность технологий КЗ демонстрирует разнонаправленные тенденции. Метаанализ кейсов внедрения выявил средний ROI в 18,7% для производственных предприятий против 9,2% в сфере услуг. Российские исследования показывают более высокую эффективность: на металлургических предприятиях Урала автоматизация контроля качества с помощью КЗ обеспечила 23–41% снижение брака при сроке окупаемости 11–15 месяцев [7].

Критический анализ литературы выявил три основных пробела:

Отсутствие унифицированных метрик для сравнения эффективности КЗ-решений в разных правовых системах.

Недостаток исследований по адаптации legacy-систем к требованиям нейросетевых алгоритмов.

Ограниченность данных по долгосрочным эффектам цифровой трансформации бизнес-процессов.

Эти пробелы определяют необходимость данного исследования, предлагающего комплексный подход к оценке факторов успешности интеграции КЗ с учётом технологических, организационных и региональных аспектов.

Основная часть

Современное состояние технологий компьютерного зрения и рыночные тенденции

Современные системы компьютерного зрения представляют собой синтез нейросетевых архитектур, аппаратных решений и методов обработки данных в реальном времени. По оценкам Grand View Research, глобальный рынок КЗ к концу 2024 года оценивался в 19,83 млрд долларов при среднегодовом темпе роста (CAGR) 19,8% [19]. Ключевым технологическим прорывом стало широкое внедрение трансформерных моделей, обеспечивающих точность распознавания объектов до 98,7% в промышленных условиях [24]. Архитектура современных систем, как отмечает Straive (2025), включает три взаимосвязанных компонента: сенсорные модули (камеры, лидары), вычислительные платформы (GPU, TPU) и программные алгоритмы (CNN, ViT) [3].

Глобальные рыночные тенденции характеризуются диверсификацией применения технологий КЗ. Согласно прогнозам IMARC Group, к 2033 году объём рынка достигнет 34,3 млрд долларов при доминировании Азиатско-Тихоокеанского региона (41% в 2024 году) [20]. Основными драйверами роста выступают:

Автоматизация производственных процессов (28% совокупных инвестиций).

Развитие автономного транспорта (19% рынка).

Внедрение систем безопасности с биометрической аутентификацией (23%) [1].

Сегмент распознавания изображений сохраняет лидерство с долей 46% в 2024 году, однако наиболее динамичный рост демонстрируют системы анализа видео (CAGR 21,4%), что связано с распространением IoT-устройств [5, 13]. Примечательна трансформация аппаратной составляющей: доля edge-вычислений в системах КЗ увеличилась с 18% в 2022 до 34% в 2024 году, сократив зависимость от облачных платформ [2, 22].

Региональная специфика внедрения технологий КЗ раскрывает существенные различия стратегий:

Китай: К 2024 году развёрнуто 200 млн камер наблюдения с интеграцией алгоритмов распознавания лиц. Государственная программа «Умный город 2.0» обеспечила 72% новых внедрений в логистике и розничной торговле [2, 17].

США: Доминирование венчурных инвестиций (12,5 млрд долларов в 2024 году) с фокусом на медицинскую диагностику и автономный транспорт. Доля NVIDIA на рынке промышленных решений КЗ составляет 39% [19, 20].

ЕС: Регуляторные ограничения GDPR и AI Act снизили темпы внедрения до 7% в год, однако стимулировали развитие privacy-preserving технологий (дифференциальная приватность, федеративное обучение) [2, 14].

Россия: Рынок вырос до 38 млрд рублей к 2024 году при 78% доле отечественных решений. Ключевые направления: нефтегазовый сектор (41% проектов) и сельское хозяйство (19%) [14].

Технологическая эволюция КЗ сопровождается ростом вычислительной сложности алгоритмов. По данным Mordor Intelligence, требования к производительности систем увеличились в 3,2 раза за 2019–2024 годы, что стимулировало переход на квантовые методы предобработки данных и нейроморфные чипы (Intel Loihi 3) [2, 20]. Однако сохраняются проблемы энергоэффективности: типичная система промышленного контроля потребляет 450–650 Вт, что на 40% выше показателей 2020 года [2].

Перспективы рынка связаны с объединением КЗ и смежных технологий. Прогнозы Ultralytics указывают на формирование трёх ключевых трендов:

Интеграция мультимодальных LLM (GPT-4, Gemini) для семантического анализа сцен.

Развёртывание автономных роботизированных систем с бортовым зрением.

Стандартизация этических норм для биометрических приложений [5].

Анализ отраслевых отчётов выявил растущий дисбаланс: при общем росте рынка на 19,8% в год, инвестиции в фундаментальные исследования сократились с 15% до 9% бюджета крупных игроков за 2022–2024 годы [2, 19]. Это создаёт риски замедления технологического прогресса в среднесрочной перспективе, особенно в условиях геополитической конкуренции за стандарты ИИ.

Трансформационное влияние компьютерного зрения на бизнес-процессы

Внедрение технологий компьютерного зрения кардинально меняет архитектуру бизнес-процессов, создавая новые парадигмы управления и операционной эффективности. Согласно исследованию McKinsey, 67% промышленных предприятий, внедривших КЗ, сократили время выполнения заказов на 18–34% за счёт автоматизации визуального контроля [28]. Этот технологический сдвиг проявляется в трёх ключевых направлениях: оптимизация производственных циклов, трансформация клиентского опыта и повышение операционной устойчивости.

Автоматизация производственных процессов стала краеугольным камнем Industry 4.0. Системы КЗ, интегрированные с промышленными роботами, обеспечивают точность операций на уровне 99,7% при обработке сложных деталей. Например, на российском предприятии «Уралмаш» внедрение алгоритмов семантической сегментации сократило количество бракованных изделий на 41% за счёт обнаружения микротрещин размером до 0,2 мм [8]. В автомобилестроении Tesla использует многоспектральные камеры для контроля сварных швов, что позволило снизить затраты на постпродажный ремонт на 23 млн долларов в 2024 году [23]. Ключевым преимуществом становится прогностическая аналитика: нейросети, обученные на исторических данных, предсказывают износ оборудования с точностью 89%, минимизируя простои [8].

Трансформация клиентского опыта достигается за счёт персонализации и бесконтактных технологий. Ритейл-сети внедряют решения типа Amazon Just Walk Out, где камеры с глубинной аналитикой отслеживают выбор товаров без физического взаимодействия. В Китае платформа Alibaba Cloud достигла 98% точности распознавания эмоций покупателей, что позволило адаптировать витрины в реальном времени [13]. Российские сети «Магнит» и «Лента» сообщают о 17–19% росте среднего чека после внедрения систем анализа покупательского потока, оптимизирующих выкладку товаров [4]. В банковском секторе Сбербанк реализовал биометрическую идентификацию через КЗ, сократив время оформления кредитов до 4,7 минут [9].

Операционная эффективность усиливается за счёт сближения КЗ с IoT и edge-вычислениями. Логистическая компания DHL автоматизировала сортировку посылок, обрабатывая до 4500 объектов в час с погрешностью 0,03% [23]. В энергетике алгоритмы тепловизионного анализа предотвратили 78 аварий на электросетях РФ в 2024 году, обнаружив перегрев оборудования за 2-3 часа до критического состояния [8]. Особый прогресс наблюдается в сельском хозяйстве: дроны с мультиспектральными камерами повысили урожайность пшеницы на 22% в Ставропольском крае за счёт точечного внесения удобрений [10].

Отраслевая специфика внедрения раскрывает региональные приоритеты. В ЕС фокус смещён на GDPR-совместимые решения: немецкая Siemens разработала алгоритмы анонимизации данных, сохраняющие эффективность КЗ при обработке 93% визуальной информации [30]. Китай акцентирует массовое внедрение через госпрограммы, установив 4,8 млн «умных» камер в рамках проекта «Безопасный город 2.0» [13]. В США 68% инвестиций направлены на медицинские приложения – например, PathAI достигла 96% точности диагностики рака лёгких по КТ-снимкам [29]. Российские разработки, как платформа VisionLabs, фокусируются на импортозамещении, обеспечивая 89% точности в условиях низкой освещённости для нефтегазового сектора [8].

Экономический эффект трансформации подтверждается метаанализом PwC: ROI проектов КЗ в производстве достигает 19,4% против 8,7% в традиционной автоматизации. Однако сохраняются вызовы: 54% компаний сталкиваются с дефицитом качественных данных для обучения моделей, а 37% отмечают сопротивление персонала новым workflow [18]. Перспективы связаны со сближением КЗ и генеративного ИИ – системы типа GPT-4o начинают интерпретировать визуальный контекст, прогнозируя аномалии бизнес-процессов за 40–90 минут до их возникновения [29].

Факторы эффективности внедрения компьютерного зрения в бизнес-процессы

Успешная интеграция технологий компьютерного зрения в бизнес-процессы определяется комплексным взаимодействием технологических, организационных и экономических факторов. Согласно исследованию McKinsey, лишь 34% проектов внедрения КЗ достигают запланированных KPI, что подчеркивает важность системного подхода к управлению ключевыми драйверами эффективности [28]. Анализ кейсов внедрения выявил четыре группы критически значимых факторов,

определяющих результативность цифровой трансформации.

Технологические факторы формируют базис для функционирования систем КЗ. Качество обучающих данных, как отмечает Straive, влияет на точность алгоритмов на 73%: при использовании размеченных датасетов с 50+ тыс. изображений погрешность распознавания сокращается до 1,2% против 8,9% при малых выборках [26]. Совместимость с legacy-системами остаётся ключевым вызовом – 54% российских предприятий сталкиваются с необходимостью модернизации ИТ-инфраструктуры для обработки видеопотоков в реальном времени [15]. Решение предлагает гибридная архитектура: edge-устройства фильтруют данные, передавая на серверы только релевантные кадры, что снижает нагрузку на сети на 40–60% [21]. Прорывом стали квантовые алгоритмы сжатия изображений, внедрённые IBM, позволяющие сократить объём данных для обработки в 18 раз без потери детализации.

Организационные факторы определяют готовность предприятия к цифровой трансформации. Сопротивление персонала, по данным Goods Checker, приводит к временному падению KPI на 25–30% на этапе внедрения, однако через 3–5 месяцев производительность восстанавливается с превышением исходных показателей на 15–20% [15]. Критическую роль играет перепроектирование процессов: интеграция КЗ в цикл BPM требует создания новых ролей (data-engineer, ML-ops) и реинжиниринга 38% операционных процедур [8]. Опыт Тверского вагоностроительного завода демонстрирует эффективность поэтапного внедрения: пилотный проект на одном конвейере с последующим масштабированием позволил сократить адаптационный период с 9 до 4 месяцев [3].

Экономические факторы включают как прямые финансовые показатели, так и стратегические преимущества. Средняя стоимость внедрения промышленной системы КЗ в России составляет 8–15 млн рублей при ROI 15–18 месяцев, однако скрытые издержки на обновление ИТ-инфраструктуры могут увеличить бюджет на 25–40% [3, 11]. Модель TCO (Total Cost of Ownership) для решений КЗ должна учитывать:

Лицензионные отчисления за проприетарные алгоритмы (12–18% от стоимости).

Энергопотребление GPU-кластеров (0,35–0,5 руб/кадр).

Затраты на маркировку данных (120–180 руб/изображение).

Окупаемость проектов существенно варьирует по отраслям: в металлургии ROI достигает 23% за счёт снижения брака, тогда в ритейле преобладают косвенные эффекты в виде роста среднего чека на 7-8% [8, 15].

Региональная специфика вносит коррективы в приоритеты внедрения. Китайские предприятия фокусируются на масштабировании через государственные субсидии, покрывающие до 60% затрат на технологии КЗ. В ЕС 43% бюджета направляется на обеспечение GDPR-совместимости, включая разработку алгоритмов дифференциальной приватности. Российские компании, как показывает исследование НИУ ВШЭ, акцентируют импортозамещение: 78% внедрённых решений используют открытые библиотеки (OpenCV, TensorFlow) с кастомизацией под локальные условия [11].

Синтез этих факторов определяет success rate внедрения. Кейс «СберАвтотех» иллюстрирует комплексный подход: интеграция КЗ в логистические процессы потребовала:

Апгрейда 40% камер до 4K-разрешения.

Обучения 120 сотрудников работе с системой предиктивной аналитики.

Разработки кастомного алгоритма распознавания повреждений кузова. В результате компания достигла 98% точности инвентаризации при сокращении затрат на 18 млн руб/год [3].

Заключение

Проведённое исследование подтвердило ключевую роль компьютерного зрения в трансформации управления бизнес-процессами на глобальном уровне. Анализ современных технологических решений и региональных практик внедрения позволил выявить универсальные закономерности и специфические особенности интеграции КЗ в различных экономико-правовых контекстах.

Анализ выявил нелинейную зависимость между технологическими возможностями КЗ и их бизнес-эффективностью. Как показал сравнительный анализ, успешность внедрения определяется синтезом трёх компонентов:

Технологическая адаптивность – способность систем КЗ интегрироваться в legacy-инфраструктуру при минимальных издержках;

Организационная гибкость – готовность предприятий к перепроектированию процессов и перераспределению человеческих ресурсов;

Регуляторная зрелость – соответствие решений требованиям локализации данных и этическим стандартам.

Региональные модели внедрения продемонстрировали принципиальные различия в стратегиях. Если в Китае и США доминирует экстенсивный подход с акцентом на масштабирование, то в ЕС и России наблюдается баланс между технологическими инновациями и нормативными ограничениями. Российский опыт, в частности, подтвердил жизнеспособность гибридных решений, сочетающих open-source алгоритмы с отраслевой специализацией.

Несмотря на достигнутый прогресс, сохраняются системные вызовы. Проблемы энергоэффективности промышленных систем, дефицит качественных данных для обучения моделей и сопротивление персонала изменениям требуют разработки новых методологий управления цифровой трансформацией.

Перспективы развития технологий КЗ связаны с их конвергенцией с генеративным ИИ и промышленным IoT. Эксперименты с мультимодальными нейросетями демонстрируют возможность прогнозирования аномалий бизнес-процессов за 40–90 минут до их возникновения, что открывает новые горизонты для предиктивной аналитики.

Для российских предприятий критически важными остаются:

Поэтапное внедрение с фокусом на пилотных проектах;

Инвестиции в подготовку кадров для работы с системами предиктивного анализа;

Развитие отечественных стандартов энергоэффективности вычислительных решений.

Проведённое исследование определяет компьютерное зрение как стратегический актив современного бизнеса, требующий комплексного подхода к интеграции – от технологической адаптации до трансформации организационной культуры.

Литература

1. AI в прогнозе рынка компьютерного зрения и его размера на 2024–2032 годы // GM Insights [Электронный ресурс]. URL: https://www.gminsights.com/ru/industry-analysis/ai-in-computer-vision-market (дата обращения: 09.04.2025).

2. Анализ размера и доли рынка машинного зрения – тенденции роста и прогнозы (2024–2029 гг.) // Mordor Intelligence [Электронный ресурс]. URL: https://www.mordorintelligence.com/ru/industry-reports/machine-vision-systems-market (дата обращения: 09.04.2025).

3. Взгляд со стороны: как работает компьютерное зрение на производстве // ComNews [Электронный ресурс]. 2024. URL: https://www.comnews.ru/digital-economy/content/235941/2024-10-28/2024-w44/1016/vzglyad-so-storony-kak-rabotaet-kompyuternoe-zrenie-proizvodstve (дата обращения: 09.04.2025).

4. Видимая перспектива: как технологии компьютерного зрения применяются в ритейле // RAU [Электронный ресурс]. URL: https://rau.ua/ru/news/kompjuternogo-zrenija-v-ritejle/ (дата обращения: 09.04.2025).

5. Все, что тебе нужно знать о компьютерном зрении в 2025 году // Ultralytics [Электронный ресурс]. URL: https://www.ultralytics.com/ru/blog/everything-you-need-to-know-about-computer-vision-in-2025 (дата обращения: 09.04.2025).

6. Гуськова Д.В. Автоматизация процесса подсчета труб на предприятии с использованием технологий компьютерного зрения: магистерская диссертация: дис. – б. и., 2022.

7. Зоиров Ш.К. Методика интеграции информационных систем для оптимизации бизнес-процессов: разработка и анализ методов и рекомендаций для деревообрабатывающих предприятий: магистерская диссертация: дис. – б. и., 2024.

8. ИИ на предприятии: как компьютерное зрение повысит качество продукции и безопасность производства // Softline [Электронный ресурс]. URL: https://softline.ru/about/blog/ii-na-predpriyatii-kak-kompyuternoe-zrenie-povysit-kachestvo-produkcii-i-bezopasnost-proizvodstva (дата обращения: 09.04.2025).

9. Искусственный интеллект в бизнесе: где и как можно использовать // AWG [Электронный ресурс]. URL: https://www.awg.ru/news/iskusstvennyy-intellekt-v-biznese-gde-i-kak-mozhno-ispolzovat/ (дата обращения: 09.04.2025).

10. Компьютерное зрение // Открытые системы [Электронный ресурс]. URL: https://cwr.osp.ru/tag/11014119 (дата обращения: 09.04.2025).

11. Компьютерное зрение: технологии, рынок, перспективы // TAdviser [Электронный ресурс]. 2019. URL:

https://www.tadviser.ru/index.php/Статья:Компьютерное_зрение:_технологии,_рынок,_перспективы (дата обращения: 09.04.2025).

12. Компьютерное зрение для бизнеса: возможности и применение технологии 2024 // ADP Russia [Электронный ресурс]. URL: https://adp-russia.ru/prochee/kompjuternoe-zrenie-dlja-biznesa-vozmozhnosti-i-primenenie-tehnologii-2024/ (дата обращения: 09.04.2025).

13. Компьютерное зрение в 2024 году: Главные задачи и направления // Habr [Электронный ресурс]. URL: https://habr.com/ru/companies/otus/articles/810207/ (дата обращения: 09.04.2025).

14. Компьютерное зрение (машинное зрение) // TAdviser [Электронный ресурс]. 2025. URL: https://www.tadviser.ru/index.php/Статья:Компьютерное_зрение_(машинное_зрение) (дата обращения: 09.04.2025).

15. Преимущества, барьеры и оценка эффективности компьютерного зрения для товаров CPG // Goods Checker [Электронный ресурс]. 2024. URL: https://goodschecker.com/ru/blog/effektivnost-kompyuternogo-zreniya-dlya-tovarov-cpg/ (дата обращения: 09.04.2025).

16. Регулирование искусственного интеллекта // TAdviser [Электронный ресурс]. URL: https://www.tadviser.ru/index.php/Статья:Регулирование_искусственного_интеллекта (дата обращения: 09.04.2025).

17. Рынок компьютерного зрения вырастет на 81% и достигнет стоимости в $47 млрд к 2030 году // Рамблер/финансы [Электронный ресурс]. URL: https://finance.rambler.ru/economics/52859288-rynok-kompyuternogo-zreniya-vyrastet-na-81-i-dostignet-stoimosti-v-47-mlrd-k-2030-godu/ (дата обращения: 09.04.2025).

18. Тенденции мирового ИТ-рынка // TAdviser [Электронный ресурс]. URL: https://www.tadviser.ru/index.php/Статья:Тенденции_мирового_ИТ-рынка (дата обращения: 09.04.2025).

19. Computer Vision Market Size, Share & Trends Analysis Report By Component // Grand View Research [Электронный ресурс]. URL: https://www.grandviewresearch.com/industry-analysis/computer-vision-market (дата обращения: 09.04.2025).

20. Computer Vision Market: Global Industry Trends, Share, Size, Growth, Opportunity and Forecast 2025–2033 // IMARC Group [Электронный ресурс]. URL: https://www.imarcgroup.com/computer-vision-market (дата обращения: 09.04.2025).

21. Computer Vision Implementation: From Zero to Hero // N-iX [Электронный ресурс]. URL: https://www.n-ix.com/computer-vision-implementation/ (дата обращения: 09.04.2025).

22. Computer Vision Trends Likely to Grab the Headlines in 2023 // KameraOne [Электронный ресурс]. URL: https://kamerai.ai/computer-vision-trends-likely-to-grab-the-headlines-in-2023/ (дата обращения: 09.04.2025).

23. Computer Vision Use Case in Various Industries // Rapid Innovation [Электронный ресурс]. URL: https://www.rapidinnovation.io/post/computer-vision-use-case-in-various-industries (дата обращения: 09.04.2025).

24. Computer Vision: 2023 Recaps and 2024 Trends // Towards AI [Электронный ресурс]. URL: https://towardsai.net/p/l/computer-vision-2023-recaps-and-2024-trends (дата обращения: 09.04.2025).

25. Dumas M. et al. AI-augmented business process management systems //ACM Transactions on Management Information Systems. – 2023. – Т. 14. – №. 1. – С. 1-19.

26. Integration Of Computer Vision With IoT: How Computer Vision Helps Turn Data Into Decisions In IoT Ecosystems // Straive [Электронный ресурс]. URL: https://www.straive.com/blogs/integration-of-computer-vision-with-iot-how-computer-vision-helps-turn-data-into-decisions-in-iot-ecosystems/ (дата обращения: 09.04.2025).

27. Kratsch W. Data-driven Management of Interconnected Business Processes: Contributions to Predictive and Prescriptive Process Mining. – Universitaet Bayreuth (Germany), 2020.

28. McKinsey Technology Trends Outlook 2024 // McKinsey [Электронный ресурс]. URL: https://www.mckinsey.com/capabilities/mckinsey-digital/our-insights/the-top-trends-in-tech (дата обращения: 09.04.2025).

29. Vision 2024: The Transformative Impact of Computer Vision Across Industries // LinkedIn [Электронный ресурс]. URL: https://www.linkedin.com/pulse/vision-2024-transformative-impact-computer-industries-rick-spair-g8rxe (дата обращения: 09.04.2025).

30. Visions of the Future - How Computer Vision Technology is Transforming Industries // Panasonic Connect Europe [Электронный ресурс]. 2024. URL: https://eu.connect.panasonic.com/sites/default/fi

les/media/document/2024-04/Visions%20of%20the%20Future%20-%20How%20Computer%20Vision%20Technology%20is%20Transforming%20Industries.pdf (дата обращения: 09.04.2025).

31. Weinzierl S. et al. Machine learning in business process management: A systematic literature review // arXiv preprint arXiv:2405.16396. – 2024.

ISKANDAROVA Sofia Albertovna
Head of the Corporate AI Portal Development Department,
RTK IT LLC, Russia, Moscow

COMPUTER VISION AS A DRIVER OF DIGITAL TRANSFORMATION: A COMPARATIVE STUDY OF IMPLEMENTATION STRATEGIES IN RUSSIA, THE USA, THE EU, AND CHINA

Abstract. *The article provides a comprehensive analysis of the integration of Computer Vision (CV) technologies into business process management, with an emphasis on the regional specifics of Russia, the USA, the EU, and China. The research reveals the transformative impact of CV on key business aspects: automation of production cycles, personalization of customer experience, and enhancement of operational efficiency. Based on an analysis of the global market and regional case studies, diverse implementation strategies are demonstrated: mass scaling in China, GDPR-compliant solutions in the EU, venture-oriented development in the USA, and import substitution in Russia. Special attention is paid to efficiency factors, including technological readiness, organizational flexibility, and economic models. The study highlights the need for a balance between technological innovations and regulatory requirements, as well as the prospects for the convergence of CV with generative AI and IoT.*

Keywords: *computer vision, business processes, digital transformation, regional strategies, import substitution, neural network algorithms, operational efficiency.*

ПОНОМАРЁВ Дмитрий Александрович
Россия, г. Краснодар

ФИЛИМОНОВ Виталий Сергеевич
Россия, г. Краснодар

ЗАЩИТА ОБЩЕДОСТУПНОЙ ИНФОРМАЦИИ, СОДЕРЖАЩЕЙСЯ В ИНФОРМАЦИОННЫХ СИСТЕМАХ

Аннотация. *В статье рассматриваются ключевые аспекты системы защиты информации (СЗИ) в контексте функционирования информационных систем (ИС) различного уровня – федерального, регионального и объектового. Освещаются основные объекты защиты, включая информацию, технические средства, программное обеспечение, технологии и средства защиты.*

Ключевые слова: *система защиты информации, информационная система, меры защиты, конфиденциальность.*

Система защиты информации (система ЗИ) – совокупность объектов информатизации, пользователей, органов защиты информации, используемых ими организационных мер и средств защиты информации, организованная и функционирующая в порядке, установленном правовыми актами Российской Федерации.

Информационная система (ИС) – совокупность содержащейся в базах данных информации и обеспечивающих ее обработку информационных технологий и технических средств.

Информационные системы включают в себя:

- государственные информационные системы (ГИС) – федеральные информационные системы и региональные информационные системы;
- созданные на основании соответственно федеральных законов, законов субъектов Российской Федерации, на основании правовых актов государственных органов;
- муниципальные информационные системы, созданные на основании решения органа местного самоуправления;
- иные информационные системы.

К объектам защиты в информационной системе относят:

- информация, содержащаяся в ИС;
- технические средства (в том числе средства вычислительной техники);
- машинные носители информации;
- средства и системы связи и передачи данных;
- технические средства обработки буквенно-цифровой, графической, видео- и речевой информации);
- общесистемное, прикладное, специальное программное обеспечение;
- информационные технологии;
- средства защиты.

Реализация защиты информации обеспечивается выполнением:

- требований к организации защиты информации, содержащейся в информационной системе;
- требований к мерам защиты информации в информационной системе.

Важным этапом подхода к защите информации является определение:

- угроз безопасности информации;
- возможных способов реализации угроз безопасности информации;
- последствий от нарушения свойств безопасности информации (конфиденциальности, целостности, доступности).

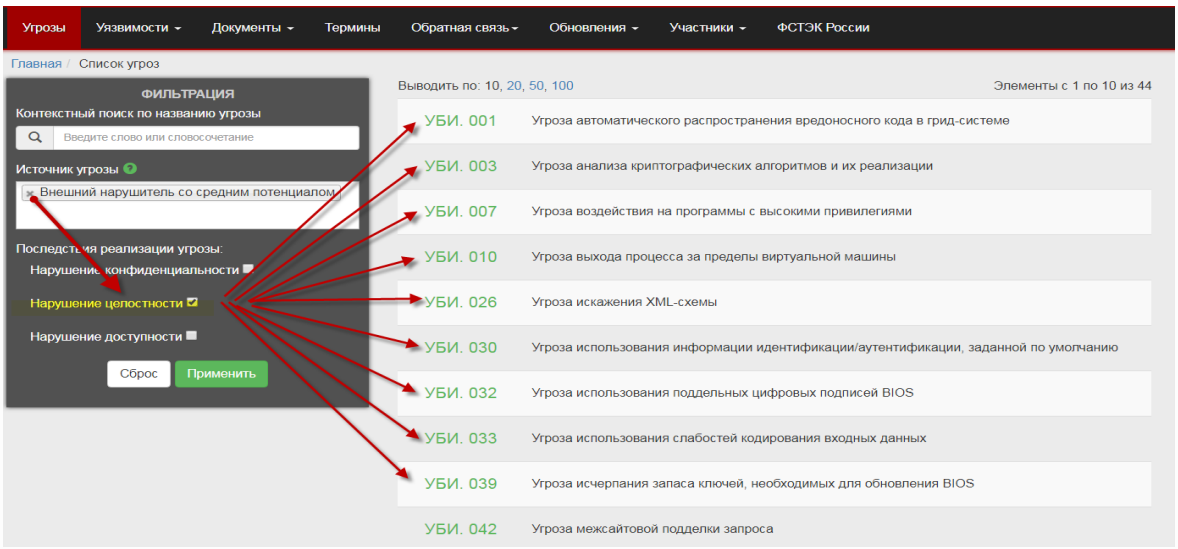


Рис. 1

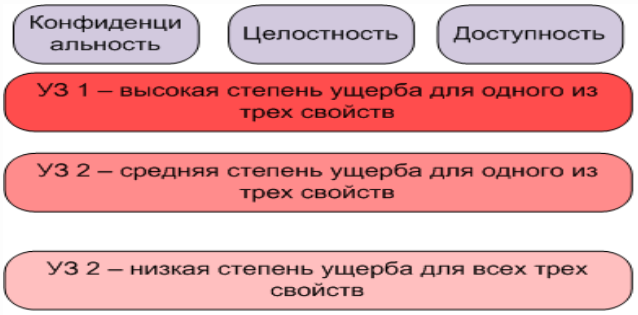
Требования к системе защиты информации ИС включаются в техническое задание на создание ИС или частное техническое задание на создание системы защиты информации информационной системы. Вводятся и систематизируются составы мер защиты информации (обеспечения безопасности) и их базовые наборы для соответствующего класса защищенности каждой категории информационных систем или объектов. Разрабатывается и вводится алгоритм выбора мер защиты.

Рис. 2

Методология защиты информации

1. Уровень защищенности.
2. Класс ИС.
3. Набор мер.
4. Подбор средств защиты информации.

Определение класса защищённости



Степень возможного ущерба	Возможный ущерб от нарушения безопасности информации и (или) функционирования ИС
Высокая	Возможны существенные негативные последствия и (или) ИС и (или) оператор, обладатель информации не могут выполнять возложенные на них функции
Средняя	Возможны умеренные негативные последствия и (или) ИС и (или) оператор, обладатель информации не могут выполнять хотя бы одну из возложенных на них функций
Низкая	Возможны незначительные негативные последствия и (или) ИС и (или) оператор, обладатель информации могут выполнять возложенные на них функции с недостаточной эффективностью или с привлечением дополнительных сил и средств

Рис. 3

Уровень значимости информации	Масштаб информационной системы		
	Федеральный	Региональный	Объектовый
УЗ 1	К1	К1	К1
УЗ 2	К1	К2	К2
УЗ 3	К2	К3	К3

Рис. 4

Порядок действий по выбору мер защиты информации для их реализации в ИС

Рис. 5

Для проведения работ по защите информации в ходе создания и эксплуатации информационной системы обладателем информации (заказчиком) и оператором в соответствии с законодательством Российской Федерации при необходимости привлекаются организации, имеющие лицензию на деятельность по технической защите конфиденциальной

информации в соответствии с Федеральным законом от 4 мая 2011 г. № 99-ФЗ «О лицензировании отдельных видов деятельности» (Собрание законодательства Российской Федерации, 2011, № 19, ст. 2716; № 30, ст. 4590; № 43, ст. 5971; № 48, ст. 6728; 2012, № 26, ст. 3446; № 31, ст. 4322; 2013, № 9, ст. 874).

Для обеспечения защиты информации, содержащейся в информационной системе, применяются средства защиты информации, прошедшие оценку соответствия в форме обязательной сертификации на соответствие требованиям по безопасности информации в соответствии со статьей 5 Федерального закона от 27 декабря 2002 г. № 184-ФЗ «О техническом регулировании» (Собрание законодательства Российской Федерации, 2002, № 52, ст. 5140; 2007, № 19, ст. 2293; № 49, ст. 6070; 2008, № 30, ст. 3616; 2009, № 29, ст. 3626; № 48, ст. 5711; 2010, № 1, ст. 6; 2011, № 30, ст. 4603; № 49, ст. 7025; № 50, ст. 7351; 2012, № 31, ст. 4322; 2012, № 50, ст. 6959).

Защита информации, содержащейся в информационной системе, является составной частью работ по созданию и эксплуатации информационной системы и обеспечивается на всех стадиях (этапах) ее создания, в ходе эксплуатации и вывода из эксплуатации путем принятия организационных и технических мер защиты информации, направленных на блокирование (нейтрализацию) угроз безопасности информации в информационной системе, в рамках системы (подсистемы) защиты информации информационной системы (далее – система защиты информации информационной системы) (в ред. Приказа ФСТЭК России от 15.02.2017 № 27).

Организационные и технические меры защиты информации, реализуемые в рамках системы защиты информации информационной системы, в зависимости от информации, содержащейся в информационной системе, целей создания информационной системы и задач, решаемых этой информационной системой, должны быть направлены на исключение:

- неправомерных доступа, копирования, предоставления или распространения информации (обеспечение конфиденциальности информации);
- неправомерных уничтожения или модифицирования информации (обеспечение целостности информации);
- неправомерного блокирования информации (обеспечение доступности информации).

Для обеспечения защиты информации, содержащейся в информационной системе, проводятся следующие мероприятия:

- формирование требований к защите информации, содержащейся в информационной системе;
- разработка системы защиты информации информационной системы;
- внедрение системы защиты информации информационной системы;
- аттестация информационной системы по требованиям защиты информации (далее – аттестация информационной системы) и ввод ее в действие;
- обеспечение защиты информации в ходе эксплуатации аттестованной информационной системы;
- обеспечение защиты информации при выводе из эксплуатации аттестованной информационной системы или после принятия решения об окончании обработки информации.

В современном цифровом мире данные стали главной ценностью, и для их защиты требуется тщательный, индивидуальный подход. Целью проводимых в организациях мероприятий по защите информации является обеспечение её безопасности.

PONOMAREV Dmitry Alexandrovich
Russia, Krasnodar

FILIMONOV Vitaly Sergeevich
Russia, Krasnodar

PROTECTION OF PUBLICLY AVAILABLE INFORMATION CONTAINED IN INFORMATION SYSTEMS

Abstract. *The article discusses the key aspects of the information security system (IIS) in the context of the functioning of information systems (IS) at various levels – federal, regional and facility. The main objects of protection are highlighted, including information, technical means, software, technologies and means of protection.*

Keywords: *information security system, information system, security measures, confidentiality.*

ЩЕТКИН Виктор Александрович
магистрант, Краснодарское высшее военное училище, Россия, г. Краснодар

КОБЕЦ Денис Гавриилович
магистрант, Краснодарское высшее военное училище, Россия, г. Краснодар

Научный руководитель – доцент Краснодарского высшего военного училища, кандидат военных наук Починок Виктор Викторович

ОБНАРУЖЕНИЕ СЕТЕВЫХ КОМПЬЮТЕРНЫХ АТАК «НУЛЕВОГО ДНЯ» С ИСПОЛЬЗОВАНИЕМ ИСКУССТВЕННЫХ НЕЙРОННЫХ СЕТЕЙ

Аннотация. *В этом документе предлагается реализация модели, которая использует данные анализа сетевого трафика (NTA) и счетчика производительности оборудования (HPC) для точного выявления атак «нулевого дня». Цель состоит в том, чтобы разработать модель на основе автоэнкодера, которая объединяет аппаратные и сетевые функции для эффективной классификации. Использовались датасеты для обучения нейросетевых моделей, такие как CICIDS2020, NSL-KDD и D.A.V.I.D.E HPC.*

Ключевые слова: *IDS, автоэнкодер, NTA, CICIDS2020, NSL-KDD, атака «нулевого дня», HPC, HMD, NIDS.*

I. Введение

Экспоненциальный рост числа кибератак приводит к появлению инновационных подходов к их противодействию атакам и новой эре киберугроз. Системы обнаружения вторжений, которые способны обнаруживать атаки на основе сигнатур, не работают всякий раз, когда возникает новая угроза или атака «нулевого дня» [1]. Это приводит к снижению безопасности до тех пор, пока не будет обнаружено нарушение. Идентификаторы, способные обнаруживать атаки «нулевого дня», являются единственным жизнеспособным вариантом для борьбы с этими киберугрозами. Однако существующие идентификаторы не отличаются высокой точностью в обнаруживании знакомых угроз, они не могут идентифицировать атаки «нулевого дня» [2].

Атаки «нулевого дня» – это атаки, схемы трафика которых не совпадают с какой-либо общей схемой трафика вредоносных программ или атаками на них [3]. Идентификаторы, которые могут идентифицировать угрозы «нулевого дня», в настоящее время используются в кибербезопасности в связи с растущим использованием методов машинного обучения. Идентификаторы в широком смысле подразделяются на три основные категории, обозначенные как:

1. Идентификаторы на основе хостов [4];
2. Сетевые идентификаторы [4, 5];
3. Гибридные IDS [5].

В связи с расширением использования искусственного интеллекта в кибернетике появилось несколько категорий идентификаторов на основе искусственного интеллекта, которые способны обнаруживать атаки «нулевого дня», что в настоящее время привлекает академических исследователей и разработчиков.

В настоящее время существуют следующие типы идентификаторов, такие как: [6, 7, 8] идентификаторы на основе сигнатур, идентификаторы, основанные на контролируемом или гибридном обучении, идентификаторы, основанные на переносе обучения, идентификаторы, основанные на аномалиях, идентификаторы, основанные на графах.

Положительные факторы использования машинного обучения – эффективность в решении проблем обнаружения атак «нулевого дня», поскольку его эффективность уже оценена с использованием таких моделей, как случайный лес, дерево решений, KNN, персептрон и т. д. [8, 9].

В существующих исследованиях в качестве критериев классификации использовались данные анализа сетевого трафика.

Предлагаемая методология

Предлагаемая методология заключается в разработке модели обнаружения атак «нулевого дня», основанной на нейронных сетях, с использованием сетевого трафика и

аппаратных данных, расширяющих возможности автоэнкодера.

В этой работе перечислены три основных рассматриваемых аспекта:

- разработка и внедрение на практике системы обнаружения атак «нулевого дня» с использованием эффективной модели автоэнкодера, встраиваемую в IDS;
- создание одноклассовой SVM-модели для обнаружения атак;
- сравнение производительности одноклассовой SVM-модели, которая действует как базовый детектор атак, с предлагаемой моделью автоэнкодера.

Проблемы, связанные с обнаружением атак «нулевого дня»

Основное препятствие для обнаружения атак «нулевого дня» с использованием нейронных сетей связано с типом набора данных и его недоступностью, поскольку в нем нет наборов данных, сочетающих аппаратные и сетевые свойства. Термин «атака «нулевого дня» используется для обозначения уязвимости, которая ранее не была выявлена [1], что затрудняет точную идентификацию и прогнозирование модели атак «нулевого дня» в практических ситуациях. Эти атаки постоянно меняются и часто используют в своих интересах новые уязвимости, что делает их более эффективными. Сложнее обнаружить их с помощью стандартных методов. В результате, когда поток данных известен и цель состоит в том, чтобы обнаружить ранее выявленные методы атаки, а не предсказывать совершенно новые и неизвестные слабые места, модели нейронных сетей оказываются более полезными, и задача состоит в том, чтобы внедрить модели, способные эффективно выявлять новые атаки

II. Обзор литературы

2.1. Этот раздел содержит описание различных методологий, которые рассматриваются и используются для обнаружения атак «нулевого дня» в области кибербезопасности. Такие исследователи, как Ханна Хинди, Ян Го, Цяньру Чжоу и другие, изучили многочисленные наборы данных, от CICIDS2020 до NSL-KDD, применив такие методы, как одноклассовая SVM, автоэнкодер и различные модели глубокого обучения. Анализ сетевого трафика, обнаружение вредоносных программ с аппаратной поддержкой, упрощенные методы принятия решений, и даже внедрение глубокого обучения с подкреплением. В целом, эти исследования предоставляют ценную информацию о том, как развивается система обнаружения атак «нулевого дня», подчеркивая потребность в передовых моделях и эталонных наборах данных в этой жизненно важной области.

2.2. Сопутствующая работа Патидара в [1] на основе использования наборов данных о вредоносных программах описано, как различные типы вредоносных программ влияют на безопасность и как можно построить модель обнаружения в режиме «нулевого дня», используя соответствующие методы обнаружения, подчеркивающие важность обнаружения атак в режиме «нулевого дня». Хинди и др. в [2] обсуждалось использование возможностей кодирования и декодирования autoencoder для создания идентификаторов на основе сигнатур для обнаружения «нулевого дня». Хинди и др. [2] использовали CICIDS2020 и NSL-KDD поверх набора данных KDD-CUP99 для обучения модели. В своем исследовании Мбона и др. [6] создали единый класс. Модель на основе классификатора SVM с использованием CICDDOS 2019. Янг Гоу [8] провел обзорное исследование и сравнительный анализ различных типов идентификаторов для обнаружения «нулевого дня» на основе сигнатур. Для анализа производительности были использованы наборы данных IDS2017 и NSL KDD, а также автоэнкодер One Class SVM, случайный лес и т. д. Чжоу и Пезаро [9] использовали данные CIC-расходомера, а именно CIC-AWS-2018, для обучения шести различных моделей выявлению нулевых дней и анализу их сравнительных характеристик. Для повышения производительности используются несколько методов, таких как случайный лес, Гауссовский наивный анализ, Дерево решений, многослойный Персептрон, KNN и квадратичный дискриминантный анализ. Макрани и др. [10] воспользовались данными в режиме реального времени и подготовили сравнительный обзорный документ, в котором сравнивались случайный лес, дерево решений, стохастический градиентный спуск и т.д. Гао и др. [12] разработали малогабаритный, чувствительный к затратам механизм принятия решений на основе дерева, который точно определяет, принимая во внимание предпочтения пользователей и компромисс между наилучшей производительностью и затратами на внедрение, классификатор машинного обучения для использования при онлайн - обнаружении вредоносных программ. Согласно результатам тестирования, предложенный метод может обнаруживать вредоносные программы на оборудовании почти в

94% случаев, значительно снижая затраты на установку. Редди и др. [13] использовали глубокое обучение с подкреплением для автоматизации задачи обнаружения вторжений, которая включает глубокое обучение в традиционное обучение с подкреплением, что приводит к усовершенствованной стратегии борьбы с киберугрозами. Делдар и др. [14] обсудили эффективность методов, основанных на частичном контроле, безнадзорности и малозатратном использовании, для эффективного обнаружения вредоносных программ с «нулевого дня». Али и др. [15] использовали набор данных CICIDS2020, чтобы описать обнаружение атак «нулевого дня» и то, как они классифицируются как методы обнаружения на основе аномалий, графиков и искусственного интеллекта. Икбал и др. [16] представили всесторонний обзор современных методик обнаружения «нулевого дня» в виде BLOSOM и CNN, а также подчеркнули необходимость в новых тестируемых наборах данных вместо традиционных. Чен и др. [17] разработали модель обнаружения вредоносного ПО «нулевого дня» для Android, которая рассматривает график потока управления приложением для обнаружения несанкционированных вызовов. Аката и др. al [18] использовал наборы данных NSL-KDD и CICIDS2020 для разработки модели, способной обнаруживать атаки «нулевого дня». Кумар и др. [19] продемонстрировали эффективность нейронных сетей Generative adversarial network (GAN) в эффективном обнаружении атак «нулевого дня», используя набор данных CIC-AWS 2018.

III. Набор данных

3.1. Предварительная обработка NSL-KDD CICIDS2020[20] и NSL-KDD [21], выпущенные CIC (Канадским институтом кибербезопасности), представляют собой наборы данных о сетевых потоках, используемые для оценки предлагаемой модели. Эти наборы данных содержат классификацию кибератак и нормального трафика. Пятидневный отчет о кибератаках в формате raw содержится в CICIDS2020 [20], а атаки со стороны внутренних и внешних нарушителей описаны следующим образом.

Набор данных NSL-KDD был представлен для смягчения ограничений набора данных KDD Cup99, предоставляющего четыре кибернетических класса, называемых от пользователя до root (U2R), от удаленного до локального нарушителя (R2L), отказ в обслуживании (DoS). Он доступен в виде пары файлов test-train.csv как KDDTrain+.csv' и 'KDDTest+.csv'. [21] D.A.V.I.D.E [22, 23, 24] Системный набор данных HPC, используемый для обучения HMD (hardware-supported malware detection system). Набор данных HPC состоит из значений программного счетчика, зарегистрированных с помощью суперкомпьютера D.A.V.I.D.E. [23, 24].

IV. Обзор методологии

В этом разделе рассматриваются наборы данных для предварительной обработки, предлагаемая модель, а также процесс обучения и оценки.

4.1. Предварительная обработка Предварительная обработка включает в себя подготовку наборов данных, включая наборы данных NSL-KDD, CICIDS2020 и DAVIDE HPC, для использования.

4.1.1. Предварительная обработка CICIDS2020. Набор данных CICIDS2020 разделяется на основе класса атаки и временных меток, предоставляемых в наборе данных, сгенерированный в отдельные файлы «pcap», сильно коррелированные признаки исключаются с учетом порогового значения «0,9».

4.1.2. Предварительная обработка NSL-KDD. Набор данных NSL-KDD поставляется в виде пары тестовых файлов train.csv, что позволяет использовать его для целей оценки, минуя обширную предварительную обработку.

4.1.3. Предварительная обработка DAVIDE HPC. Набор данных DAVIDE включает данные с узлов суперкомпьютера, собранные для анализа аномалий в поведении узлов. Его предварительная обработка включает определение временных меток для обработки и идеальных временных интервалов для необязательного удаления перед передачей данных в автоматический кодировщик.

4.2. Модель на основе автоэнкодера. Основой предлагаемой модели на основе автоэнкодера служит искусственная нейронная сеть (ANN). Для выбора структуры сети, количества периодов и скорости обучения для оптимизации гиперпараметров используется случайный поиск. Хорошо известно, что случайный поиск быстрее приводит к полуоптимальному набору параметров, чем поиск по сетке. Когда требуется всего несколько параметров, было продемонстрировано, что он улучшает поиск по сетке [1]. Это уменьшает вероятность получения завышенных параметров. Обучающая выборка разделена на тренировочную и тестовую на 75% и 25%, соответственно. Таким образом, для инициализации модели используется идеальная схема ANN, которая включает количество

скрытых слоев и нейронов в каждом слое. Эта модель обучалась в течение «n» периодов времени. При анализе кривых точности и потерь проверяется сходимость автоэнкодера.

4.3. Одноклассовая модель на основе SVM. Одноклассовый SVM является расширением модели SVM, основанной на контролируемом обучении, и позволяет проводить обучение без контроля, когда определяется один класс. В отличие от автоэнкодера, где выходные данные основаны на пороговом значении, на выходе генерируется двоичный код, определяющий соответствует ли экземпляр классу, для которого обучается SVM, или нет. Для NIDS в предлагаемой нами модели используется одноклассовый SVM для сравнения его производительности с автоэнкодером. Обученные модели предлагается объединить вместе, чтобы объединить эффективность функций HIDS и NIDS, что еще больше повысит решающую или прогностическую способность предлагаемой модели для прогнозирования атаки «нулевого дня». Предлагаются модели на основе автоэнкодера, которые имеют AUC от 90 до 95% и выше [1, 10]. В отдельности предлагаемая объединенная модель направлена на достижение целевого AUC составляет 90% или выше.

V. Заключение

Мировые исследователи и разработчики с интересом следят за последними достижениями в области искусственного интеллекта в области кибербезопасности. Использование моделей машинного обучения позволяет не только прогнозировать атаки, которые известны системе, но и выявлять атаки «нулевого дня», сигнатуры которых отсутствуют в системе. Но прогресс ограничивается изобретениями с учетом многих проблем и недостатков современных технологических парадигм. Предложенные методы являются многообещающими с точки зрения эффективного использования аппаратных средств и сетевых данных для выявления угроз «нулевого дня». В модель включены функции анализа, кодирования, отображения и обнаружения. Эта идея привела к появлению нескольких новых концепций, бизнес-возможностей и возможностей для разработки широкого спектра услуг и продуктов. В этой работе описаны технические требования для реализации моделей обнаружения атак «нулевого дня» на основе сигнатур. Прежде всего, в ней представлен современный пример использования кибербезопасности и искусственного интеллекта, над которым работают исследователи и разработчики. В этой статье дается представление о том, как модели машинного обучения могут быть использованы для обнаружения «нулевого дня» и расширяет методологию моделирования на основе автоэнкодера для обнаружения атак «нулевого дня».

Литература

1. Патидар К.П., Харшита Х. «Обнаружение атак «нулевого дня» с использованием методов машинного обучения», 2019 г., ХИДЖРА.

2. Беллекенс К., Хинди Х., Жан-Ноэль К., Тахтацис К., Аткинсон Р. и Бейн И. Использующий методы глубокого обучения для эффективного Обнаружение атак «нулевого дня», 14 октября 2020 года, MPDI Электроника 2020

3. Лайеги С., Портманн М., Галлахер М., Сархан М. «От машинного обучения с нуля до обнаружения атак с «нулевого дня», 2023, IJIS.

4. Ахмад Х., Аршад М.Дж., Джавед М., Уппал М., Обзор систем обнаружения вторжений Система (IDS) вместе с ее широко используемыми методами и классификациями, 2014, IJCST.

5. Аммар О., Мохаммед С., Захари Т., Набиль Т. Обзор по обнаружению вторжений Типы систем, 2018, IJCSDF, SDIWC.

6. Ян Х.П.Э., Мбона И. обнаруживающие Атаки на проникновение с «нулевого дня» с использованием полууправляемых Подходы к машинному обучению, опубликованные 29 июня 2022 года, IEEE.

7. Алексакис Т., Деместихас К., Адамопулу Е., Пепперс Н. проанализировали эффективность атак «нулевого дня» на выборках данных Сгенерированных с помощью GANs на основе классификаторов глубокого обучения, 2023, Журналы MPDI Sensors, Том 23, выпуск 2.

8. Ян Го. «Обнаружение атак «нулевого дня» на основе машинного обучения: проблемы и направления на будущее», 2023, «Компьютерные коммуникации».

9. Пезарос Д., Чжоу Ц. Оценка классификаторов машинного обучения для обнаружения атак «нулевого дня». Обнаружение вторжений: анализ набора данных CIC-AWS-2018, 2019.

10. Чжан Ин Хэ, Хомаюн Х., Алиасгари М., Мохаммади М.Х., Миари Т., Саяди Х. Когда машинное обучение вступает в силу Аппаратная кибербезопасность: разработка точных программ «нулевого дня» Обнаружение вредоносных программ, 2021, ISQED.

11. Хоссейн Д.А., Солтани М., Усат Б., Джафари С.М. Способные к адаптации Система

обнаружения вторжений на основе глубокого обучения сведена к нулю День терактов, 2021.

12. Гао И., Хомаюнц Х., Лин Д., Резайкс А., Алиасгарикс М., Мохаммади М.Х., Саяди Х. Adaptive HMD: Точное и экономичное машинное обучение Обнаружение вредоносных программ на основе микроархитектуры Мероприятия, 2021 год, 27-я сессия IEEE IOLTS.

13. Хан Т.Н., Джанапа Р.В., Углубленное обучение с подкреплением для кибербезопасности, 2021 год, IEEE Trans. Нейронная сеть. Учить. Сестра.

14. Абади М., Дельдар Ф. Обучение для обнаружения вредоносных программ «нулевого дня» и их классификации Обзор, 2023, ACM Computing Surveys.

15. Ким К., Али С., Рехман С.У., Имран А., Адим Дж., Икбал З. Сравнительная оценка технологий, основанных на ИИ Методы обнаружения атак «нулевого дня». Электроника 2022, 11, 3934.

16. Мондонго, Токмак М. Угрозы «нулевого дня» Обнаружение критических инфраструктур, 2023, arXiv Labs.

17. Грейс М., Лю П., Чен Я. Risk Ranker: Масштабируемый и точный Android «нулевого дня».

18. Xian, Akata B., Schiele Y. From zero-shot machine learning to zero-day attack detection, 2019.

19. Pandey, S.K. Kumar, Sinha, The Effectiveness of Zero-Day Attacks Data Samples Generated via GANs on Deep Learning Classifiers, 2023, Advanced Computing and Systems for Security: Volume 14.

20. Canadian Institute for Cybersecurity. Intrusion Detection Evaluation Dataset (CICIDS2017). 2017. Available online: http://www.unb.ca/cic/datasets/ids-2017.html.

21. Canadian Institute for Cybersecurity. NSL-KDD Dataset. Available online: http://www.unb.ca/cic/datasets/nsl.html.

22. Data Set for Anomaly Detection on HPC system, Data set available online: https://zenodo.org/records/3251873.

23. Luca Benini, Michela Milano, Michele Lombardi, Andrea Bartolini, Andrea Borghesi, Anomaly Detection using Autoencoders in High Performance Computing Systems, 2019, IAAI19.

24. Luca Benini, Andrea Bartolini, Andrea Borghesi, and Antonio Libri, Online Anomaly Detection in HPC Systems, 2019, AICAS19.

SHCHETKIN Viktor Aleksandrovich
Master's Student, Krasnodar Higher Military College, Russia, Krasnodar

KOBETS Denis Gavrilovich
Master's Student, Krasnodar Higher Military College, Russia, Krasnodar

Scientific Advisor – Associate Professor of the Krasnodar Higher Military College, Candidate of Military Sciences Pochinok Viktor Viktorovich

DETECTION OF "ZERO-DAY" NETWORK COMPUTER ATTACKS USING ARTIFICIAL NEURAL NETWORKS

Abstract. *This document proposes an implementation of a model that uses Network traffic Analysis (NTA) and hardware Performance Counter (HPC) data to accurately detect zero-day attacks. The goal is to develop an autoencoder-based model that combines hardware and network functions for efficient classification. Datasets were used to train neural network models, such as CICIDS2020, NSL-KDD and D.A.V.I.D.E HPC.*

Keywords: *IDS, autoencoder, NTA, CICIDS2020, NSL-KDD, zero-day attack, HPC, HMD, NIDS.*

ШИБИН Андрей Сергеевич
слушатель, Краснодарское высшее военное училище имени генерала армии С. М. Штеменко, Россия, г. Краснодар

ПОЛТАРАК Игорь Валерьевич
слушатель, Краснодарское высшее военное училище имени генерала армии С. М. Штеменко, Россия, г. Краснодар

ИЛЬИН Кирилл Алексеевич
слушатель, Краснодарское высшее военное училище имени генерала армии С. М. Штеменко, Россия, г. Краснодар

СИНТЕЗ МОДЕЛИ ФОРМИРОВАНИЯ ТРЕБОВАНИЙ К СИСТЕМЕ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ МЕЖВИДОВОЙ СИСТЕМЫ ИНФОРМАЦИОННОГО ОБМЕНА ВООРУЖЕННЫХ СИЛ РОССИЙСКОЙ ФЕДЕРАЦИИ

Аннотация. *В статье представлена модель формирования требований к системе обеспечения информационной безопасности (СОИБ) в межвидовой системе информационного обмена (МСИО) Вооруженных Сил Российской Федерации. Модель предназначена для выработки перечня правовых, организационных и технических мер защиты информации, обрабатываемой в военных автоматизированных системах (АС), с учетом угроз информационной безопасности (ИБ), нормативной правовой базы и характеристик объектов информатизации.*

Ключевые слова: *информационная безопасность, СОИБ, межвидовая система информационного обмена, Вооруженные Силы РФ, автоматизированная система, классификация угроз, уровень значимости информации, защита информации, требования к ИБ, модель ИБ.*

Модель формирования требования к системе обеспечения безопасности информации (далее – СОИБ) межвидовой системы информационного обмена Вооруженных Сил Российской Федерации (далее – МСИО) предназначена для формирования перечня требований по правовым, организационным и техническим мерам защиты информации и к СОИБ в целом.

Постановка задачи синтеза модели формирования требования.

Необходимо с учетом угроз безопасности информации (далее – ИБ), нормативных правовых актов и нормативных документов сформировать перечень требований к СОИБ, обеспечивающих нейтрализацию угроз безопасности информации, обрабатываемой на объекте информатизации (далее – ОИ) военной организации.

В качестве исходных данных для синтеза модели используются:

- система нормативной правовой базы в области ИБ, множество требований $Р^{П}$;
- виды обрабатываемой информации, множество видов, обрабатываемой информации $Н^{И}$;
- множество угроз безопасности информации $W^{М}$.

Результаты, проведенных исследований показали, что в состав модели формирования требований должны входить:

- процедуры формирования требований к правовым мерам ЗИ (состав и содержание организационно-распорядительных документов);
- процедуры формирования требований к организационным мерам (структура органа по обеспечению безопасности информации (ИБ), укомплектованность и уровень подготовленности сотрудников);
- классификация ОИ военной организации;

- процедуры формирования технических требований к системе защиты информации (далее – СЗИ).

Структура модели формирования требований представлена на рисунке 1.

Процедуры формирования требований к ОРД и структуре службы (подразделений), обеспечивающих ИБ, заключаются: в анализе нормативных правовых актов и нормативных документов в области ИБ; формировании перечня организационно-распорядительных документов необходимых для создания и функционирования СОИБ; требований к структуре службы (подразделений) обеспечивающих ИБ; требований к квалификации специалистов (должностных лиц по защите информации) службы (подразделений).

Руководящий документ [1] определяет порядок классификации автоматизированных систем, подлежащих защите от несанкционированного доступа к информации, и требования по защите информации в АС различных классов.

Исходными данными для определения класса защищенности автоматизированной системе (далее – АС) являются:

- множество уровней значимости информации U^3, $U^3 = \{u^3_j\}$, $j = 1 \div J$ – количество уровней значимости служебной информации, $J = 4$, где u^3_1, u^3_2, u^3_3, u^3_4 – 1 категория, 2 категория, 3 категория и объекты, которым отсутствует необходимость присвоения категории значимости соответственно;
- масштаб АС (ОИ) $M^{ИС}$, $M^{ИС} = \{m^{ИС}_1, m^{ИС}_2, m^{ИС}_3\}$, где $m^{ИС}_1$, $m^{ИС}_2$, $m^{ИС}_3$ – распределенная, локальная сеть либо отдельный ОВТ соответственно;
- множество видов информации $H^И$, $H^И = \{h^И_i\}$, где $i = 1, 2, ..., I$ – количество видов информации;
- множество свойств безопасности информации C, $C = \{C_П\}$, где $n = 1 \div N$ – количество свойств безопасности информации;
- множество областей деятельности D, $D = \{d_g\}$, $g = 1 \div G$ – количество областей деятельности;
- W^A – множество актуальных угроз безопасности информации $W^A = \{w^A_r\}$, $r = 1 \div R$ – количество актуальных угроз безопасности;
- $У^в$ – множество видов ущерба, $У^в = \{y^B_к\}$, $k = 1 \div K$ – количество видов ущерба;
- $У^с$ – множество степеней возможного ущерба, $У^с = \{y^c_m\}$, $m = 1 \div M$ – количество степеней ущерба $M = 3$, где y^c_1, y^c_2, y^c_3 – высокий, средний, низкий уровни возможного ущерба соответственно;
- $Q^{ИС}$ – множество режимов обработки данных и прав доступа пользователей, $Q^{ИС} = \{q^{ИС}_z\}$, $z = 1 \div Z$ – количество возможных вариантов совмещения.

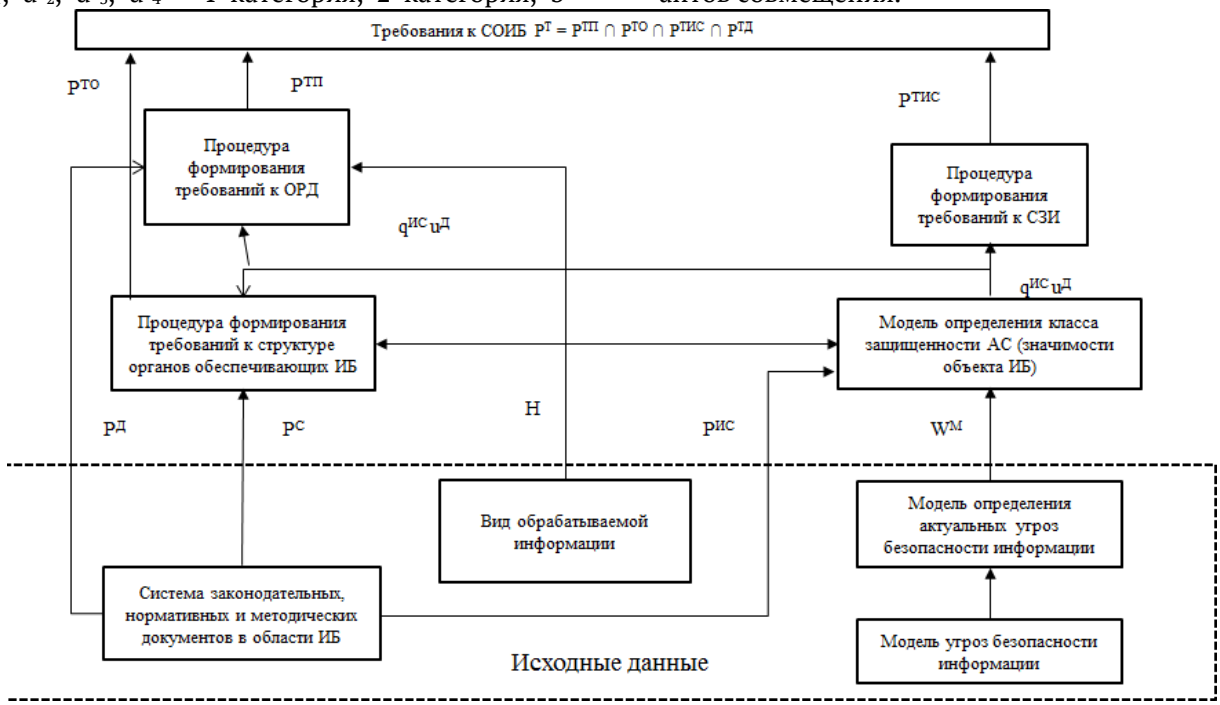


Рис. 1. Модель технологии формирования требований к системе обеспечения информационной безопасности

Таким образом, модель определения класса защищенности АС должна включать в себя:

- определение вида информации $H = \{h_\psi\}$;
- масштаб объекта защиты $М^{ИС} = \{m^{ИС}_1\}$;
- определения степени ущерба $У^с$ (множество свойств безопасности информации С, $С = \{С_п\}$; области деятельности $D = \{d_g\}$; виды ущерба, $У^в = \{у^в_к\}$;
- степени возможного ущерба, $У^с = \{у^с_m\}$);
- определение уровня значимости информации $U^З = F_6$ (С, $У^с$);
- определение режима обработки данных и прав доступа пользователей $Q^{ис}=F_7$ ($U^З$, $М^{ИС}$).

Для каждого свойства безопасности информации ($с_1$, $с_2$, $с_3$) устанавливаются следующие степени возможного ущерба:

- высокой, если в результате нарушения одного из свойств безопасности информации возможны существенные негативные последствия и (или) АС перестала выполнять возложенные на неё функции;
- средней, если в результате нарушения одного из свойств безопасности информации возможны умеренные негативные последствия и (или) АС не может выполнять хотя бы одну из возложенных на неё функций;
- низкой, если в результате нарушения одного из свойств безопасности информации возможны незначительные негативные последствия и (или) АС выполняет возложенные функции с кратковременным снижением эффективности с привлечением дополнительных сил и средств.

Определяем следующие уровни значимости информации:

- информация имеет высокий уровень значимости ($u^З_1$), если хотя бы для одного из свойств безопасности информации определена высокая степень возможного ущерба;
- информация имеет средний уровень значимости ($u^З_2$), если хотя бы для одного из свойств безопасности информации определена средняя степень ущерба и нет ни одного свойства, для которого определена высокая степень ущерба;
- информация имеет низкий уровень значимости ($u^З_3$), если для всех свойств безопасности информации определены низкие степени ущерба;
- информация имеет минимальный уровень значимости ($u^З_4$), если обладателем информации и (или) оператором степень ущерба от нарушения свойств безопасности информации не может быть определена, но при этом информация подлежит защите в соответствии с законодательством Российской Федерации.

В случае обработки в информационных системах двух и более видов значимой информации (конфиденциальные данные и иные установленные законодательством Российской Федерации виды информации ограниченного доступа) уровень значимости информации определятся отдельно для каждого вида информации.

Итоговый уровень значимости информации, обрабатываемой в ИС, устанавливается по наивысшим значениям степени возможного ущерба, определенным для конфиденциальности, целостности, доступности информации каждого вида информации.

Множество требований к СОИБ ($Р^Т$), в общем случае, включает в себя:

- множество требований, предъявляемых к правовым мерам ОИБ ($Р^{ТП}$);
- множество требований, предъявляемых к организационным мерам ОИБ ($Р^{ТО}$);
- множество требований, предъявляемых к техническим мерам ОИБ ($Р^{ТИС}$).

Данные процедуры целесообразно реализовывать с использованием логических операций алгебры логики.

Требования к СОИБ определяются с учетом: вида обрабатываемой информации (Н); используемых АС и систем передачи данных ($Q^{ИС}$) и уровня значимости информации ($U^{ПД}$).

Процесс реализации процедур определения требований к ОИБ военной организации может быть представлен в виде, как показано на рисунке 2.

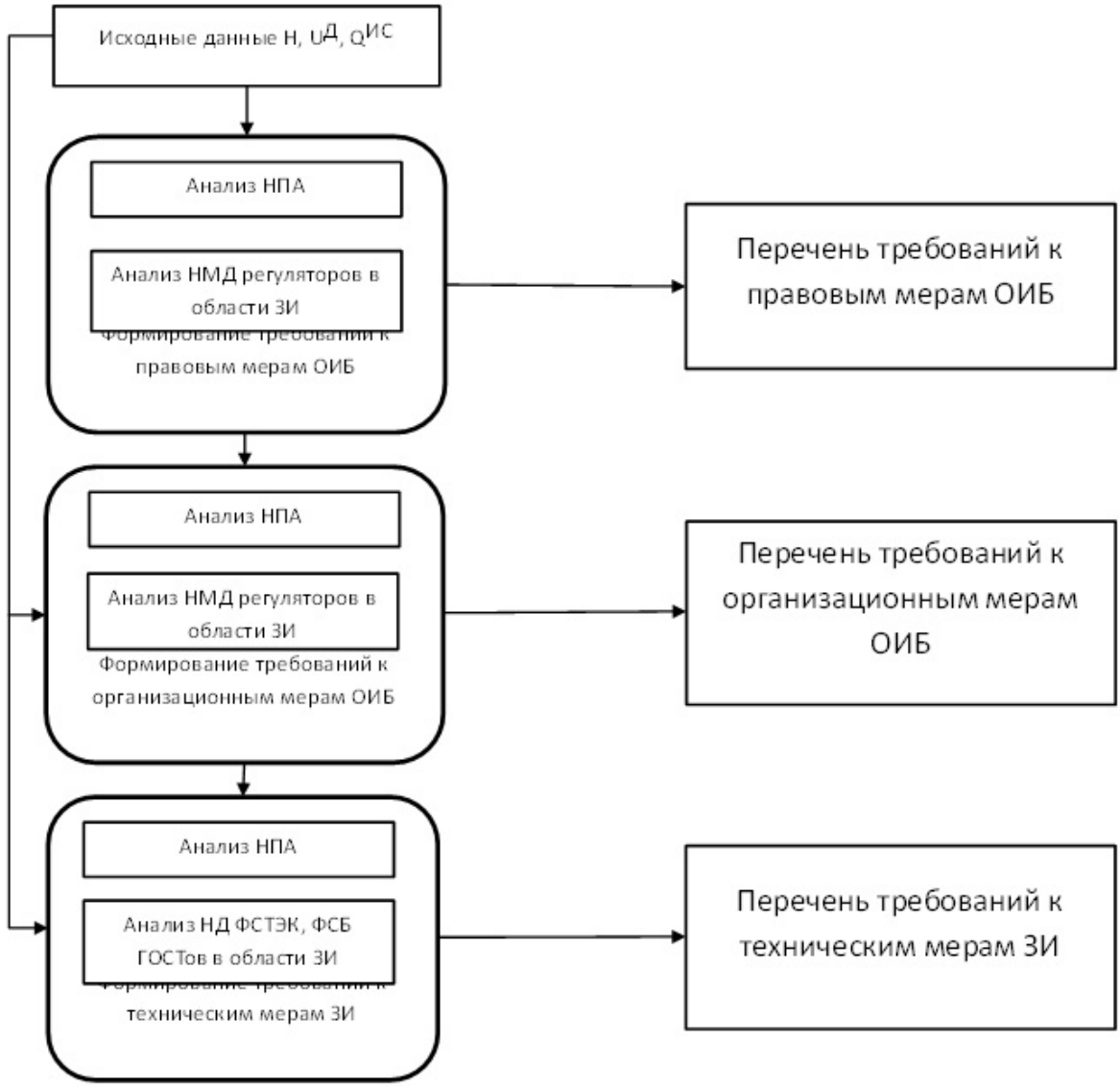


Рис. 2. Порядок реализации процедур определения требований к обеспечению информационной безопасности организации

Таким образом, сформированная модель перечней требований позволяет осуществить создание СОИБ в межвидовой системе информационного обмена Вооруженных Сил Российской Федерации. Для определения уровня ИБ военной организации потребуется провести синтез математической модели оценки состояния СОИБ.

Литература

1. Руководящий документ от 30.03 1992 г. «Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации».

SHIBIN Andrey Sergeevich
Student, Krasnodar Higher Military College named after Army General S. M. Shtemenko, Russia, Krasnodar

POLTARAK Igor Valerievich
Student, Krasnodar Higher Military College named after Army General S. M. Shtemenko, Russia, Krasnodar

ILYIN Kirill Alekseevich
Student, Krasnodar Higher Military College named after Army General S. M. Shtemenko, Russia, Krasnodar

SYNTHESIS OF A MODEL FOR THE FORMATION OF REQUIREMENTS FOR THE INFORMATION SECURITY SYSTEM OF THE INTERSPECIFIC INFORMATION EXCHANGE SYSTEM OF THE ARMED FORCES OF THE RUSSIAN FEDERATION

Abstract. *The article presents a model for the formation of requirements for the information security management system (IIS) in the interspecific information exchange system (IIS) The Armed Forces of the Russian Federation. The model is designed to develop a list of legal, organizational and technical measures to protect information processed in military automated systems (AS), taking into account threats to information security, the regulatory framework and characteristics of information technology facilities.*

Keywords: *information security, interspecific information exchange system, the Armed Forces of the Russian Federation, automated system, threat classification, information significance level, information security requirements, information security model.*

ЯКШИН Андрей Алексеевич
слушатель, Краснодарское высшее училище, Россия, г. Краснодар

ДЕМЯНЕНКО Андрей Николаевич
слушатель, Краснодарское высшее училище, Россия, г. Краснодар

ЖИВУЧЕСТЬ СИСТЕМЫ УПРАВЛЕНИЯ И ИНФОРМАЦИИ, ПЕРЕДАВАЕМОЙ ПО РАДИОЛИНИЯМ РОБОТОТЕХНИЧЕСКИХ КОМПЛЕКСОВ

Аннотация. *В статье рассматриваются ключевые аспекты обеспечения информационной безопасности и устойчивости функционирования робототехнических комплексов (РТК) военного назначения в условиях информационно-технического воздействия (ИТВ). Подчеркивается рост числа угроз безопасности информации в связи с применением импортной элементной базы, использованием беспроводных каналов связи и ограниченным использованием средств криптографической защиты информации.*

Ключевые слова: *робототехнический комплекс (РТК), информационная безопасность, критически важные элементы системы (КВЭС), информационно-техническое воздействие (ИТВ), радиоэлектронное подавление (РЭП), спуфинг, криптографическая защита (СКЗИ).*

Разработка и внедрение робототехнических комплексов (РТК) неизбежно приводит к вопросам безопасности и живучести системы управления при их использовании.

Одновременно с появлением новых типов РТК увеличивается количество угроз безопасности информации, циркулирующей в радиолинии, а наличие уязвимостей в протоколах взаимодействия сегментов РТК и применение элементной базы и программного обеспечения зарубежного производства позволяют противнику осуществлять целенаправленное информационно-техническое воздействие (ИТВ) на критически важные элементы системы (КВЭС) РТК.

Информационно-техническое воздействие может осуществляться в виде программно-аппаратного и радиоэлектронного подавления. В условиях информационно-технического воздействия параметры КВЭС выходят за допустимые пределы или меняют свои значения, что приводит не только к нарушению информационной безопасности РТК, но и к нарушению устойчивости функционирования соответствующей КВЭС и РТК в целом, а также может привести к переходу РТК ВН в качестве субъекта угроз, что снижает его живучесть. При таких условиях противник может воздействовать, как на процесс обмена информацией – то есть проводить сетевые атаки, так и на физическую безопасность РТК – то есть проводить кибератаки, а также осуществлять воздействие непосредственно на систему управления РТК и на процесс взаимодействия робота с пунктом управления.

Современные угрозы безопасности информации при ее передаче формируют проблему незаконного (несанкционированного) внедрения (воздействия) в (на) радиолинию, обеспечивающую информационный обмен между РТК ВН и пунктом управления. Основные типы ИТВ, осуществляемые на РТК ВН направлены на перехват управления, вывод их из строя, получение телеметрической информации или проведения дальнейшей атаки на КВЭС.

К общепринятым уязвимым элементам РТК относятся:

- применение импортной элементной базы;
- необходимость постоянного обмена информацией с ПУ;
- использование на отдельных РТК беспроводных каналов связи (Wi-Fi, Bluetooth), имеющих свои характерные уязвимости;
- отсутствие или ограниченное использование СКЗИ;
- низкая живучесть;
- наличие возможных программных и аппаратных уязвимостей;
- универсальность исполнения РТК, что позволяет реализовать однотипные

программно-аппаратное воздействие (ПАВ) на большинство образцов.

Благодаря уязвимостям появляется возможность реализовать угрозы безопасности информации, которые обусловлены совокупностью способов несанкционированного и (или) случайного доступа к системам РТК, в результате которого возможно нарушение конфиденциальности, целостности и доступности информации. Угроза безопасности информации реализуется в результате образования канала реализации угроз между источником угрозы и РТК, что создает условия для проведения атакующего воздействия. Основными элементами канала реализации угроз безопасности информации РТК являются источник угрозы, среда распространения информации и носитель информации.

При передаче информации в радиолиниях РТК характерны следующие угрозы безопасности информации:

1. Радиоэлектронное подавление канала управления;
2. Нарушение или перехват управление РТК;
3. Перехват и дешифрование информации;
4. Навязывание ложной информации.
5. Воздействие на парольно-ключевые системы;
6. Внедрение средств негласного сбора информации.

С точки зрения информационной безопасности наибольший интерес представляют угрозы воздействия на канал управления РТК путем радиоэлектронного подавления (РЭП) средствами РЭБ и навязывания ложной информации. Атаки, относящиеся к реализации данных угроз, связаны между собой.

Угроза РЭП канала управление РТК заключается в возможности осуществления противником целенаправленного подавления радиолинии пункта управления – РТК путем формирования на вход приемных трактов РТК такого значения отношение сигнал/шум, которое не позволит обеспечить прием данных с требуемой степенью достоверности. Наиболее критичным элементом для РТК является радиолиния. Именно подавление радиолинии способно обеспечить максимальный эффект с точки зрения нарушения функционирования РТК.

Угроза нарушения или перехвата управления РТК заключается в возможности осуществления противником несанкционированного доступа (НСД) к информационной инфраструктуре РТК за счет получения прав доступа с функционалом оператора. Данная угроза обусловлена возможностью НСД к КВЭС РТК посредством перехвата информации, передающейся по беспроводному каналу.

В представленной структуре РТК выделены следующие системы, которые можно отнести к КВЭС:

- защиты информации;
- обработки данных;
- управления РТК и целевыми нагрузками;
- приема-передачи данных.

Модель угроз безопасности информации, циркулирующей в РТК, должна строиться с учетом угроз безопасности информации, уязвимостей и объектов защиты.

С учетом того, что РТК различного назначения представляют собой сложные системы, которые характеризуются следующими особенностями с точки зрения их рассмотрения как объектов, подверженных деструктивному информационному воздействию (ДИВ) злоумышленника:

- наличие сложных взаимосвязей между разнородными информационными потоками, функционирующими внутри РТК, например, снижение имитозащищенности, определяющей устойчивость управления РТК, может привести к переходу РТК в объект угроз;
- деструктивному информационное воздействие на информацию может привести к формированию ложных команд управления РТК и нарушению их функциональной устойчивости; ДИВ на инерциально-навигационную систему, интегрированную с высокоточной спутниковой аппаратурой (при движении у (на) поверхности воды) и системой машинного зрения может привести к нарушению достоверности специальной информации;
- наличие разнородных по структуре, формату и избыточности видов информации предполагает применение криптографических средств ЗИ и специальных протоколов передачи данных;
- массогабаритные и энергетические ограничения РТК определяют дополнительные требования к средствам обнаружения ДИВ и защиты систем РТК и информации, функционирующей в них.

Проведем классификацию угроз по стратегии нарушителя для достижения поставленной цели (таблица):

Таблица

Стратегии нарушителя

Уровень	Тип стратегии	Сценарий нарушителя
1 тип	Нарушение конфиденциальности	Компрометация ключевой документации на НПУ и РТК. Перехват и дешифрование информации. Вскрытие шифра в результате криптоанализа.
2 тип	Нарушение имитостойкости	Вскрытие алгоритма и ключа обеспечения имитостойкости. Навязывание ложных команд управления РТК, СИ, ТМИ и навигационных данных.
3 тип	Нарушение достоверности и доступности	Радиоэлектронное подавление команд управления РТК, СИ, ТМИ и навигационных данных. Нарушение правил вхождения в связь. Срыв синхронизации сеанса.
4 тип	Нарушение сохранности (работоспособности) элементов и подсистем РТК	Внедрение закладочных устройств. Модификация ПО. Подмена, уничтожение, хищение наиболее важных компонентов АНПА. Воздействие на элементы инфраструктуры: электропитание, линии связи и т. д. Снижение живучести системы управления РТК.

- первого типа направлены на установление (раскрытие) языка информационного обмена РТК-наземный (корабельный) пункт управления; цель - получить специальную информацию РТК (данные разведки, интеллектуальной системы принятия решений, команды управления в рамках боевой информационной системы);
- второго типа направлены на навязывание ложной информации; в данном случае предполагается навязывание ложных команд управления с наземных (корабельных) ПУ, а также перехват и целенаправленное искажение навигационных данных (спуфинг-атака); цель – перехват, затруднение или потеря управления РТК, навязывание ложной специальной информации;
- третьего типа направлены на срыв или ухудшение качества информационных взаимодействий путем создания агрессивной среды осуществления информационных взаимодействий, что достигается, например, при постановке помех средствами радиоэлектронного подавления и другими; цель – затруднить или нарушить управление РТК, искажение целевой информации;
- четвертого типа направлены на нарушение целостных характеристик систем обработки и защиты информации, а также других КВЭС; данные стратегии могут использоваться, когда отсутствуют возможности по реализации вышестоящих типов стратегий; цель – нанесение ущерба системам РТК путем ПАВ. При этом результатом воздействия является нарушение тех же составляющих информационной безопасности (конфиденциальности, целостности и доступности), а также нарушение устойчивости функционирования робототехнического комплекса военного назначения.

Как показано в таблице, предложенная классификация угроз по стратегии нарушителя для достижения поставленной цели определяет цели воздействия, которые коррелируют со свойствами безопасности информации, что позволяет в дальнейшем синтезировать систему защиты с оптимизацией данных параметров.

Рассматривая третий тип угрозы по стратегии нарушителя, что для обеспечения защиты конфиденциальной информации, передаваемой по радиолиниям, применяются средства криптографической защиты информации (СКЗИ). Информация, по радиолинии передается в виде пакета данных, состоящего из служебных данных широкополосной радиолинии, синхропосылки, зашифрованной информации и имитовставки.

Однако, при передаче пакета данных предъявляются высокие требования к синхропосылке, которая обеспечивает синхронизацию средств криптографической защиты информации (СКЗИ) на принимающей и передающей стороне. Причем надежная синхронихзация наземных и бортовых СКЗИ, сводится к требованиям обеспечения высокого уровня помехоустойчивости и приобретает важный проблемный характер.

Подразумевается, что противник не имеет физического доступа к структурным компонентам комплекса РТК, но может осуществлять

воздействия на систему синхронизации, провоцировать в ней помехи с целью нарушения процедуры обработки информации и, как следствие, снижать результативность его функционирования. Кроме того, беспроводное взаимодействие между комплексом РТК и наземным пунктом управления дает возможность противнику воздействовать на информацию, передаваемую по радиолиниям, что не позволяет обеспечить требуемую достоверность полученной синхропосылки.

Вместе с тем, основными объектами воздействия для угроз ИБ являются, подлежащие защите ресурсы РТК: программные, аппаратные, информационные.

Реализовать угрозы противник может на всех уровнях обработки информации в РТК. Для обоснованного применения механизмов защиты необходимо оценить уровень угроз на информационное обеспечение РТК.

Рассмотренные выше сценарии воздействия противника на радиолинию РТК, при их реализации, позволят противнику нарушить конфиденциальность, целостность и доступность обрабатываемой РТК информации, что в свою очередь, будет способствовать снижению эффективности применения РТК и живучести системы управления.

YAKSHIN Andrey Alekseevich
Student, Krasnodar Higher School, Russia, Krasnodar

DEMYANENKO Andrey Nikolaevich
Student, Krasnodar Higher School, Russia, Krasnodar

SURVIVABILITY OF THE CONTROL SYSTEM AND INFORMATION TRANSMITTED OVER THE RADIO LINES OF ROBOTIC COMPLEXES

Abstract. *The article discusses the key aspects of ensuring information security and the stability of the functioning of military-purpose robotic complexes (RTCs) in the context of information technology impact (ITV). The growing number of threats to information security is highlighted due to the use of imported hardware, the use of wireless communication channels and the limited use of cryptographic information protection tools.*

Keywords: *robotic complex (RTK), information security, critical elements of the system (CES), information technology impact (ITV), electronic suppression (RAP), spoofing, cryptographic protection (SCSI).*

АРХИТЕКТУРА, СТРОИТЕЛЬСТВО

КОЛЫБЕЛКИНА Ирина Николаевна
студентка,
Санкт-Петербургский государственный архитектурно-строительный университет,
Россия, г. Санкт-Петербург

ОПТИМАЛЬНЫЙ ВЫБОР БЫТОВОГО ГАЗОВОГО КОТЛА

Аннотация. *В статье сравниваются бытовые газовые котлы с открытой и закрытой камерой сгорания, приведены преимущества и недостатки, представлен анализ устанавливаемых котлов в частных домовладениях.*

Ключевые слова: *газификация, строительство, природный газ, газовый котел, частный дом, камера сгорания.*

Темпы газификации в России достигли отметки в 89 из 100% технически возможных на начало 2024 года [1]. Судя по представленным данным ПАО «Газпром» на 2021–2025 гг. наиболее высокий уровень газификации был запланирован и реализуется в центральной части страны, тогда как в отдаленных регионах ввиду территориальных особенностей и сравнительно низких объемов потребления природного газа скорость газификации значительно ниже.

Карта целей программы газификации приведена ниже (рис. 1).

Также в 2024 году постановлением правительства РФ [2] в программу социальной газификации были включены садоводческие некоммерческие товарищества (СНТ), что в разы повышает количество подключаемых участков и рост газифицируемых домовладений.

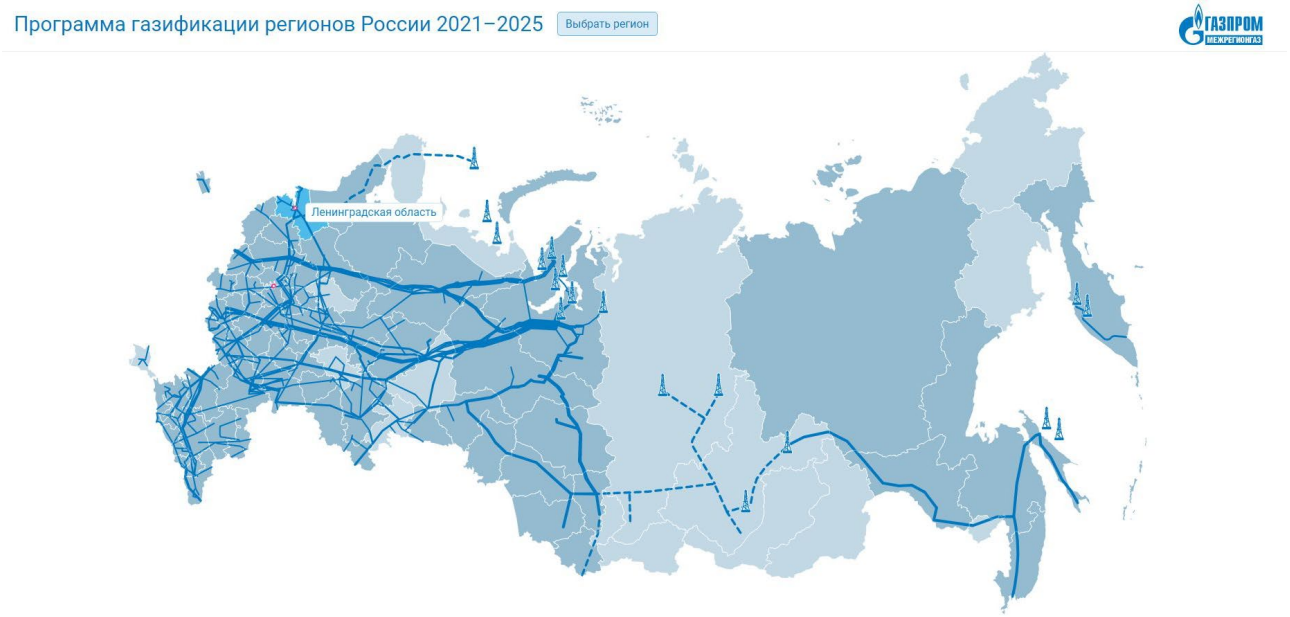


Рис. 1. Интерактивная карта целей программы газификации регионов РФ 2021–2025 гг.

Ввиду увеличивающегося количества подключений по программе газификации возрастает спрос на газовое оборудование. Для бытового использования применяются газовые варочные панели или газовые плиты с духовыми шкафами, для отопления и нужд горячего водоснабжения – газовые котлы. С выбором

последнего возникает ряд вопросов перед владельцем индивидуального жилого дома.

Рассмотрим классификацию газовых котлов [3], устанавливаемых в частных домовладениях (рис. 2).

Рис. 2. Схема классификации бытовых газовых котлов

От выбора котла зависят во многом параметры, на которые будет проверяться помещение теплогенераторной (котельной). Например, для размещения газового котла с открытой камерой сгорания согласно [4] минимальный объем помещения должен быть 15 м^3, а для котлов с закрытой камерой сгорания требование к минимальному объему – из удобства обслуживания оборудования. Связано это с тем, что последний всасывает воздух для поддержания горения с улицы и является явным преимуществом для тех домов, в которых на момент проектирования и строительства не предполагалось размещения котельной, работающей на природном газе.

Рассмотрим преимущества котлов с закрытой камерой сгорания.

1. Эффективность: в сравнении с открытой камерой сгорания КПД выше;
2. Безопасность: принудительная тяга воздуха обеспечивает стабильность горения и не затухание пламени;
3. Удобство монтажа: не требуется строительство и эксплуатация дымохода, отвод продуктов сгорания через коаксиальный патрубок.

Однако на ряду с этим, в качестве основного недостатка, выделяют дороговизну таких котлоагрегатов.

В сравнении с этим котлы с открытой камерой сгорания стоят дешевле, что является их преимуществом. Так же как простоту конструкции, отсутствие необходимости подключения к сети электропитания (особенно актуально для отдаленных районов, с перебоями электросетей).

Явным недостатком установки таких котлов является повышенный риск попадания продуктов сгорания в помещение.

Рассмотрев основные достоинства и недостатки каждой модели, был произведен анализ на примере из 100 проектных решений по газификации частных домовладений в Воронежской области. В ходе исследования были собраны данные об устанавливаемых газовых котлах. На диаграмме представлено распределение по критерию камеры сгорания (рис. 3).

Ввиду полученных результатов был сделан вывод о том, что преимущественно к установке принимались бытовые котлы с открытой камерой сгорания по причине наличия существующего дымохода (при переустройстве домов с печного отопления), также из-за невозможности подключения к сети электропитания надувного вентилятора (при перебоях в работе сети электроснабжения), а также по стоимостным характеристикам, что было отражено в проектной документации.

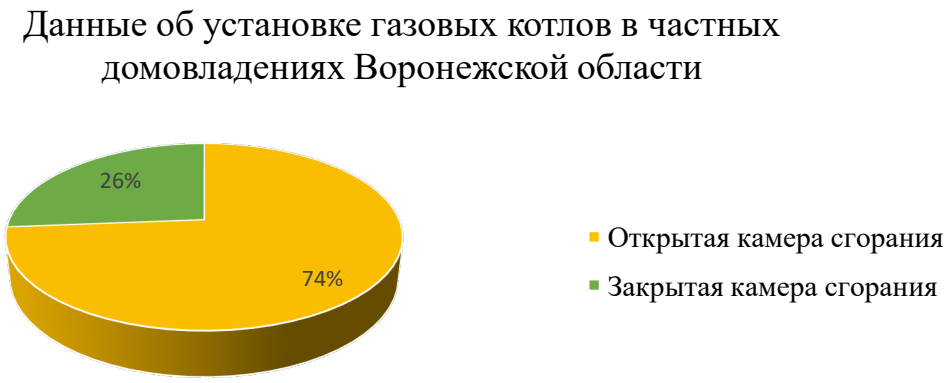


Рис. 3. Диаграмма вида устанавливаемых газовых котлов

Также были рассмотрены марки устанавливаемого оборудования и отображены на диаграмме ниже (рис. 4).

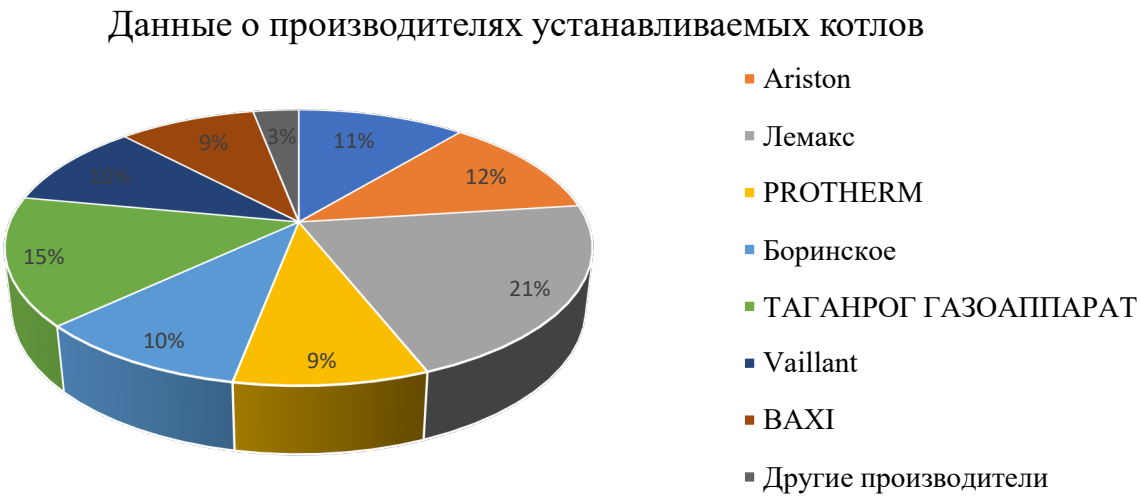


Рис. 4. Диаграмма выбираемых производителей газового оборудования

Производителем, занимающим лидирующее место (21%) стал российский завод Лемакс, что в первую очередь связано в широким ассортиментом предлагаемого к установке оборудования, в том числе не нуждающегося в электропитании, различного ценового сегмента и вариантов установки (настенного и напольного).

За ним с показателем в 15% выступает группа компаний «ТАГАНРОГ ГАЗОАППАРАТ», зарекомендовавшая себя, как производителя бюджетных и долговечных газовых котлов.

Оставшиеся позиции практически наравне разделили отечественные и зарубежные компании, предлагающие сертифицированное газовое оборудование под индивидуальные особенности каждого проекта.

Таким образом, оптимальный выбор бытового газового котла требует комплексного подхода и учета множества факторов, так как выбор зависит от конкретных особенностей и целей потребителя.

Выбирая между котлом с открытой и закрытой камерой сгорания, домовладельцы, проживающие в центральной части нашей страны, предпочтительно (74%) устанавливают – первый, ввиду перечисленных преимуществ и выполнения заданных потребностей.

Литература

1. В 2024 году «Газпром» выделил рекордные средства на развитие газификации и догазификацию регионов России // Газпром URL: https://www.gazprom.ru/press/news/2024/april/article573823 (дата обращения: 02.04.2025).

2. Постановление Правительства Российской Федерации «О внесении изменений в некоторые акты Правительства Российской Федерации» от 16.04.2024 № 484 // Официальный интернет-портал правовой информации. – 2024.

3. Вершилович В.А. Внутридомовое газовое оборудование. - М-Вологда: Инфра-Инженерия, 2017. – 320 с.

4. СП 402.1325800.2018 «Здания жилые Правила проектирования систем газопотребления»: издание официальное приказом Министерства строительства и жилищно-коммунального хозяйства Российской Федерации от 5 декабря 2018 г. № 789/пр: дата введения 06.06.2019. – М.: Минстрой России, 2018. – 32 с.

KOLYBELKINA Irina Nikolaevna
Student, Saint Petersburg State University of Architecture and Civil Engineering,
Russia, Saint Petersburg

OPTIMAL DOMESTIC GAS BOILER SELECTION

Abstract. *The article compares household gas boilers with open and closed combustion chambers, highlights their pros and cons, and examines the types installed in private homes.*

Keywords: *gasification, construction, natural gas, natural gas boiler, individual house, combustion chamber.*

СЕЛЬСКОЕ ХОЗЯЙСТВО

10.5281/zenodo.15192510

БЕЛКИН Андрей Алексеевич
директор, ООО «ВФ» Вольный фермер, Россия, г. Екатеринбург

УНИВЕРСАЛИЗАЦИЯ ОБОРУДОВАНИЯ КАК ФАКТОР УСТОЙЧИВОГО РАЗВИТИЯ МАЛЫХ МОЛОЧНЫХ ПРОИЗВОДСТВ

Аннотация. *Малые молочные хозяйства, особенно в сельских регионах, сталкиваются с проблемами нехватки ресурсов, ограниченности производственных площадей и высокой стоимости оборудования. В условиях ограниченного бюджета для них критически важна возможность гибкой и экономичной переработки молока без ущерба для качества продукции. В статье рассматривается универсализация технологического оборудования как решение, позволяющее повысить устойчивость таких предприятий. На основе авторского опыта создания мини-фермы и разработки совместно с производителем серии универсальных установок обосновываются преимущества компактных многофункциональных решений. Универсализация позволяет существенно сократить площадь цехов, снизить затраты и повысить производственную эффективность. Статья подчеркивает потенциал таких решений для масштабирования и широкого внедрения в агропромышленный сектор.*

Ключевые слова: *малые молочные хозяйства, универсальное оборудование, устойчивое производство, агробизнес, молочная переработка, технологическая оптимизация, фермерские предприятия, сельское хозяйство, многофункциональные установки, снижение себестоимости, локальное производство, инновации в АПК, компактные производственные линии, модернизация пищевой промышленности.*

Введение

Малые фермерские хозяйства играют важную роль в обеспечении продовольственной безопасности и развитии сельских территорий. Однако на фоне доминирования крупных агрохолдингов они сталкиваются с рядом системных ограничений: дефицит инвестиций, недостаток кадров, сложность доступа к современным технологиям. Особенно остро эти проблемы проявляются в молочной переработке, где даже базовая линия требует значительных затрат на закупку оборудования и организацию производственных помещений.

Традиционные технологические решения ориентированы, как правило, на средние и крупные предприятия. Специализированное оборудование занимает большие площади, требует высокой квалификации персонала и часто не адаптировано под переменные объёмы переработки. В результате малые производители оказываются в невыгодных условиях и теряют возможность конкурировать за счёт качества.

В данной статье рассматривается альтернативный подход – универсализация оборудования. На примере работы мини-фермы, построенной «с нуля», демонстрируется, как создание и внедрение многофункциональных агрегатов позволяет преодолеть ключевые ограничения малого бизнеса и обеспечить устойчивую модель молочной переработки с минимальными ресурсами.

Проблематика традиционного подхода к оснащению молочных производств

Оснащение молочного производства традиционно предполагает поэтапную организацию технологического цикла с использованием специализированного оборудования для каждого процесса: сепарации, пастеризации, охлаждения, гомогенизации, ферментации, розлива и пр. Такое оборудование разрабатывается и поставляется в расчёте на определённые объёмы переработки, стандартные условия и наличие

производственных площадей. Однако малые фермерские хозяйства часто не соответствуют этим параметрам.

Во-первых, пространственные ограничения не позволяют разместить все необходимые машины. Даже компактная линия в классическом исполнении требует 60–100 квадратных метров, что зачастую невозможно для небольших помещений в сельской местности.

Во-вторых, стоимость закупки полного комплекта оборудования часто превышает бюджет малых фермеров. Это приводит либо к недооснащению производства, либо к попыткам работать на устаревшем или б/у оборудовании, что снижает стабильность качества и увеличивает затраты на обслуживание.

В-третьих, ограниченные кадровые ресурсы делают затруднительным обслуживание сложной техники. Специализированные машины требуют соответствующей квалификации, которую сложно найти или подготовить на местах.

Кроме того, традиционные линии, как правило, плохо приспособлены к гибкому производству. В условиях малых партий и нестабильного объема сырья оборудование либо простаивает, либо работает с перегрузкой, что сказывается на его ресурсе и экономике производства [1, с. 163].

Таким образом, традиционный подход к оснащению молочных производств становится барьером для устойчивого развития малых предприятий. Это формирует объективный запрос на новое поколение оборудования – универсального, компактного, многофункционального, простого в эксплуатации и обслуживании.

Разработка и внедрение универсального оборудования: практический кейс мини-фермы

В условиях описанных ограничений было принято решение о создании собственной мини-фермы с перерабатывающим цехом, полностью адаптированным под реалии малого бизнеса. Одним из ключевых факторов успеха стало решение отказаться от традиционного набора оборудования в пользу разработки универсальных агрегатов, способных выполнять сразу несколько технологических операций.

Проектирование оборудования велось совместно с инженерной компанией, специализирующейся на производстве техники для молочной промышленности. При этом в основу легли следующие **принципы**:

- **Многофункциональность**: одна установка должна выполнять несколько этапов – например, нагрев, пастеризацию, охлаждение и перемешивание;
- **Компактность**: оборудование должно занимать минимум места, позволяя существенно сократить площадь цеха;
- **Простота эксплуатации**: управление должно быть интуитивно понятным, без необходимости привлечения узкопрофильных специалистов;
- **Лёгкость в обслуживании и очистке**: агрегаты должны быстро разбираться и дезинфицироваться, соответствуя санитарным требованиям;
- **Гибкость в работе с разными продуктами**: оборудование должно быть адаптировано к производству различных типов молочной продукции – от пастеризованного молока до йогурта и сливок.

В результате были созданы **универсальные станции**, каждая из которых объединяла в себе функции сразу нескольких специализированных машин. Благодаря этому удалось:

- сократить количество оборудования более чем в два раза;
- уменьшить площадь производственного цеха почти вдвое;
- снизить энергопотребление и затраты на обслуживание;
- организовать переработку молока с минимальным количеством персонала;
- обеспечить стабильное качество продукции, соответствующее нормативным требованиям [2, с. 599].

Особое внимание при разработке уделялось модульному принципу: каждая установка могла быть легко дооснащена или интегрирована с другими в рамках увеличения производительности или расширения ассортимента. Это делает модель пригодной как для старта, так и для масштабирования бизнеса без необходимости полной модернизации цеха.

Опыт внедрения подтвердил эффективность универсализации оборудования как технологического решения для малого молочного бизнеса. Более того, он стал основой для формирования целостной производственной модели, в которой минимальные ресурсы обеспечивают устойчивый и предсказуемый результат.

Устойчивость как результат технологической оптимизации

Внедрение универсального оборудования оказало комплексное влияние на устойчивость производства – как в экономическом, так и в экологическом и социальном измерениях. Такой подход стал не просто технологическим решением, а стратегией, обеспечивающей выживаемость и развитие малого агробизнеса [3, с. 18].

Экономическая устойчивость

Универсализация оборудования позволила добиться существенного снижения издержек:

- **Сократились капитальные вложения** – одно многофункциональное устройство заменило несколько узкоспециализированных машин.
- **Уменьшились операционные затраты** – за счёт компактности оборудования снизились расходы на электроэнергию, вентиляцию, водоснабжение и обслуживание.
- **Оптимизировался фонд оплаты труда** – благодаря простоте управления и автоматизации уменьшилась потребность в высококвалифицированном персонале.
- **Снизилась себестоимость продукции**, что позволило удерживать конкурентные цены на рынке и обеспечивать рентабельность даже при небольших объёмах.

В условиях, когда малые предприятия зачастую работают с нестабильной финансовой моделью, такие изменения оказываются критическими для выживания и масштабирования бизнеса.

Экологическая устойчивость

Меньшее количество оборудования и компактность производственных линий способствуют:

- снижению потребления ресурсов (энергии, воды, моющих средств);
- уменьшению количества отходов и выбросов;
- более рациональному использованию помещений и строительных материалов.

Кроме того, технологическая универсальность уменьшает потребность в обновлении и утилизации оборудования при смене ассортимента продукции – достаточно перенастроить существующие модули [4].

Социальная устойчивость

Проект оказался значим не только для бизнеса, но и для местного сообщества. Он создал:

- новые **рабочие места в сельской местности**;
- возможность **самореализации и предпринимательства** в аграрной сфере;
- **доступ населения к качественной натуральной продукции**, произведённой без применения консервантов и усилителей вкуса.

Дополнительно универсальность оборудования снизила порог входа в отрасль для начинающих фермеров и семейных хозяйств, поскольку сняла необходимость в серьёзной технической подготовке и крупных стартовых инвестициях.

Таким образом, универсализация оборудования выступает не просто как техническая мера, а как полноценный инструмент формирования устойчивых производственных систем, способных адаптироваться к экономическим, экологическим и социальным вызовам.

Заключение

Опыт разработки и внедрения универсального оборудования на малой ферме показал, что технологическая универсализация способна радикально изменить подход к организации молочного производства в малом и среднем бизнесе. За счёт объединения нескольких функций в одном агрегате удалось:

- сократить производственные площади и затраты;
- повысить гибкость переработки молока;
- обеспечить выпуск качественной продукции при минимальных ресурсах;
- создать устойчивую модель, не зависящую от внешних колебаний и больших объёмов производства.

Это подтверждает: универсальное оборудование может быть не просто решением частных задач, а фундаментом для новой парадигмы молочной переработки – адаптированной к реалиям локального производства, потребностей сельских территорий и тенденций устойчивого развития.

Потенциал масштабирования данной модели очевиден. Она может быть:

- внедрена в рамках программ **поддержки сельхозкооперации**;
- использована в **образовательных проектах** для подготовки фермеров;
- адаптирована для **контейнерных модульных цехов**, включая мобильные комплексы;
- рекомендована как база для **социальных и экспортных агропроектов**.

С учётом глобального тренда на экологичность, локальность и натуральность продуктов

питания, универсализация оборудования становится не просто технологическим выбором, а стратегическим направлением развития устойчивого агробизнеса.

Литература

1. Рябова А.Е., Пряничникова Н.С., Хуршудян С.А. Молочная промышленность России: реалии в историческом контексте. – М.: ВНИМИ, 2022. – 163 с.

2. Шаршунов В.А. Технологическое оборудование молокоперерабатывающих предприятий: учебное пособие. – Минск: Мисанта, 2011. – 599 с.

3. Улитенко А.И., Пушкин В.А. Энергосберегающая технология первичной обработки молока // Аграрная наука. – 2003. – № 7. – С. 18-20.

4. Рыжово (агропредприятие) [Электронный ресурс] // Википедия – свободная энциклопедия. URL: https://ru.wikipedia.org/wiki/Рыжово_(агропредприятие) (дата обращения: 10.04.2025).

BELKIN Andrey Alekseevich
Director, LLC "VF" Volnyy Fermer, Russia, Yekaterinburg

UNIVERSALIZATION OF EQUIPMENT AS A FACTOR OF SUSTAINABLE DEVELOPMENT FOR SMALL-SCALE DAIRY ENTERPRISES

Abstract. *Small-scale dairy farms, particularly in rural areas, face challenges such as limited resources, restricted production space, and the high cost of equipment. Under constrained budgets, the ability to process milk flexibly and cost-effectively without compromising product quality becomes critical. This article explores the universalization of technological equipment as a solution that enhances the sustainability of such enterprises. Based on the author's experience in creating a mini-farm and collaborating with an equipment manufacturer to develop a series of universal installations, the paper demonstrates the advantages of compact multifunctional solutions. Universalization significantly reduces the required production area, cuts costs, and improves operational efficiency. The article highlights the potential for scaling and widespread implementation of such solutions in the agro-industrial sector.*

Keywords: *small-scale dairy farms, universal equipment, sustainable production, agribusiness, milk processing, technological optimization, farming enterprises, agriculture, multifunctional units, cost reduction, local production, agro-industrial innovation, compact production lines, modernization of the food industry.*

ФИЛОЛОГИЯ, ИНОСТРАННЫЕ ЯЗЫКИ, ЖУРНАЛИСТИКА

ИКРАМОВА Масъуда Тоджидиновна
к.ф.н., доцент кафедры фонетики и лексикологии английского языка,
Худжандский государственный университет имени академика Б. Гафурова,
Республика Таджикистан, г. Худжанд

КУРБОНОВА Парвина Содиковна
магистр первого курса,
Худжандский государственный университет имени академика Б. Гафурова,
Республика Таджикистан, г. Худжанд

КЛАССИФИКАЦИЯ ОМОНИМОВ В АНГЛИЙСКОМ ЯЗЫКЕ

Аннотация. *Статья посвящена омонимам и их классификации в английском языке. Следует отметить, что в современной лингвистике они классифицируются на основе определённых критериев.*

Ключевые слова: *омонимы, классификация, современная лингвистика, абсолютные и неабсолютные омонимы.*

Дар системаи луғавии забони англисӣ, аз он ҷумла дар системаи суффиксҳои он, ҳодисаи омонимия васеъ ба назар мерасад, ки барои омӯзандагони забон муаммоҳои зиёд пеш меорад. Дар рафти омӯзиши забонҳо, инчунин забони англисӣ, омӯзандагон ба мушкилиҳое бармехӯранд, ки яке аз сабабҳои паҳнгашта маъноҳои гуногунро ифода кардани як шакли забонӣ мебошад. Чунин ҳодисаи забон дарк намудани матну маълумотҳоро ба забони хориҷӣ хеле мушкил месозад. Омӯзиши омонимҳоро талаботҳои забоншиносии амалӣ низ водор менамояд, барои он ки оминимҳо дар ҷараёни муошират ҳам ба шунаванда ва ҳам ба гӯянда монеъаҳои муайян ба миён меоранд. Бисёрии вақт дар ҷараёни муошират шунаванда, аз сабаби он ки як шакли забон метавонад маъноҳои гуногунро ифода кунад, барои интихоби дурусти маъно ва дуруст дарк намудани фикри гӯянда ба ҳолати ногувор дучор мешавад. Дар ҳолати изҳори фикр бошад, гӯянда кӯшиш ба харҷ медиҳад, ки ӯро аниқу дуруст фаҳманд.

Инчунин ҳодисаи омонимия барои азхудкунии матнҳои забони хориҷӣ, корҳои лексикографӣ – барои муайян намудани меъёрҳо байни калимаҳо, барои коркарди роҳҳои нишон додани омонимҳо дар луғатҳо ва монанди инҳо, мушкилиҳо пеш меорад. Дар байни олимони забоншинос оид ба таснифоти омонимҳо баҳсу мунозира қариб дида нашавад ҳам, нисбат ба ин масъала нуқтаҳои назари гуногун дида мешавад. Дар забоншиносии муосир омонимҳо дар асоси ин ё он меъёрҳо тасниф карда шудаанд. Дар мақолаи мазкур таснифи омонимҳо дар забони англисӣ дида баромада шудааст.

Дар луғати истилоҳии забоншиносӣ хелҳои асосии омонимҳо қайд шудааст:

- омонимҳои мутлақ (комил);
- омонимҳои номутлақ;
- омонимҳои содда;
- омонимҳои сохта;
- омофонҳо;
- омографҳо;
- омоформҳо [4, с. 148].

Забоншиноси англис Ҷон Лайонз таснифоти монандро пешниҳод намудааст, ки дар он ӯ омонимҳои мутлақро абсолютӣ меномад. Ҷон Лайонз се шартро муайян намудааст, ки аз рӯи он омонимҳо ба гурӯҳи мутлақ, чи хеле ки ӯ

мегӯяд, абсолютӣ, дохил карда мешаванд [3, с. 292]:

- онҳо бояд аз ҷиҳати маъно ба якдигар алоқамандӣ надошта бошанд;
- ҳамаи шаклҳои онҳо (шаклҳои хаттӣ, овозӣ) мувофиқат кунанд;
- шаклҳои якхела аз ҷиҳати грамматикӣ эквивалентӣ бошанд [3, с. 294].

Аз рӯи нуқтаи назари Ҷон Лайонз, агар омонимҳо аз рӯи як ё ду шарти додашуда мувофиқат кунанд, онҳо омонимҳои номутлақанд [3, 294].

Бояд қайд кард, ки дар забоншиносии муосир мафҳуми омонимҳои байнизабонӣ ва паронимҳо низ ба назар мерасад. Масалан: калимаи **magazine** (маҷалла) - дар забони русӣ **мағоза.** Омонимҳои байнизабонӣ, аз сабаби он ки ҳодисаи тасодуфианд, дар забонҳо кам дида мешаванд.

Дар забоншиносии муосир олимон дар тадқиқи омонимҳо бештар ба таснифоти А.И. Смирнидский [5] ва И.В. Арнолд [1] такя мекунанд. Дар таснифоти онҳо ҳамаи масъалаҳои ин ё он шакли омонимҳо муфассал дида баромада шудааст.

Забоншинос А.И. Смирнидский омонимҳоро ба ду гурӯҳи калон ҷудо мекунад [5, с. 69]:

- омонимҳои мутлақ;
- омонимҳои номутлақ.

Аз рӯи нуқтаи назари А.И. Смирнидский, омонимҳои мутлақ чунин таъриф дода шудаанд: “Омонимҳои мутлақ – ин калимаҳое мебошанд, ки ба як ҳиссаи нутқ тааллуқ дошта, дорои парадигмаҳои якхелаанд (масалан, match – mach)” [5, с. 69].

Дар навбати худ А.И. Смирнидский омонимҳои номутлақро ба се гуруҳ тақсим мекунад:

1) омонимҳои соддаи лексико-грамматикӣ (як ҳиссаи нутқ, ки парадигмаҳояш як шакл доранд, яъне ҳамшакланд): to found – found;

2) омонимҳои мураккаби лексико-грамматикӣ (воҳидҳои ба ҳиссаҳои гуногуни нутқ тааллуқдошта, ки дар парадигмаҳояшон як шакл доранд, яъне ҳамшакланд): maid – made; bean – been;

3) омонимҳои лексикӣ (калимаҳои ба як ҳиссаи нутқ тааллуқдошта, ки фақат дар шакли аввала мувофиқат мекунанд): to can – can [5, с. 75].

Олими дигари рус И.В. Арнолд бошад ҳамаи омонимҳоро ба се гурӯҳи калон ҷудо мекунад:

- омонимҳо;
- омофонҳо;
- омографҳо.

Барои таснифоти пурраву муфассали омонимҳо И.В. Арнолд 12 гурӯҳи омонимҳоро пешниҳод намудааст:

- омонимҳои номутлақ, ки шакли аввалаи якхела, лекин парадигмаҳои гуногун доранд (light исм, равшанӣ - light сифат, сабук);
- омонимҳои номутлақ, ки шакли аввала не, балки шаклҳои алоҳидаашон мувофиқат мекунад (might исм, қувват – might феъл, шакли замони гузаштаи феъли may);
- калимаҳое, ки ба як ҳиссаи нутқ тааллуқ доранд, шакли аввалаашон гуногунанд, лекин дар ягон дигар шакл мувофиқат мекунанд (axe-axes, axis – axes);
- калимаҳое, ки аз ҷиҳати маънои лексикӣ ва грамматикӣ гуногун мебошанд. Ин асосан калимаҳое мебошанд, ки парадигма надоранд, ва ба қатори калимаҳои тағирнаёбандаи ёрирасон дохил мешаванд (for пешоянд – for пайвандак);
- маъноҳои гуногуни лексикӣ бо шаклҳои авалаи якхела, маъноҳои грамматикии якхела бо парадигмаҳои гуногун (lay – lain, lie – lied - lied);
- калимаҳое, ки ба як ҳиссаи нутқ таааллуқ доранд, лекин маъноҳои лексикиашон гуногунанд (spring – ҷаҳиш, spring – чашма, spring – баҳор);
- мавҷуд будани ҷузъи умумӣ дар маънои лекликӣ (before – пешоянд, before – зарф, before – пайвандак);
- ҷуфти калимаҳое, ки монандии хело наздик дошта, ҳамчун вариантҳои калимаи сермаъно дида мешаванд;
- омонимҳои бо роҳи конверсия сохташуда (eye – исм; eye – феъл);
- калимаҳои ба ҳиссаҳои нутқи гуногун тааллуқдошта, ки монандии онҳо дар асоси реша дида мешавад (thought – исм; thought – феъл);
- монандии маъноҳои лексикӣ ва грамматикӣ, ки дорои шаклҳои гуногун мебошанд [1, с. 56].

Баъзе олимони забоншинос паронимҳоро (калимаҳои талаффузашон наздик) ба қатори омонимҳо дохил мекунанд, лекин бо вуҷуди хеле наздик будан паронимҳо аз омоним фарқ доранд. Агар омонимҳо аз ҷиҳати талаффуз пурра мувофиқат кунанд, паронимҳо мувофиқати овозии нопурра доранд [2, с. 152].

Хулоса, дар забоншиносии муосир асосан ду намуди омонимҳо шинохта мешаванд: мутлақ, ки дар ин ҳолат шаклҳо аз ҳама ҷиҳат пурра мувофиқат мекунанд, ва номутлақ, дар ҳолате ки шаклҳо фақат аз ягон ҷиҳат мувофиқат доранд, яъне пурра мувофиқат намекунанд.

Адабиёт

1. Арнольд И. В. Лексикология современного английского языка. – 3-е изд., перераб. и доп. – М.: Высшая школа, 1986. – 295 с.
2. Каращук П. М. Аффиксальное словообразование в английском языке. М., 1965. – 173 с.
3. Лайонз Дж. Введение в теоретическую лингвистику. – М.: Прогресс, 1978. – 540 с.
4. Маҷидов Х. Забони адабии муосири тоҷик. Ҷ.1. Луғатшиносӣ. Душанбе. Деваштич, 2007. – 244 с.
5. Смирницкий А. И. Лексикология английского языка. – М.: Московский Государственный Университет, 1998. – 260 с.
6. Ахманова О. С. Словарь лингвистических терминов. – М.: Советская энциклопедия, 2010. – 576 с.
7. Лингвистический энциклопедический словарь / Гл. ред. В. И. Ярцева. – М. 6 Сов. Энциклопедия, 1990. – 685 с.

IKRAMOVA Masuda Tojidinovna
Candidate of Philological Sciences,
Associate Professor of the Department of Phonetics and Lexicology of the English Language,
Khujand State University named after academician B. Gafurov,
Republic of Tajikistan, Khujand

KURBONOVA Parvina Sodikovna
Master's Student,
Khujand State University named after academician B. Gafurov,
Republic of Tajikistan, Khujand

CLASSIFICATION OF HOMONYMS IN ENGLISH

Abstract. *The article is devoted to homonyms and their classification in the English language. It should be noted that in modern linguistics homonyms are classified based on certain criteria.*

Keywords: *homonyms, classification, modern linguistics, absolute and non-absolute homonyms.*

СОЦИОЛОГИЯ

БОГДАНОВА Екатерина Геннадьевна
студентка, Тихоокеанский государственный университет, Россия, г. Хабаровск

СОЦИАЛЬНАЯ АДАПТАЦИЯ ВОЕННОСЛУЖАЩИХ ОФИЦЕРСКОГО СОСТАВА, УВОЛЕННЫХ В ЗАПАС

Аннотация. *Данная статья посвящена рассмотрению социальных проблем, возникающих у военнослужащих офицерского состава после увольнения в запас на адаптационном этапе, их изучению и предполагаемым путям разрешения. Также обращено внимание на особые ценностные системы, мышление и поведение военных, выработанные за годы службы и влияющие на ресоциализацию. Анализируются жизненные планы офицеров, уволенных в запасах, и их реализация.*

Ключевые слова: *социальная помощь, военные, военнослужащие, бывшие военнослужащие, офицеры, бывшая военная служба, социальная адаптация, социальные проблемы, общество.*

После начала Специальной Военной Операции в 2022 году увольнение военных было приостановлено. Однако рассматриваемая тема была актуальной до СВО и будет такой являться после ее окончания. Оглянувшись на историю нашей страны, в которой быть офицером всегда считалось почетным, и сравнивая нынешние поколения, можно сделать вывод, что статус военнослужащих и престиж армии значительно упал. На это есть множество причин, но для нас представляют интерес вызывающие социальную дезадаптацию проблемы, с которыми сталкиваются военнослужащие после ухода со службы.

Увольнение офицеров из ВС РФ имеет отрицательный окрас в первую очередь из-за отсутствия гражданских специальностей и опыта работы в них. Работая годами в одной сфере и выполняя день за днем задачи и поручения определенного характера, военнослужащие в большинстве вырабатывают в себе совершенно иное мышление и поведение. Процесс ресоциализации офицеров, уволенных в запас, важен не только для каждого из них, но и для социума в целом. Обществу необходима стабильность и укрепление социальных структур. Успешно интегрированные в гражданскую жизнь бывшие военнослужащие могут привнести вклад в развитие страны с еще неизведанной для них экономической ниши.

Адаптация военнослужащих офицерского состава, уволенных в запас – это сложный комплекс новообразований, включающих в себя познание неведанных ранее социальных ролей, изменение ощущения себя и своего окружения, преобразование личности во всех сферах [5, с. 1-11].

Согласно результатам исследования Щипакова В. Э., основными трудностями, с которыми сталкиваются уволенные в запас офицеры, являются трудоустройство и профессиональный рост, первоочередно связанные с качеством программ обучения и переподготовки [1, с. 23-31]. В целом данные программы оцениваются положительно экспертами ресоциализации, однако при этом же ими подчеркивается необходимость их улучшения в некоторых особо важных аспектах – повышении качества образовательных программ, улучшении механизмов трудоустройства, обеспечении жильем и увеличении финансовой поддержки [1, с. 23-31; 4, с. 120-132].

Профессиональная адаптация военнослужащих состоит из ряда компонентов, каждый из которых представляет определенное направление. Так, можно выделить четыре основных: образовательный (приобретение новых необходимых знаний по выбранной специальности), психологический (внутреннее принятие новой неизвестной профессии), физический (возможности здоровья уволенного) и трудовой

(непосредственная деятельность бывшего военнослужащего в рамках выбранной им новой профессии) аспекты [2, с. 153-158].

Здесь большое влияние должны оказывать региональные меры поддержки и общественные программы. Так местными органами разрабатываются и реализуются проекты оказания помощи в сферах здравоохранения, образования трудоустройства и социальной поддержки [1, с. 23-31]. Такие программы направлены не в частности на офицеров в запасе, но в принципе на уязвимые группы населения, нуждающиеся в ресурсах для положительной адаптации в социуме. В основу адаптации трудовой занятости бывших военнослужащих могут быть положены уже многим знакомые организации содействия трудоустройству выпускников образовательных организаций, когда центры трудоустройства «передают в руки» бывших студентов потенциальным работодателям [4, с. 120-132]. Такой же механизм может быть применен в каждом субъекте РФ при взаимодействии Министерства обороны и региональных властей к уволенным в запас офицерам.

Стоит уделить также внимание повышению информированности о правах, существующих возможностях социальной поддержки и профессиональной переподготовки среди военнослужащих, так как многие не могут воспользоваться помощью в силу того, что просто не знают о ее существовании. Необходимая информация должна распространяться через доступные источники информации с подачи региональных структур власти.

Несмотря на поддержку со стороны государства, в большей степени на успешность ресоциализации бывший военнослужащих влияет внутренняя мотивация – психологический аспект – поддержка со стороны семьи, друзей, родственников и т. д. Перед офицерами стоит задача преодоления психологических и культурных барьеров, связанных с переходом к гражданской жизни. Именно поэтому также государственным структурам стоит обратить большее внимание социально-психологическому состоянию военнослужащих – психологическая подготовка перед увольнением и после как самим офицерам, так и членам их семей, интеграция в профессиональные сообщества и кружки по интересам и пр. [3, с. 159-165].

Так, например, С. Л. Косик предлагает за 1-2 года до возможного ухода со службы начинать проводить ознакомительные тренинги-семинары, посвященные ознакомлению с нынешним рынком труда, а также тактике поведения при поиске новой работы. При этом устраивать психодиагностику с целью выявления существующих внутренних барьеров при будущей смене места работы и профессии [5, с. 1-11]. Такой период, по мнению автора научных статей, мог бы облегчить военнослужащим процесс увольнения и первое время после него.

По мнению Т. А. Чертушкиной, «развитие социальной работы и пенсионного обеспечения военнослужащих, уволенных в запас, и членов их семей непосредственно взаимосвязано с развитием вооруженных сил в стране, состоянием ее экономики, уровнем национального дохода и повышением материального благосостояния людей» [6, с. 129-135].

Первоочередным программным документом социального планирования, на который опиралось Министерство обороны РФ в вопросе социальной адаптации, являлась Стратегия социального развития Вооруженных Сил Российской Федерации на период до 2020 г. [7]. В данном документе от 28.03.2008 г. прописана система мер долгосрочного характера, основная цель которых – улучшение военно-социальной сферы в различных направлениях. Образование, медицина, культура, спорт, социально-бытовые условия, заработная плата, пенсия, денежное довольствие и социальная защита – те сферы, которые охватывает Стратегия социального развития.

Военнослужащие офицерского состава, уволенные в запас – вынесены в данном документы как отдельная социальная группа с соответствующими для них мероприятиями. Там прописаны такие меры по оказанию содействия в получении профессиональных навыков по гражданской специальности: развитие регионального комплекса военно-учебных центров; создание сети подготовительных центров при образовательных учреждениях высшего профессионального образования; переподготовка военнослужащих по гражданским специальностям в период прохождения военной службы по призыву [6, с. 129-135]. На официальном сайте Министерства обороны Российской Федерации можно ознакомиться с итогами социального развития ВС РФ в 2024 г. В относительно небольшой презентации, охватывающий целый год, освящены итоги во всех сферах

– финансовое и жилищное обеспечение, образование, медицинское обеспечение, культурно-досуговое обслуживание, движение «ЮНАРМИЯ» и электронная приемная [8]. На данный момент итоги по работе с изучаемой социальной группой отсутствуют в силу того, что действует указ Президента РФ от 21.09.2022 № 647 «Об объявлении частичной мобилизации в Российской Федерации», фактически означающий, что все контракты продолжают действовать [9]. В настоящее время фокус смещен на оказание социальной помощи участникам СВО и их семьям. Однако, после окончания Специальной военной операции и отмены вышеупомянутого указа, изучаемая мною тема приобретет еще большую актуальность.

Социальная защита военнослужащих исторически складывалась как важнейшая система и элемент государственной политики, так как она непосредственно влияет на экономическую и социальную структуры страны. Военнослужащие офицерского состава, уволенные в запас, являются не только особой социальной группой, но и значимым трудовым ресурсом, который в умелых государственных руках сможет дважды послужить своему отечеству.

Из рассмотренного, можно сделать вывод, что в первую очередь государственным властям необходимо улучшить программы профессиональной переподготовки, оказать более значительную финансовую, жилищную поддержку, изменить подход к организационной помощи и донесению важной информации, связанной с правами и возможностями бывших военнослужащих. Также стоит обратить особое внимание развитию социальных и психологических программ, способных поднять моральный дух среди ушедших со службы офицеров. Отдав значительную часть своей жизни служению Родине, военный пенсионер заслуживает особого внимания со стороны государства.

Литература

1. Щипаков В.Э. Основные направления оптимизации процесса ресоциализации российских офицеров, уволенных в запас // Общество: социология, психология, педагогика. 2024. № 7. С. 23-31. (дата обращения: 01.04.2025).

2. Вольф К.В., Геронтьев Е.А. Современные аспекты профессиональной адаптации военнослужащих, увольняемых в запас // Власть. 2024. № 1. С. 153-158. (дата обращения: 03.04.2025).

3. Деникина З.Д., Дроконова К.Е. Особенности социально-психологического состояния военнослужащих в процессе увольнения в запас // Власть. 2024. № 1. С. 159-165. (дата обращения: 03.04.2025).

4. Монахов О.Н. Профессиональная адаптация военных пенсионеров: инклюзивный подход // Профессиональное образование и рынок труда. 2024. Т. 12. № 2. С. 120-132.

5. Бессонова Т.И. Психологическая адаптация военных пенсионеров к новым видам деятельности // Ученые записки. Электронный научный журнал Курского государственного университета. 2023. № 2 (66). С. 1-11.

6. Евенко С.Л., Попов И.А. Государственные стратегии управления рисками социальной адаптации российских военнослужащих, уволенных в запас // Власть. 2020. № 3. С. 129-135.

7. Стратегия социального развития Вооруженных Сил Российской Федерации до 2020 года [Электронный ресурс] // Информационно-правовое обеспечение ГАРАНТ. URL: https://base.garant.ru/406030733/ (дата обращения: 07.04.2025).

8. Социальное развитие ВС РФ в 2024 году [Электронный ресурс] // Министерство обороны Российской Федерации (Минобороны России): офиц. сайт. URL: https://sc.mil.ru/social/itogi.htm (дата обращения: 07.04.2025).

9. Теперь получается контрактник уволиться не сможет? [Электронный ресурс] // Pravoved. URL: https://pravoved.ru/question/3475209/ (дата обращения: 07.04.2025).

BOGDANOVA Ekaterina Gennadevna
Student, Pacific State University, Russia, Khabarovsk

SOCIAL ADAPTATION OF RETIRED MILITARY OFFICERS

Abstract. *This article is devoted to the consideration of social problems that arise among military officers after their discharge into the reserve at the adaptation stage, their study and proposed solutions. Attention is also drawn to the special value systems, thinking and behavior of the military, developed over the years of service and influencing resocialization. The life plans of officers discharged from the reserves and their implementation are analyzed.*

Keywords: *social assistance, military, military personnel, former military personnel, officers, former military service, social adaptation, social problems, society.*

Актуальные исследования

Международный научный журнал
2025 • № 14 (249)
Часть I

ISSN 2713-1513

Подготовка оригинал-макета: Орлова М.Г.
Подготовка обложки: Ткачева Е.П.

Учредитель и издатель: ООО «Агентство перспективных научных исследований»
Адрес редакции: 308000, г. Белгород, пр-т Б. Хмельницкого, 135
Email: info@apni.ru
Сайт: https://apni.ru/

Отпечатано в ООО «ЭПИЦЕНТР».
Номер подписан в печать 14.04.2025г. Формат 60×90/8. Тираж 500 экз. Цена свободная.
308010, г. Белгород, пр-т Б. Хмельницкого, 135, офис 40