REDS:

Телекоммуникационные устройства и системы

№1

2025

СОДЕРЖАНИЕ

О ВКЛАДЕ АКАДЕМИКА И.А. МИЗИНА В РЕШЕНИЕ ОСНОВНЫХ ПРОБЛЕМ РАЗВИТИЯ ИНФОРМАЦИОННОГО ОБЩЕСТВА

Зацаринный Александр Алексеевич
Федеральный исследовательский центр "Информатика и управление" РАН, главный научный сотрудник, доктор технических наук, Москва, Россия.
alex250451@mail.ru

Колин Константин Константинович
Федеральный исследовательский центр "Информатика и управление" РАН, главный научный сотрудник, доктор технических наук, Москва, Россия.
kolinkk@mail.ru

Аннотация
Рассмотрены современные проблемы развития информационного общества в России и показан вклад в их решение академика И.А. Мизина, в 1989-1999 гг. директора Института проблем информатики РАН. В этот период концепция создания глобального информационного общества находилась в начальной стадии формирования. При этом Россия находилась в условиях отсутствия собственной технологической базы. Поставленные И.А. Мизиным основные проблемы развития информационного общества в России и предложенная им концепция решения этих проблем оказали существенное влияние на развитие процессов информатизации общества и в целом сохраняют актуальность в настоящее время. В статье также приведены приоритетные задачи развития информационного общества в России, которые необходимо решать в сложных современных условиях.

Ключевые слова
Информатизация общества, информационная инфраструктура, искусственный интеллект, средства информатизации, ситуационные центры, телекоммуникационные технологии

Введение

Процесс становления глобального информационного общества является одной из наиболее важных тенденций развития мировой цивилизации в XXI веке. Сегодня этот процесс охватывает все страны мира, включая Россию, и коренным образом изменяет многие стереотипы жизнедеятельности общества. Однако, по прогнозам системных аналитиков, еще более глубокие перемены нас ожидают впереди. При этом революционным фактором здесь будет процесс цифровой трансформации общества, основанный на все более широком использовании средств и методов искусственного интеллекта.

Уже в настоящее время уровень развития информационного общества в той или иной стране в значительной мере определяет конкурентоспособность ее экономики, качество жизни населения, а также положение этой страны в мировом сообществе. Поэтому в новой стратегии развития России этой проблематике уделяется особое внимание, которое находит свое отражение в содержании и приоритетах задач комплекса новых национальных проектов [1].

Приоритетными задачами развития информационного общества в России в настоящее время являются [1, 19-23]:

– комплексное развитие информационной инфраструктуры на всей территории страны, включая районы Сибири, Дальнего Востока и Крайнего Севера;

– создание современной отечественной технологической базы информационного общества, которая должна обеспечить переход экономики страны к шестому технологическому укладу;

– подготовка необходимого количества специалистов в области современных информационных и коммуникационных технологий;

– научное просвещение общества и формирование новой информационной культуры, адекватной новым условиям жизнедеятельности в глобальном информационном обществе.

Стратегическая значимость этих проблем начала осознаваться в нашей стране еще в период двух последних десятилетий XX века, когда формировались концептуальные основы построения глобального информационного общества. Важный вклад в формирование этих основ внес академик Мизин Игорь Александрович, который в период 1989-1999 гг. был директором Института проблем информатики РАН (ИПИ РАН). 12 апреля 2025 г. исполняется 90 лет со дня рождения этого выдающегося ученого и конструктора сложных систем оборонного назначения [2]. Авторам настоящей статьи довелось

длительное время сотрудничать с ним в области создания этих систем, а полученный при этом опыт они используют в своей деятельности и в настоящее время.

Формирование концептуальных основ развития телекоммуникационных технологий в России

Исследования показывают, что ключевым фактором развития информационного общества являются телекоммуникационные технологии, которые в последние годы проникают во все сферы жизнедеятельности общества. Их становление в России началось в период 90-х годов XX века, а концептуальные основы этого процесса были разработаны в ИПИ РАН под руководством академика И.А. Мизина. Представление о сложности и масштабах этой проблемы дает содержание его статей, опубликованных в 1998 и 1999 годах [3, 4]. В них проведен анализ основных проектов создания международной информационной инфраструктуры, разработанных в США и странах Западной Европы, а также различных методов и технологий передачи данных по каналам связи в телекоммуникационных сетях. При этом для каждого из них определена область применения и возможности использования в интересах формирования информационной инфраструктуры России. Особое внимание было уделено проблематике создания распределенных телекоммуникационных сетей, которые необходимы для нашей страны, обладающей огромной по протяженности территорией. В этих работах проведен также системный анализ состояния и перспектив развития международной сети Интернет.

И.А. Мизин обладал большим опытом проектирования и ввода в эксплуатацию высоконадежных информационно-телекоммуникационных систем оборонного назначения и использовал этот опыт при разработке концептуальных основ создания таких систем в интересах развития информационного общества. Эти же принципы положены, например, в основу построения Системы распределенных ситуационных центров России, которая в ближайшие годы должна обеспечивать информационно-аналитическую поддержку деятельности органов государственного управления нашей страны на федеральном и региональном уровнях [5, 6].

Проблемы создания технологической базы информационного общества в России

Для формирования информационного общества необходима принципиально новая технологическая база. Ее основу составляют средства вычислительной техники и связи массового применения, прежде всего мобильной. Они должны быть надежными и удобными для практического использования людьми, не обладающими специальной подготовкой, а также доступными по цене. В настоящее время такие средства имеются во многих странах, а их пользователями становятся даже дети дошкольного возраста и пожилые люди. Для современной России актуальная проблема здесь заключается в том, чтобы обеспечить замещение доминирующих сегодня импортных средств информатизации отечественными разработками мирового уровня. А это требует не только организации таких разработок, но и создания собственного промышленного производства электронно-компонентной базы. Концептуальные основы такой национальной стратегии были разработаны в Российской академии наук в середине 90-х годов XX века и остаются актуальными в настоящее время.

И.А. Мизин активно участвовал в формировании этой стратегии, основные положения которой представлены в фундаментальной статье, подготовленной совместно с одним из ведущих ученых ИПИ РАН А.В. Филиным [7]. На основе аналитического обзора различных подходов к формированию концептуальных основ создания компьютерной техники нового в статье сформулирован главный принцип отечественной стратегии – *опережающее развитие на основе использования интеллектуального потенциала России.* Этот принцип сохраняет свою актуальность и в настоящее время, когда нашу страну пытаются изолировать от научно-технологического сотрудничества с передовыми странами в области информационной техники.

Особую значимость сегодня приобретает проблема обеспечения надежного функционирования средств электронной вычислительной техники, в особенности, в тех системах управления, которые используются на критически важных объектах информационной инфраструктуры. Для решения этой проблемы в Институте проблем информатики РАН создано и уже более 30 лет развивается принципиально новое научно-технологическое направление, которое основано на использовании методов самосинхронизации электронных схем [8]. И.А. Мизин активно поддерживал развитие этого направления, понимая его стратегическую значимость для обеспечения необходимых характеристик технологической базы развития информационного общества в России. В результате этого была разработана теория и методология проектирования самосинхронных схем для отечественной вычислительной техники,

обладающей высокими показателями надежности, а также система их автоматизированного проектирования, которая успешно используется и в настоящее время [9].

Образование для информационного общества

Проблема становления глобального информационного общества требует для своего решения адекватного содержания и методологии в системе образования. Стратегическая важность этой проблемы стала осознаваться и отражаться на уровне государственной политики России в середине 90-х годов XX века. Знаковым событием здесь стал Второй международный конгресс ЮНЕСКО “Образование и информатика”, который состоялся в 1996 году в России на базе МГУ им. М.В. Ломоносова с участием делегаций из более 100 стран мира. Половина из них представили участникам этого Конгресса свои Национальные доклады о государственной политике в области использования новых информационных технологий в сфере образования. Россия также представила такой доклад [10]. Его отличительная особенность заключалась в том, что основное внимание было сосредоточено не на инструментально-технологических аспектах развития системы образования, а на его содержании, которое должно стать адекватным требованиям информационного общества. С этой целью было предложено разработать, под эгидой ЮНЕСКО, и внедрить в практику на всех уровнях системы образования новый общеобразовательных курс “Фундаментальные основы информатики”.

Структура содержания этого курса и его научное обоснование были представлены участникам Конгресса в виде специального выпуска сборника научных трудов ИПИ РАН [11], а также в виде нескольких докладов ученых этого Института [12-14]. В своем пленарном докладе на Конгрессе академик И.А. Мизин [15] представил глубокий анализ состояния проблемы информатизации образования в России и сформулировал предложения по развитию международного сотрудничества в этой области.

Общая и принципиально важная идея этих докладов состояла в том, что в процессе становления информационного общества содержание образования должно иметь комплексный и опережающий характер [16]. Эта концепция получила поддержку участников Конгресса, нашла отражение в его итоговых документах и остается актуальной в настоящее время.

Отметим также, что на этом Конгрессе были впервые представлены результаты формирования российской научной школы изучения проблем социальной информатики в науке и образовании [17]. Эти результаты сегодня хорошо известны специалистам не только в России, но и в других странах. Так, например, Пражский университет Чехии в 2021 г. опубликовал развития выпуск журнала этого Университета, который был целиком посвящен проблематике этого направления в России и других странах. По предложению Главного редактора этого журнала, для него была подготовлена обзорная статья, в которой был представлен 30-летний опыт развития научной школы Социальной информатики в России [18].

Заключение

В настоящее время Россия приступает к реализации новой стратегии своего развития. Ее реализация будет происходить в исключительно сложных геополитических условиях и потребует мобилизации не только интеллектуального и научно-технического, но и духовно-нравственного потенциала нашего народа. При этом огромное значение будет иметь эффективность процессов цифровой трансформации. Приоритетными в этой сфере являются три крупных задачи:

1. Формирование современной информационной инфраструктуры на всей территории страны, что должно существенным образом повысить связанность ее регионов и эффективность использования трудовых и интеллектуальных ресурсов. Технологической основой этой инфраструктуры должны стать беспроводные и спутниковые системы связи, замещение зарубежных технологий отечественными, переход на использование доверенного программного обеспечения, а также создание отечественной элементно-компонентной базы средств информатизации общества.

2. Создание условий для перехода экономики страны к шестому технологическому укладу, основанному на широком использовании информационно-телекоммуникационных технологий, цифровых платформ и обработки больших данных методами искусственного интеллекта [19]. Решение этой задачи требует адекватных перемен в системе образования и подготовки руководящих кадров [20]. С этой целью необходимо сформировать новую научную отрасль “Информационные науки” [21], а также создать комплексную систему информационного образования, концептуальные основы которой

разработаны в Российской академии наук [22]. Должен быть существенно повышен престиж инженерных профессий и уровень математического образования специалистов и научных работников.

3. Формирование нового уровня информационной культуры российского общества, которая является необходимым условием повышения качества жизни населения нашей страны в условиях становления глобального информационного общества [23].

Литература

1. Стратегия научно-технологического развития Российской Федерации. Утверждена Указом Президента РФ от 28 февраля 2024 г. № 145.

2. Игорь Александрович Мизин – ученый, конструктор, человек. М.: ИПИ РАН, 2010. 319 с.

3. *Мизин И.А*. Телекоммуникационные технологии. Состояние и перспективы развития // Электроника: Наука, Технология, Бизнес, 1998, № 1. С. 13-18.

4. *Мизин И.А.* Современное состояние проблематики интегрированных информационно-телекоммуникационных систем и сетей //Системы и средства информатики: Вып. 9 / Под ред. И.А. Мизина. М.: Наука. Физматлит, 1999. С. 11-33.

5. Методы построения и технологии функционирования ситуационных центров / Сборник статей под ред. А.А. Зацаринного. М.: 2011. 258 с.

6. *Зацаринный А.А., Шабанов А.П*. Системные аспекты эффективности ситуационных центров // Вестник Московского университета им. С.Ю. Витте. Серия 1: Экономика и управление, 2023, № 2(4). С. 110-123.

7. *Мизин И.А., Филин А.В.* Принципиальная база архитектуры естественно-надежных компьютеров // Системы и средства информатики: Вып. 7. М.: Наука. Физматлит, 1995. С. 172-197.

8. *Степченков Ю.А., Дьяченко Ю.Г., Горелкин Г.А.* Самосинхронные схемы – будущее микроэлектроники // Вопросы радиоэлектроники, 2011, Т.4, № 2. С. 153-184.

9. *Зацаринный А.А., Степченков Ю.А., Морозов Н.В., Степченков Д.Ю.* Автоматизация синтеза самосинхронных схем // Системы высокой доступности, 2023, Т. 19, № 3. С. 48-56.

10. Политика в области образования и новые информационные технологии. Национальный доклад Российской Федерации // Информационное общество, 1996, № 1. С. 3-30.

11. Системы и средства информатики: Вып. 8. Информационные технологии в образовании: от компьютерной грамотности к информационной культуре общества. М.: Наука. Физматлит, 1996. 236 с.

12. *Мизин И.А., Киселев Э.В., Соколов И.А., Шоргин С.Я.* Некоторые проблемы создания единой информационно-телекоммуникационной системы общенационального масштаба как основы информатизации сферы образования России //Системы и средства информатики: Вып. 8. М.: Наука. Физматлит, 1996. С. 114-124.

13. *Колин К.К*. Курс информатики в системе образования: современное состояние и перспективы развития // Системы и средства информатики: Вып. 8. М.: Наука. Физматлит, 1996. С. 74-84.

14. *Христочевский С.А, Вихрев В.В., Федосеев А.А., Филинов Е.Н*. Курс “Информационные технологии” – шаг к информационной культуре // Системы и средства информатики: Вып. 8. М.: Наука. Физматлит, 1996. С. 105-113.

15. *Мизин И.А*. Состояние и перспективы развития телекоммуникационных технологий. Доклад на II Международном конгрессе ЮНЕСКО “Образование и информатика” // Информационное общество, 1996, № 5. С. 3-22.

16. *Колин К.К*. Информатика в системе опережающего образования // Вестник Российского общества информатики и вычислительной техники, № 3. С. 19-39.

17. *Колин К.К., Соколова И.В., Суслаков Б.А*. Опыт изучения проблем социальной информатики в системе образования России // Труды II Международного конгресса ЮНЕСКО «Образование и информатика». М.: ИИТО. 1997. С. 98-106.

18. *Kolin K.K*. Social Informatics: 30 Years of Scientific School Development in Russia //Acta Informatica Pragensia, 2021. Т.10, № 3. С. 289-300.

19. *Зацаринный А.А., Колин К.К.* Цифровые платформы как основа устойчивого развития стран Большой Евразии в условиях новых вызовов и угроз в информационной сфере // Стратегические приоритеты, 2018, № 1. С. 71-77.

20. *Зацаринный А.А., Колин К.К*. Подготовка руководителей организационных систем как ключевая проблема цифровой трансформации России // В сборнике: Социогуманитарные проблемы укрепления субъектности России. М.: Когито-Центр, 2023. С. 69-64.

21. *Колин К.К*. Новая информационная реальность и проблема формирования научной отрасли “Информационные науки” // International Journal of Open Information Technologies. 2024. Т. 12, № 1. С. 137-143.

22. *Колин К.К*. Образование для информационного общества: проблемы и приоритеты // Информационное общество, 2022, № 5. С. 16-34.

23. *Колин К.К*. Информационная культура и качество жизни в информационном обществе // Открытое образование. 2010, № 6. С. 84-89.

ОЦЕНКА СТАТИСТИЧЕСКИХ МЕТОДОВ АНОНИМИЗАЦИИ ПЕРСОНАЛЬНЫХ ДАННЫХ

Джениа Алмас Даурович
МТУСИ, студент, Москва, Россия
almas@dzhenia.ru

Панков Константин Николаевич
МТУСИ, доцент кафедры «Информационная безопасность», к.ф.-м.н., доцент, Москва, Россия
pankov_kn@mtuci.ru

Аннотация
В данной работе проводится анализ основных методов анонимизации персональных данных, обеспечивающих защиту конфиденциальной информации при хранении в реляционных базах данных. Особое внимание уделяется потенциальным угрозам, возникающим при использовании этих методов, включая риски для безопасности, которые могут возникнуть при доступе злоумышленников к данным. Работа подчеркивает важность контекстуального использования методов обезличивания для повышения эффективности защитных мер, а также рассматривает влияние анонимизации на полезность данных. Предлагается комплексный подход к оценке применимости методов анонимизации, учитывая специфику обрабатываемых данных и потенциальное ухудшение их полезности.

Ключевые слова
Анонимизация, персональные данные, информационная безопасность, конфиденциальность, угрозы безопасности, обезличивание, статический анализ

Введение

Стремительные технологические изменения и глобализация последних десятилетий существенно трансформировали подходы к защите персональных данных. Разрастание объемов собираемой информации и развитие методов её обработки привели к появлению новых вызовов в области информационной безопасности. В условиях, когда как частные компании, так и государственные органы получают возможность использовать персональные данные на беспрецедентном уровне, важность эффективных методов обеспечения конфиденциальности становится критически важной.

Цель данной работы - рассмотреть основные методы анонимизации персональных данных, которые позволяют маскировать информацию при её хранении в реляционных базах данных. В контексте этих методов особое внимание уделяется анализу угроз, которые могут возникнуть при их использовании и комбинации, в том числе риски, связанные с доступом злоумышленников к конфиденциальной информации.

Обезличивание данных служит важным инструментом обеспечения безопасности, направленным на предотвращение раскрытия данных и разрыва связи между записью в хранилище и конкретным лицом. Внедрение техник обезличивания в системы, работающие с базами данных, позволяет осуществлять комплексное преобразование информации, что способствует обеспечению конфиденциальности на всех уровнях обработки данных.

Использование методов анонимизации существенно освобождает от юридических обязательств по обеспечению законности обработки данных, однако также сопряжено с проблемой потери семантической полноценности информации. В связи с этим предлагается провести комплексную оценку применимости различных методов обезличивания с учетом объекта воздействия – будь то отдельная запись, столбец или вся таблица – и потенциальных потерь полезности информации.

Контекст исследования

Обезличивание как инструмент обеспечения безопасности, направлено на предотвращение к раскрытию данных, а именно определению связи между записью в хранилище данных и конкретным физическим лицом. Обезличивание преследует преобразование исходной информации. Применение обезличивания в вычислительных системах, реализующих логическое объединение связанных данных [1] (далее базы данных), предоставляет возможность полноценного преобразования информации ко всему набору данных. Условием представляемое к таким базам данных является соблюдения таких

характеристик:

Структурированность – это сохранение отношении (relation) между данными, независимо от их физического расположения

Целостность – это соблюдение единообразия в форме наполнения данных согласно значению атрибутов в кортежах отношений.

Реляционность означает, что база данных должна поддерживать реляционную алгебру при реализации запросов к ней [2].

В фундаментальных работах по теме анонимизации, отмечается что даже прямое удаление идентификаторов, имен и адресов, не может обеспечить однозначного сокрытия связи с личностью, так как связывание оставшихся параметров может дать, как минимум вероятностное значение принадлежности личности к записи в базе данных [3].

Применение методов обезличивания к данным, включает преобразование записей в базах данных, может включать в себя как частичное преобразования записи, так и её полное изменение. И хотя потеря семантического представления в записи, прямо влияет на полезность применения таких массивов данных, [4] важным аспектом в использовании таких данных, является возможность преобразование данных в исходную форму (деанонимизацией).

По возможности деанонимизаций выделяются [5] два основных вида обезличенных данных: анонимизированные и псевдоанонимизоравнные данные.

Анонимизированные данные – это сведения, которые были безвозвратно изменены таким образом, который не позволяет отнести их к конкретному человеку, даже если использовать дополнительную информацию.

Псевдонимизированные данные – это сведения, которые были изменены таким образом, который не позволяет отнести их к конкретному человеку без использования дополнительной информации. При этом, дополнительная информация должна храниться отдельно.

И хотя применение методов анонимизации персональных данных значительно расширяет возможности обработки, освобождая от определенных мер обеспечения правомерности обработки, [6] проверить на применимость в исследованиях можно с помощью вычисления значения потери полезности данных, по метрикам остаточная сумма квадратов и потеря полезности/потеря информации, эти и другие метрику будут рассмотрены далее. Применяются оценочные метрики после применения методов из области статистического контроля качества. Их применение направлено на снижение рисков раскрытия информации, относительно каждой записи в таблице, с учетом возможности связи с другими таблицами. К ним относятся: метод микроагрегации, добавление шума и дифференциальная приватность. [7]

Хранение в базах данных информации физических лиц, помимо хранения идентификаторов и персональных данных, может включать и особо чувствительные данные [8], как например состояние здоровья, материальное состояние и другие. Поэтому при преобразовании отдельных единиц записи применяют такое разделение на семантическое наполнение текста, как идентификаторы, квази-идентификаторы и чувствительные данные. Такое разделение позволяет применить различные методы обезличивания, основываясь на степени полезности поля записи для конкретного исследования. Так, к примеру в целях обеспечения безопасности достоверной практикой является удаление прямых идентификаторов (далее – ИД) как в примере из таблицы 1.

Таблица 1

Оригинальная таблица

ИД	ФИО	Номер телефона
2153	Сазонов Аркадий Христофорович	+79412443125
2154	Лобанова Харита Германновна	+79231252452
2155	Петрофанов Евгений Янович	+79334212482

Таблица 2

Данные после удаления ИД

ФИО	Номер телефона
Сазонов Аркадий Христофорович	+79412443125
Лобанова Харита Германновна	+79231252452
Петрофанов Евгений Янович	+79334212482

Выделив необходимый к преобразованию атрибут (идентификатор, квази-идентификаторы или чувствительные данные), можно приступить к выбору методу обезличивания.

Различают методы по типу их преобразования исходных данных:

1. Методы, основанные на дифференциальной приватности:

- Differential Privacy (ε-DP). Данный метод обеспечивает, что любые два набора данных, различающихся только одной записью, будут выдавать почти неотличимые результаты для всех запросов.
- Добавление шума Лапласа или Гаусса к числовым атрибутам для достижения ε-дифференциальной приватности.

2. Методы, основанные на *k*-анонимности:

- k-анонимизация однозначно гарантирует, что каждая запись неотличима минимум от $k-1$ других записей в наборе данных.
- Incognito algorithm – модифицированный метод для k-анонимизации, использующий рекурсивное обобщение.
- Расширение *k*-анонимизации *p*-sensitive *k*-anonymity, обеспечивающее, что каждый чувствительный атрибут также анонимизирован для минимум $k-1$ других записей [9].

3. Методы, основанные на обобщении и перемешивании:

- Top Down – метод, использующий иерархическое обобщение от наиболее общего уровня к наиболее конкретному.
- GreedyPKClustering algorithm – метод, основанный на кластеризации данных с целью минимизации потери информации и увеличения анонимности.
- Рассеивание, перемешивание и гаммирование – подгруппа техник, которые изменяют данные для увеличения анонимности путем искажения или перемешивания значений.
- Перемешивание данных (относительно строк) – техника, перемешивающая строки данных для предотвращения отслеживания или идентификации отдельных записей.

4. Методы, основанные на модификации данных:

- Уменьшение перечня – удаление или маскировка определенных данных для уменьшения их идентифицируемости.
- Замена части сведений идентификаторами – к примеру чувствительных данных на неидентифицируемые маркеры, где идентифицируемая информация хранится в иной базе данных.
- Замена реальных значений на статистические меры (минимум, среднее или максимум) для сокрытия точных данных.
- Сокращение детализации данных (уменьшение объема атрибута) для уменьшения вероятности идентификации [10].
- Разделение данных на части и их раздельная обработка в различных системах для уменьшения риска утечки [11].

5. Специфические технические методы:

- BCF-ANONYMITY – метод, предназначенный для защиты от конкретных типов атак (BCF), который может иметь ограниченное применение в узких условиях.
- The minimum spanning tree (MST), the variable MDAV (VMDAV), two fixed reference points (TFRP) - специфические алгоритмические подходы, которые могут быть использованы для реализации различных методов анонимизации, включая кластеризацию или многоразмерное сжатие данных для анонимизации.

6. Методы, основанные на криптографических методах преобразовании информации:

- Использование шифрования с открытым ключом для защиты данных при передаче, где каждый участник имеет пару ключей: открытый для шифрования и секретный для расшифрования данных. Этот метод позволяет пользователям безопасно обмениваться данными при ограничении доступа к секретному ключу. Отметим, что в условиях стоящего перед современным обществом квантового вызова [12], при использовании данного метода актуально применения квантовых [13] и постквантовых алгоритмов [14] защиты информации.
- Хеширование, которое с помощью применения криптографической хеш-функции к содержимому записи в таблице позволяет получить уникальный квази-случайный битовый вектор, минимизируя риск восстановления, основанную на хешируемой записи [15].

В качестве примера микроагрегации с помощью *k*-анонимизации, представлен пример по преобразованию столбцов в квази-идентификаторы.

Таблица 3

Оригинальная таблица

ФИО	Номер телефона	Индекс
Сазонов Аркадий Христофорович	+79412443125	35600
Лобанова Харита Германновна	+79231252452	35623
Петрофанов Евгений Янович	+79334212482	35683

Таблица 4

Данные после *k*-анонимизации

ФИО	Номер телефона	Индекс
Сазонов Аркадий Христофорович	+79412443125	356**
Лобанова Харита Германновна	+79231252452	356**
Петрофанов Евгений Янович	+79334212482	356**

В качестве примера анонимизации персональных данных представлен пример хеширования единицы записи

Таблица 5

Оригинальная таблица

ФИО	Номер телефона	Зарплата	Семейное положение
Сазонов Аркадий Христофорович	+79412443125	45000	Холост
Лобанова Харита Германновна	+79231252452	65000	Помолвлена
Петрофанов Евгений Янович	+79334212482	10000	Женат

Таблица 6

Данные после применения хеш-функции

ФИО	Номер телефона	Зарпалата	Семейное положение
Сазонов Аркадий Христофорович	+79412443125	45000	10412375520728980495…
Лобанова Харита Германновна	+79231252452	65000	84130391529128980461..
Петрофанов Евгений Янович	+79334212482	10000	46122519638128980448..

Атака на обезличенные данные

Проведение атаки на обезличенные данные направлено на раскрытие оригинальных сведений, и восстановление структурных изменений, которые могли быть применены при обеспечении конфиденциальности данных. Хотя не все атаки могут привести к раскрытию информации некоторые из них могут помочь определить вероятностные значения принадлежности чувствительной информации к физическому лицу, что в комбинации с другими атаками может привести к конкретному определению связи между записью и физическим лицом.

Проведение симуляции на этапе оценки эффективности мер по обезличиванию, поможет точно определить параметры необходимые для достаточного уровня конфиденциальности, с учетом сохраняемой полезностью данных.

Оценка методов

Оценка успешности обезличивания проводится с помощью тестирования возможности раскрытия информации при её историческом изменении. Так, оценка происходит по трем способам раскрытия информации, раскрытие отдельных записей (discernability measure [Truta_SDM_submitted]), распределение образованных кластеров (в частности, при k-анонимизации) (normalized average cluster size metric), оценка риска раскрытия физического лица в наборе данных (Identity Disclosure) и оценка риска принадлежности лица к анонимизированному атрибуту (к примеру, чувствительному столбцу) (attribute disclosure). Именно при проведении оценки анонимизации возможно сравнить степень обеспечения конфиденциальности на различных этапах преобразования.

В вопросе оценки полезности, использование существующих метрик направлено на оценку эффективности при выполнении определённых действия с набором данных, как итог их применимость для дальнейших исследовании.

В существующих источниках рассматриваются метрики для следующих операции с данными: оценку полезности среди запросов ко всем записям в сравнении с оригинальным набором производится с помощью querry error, что помогает выделить процентную составляющую ошибочных ответов, т.е. ответов заведомо ложных. Как итог применение неоптимальных методов приводит к неточностям, несогласованности и неполноте данных, что приводит к неправильным решениям при исследовании.

Отметим, что задача оценки систем, в которых используются криптографические методы, с помощью тестирования, верификации и валидации в приложении к системам распределенного реестра [16] как полностью реплицированным базам данных, работающим на основе децентрализованных сетей, ставилась в [17] и была развита в [18]. Защита персональных данных в подобных базах данных рассматривалась в [19].

Предложение по дальнейшему направлению исследования

Можно сделать вывод, что ни один из рассмотренных выше методов не может обеспечить полноценную защиту данных при обеспечении семантической полноценности. В таких условиях при выборе методологии обезличивания персональных данных, необходимо продемонстрировать эффективность выбранных мер. Эффективность же описывается, в частности, в рамках статистического контроля или специфичных метрик аналитики. Работа в направлении оценки методов в целях предоставлениях конфиденциальности, с сохранением высокую полезность данных, может значительно облегчить процесс составления методологии и их реализации. Так новые исследования, могут учитывать различные актуальные условия применимые к формату данных (файлы, графы, таблицы) способам хранения (локальные данные, распределенные системы) и целостности данных (статичные или динамичные данные [20]). Разработка новых требований к свойствам обезличенных данных поможет облегчить выбор методов, в зависимости от целей исследований.

Заключение

Использование методов анонимизации персональных данных в значительной степени освобождает от обязательств по обеспечению правомерности обработки данных. Однако проблема потери семантической полноценности ограничивает от таких преобразовании.

Предлагается проведение комплексной оценки применимости различных методов обезличивания с учетом объектом воздействия (отдельная запись в таблице, столбец или вся таблица) и возможных потерь полезности информации. Отметим, что к числу методов обезличивания относятся в том числе и криптографические методы, которые являются универсальными методами обеспечения информационной безопасности, развитие которых требуют глубоких математических исследований (к примеру, как в [21-24]).

Литература

1. *Когаловский М.Р*. Энциклопедия технологий баз данных. 1-е изд. Socionet & Институт проблем рынка РАН, 2002. 800 с.

2. *Кузнецов С.Д*. Базы данных: языки и модели. М.: Бином, 2008. 720 с.

3. *Sweeney L*. k-anonymity: a model for protecting privacy // International Journal on Uncertainty. 2002. № 10 (5). С. 557-570.

4. *Majeed A., Hwang S.O*. Quantifying the Vulnerability of Attributes for Effective Privacy Preservation Using Machine Learning // IEEE Access. 2023. № 11. С. 4400-4411.

5. *Rebollo-Monedero D., Hernandez-Baigorri C., Forne J., Soriano M.* Incremental k-anonymous microaggregation in large-scale electronic surveys with optimized scheduling // IEEE Access. 2018. № 6. С. 60016-60044.

6. *Гончаров А.М., Чекудаев К.В., Денисенко В.В*. Защита персональных данных в соответствии с GDPR // Моделирование энергоинформационных процессов. Воронеж: Воронежский государственный университет инженерных технологий, 2024. С. 350-354.

7. *Кузнецов П.П., Столбов А.П.* Автоматизированная обработка и защита персональных данных в медицинских учреждениях. М.: ИД «Менеджер здравоохранения», 2010. 270 с.

8. *Athanasios Andreou, Oana Goga, Patrick Loiseau*. Identity vs. Attribute Disclosure Risks for Users with Multiple Social Profiles // ASONAM '17: Proceedings of the 2017 IEEE/ACM International Conference on Advances in Social Networks Analysis and Mining. 2017. С. 163-170.

9. *Rebollo-Monedero D., Forne J.* и др. k-Anonymous microaggregation with preservation of statistical dependence // Inf. Sci. 2016. № 342. С. 1-23.

10. *Куракин А.С.* Алгоритм деперсонализации персональных данных // Научно-технический вестник информационных технологий, механики и оптики. 2012. № 6 (82). С. 130-135.

11. Introduction to the hash function as a personal data pseudonymisation technique. // European Data Protection Supervisor: https://www.edps.europa.eu/sites/default/files/publication/19-10-30_aepd-edps_paper_hash_final_en.pdf (дата обращения: 15.07.2024).

12. Распоряжение Правительства РФ от 11 июля 2023 г. № 1856-р. Об утверждении Концепции регулирования отрасли квантовых коммуникаций в РФ до 2030. // ГАРАНТ.РУ: [сайт]. https://www.garant.ru/products/ipo/prime/doc/407297268/

13. *Панков К.Н., Миронов Ю.Б.* Применение квантовых методов в задачах защиты информации. М.: Горячая линия – Телеком, 2022. 212 с.

14. *Панков К.Н., Миронов Ю.Б.* Использование постквантовых алгоритмов в задачах защиты информации в телекоммуникационных системах. Москва: Горячая линия – Телеком, 2023. 236 с. ISBN 978-5-9912-1015-7. EDN MTJUJL

15. Xiao Xiaokui, Tao Yufei. Personalized Privacy Preservation // Proceedings of the 2006 ACM SIGMOD international conference on Management of data. 2006. № 34. С. 229-240.

16. *Панков К.Н.* Использование криптографических средств для сквозных цифровых технологий на примере систем распределенного реестра // Технологии информационного общества : Материалы XII Международной отраслевой научно-технической конференции, Москва, 14-15 марта 2018 года. Том 1. М.: Издательский дом Медиа Паблишер, 2018. С. 365-366. EDN UUHHSM

17. *Pankov K.N.* Testing, Verification and Validation of Distributed Ledger Systems // 2020 Systems of Signals Generating and Processing in the Field of on Board Communications, Moscow, 19-20 марта 2020 г. Moscow: Institute of Electrical and Electronics Engineers Inc., 2020. P. 9078541. DOI 10.1109/IEEECONF48371.2020.9078541. EDN CITRFX

18. *Панков К.Н., Эйнман А.Д.* Сертификация систем распределенного реестра как инструмент обеспечения информационной безопасности // REDS: Телекоммуникационные устройства и системы. 2021. Т. 11, № 2. С. 37-49. EDN CGQQYR

19. *Pankov K.* Enumeration of Boolean Mapping with Given Cryptographic Properties for Personal Data Protection in Blockchain Data Storage // Conference of Open Innovations Association, FRUCT. 2019. No. 24, pp. 300-306. DOI 10.23919/FRUCT.2019.8711894. EDN BOVLMR

20. *Майкова П.Н., Майкова Е.Н.* Статистический контроль качества в производстве // Форум молодых ученых. 2022. № 4 (68). С. 187-191.

21. *Панков К.Н.* Локальная предельная теорема для распределения части вектора весов подфункций компонент случайного двоичного отображения // Математические вопросы криптографии. 2014. Т. 5, № 3. С. 49-80. EDN TFNXVD

22. *Pankov K.N.* Improved asymptotic estimates for the numbers of correlation-immune and k-resilient vectorial Boolean functions // Discrete Mathematics and Applications. 2019. Vol. 29, No. 3, pp. 195-213. DOI 10.1515/dma-2019-0018. EDN CFOLBU

23. *Kamlovskii O.V., Pankov K.N.* Some Classes of Balanced Functions over Finite Fields with a Small Value of the Linear Characteristic // Problems of Information Transmission. 2022. Vol. 58, No. 4, pp. 389-402. DOI 10.1134/s0032946022040093. EDN QSFFJO

24. *Панков К.Н.* Оценки мощности классов отображений, применяемых в протоколах квантового распределения ключей // Наукоемкие технологии в космических исследованиях Земли. 2022. Т. 14. № 4. С. 4-18.

ПРИМЕНЕНИЕ ТЕХНОЛОГИЙ ОБЪЕМНОГО ЗВУЧАНИЯ DOLBY В ЦИФРОВОМ РАДИОВЕЩАНИИ СТАНДАРТА DRM

Метёлкин Вячеслав Васильевич
МТУСИ, студент, Москва, Россия

Кузнецов Андрей Владимирович
МТУСИ, студент, Москва, Россия

Варламов Олег Витальевич
МТУСИ, начальник отдела, д.т.н., Москва, Россия,
vov@mtuci.ru

Аннотация
Рассмотрена техническая возможность использования технологий объемного звучания Dolby Stereo / Dolby Surround для улучшения восприятия музыкальных программ в системе цифрового радиовещания стандарта Digital radio mondiale (DRM) диапазонов низких (НЧ), средних (СЧ) и высоких (ВЧ) частот. Показана техническая реализуемость данного предложения в режимах "стерео" и "параметрическое стерео" при вещании в полосах частот 9 / 10 кГц в режиме помехоустойчивости "A" с модуляцией 64QAM и уровнями помехозащищенности "1", "2" и "3" (в диапазонах НЧ и СЧ), и в режиме помехоустойчивости "B" с модуляцией 64QAM и уровнями помехозащищенности "2" или "3" - в стабильных каналах диапазона ВЧ с полосой частот 10 кГц.

Ключевые слова
Dolby Stereo, Dolby Surround, DRM, объемное звучание, параметрическое стерео, разделение стереоканалов, цифровое радиовещание

Введение

Digital radio mondiale (DRM) – стандарт цифрового радиовещания [1], разработанный для использования в диапазонах длинных, средних и коротких волн в качестве замены аналогового вещания с применением амплитудной модуляции (АМ) [2-10]. Стандарт DRM имеет преимущество перед АМ в виде возможности передачи до четырех аудио каналов с помощью различных кодеков, или более качественного вещания, включая стереофоническое [11], а также малопиксельного телевидения [12]. Также возможна одновременная передача аналогового и цифрового сигналов в режиме Simulcast [13]. Для использования в диапазоне УКВ, в дополнение к вещанию с частотной модуляцией, разработано расширение DRM+ [14]. Вопросы построения передающего [15] и приемного [16, 17] оборудования к настоящему времени подробно рассмотрены. Применяемый в последней версии DRM аудиокодек xHE-AAC может поддерживать адаптивную потоковую передачу со скоростями от 12 до более чем 320 кбит/с для стерео и обеспечивает наилучшее качество звучания по результатам экспертных оценок при низких скоростях кодирования (Рис. 1, https://www.iis.fraunhofer.de/en/ff/amm/broadcast-streaming/xheaac.html).

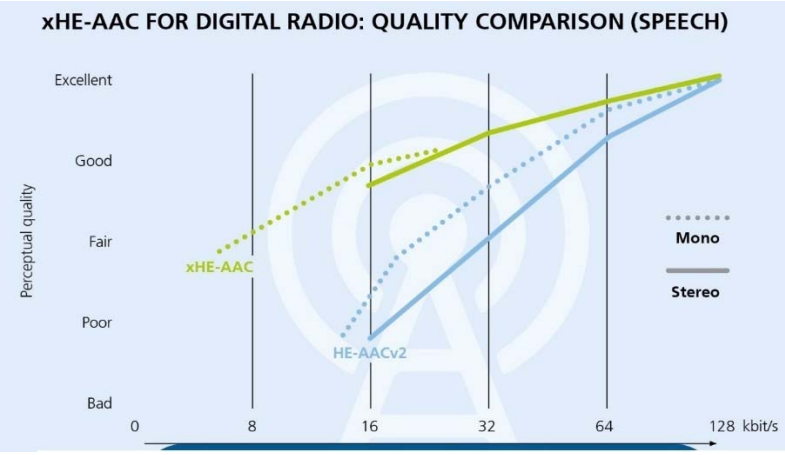


Рис. 1. Сравнение качества звучания по результатам экспертных оценок кодеков xHE-AAC и HE-AACv2 (https://www.iis.fraunhofer.de/en/ff/amm/broadcast-streaming/xheaac.html)

Кодек xHE-AAC является надмножеством кодеков MPEG, в которых реализована возможность организации объемного звучания по технологии MPEG Surround. Однако требуемые для работы данной системы скорости передачи доступны только в диапазоне УКВ в стандартах цифрового радиовещания DRM+ [14] и DAB, а также могут быть использованы в цифровом телевизионном вещании. В стандарте DRM доступны только режимы "моно", "стерео" и "параметрическое стерео".

Для улучшения аудиовосприятия сигнала DRM посредством создания объемного звучания предлагается рассмотреть потенциальную возможность применения технологии объемного звучания Dolby для стереофонического канала DRM, используемого как "черный ящик".

Эта опция также может быть использована для улучшения диалогов (Dialog Enhancement) в разговорных программах [18]. Существует также множество архивных 2-канальных стереозаписей (включая цифровые), которые могут быть более привлекательными при постобработке до 5.0-канального стандарта. Для восстановления истинного пространственного акустического поля для систем объемного звучания 5.0 или с аналоговым кодированием Dolby Surround может быть использован алгоритм, предложенный в [19].

Dolby Stereo – аналоговая четырехканальная система объемного звука, изначально созданная для кинотеатров, с упрощенной трехканальной домашней версией Dolby Surround, развившейся впрследствии до 4-х канальной Dolby Pro Logic и трансформировавшейся в цифровую эру в Dolby Digital с битрейтом от 320 кбит/с для AC3 компрессированного 5.1 звукового сопровождения.

Несмотря на то, что компания Dolby является одним из участников DRM -Консорциума, можно не ожидать появления "фирменных" решений по симбиозу данных технологий, поскольку они используют конкурирующие форматы компрессии аналогового звукового сигнала. Тем не менее, никто не мешает вещателям перед подачей стереосигнала на кодер передающего тракта DRM применить к нему преобразование в соответствии с Dolby Surround или Dolby Pro Logic, а после декодирования сигнала DRM в пользовательском приемнике включить декодер объемного звука.

Кодеры Dolby Surround и Pro Logic 2 по-прежнему являются широкодоступным и недорогим оборудованием, пример которого представлен на рисунке 2.

В данной статье рассматриваются особенности стереорежимов в стандарте DRM, процедуры преобразования каналов в системе Dolby и анализируется техническая возможность их совместимости.

Рис. 2. Пример кодера Dolby Surround и Pro Logic 2

Особенности стереорежимов в стандарте DRM

Структурная схема аудио кодирования / декодирования в соответствии со стандартом DRM [20] приведена на рисунке 3. Как уже отмечалось выше, опция объемного окружения доступна только в режиме DRM+ в диапазоне УКВ. В Диапазонах ДВ, СВ и КВ (режим DRM) доступны режимы "стерео" и "параметрическое стерео". Требуемые скорости передачи для обеспечения различных полос пропускания звукового тракта в режимах "моно" / "параметрическое стерео" / "стерео" приведены в таблице 1.

Такие скорости передачи могут быть достигнуты в полосах частот вещания 9/10 кГц в режиме помехоустойчивости "A" с модуляцией в основном канале обслуживания 64QAM и уровнями помехозащищенности "1", "2" и "3". Это позволяет обеспечить качественное вещание в диапазонах НЧ и СЧ как в дневное, так и в ночное время [7]. Также возможно использование режима помехоустойчивости "B" с модуляцией в основном канале обслуживания 64QAM и уровнями помехозащищенности "2" или "3", что позволит использовать и ряд достаточно стабильных (преимущественно односкачковых одно - двухлучевых) каналов диапазона ВЧ с полосой частот 10 кГц. Напомним, что в относительно "сложных" каналах распространения, к которым относится, в частности, зенитное излучение, DRM вещание возможно только с "информационным" качеством [5].

Проведенные инструментальные измерения [11] показали, что переходное затухание между стереоканалами в режиме «стерео» составляет –77/–78 дБ. Это позволяет предполагать возможность

использования практически любой обработки многоканального звука для передачи его по стереоканалу.

Переходное затухание между стереоканалами в режиме «параметрическое стерео» (в соответствии с алгоритмом его работы) зависит от частоты и приведено в таблице 2 [11]. Как видно из таблицы 2, переходное затухание в диапазоне частот изменяется от -9 до -35 дБ. Возможность использования данного режима для передачи предварительно обработанного многоканального звука требует рассмотрения совместно с алгоритмами кодирования звукового окружения.

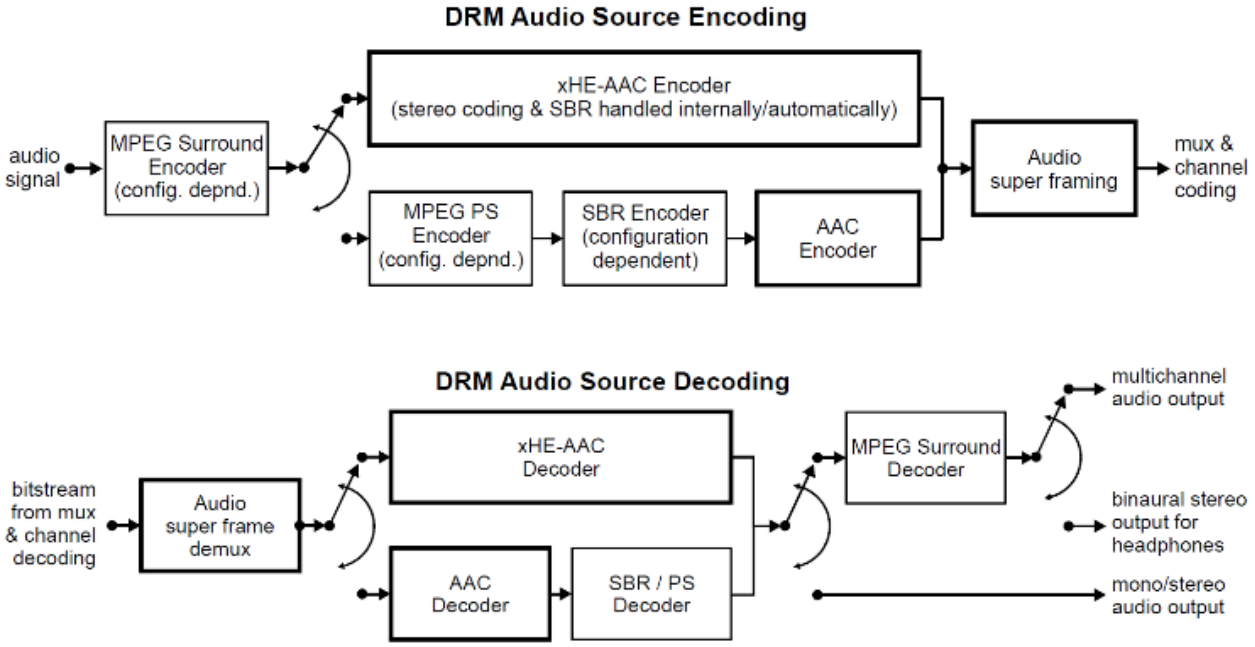


Рис. 3. Структурная схема аудио кодирования / декодирования в стандарте DRM [20]

Таблица 1

Требуемые скорости передачи для обеспечения различных полос пропускания звукового тракта в режимах моно / параметрическое стерео / стерео

Полоса пропускания звукового тракта, Гц	10 875	13 125	15 375
Режим работы	Требуемые скорости передачи, бит/с		
AAC+SBR моно	14 000 – 18 460	18 480 – 22 460	22 480 – 28 460
AAC+SBR параметрическое стерео	16 480 – 20940	20960 – 24940	> 24960
AAC+SBR стерео	Не поддерживается	26 480 – 28 480	> 28 480

Таблица 2

Переходное затухание между стереоканалами в режиме «параметрическое стерео»

Частота, Гц	120	400	1 000	5 000	10 000
Затухание между стереоканалами, дБ	-9	-11,6	-14	-21	-35

Преобразование каналов в системе Dolby

Прежде чем описывать аналоговую систему Dolby Stereo/Dolby Surround, рассмотрим результаты библиометрического анализа. Анализ проводился на основе публикаций в крупнейшей технической цифровой библиотеке IEEE Xplore с учетом методологии [21] и коллабораций организаций и авторов [22]. На рисунке 4 левая ось показывает распределение публикаций (журнальных статей, докладов конференций и книг) по годам. Правая ось показывает количество цитирований в статьях и патентах отдельно.

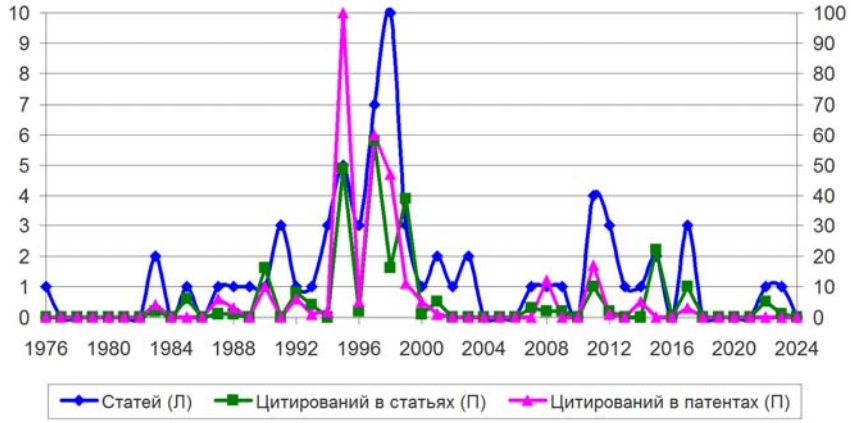


Рис. 4. Результаты библиометрического анализа по тематике "Dolby"

Как видно из рисунка 4, публикации по тематике Dolby (всего рассмотрено 69 публикаций с 1976 по 2024 гг.) имеют специфическую особенность – они больше цитируются в патентах (всего 299 ссылок из патентов), чем в статьях (265 ссылок в статьях). Это, несомненно, связано с коммерческим использованием продукта. Этим же объясняется и тот факт, что большинство публикаций написано сотрудниками различных подразделений Dolby или при их участии. Максимальная активность отмечена в периоды с 1995 по 1999 гг. и связана с переходом на цифровые технологии. Второй пик активности в 2011-2017 гг. был обусловлен активным внедрением lossy-кодеков и увеличением количества аудиоканалов.

В аналоговой системе Dolby Stereo/Dolby Surround четырёхканальный звук: левый (E_L), центральный (E_C), правый (E_R) и моно-суррaунд (E_S) – подвергаются матричному перекодированию на две аудиодорожки в соответствии с выражениями:

$$E_{LT} = E_L + \frac{\sqrt{2}}{2}E_C - \frac{\sqrt{2}}{2}jE_S,$$
$$E_{RT} = E_R + \frac{\sqrt{2}}{2}E_C + \frac{\sqrt{2}}{2}jE_S$$

или, в матричной форме:

$$\begin{bmatrix} E_{LT} \\ E_{RT} \end{bmatrix} = \begin{bmatrix} 1 & \frac{\sqrt{2}}{2} & 0 & -\frac{\sqrt{2}}{2}j \\ 0 & \frac{\sqrt{2}}{2} & 1 & \frac{\sqrt{2}}{2}j \end{bmatrix} \begin{bmatrix} E_L \\ E_C \\ E_R \\ E_S \end{bmatrix}.$$

Структурная схема кодера, реализующая данное преобразование, приведена на рисунке 5. После этого двухканальный сигнал может быть передан через систему стереофонического вещания. Сигнал декодируется конечным устройством обратно в четырёхканальный звук (рис. 6) и описывается выражениями:

$$\begin{bmatrix} E_L' \\ E_C' \\ E_R' \\ E_S' \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ \frac{\sqrt{2}}{2} & \frac{\sqrt{2}}{2} \\ 0 & 1 \\ \frac{\sqrt{2}}{2} & -\frac{\sqrt{2}}{2} \end{bmatrix} \begin{bmatrix} E_{LT} \\ E_{RT} \end{bmatrix},$$

и в результате преобразования получаем:

$$E_L' = E_L + \frac{\sqrt{2}}{2}E_C - \frac{\sqrt{2}}{2}jE_S; E_C' = \frac{\sqrt{2}}{2}E_L + E_C + \frac{\sqrt{2}}{2}E_R;$$
$$E_R' = E_R + \frac{\sqrt{2}}{2}E_C + \frac{\sqrt{2}}{2}jE_S; E_S' = \frac{\sqrt{2}}{2}E_L - \frac{\sqrt{2}}{2}E_R - jE_S;$$

После завершения декодирования перекрестные помехи между противоположными каналами исчезают, т. е. разделение между противоположными каналами бесконечно. В частности, исходный сигнал центрального канала не появляется в окружающем канале после декодирования и наоборот, что является преимуществом кодирования/декодирования Dolby Surround. Однако отношение амплитуд между перекрестными помехами соседнего канала и желаемого сигнала (разделение между соседними каналами) составляет всего 3 дБ, что неизбежно для всех матричных систем формата "4-2-4" [23]. Без декодера сигнал воспроизводится как стандартный стереофонический или монофонический.

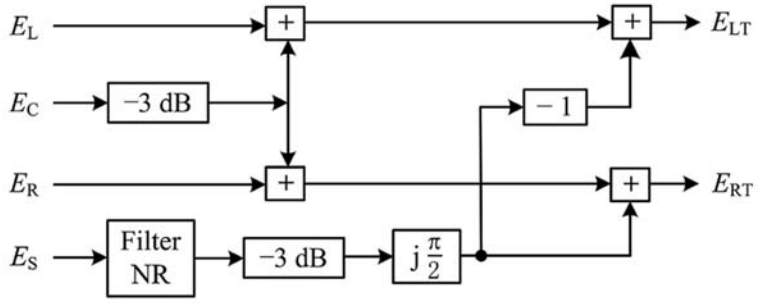


Рис. 5. Структурная схема кодера Dolby Surround [23]

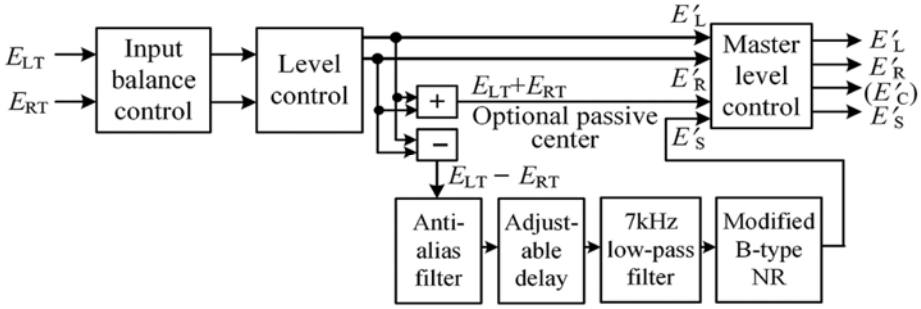


Рис. 6. Структурная схема декодера Dolby Surround [23]

Учитывая, что разделение между стереоканалами в режиме «параметрическое стерео» составляет в системе DRM от 9 до 35 дБ (в зависимости от частоты), можно предположить, что с формальной точки зрения оно не сможет оказать существенного влияния на параметры системы, в которой разделение между соседними каналами составляет всего 3 дБ.

Таким образом, канал цифрового радиовещания стандарта DRM представляется "прозрачным" для использования технологий объемного звучания Долби. Вопросы сохранения фазовой расстановки источников звука могут быть получены с помощью прослушивания, что является направлением дальнейших исследований.

Техническая реализация радиоприемного устройства DRM

Проблема технической реализации радиоприемного устройства, способного принимать и декодировать сигнал стандарта DRM с приемлемым для носимого аппарата уровнем потребления электроэнергии, долгие годы сдерживала распространение технологии DRM. В отсутствие специализированного недорогого чипа с малым потреблением (как для цифрового телевидения DVB-T/T2 или цифрового радиовещания DAB+), приемники DRM выполнялись на сигнальных процессорах общего применения, что обуславливало потребляемую мощность на уровне единиц Ватт. По этой причине к настоящему времени распространение получили только автомобильные реализации, в основном, в Индии, где законодательно запрещен выпуск новых автомобилей без приемников DRM, используемых, в том числе, для передачи сигналов оповещения.

В этой ситуации начало коммерческого производства недорогого (US$35) приемного модуля "DRM-1000" фирмы CMLMicro, представляющего собой полный тракт обработки сигналов AM/FM/DRM/DRM+ от антенны до громкоговорителя в диапазоне частот от 530 кГц до 108 МГц (рис. 7) с габаритами 46x29x5 мм и потребляющего 200 мВт [24] (без учета УНЧ) предоставляет разработчикам новые возможности по расширению использования данной технологии.

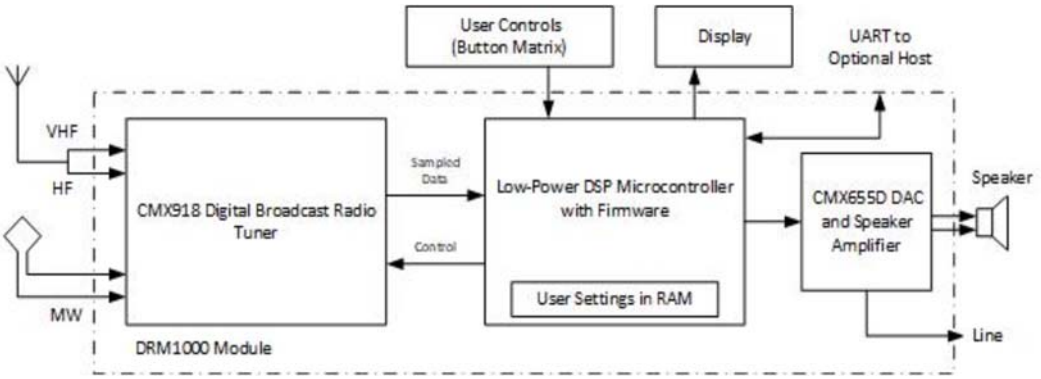


Рис. 7. Структурная схема приемного модуля DRM-1000

Заключение

Проведенный анализ показал, что с формальной точки зрения канал цифрового радиовещания стандарта DRM представляется "прозрачным" для использования технологий объемного звучания Долби. Он может использоваться в режимах «стерео» и «параметрическое стерео» при вещании в полосе частот 9/10 кГц в режиме помехоустойчивости «А» с модуляцией 64QAM и уровнями помехозащищенности «1», «2» и «3» (в диапазонах НЧ и СЧ), а также в режиме помехоустойчивости «В» с модуляцией 64QAM и уровнями помехозащищенности «2» или «3» — в стабильных каналах КВ диапазона с полосой частот 10 кГц.

Вопросы сохранения фазового расположения источников звука [25] и более точные результаты, учитывающие особенности параметрического стереокодирования с низкой скоростью передачи данных, могут быть получены путем прослушивания, как это было сделано, например, в совместной работе авторов из Fraunhofer Institut für Integrierte Schaltungen, Эрланген, Германия и Dolby Sweden AB, Стокгольм, Швеция [26], с использованием методики ITU MUSHRA [27].

Литература

1. *Варламов О.В*. Разработка отечественной нормативной базы цифрового радиовещания стандарта DRM // T-Comm: Телекоммуникации и транспорт. 2013. Т. 7. № 9. С. 47-50.

2. *Варламов О.В*. Особенности частотно-территориального планирования сетей радиовещания DRM диапазонов НЧ И СЧ // T-Comm: Телекоммуникации и транспорт. 2013. Т. 7. № 9. С. 43-46.

3. *Варламов О.В*. Организация одночастотных сетей цифрового радиовещания стандарта DRM. Особенности и результаты практических испытаний // T-Comm: Телекоммуникации и транспорт. 2018. Т. 12. № 11. С. 4-20.

4. *Варламов О.В*. Способ организации глобальной сети цифрового радиовещания в диапазоне ДВ // T-Comm: Телекоммуникации и транспорт. 2015. Т. 9. № 5. С. 63-68.

5. *Варламов О.В*. Использование необыкновенной волны для цифрового радиовещания DRM зенитным излучением // T-Comm: Телекоммуникации и транспорт. 2015. Т. 9. № 1. С. 32-38.

6. *Varlamov O.V., Bychkova A.A*. Basis of technical design and development a single-frequency DRM digital broadcasting network for Venezuela // 2021 Systems of Signal Synchronization, Generating and Processing in Telecommunications, SYNCHROINFO 2021 – Conference Proceedings. 2021. С. 9488396.

7. *Варламов О.В.* Исследование цифрового радиовещания DRM в диапазоне СВ в зоне федингa // T-Comm: Телекоммуникации и транспорт. 2015. Т. 9. № 2. С. 41-45.

8. *Варламов О.В.* Корректное планирование сетей DRM-вещания // Электросвязь. 2014. № 6. С. 26-34.

9. *Варламов О.В., Варламов В.О., Долгопятова А.В.* Международная сеть DRM вещания для создания информационного поля в Арктике // T-Comm: Телекоммуникации и транспорт. 2019. Т. 13. № 9. С. 9-16.

10. *Varlamov O*. The radio noise effect on the coverage area of DRM broadcast transmitter in different regions // T-Comm: Телекоммуникации и транспорт. 2015. Т. 9. № 2. С. 90-93.

11. *Varlamov O.V*. DRM digital broadcasting system audio path qualitative characteristics // Synchroinfo Journal. 2022. Т. 8. № 4. С. 2-8.

12. *Махнырь А.В., Коротченко Н.В., Варламов О.В.* Некоторые алгоритмы, применяемые при реализации приложения малопиксельного телевидения DIVEEMO в стандарте DRM // Системы синхронизации, формирования и обработки сигналов. 2023. Т. 14. № 1. С. 18-29.

13. *Варламов О.В.* Соотношение мощностей аналогового и цифрового сигналов при DRM радиовещании в режиме Simulcast // T-Comm: Телекоммуникации и транспорт. 2016. Т. 10. № 12. С. 81-84.

14. *Dolgopyatova A.V., Varlamov O.V.* Analysis of long-range VHF radio waves propagation to specify protection ratios between coexisting DRM+, RAVIS and IBOC systems // 2021 Systems of Signal Synchronization, Generating and Processing in Telecommunications, SYNCHROINFO 2021 – Conference Proceedings. 2021. С. 9488392.

15. *Варламов О.В., Лаврушенков В.Г*. Критерии качества передающего устройства для стандарта DRM и измерительное оборудование // Broadcasting. Телевидение и радиовещание. 2004. № 3. С. 44-48.

16. *Варламов О.В*. Разработка требований к приемному оборудованию сетей цифрового радиовещания стандарта DRM // T-Comm: Телекоммуникации и транспорт. 2013. Т. 7. № 9. С. 39-42.

17. *Varlamov O.V*. DRM digital radio receivers sensitivity // В сборнике: 2023 International Conference on Engineering Management of Communication and Technology, EMCTECH 2023. Proceedings. New York, 2023. С. 10296930.

18. *Master A*. et al. Deepspace: Dynamic Spatial and Source CUE Based Source Separation for Dialog Enhancement // ICASSP 2023 - 2023 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP), Rhodes Island, Greece, 2023, pp. 1-5, doi: 10.1109/ICASSP49357.2023.10095497.

19. *Komatowski E.* Stereo to the "Real Surround Sound" conversion algorithm // 2011 34th International Conference on Telecommunications and Signal Processing (TSP), Budapest, Hungary, 2011, pp. 339-342, doi: 10.1109/TSP.2011.6043713.

20. ETSI ES 201 980 V4.1.1 (2014-01) Digital Radio Mondiale (DRM); System Specification.

21. *Dymkova S.* Methodology for organizing scientific work in telecommunications university // Systems of Signals Generating and Processing in the Field of on Board Communications. 2023. Т. 6. № 1. С. 104-109.

22. *Dymkova S.S., Varlamov O.V*. Scientometric analysis of authors collaborations at the international conference “Engineering management of communications and technologies“ // 2023 International Conference on Engineering Management of Communication and Technology, EMCTECH 2023. Proceedings. New York, 2023. С. 10296946.

23. Bosun Xie. Spatial Sound. Principles and Applications // CRC Press. Second (English) edition, 2023.

24. DRM1000Datasheet. Интернет ресурс: https://cmlmicro.com/Content/Downloads/DRM1000Datasheet.pdf (доступно январь 2025).

25. *Gusó E., Pons J., Pascual S., Serrà J.* On Loss Functions and Evaluation Metrics for Music Source Separation // ICASSP 2022 - 2022 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP), Singapore, Singapore, 2022, pp. 306-310, doi: 10.1109/ICASSP43922.2022.9746530.

26. *Helmrich C.R*. и др. Efficient transform coding of two-channel audio signals by means of complex-valued stereo prediction // 2011 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP), Prague, Czech Republic, 2011, pp. 497-500, doi: 10.1109/ICASSP.2011.5946449.

27. International Telecommunication Union, Radiocommunication Assembly, “Recommendation ITU-R BS.1534-3: Method for the subjective assessment of intermediate quality level of audio systems,” Geneva, October 2015.

ИССЛЕДОВАНИЕ МЕТОДОВ КОНТРОЛЯ ВЫПОЛНЕНИЯ УПРАЖНЕНИЙ ВОССТАНОВИТЕЛЬНОЙ ГЛАЗНОЙ ГИМНАСТИКИ

Власюк Игорь Викторович
Московский технический университет связи и информатики, к.т.н., доцент, Москва, Россия
i.v.vlasiuk@mtuci.ru

Жабицкая Александра Павловна
Московский технический университет связи и информатики, студент, Москва, Россия
AlexandraZhabitskaya@yandex.ru

Пантелеева Юлия Валерьевна
Московский технический университет связи и информатики, студент, Москва, Россия
Julia.panteleeva01@yandex.ru

Аннотация
Длительная нагрузка на глаза, продолжительная эксплуатация гаджетов и смартфонов в совокупности с плохой экологией, постоянной усталостью и нехваткой сна негативно сказывается на здоровье глаз и приводит к ухудшению остроты зрения. Применение научных методов и технологий для мониторинга выполнения упражнений глазной гимнастики может способствовать более точному и эффективному их выполнению, что, в свою очередь, приводит к более высоким результатам и благоприятно сказывается на здоровье глаз. Это сделает глазную гимнастику более доступной и результативной для множества людей.

Ключевые слова
Зрение, глазная гимнастика, мониторинг движения глаз, электроокулография, видеоокулография, айтрекинг

Введение

Доктор Уильям Бейтс, посвятивший 30 лет исследованию функционирования человеческого глаза, предположил, что снижение остроты зрения напрямую связано с нарушением работы глазодвигательных мышц. Согласно его теории, близорукость возникает из-за хронического перенапряжения косых мышц глаза, в то время как дальнозоркость – результат чрезмерного напряжения прямых мышц.

Регулярная глазная гимнастика – действенный профилактический метод, способствующий сохранению здоровья глаз и снижающий риск развития офтальмологических патологий на протяжении всей жизни. Этот щадящий подход к поддержанию зрения показан практически всем, за исключением пациентов с острым конъюнктивитом или в послеоперационном периоде после офтальмологических вмешательств.

Целенаправленные упражнения решают ряд важных задач: снижают зрительное утомление после длительной работы за компьютером или другими устройствами, укрепляют глазодвигательные мышцы, улучшают кровообращение и снабжение тканей кислородом, уменьшают отёчность и стимулируют работу слезных желёз [1].

Методики гимнастики для глаз

Методики гимнастики для глаз имеют свои особенности:

1. Методика Аветисова состоит из трех групп упражнений. Первая помогает улучшить кровообращение глаз и циркуляцию слезной жидкости. Вторая группа укрепляет глазодвигательные мышцы, а третья тренирует аккомодацию
2. Методика Бейтса направлена на расслабление и тренировку глазных мышц. В работе участвуют только глаза, голова остается неподвижна. После каждого упражнения нужно устраивать глазам отдых, легко моргая в течение 3-5 секунд.
3. Методика Норбекова основана на положительном настрое и рефлекторном стимулировании определенных участков внутренних органов. Комплекс вначале проводят с открытыми глазами, а затем повторяют упражнения мысленно, прикрыв веки.
4. Методика Жданова предполагает ежедневное выполнение специальных упражнений и ведение дневника. Ученый утверждает, что при соблюдении этих условий уже через семь дней зрительная система восстановит свои функции и человек сможет отказаться от очков и контактных линз [2].

Наукометрический анализ

Наукометрический анализ методик гимнастики для глаз, предложенных Аветисовым, Бейтсом, Норбековым и Ждановым.

1. Методика Аветисова

Существует ряд научных публикаций, связанных с именем Аветисова и его методикой, в основном в российских и советских офтальмологических журналах.

Оценка цитируемостии: работы Аветисова активно цитируются в российских и русскоязычных публикациях по детской офтальмологии и профилактике близорукости. В международных базах данных цитируемость может быть менее выраженной.

Методология: исследования, проводимые Аветисовым и его последователями, обычно имеют чёткую методологическую базу, включая контролируемые исследования с использованием объективных методов оценки зрительных функций.

Эффективность: существуют научные данные, подтверждающие эффективность методики Аветисова для профилактики и замедления прогрессирования близорукости у детей, а также улучшения аккомодационной функции. Метод признан в российском научном сообществе.

2. Методика Бейтса

Основной массив публикаций, относящихся к методу Бейтса, приходится на начало и середину 20-го века. Современные работы, как правило, критические или носят описательный характер.

Оценка цитируемостии: работы Бейтса цитируются, но их научная ценность оспаривается, и цитирования в основном происходят в работах, критикующих этот подход.

Методология: исследования, посвящённые методу Бейтса, чаще всего имеют слабый методологический дизайн, они не являются контролируемыми, не имеют слепой оценки и часто используют маленькие выборки.

Эффективность: современные научные исследования не подтверждают эффективность метода Бейтса для лечения нарушений зрения. Метод часто считается псевдонаучным.

3. Методика Норбекова

Крайне мало научных публикаций в рецензируемых журналах, посвящённых методике Норбекова. Публикации в основном представлены в форме отзывов и отчётов о практике.

Оценка цитируемости: работы по методике Норбекова практически не цитируются в научной литературе.

Методология: исследования отсутствуют или имеют очень слабую методологическую базу. Часто исследования носят описательный характер и не являются контролируемыми.

Эффективность: научные доказательства эффективности методики Норбекова отсутствуют или являются очень слабыми. Результаты часто объясняются эффектом плацебо.

4. Методика Жданова

Аналогично методике Бейтса, научных публикаций в рецензируемых журналах, посвящённых непосредственно методу Жданова, практически нет.

Оценка цитируемости: работы, связанные с методом Жданова, не цитируются в научной литературе.

Методология: исследования, подтверждающие эффективность метода Жданова, не опубликованы в рецензируемых научных журналах. Основная масса источников является неформальной.

Эффективность: нет научных доказательств, подтверждающих эффективность методики Жданова. Метод основан на псевдонаучных концепциях.

Сравнение и выводы:

Методика Аветисова является единственной из рассмотренных, которая имеет научное обоснование и признание в российском офтальмологическом сообществе. Она основана на физиологических принципах и имеет подтверждение своей эффективности в ряде исследований. Методики Бейтса, Норбекова и Жданова не имеют научного обоснования и их эффективность не подтверждена научными исследованиями. Эти методы часто основаны на псевдонаучных концепциях. При разработке программно-аппаратного комплекса для коррекции зрения следует отдавать предпочтение научно обоснованным методикам, таким как методика Аветисова, а не псевдонаучным подходам, основанным на недоказанных предположениях [3].

Методы регистрации движений глаз

Методы регистрации движений глаз подразделяются на две основные категории: инвазивные и неинвазивные.

Инвазивные методы предполагают непосредственный контакт датчиков с глазом или его окрестностями, датчики устанавливаются прямо на роговицу глаза и вокруг него, например, электроокулография, фотооптические и электромагнитные методики.

Неинвазивные методы, в свою очередь, основаны на дистанционном измерении, и включают в себя фотоэлектрические и видеорегистрационные технологии.

Электроокулография

Метод основан на измерении собственного электрического поля глаза, представляющего собой диполь с положительным потенциалом на уровне роговицы относительно отрицательного потенциала сетчатки. Электрическая ось этого диполя приблизительно совпадает с оптической осью глаза, позволяя использовать её в качестве индикатора направления взгляда.

Изменения потенциала между роговицей и сетчаткой регистрируются посредством измерения электрической активности в приорбитальных тканях (вокруг глазницы). Для этого используются электроды, расположенные крестообразно вокруг глазницы, фиксирующие изменения потенциала, вызванные движениями глазного яблока.

Рис. 1. Электроокулография (установка электродов при регистрации электроокулограммы)

Преимуществами метода является высокая чувствительность и точность, так как ЭОГ способна регистрировать даже очень мелкие и быстрые движения глаз, которые могут быть неразличимы даже при визуальном наблюдении. Точное отслеживание не только горизонтальных и вертикальных движений, но и торсионных движения (вращение глаза).

Также преимуществом является возможность регистрации скрытых движений глаз, ЭОГ может регистрировать движения глаз, происходящие при закрытых веках, что может быть полезно для оценки некоторых упражнений. Метод может выявить микросаккады (небольшие, быстрые непроизвольные движения глаз), которые могут быть важными при оценке усталости или концентрации внимания.

К недостаткам метода можно отнести инвазивность, это значит, что для проведения ЭОГ необходимо прикрепление электродов к коже вокруг глаз, что может вызвать дискомфорт или раздражение у некоторых пользователей. А также то, что процедура ЭОГ требует тщательной подготовки кожи, чтобы обеспечить хороший контакт электродов.

Еще одним недостатком является чувствительность к артефактам и ограничения в мобильности: данные ЭОГ могут быть искажены из-за мышечной активности вокруг глаз, движения головы. ЭОГ может быть сложно использовать в условиях, когда требуется мобильность или свобода движений.

Все это сопровождается сложностью и высокой стоимостью оборудования, так как оно является более сложным, чем оборудование для визуального наблюдения или айтрекинга на основе камеры.

Таким образом, ЭОГ является мощным инструментом для точной и объективной оценки движений глаз, и теоретически может быть использована для контроля упражнений глазной гимнастики. Однако, практическое применение ЭОГ в этой области ограничено её инвазивностью, сложностью, высокой стоимостью и наличием артефактов. ЭОГ больше подходит для научных исследований, чем для массового применения в домашних или клинических условиях.

Фотооптический и электромагнитный методы

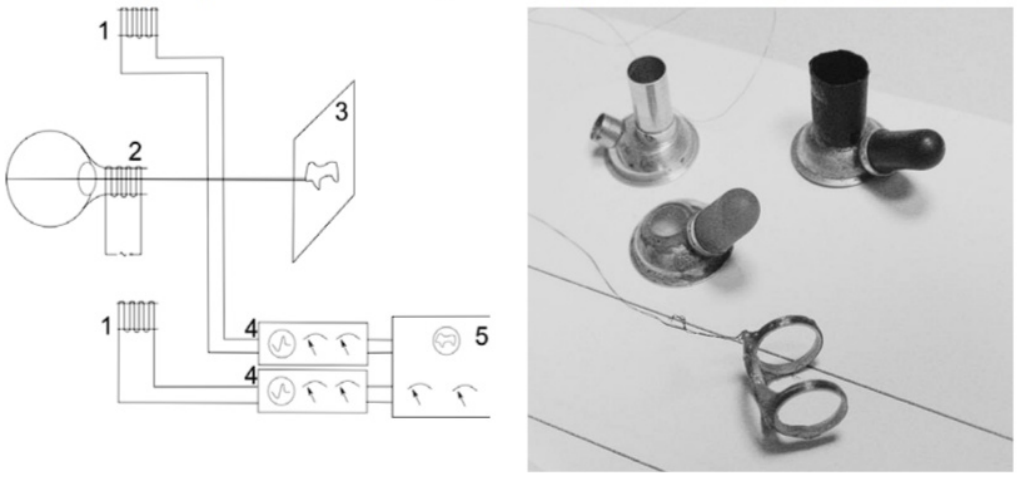
Фотооптический метод.

Разработанный А.Л. Ярбусом в середине XX века фотооптический метод основывался на регистрации отражения узкого светового пучка от миниатюрного зеркала, прикреплённого к глазу. Сигналы регистрировались фотоприёмником.

Несмотря на высокое пространственное разрешение, метод требовал жёсткой фиксации головы, был контактным и применялся только в условиях затемнённого помещения. В настоящее время он вытеснен контактными электромагнитными методами, обеспечивающими сопоставимую точность, но обладающими большей практической удобностью.

Электромагнитный метод.

Разработка электромагнитного метода регистрации движений глаз произошла независимо в США и СССР в 1960-х годах. Принцип метода основан на детектировании изменений электромагнитного поля, возникающих при изменении расстояния между излучателем (крепящимся к глазу с помощью присоски, контактной линзы или кольца) и неподвижными приёмными катушками, расположенными вокруг головы испытуемого. В некоторых модификациях на излучатель устанавливались оптические элементы для обработки изображения. Метод характеризуется исключительно высокой точностью (разрешение до 0.0002° в современных системах, таких как CS681 от Primelec, с частотой регистрации до 8000 Гц), однако остаётся контактным методом [4].



а б

Рис. 2. а – схема установки для электромагнитного метода; б – присоски и излучатель

Достоинством фотооптического метода является высокая разрешающая способность, для своего времени обеспечивал относительно высокую точность измерения угловых перемещений глаза.

К недостаткам относится жесткая фиксация головы, это крайне неудобно для выполнения любых упражнений глазной гимнастики, требующих естественных движений. Фиксация головы нарушает естественность движений и снижает достоверность данных.

Помимо этого, контактный характер, так как установка миниатюрного зеркальца на глазном яблоке – инвазивная процедура, неудобная и потенциально опасная. Ограничение на условия проведения измерений также сильно сужает возможности использования метода.

Преимущества электромагнитного метода: высокая разрешающая способность, а именно высокая точность измерения угловых перемещений, а также высокая частота регистрации, так как современные реализации (например, CS681) позволяют регистрировать движения с очень высокой частотой, что может быть полезным для анализа быстрых движений глаз.

К недостаткам можно отнести контактный характер, несмотря на то что метод не такой инвазивный, как фотооптический, установка излучателя находится на глазном яблоке, что может вызывать дискомфорт и раздражение.

Крепление элементов вокруг головы ограничивает свободу движений. Это критично для выполнения упражнений глазной гимнастики.

Электромагнитные системы являются дорогостоящими и требуют специальной подготовки для использования, что также является недостатком.

Оба метода, фотооптический и электромагнитный (в их классических реализациях), абсолютно непригодны для использования в системах контроля выполнения упражнений глазной гимнастики из-за их контактного характера и ограничений свободы движений. Современные методы отслеживания взгляда (видео-окулография на основе обычных или инфракрасных камер) обеспечивают значительно больше удобства и свободы движений, сохраняя при этом достаточно высокую точность.

Фотоэлектрический метод

Фотоэлектрические методы регистрации движений глаз используют преобразование отражённого от роговицы инфракрасного излучения в электрический сигнал. Обычно применялась схема с фотодиодами или фоторезисторами, установленными на очковой оправе и объединёнными по мостовой схеме. Известный с начала 1960-х годов, этот метод в настоящее время практически не применяется из-за появления более совершенных технологий [4].

Рис. 3. Установка для фотоэлектрического метода

Преимуществом метода является стоимость, так как использование простых фотодиодов и минималистичной электроники может сделать такую систему сравнительно недорогой, а также простота реализации, так как простая система может быть сравнительно легко разработана и реализована.

Несмотря на достоинства, данный метод также сопровождается рядом недостатков. Точность измерения положения зрачка будет сильно ограничена. Фотодиоды не обеспечивают достаточно высокой разрешающей способности для точного отслеживания движений глаз.

Чувствительность к внешним факторам, таким как освещенность окружающей среды, отражения, тени, изменение расстояния до источника света – все это будет сильно влиять на точность измерений.

Еще один недостаток – ограниченная функциональность, такая система сможет отслеживать только очень грубые движения глаз. Она не подойдет для отслеживания быстрых движений, саккад или других тонких параметров.

Неудобство в использовании и недостаток обратной связи также минусы этой системы, она потребует точной настройки и не будет удобной для использования при выполнении глазной гимнастики. Система, основанная только на фотодиодах, вряд ли сможет обеспечить достаточный уровень обратной связи для пользователя.

В общем, фотоэлектрическая система, основанная на использовании только фотодиодов, является крайне неэффективной и непрактичной для контроля выполнения упражнений глазной гимнастики. Современные методы, такие как видеоокулография (ВОГ) с использованием камер и айтрекинг с инфракрасным излучением, значительно превосходят по точности, удобству использования и функциональности.

Видеоокулография

Методы кино- и видеорегистрации движений глаз, известные с середины 1960-х годов, раньше ограничивались высокой трудоёмкостью обработки данных. Распространение персональных компьютеров и цифровых видеокамер сделало видеорегистрацию широкодоступной. В современных системах используется инфракрасный источник подсветки и высокоскоростная ИК-камера. Положение и размеры зрачка (представляющего собой тёмное пятно в инфракрасном диапазоне) и роговичного рефлекса определяются программным обеспечением. Направление взгляда рассчитывается на основе вектора, соединяющего центр зрачка и точку роговичного рефлекса.

Бесконтактный характер и возможность одновременной регистрации диаметра зрачка являются преимуществами видеорегистрации движений глаз. Однако, метод имеет ограничения: невозможность точного определения направления взгляда при частичном перекрытии зрачка ресницами или при наличии паразитного инфракрасного излучения (например, яркого солнечного света). Повышение временного и пространственного разрешения требует использования дорогостоящих высокоскоростных видеокамер высокого разрешения. Хотя слежение за уникальными паттернами радужной оболочки потенциально позволяет регистрировать торсионные (вращательные) движения глаз, практическая реализация требует дальнейшего совершенствования как качества видеокамер, так и вычислительных мощностей.

Рис. 4. Схема работы ИК-камеры [5]

Видеоокулография обладает рядом преимуществ:

Высокая точность метода благодаря ИК-системам, особенно высококачественным, которые могут обеспечить высокую точность отслеживания движений глаз. Они способны регистрировать даже очень быстрые движения (саккады) и микросаккады, что важно для анализа различных параметров зрительной функции.

В отличие от электроокулографии (ЭОГ) или механических методов, ИК-системы не требуют контакта с глазом или фиксации головы, а следовательно, неинвазивны. Это обеспечивает комфорт пользователя и свободу движений, необходимых для выполнения глазной гимнастики.

Относительно высокая скорость отслеживания, современные ИК-системы способны отслеживать движения глаз с высокой частотой, что позволяет анализировать динамику выполнения упражнений.

Возможность удаленного мониторинга, в зависимости от типа системы, ИК-трекер может быть размещен на некотором расстоянии от пользователя, что обеспечивает большую свободу движений.

Большинство ИК-систем предоставляют визуализацию данных о движении глаз в реальном времени, что позволяет пользователю и специалисту наблюдать за выполнением упражнений и получать обратную связь.

Данные, полученные с помощью ИК-айтрекеров, легко интегрируются с другими системами и программным обеспечением.

Несмотря на все преимущества, обозначим ряд недостатков:

Высококачественные ИК-айтрекеры могут быть довольно дорогими, что ограничивает их доступность, стоимость является недостатком.

Необходимость калибровки перед каждым использованием, что может занять некоторое время. Неправильная калибровка может значительно снизить точность измерений.

Влияние внешних факторов, таких как сильное освещение, блики, отражения могут негативно влиять на точность отслеживания. Необходимо обеспечить оптимальные условия освещения.

Зависимость от программного обеспечения: функциональность и точность ИК-системы сильно зависят от качества используемого ПО для обработки данных.

Таким образом, ИК-айтрекеры представляют собой наиболее подходящий вариант для контроля выполнения упражнений глазной гимнастики среди существующих технологий отслеживания взгляда. Они обеспечивают хороший баланс между точностью, неинвазивностью, удобством использования и доступностью. Однако, при выборе системы необходимо учитывать её стоимость, необходимость калибровки, влияние внешних факторов и ограничения по типу упражнений. Выбор конкретной системы зависит от требований к точности, бюджета и условий использования.

Айтрекинг-системы на основе веб-камер

Этот метод использует стандартную веб-камеру для отслеживания положения глаз, не требуя специального оборудования. Однако, его существенным недостатком является низкая точность и, как следствие, невысокое качество получаемых данных.

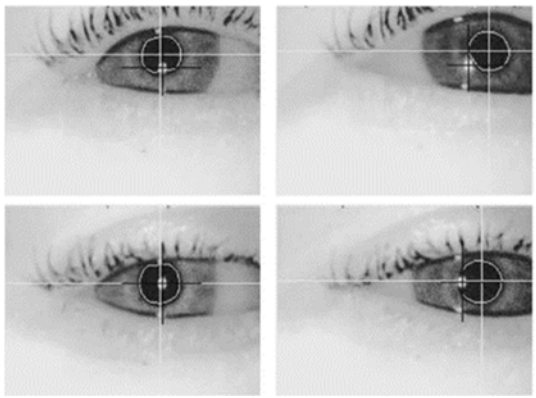


Рис. 5. Мониторинг расположения центра зрачка и роговичного блика

К преимуществам метода относится низкая стоимость, исходя из того, что веб-камеры значительно дешевле специализированных айтрекеров. Это делает технологию доступной для большего круга пользователей, включая домашнее использование и небольшие клиники.

А также простота, так как установка и использование, как правило, проще, чем у профессиональных систем. Многие программы работают "из коробки" и требуют минимальной настройки.

Портативность, а именно возможность использования практически везде, где есть веб-камера и компьютер. Это удобно для выполнения упражнений в разных местах.

Система не требует физического контакта с глазом, является неинвазивной, что делает её комфортной для пользователя.

Возможность интеграции с другими приложениями также является преимуществом, данные с веб-камеры можно использовать в сочетании с другими приложениями для анализа данных.

К недостаткам мы можем отнести меньшую точность по сравнению со специализированными айтрекинговыми системами, точность веб-камер существенно ниже. Это может приводить к ошибкам в измерении движений глаз, особенно при быстрых или мелких движениях, что критично для некоторых упражнений.

Влияние внешних факторов также негативно сказывается на работе утройства: качество отслеживания сильно зависит от освещения, расстояния до камеры, наличия бликов и других внешних факторов. Даже небольшие изменения могут существенно повлиять на результаты.

Веб-камеры обычно не могут отслеживать все параметры движений глаз, которые важны для оценки эффективности глазной гимнастики, поэтому к недостаткам можно отнести ограниченные возможности.

Калибровка может быть сложной и требовать нескольких попыток, чтобы обеспечить приемлемую точность, а результат калибровки может быть нестабильным.

Зависимость качества отслеживания от качества веб-камеры также скорее относится к недостаткам. Дешевые веб-камеры будут давать менее точные результаты. Также моргание глаз сильно влияет на точность отслеживания и может приводить к пропускам данных.

Исходя из этого, веб-камеры могут быть полезны для базового мониторинга выполнения некоторых упражнений глазной гимнастики, особенно в ситуациях, где высокая точность не является критичной. Однако для точных измерений и анализа сложных движений глаз лучше использовать специализированные айтрекинг-системы.

Методы настройки, калибровки и проверки

Современные системы отслеживания взгляда обычно требуют минимальной настройки. Процессы обнаружения зрачка и рефлексов от роговицы, а также подавления артефактов, автоматизированы и постоянно калибруются. Эти системы демонстрируют хорошую адаптивность к различным цветам глаз, их размерам, форме и межзрачковому расстоянию.

Для проведения исследования испытуемый должен находиться в пределах поля зрения камеры. В случае использования очков с функцией отслеживания взгляда, устройств дополненной (AR) или виртуальной (VR) реальности, либо головных креплений, камера устанавливается на самом испытуемом. Экспериментальная процедура должна быть разработана таким образом, чтобы обеспечить постоянное нахождение испытуемого в поле зрения камеры и исключить любые факторы, затрудняющие процесс отслеживания.

Системы отслеживания взгляда требуют процедуры калибровки, алгоритмически сопоставляющей физическое положение глаза с точкой фиксации взгляда. Эта необходимость обусловлена индивидуальными анатомическими вариациями (размер глаз, положение центральной ямки сетчатки и т.д.), влияющими на точность измерений. Процесс калибровки обычно включает фиксацию взгляда на заранее определённых точках, отображаемых на экране (для систем экранного трекинга) или расположенных в окружающем пространстве (для очков с функцией отслеживания взгляда). Таким образом, калибровка учитывает субъективное восприятие участника.

Процедура калибровки может использовать одну центральную точку, хотя чаще применяется от 5 до 13 точек. Алгоритм системы вычисляет математическое соответствие между положением глаза (с учётом роговичного рефлекса) и направлением взгляда для каждой точки калибровки, создавая затем матрицу преобразования для всей калибровочной области. Увеличение числа точек калибровки обеспечивает более высокую и равномерную точность по всему полю зрения системы. Однако, точность снижается при отклонении взгляда за пределы области, охватываемой точками калибровки.

Передовые системы отслеживания взгляда способны к самокалибровке, создавая сложные модели глаза и пассивно определяя индивидуальные параметры. Калибровка может осуществляться и без активного участия испытуемого, путем определения направления взгляда на основе анализа изображений, "маскируя" калибровочные точки в других визуальных данных.

Наконец, некоторые устройства, например, медицинские приборы для оценки вестибуло-окулярного рефлекса или системы контроля усталости, вообще не требуют калибровки, извлекая необходимую информацию из исходного положения зрачка [6].

Типы айтрекинг-устройств

Системы отслеживания взгляда (айтрекинг) можно классифицировать по четырем основным типам: системы с фиксацией головы, удаленные системы, мобильные (надеваемые на голову) и встроенные (интегрированные в другие устройства) системы.

1. Отслеживание глаз с фиксацией головы.

Системы отслеживания взгляда с фиксацией головы – высокоточные исследовательские инструменты, применяемые преимущественно в нейрофизиологии и офтальмологии, где точность измерений приоритетнее комфорта испытуемого. Фиксация головы осуществляется с помощью подголовников или прикусных планок. Такой подход обеспечивает уровень точности и временное разрешение, недостижимые другими методами, позволяя проводить детальный анализ быстрых движений глаз.

2. Удаленное отслеживание глаз.

Дистанционные системы отслеживания взгляда осуществляют мониторинг в пределах ограниченной зоны, часто представляющей собой экран компьютера. Эти бесконтактные системы, часто устанавливаемые на мониторе, автоматически компенсируют небольшие изменения положения головы пользователя. Они позволяют регистрировать естественные движения глаз и являются единственно возможным решением для отслеживания взгляда у младенцев или пациентов, не способных использовать головные крепления.

3. Мобильное отслеживание глаз.

Мобильные системы отслеживания взгляда, часто выполненные в виде очков с несколькими камерами, позволяют регистрировать движения глаз в широком поле зрения в реальном времени. Камеры, расположенные в поле зрения пользователя, фиксируют положение глаз и сетчатки, в то время как другие камеры регистрируют окружающее пространство. Эти системы находят применение в

различных областях: спорте, исследованиях водительского поведения, навигации, социальной психологии, анализе зрительно-моторной координации, тестировании мобильных устройств и других.

4. Интегрированные или встроенные системы

Встроенные системы отслеживания взгляда интегрируются в другие технологии, например, в хирургические инструменты для офтальмологических операций или системы автофокусировки камер, ориентирующиеся на положение взгляда в видоискателе. Наиболее масштабное применение наблюдается в технологиях дополненной (AR) и виртуальной (VR) реальности [11-18]. В VR-системах айтрекинг оптимизирует производительность, фокусируя ресурсы на область прямого взгляда и снижая разрешение периферического изображения.

Преимущества и недостатки

1. Системы отслеживания глаз со стабилизацией головы:

Плюсы:

Обеспечение самой высокой точностью из всех типов айтрекеров, а также высокое временное разрешение, они позволяют регистрировать быстрые движения глаз с высокой частотой.

Минусы:

Фиксация головы делает использование неудобным и ограничивает естественные движения, что делает их непригодными для контроля глазной гимнастики. Система полностью исключает возможность использования для упражнений, требующих свободы движений головы.

2. Удаленное отслеживание глаз:

Плюсы:

Не требует никакой фиксации на голове пользователя (бесконтактное), обеспечивая комфорт и свободу движений. Подходит для динамических упражнений, а следовательно, позволяет отслеживать движения глаз во время выполнения упражнений глазной гимнастики. Относительно простые в установке и использовании, а также подходит для детей и пациентов с ограниченными возможностями: это единственный вариант для таких категорий пользователей.

Минусы:

Ограниченная область отслеживания, система точно отслеживает взгляд только в пределах поля зрения камеры, обычно на экране монитора. Движения глаз вне этой зоны не регистрируются. Меньшая точность, чем у систем со стабилизацией головы, а также влияние окружающего освещения на качество отслеживания.

3. Мобильное отслеживание глаз (очки):

Плюсы:

Отслеживают движения глаз в широком поле зрения. Полная свобода движений. Подходит для различных сценариев: подходят для многих видов активности, включая исследование в области спорта, вождения, и т.д.

Минусы:

Высокая стоимость. Сложность в использовании, а именно более сложные в установке и калибровке, чем удалённые системы. Ношение специальных очков может быть неудобно для длительных сеансов глазной гимнастики.

4. Интегрированные системы:

Плюсы:

Позволяют интегрировать отслеживание взгляда в другие устройства или приложения (возможность интеграции).

Минусы:

Подходят только для очень специфических задач и не являются универсальными решениями для контроля глазной гимнастики (специализированные).

Исходя из проведенного анализа можно сделать выбор лучшей системы для контроля глазной гимнастики. Для контроля выполнения упражнений глазной гимнастики удаленное отслеживание глаз является наиболее подходящим вариантом. Хотя точность может быть немного ниже, чем у систем со стабилизацией головы, это компенсируется комфортом и свободой движений, которые являются критичными для выполнения упражнений. Более того, удаленное отслеживание позволяет наблюдать за движениями глаз во время выполнения упражнений, а не просто фиксировать точки фиксации. Важно отметить, что качество контроля также будет зависеть от программного обеспечения, которое обрабатывает данные, полученные от айтрекера. Программное обеспечение должно быть способно не только

регистрировать движения глаз, но и анализировать их, сравнивать с эталонами и предоставлять обратную связь пользователю [8].

Характеристики приборов

Приборы для регистрации движения глаз характеризуются рядом ключевых параметров.

1. Частота регистрации (sampling rate): определяет количество измерений положения глаз в секунду. Для видеосистем она варьируется от 30 до 2000 Гц, электромагнитные системы достигают 8000 Гц, а инфракрасные – около 1000 Гц. Высокая частота необходима для точного анализа быстрых движений глаз, характерных для многих упражнений глазной гимнастики, включая саккады и гладкие преследования. Для оценки динамики выполнения упражнений, особенно высокоскоростных, необходима частота не ниже 500 Гц.

2. Точность (accuracy): измеряется в угловых градусах и представляет собой отклонение измеренного положения от реального. Для объективной оценки выполнения упражнений глазной гимнастики, требующих точности фиксации взгляда, необходима точность не хуже 0.5 градуса. Более низкая точность может приводить к искажению результатов, особенно при оценке выполнения упражнений на малых амплитудах.

3. Стабильность (precision): определяет воспроизводимость результатов измерения. Вычисляется как среднеквадратичное отклонение последовательных измерений. Значение стабильности должно быть как можно меньше. Высокая стабильность важна для исключения погрешностей, вызванных шумами системы, позволяя достоверно оценить изменения в движениях глаз в ходе выполнения упражнений.

4. Поле охвата: определяет угол обзора, доступный для отслеживания. Средние значения составляют 80 градусов по горизонтали и 60 по вертикали. Для некоторых упражнений глазной гимнастики может потребоваться более широкое поле охвата для регистрации полных траекторий движения глаз.

Выбор системы определяется задачами исследования. Дистанционные системы, удобные для изучения чтения, достигают частоты 2000 Гц с фиксацией головы и 500 Гц без неё. Для мобильных исследований подходят системы в виде очков (до 220 Гц) или шлемов (до 400 Гц), однако, они сложнее в настройке и обработке данных, особенно при учете торсионных движений глаз. Для анализа упражнений глазной гимнастики важна балансировка между точностью, частотой регистрации и полем охвата, причем выбор частоты зависит от скорости выполняемых движений глаз [9].

Заключение

Инфракрасные трекеры представляют собой оптимальный инструмент для контроля выполнения упражнений глазной гимнастики. Сочетание высокой точности, комфорта, простоты использования и высокой частоты регистрации делает их незаменимыми как для исследовательских целей, так и для личного использования в рамках домашних тренировок. Инфракрасные трекеры открывают новые возможности для оптимизации глазной гимнастики и достижения максимального терапевтического эффекта [10].

Рассмотрим применение в разных типах упражнений. Инфракрасные трекеры отлично подходят для контроля выполнения различных упражнений глазной гимнастики, независимо от их сложности. В качестве примеров приведем самые популярные:

Упражнения на фиксацию взгляда. Трекер точно зафиксирует, насколько долго и точно пользователь может удерживать взгляд на конкретной точке. Это особенно важно для тренировки аккомодации и конвергенции.

Упражнения на слежение. Система позволит отслеживать плавность и точность слежения взгляда за движущимся объектом, помогая определить наличие и степень нарушения глазодвигательных функций.

Упражнения на расслабление глазных мышц. Анализ данных, полученных с помощью инфракрасного трекера, поможет оценить степень расслабления глазных мышц после выполнения упражнения, сравнивая показатели частоты микродвижений глаз до и после тренировки.

Комплексные упражнения. Инфракрасный трекер позволяет анализировать сложные последовательности движений глаз, характерные для многих комплексных упражнений, что позволяет оценить эффективность всей программы в целом.

Современные инфракрасные системы часто интегрируются с программным обеспечением, которое визуализирует данные в удобном для пользователя формате. Это позволяет не только отслеживать движения глаз в реальном времени, но и анализировать полученные данные в последующем, создавая графики, отчеты и другие визуализации, что позволяет отслеживать динамику прогресса и эффективность тренировок. Развитие технологий инфракрасного трекинга открывает новые возможности для персонализации глазной гимнастики.

Литература

1. *Пьянзина Н.Н., Колесникова О.Б., Эриванова С.А.* Физические упражнения и гимнастика для глаз как средство коррекции зрения студентов вуза // Известия Тульского государственного университета. Физическая культура. Тула, 2021.

2. Пальминг для глаз: что это такое, методы выполнения по Норбекову, Бейтсу, Жданову. URL: https://center-dental-clinic.com/articles/palming-dlya-glaz-chto-eto-takoe-metody-vypolneniya-po-norbekovu-bejtsu-zhdanovu (дата обращения 15.01.2024).

3. *Локтинова Ю.И., Савкина Н.В.* Обзор научных публикаций о пользе занятий физической культурой при заболеваниях зрительного аппарата // Наука-2020: Физическая культура и спорт: наука, практика, образование, 2019 №7.

4. *Фазылзянова Г.И., Балалов В.В.* Айтрекинг: когнитивные технологии в визуальной культуре // Вестник российских университетов. Математика, 2014 №2.

5. *Третьякова В.М., Рыбанов А.А.* Анализ применения технологии Ай-трекинга // Современные научные исследования и инновации, 2016 № 7.

6. Айтрекинг. https://cmi.to/%D0%B0%D0%B9%D1%82%D1%80%D0%B5%D0%BA%D0%B8%D0%BD%D0%B3/ (дата обращения 15.01.2024).

7. *Барабанщиков В.А., Жегалло А.В.* Айтрекинг: Методы регистрации движений глаз в психологических исследованиях и практике. М.: Когито-Центр, Москва, 2014. 128 с.

8. *Фарахутдинов Ш.Ф., Панова А.В.* Айтрекинг в маркетинговых и социологических исследованиях // Социология, 2019 №5.

9. *Черниговская Т.В., Петрова Т.Е.* Взгляд кота Шрёдингера: регистрация движений глаз в психолингвистических исследованиях. 2-е изд. Санкт-Петербург: Санкт-Петербургский государственный университет, 2018. 228 с.

10. *Шанхоева Д.М., Самедова Э.Ш., Трегуб П.П.* Использование метода трекинга движения глаз для диагностики неврологических нарушений // Вестник новых медицинских технологий, 2024 №5.

11. *Ivanchev V.V., Vlasuyk I.V., Stroganova E.P.* Objective assessment of colours' warmth // T-Comm. 2024. Т. 18. № 1. С. 44-50.

12. *Степанов Н.С., Матуа Д.Д., Мазин В.А., Вотяков С.Ю., Винецкий В.В., Власюк И.В.* Анализ текущих алгоритмов вычисления области регионов интереса пользователей при потоковой передачи видеоконтента // T-Comm: Телекоммуникации и транспорт. 2023. Т. 17. № 2. С. 27-32.

13. *Власюк И.В., Узеев А.А., Пахомова Е.А.* Исследование методов коррекции изображений с расширенным динамическим диапазоном для воспроизведения на устройствах с ограниченными параметрами отображения // Телекоммуникации и информационные технологии. 2023. Т. 10. № 1. С. 135-144.

14. *Mozhaeva A., Vashenko E., Selivanov V., Potashnikov A., Vlasuyk I., Streeter L.* Analysis of current video databases for quality assessment // T-Comm. 2022. Т. 16. № 2. С. 48-56.

15. *Власюк И.В., Киселева А.С.* Анализ эффективности безреференсных метрик применительно к оценке качества видео при потоковой передаче // Телекоммуникации и информационные технологии. 2022. Т. 9. № 2. С. 65-74.

16. *Кремлева Э.А., Власюк И.В.* Оценка эффективности методов визуализации одноканальных изображений в условных цветах // Телекоммуникации и информационные технологии. 2021. Т. 8. № 1. С. 29-37.

17. *Valitskaya N.S., Vlasyuk I.V., Potashnikov A.M.* Video compression method on the basis of discrete wavelet transform for application in video information systems with non-standard parameters // T-Comm. 2020. Т. 14. № 3. С. 47-53.

18. *Поташников А.М., Власюк И.В.* Метод построения равноконтрастного цветового пространства для заданной системы отображения информации и условий контроля // T-Comm: Телекоммуникации и транспорт. 2020. Т. 14. № 4. С. 15-22.

АНАЛИЗ СПОСОБОВ ОРГАНИЗАЦИИ ТАБЛИЦЫ МАРШРУТИЗАЦИИ

Гадасин Денис Вадимович
МТУСИ, доцент кафедры СИТиС, к.т.н., Москва, Россия
dengadiplom@mail.ru

Шустов Сергей Александрович
МТУСИ, магистрант, Москва, Россия
sidious265@mail.ru

Калининский Даниил Сергеевич
МТУСИ, аспирант кафедры СИТиС, Москва, Россия
daniilblag28@mail.ru

Комкова Марина Георгиевна
МТУСИ, старший преподаватель кафедры СИТиС, Москва, Россия
m.g.komkova@mtuci.ru

Аннотация
Одной из важнейших задач в сетевых технологиях является маршрутизация трафика. Важной частью обеспечения эффективности маршрутизации является обеспечение низкой задержки. Поиск маршрута в таблице маршрутизации является важным аспектом обеспечения эффективности маршрутизации. Постоянный рост использования сетевых технологий, а также переход на новую версию интернет-протокола IPv6 негативно сказываются на производительности повсеместно используемых алгоритмов. В данной статье рассматриваются подходы к организации и хранению таблицы маршрутизации.

Ключевые слова
Динамическая маршрутизация, протокол маршрутизации, таблица маршрутизации, префиксное дерево, сжатое префиксное дерево, LC-дерево, Tree Bitmap

Введение

В современном мире информационные технологии и Интернет играют ключевую роль в жизни людей и деятельности организаций. Благодаря тому, что всё большее число людей и организаций начинает применять современные технологии в своей повседневной жизни, число подключенных к сети устройств постоянно растёт.

Одной из самых важных задач в сетевых технологиях является маршрутизация трафика. С ростом использования сетевых технологий, усложнением архитектуры современных сетевых приложений и сервисов, а также расширением инфраструктуры поставщиков сетевых услуг, растёт необходимость в новых средствах, позволяющих обеспечить должный уровень производительности для сетевого взаимодействия.

Важной частью обеспечения производительности является обеспечение низкой задержки маршрутизации. Одним из аспектов, влияющих на задержку маршрутизации, можно назвать организацию хранения таблицы маршрутизации, а также алгоритм поиска по этой таблице.

В связи с постоянным ростом использования сетевых технологий, таблицы маршрутизации также становятся больше. Помимо этого, одной из важных особенностей современных сетей является постепенный переход на новую версию интернет-протокола – IPv6. По сравнению с IPv4, где размер адресного пространства ограничен 232 = 4,294,967,296 адресами, при использовании IPv6 число адресов значительно возрастает, так как длина адреса в IPv6 также намного больше и составляет 128 бит.

Вышеперечисленные особенности негативно сказываются на производительности повсеместно применяемых алгоритмов поиска маршрута и методов хранения таблицы маршрутизации.

В данной статье рассмотрены подходы к организации и хранению таблицы маршрутизации, а также возможные улучшения данных подходов для обеспечения более быстрой и эффективной работы маршрутизатора в условиях растущих таблиц маршрутизации.

Таблица маршрутизации

Таблица маршрутизации – это структура данных, используемая маршрутизатором или другим сетевым устройством для хранения информации о возможных путях передачи пакетов данных по сети. Записи, содержащиеся в таблице маршрутизации, позволяют определить дальнейшее направление сетевого трафика в зависимости от адреса назначения [1-4].

В современных маршрутизаторах зачастую используется две или более таблицы маршрутизации – Routing Information Base – RIB – общая таблица, содержащая все маршруты и требующая соблюдения эффективности по памяти, и Forwarding Information Base – FIB – специальная таблица, компилируемая для дальнейшего использования Data plane для увеличения скорости поиска маршрутов и, как следствие, ускорения маршрутизации.

Для хранения RIB в общем случае может подойти любая структура данных, эффективная по памяти – списки, массивы, деревья и другие структуры, позволяющие хранить данные со сложностью по памяти O(n).

Для хранения FIB, в свою очередь, потребуется структура данных с возможностью быстрого поиска префикса.

Задача поиска LPM

Основной задачей в маршрутизации, связанной с поиском в таблице маршрутизации, является поиск «наиболее длинного совпадающего префикса» [5] (longest prefix match, LPM). Это связано с тем, что в контексте IP-адресации с помощью наиболее длинного совпадающего префикса можно добиться более специфичного указания маршрута.

Поскольку IP-адреса и их префиксы организованы иерархически, один и тот же адрес назначения может соответствовать нескольким префиксам, но более длинный префикс является более точным указанием на конкретную сеть или хост. Это позволяет избежать неопределенностей и отправить пакеты на правильный маршрут.

Помимо этого, когда маршрутизатор использует наиболее длинный совпадающий префикс, он минимизирует вероятность конфликта маршрутов и ошибок маршрутизации. Это особенно важно в сложных сетях, где могут быть перекрывающиеся или пересекающиеся адресные пространства. Пакеты всегда направляются по максимально конкретному маршруту, что позволяет избежать отправки пакетов в неправильное место.

Иерархическая структура IP-адресов подразумевает наличие вложенных префиксов разной длины. Например, у провайдера может быть выделен большой блок адресов, внутри которого разные организации или устройства получают свои подмножества адресов. Использование наиболее длинного совпадающего префикса позволяет корректно маршрутизировать трафик в таких случаях, направляя его к конкретной сети или устройству внутри общего блока адресов.

Алгоритм нахождения наиболее длинного совпадающего префикса выглядит следующим образом:

1) Инициализация переменной для хранения текущего наиболее длинного совпадающего префикса

2) Для каждой записи в таблице маршрутизации:

2.1) Извлечение маски сети и префикса текущей записи

2.2) Применение маски сети к IP-адресу назначения для получения сети назначения

2.3) Сравнение полученной сети назначения с префиксом текущей записи; если они совпадают и длина префикса больше, чем длина сохранённого префикса – обновить сохранённый префикс и маршрут.

3) После проверки всех записей в таблице маршрутизации наиболее длинный совпадающий префикс и соответствующий ему маршрут будут являться результатом поиска.

Данный алгоритм поиска LPM по таблице маршрутизации подразумевает использование любого стандартного вида списка, и имеет сложность O(n), где n – количество записей в таблице маршрутизации. Такой метод является рабочим, но абсолютно неэффективен ни в каких условиях, кроме очень малого числа записей, поскольку сложность поиска зависит от числа элементов. Сложность по памяти также O(n), поскольку данные хранятся в чистом виде. Алгоритмы вставки и удаления имеют временную сложность O(1), предполагая, что местоположение последнего префикса в списке известно.

Для поиска LPM в хэш-таблице можно использовать алгоритм поиска по длинам префиксов:

1) Префиксы хранятся в отдельных списках для каждой длины, ключом выступает длина префикса.

2) Процесс поиска для каждой длины префикса, начиная с самого длинного:

2.1) Производится бинарный поиск по списку,

2.2) Если такой префикс есть, то он выдаётся в качестве результата поиска.

3) В случае, если префикс не найден в списке для самой маленькой длины, выдаётся префикс по умолчанию.

Сложность такого поиска в худшем случае будет равна O(m*log n), где *m* – длина префикса, *n* – число элементов в списке для ключа длины. Возможно заменить списки на такие же хэш-таблицы, но в таком случае сложность в худшем случае будет равняться O(m) и помимо этого, требовать по лишней операции вычисления хэш-функции для каждой длины префикса. В зависимости от затрат ресурсов на хэш-функцию данный вариант может быть медленнее.

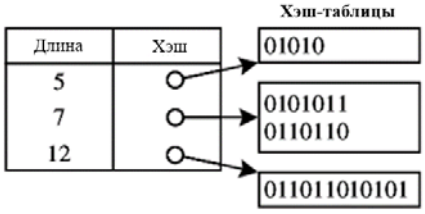


Рис. 1. Поиск по длинам префиксов в хэш-таблицах

В теории существует возможность производить поиск наиболее длинного совпадающего префикса с использованием бинарного поиска по длинам префиксов, но в таком случае основными проблемами для решения будут являться возвращение назад (backtracking) при неудачном поиске, и «направленность» бинарного поиска в таблице, где не прописаны для избыточности все возможные варианты префиксов. Эту проблему можно решить добавлением специальных маркеров и несколькими проходами бинарного поиска. В идеальном варианте таким образом можно добиться алгоритмической сложности поиска наибольшего совпадающего префикса O(log m), однако техническая реализация таких методов может быть затруднительной в реальных условиях.

Учитывая имеющуюся задачу, можно сказать, что префиксное дерево лучше подойдёт для применения в таблице маршрутизации, поскольку алгоритм для поиска LPM совпадает с алгоритмом поиска точного совпадения:

1) Начало алгоритма в корне дерева
2) Пока встречаются узлы, соответствующие битам адреса назначения, переходить по ним
3) В случае появления узла с совпадающим префиксом сохранить его как наилучший
4) После того, как пути закончились, или встречается несоответствие, прекратить поиск.

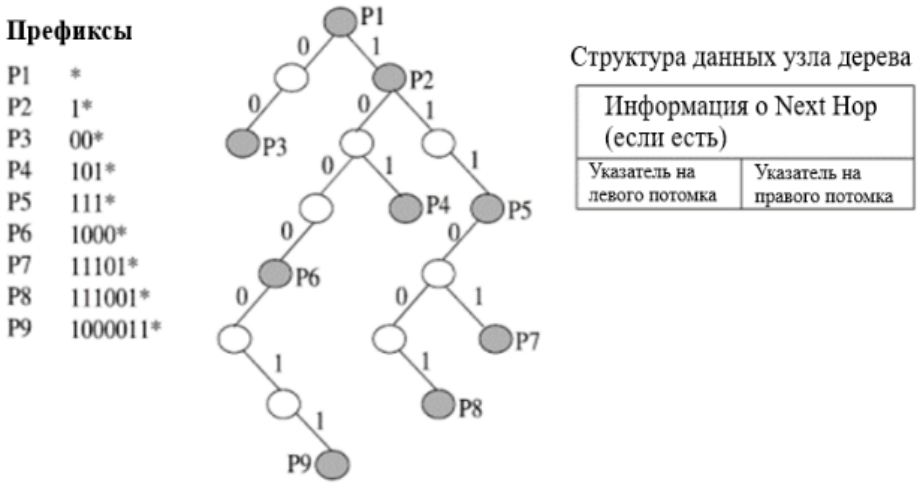


Рис. 2. Бинарное префиксное дерево

Данный алгоритм позволяет находить префикс максимальной длины за O(m), где *m* – длина префикса. По сути, эта сложность также является и гарантированной – она не зависит от числа элементов. Однако, обычное бинарное префиксное дерево без оптимизаций будет занимать много места за счёт того, что оно будет хранить все промежуточные узлы отдельно.

Протоколы IPv4 и IPv6

Internet Protocol v6 (IPv6) [6] – это более продвинутая версия интернет-протокола, которая имеет массу нововведений относительно своего предшественника.

Одним из главных отличий данных версий протокола является адресация. Протокол IPv4 [7] использует адреса длиной 32 бита, и этого адресного пространства хватает для выделения 232 = 4294967296 адресов. С учётом количества устройств, подключенных на текущий день к Интернету, данного адресного пространства явно недостаточно, из-за чего используются такие технологии, как NAT и Port Forwarding. IPv6, в свою очередь, обладает адресами длиной 128 бит, поэтому IP-адресов может быть выделено значительно больше. Из этого следует, что при использовании IPv6 узлам в сети не требуется использование NAT для выхода в глобальную сеть – поскольку не может возникнуть конфликтов адресации.

Статистически, наибольшее количество префиксов в Интернете для 32-битных адресов IPv4 приходится на диапазон длин 16-24, где подавляющее число префиксов имеют длину 24 (рис. 3). Данное явление объясняется тем, что префиксы короче 16 бит захватывают в себя слишком большую долю адресного пространства, а префиксы длиннее 24 слишком специфичны и поэтому не используются большей частью маршрутизаторов (кроме как для локальной маршрутизации) [8].

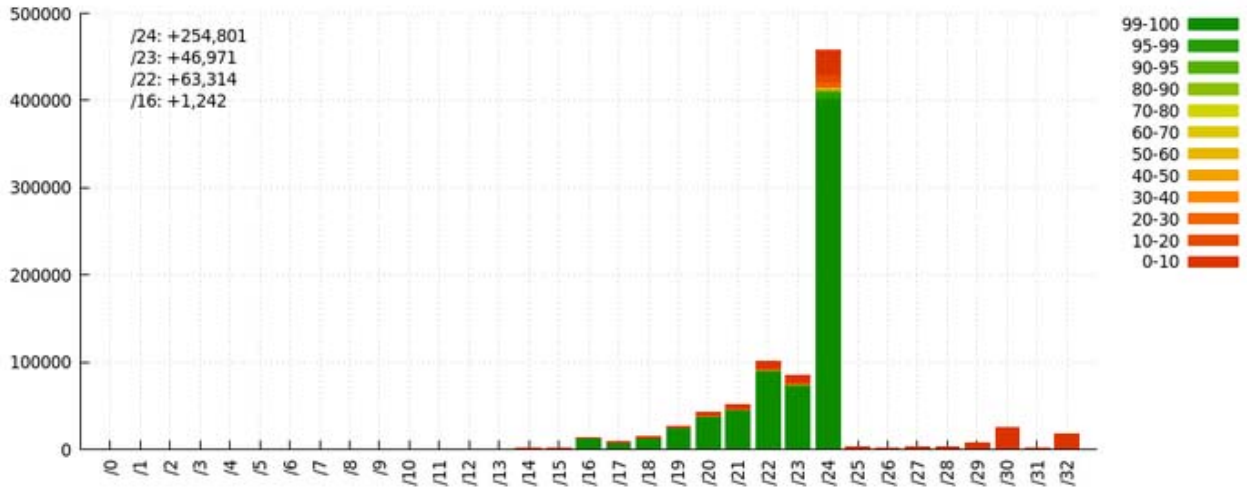


Рис. 3. Распределение префиксов по их длине для IPv4

Для IPv6 ситуация с распределением длин префиксов выглядит следующим образом (рис. 4):

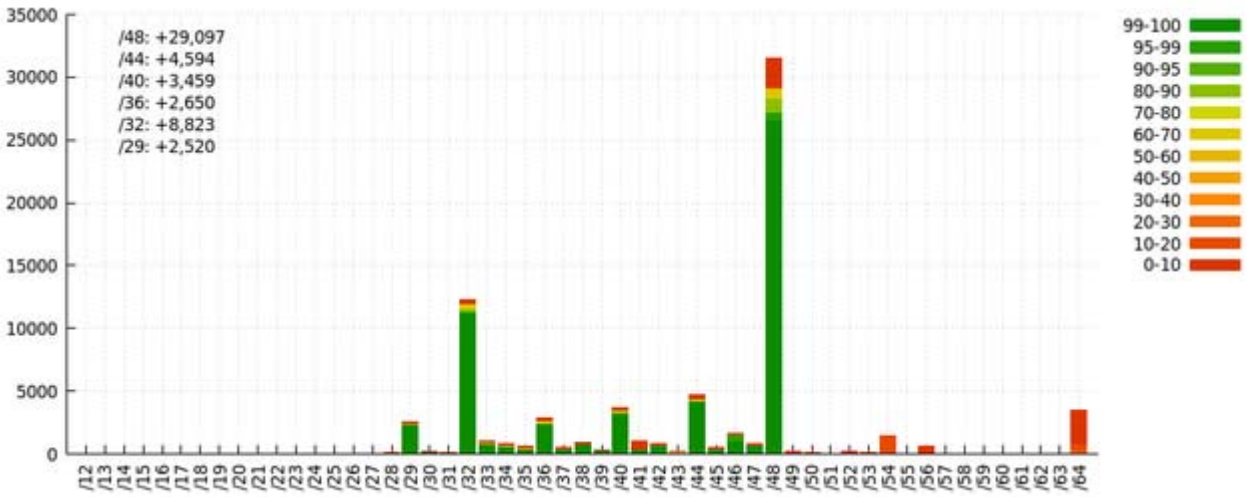


Рис. 4. Распределение префиксов по их длине для IPv6

Это распределение показывает, что чаще всего для определения сетей, видимых глобально, в IPv6 используются префиксы длиной от 32 до 48 бит. Это обусловлено тем, что /48 – маска сети, которая выдаётся провайдером для пользования организацией. Сеть с маской /48 позволяет создать внутри себя до 65536 сетей IPv6 с маской /64. Длина префикса от 12 до 23 приходится на региональных Интернет-регистраторов, от 24 до 32 – на провайдеров. Дополнительно стоит отметить сети с маской 29, которые приходятся на независящие от провайдера адресные пространства и корневые именные сервера.

Данные рассмотренных распределений показывают, что использование сжатого префиксного дерева, за счёт отсутствия или малого распространения префиксов определённой длины будет выгоднее, чем использование обычного бинарного префиксного дерева. Тем не менее, с учётом необходимости маршрутизации IPv6, где длина адреса составляет 128 бит, в отличие от 32 бит адреса IPv4, необходимо рассмотреть дополнительные варианты оптимизаций структуры дерева.

Модификации префиксного дерева для поиска LPM

Для оптимизации использования префиксного дерева в задаче поиска LPM были созданы различные его разновидности, в которых за счёт уменьшения глубины дерева достигается более быстрый поиск. [9-13] Эти разновидности включают в себя:

– Сжатое префиксное дерево (Patricia trie);

– LC-trie (Level Compressed trie);

– Tree Bitmap.

Сжатое префиксное дерево (Patricia Trie, также известный как Radix Trie) – это оптимизированное по пространству префиксное дерево, где каждый узел с одним потомком объединяется со своим потомком. Это сокращение узлов приводит к более компактному представлению дерева.

Вместо того чтобы хранить отдельные символы в каждом узле, сжатое префиксное дерево хранит целые префиксы во внутренних узлах, что значительно уменьшает глубину дерева. Каждая ячейка в дереве может представлять сразу несколько битов IP-адреса. На рисунке 5 представлен пример использования сжатого префиксного дерева для хранения префиксов. В нём представлены следующие префиксы:

Таблица 1

Пример префиксов

Обозначение	Префикс
A	000*
B	01*
C	10*
D	110*
E	111*
F	11001*

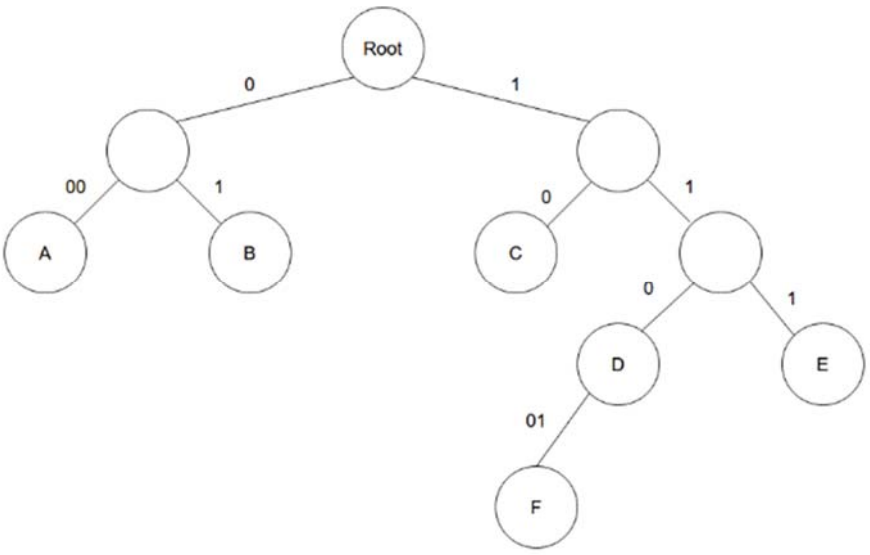


Рис. 5. Пример использования сжатого префиксного дерева

Для IP-адресов в таблице маршрутизации данный подход означает, что в дереве теперь будут оказываться только действительно существующие префиксы. Это может позволить сократить время на поиск более длинных префиксов в префиксном дереве, поскольку за один шаг теперь можно пройти больше 1 уровня дерева. Тем не менее, сжатое префиксное дерево при условии наличия большого количества префиксов с разной длиной (в худшем случае) может сводиться к обычному бинарному префиксному дереву. В реальных условиях оно будет отрабатывать лучше за счёт специфичного распределения длины префиксов в таблице маршрутизации.

LC-Trie (Префиксное дерево с уровневым сжатием) – версия префиксного дерева, которая экономит больше места и находит искомый префикс быстрее, чем Patricia Trie.

Сжатие узлов в таком дереве производится группировкой нескольких уровней дерева в один узел. Благодаря этому уменьшается высота дерева, и, как следствие, количество обращений к памяти, которое необходимо произвести. За счёт меньшего числа обращений к памяти данная структура лучше подходит для кэширования.LC-Trie использует комбинацию сжатия уровней (Level Compression) и сжатия путей (Path Compression), как у Patricia Trie.

Например, для таблицы префиксов вида:

Таблица 2

Таблица префиксов

Обозначение	Префикс
A	000*
B	01*
C	10*
D	110*
E	111*
F	11001*
G	10010*
H	10011*
I	1011*
J	110*
K	111*

Это распределение показывает, что чаще всего для определения сетей, видимых глобально, в IPv6 используются префиксы длиной от 32 до 48 бит. Это обусловлено тем, что /48 – маска сети, которая выдаётся провайдером для пользования организацией. Сеть с маской /48 позволяет создать внутри себя до 65536 сетей IPv6 с маской /64. Длина префикса от 12 до 23 приходится на региональных Интернет-регистраторов, от 24 до 32 – на провайдеров. Дополнительно стоит отметить сети с маской 29, которые приходятся на независящие от провайдера адресные пространства и корневые именные сервера.

Представление LC-префиксного дерева будет выглядеть следующим образом (рис. 6).

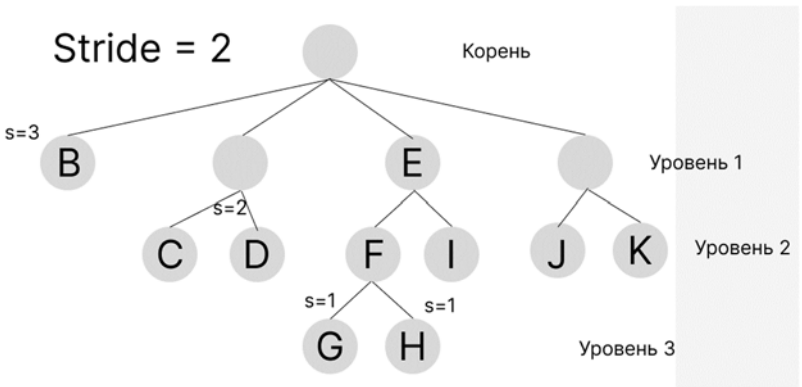


Рис. 6. Пример LC-дерева

Как можно видеть, в данном дереве производится уровневое сжатие – из корня дерева выходит сразу 4 ветви (что равно stride = 2), в остальных же узлах (stride = 1) можно заметить пропуски (skip), которые обозначают, какое число бит адреса мы должны пропустить, чтобы добраться до нужного листа в дереве.

Благодаря тому, что поиск в LC-дереве производится шагами в *k* бит, алгоритмическая сложность поиска префикса в таком дереве становится равна O(m/k), где *m* – длина префикса. Взамен на быстрый поиск, дерево теперь требует O(*m*/*k* + 2*k*) для добавления нового элемента, а потребление памяти в худшем случае может достигать O((2k * *n* * *m*) / *k*). Предусматривается, что перестраивать такое дерево после определённого числа изменений проще, чем обновлять его.

Tree Bitmap– структура данных, которая объединяет аспекты префиксных деревьев и «битовых карт» (bitmaps) для представления префиксов IP CIDR. Она использует иерархическую структуру префиксного дерева, но вместо традиционных указателей использует битовые карты для указания наличия дочерних узлов. Такой подход делает ее компактной и быстрой, используя побитовые операции, которые эффективны на современных процессорах.

Структура Tree Bitmap разработана для минимизации количества обращений к памяти во время поиска, что имеет решающее значение для высокоскоростных приложений маршрутизации [14].

Каждый узел в Tree Bitmap представляет собой сегмент дерева, соответствующий определенному количеству бит IP-адреса. Он содержит в себе информацию о наличии в текущем листе дерева префиксов, и указатели на потомков.

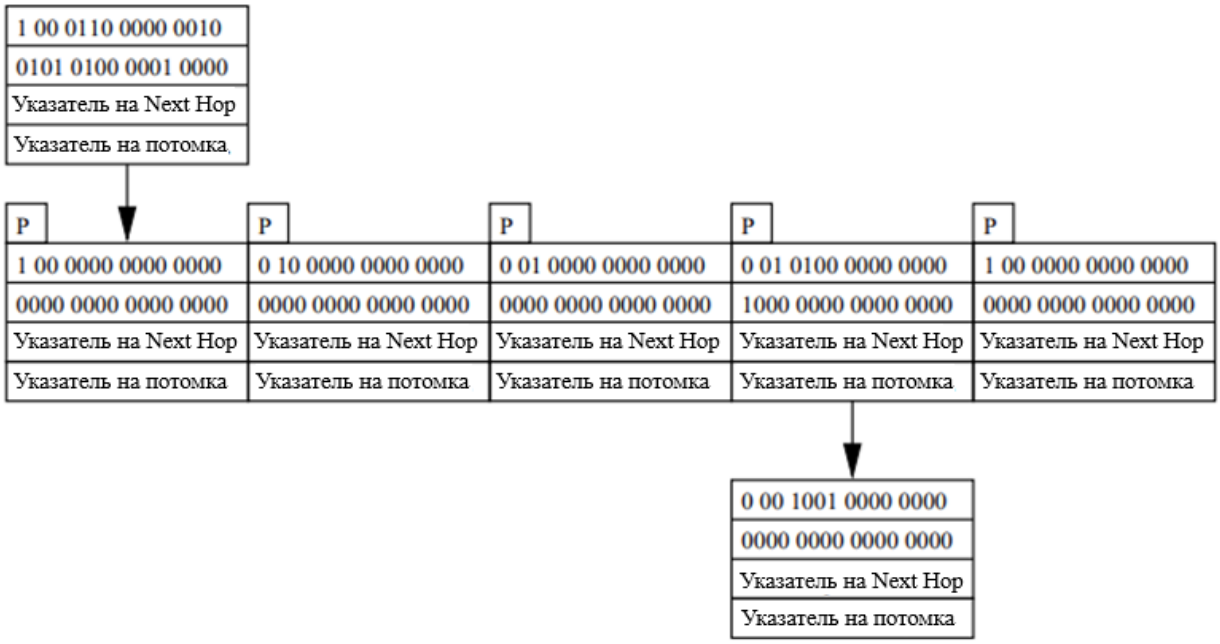


Рис. 7. Пример Tree Bitmap

Данная структура позволяет добиться сложности поиска LPM, равной O(m/k) – как и LC-дерево, за счёт «прохода» сразу нескольких (k) бит адреса за один доступ к памяти. Операции добавления и удаления также будут иметь сложность O(m/k) – так как установка значений в битовой карте производится по адресу, который можно статически вычислить.

Расход памяти – O(n*(2k + P)), где n – число узлов в дереве, 2k – размер битовой карты в каждом узле, P – размер указателей.

Исходя из описанных структур данных, можно построить сравнительную таблицу для этих структур, основываясь на которой будет принято решение о выборе более подходящей. Сравнение будет проводиться по таким параметрам, как: алгоритмическая сложность поиска LPM, вставки, удаления записей, создания структуры, сложность по памяти для структуры.

Данные о сравнении приведены в таблице 3:

Таблица 3

Сравнительные показатели

№ п/п	LPM	Вставка	Удаление	Создание	Память
Префиксное дерево	O(m)	O(m)	O(m)	O(n * m)	O(n * m)
Patricia Trie	O(m)	O(m)	O(m)	O(n * m)	O(n)
LC-Trie (k-stride)	O(m/k)	O(m/k + 2^k)	-	O(n * m)	O((2^k∗n∗m)/k)
Tree Bitmap	O(m/k)	O(m/k)	O(m/k)	O(n * m/k)	O(n*(2^k + P))

Как можно подытожить из полученного сравнения, структуры данных с самыми быстрыми алгоритмами поиска LPM – LC-дерево и Tree Bitmap. Из выбранных структур более предпочтительным вариантом является Tree Bitmap, поскольку позволяет оперативно вносить изменения в таблицу, в отличие от LC-дерева. Кроме того, Tree Bitmap позволяет удалять элементы из дерева, что может пригодиться при управлении большими таблицами.

Пример организации таблицы маршрутизации

После того, как были определены самые эффективные структуры данных для хранения таблицы маршрутизации, можно рассмотреть пример организации таблиц маршрутизации.

Исходя из того, что современные маршрутизаторы должны обладать возможностью маршрутизации как трафика IPv4, так и трафика IPv6, требуется определить, как будет храниться маршрутная информация для обеих версий протокола.

Для хранения таблиц маршрутизации обеих версий протокола можно использовать метод с раздельными таблицами – две таблицы с полными данными о маршрутах для RIB и Tree Bitmap для FIB для разных версий протокола. Использование данного подхода обусловлено тем, что при использовании сдвоенной таблицы маршрутизации для обеих версий протокола может снизиться производительность для IPv4, как следствие более длинной адресации IPv6 и организации соответствующих структур данных. Статистика за 2023 год, представленная RIPE NCC, показывает, что количество трафика IPv6 в мире составляет 39,15%, в то время как в России этот показатель пока находится на отметке 7,88% [5]. Это означает, что на данный момент нет выгоды от использования общей таблицы маршрутизации для обеих версий протокола.

Задача хранения таблицы маршрутизации подразумевает использование двух таблиц маршрутизации, для упрощения работы со всей базой маршрутов – Routing Information Base (RIB) и Forwarding Information Base (FIB).

Для RIB характерно использование эффективных по памяти структур данных, которые позволяют оперативно распоряжаться элементами – для вставки или удаления элементов. В рамках текущего исследования предлагается использование сжатого префиксного дерева для хранения полных и требуемых для создания FIB данных о маршрутах, получаемых как из статической маршрутизации, так и от протоколов динамической маршрутизации.

Для FIB обычно используются структуры данных, позволяющие как можно быстрее найти требуемый префикс в таблице. Из представленных, для данной задачи лучше всего подходят LC-Trie и Tree Bitmap – обе структуры данных позволяют находить требуемый префикс за заданное время O(m/k). При k (stride) = 4 это означает, что максимальное число обращений к памяти для нахождения префикса IPv4 составит 8 для обеих структур, для нахождения префикса IPv6 – 32 обращения к памяти. На практике, с учётом распределений, показанных ранее, в среднем это будет 6 и 16 обращений. В рамках данного исследования было принято решение использовать Tree Bitmap в качестве структуры данных для хранения FIB.

После того, как выбрана структура данных, в виде которой будут храниться записи в таблице маршрутизации, необходимо определить структуру хранимых данных.

Структура хранимых данных в таблице маршрутизации RIB будет выглядеть следующим образом, в соответствии с выбранным способом их хранения:

Таблица 4

Структура данных RIB (v6)

#	Dest.	Mask	Next Hop	Int.	Metric	A.D.	Prot.	Timestamp
1	2001:db8::	64	fe80::1	eth0	10	20	BGP	1724719511
2	2001:db8:1::	64	fe80::2	eth1	10	110	OSPF	1724753691

Таблица 5

Структура данных RIB (v4)

#	Dest.	Mask	Next Hop	Int.	Metric	A.D.	Prot.	Timestamp
1	10.0.0.0	8	192.168.1.1	eth0	10	110	OSPF	1724719511
2	172.16.32.0	24	172.16.1.1	eth1	6	120	RIP	1723347025

В данной структуре для IPv6 и IPv4 будут использоваться отдельные таблицы с маршрутной информацией.

Destination – префикс назначения;
Mask – маска сети префикса назначения;
Next hop IP – IP-адрес следующего маршрутизатора, которому будет перенаправлен пакет;
Interface – указатель на физический интерфейс, на который отправляется пакет;
Metric – метрика, указываемая вручную или протоколом маршрутизации;
Adm. Distance – административное расстояние;
Protocol – тип протокола, либо обозначение ‘Static’ (для статически настроенных маршрутов) или ‘Direct’ (для маршрутов с прямым подключением);
Timestamp – время добавления/последнего обновления маршрута.

Статические маршруты и узел по умолчанию будут храниться в специальном текстовом файле в постоянной памяти. Данные маршруты будут добавляться в таблицу при инициализации таблицы маршрутизации RIB. Пример структуры текстового файла, соответствующего структуре таблицы маршрутизации:

Таблица 6

Формат файла статических маршрутов

```
id,ip_dst,netmask,ip_nh,netif,metric,admdist,protocol;
1,0.0.0.0,0,192.168.1.254,eth0,1,1,default;
```

Для навигации по таблице RIB будет использоваться структура данных префиксного дерева. Данная структура будет храниться в оперативной памяти, с динамическим выделением памяти при создании новых узлов дерева. Узел дерева содержит в себе информацию о наличии маршрутной информации, указатель на запись в таблице маршрутизации и данные о потомках (префиксах, у которых следующий бит адреса соответственно 0 или 1).

Структура хранимых данных в таблице FIB будет выглядеть следующим образом (рис. 8):

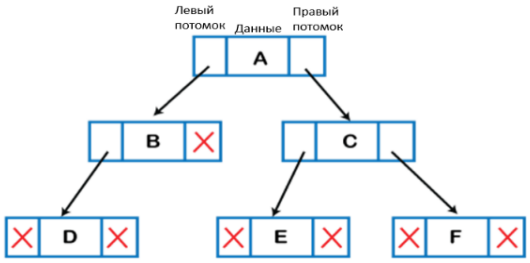


Рис. 8. Структура дерева

В качестве навигации по таблице FIB будет использоваться структура данных Tree Bitmap. Структура представляет собой мультибитовое дерево с фиксированным значением stride (в нашем случае оно будет равно 4). Каждый узел дерева содержит в себе данные о потомках и о наличии префикса, сгруппированной в виде bitmap, а также указатели на узлы-потомки в дереве и на строку в таблице Next Hop. Итоговая структура узла дерева в памяти будет выглядеть следующим образом (табл. 7):

Таблица 7

Структура узла Tree Bitmap

№ бита	**0**	**1**	**2**	**3**		**4**	**5**	**…**	**14**	**15**
Описание	*	0*	1*	00*		01*	10*	…	111*	End

№ бита	**16**	**17**	**18**	**19**	**20**	**21**	**..**	**31**
Описание	0000	0001	0010	0011	0100	0101	..	1111

№ бита	**32-47**	**48-63**
Описание	Базовый индекс потомка	Базовый индекс NextHop

В данном представлении, биты в позициях 0-14 представляют собой данные о существующих префиксах в узле, 15 – сообщает о том, является ли узел конечным, 16-31 – данные о наличии потомков (или, если узел конечный, дополнительную информацию о префиксах), 32-47 – указатель на первый

элемент массива потомков относящийся к данному узлу, 48-63 – указатель на первый элемент массива Next Hop относящийся к данному узлу.

Маршрутная информация, как и информация о потомках конкретного узла, в памяти хранится в виде отдельной таблицы, на которую ссылается битовая карта. В данном примере битовой карты к каждому узлу прикреплён базовый индекс в соответствующих таблицах/векторах, с которого начинается отсчёт элементов.

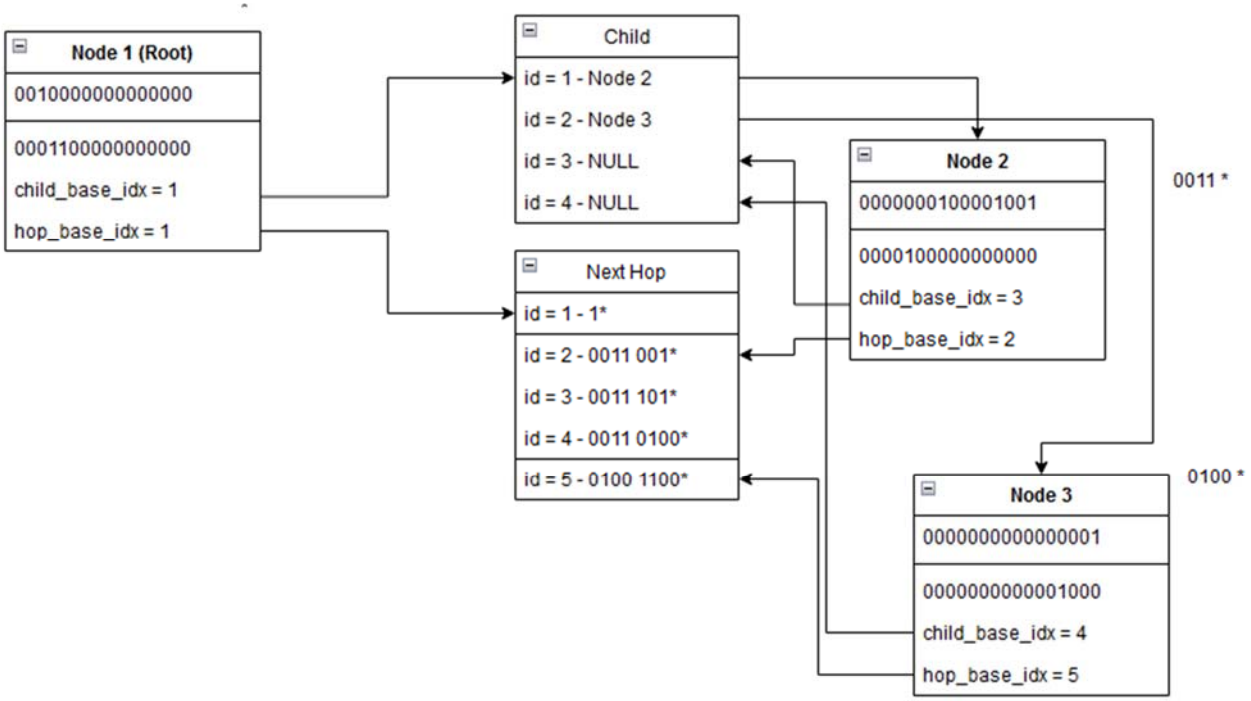


Рис. 9. Структура Tree Bitmap

Массив Next Hop, представленный в виде отдельной таблицы, выглядит следующим образом (табл. 8):

Таблица 8

Массив Next Hop

#	Next Hop IP	Interface	Metric
1	192.168.1.254	eth0	1
…	…	…	…
4	192.168.1.1	eth0	10
…	…	…	…
17	172.16.1.1	eth1	6

Так как в дереве хранится базовый индекс для массивов потомков и Next Hop, для получения конкретного потомка или конкретной маршрутной записи необходимо к базовому индексу прибавить позицию установленного бита, для которого требуется получить запись. К примеру, если базовый индекс узла равен 2 и требуется получить запись для 2-го по счёту бита в узле, значение которого равно 1, позиция элемента в массиве будет рассчитана следующим образом:

Element_idx = Base_idx + Set_bit_pos = 2 + 1 = 3.

Этот элемент массива и будет содержать необходимую информацию.

Благодаря последовательной организации памяти для структуры данных, есть возможность использовать механизмы кэширования, предусмотренные процессором.

Для ещё большего ускорения работы механизма поиска пути можно реализовать собственное кэширование маршрутов с помощью хэш-таблицы. Количество записей в этой таблице будет сильно ограничено, а записи будут добавляться и удаляться по мере работы маршрутизатора. Данная таблица может иметь вид:

Таблица 9

Кэшируемые маршруты

Ключ	Next Hop	Interface
key_1	..	..
key_2	..	..

В качестве ключа можно применять сочетание таких параметров, как адрес отправителя, адрес назначения, тип сервиса (или класс трафика / flow label для IPv6). В случае кэш-попадания, поиск маршрута в такой таблице имеет сложность O(1). При кэш-промахе, поиск маршрута займёт больше времени из-за необходимости вычисления хэш-функции для ключа.

Использование такого метода кэширования сильно зависит от вычислительных возможностей процессора, поскольку операция вычисления хэш-функции может быть дороже по времени.

Пример получения таблицы маршрутизации

Для описания процессе построения итоговой таблицы маршрутизации с использованием структуры данных Tree Bitmap необходимо описать примерную топологию сети, которая позволит показать данный процесс.

Выбранная топология сети представлена на рисунке 10.

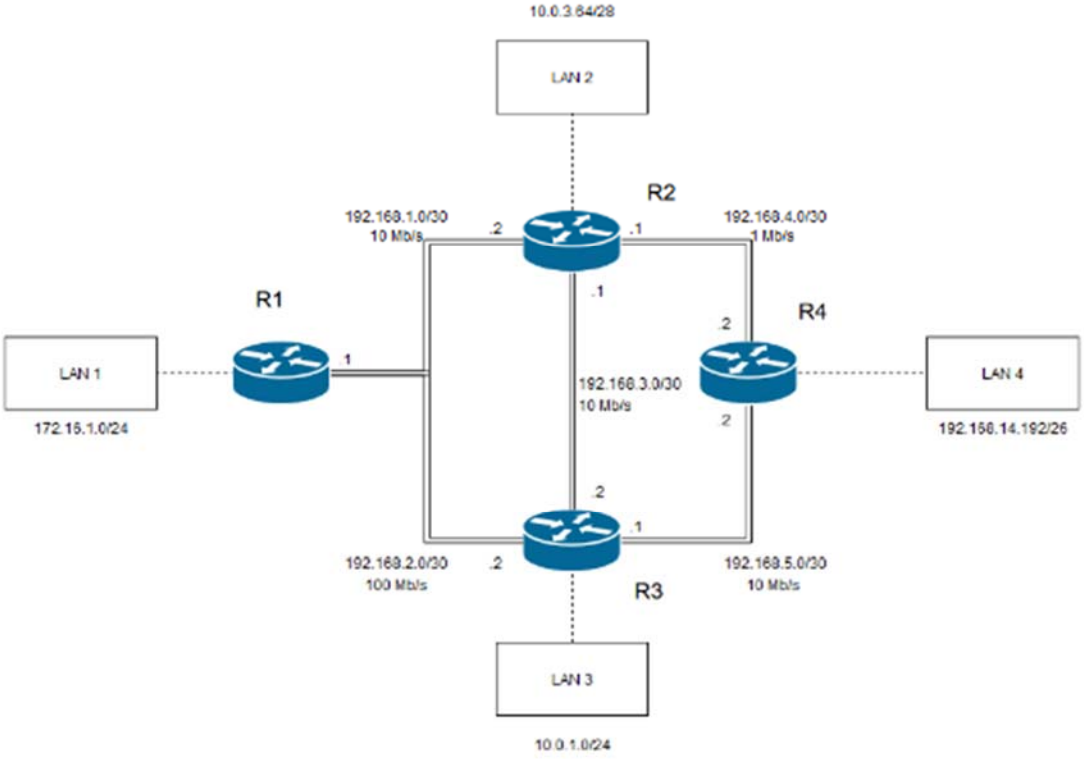


Рис. 10. Топология сети

В данной топологии представлены четыре маршрутизатора, каждый из которых подключен к собственной локальной сети.

Таблица 10

Маршрутизаторы и адреса

Маршрутизатор	Локальная сеть	Маска
R1	172.16.1.0	24
R2	10.0.3.64	28
R3	10.0.1.0	24
R4	192.168.14.192	26

Таблица 11

Соединения между маршрутизаторами

Маршрутизаторы	Соединение	Интерфейс 1	Интерфейс 2	Cost
R1<->R2	192.168.1.0/30	192.168.1.1 (eth0)	192.168.1.2	10
R1<->R3	192.168.2.0/30	192.168.2.1 (eth1)	192.168.2.2	1
R2<->R3	192.168.3.0/30	192.168.3.1	192.168.3.2	10
R2<->R4	192.168.4.0/30	192.168.4.1	192.168.4.2	100
R3<->R4	192.168.5.0/30	192.168.5.1	192.168.5.2	10

Протоколы маршрутизации, настроенные на данных маршрутизаторах в примере – RIPv2 и OSPF; также у каждого маршрутизатора прописан статический маршрут по умолчанию.

Рассмотрение итоговой таблицы маршрутизации можно произвести на примере маршрутизатора R1. Изначально таблица маршрутизации (до инициализации) выглядит следующим образом:

Таблица 12

Прямые подключения R1

#	Destination	Mask	Next hop IP	Interface	Protocol
1	172.16.1.0	24	-	LAN	Direct
2	192.168.1.0	30	-	eth0	Direct
3	192.168.2.0	30	-	eth1	Direct

Данная таблица включает в себя маршруты, основанные на факте прямого подключения R1 к маршрутизаторам R2, R3 и к локальной сети 172.16.1.0/24.

После инициализации статических маршрутов из файла конфигурации, в таблице появляется ещё один новый маршрут:

Данная запись означает, что весь трафик, который имеет адрес назначения, не описанный в таблице маршрутизации, будет проходить через шлюз 192.168.1.2 – маршрутизатор R2.

Таблица 13

Таблица маршрутов R1

#	Destination	Mask	Next hop IP	Interface	Protocol
1	172.16.1.0	24	-	LAN	Direct
2	192.168.1.0	30	-	eth0	Direct
3	192.168.2.0	30	-	eth1	Direct
4	0.0.0.0	0	192.168.1.2	eth0	Static

Протоколы маршрутизации RIPv2 и OSPF должны в результате своей работы обеспечить полное отображение топологии сети в таблице маршрутизации. В соответствии со спецификой протокола RIPv2, маршрутизаторы R1 и R2, R3, R4 обмениваются маршрутной информацией между собой, в результате чего получается следующая база данных маршрутов RIP:

Таблица 14

База данных маршрутов RIPv2

#	Destination	Mask	Hop count	Next hop IP	Interface	Source
1	10.0.3.64	28	2	192.168.1.2	eth0	R2
2	10.0.1.0	24	2	192.168.2.2	eth1	R3
3	192.168.14.192	26	3	192.168.1.2	eth0	R2
4	192.168.14.192	26	3	192.168.2.2	eth1	R3

Посредством применения алгоритма Беллмана-Форда для поиска кратчайшего пути, протоколом RIP была составлена таблица маршрутов, содержащая оптимальные пути до каждой подсети назначения. Протокол OSPF в свою очередь составляет граф соединений посредством использования информации, полученной от соседей. Маршруты, которые собирает в итоге протокол OSPF, выглядят следующим образом:

Таблица 15

База данных OSPF

#	Destination	Mask	T. cost	Next hop IP	Interface
1	10.0.3.64	28	10	192.168.1.2	eth0
2	10.0.1.0	24	1	192.168.2.2	eth1
3	192.168.14.192	26	11	192.168.2.2	eth1

Общая таблица маршрутной информации, с дополнениями, полученными от протоколов, будет выглядеть следующим образом:

Таблица 16

Общая таблица RIB

#	Destination	Mask	Next hop	Int.	Prot.	A. D.	Metric
1	172.16.1.0	24	-	LAN	Direct	0	-
2	192.168.1.0	30	-	eth0	Direct	0	-
3	192.168.2.0	30	-	eth1	Direct	0	-
4	0.0.0.0	0	192.168.1.2	eth0	Static	1	-
5	10.0.3.64	28	192.168.1.2	eth0	RIP	120	2
6	10.0.1.0	24	192.168.2.2	eth1	RIP	120	2
7	192.168.14.192	26	192.168.1.2	eth0	RIP	120	3
8	192.168.14.192	26	192.168.2.2	eth1	RIP	120	3
9	10.0.3.64	28	192.168.1.2	eth0	OSPF	110	10
10	10.0.1.0	24	192.168.2.2	eth1	OSPF	110	1
11	192.168.14.192	26	192.168.2.2	eth1	OSPF	110	11

Для составления Tree Bitmap используются маршруты из данной таблицы. Из маршрутов с одинаковыми префиксами выбираются те, которые имеют меньшую административную дистанцию – в данном случае маршруты, попадающие в итоговую структуру, будут выглядеть следующим образом:

Таблица 17

Маршруты для Tree Bitmap

#	Destination	Mask	Next hop	Int.	Prot.	A. D.	Metric
1	172.16.1.0	24	-	eth2	Direct	0	-
2	192.168.1.0	30	-	eth0	Direct	0	-
3	192.168.2.0	30	-	eth1	Direct	0	-
4	0.0.0.0	0	192.168.1.2	eth0	Static	1	-
5	10.0.3.64	28	192.168.1.2	eth0	OSPF	110	10
6	10.0.1.0	24	192.168.2.2	eth1	OSPF	110	1
7	192.168.14.192	26	192.168.2.2	eth1	OSPF	110	11

Итоговое дерево будет иметь примерно следующий вид (штриховкой на схеме обозначаются пропуски промежуточных узлов):

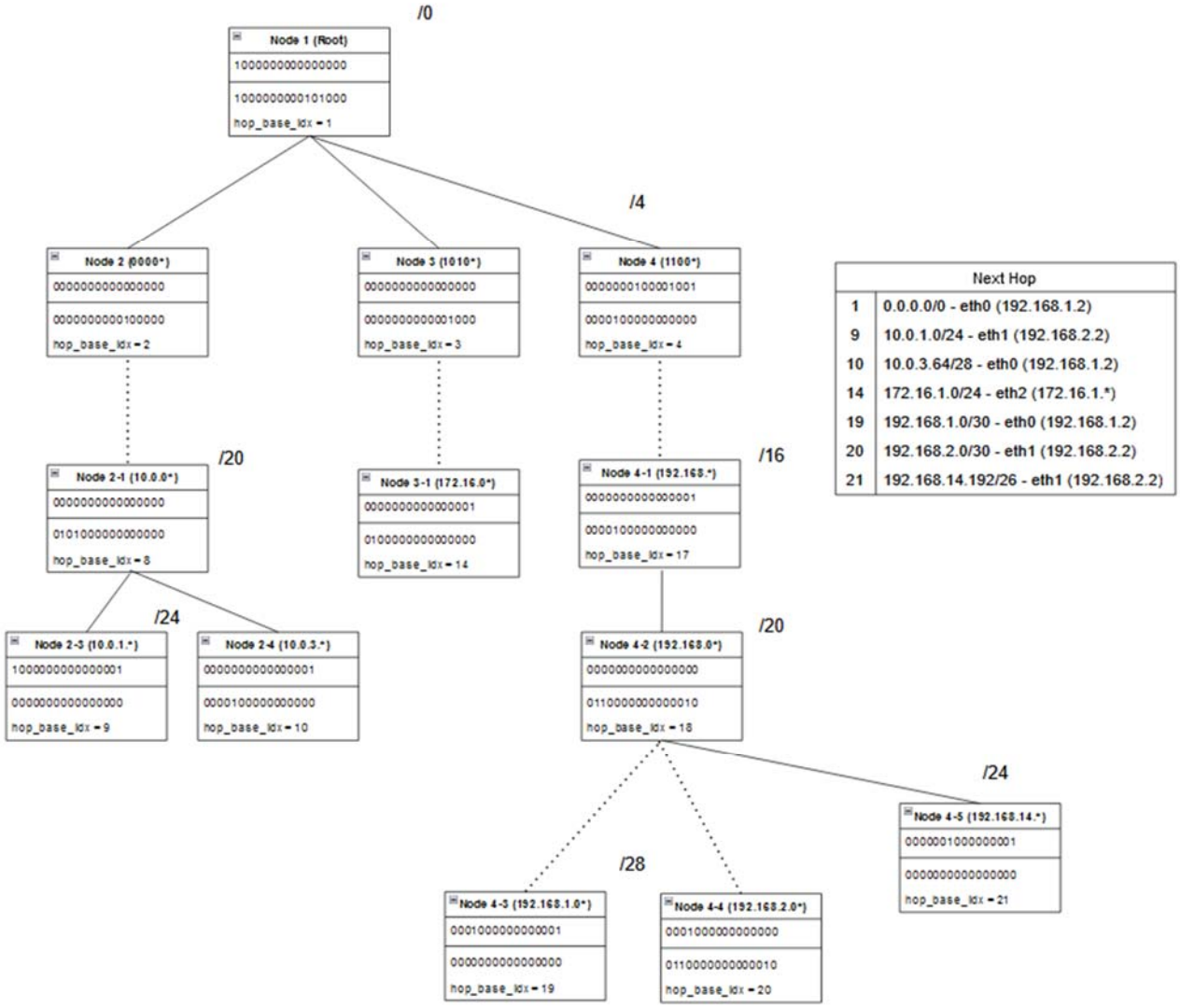


Рис. 11. Схема Tree Bitmap

Как можно заметить, на примере с небольшим количеством маршрутов в таблице — здесь их всего 7 — структура Tree Bitmap показывает себя достаточно плохо. Однако, главным преимуществом данной структуры является хорошая масштабируемость — в случае с граничными маршрутизаторами при выходе в Интернет, или в случае с маршрутизаторами в больших датацентрах данная структура будет отрабатывать гораздо эффективнее из-за высокой плотности организации данных, объединенных в кластеры [15-18].

Дополнительные методы оптимизации Tree Bitmap

Tree Bitmap как структуру данных также можно оптимизировать ещё больше в сторону компактности или скорости поиска. Далее представлены несколько вариантов оптимизации, которые можно произвести для более эффективной работы с данной структурой.

1. Для оптимизации скорости поиска LPM можно увеличить битовую ширину. К примеру, если увеличить stride до 8, то в таком случае можно будет обойтись всего 3 и 8 (в среднем) обращениями к памяти.

В реальности такую операцию придется выполнять по частям в связи с тем, что процессор не сможет сразу прочитать 28 = 256 бит информации из памяти одним циклом. Для этого данная операция может быть поделена на несколько меньших, что в совокупности может дать обратный эффект. В современных проприетарных сетевых решениях (в частности – в физических маршрутизаторах) для увеличения битовой ширины используются собственные механизмы работы с памятью.

2. Можно произвести сжатие дерева для получения более компактного представления дерева. К

примеру, можно воспользоваться стратегией, как в случае с сжатым префиксным деревом – Path Compression – это позволит, сжав пути с единичным потомком, получить более компактное дерево за счёт меньшего числа bitmap, не содержащих в себе действительных префиксов.

3. Метод оптимизации под названием «Split-trie optimization». Данный метод опирается на статистические данные о распределении количества префиксов по их длине. Так как статистически известно, что большая часть префиксов в таблицах маршрутизации – это префиксы, чьи маски кратны 4, можно воспользоваться простой логикой и произвести смещение на 1 бит вниз. В результате такого смещения, Tree Bitmap разделяется на два дерева с однобитовым корнем, имеющим в себе указатели на оба этих дерева.

Заключение

В данной работе рассмотрены современные подходы к организации таблиц маршрутизации и оптимизации алгоритмов поиска маршрутов, особенно в контексте работы с протоколом IPv6. Основной задачей является минимизация задержек и повышение производительности маршрутизации при увеличении объёма данных в таблицах. [19-28]

Особое внимание уделено различным структурам данных, включая Patricia Trie, LC-Trie и Tree Bitmap, которые обладают преимуществами по скорости и эффективности использования памяти относительно обычных префиксных деревьев. Tree Bitmap признан наиболее подходящей структурой для хранения FIB, благодаря своей способности обеспечивать предсказуемый по времени и быстрый поиск префиксов при сохранении умеренных требований к памяти.

В качестве примера была приведена модель организации таблицы маршрутизации с использованием структуры данных Tree Bitmap, а также рассмотрен процесс её составления с использованием статической и динамической маршрутизации в заданной топологии.

Полученные результаты демонстрируют, что структура Tree Bitmap обладает наилучшим балансом между скоростью поиска, компактностью хранения и возможностью внесения изменений в таблицу маршрутизации. Это делает её перспективной для использования в высоконагруженных сетевых инфраструктурах.

Перспективными направлениями дальнейших исследований по данной теме являются методы оптимизации структуры Tree Bitmap, которые позволят сделать её ещё эффективнее как в плане скорости, так и в плане потребления памяти.

Литература

1. *Таненбаум Э.С., Уэзеролл Д.Дж.* Компьютерные сети. 5-е изд. СПб.: Питер, 2012. 960 с.

2. *Шведов А.В., Гадасин Д.В., Клыгина О.Г*. Организация взаимодействия туманных вычислений и сегментной маршрутизации для предоставления сервисов IOT в smart grid // Системы синхронизации, формирования и обработки сигналов. 2022. Т. 13, № 3. С. 40-49. EDN TRRYZN

3. *Марченко Д.О., Клыгина О.Г., Гадасин Д.В., Шведов А.В.* Обеспечение механизмов балансировки нагрузки в сетях с сегментной маршрутизацией на основе данных мониторинга // Перспективные технологии в средствах передачи информации : материалы 14-ой международной научно-технической конференции, Владимир, 06-07 октября 2021 года. Владимир: Владимирский государственный университет имени Александра Григорьевича и Николая Григорьевича Столетовых, 2021. С. 419-422. EDN ZSCNIR

4. *Гадасин Д.В., Шустов С.А*. Исследование эффективности протоколов маршрутизации в условиях сетей с высокой нагрузкой // Теория и практика экономики и предпринимательства : Труды XXI Международной научно-практической конференции, Симферополь – Гурзуф, 18-20 апреля 2024 г. Симферополь: ИП Зуева Т. В., 2024. С. 236-237. EDN WNVEOC

5. *Goralski W.* The Illustrated Network: How TCP/IP Works in a Modern Network. 2nd ed. Morgan Kaufmann, 2017. 936 p.

6. RFC 2460 Internet Protocol, Version 6 (IPv6) Specification / IETF. https://datatracker.ietf.org/doc/html/rfc2460 (дата обращения: 18.12.2024).

7. RFC 791 Internet Protocol / IETF. https://datatracker.ietf.org/doc/html/rfc791 (дата обращения: 18.12.2024).

8. RIPE NCC Articles. https://www.ripe.net/ (дата обращения: 18.12.2024).

9. *Гадасин Д.В*. Построение бинарного дерева минимальной цены // T-Comm: Телекоммуникации и транспорт. 2024. Т. 18, № 11. С. 38-44. DOI 10.36724/2072-8735-2024-18-11-38-44. EDN GMCEWG

10. *Shvedov A.V., Gadasin D.V., Alyoshintsev A.V*. Segment routing in data transmission networks // T-Comm: Телекоммуникации и транспорт. 2022. Vol. 16, No. 5, pp. 56-62. DOI 10.36724/2072-8735-2022-16-5-56-62. EDN VAYLJQ

11. *Гадасин Д.В., Вакурин И.С., Тремасова Л.А.* Алгоритм распределения данных между системами хранения на основе свойства самоподобия // Электросвязь. 2024. № 4. С. 44-50. DOI 10.34832/ELSV.2024.53.4.015. EDN BRSLCL

12. *Тремасова Л.А., Первухина А.А., Гадасин Д.В.* Использование методов Косарайю и k-средних для формирования кластеров // Электросвязь. 2024. № 9. С. 47-55. DOI 10.34832/ELSV.2024.58.9.007. EDN DOZTZK

13. *Гадасин Д.В., Шведов А.В*. Применение транспортной задачи для балансировки нагрузки в условиях нечеткости исходных данных // T-Comm: Телекоммуникации и транспорт. 2024. Т. 18, № 1. С. 13-20. DOI 10.36724/2072-8735-2024-18-1-13-20. EDN WKNPIX

14. *Srinivasan V., Suri S., Varghese G.* Packet classification using tuple space search // ACM SIGCOMM. 1999. Vol. 24, No.4, pp. 135-146.

15. *Melkova E.K., Korovushkina V.M., Shvedov A.V., Gadasin D.V*. Cluster implementation based on the belonging function // Systems of Signal Synchronization, Generating and Processing in Telecommunications. 2023. Vol. 6, No. 1, pp. 245-250. DOI 10.1109/SYNCHROINFO57872.2023.10178611. EDN NBSLVV

16. *Gadasin D.V., Koltsova A.V., Gadasin D.D*. Algorithm for Building a Cluster for Implementing the 'Memory as a Service' Service in the IoT Concept // 2021 Systems of Signals Generating and Processing in the Field of on Board Communications, Conference Proceedings, Moscow, 16-18 марта 2021 г. Moscow, 2021. P. 9416112. DOI 10.1109/IEEECONF51389.2021.9416112. EDN VRPCFG

17. *Gadasin D.V., Shvedov A.V., Koltsova A.V*. Cluster model for edge computing // 2020 International Conference on Engineering Management of Communication and Technology, EMCTECH 2020 : Proceedings, Vienna, 20-22 октября 2020 г. New York: Institute of Electrical and Electronics Engineers Inc., 2020. P. 9261538. DOI 10.1109/EMCTECH49634.2020.9261538. EDN FGDLSA

18. *Гадасин Д.В., Вакурин И.С.* Кластерное проектирование сетей Wi-Fi с высокой плотностью абонентов // Труды Северо-Кавказского филиала Московского технического университета связи и информатики. 2020. № 1. С. 138-144. EDN EHXMFJ

19. *Андриянова А.К., Тремасова Л.А., Гадасин Д.Д., Гадасин Д.В.* Соотношение метрик связности и коэффициента баланса весов в экстремальных задачах // REDS: Телекоммуникационные устройства и системы. 2024. Т. 14, № 3. С. 4-13. EDN OJHSVO

20. *Гадасин Д.В., Пак Е.В*. Применение модели бэкмена для распределения потоков в сетях с сегментной маршрутизацией // REDS: Телекоммуникационные устройства и системы. 2020. Т. 10, № 4. С. 18-23. EDN PCGGHF

21. *Shvedov A.V., Gadasin D.V., Pak E.V.* Application of the Backman Model for the Distribution of Traffic Flows in Networks with Segment Routing // 2022 Systems of Signals Generating and Processing in the Field of on Board Communications, SOSG 2022 – Conference Proceedings, Moscow, 15-17 марта 2022 г. Moscow, 2022. DOI 10.1109/IEEECONF53456.2022.9744344. EDN RBMTBQ

22. *Гадасин Д.В., Шведов А.В., Кузин И.А.* Трехмерная реконструкции объекта по одному изображению с использованием глубоких свёрточных нейронных сетей // T-Comm: Телекоммуникации и транспорт. 2022. Т. 16, № 7. С. 29-35. DOI: 10.36724/2072-8735-2022-16-7-29-35. EDN: YTLCNW

23. *Назаров М.Д., Шведов А.В.* Корреляция атрибутов соглашения об уровне обслуживания с основными параметрами QoS в корпоративных сетях // Телекоммуникации и информационные технологии. 2020. Т. 7. № 2. С. 73-79. EDN: VQHDTJ

24. *Kalmykov N.S., Dokuchaev V.A.* Segment routing as a basis for software defined network // T-Comm. 2021. Т. 15. № 7. С. 50-54. EDN: LYVZCV

25. *Dokuchaev V.A., Maklachkova V.V., Statev V.Yu.* Classification of personal data security threats in information systems // T-Comm. 2020. Т. 14. № 1. С. 56-60. EDN: QOGYHH

26. *Докучаев В.А., Маклачкова В.В., Статьев В.Ю.* Цифровизация субъекта персональных данных // T-Comm: Телекоммуникации и транспорт. 2020. Т. 14. № 6. С. 27-32. EDN: XVWYJP

27. *Pavlov S.V., Dokuchaev V.A., Mytenkov S.S.* Model of a fuzzy dynamic decision support system // T-Comm. 2020. Т. 14. № 9. С. 43-47. EDN: VYFNLB

28. *Кузин И.А., Гадасин Д.В.* Модель контейнера данных для минимизации трафика при передаче субъективных характеристик объектов на изображении трехмерной сцены // Телекоммуникации и информационные технологии. 2021. Т. 8. № 2. С. 96-100. EDN: TYFFBH

ПРОМЫШЛЕННЫЙ ИНТЕРНЕТ ВЕЩЕЙ В РОССИИ

Беляев Антон Сергеевич
Московский Технический Университет Связи и Информатики,
Лаборант учебной лаборатории кафедры Бизнес-Информатики, Москва, Россия
a.s.belyaev@mtuci.ru

Липатов Вячеслав Анатольевич
Московский Технический Университет Связи и Информатики,
доцент, кандидат полит. наук, Москва, Россия
v.a.lipatov@mtuci.ru

Аннотация
Статья исследует текущее состояние и перспективы развития Интернета вещей (IoT) в России. На фоне роста мирового рынка IoT, российский рынок демонстрирует позитивные тенденции, несмотря на кадровый дефицит и недостаточную цифровизацию. В статье рассматриваются ключевые компоненты IoT и его применение в промышленности для оптимизации процессов. Также акцентируется внимание на вопросах безопасности и надежности IoT-сетей, подчеркивая необходимость защиты от киберугроз. Успешная реализация IoT в России требует комплексного подхода к управлению рисками и обеспечению безопасности, что может способствовать экономическому росту и повышению качества жизни.

Ключевые слова
Цифровая трансформация, цифровизация, Интернет Вещей, киберугрозы, IoT-сети, умный дом

Введение

На конец 2023 года объем мирового рынка IoT достиг около $406 млрд. Ожидается, что к 2032 году глобальный рынок IoT вырастет до $1,56 трлн с ежегодным ростом примерно 17%. В России рынок IoT составил ₽170 млрд, с прогнозом роста до ₽188,9 млрд к 2026 году. Количество подключенных IoT-устройств в стране превысило 80 млн. Темпы роста IoT в России соответствуют мировым тенденциям, несмотря на отставание от глобального рынка и спад в 2022 году. Несмотря на относительную новинку для российского рынка, IoT очень выгоден предприятиям. Это отчасти облегчает ситуацию кадрового голода, снижает тем самым также и затраты на производстве. Можно с уверенностью сказать, что IoT становится весьма важным фактором развития российской промышленности, способствуя повышению эффективности и внедрению инноваций. Кроме того, несмотря на рост, количество IoT устройств в мире кратно превышает это значение в нашей стране. Интернет вещей – благо, которое может помочь нам реализовать необходимые задачи более эффективно. Это входит в понятие цифровой трансформации и является важным этапом развития.

Результаты исследований

С точки зрения технологий, концепция IoT представляет собой многослойную архитектуру, состоящую из четырех ключевых компонентов: подключаемых устройств (включая сенсоры, датчики и терминалы), сетевой инфраструктуры, обеспечивающей взаимодействие этих устройств, IoT-платформ, а также приложений для конечных пользователей. Первые два уровня – устройства и сети – фундаментальные элементы, без которых невозможно функционирование всей системы. IoT-платформы могут варьироваться в зависимости от специфики решения, а клиентский интерфейс, как правило, присутствует в большинстве современных приложений. Однако в перспективе возможно, что уровень приложений и другие дополнительные элементы управления могут утратить свою актуальность.

В будущем взаимодействие может сводиться к бэкенд-приложениям, которые будут анализировать действия пользователей и, основываясь на этом анализе, автоматически управлять конечными устройствами без необходимости дополнительного ввода со стороны оператора. Например, в контексте промышленного предприятия такая система будет способна предугадывать потребности в ресурсах и оптимизировать производственные процессы. Она будет собирать данные о состоянии оборудования, уровне запасов и производительности, а затем на основе анализа этих данных принимать решения о перераспределении ресурсов, планировании технического обслуживания или оптимизации

производственного расписания. Эти действия будут осуществляться на основе заранее определенных шаблонов и алгоритмов, хранящихся в базе данных системы, что позволит системе функционировать автономно, без вмешательства человека.

В этой модели роль разработчиков и операторов будет сводиться к контролю за системой, который может осуществляться либо через специализированные интерфейсы, либо посредством механического выполнения определенных действий. Возвращаясь к современным реалиям, IoT можно разбить на несколько этапов: сбор данных, принятие решений на основе собранных показателей и выполнение корректирующих действий. На массовом уровне IoT часто воспринимается как источник данных для Big Data, однако его истинная ценность заключается в автоматизации процессов и возможности управления реальными объектами без участия человека. Это делает IoT концепцией, объединяющей цифровое пространство с реальным миром. IoT представляет собой не столько новую технологию, сколько новую концепцию, позволяющую эффективно использовать уже существующие технологии автоматизации. Это далеко не подразумевает глобального переворота, но открывает новые возможности для решения современных задач.

В контексте промышленности же часто встречается термин «Промышленный интернет». Его использовать достаточно уместно, но для упрощения мы оставим привычную терминологию. Определенно можно сказать – в сфере промышленности Интернет вещей может упростить и оптимизировать производственные процессы. На предприятиях, в большей степени, IoT-системы собирают информацию о состоянии оборудования, состоянии различных компонентов и производительности. Зачастую, это требует работы программистов и специалистов по настройке сетей, так как подобные сети на предприятиях могут быть крайне сложны, что осложняет моментальное введение. Однако, это позволяет анализировать данные и принимать решения о перераспределении ресурсов, планировании, технического обслуживания и улучшении производственных процессов.

Впрочем, реальный список улучшений зависит от конфигурации оборудования, назначения и т.д. И хотя IoT часто рассматривается как источник данных для анализа больших объемов информации (Big Data), его настоящая ценность – отсутствие участия человека. Это выгодно, ведь машина не требует зарплаты, а кроме того – неприхотлива. Человек лишь получает готовые данные при необходимости, а все процессы происходят автоматизированно. На текущий момент, в России введение подобных систем в меру ограничено ввиду дефицита некоторого оборудования в достаточном количестве, отсутствия мотивации для введения подобных сетей, а зачастую и ненужности введения, так как многие предприятия в должной степени не перешли порог базовой цифровизации, под которой мы подразумеваем базовый перевод части внутренних документов в цифровые аналоги, закупку персональных ПК и серверных решений в достаточном количестве.

Эти доводы не безосновательны, согласно исследованию «Цифровая Россия» от 2019 года, опубликованному «Центром финансовых инноваций и безналичной экономики Московской школы управления СКОЛКОВО», можно с уверенностью сказать, что в России наиболее полное освещение цифровизации отмечается в центральной и западной частях страны, в то время как юго-западные регионы демонстрируют наименьший уровень. Во многом, высокие показатели цифровизации отмечаются лишь в крупных городах. Но не стоит допускать и чрезмерно пессимистичных мыслей, ведь согласно отчёту, подготовленному компанией «Comindware», специализирующейся на проектах введения методов цифровой трансформации и IoT сетях, есть и положительные данные.

Так, около трети компаний продолжают внедрять проекты цифровой трансформации, несмотря на снижение выручки. А 74% респондентов отметили, что продолжают автоматизацию бизнес-процессов даже при нехватке финансирования. Результаты опроса свидетельствуют о высоком уровне доверия к IT сфере и IoT в частности. Предложений на рынке цифровой трансформации достаточно много, а спрос – ниже предложения. Возможно, введение льготного кредитования и субсидий могли бы стимулировать отечественные компании на обновление своего оборудования и закупку новых систем, в том числе и IoT оборудования.

На текущий момент, специалисты кафедры Бизнес-Информатики при Московском Техническом Университете Связи и Информатики уже проводили опыты по созданию IoT и блокчейн сетей. В частности, были закуплены тестовые одноплатные компьютеры Raspberry Pi версий 3 и 4 для проведения опытов и созданию внутренней документации, которая, впрочем, ещё не была опубликована. Однако, в качестве промежуточного вывода было установлено, что даже устаревающие одноплатные компьютеры, подходящие лишь для простой обработки входящих данных с датчиков, в целом неплохо способны работать и проводить вычисления достаточные для существования простой IoT сети.

Также одним из выводом послужил факт возможности введения подобной сети в университетах. Это позволяет с уверенностью сказать, что Интернет вещей как концепция не обязательно требует больших вложений и сложного оборудования, а напротив, может создаваться специалистами на местах, тем самым популяризируя технологию и расширяя её влияние.

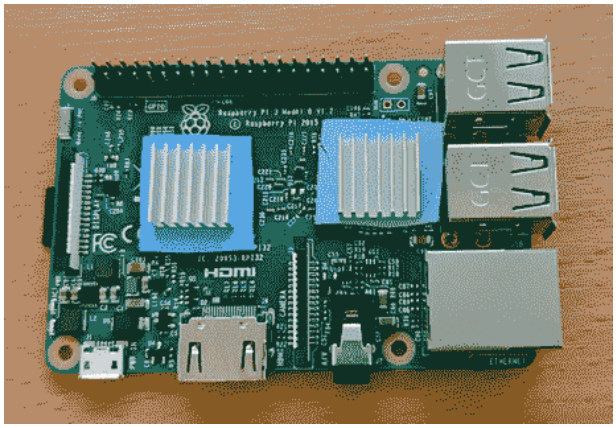


Рис. 1. Одноплатный компьютер Raspberry Pi 3

Стоит понимать, что IoT сеть отлично приживается и в быту. Это вряд ли позволит Вам экономить, но точно сможет улучшить качество жизни. Самое главное преимущество – требования в домашней IoT сети гораздо ниже, нежели на предприятии. При достаточном уровне знаний и умений, такую сеть может создать и обычный человек, используя одноплатные компьютеры бытового назначения и простые датчики, например – для Arduino. Упомянутые устройства имеют демократичную цену и могут использоваться в различных сценариях. Подобные проекты создавались как энтузиастами, так и крупными корпорациями. Так, компания Intel, производящая и создающая полупроводниковые продукты, долгие годы работала над созданием IoT систем и их прототипов. С их поддержкой энтузиасты разработали рабочий концепт умного дома.

Суть проекта Intel по созданию системы умного дома заключалась в разработке функционального решения для автоматизации управления входной и гаражной дверями с использованием доступных технологий и компонентов. Проект начался с выявления потребности в эффективном управлении доступом в дом, что включало в себя автоматизацию открытия и закрытия дверей, а также мониторинг их состояния. Команда использовала "слабое" оборудование, такое как плата Arduino 101 и компьютер Intel NUC, что сделало проект доступным для широкого круга разработчиков и энтузиастов.

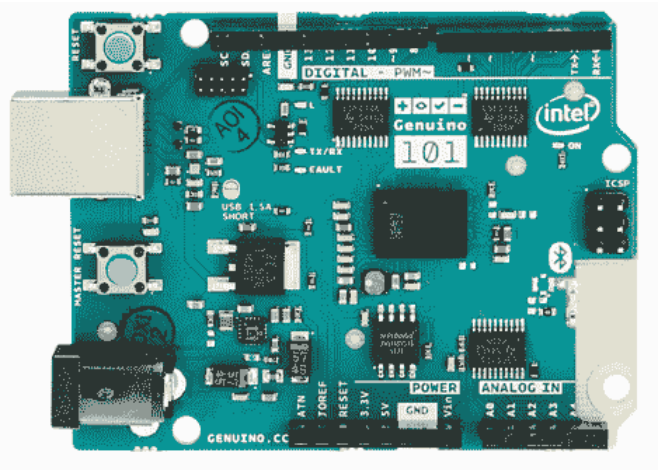


Рис. 2. Одноплатный компьютер Arduino 101

Активно использовались IoT-технологии для сбора и анализа данных, предоставления удаленного доступа и управления системой через мобильные и административные приложения. Проект следовал структурированному подходу, который позволил команде эффективно пройти все этапы разработки — от идеи до готового продукта, что сделало его примером для других IoT-проектов. Проект пусть и не связан с предприятиями и промышленным комплексом, но позволяет наглядно понять, что для работы

интернета вещей не обязательно иметь сложное оборудование – достаточно иметь мотивацию и знания в этой сфере. Также Intel оставила проект умного дома в репозитории GitHub и каждый желающий может воспользоваться средствами разработки для развития уже собственных проектов.

На данный момент, упоминаний о данном исследовании Intel уже нет на официальном сайте данной компании, однако имеются и другие примеры развития данной технологии, а также новости о будущих свершениях. В сторонних источниках по-прежнему можно найти описание упомянутого ранее проекта. Подобный проект можно реализовать и в любом уголке России, так как затраты на внедрение бытовых IoT сетей низки и позволить их внедрение может даже человек со средним заработком, а использовать можно даже простые и, зачастую, даже неподходящие устройства.

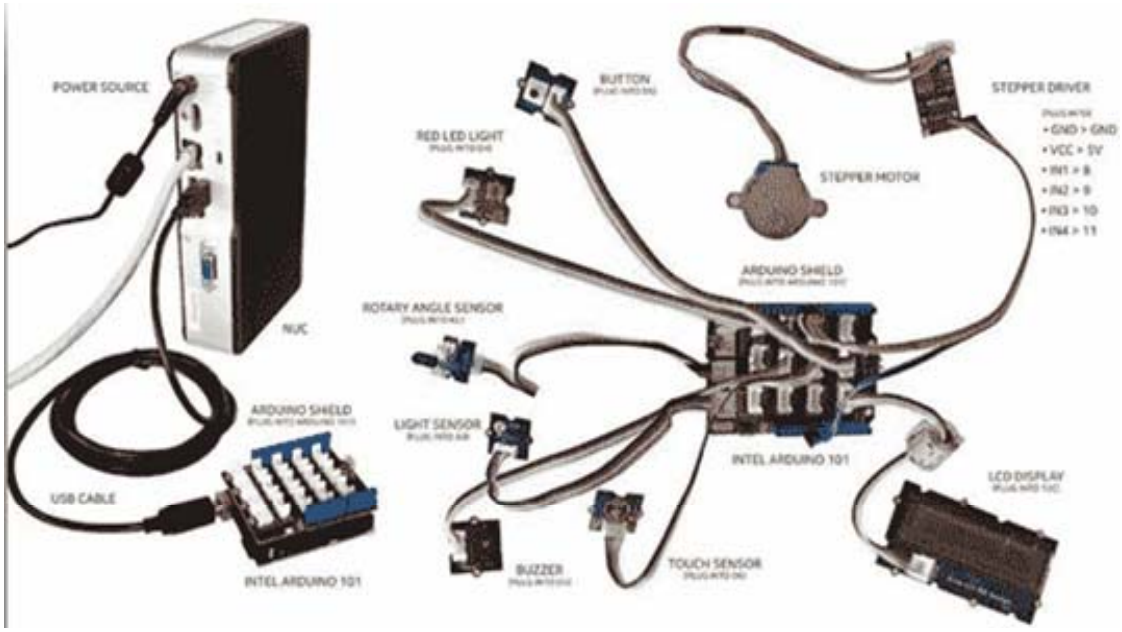


Рис. 3. Устройства, использованные Intel в проекте умного дома

Согласно ранее обозначенной информации, введение IoT сетей – отличная концепция будущего. Но, как и любая современная идея в сфере цифрового развития, Интернет вещей может скрывать в себе ряд уязвимостей, прежде всего связанных с возможностью несанкционированного доступа к сети и уязвимости чувствительных данных, производимых существующих внутри сети. Серверные решения в таких сетях должны в обязательном порядке быть защищены от ряда угроз, а звенья в сети цепи должны обладать достаточно защищенным каналом связи.

Из современных угроз стоит наиболее полное внимание обратить на угрозы создания DDoS-атак и создания ботнет сетей, служащих для совершения противоправных действий. Так, печально известное вредоносное ПО «IoT Reaper» только в 2017 году заразило более 2 млн. устройств по всему миру, согласно проведенным исследованиям сообщества «Check Point Research». При недостаточной защищенности соединения или ПО маршрутизаторов злоумышленники могут перехватывать чувствительные данные компаний и простых пользователей.

Это важная проблема, которую стоит учитывать при работе с Интернетом вещей. Для предотвращения совершения противоправных действий следует тщательно планировать уровни безопасности вашей сети и не допускать уязвимостей. При работе с IoT стоит отдать предпочтение работе квалифицированных специалистов, нежели попыткам создать её самому. На текущий момент присутствует также некоторый кадровый голод, связанный с недостатком специалистов в данной области, отягощающий влияние внешних угроз и этот факт также необходимо учитывать.

Заключение

Использование IoT сетей – достаточно новая и смелая концепция по цифровой трансформации. Как показал опыт предыдущих лет и проведенных экспериментов сторонних компаний, Интернет вещей в перспективе может стать популярным инструментом снижения рисков и затрат, а также улучшения качество жизни обывателя.

Внедрение подобных структур может улучшить экономическое благополучие, но в погоне за выгодой не стоит забывать и о рисках и потенциальных уязвимостях, связанных с безопасностью данных и сетевой инфраструктуры. Необходимость тщательной проработки уровней безопасности и защиты от киберугроз становится весьма важной в условиях растущей зависимости от технологий. Только с учетом этих аспектов можно уверенно двигаться вперед, используя возможности, которые предоставляет Интернет вещей для создания более безопасной и эффективной цифровой среды. В конечном итоге, успешная реализация IoT в России требует не только технических решений, но и комплексного подхода к управлению рисками и обеспечению безопасности. Необходимость освещения технологии IoT в России в перспективе станет залогом успешного будущего этой технологии и будет способствовать стабильному экономическому рост

Литература

1. *Довгаль В.А., Довгаль Д.В*. Интернет Вещей: концепция, приложения и задачи // Вестник АГУ. 2018. Вып. 1(216). С. 129-135.

2. Индекс «Цифровая Россия» (исследование). [Электронный ресурс]. URL: https://www.skolkovo.ru/researches/indeks-cifrovaya-rossiya/ (дата обращения: 12.01.2025).

3. Итоги исследования «Эффективность цифровой трансформации в России» (Отчет). [Электронный ресурс]. URL: https://www.comindware.ru/bpm-effectiveness-russia-2022/ (дата обращения: 12.01.2025).

4. *Питер Н.* IoT-проект для умного дома: путь от идеи к производству // Хабр. [Электронный ресурс]. URL: https://habr.com/ru/companies/intel/articles/396737/ (дата обращения: 02.12.2024).

5. Arduino. Официальный сайт. [Электронный ресурс]. URL: https://www.arduino.cc/ (дата обращения: 10.12.2024).

6. A New IoT Botnet Storm is Coming. [Электронный ресурс]. URL: https://research.checkpoint.com/2017/new-iot-botnet-storm-coming/ (дата обращения: 19.10.2017).

7. Intel. Industrial IoT Overview. [Электронный ресурс]. URL: https://www.intel.com/content/www/us/en/internet-of-things/industrial-iot/overview.html (дата обращения: 12.12.2024).

8. Raspberry Pi. Официальный сайт. [Электронный ресурс]. URL: https://www.raspberrypi.org/ (дата обращения: 10.12.2024).

ПРОТИВОДЕЙСТВИЕ ПРОДВИЖЕНИЮ НЕЖЕЛАТЕЛЬНОЙ ИНФОРМАЦИИ В МЕДИАПРОСТРАНСТВЕ

Харитонов Артемий Андреевич
Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича, студент, Санкт-Петербург, Россия

Сахаров Дмитрий Владимирович
Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича, доцент, кандидат технических наук, Санкт-Петербург, Россия

Борисов Сергей Валерьевич
Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича, аспирант, Санкт-Петербург, Россия
serbor2016@yandex.ru

Аннотация
Статья посвящена анализу проблемы распространения нежелательной информации в современном медиапространстве. На основе иерархического подхода автором предложена классификация различных видов нежелательного контента, охарактеризовано его многоуровневое деструктивное влияние на общественное сознание. Выявлены составляющие элементы российской организационной и нормативно-правовой инфраструктуры противодействия информационным угрозам, констатирована ограниченная эффективность традиционных рестриктивных мер в условиях нарастания геополитической напряженности и технологических вызовов. Обоснована необходимость проактивного подхода к информационной безопасности с опорой на передовые разработки в сфере искусственного интеллекта. С учетом российского и китайского опыта сформулированы приоритетные направления оптимизации системы противодействия нежелательной информации, интегрирующие нормативно-правовые, организационные, технологические и социокультурные механизмы.

Ключевые слова
Медиапространство, нежелательная информация, информационная безопасность, искусственный интеллект, цифровая грамотность, информационные угрозы, противодействие

Введение

Медиапространство в современном мире выступает в качестве широкоформатной и многоканальной системы, обеспечивающей стремительное распространение информации. Будучи коммуникативным и информационным средством, медиапространство одновременно предстает как мощный инструмент целенаправленного воздействия и как семиотическая система, формирующая и транслирующая смыслы – иначе говоря, как подчеркивает Л. Б. Зубанова, любая информация в медиапространстве может рассматриваться «в качестве носителя ценностного содержания» [1, с. 16]. Позитивный потенциал данной характеристики, несомненно, доминирует и проявляется в информировании широкой аудитории, оперативном освещении значимых событий, предоставлении платформы для общественного диалога и дискуссий. Однако наряду с конструктивными аспектами функционирования медиапространства существуют и негативные проявления, и вытекающие из них деструктивные последствия, требующие пристального внимания и анализа.

Одной из наиболее серьезных проблем современного медиапространства является распространение нежелательной информации, в рамках данного исследования понимается широкий спектр контента, способного нанести вред индивидуальному и общественному сознанию, спровоцировать социальную напряженность, дестабилизировать политическую ситуацию и подорвать духовно-нравственные основы социума. Вопросы мониторинга и противодействия вредоносной и нежелательной информации представляют особый интерес ученых [12]. В средствах массовой информации, равно как и в научных кругах, обсуждается аспект, касающийся национальной безопасности, а именно информационно-психологическая безопасность и информационные войны [11]. Усугубляется проблема распространения информации рекомендательными технологиями в пространствах социальных сетей [13]. Такого рода информация может использоваться в проведении социоинженерных атак, например, фишинг [14, 15, 17, 18].

Цель данной статьи заключается в освещении проблемы распространения нежелательной информации в медиапространстве, анализе ее деструктивных последствий и систематизации методов противодействия данному феномену.

Результаты исследований

В рамках настоящего исследования представляется целесообразным осуществить разграничение различных видов нежелательной информации, циркулирующей в современном медиапространстве. Применяя иерархический подход, мы можем выстроить следующую классификацию и отобразить ее графически: на наиболее общем уровне выделяются две основные категории - недостоверная информация и деструктивный контент (рис. 1).

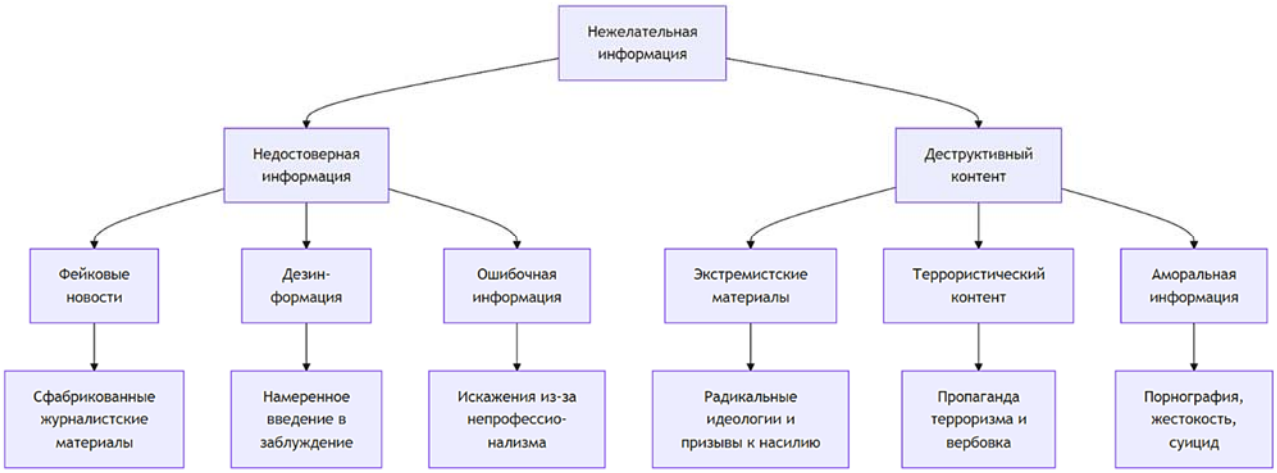


Рис. 1. Классификация нежелательной информации в медиапространстве

Недостоверная информация, в свою очередь, подразделяется на фейковые новости (преднамеренно сфабрикованные сообщения, имитирующие журналистские материалы), дезинформацию (ложные или вводящие в заблуждение сведения, распространяемые с целью введения аудитории в заблуждение) и непреднамеренно ошибочную информацию (искаженные данные, возникающие вследствие непрофессионализма или добросовестных заблуждений коммуникаторов). Деструктивный контент, со своей стороны, включает в себя экстремистские материалы (пропаганду радикальных идеологий, призывы к насильственным действиям, возбуждение ненависти и вражды), террористический контент (информацию, направленную на пропаганду терроризма, вербовку сторонников, инструктирование по совершению терактов), а также информацию, нарушающую нормы морали и нравственности (порнографию, пропаганду жестокости, насилия, суицидального поведения).

Глубинное воздействие нежелательной информации на общественное сознание также может быть представлено в виде многоуровневой модели:

1) На первичном уровне происходит искажение фактов, создание ложной картины реальности, что приводит к дезориентации аудитории и формированию ошибочных представлений.

2) Вторичный уровень воздействия связан с эмоциональными и психологическими эффектами – нежелательная информация способна провоцировать тревожность, страх, агрессию, стимулировать иррациональное поведение.

3) Третий, глубинный уровень затрагивает ценностно-мировоззренческие основы личности – под влиянием деструктивного контента происходит трансформация базовых убеждений, морально-этических принципов, что может привести к радикализации взглядов и девиантному поведению.

Как становится ясно, нежелательная информация оказывает многоаспектное негативное воздействие на индивидуальное и массовое сознание, подрывая основы социальной стабильности и затрагивая различные сферы общественной жизни. Согласно последнему международному исследованию, проведенному в феврале 2024 года, значительная часть пользователей новостных ресурсов регулярно сталкивается с недостоверными сведениями, причем наиболее подвержена искажениям политическая тематика (рис. 2) [8].

Рис. 2. Доля потребителей новостей, столкнувшихся с ложной или вводящей в заблуждение информацией по ключевым темам за последнюю неделю в мире (февраль 2024)

Любое значимое событие вызывает общественную реакцию и резонанс [16]. Исходя из этого, одним из серьезных последствий распространения нежелательной информации является снижение доверия к средствам массовой информации и в целом к информационным структурам страны. В США, как показывают опросы, только около 40% опрошенных выразили доверие к большинству источников новостей, связанных с президентскими выборами 2024 года [9]. Согласно другим статистическим данным, в ряде стран все больше растет общественный тренд избегания новостей: так, в Греции и Болгарии 57% респондентов заявили, что намеренно решили не читать новости; активное избегание новостей также было распространено в Аргентине, Польше и Великобритании, где доля респондентов, заявивших, что они так поступают, составила более 40% [7].

Несмотря на то, что в России существует как развитая организационная, включающая специализированные подразделения органов государственной власти (Роскомнадзор, управления МВД по противодействию экстремизму, кибердружины и др.), так и нормативно-правовая база, регулирующая информационную сферу (в частности, Федеральный закон от 27.07.2006 N 149-ФЗ «Об информации, информационных технологиях и о защите информации», Доктрина информационной безопасности Российской Федерации от 5 декабря 2016 г. № 646, Стратегия развития информационного общества в Российской Федерации на 2017-2030 годы от 9 мая 2017 г. N 203), проблема также растет.

Согласно опросам ВЦИОМ, 40% россиян сталкивались с новостями в медиапространстве, которые впоследствии оказывались недостоверными, при этом наибольшая доля фейковой информации была характерна для интернет-платформ (18%), социальных сетей (17%) и телевидения (11%) [3]. Данная статистика свидетельствует о недостаточной эффективности существующих механизмов противодействия нежелательной информации, особенно в контексте напряженного политического расклада последних лет, характеризующегося конфликтами между Россией и Украиной, Россией и Западом. Как в общественном дискурсе (по состоянию на 2023 г. 87% опрошенных россиян считают, что в настоящий момент «ведется информационная война в связи с военной операцией России на Украине») [3], так и в научном дискурсах все чаще звучит понятие «информационной войны», трактуемое как противоборство в информационном пространстве с целью достижения информационного превосходства, нанесения ущерба информационным системам, процессам и ресурсам противника [6]. Информационная война становится неотъемлемым аспектом современных геополитических противостояний [2], что актуализирует необходимость разработки эффективных стратегий информационной безопасности.

Негативные последствия распространения нежелательной информации в медиапространстве диктуют императив активного противодействия данному феномену. Несмотря на существование многочисленных IT-отделов модерации контента, масштабы распространения нежелательной информации растут примеру – так, в 2021 г. в соц. сети Facebook[1] было удалено практически 100 млн. публикаций противоправного и экстремистского контента [5].

[1] Принадлежит Meta – признана в России экстремистской организацией и запрещена.

Традиционный подход, основанный на постфактумном реагировании и блокировке деструктивного контента, демонстрирует свою ограниченность в условиях стремительного развития информационно-коммуникационных технологий. Учитывая стратегический курс России на достижение технологического суверенитета, представляется очевидным, что технологические инструменты должны быть интегрированы в систему обеспечения информационной безопасности. Это предполагает несколько перспективных направлений: внедрение автоматизированных систем мониторинга и анализа медиапространства, способных оперативно выявлять нежелательный контент; разработка алгоритмов машинного обучения для идентификации фейковых новостей и манипулятивных техник; создание платформ верификации информации на основе блокчейн-технологий.

Наиболее инновационным и многообещающим направлением противодействия нежелательной информации является использование достижений искусственного интеллекта (ИИ), активно обсуждаемое в научном дискурсе [4]. Несмотря на то, что правовое регулирование ИИ в России находится на начальной стадии (Федеральный закон от 31.07.2020 г. No 258-ФЗ «Об экспериментальных правовых режимах в сфере цифровых инноваций в Российской Федерации» охватывает 14 направлений, среди которых отсутствует информационная безопасность), разработки в данной сфере ведутся. Примерами являются информационные системы «Окулус» и «Вепрь», функционирующие при поддержке Роскомнадзора и работающие в связке, а также эффективно зарекомендовавшее себя частное программное обеспечение «Крибрум» (табл. 1).

Таблица 1

Система	Функциональные возможности
«Окулус»	Система осуществляет комплексный мультимедийного контента, используя передовые алгоритмы обработки изображений. В основе работы лежит многоуровневая проверка содержания на предмет наличия запрещённых материалов (пронакротического, ЛГБТ- и экстремистского характера), тип анализируемого контента – изображения и видео. Дополнительно реализована возможность автоматической генерации отчётов и прямой интеграции с государственными информационными системами.
«Вепрь»	Данная система реализует непрерывный мониторинг средств массовой информации и социальных сетей, концентрируясь на выявлении противоправного контента, тип анализируемого контента - текст. Производится углубленный анализ метаданных и отслеживание первоисточников распространения информации. Реализованы инструменты для определения точек «напряженности», моделирования различных сценариев распространения информации и оценки потенциальных рисков.
«Крибрум»	Программное обеспечение реализует многоуровневый семантический анализ с возможностью распознавания контекста, подтекста и эмоциональной окраски сообщений. Система способна выявлять скрытые смысловые связи, манипулятивные конструкции и различные пропагандистские техники. Особое внимание уделяется отслеживанию информационных кампаний и оценке достоверности источников. В области прогнозирования система предлагает инструменты для анализа социальных графов, оценки влияния на целевую аудиторию и выявления потенциальных угроз. Дополнительный функционал включает возможности построения детальных социальных графов, анализа целевой аудитории, выявления ботов и фейковых аккаунтов.

Данные системы способны осуществлять семантический анализ контента, выявлять манипулятивные техники, прогнозировать распространение информации в социальных медиа. Однако для полноценной реализации потенциала ИИ в сфере информационной безопасности необходимо формирование соответствующей стратегии на законодательном уровне. Показательным примером в данном контексте является стратегический партнер России – Китайская Народная Республика, где ИИ уже давно интегрирован в систему правового регулирования (в частности, в Закон КНР «О кибербезопасности», "План развития искусственного интеллекта нового поколения" (2017 г.)). В 2023 году в Китае было принято Положение о глубоком синтезе (дипфейках), устанавливающее правовые рамки использования технологий на основе ИИ [10]. Данный опыт свидетельствует о важности не только активного, но и проактивного подхода к противодействию нежелательной информации, предполагающего опережающее правовое регулирование и стимулирование технологических разработок.

Учитывая вышесказанное, в рамках проактивного подхода к обеспечению информационной безопасности представляется необходимым развитие следующих направлений:

1. Дальнейшая актуализация и гармонизация нормативно-правовой базы, регулирующей информационную сферу, с учетом динамики технологического развития и появления новых типов

информационных угроз. Приоритетное внимание должно быть уделено расширению правовых основ применения ИИ-инструментов информационной безопасности, обеспечению баланса между свободой информации и защитой от деструктивного контента.

2. Укрепление организационной инфраструктуры противодействия нежелательной информации за счет усиления координации профильных государственных органов, общественных организаций, научно-экспертного сообщества. Повышение уровня компетенций и ресурсного обеспечения специализированных подразделений, осуществляющих мониторинг и анализ информационного пространства.

3. Стимулирование разработки и внедрения передовых технологических решений в сфере информационной безопасности, в том числе основанных на использовании ИИ. Формирование полноценной инновационной экосистемы в данной области, включающей как прикладные исследования и разработки, так и механизмы трансфера и коммерциализации технологий. Особое внимание должно быть уделено созданию ИИ-инструментов автоматизированного выявления фейковых новостей, дезинформации, деструктивного контента.

4. Повышение цифровой грамотности и информационной культуры населения, развитие компетенций критического восприятия и верификации потребляемого контента. Реализация масштабных программ информационного просвещения и медиаобразования для различных возрастных и социальных групп. Культивирование высоких этических стандартов коммуникации в цифровом пространстве.

5. Укрепление международного сотрудничества в области противодействия информационным угрозам, в том числе на базе механизмов ООН, ШОС, БРИКС, ОДКБ. Обмен передовыми практиками и технологическими решениями, выработка общих подходов и стандартов информационной безопасности. Формирование коалиций государств (возможно рассмотрение сотрудничества в триаде Россия-Индия-Китай, где информационные достижения имеют достаточно высокий уровень и могут взаимодополнять друг друга) для противостояния попыткам деструктивного воздействия в глобальном информационном пространстве.

Реализация данных направлений позволит сформировать многоуровневую систему противодействия нежелательной информации, интегрирующую правовые, технологические, институциональные и социокультурные механизмы. Проактивный подход, основанный на опережающем реагировании и превентивных мерах, станет залогом обеспечения информационной безопасности в условиях стремительно меняющегося технологического ландшафта и геополитических вызовов современности равно как для России, так и для прочих – уже развитых и еще развивающихся – государств.

Литература

1. *Зубанова Л.Б.* Современное медиапространство: подходы к исследованию и принципы интерпретации // Вестник Челябинской государственной академии культуры и искусств. 2008. № 2(14). С. 6-17. EDN JXEKLH

2. *Лисиченко Е.Т., Трофимюк В.К.* Информация как оружие: проблема информационных войн в современном мире // Международный терроризм как инструмент внешней политики США и НАТО : Материалы IV-й республиканской студенческой научной конференции, Донецк, 19 мая 2023 года / Отв. редактор Т.Э. Рагозина. Донецк: Донецкий национальный технический университет, 2023. С. 54-58. EDN RFSHHV

3. Фейк-ньюс – и как с ними бороться? [Электронный ресурс] // ВЦИОМ. URL: https://wciom.ru/analytical-reviews/analiticheskii-obzor/feik-njus-i-kak-s-nimi-borotsja?ysclid=m5w3o4qapt125686604 (дата обращения: 14.01.2025).

4. *Pervaiz Akhtar, Ghouri Arsalan, Khan Haseeb, Amin Ul Haq Mirza, Awan Usama, Zahoor Nadia, Khan Zaheer, Ashraf Aniqa.* Detecting fake news and disinformation using artificial intelligence and machine learning to avoid supply chain disruptions. Annals of Operations Research. 2022. 327. 10.1007/s10479-022-05015-5.

5. Actioned hate speech content items on Facebook worldwide from 4th quarter 2017 to 2nd quarter 2024 [Электронный ресурс] // Statista. URL: https://www.statista.com/statistics/1013804/facebook-hate-speech-content-deletion-quarter/ (дата обращения: 10.10.2024).

6. *Brichkov A.S., Nikonorov G.A., Pertsev A.A*. Russian information space in the era of «hybrid war»: defense or attack // Bulletin of Polessky State University. Series in Social Sciences and Humanities. 2023. No. 2, pp. 53-60. EDN PGHCAH

7. Countries with the highest share of audiences actively avoiding the news worldwide as of February 2023[Электронный ресурс] // Statista. URL: https://www.statista.com/statistics/235550/daily-news-access-in-the-us-by-age/ (дата обращения: 14.01.2025).

8. News consumers who saw false or misleading information about key topics in the last week worldwide as of February 2024 [Электронный ресурс] // Statista. URL: https://www.statista.com/statistics/1317019/false-information-topics-worldwide/ (дата обращения: 14.01.2025).

9. Most trusted news sources for information about the 2024 presidential election in the United States as of June 2023, by political affiliation [Электронный ресурс] // Statista. URL: https://www.statista.com/statistics/1451327/trust-in-election-news-source-us-by-politics/ (дата обращения: 14.01.2025).

10. 2023 Новые правила в области искусственного интеллекта в Китае/China's New AI Regulations, Latham&Watkins [Электронный ресурс] // ИИ РФ. URL: https://ai.gov.ru/knowledgebase/normativnoe-regulirovanie-ii/2023_novye_pravila_v_oblasti_iskusstvennogo_intellekta_v_kitae_china_s_new_ai_regulations_latham_watkins_/ (дата обращения: 14.01.2025).

11. *Виткова Л.А., Проноза А.А., Сахаров Д.В., Чечулин А.А*. Проблемы безопасности информационной сферы в условиях информационного противоборства // В сборнике: Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2018). VII Международная научно-техническая и научно-методическая конференция. Сборник научных статей. В 4-х томах. Под редакцией С.В. Бачевского. 2018. С. 191-195.

12. *Виткова Л.А., Чечулин А.А., Сахаров Д.В*. Выбор мер противодействия вредоносной информации в социальных сетях // Вестник Воронежского института ФСИН России. 2020. № 3. С. 20-29.

13. *Борисов С.В., Мосикян А.А., Сахаров Д.В.* Боты в социальных сетях // В сборнике: Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2024). Сборник научных статей XIII Международной научно-технической и научно-методической конференции. Санкт-Петербург, 2024. С. 560-563.

14. *Борисов С.В., Севостьянов В.А., Цветков А.Ю.* Определение признаков фишинговых сообщений в электронной почте // В сборнике: Студенческая весна - 2023. Материалы 77-ой региональной научно-технической конференции студентов, аспирантов и молодых ученых. Санкт-Петербург, 2023. С. 88-92.

15. *Штеренберг С.И., Стародубцев И.В., Шашкин В.С*. Разработка комплекса мер для защиты предприятия от фишинговых атак // Защита информации. Инсайд. 2020. № 2 (92). С. 24-31.

16. *Сахаров Д.В., Шашкин В.С.* Система противодействия распространению вредоносной информации в социальных сетях // В сборнике: Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2020). IX Международная научно-техническая и научно-методическая конференция : сборник научных статей. Санкт-Петербург, 2020 С. 783-787.

17. *Борисов С.В.* Актуальность проблемы выявления сгенерированного видео с использованием технологий искусственного интеллекта в социальных сетях и цифровых медиа // В сборнике: Безопасные информационные технологии. Сборник трудов Тринадцатой международной научно-технической конференции. Москва, 2024 С. 42-45.

18. *Бударный Г.С., Дюсметова А.А., Казанцев А.А., Красов А.В.* Социальная инженерия: её методы и способы защиты // В сборнике: Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2023). Сборник научных статей. XII Международная научно-техническая и научно-методическая конференция. В 4 т. Санкт-Петербург, 2023 С. 200-204.