DSPA:

Вопросы применения цифровой обработки сигналов

№2

2025

СОДЕРЖАНИЕ

ИСПОЛЬЗОВАНИЕ РАДИООПТИЧЕСКИХ УСТРОЙСТВ В СВЕРХШИРОКОПОЛОСНЫХ СВЧ СИСТЕМАХ

Крячко Александр Федотович
ГУАП, заведующий кафедрой, д.т.н., Санкт-Петербург, Россия
kryachko@guap.ru

Тюрина Анастасия Игоревна
ГУАП, ассистент кафедры, Санкт-Петербург, Россия
nastyrciy@yandex.ru

Аннотация
В работе отмечена одна из тенденций развития систем связи и радиолокации – применение сигналов с большой относительной шириной спектра, проанализированы их преимущества и недостатки. Рассматриваются преимущества использования радиооптических приборов по сравнению с традиционными системами передачи СВЧ энергии. Оценены перспективы их использования для генерации сверхширокополосных сигналов, передачи СВЧ энергии на значительные дистанции, в распределителях активных фазированных антенных решеток (АФАР).

Ключевые слова
Сверхширокополосный ЛЧМ сигнал, радиооптический элемент, генератор, лазерный диод, оптический разветвитель, катушка, интерферометр, зеркало, EDFA, биения, фотодиод

Введение

Одним из перспективных направлений развития радиолокационной техники является применение сверхширокополосных (СШП) сигналов – сигналов с большой относительной шириной спектра [1]. Их использование позволяет повысить информативность радара за счет уменьшения импульсного объема по дальности. Уменьшается "мертвая зона", повышается разрешающая способность по всем координатам, устойчивость радара к воздействию внешних электромагнитных излучений и помех и скрытность его работы. За счет увеличения «обобщенного» поперечника рассеяния улучшается способность радара обнаруживать цели, снимается проблема "слепых" скоростей, пропадает проблема "мертвого" времени. СШП радиолокационноая станция (РЛС) позволяет получать «радиоизображение» цели, что позволяет проводить ее идентификацию по ранее созданным «базам радиопортретов» с использованием искусственного интеллекта [2].

Однако в процессе генерации, излучения, приема и обработки СШП сигналов существуют определенные сложности. Сигнал претерпевает изменения в процессе излучения, распространения, рассеянии на цели и приеме РЛС. Эти изменения необходимо учитывать.

Кроме того, традиционная элементная база сверхвысокочастотной (СВЧ)-техники (клистроны, магнетроны), используемая для генерации и передачи таких сигналов (коаксиальные кабели, волноводы) имеет большой вес, стоимость и энергопотребление. Во многих случаях это не приемлемо для бортовых устройств. Один из путей преодоления этих сложностей – использование радиооптических устройств [3].

Их основными преимуществами являются низкие потери и дисперсия, широкая рабочая полоса частот, малые фазовые шумы и высокая фазовая стабильность [4]. При затухании оптической несущей с частотой 200 ТГц менее 0.2 дБ/км доступная полоса частот составляет десятки террагерц [5].

Для радиооптических элементов характерна малая масса, размеры. Они устойчивы к воздействию паразитных электромагнитных полей. Оптические схемы не создают помех в этом диапазоне и устойчивы к фазовым шумам [5].

На основе радиоптических элементов могут быть созданы электронные устройства с параметрами, недостижимыми традиционной элементной базы СВЧ диапазона [6].

В ряде случаев представляется возможным непосредственное преобразование оптического сигнала в СВЧ колебание и излучение его с помощью радиофотонной антенны. Этот вариант особенно

привлекателен при проектировании бортовых устройств, так как позволяет существенно снизить габариты и массу радиолокационной аппаратуры [7].

Основной недостаток фотонных элементов – подверженность амплитудным шумам и значительное ослабление сигнала при модуляции/демодуляции, которое приходится компенсировать усилением. Однако достоинства рассматриваемых устройств превалируют над их недостатками [7].

Результаты исследований

В радиолокационной практике часто возникает необходимость использования сигнала линейной частотной модуляцией (ЛЧМ)-сигнала. Частота внутри импульса такого сигнала меняется по линейному закону либо возрастая, либо убывая.

Генерация сверхширокополосных ЛЧМ сигналов с использованием радиооптики

Для генерации сверхширокополосного сигнала этого типа в ряде случаев может быть использован компактный радиооптический генератор (рисунок 1).

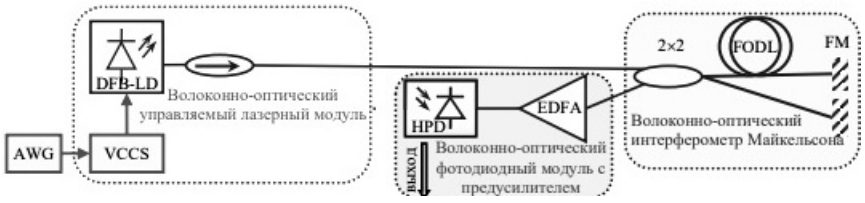

Рис. 1. Схема радиооптического генератора [2]

В литературе для генерации сверхширокополосных СВЧ-сигналов предложены различные варианты фотонных схем [4-8]. В качестве иллюстрации возможностей радиооптических устройств в [8] приведено устройство на основе автогетеродинирования лазера. Принцип его работы состоит в изменении частоты светового сигнала за счет изменения тока накачки. Изменение накачки приводит к изменению плотности носителей в резонаторе лазера. Исходная нелинейная зависимость частоты генерации от тока должна быть скорректирована по закону, позволяющую на выходе линейную зависимость (рис. 2). На одно плечо интерферометра поступает сигнал от лазера на фиксированной длине волны, на второе - сигнал с изменяющейся частотой. Биения усиливаются и детектируются фотодиодом. Глубина модуляции регулируется с помощью изменения длительности импульсов тока за счет напряжения смещения [8]. Зеркала Фарадея сдвигают фазу на 90°.

На рисунке 2 приведен закон изменения во времени частоты выходного СВЧ сигнала. Частота меняется линейно. Для этого ток накачки также меняют линейно с периодом повторения, равным удвоенному времени задержки катушки.

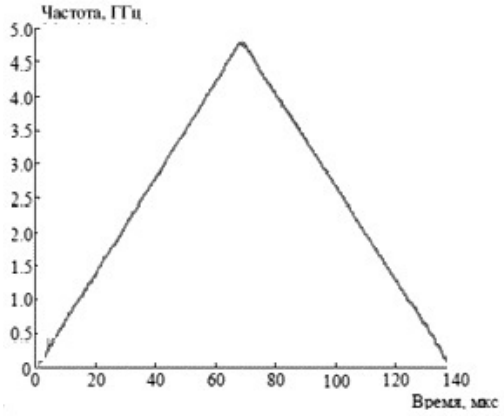

Рис. 2. Закон изменения частоты от времени

Длительность ЛЧМ сигнала превосходит время термализации частоты лазерного диода, составляющее единицы микросекунд.

Оптические каналы передачи СШП СВЧ сигналов на большие расстояния

Для передачи сверхширокополосного сигнала на десятки километров он преобразовывается в световой сигнал с использованием источника оптического излучения, модулятора (рис. 3) и подается на оптическое волокно. В качестве источника оптического излучения выступает полупроводниковый лазер на основе полупроводникового материала InGaAsP, в качестве модулятора – используется интерферометр Маха-Цандера на основе ниобата лития с СВЧ усилителем, фотодетектор. Информационный сигнал, преобразованный в оптический, для системы является узкополосным и при передаче претерпевает незначительные изменения. Поэтому он может быть передан на значительное расстояние, превышающее сотню км, практически без изменений и необходимости усиления. Такая способность волокна также используется в системах квантовой криптографии для передачи ключей шифрования [3]. На приемной стороне сигнал преобразовывается фотодетектором в СВЧ колебание, усиливаемое малошумящим усилителем, и подается на выход.

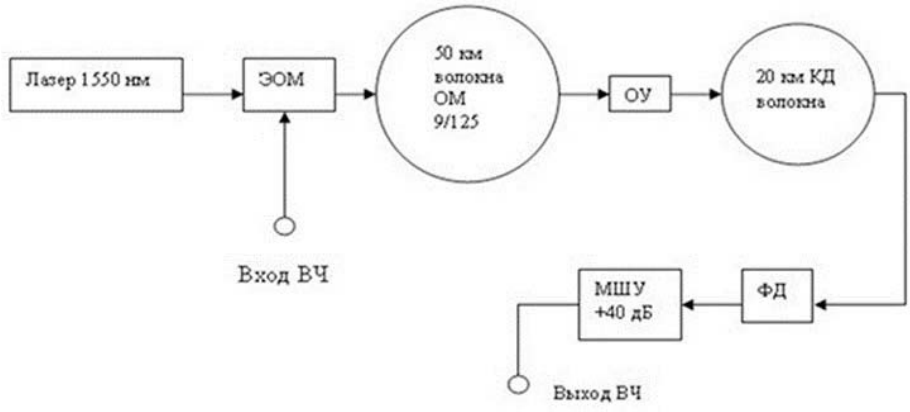

Рис. 3. Конструкция фотонного канала передачи

На рисунке 4 представлены графики амплитудно-частотной (АЧХ) и фазочастотной (ФЧХ) характеристик оптического канала передачи. Анализ характеристик позволяет сделать вывод, что оптический канал передачи СШП СВЧ сигнала практически не вносит искажений в спектр передаваемого сигнала. Такие каналы могут быть использованы в радиолокационных системах многопозиционной локации, для удаленного размещения передающего центра и т.д.

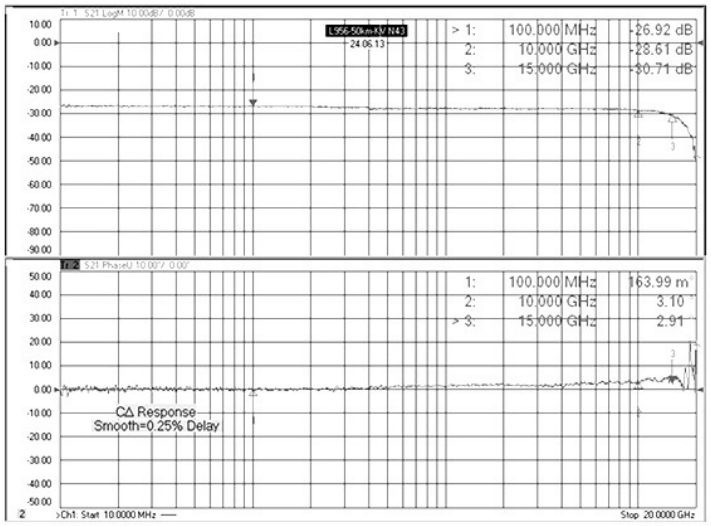

Рис. 4. АЧХ и ФЧХ оптической системы передачи в полосе 5-10 ГГц

Радиооптические измерительно-калибровочные средства для СШП РЛС

Радиооптические устройства могут быть использованы для проведения испытаний, измерений, калибровки и юстировки сверхширокополосных РЛС. При этом нет необходимости покидать цех завода-изготовителя, отпадает необходимость в проведении дорогостоящих аттестационных натурных испытаний в «поле» и экономятся существенные временные и денежные ресурсы, значительно упрощается проверка юстировка и аттестация РЛС [10]. На рисунке 5 приведена структурная схема измерительно- калибровочного стенда для приемо-сдаточных испытаний СШП РЛС.

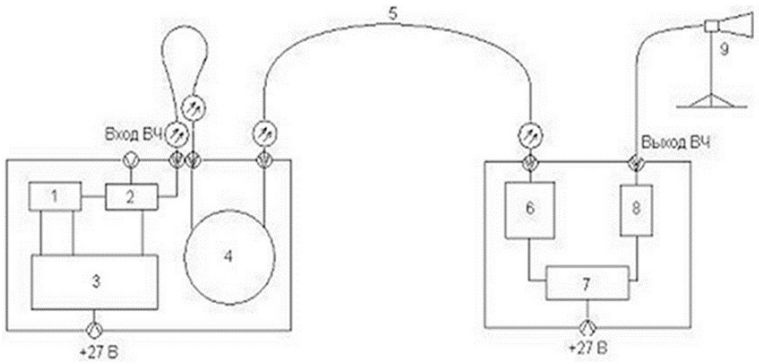

Рис. 5. Юстировочный испытательный стенд

Стенд для проведения испытаний и юстировки сверхширокополосной РЛС имитирует прохождение зондирующего сигнала от РЛС через среду распространения. В устройство входит два основных блока, соединенных волоконно-оптическим кабелем. В первом блоке осуществляется перенос зондирующего радиосигнала с помощью лазера (1) и модулятора (2) в световой сигнал, который подается на оптическую линию задержки (4), имитирующую задержку эхо сигнала.

На стенде могут использоваться различные линии задержки, позволяющие менять итоговую задержку информационного сигнала. Во втором блоке происходит обратное преобразование информационного сигнала в радиосигнал фотодетектором, усиление и излучение его через рупорную антенну. Сигнал с рупорной антенны поступает на антенную систему испытываемого радара к качеству эхосигнала от цели.

Рабочая полоса рассматриваемого стенда превышает 3 ГГц. Неравномерность АЧХ стенда в рабочей полосе частот не превышает 3 дБ, нелинейность ФЧХ – не более 10°, коэффициент передачи – не менее 10 дБ.

Архитектура оптической системы распределения СШП СВЧ сигнала по полотну АФАР

Современные активные фазированные антенные решетки широко применяются в авиации, в цифровых коммуникационных системах, радиолокационных станциях, системах спутниковой связи, радиопеленгации. Их применение позволяет обойти многие из ограничений геометрии пассивных решёток, управлять радиолучом в более широком диапазоне углов, достигать более высокого коэффициента усиления антенной системы, устранять помехи с определенных направлений, обеспечивать разнесение путей (MIMO), что повышает надежность связи. АФАР обладают большей надежностью по сравнению с другими антенными системами. Дополнительное важное преимущество АФАР – существенно меньший вес. В рассматриваемой схеме нет ни клистронов, ни магнетронов, ни их громоздких систем питания и охлаждения.

По сравнению с обычными антенными системами или пассивными антенными решетками РЛС в радаре с активной фазированной решёткой за счет лучшей энергетики можно обеспечить лучшую следящую способность. Для подведения/снятия сигнала с приемо-передающих модулей активной решетки используется распределительная система.

Традиционная распределительная система СВЧ на основе коаксиальных кабелей или волноводов весьма громоздка и дорогостояща. В качестве перспективной альтернативы может выступить оптический распределитель. Его основное достоинство-существенно меньшая масса, стоимость и габариты.

Еще одно неоспоримое достоинство рассматриваемой конструкции – помехоустойчивость, а также стабильность распределения фазы по полотну антенной системы [11].

Входная оптическая мощность и мощность выходного СВЧ сигнала связаны в распределителе квардратичной зависимостью. По этой причине в состав системы кроме электрооптических преобразователей, разветвителей должно входить два каскада усиления, что позволяет запитать необходимое число приемо-передатчиков. Элементы системы должны быть соединены волокном одинаковой длины.

Потери, возникающие при преобразовании исходного сверхширокополосного сигнала в свет и обратно, могут быть компенсированы за счет применения операционных усилителей с токовой обратной связью, достоинством которых является большая полоса пропускания и высокое быстродействие.

Стоящий на выходе фотодетектор основе фотодиода преобразует световой сигнал обратно в сверхширокополосное СВЧ-колебание, подающееся на приемо-передающий модуль АФАР.

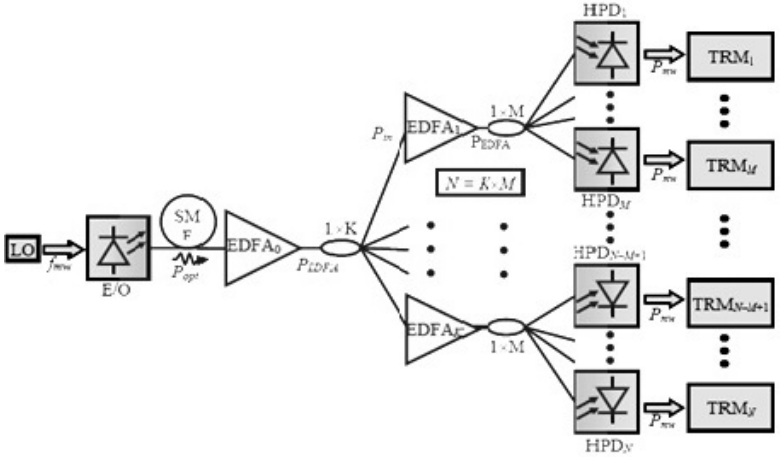

Рис. 6. Схема волоконно-оптического распределителя сигнала по полотну АФАР

Режим насыщения работы оптических усилителей можно реализовать при использовании двухкаскадной схемы. В этом режиме обеспечивается низкий уровень собственных шумов на выходе каждого канала системы что позволяет обеспечить разводку опорного СВЧ-сигнала на тысячи каналов. По сравнению с традиционными оптическая схема распределителя СВЧ энергии по полотну АФАР облает меньшими габаритами, массой, потерями. Стоимостные характеристики такой системы также более привлекательные чем у традиционных систем, использующих дорогостоящие цветные и полудрагоценные металлы [11].

Конструкция модулей системы распределения

Ключевыми элементами оптического распределителя являются лазерные модули, оптические усилители, разветвители, соединительное волокно и фотодиодные модули [11] (рис. 7).

Электрооптический модулятор (лазерный модуль) меняет интенсивность светового сигнала в соответствии с законом изменения, поданного на вход системы СШП СВЧ сигнала. В качестве электрооптического преобразователя (рис. 8) используется лазерный модуль с внешней модуляцией оптического излучения по интенсивности с помощью модулятора Маха-Цандера (MZM). Модулятор подключается через драйвер, представляющий собой объединенный в одно устройство широкополосный СВЧ усилитель и источник постоянного напряжения смещения, задающей рабочую точку. Как правило выбирается «квадратурная» рабочая точка, в которой производная функции передачи модулятора максимальна.

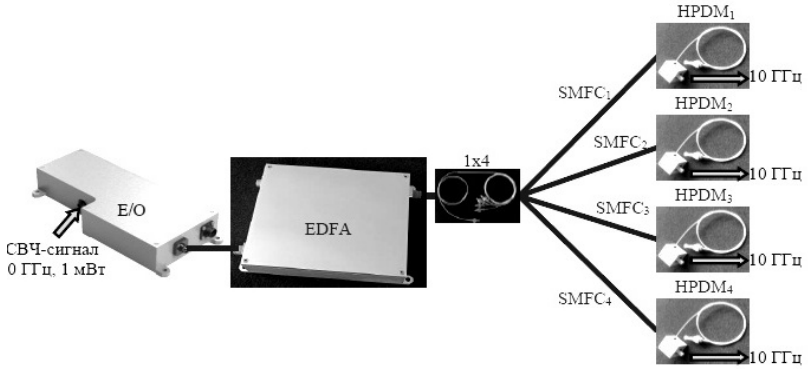

Рис. 7. Распределить на 4 канала

Ввиду значительных габаритов электрооптические модуляторы обычно размещаются за пределами полотна АФАР.

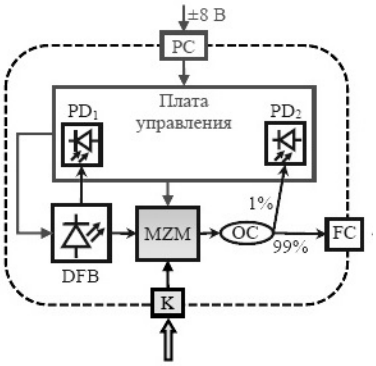

Рис. 8. Лазерный модуль

В качестве оптического усилителя может быть использован рамановский или полупроводниковый оптический усилитель. Однако в рассматриваемой системе целесообразно использовать усилители на основе оптического волокна, легированного эрбием (Erbium Doped Fibre Amplifier, сокращенно EDFA), получившие в настоящее время наибольшую популярность за счёт низкой стоимости и простоты производства (рис. 9). EDFA усиливает оптический сигнал, не преобразуя его в электрический и обладает широкой полосой. Накачку обеспечивают два одночастотных диода с обратной связью. Лазеры накачки могут устанавливаться как по направлению распространения полезного сигнала, так и против него. В двухступенчатых усилителях используются оба типа накачки для получения преимуществ обоих типов. WDM-фильтры предназначены для смешивания полезного сигнала с сигналом накачки. Оптический изолятор ISO пропускает через себя только полезный сигнал, отсекая сигнал накачки.

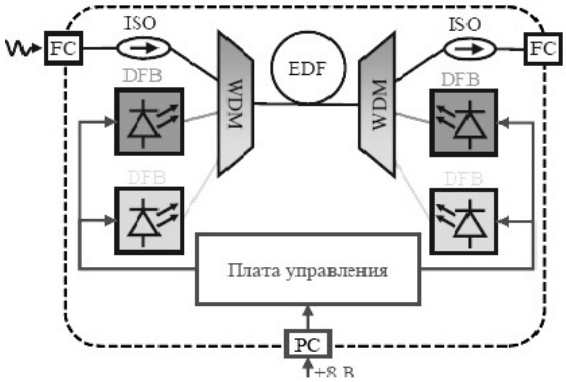

Рис. 9. Оптический усилитель

Фотодиодный модуль (рисунок 10) системы предназначен для преобразования поступающего на его вход светового сигнала обратно в СШП СВЧ колебание и передаче его на приемопередатчик. [12].

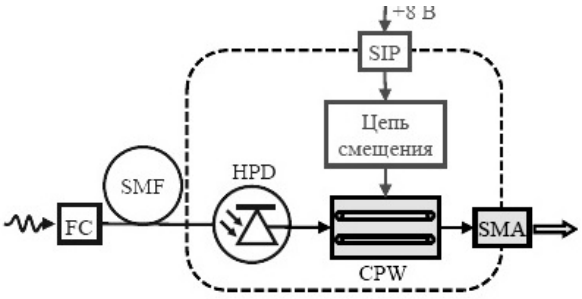

Рис. 10. Конструкция фотодиодного модуля

Электрический сигнал с выхода мощного фотодиода подается на вход компланарной СВЧ линии передачи и далее на вход приемо-передатчика АФАР.

Для решения задачи миниатюризации в состав СВЧ антенны передающего или приемного модуля может быть включен лазерный диод или фотодиод соответственно. Традиционная линии передачи (коаксиальная или волноводная) заменена в таком устройстве оптическим волокном.

Следует отметить, что при всех достоинствах такой антенны она может быть либо только приемной, либо передающей.

Характеристики системы распределения

Достоинством рассматриваемой типовой волоконно-оптической системы распределения СВЧ сигнала по полотну АФАР СШП РЛС является высокая временная стабильность амплитуды распределяемого СВЧ-сигнала в каналах, что обеспечивает точность электронного управления лучом.

На рисунке 11 приведена зависимость амплитуды от времени на частоте 10 ГГц в одном из каналов системы. Изменение амплитуды за половину суток не превысило значения ±0.6 дБ.

Возможность управления амплитудным распределением по полотну АФАР позволяет осуществлять управление лучом в диапазонах, не достижимых для пассивных антенных решеток.

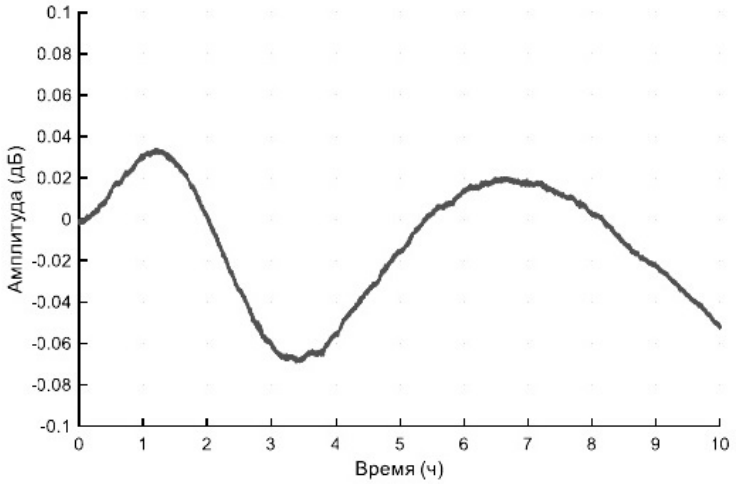

Рис. 11. Зависимость амплитуды сигнала канала системы распределения на рабочей частоте 10 ГГц от времени [12]

Для уменьшения вероятности возникновения паразитного фазового сдвига между каналами распределителя необходимо с высокой точностью выдерживать равенство длин волокна, связывающего элементы системы. Если это условие выполняется, то относительный сдвиг между каналами невелик и за 10 часов не превышает значения ±0.5 (рис. 12).

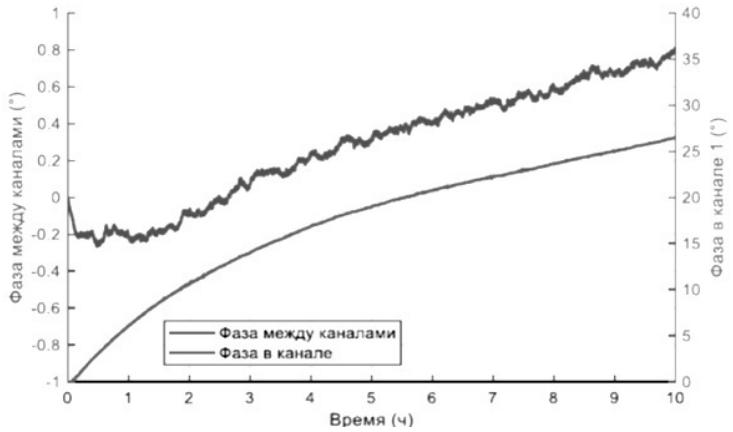

Рис. 12. График дрейфа фазы СШП сигнала

Если сравнить уровень фазового шума входного СШП колебания на входе и на выходе оптического распределителя (рис. 13), то можно сделать вывод, что для значительного диапазона отстройки уровень шума меняется незначительно, что свидетельствует о так как уровень собственных шумов системы что свидетельствует о малом уровне собственных шумов оптического тракта [12].

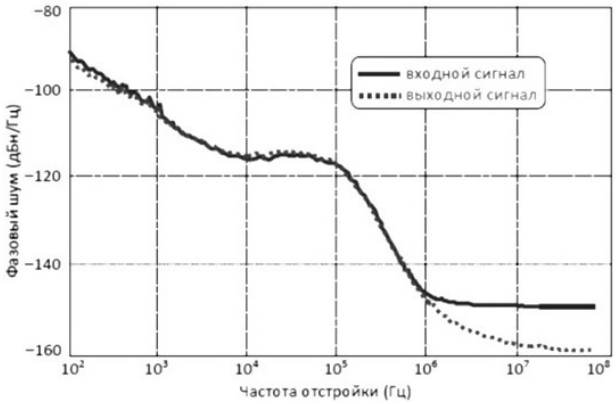

Рис. 13. Фазовый шум СШП сигнала на входе (пунктир) и на выходе (сплошная) распределителя

Оценка степени искажения зондирующего сверхширокополосного сигнала оптическим распределителем

Для оценки степени искажений зондирующего сверхширокополосного сигнала целесообразно проанализировать неравномерность амплитудо-частотной и нелинейность фазочастотной характеристики системы, а также взаиморасположение амплитудного спектра информационного сверхширокополосного колебания и АЧХ системы.

Сверхширокополосный сигнал после переноса в световую область для оптической системы является узкополосным. Неравномерность АЧХ в области несущей частоты (рис. 14) не превышает 3 дБ.

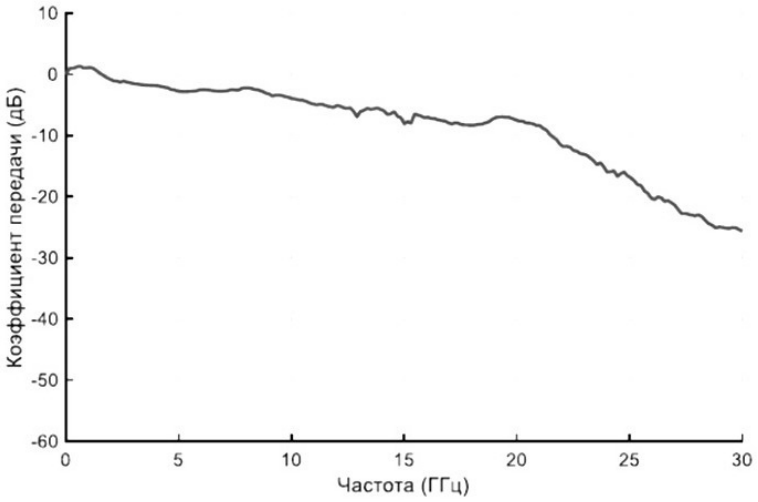

Рис. 14 АЧХ оптического канала

При прохождении оптического тракта уровень спектральных составляющих СШП сигнала достаточно равномерно уменьшается, что приводит к уменьшению энергии сигнала. Чуть значительней уменьшается уровень высокочастотных составляющих спектра, что вызывает незначительное увеличение длительности и затягивание фронта.

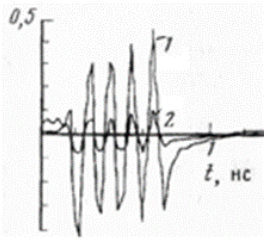

Рис. 15. Сигнал на входе и выходе радиофотонной системы:
1-входной сигнал, 2-выходной сигнал

В целом можно сделать вывод о том, что при прохождении исходного сверхширокополосного колебания через канал оптического распределителя СВЧ энергии по полотну АФАР изменения сигнала минимальны.

Заключение

Использование сверхширокополосных сигналов в радиолокационных системах дает возможность повысить информативность, разрешающую способность, помехоустойчивость, скрытность работы. СШП РЛС позволяют распознавать цели на основе ее «радиоизображения». Некоторые сложности, возникающие при генерации, передаче, излучении, приеме сигналов с большой относительной шириной спектра могут быть преодолены за счет использования радиооптических устройств. Их использование существенно уменьшает массогабаритные, стоимостные и энергетические характеристики таких систем.

При прохождении СШП сигнала через оптический тракт передаваемые сигналы претерпевают незначительные изменения. Перспективным направлением использования радиооптических устройств является их применение в активных фазированных антенных решетках СШП РЛС и системах связи. Двухкаскадная схема позволяет распределить исходный сигнал на большое количество приемо-передающих элементов. В качестве приемного или передающего элемента возможно использование фотонной антенны. В этом случае сигнал подводится или снимается с подобного элемента с помощью оптического волокна.

При этом открытым вопросом остается учет искажений, вносимых в излучаемый (принимаемый) сигнал фотонной антенной.

Литература

1. *Иммореев И.Я.* Сверхширокополосные радары: новые возможности, необычные проблемы, системные особенности // Вестник МГТУ. Сер. Приборостроение, 1998, №4.

2. *Тейлор Д.Д.* Сверхширокополосные технологии в радиолокации, Бока Ратон, Лондон, Нью-Йорк, Вашингтон, СИ ЭР СИ Пресс, 2000, 27 с.

3. О практике применения радиофотонных устройств в радиолокации [Электронный ресурс] https://centervospi.ru/articles/o-praktike-primeneniya-radiofotonnyh-ustrojstv-v-radiolokacii/ (дата обращения: 21.01.2025).

4. *Kun Xu, Ruixin Wang, Yitang Dai, Feifei Yin, Jianqiang Li, Yuefeng Ji, Jintong Lin.* Microwave photonics: radio-over-fiber links, systems, and applications // Photonics Research. 2014. Vol. 2. №4, pp. B54-B63.

5. *Luo X., Wang A., Wo J., Wang Y., Fu J., Zhu Y., Zhang J., Cong W., Liu R., Yang H., Yu L.* Microwave photonic video imaging radar with widely tunable bandwidth for monitoring diverse airspace targets // Optics Communications. 2019. Vol. 451, pp. 296-300.

6. *Pan S., Zhang Y.* Microwave photonic radars. Journal of Lightwave Technology. 2020. Vol. 38. №19, pp. 5450-5484.

7. *Chi H., Wang C., Yao J.* Photonic generation of wideband chirped microwave waveforms // IEEE Journal of Microwaves. 2021. Vol. 1. №3, pp. 787-803.

8. *Serafino G., Scotti F., Lembo L., Hussain B., Porzi C., Malacarne A., Maresca S., Onori D., Ghelfi P., Bogoni A.* Toward a new generation of radar systems based on microwave photonic technologies. Journal of Lightwave Technology. 2019. Vol. 37. №2, pp. 643-650.

9. *Микитчук К.Б., Лебедев А.С., Чиж А.Л.* Метод генерации сверхширокополосных СВЧ-сигналов с линейно-частотной модуляцией на основе самогетеродинирования излучения лазерного диода // Журнал радиоэлектроники. 2022. №12.

10. Использование аналоговой волоконно-оптической линии передачи СВЧ сигналов для контроля параметров радиолокационной станции X-диапазона. https://centervospi.ru/technology/sistemy-kontrolya-rls/ispolzovanie-analogovoj-volokonno-opticheskoj-linii-peredachi-svch-signalov-dlya-kontrolya-parametrov-radiolokacionnoj-stancii-x/ (дата обращения: 21.01.2025).

11. *Чиж А.Л., Микитчук К.Б.* Волоконно-оптическая система распределения сигнала СВЧ- гетеродина для активных фазированных антенных решеток // Журнал радиоэлектроники. 2023. №2.

12. *Малышев С.А., Чиж А.Л., Микитчук К.Б.* Волоконно-оптические лазерные и фотодиодные модули СВЧ-диапазона и системы радиофотоники на их основе // IV Всероссийская научно-техническая конференция «Электроника и микроэлектроника СВЧ».

АНАЛИЗ АЛГОРИТМОВ ОТСЛЕЖИВАНИЯ ДВИЖЕНИЯ НА БАЗЕ ГЛУБОКОГО ОБУЧЕНИЯ

Горохов Кирилл Игоревич
магистрант МТУСИ, Москва, Россия
studentGorokhov@gmail.com

Тремасова Лилия Андреевна
МТУСИ, аспирантка группы АЭФ2301(15), Москва, Россия
l.a.tremasova@mtuci.ru

Савин Всеволод Артёмович
МТУСИ, аспирант группы АЭФ2401(15), Москва, Россия
savin.vsevolod@icloud.com

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

Аннотация
Проводится сравнительный анализ алгоритмов отслеживания движения на базе глубокого обучения. Рассматриваются такие решения, как OpenPose, AlphaPose. Каждый из этих инструментов использует различные подходы и методы для распознавания и отслеживания движений человека, что делает их актуальными в задачах компьютерного зрения и глубокого обучения. В статье подробно исследуются их архитектурные особенности, точность работы, скорость обработки и применимость в реальных задачах. Проведённые эксперименты позволяют выявить сильные и слабые стороны каждого подхода и дают рекомендации по выбору наиболее оптимального решения для создания систем отслеживания движения в зависимости от требований проекта.

Ключевые слова
Алгоритмы, отслеживание движений, оценка точности, компьютерное зрение, глубокое обучение

Введение

За период с 1993 по 2024 год наблюдается рост интереса к алгоритмам отслеживания движений. Косвенным методом оценки того, что наблюдается резкий всплеск к проблематике распознавания движения есть рост количества статей на эту тему, исходя из данных электронного архива с открытым доступом ArXiv.org. В 2024 году был достигнут пик в 3967 статей, что на 9,88% больше, чем в 2023 году. Графическое представление статистики показано на рисунке 1.

Технологии отслеживания движений находит применение в таких основных сферах, как: робототехника, кино, игры, видеонаблюдение, биомеханике. Задача алгоритмов отслеживания движений заключается в распознавании позы человека в пространстве (*Pose detection*), локализуя ключевые точки тела (суставы), также называемые ориентирами – локти, плечи, колени и т.д., что в общем можно определить как кластеры данных [1-4, 21-27].

Реализация такой задачи производится по средствам 2 категорий оценивания позы человека:

1) Оценка позы человека в двумерном пространстве. Эта технология основана на обработке двумерных изображений или видеоматериалов. Считываются 2 измерения и определяется поза человека, относительно координат x и y. Такой метод является наиболее распространённым.

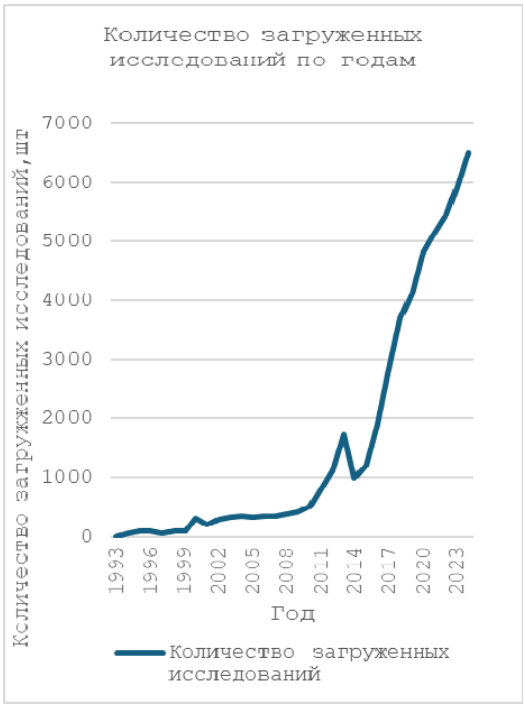

Рис. 1. Статистка загрузки исследований по годам

2) Оценка позы человека в трёхмерном пространстве. Данный метод основывается на определении позы человека, относительно трёхмерного пространства. Таким образом, формируется более точное представление о движениях человека. Не смотря на высокую точность, реализация данного метода является более сложной задачей, чем в двумерном пространстве. Однако, на текущий момент происходит развитие различных алгоритмов для упрощения решения данной задачи.

На сегодняшний день, методы оценки и отслеживания позы человека, для формирования трехмерной модели [5-7] опираются на несколько фундаментальных принципов.

Первым этапом, необходимо обнаружить человека на изображении. Этот этап основывается на использовании инструментов, например, готовых библиотек для определения человека. Дополнительно, существуют более простые способы распознавания объекта на кадре, например, детектирование краёв или же определение объекта с помощью алгоритмов изменения цветов на изображении или видеокадре.

Второй этап – определение признаков человека. Данный этап основывается на определении характеристик человека. В этот момент выделяются такие характеристики как: края силуэта человека, ключевые точки (напр. суставы) или готовое трёхмерное изображение (модель) человека. На основании данных характеристик формируется карта признаков и уже с помощью неё, алгоритм определяет положение и ориентацию человека в пространстве. Стоит заметить, что данный этап основывается на методах моделирования человека или же с помощью статистических методов.

Результатом решения данной задачи является макет скелета человека с расставленными ключевыми точками. Для решения этой задачи применим 2 алгоритма: OpenPose и AlphaPose. Необходимо выяснить их архитектурные особенности, точность работы, скорость обработки и применимость в реальных задачах, а также условия применения данных алгоритмов.

Модель алгоритма OpenPose

OpenPose представляет собой библиотеку с открытым исходным кодом, которая предназначена для определения множества двумерных поз человека в режиме реального времени [8]. Схема работы алгоритма OpenPose и этапы обработки изображений показаны на рисунке 2.

1) Этап 1 *(t < Tp)* – обработка исходных признаков. Несколько свёрточных блоков (обозначены зелёными и жёлтыми блоками "С" и "БС" соответственно) извлекают пространственные признаки из входного изображения. Затем, после применения нескольких свёрточных слоёв, результат проходит

через блок, который формирует промежуточное представление, обозначенное L^t, и подаётся на функцию потерь, которая используется для оптимизации на этом этапе.

2) Этап 2 *(Tp < t ≤ Tp + Tc)* – обработка результатов первого этапа и прохождение их через дополнительную серию свёрточных блоков. Итоговая функция потерь *f* направлена на обучение этой части модели, чтобы она выдавала результат S^t с необходимыми пространственными разрешениями h′×w′.

Первоначально, из изображения извлекаются карты признаков с помощью сети *Very Deep Convolutional Network*, которая состоит из 10 слоёв. Затем полученные карты признаков обрабатываются на многоэтапном конвейере *Convolutional Neural Network*. В результате такой обработки создаётся карты достоверности (*Confidence Maps*) и поля сходства частей (*Part Affinity Fields*). Для того, чтобы описать карту достоверности используется формула 1.

$$S = (S_1, S_2, ..., S_j) \tag{1}$$

Ограничения карты достоверности показаны в формуле 2.

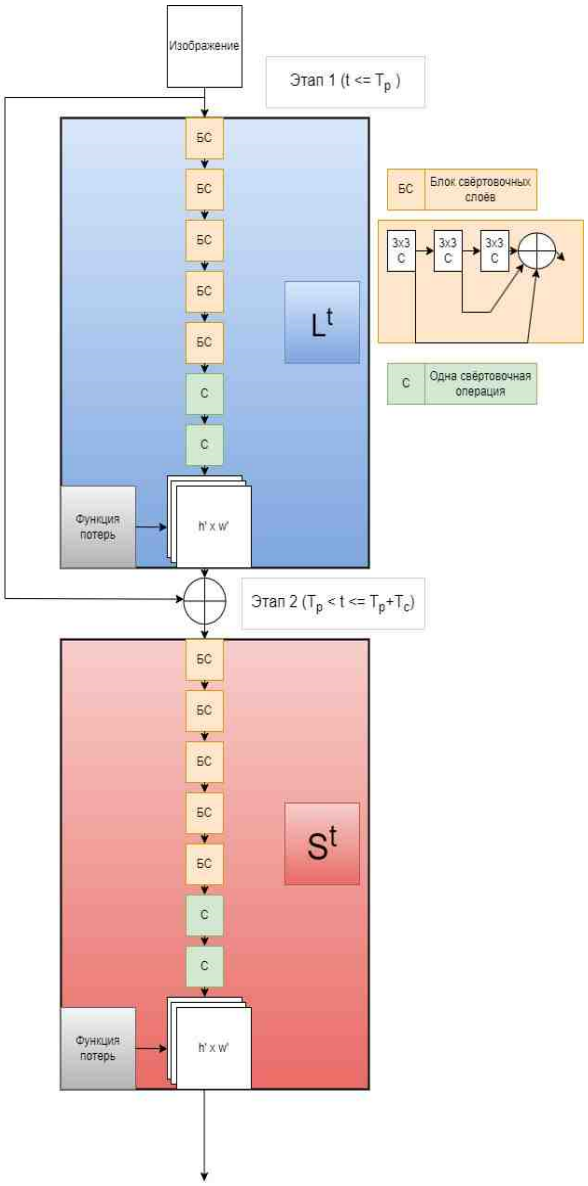

Рис. 2. Схема работы алгоритма *OpenPose*

$$S_j \in R^{w \cdot h}, j \in 1...J \quad (2)$$

где

S – это совокупность (конечное множество или вектор) карт тепловых карт или карт вероятностей, которые описывают некоторые пространственные характеристики в изображении,

S_j – отдельная тепловая карта или карта вероятностей для *j*-го элемента (например, для *j*-й ключевой точки или части тела). Она представляет собой матрицу размером $w \times h$,

R^{wh} – обозначает, что каждая карта S_j является матрицей вещественных чисел размером $w \times h$,

w – ширина карты,

h – высота карты,

J – количество карт S_j. Например, если каждая карта соответствует конкретной ключевой точке на изображении, то *J* будет равно количеству отслеживаемых ключевых точек.

Для того, чтобы описать поля сходств частей для начала необходимо получить координаты пикселя на изображении, которые отвечают за ключевые точки (p_a, p_b) – *x, y*.

Далее, необходимо построить вектор, указывающий направление от ключевых точек для каждой позиции пикселя в определённой области. Данное действие показано в формуле 3

$$f(a,b)(x,y) = \begin{bmatrix} f_x \\ f_y \end{bmatrix} \quad (3)$$

Если точки p_a и p_b находятся на расстоянии $d_{ab} = \|p_a - p_b\|$, то единичный вектор направления от p_a к p_b определяется как показано в формуле 4.

$$V(a,b) = \frac{p_b - p_a}{d_{ab}} \quad (4)$$

Следующий шаг – определение значений *PAF* в окрестности линии между ключевыми точками. Для каждой пары ключевых точек (a, b), *PAF* задаётся следующим образом:

1) В области между p_a и p_b каждый пиксель получает векторное значение $f(a,b)(x,y) = V(a,b)$, которое указывает направление от p_a к p_b.

2) Если существуют такие значения, которые не попадают в полосу $f(a,b)(x,y)$, то их значения приравниваются к 0

Как итог, *PAF* для одной пары ключевых точек описывает направленное поле, которое заполняет область между точками и помогает связать их в единую цепочку.

Таким образом, пусть *J* – количество всех пар ключевых точек, тогда *PAF* для всего изображения можно записать как набор векторных полей, где каждое *f*(*a,b*) соответствует одной связи между ключевыми точками. Таким образом, *PAF* представляет собой семейство функций, которые индексируемые множество *J*. Соответственно, для построения формулы мы будем использовать формат как при обсуждении поведения функций при непрерывных или дискретных значениях параметров. Формула (5) демонстрирует общую формулу для описания всех *PAF*.

$$F = \left\{ f_{(a,b)} \right\}, (a,b) \in J \quad (5)$$

После получения карт достоверности (*Confidence Maps*) и поля сходства деталей (*Part Affinity Fields*) применяется. Венгерский алгоритм (Двудольное соответствие в теории графов – максимальное количество совпадений рёбер среди всех совпадений графа), чтобы найти связь частей и соединить суставы одного и того же человека. Из-за векторной природы самого *PAF* сгенерированные совпадения объединяют общий скелет человека.

На основе вышеизложенной информации посчитаем алгоритмическую сложность алгоритма OpenPose. Как говорилось ранее, основной этап работы алгоритма заключается в детекции ключевых точек тела на изображении, что требует выполнения некоторых преобразований на каждом уровне сети. Таким образом получаем, что данные операции имеют следующую сложность, предоставленную в формуле 6:

$$\theta(n \cdot k^2 \cdot c \cdot m) \quad (6)$$

где:

n – количество пикселей на изображении,

k – размер фильтра,

c – число каналов изображения

m – число фильтров.

Стоит заметить, что в формуле, описанной выше, не учитываются дальнейшие этапы обработки, например, расчёт PAF's. Таким образом, принимая во внимание последующие расчёты PAF's и использование методов оптимизации, сложность которых может варьироваться от $\theta(p^2)$ до $\theta(p^3)$, где *p* – количество ключевых точек, общая формула принимает вид как в формуле 7.

$$\theta(T) = \theta(n \cdot k^2 \cdot c \cdot m) + \theta(r \cdot p^2) + \theta(d \cdot s) \quad (7)$$

где:

p – количество предполагаемых ключевых точек на изображении,

r – количество итераций построения связей между ключевыми точками с использованием *Part Affinity Fields (PAF),*

d – число масштабов (разрешений), на которых производится обработка,

s – стоимость дополнительной постобработки, включая интерполяцию, сглаживание и формирование финальной карты ключевых точек.

Воспользуемся правилами Big O нотации, в следствии чего преобразиться формула 7. Результат преображения показан в формуле 8.

$$T(n, p) = \theta(n + p^2) \quad (8)$$

Таким образом, общая сложность OpenPose носит смешанный характер — она линейная по отношению к размеру изображения и квадратичная по отношению к числу ключевых точек.

Как итог, получается модель, которая может определять ключевые точки на человеке в реальном времени. Стоит заметить, что алгоритм определяет эти точки как на 1 человеке, так и на нескольких. Результат работы модели показан на рисунке 3.

Рис. 3. Результат работы алгоритма OpenPose

В результате была получена скелетная модель человека. Стоит обратить внимание на то, что OpenPose смог определить несколько людей в кадре. Из результирующего изображения следует, что при определении ключевых точек на человеке алгоритм выбирает случайный цвет для соединения их в скелет. Алгоритм точно смог определить черты лица и плечи позирующих людей на кадре. В то же время, точность алгоритма заметно снизилась на кистях человека, демонстрируя погрешность в вычислениях позиции руки человека.

Модель алгоритма AlphaPose

AlphaPose – это алгоритм отслеживания движений и её оценки. Он основан на глубоком обучении, в следствии чего, алгоритм хорошо справляются с обнаружением и анализом ключевых точек человеческого тела в режиме реального времени. Этот алгоритм работает со множеством людей в кадре. Схема работы алгоритма показано на рисунке 4.

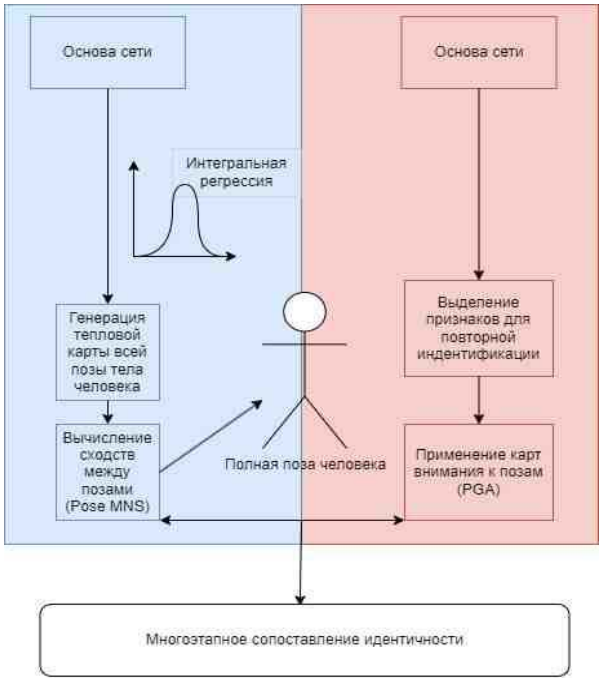

Рис. 4. Общая схема архитектуры алгоритма AlphaPose и результат работы

AlphaPose работает по принципу “сверху-вниз”, при котором ключевые точки человеческого тела на изображении или видеокадре ограничиваются с помощью рамок вокруг человека. Данные рамки формируются за счёт использования алгоритмов обнаружения объектов, например *Faster R-CNN*. Это необходимо, чтобы изначально сфокусироваться на тех частях изображения, которые точно содержат человека, и уменьшить количество ложных срабатываний. Таким образом, пусть изображение обозначается как I, а детектор возвращает множество рамок $B = \{b_1, b_2,\ldots, b_n,\}$, где каждая рамка представляет область, потенциально содержащую человека. Задача заключается в нахождении всех рамок b_i на изображении I с максимальной точностью и минимальном количеством пропущенных объектов.

После того как рамки были сформированы, в каждой из них применяется алгоритм, в следствии которого, определяются такие точки как: плечи, локти, колени и т.д. Для выполнения такого рода расчётов используется алгоритм – *Single-Person Pose Estimation Network (SPPE)* [10-11]. Сама сеть предсказывает координаты ключевых точек тела человека. На вход подаётся изображение, $I \in R^{w \times h \times 3}$, где w – ширина изображения, высота h и тремя цветовыми каналами *RGB*. Дополнительно, передаётся θ – веса для обучения сети *SPPE*. На данном этапе, модель проходит обучение через свёрточные слои, каждый из которых обучает распознавать характерные черты такие как: края, текстуры, формы.

Следующий шаг – генерация тепловых карт. Пусть $H_j(x,y)$ – тепловая карта для j-й точки, где (x,y) – координаты внутри изображения. J – общее количество ключевых точек. Тогда тепловая карта H для всех ключевых точек представляет собой тензор размерностью $w \times h \times J$, где $H_j(x,y)$ определяет вероятность присутствия ключевой точки j в позиции (x,y).

Таким образом, чтобы описать тепловую карту, необходимо воспользоваться формулой 9.

$$H_j^{true} = \exp\left(-\frac{(x - x_j)^2 + (y - y_j)^2}{2\sigma^2}\right), \tag{9}$$

где σ – параметр, контролирующий разброс вероятностного распределения, что позволяет задавать "неопределенность" положения точки.

После того как модель построила тепловую карту для локализации ключевых точек, то следующим шагом является – уточнения позы человека и идентификация. На основе полученной тепловой карты система *AlphaPose* применяет метод интегральной регрессии ключевых точек *(Symmetric Integral Keypoint Regression, SIKR)* для точного определения положения ключевых точек, используя предсказанные вероятности с тепловой карты.

Для расчёта *SIKR* для каждой точки *AlphaPose* производит вычисления в несколько этапов:

1) Вероятностное распределение. Используя тепловую карту, производится нормализация с помощью функцию сигмоиды для получения доверительной карты. Соответственно данный этап описан в формуле 10.

$$H'(x,y) = \frac{1}{1+e^{-H(x,y)}} \tag{10}$$

2) Интегральная регрессия**:** Вычисляются координаты каждой ключевой точки (x,y) с использованием *soft-argmax*, применяемого к нормализованному распределению вероятностей H′. Интегральная регрессия вычисляется по формуле 11 и 12.

$$x = \sum_i \sum_j j \cdot H'(i,j) \tag{11}$$

$$y = \sum_i \sum_j j \cdot H'(i,j) \tag{12}$$

Здесь каждое значение на карте взвешивается по его вероятности, что позволяет получить непрерывные координаты ключевой точки

3) Глобальная нормализация. На финальной стадии применяется нормализация вероятностей в пределах каждого ключевого региона, чтобы гарантировать, что координаты ключевых точек попадают в допустимые границы изображения.

Как итог, *SIKR* позволяет быстро и точно определить ключевые точки в пределах рассматриваемого изображения.

В ходе обучения, могут возникнуть проблемы с повторением поз, которые могут возникать из-за низких порогов при распознавании в задачах мультиперсонного позного отслеживания. Для каждого обнаруженного тела вычисляется мера сходства, учитывающая как пространственные расстояния между ключевыми точками, так и их совпадения. Для этого служит функция *Pose Non-Maximum Suppression (Pose NMS)*. Формула 13 служит для меры сходства между позами $S(P_1, P_2)$.

$$S(P_1P_2) = \frac{1}{N}\sum_{i=1}^{N} H_j^{true}(x,y) \tag{13}$$

После вычисления значений сходства для всех пар поз, используется пороговое значение T: если $S(P_1, P_2) > T$, поза с более низкой уверенностью (на основе среднего значения вероятностей ключевых точек) удаляется из списка детекций.

При решении предыдущей проблемы, исключили повторение поз. При этом модель должна уметь распознавать на разных изображениях или видеоряде одного и того же человека. Для этого требуется повторная идентификация человека(*re-ID*). Для этого из каждого обнаруженного человека извлекаются уникальные признаки в ограничительной рамке. Однако эти рамки включают в себя фоновые помехи или части других людей, что затрудняет повторную идентификацию.

Для каждого обнаруженного человека H внимание вычисляется следующим образом:

Построение карты ключевых точек показано в формуле 14.

$$H_{attention} = f(K_{heatmap}) \tag{14}$$

где $K_{heatmap}$ – тепловая карта ключевых точек; f – функция свертки, которая преобразует тепловую карту в карту внимания.

Далее применяются карты внимания к характеристикам идентификации, как показано в формуле (15).

$$F_{PGA} = H_{attention} \cdot F_{reID} \tag{15}$$

где F_{reID} – карта характеристик идентификации; F_{PGA} – итоговая взвешенная характеристика идентификации, которая акцентирует значимость человека и минимизирует влияние фона.

Под конец, *AlphaPose* применяет многоэтапное сопоставление идентичностей *(Multi-Stage Identity Matching, MSIM)*. Этот комплексный подход позволяет точно идентифицировать и отслеживать несколько человек, особенно в сложных или плотных сценах, что делает его востребованным для задач реального времени, таких как отслеживание действий и анализа поведения.

На основе приведённой архитектуры, посчитаем алгоритмическую сложность AlphaPose. Общую формулу необходимо описать в несколько этапов, продемонстрированных в формулах (16)-(19):

1) Обработка изображения через сверточную нейронную сеть (*CNN*):

$$\theta_{CNN} = \theta(n \cdot k^2 \cdot c \cdot m) \tag{16}$$

где n – количество пикселей в изображении; k – размер фильтра; c – число каналов (например, 3 для RGB); m – количество фильтров.

2) Детекция объектов (*bounding box generation*):

$$\theta_{bbg} = \theta(b \cdot h \cdot w) \tag{17}$$

где b – число обнаруженных объектов; h и w – размер входного изображения.

3) Уточнение позы и согласование (pose refinement and association)

$$\theta_{pra} = \theta(b \cdot p \cdot r) \tag{18}$$

где b – число объектов; p – количество ключевых точек; r – число итераций уточнения.

4) Сглаживание поз (temporal smoothing):

$$\theta_{ts} = \theta(b \cdot f \cdot p) \tag{19}$$

где f – число кадров в последовательности; b – число объектов; p – количество ключевых точек.

Таким образом, общая формула будет принимать вид, продемонстрированный в формуле 20.

$$T(n, b, p, r, f) = \theta_{CNN} + \theta_{bbg} + \theta_{pra} + \theta_{ts} \tag{20}$$

Воспользуемся принципами *Big O* нотации, тогда общая формула преобразуется как показано в формуле 21.

$$T(n, p) = \theta(n) + \theta_{pra} + \theta_{ts} \tag{21}$$

Если на вход подаётся большое изображение, то сложность можно считать линейной, в случае если во входном изображении много объектов и ключевых точек, то алгоритм усложняется дополнительной линейной зависимостью по числу объектов и ключевых точек.

Рисунок 5 демонстрирует полный результат работы алгоритма.

Рис. 5. Результат работы алгоритма

На вход подаётся изображение пары людей. Исходя из архитектуры AlphaPose, для входных данных есть три важных этапа. Первый – определение рамок человека. Исходя из результата, с учётом того, что рамки пересекаются, алгоритм правильно их расставил. Следующий этап – определение позы человека. Данный шаг сопоставим с результатом работы алгоритма OpenPose, однако точность на кистях оказалась выше. Заметим, что AlphaPose вычислил идентификационный номер каждого определённого человека, который поможет в дальнейшем отслеживании движений.

Анализ результатов работы алгоритмов

Произведя анализ алгоритмов отслеживания движений на базе глубокого обучения, выяснили, что алгоритмы используют различные подходы к архитектуре и обработке данных [12-14]. Таким образом, данные отличия будут существенно влиять на результат. Для того, чтобы объективно провести исследование необходимо запускать тестирование на одной и той же конфигурации. Конфигурация стенда следующая:

1) Процессор – AMD Ryzen 9 9950X,
2) Графический процессор – NVIDIA RTX 4090,
3) Оперативная память – 64 Гб,
4) Операционная система - Ubuntu 20.04 LTS с поддержкой CUDA и драйверов NVIDIA.

Тестировались алгоритмы с использованием наборов данных, включающие в себя конечное множество объектов в том числе и позы человека. Сложность поз изменяется от простой до поз, используемых в йоге. В рамках тестирования воспользовались наборами данных *COCO* и *MPII*.

Common Objects in Context (COCO) – это набор данных, использующийся для задач компьютерного зрения. Относительно задачи отслеживания движений *COCO* предоставляет различные позы человека, которые могут отличатся по своей сложности определения. Дополнительно, предоставляются изображения для множественного определения поз [15].

Max Planck Institute for Informatics Human Pose Dataset (MPII) – это набор данных, созданный для решения задач анализа человеческой позы. В отличие от предыдущего набора данных, *MPII* включает в себя только объекты отображающие различные позы человека [16]. Стоит отметить, что *MPII* является стандартом для оценки качества алгоритмов.

Основные метрики, используемые для оценки точности и производительности алгоритмов, включают:

PCK (Percentage of Correct Keypoints). Измеряет долю правильно определённых ключевых точек, где ключевая точка считается корректной, если расстояние до истинного положения меньше определённого порога, обычно зависящего от размеров тела на изображении. Расчёт PCK метрики показано в формуле (22).

$$\mathrm{PCK} = \frac{\mathrm{N}_{\mathrm{keypoints}}^{\mathrm{true}}}{\mathrm{N}_{\mathrm{keypoints}}} \cdot 100\% \tag{22}$$

где $\mathrm{N}_{\mathrm{keypoints}}^{\mathrm{true}}$ – количество правильных определённых точек; $\mathrm{N}_{\mathrm{keypoints}}$ – общее количество ключевых точек.

AP (Average Precision) и *AR (Average Recall)*. Эти метрики используются в основном на датасете *COCO*. Они оценивают точность и полноту детекции ключевых точек при различных уровнях порога *OKS (Object Keypoint Similarity)*, который учитывает расстояние между предсказанной и истинной позой с учётом масштаба и возможных ошибок аннотаций. Формула (23) демонстрирует расчёт метрики AP.

$$\mathrm{AP} = \int_0^1 \mathrm{Precision}(\mathrm{R})\,\mathrm{dR} \tag{23}$$

где *R* – полнота (*Recall*); *Precision* – точность.

На формулах 24 и 25 показаны расчёты для оценки полноты и точности соответственно.

$$\mathrm{Precision} = \frac{\mathrm{TP}}{\mathrm{TP} + \mathrm{FP}'} \tag{24}$$

$$\mathrm{Recall} = \frac{\mathrm{TP}}{\mathrm{TP} + \mathrm{FN}'} \tag{25}$$

Перед началом тестирования, необходимо указать параметры запуска моделей.

Для OpenPose входное разрешение изображение применялось 658x368 пикселей. Дополнительно использовались модели *BODY_25* и *MPI*.

Для AlphaPose использовался детектор объектов *YOLOv3* для быстрой обработки объектов и *Faster R-CNN* для более точного определения объектов. Размер батча равен 8. Разрешение изображения – 658x368 пикселей.

Провели первый эксперимент на статических изображениях в рамках наборов данных *COCO* и *MPII*.

Таблица 1

Результаты эксперимента с статическими изображениями

Алгоритм	Набор данных	mAP (Mean Average Precision)	PCK (Percentage of Correct Keypoints)
OpenPose	COCO	~70-79%	-
	MPII	-	~88-92%
AlphaPose	COCO	~80-88%	-
	MPII	-	~90-92%

1) Результаты на *COCO*:

OpenPose показывает высокие результаты на *COCO*, особенно при оценке ключевых точек, таких как плечи и локти, достигая точности более 70% *AP* для этих областей. Показатели *OpenPose* на этом наборе данных стабильно высоки благодаря тому, что набор сбалансирован таким образом, что количество изображений, в которых присутствует необходимость множественного определения позы человека меньше, чем изображений с 1 человеком.

AlphaPose превосходит *OpenPose* по метрике AP на плотных сценах, особенно в условиях перекрытия, так как подход "сверху вниз" помогает минимизировать ошибки ассоциации ключевых точек. Средний показатель точности *AlphaPose* на *COCO* достигает около 84% AP для всего тела, при этом точность на ключевых суставах (локтях, коленях) превышает 90% в отдельных тестах.

2) Результаты на *MPII*:

OpenPose и *AlphaPose* показывают близкие результаты по метрике *PCK* на *MPII*, так как этот набор данных лучше подходит для одиночной детекции. Оба алгоритма достигают более 90% точности на ключевых суставах, таких как запястья и лодыжки. Однако *AlphaPose* часто превосходит *OpenPose* на несколько процентов при детекции мелких деталей, что связано с подходом к разделению людей в кадре.

Дополнительно отметим следующие параметры, как скорость. *OpenPose* требует меньше вычислительных ресурсов, но при этом имеет меньшую точность по сравнению *AlphaPose*.

Ещё одним видом тестирования являлась трансляция изображения в реальном времени, при котором на вход алгоритмам подаётся видео в 1280x720p, 30 кадров в секунду, с тремя RGB каналами. Результаты эксперимента отражены в таблице 2.

Таблица 2

Результаты эксперимента с динамическими изображениями

Алгоритм	Средний FPS (average frames per second)	AP (Average Precision)
OpenPose	~20	~60-75%
AlphaPose	~16	~73-88%

В одинаковых условиях, OpenPose показывал результат в среднем 67% AP с частотой кадров равной 20. AlphaPose демонстрировал результат в 80% AP с частотой кадров в среднем равный 16.

На изменение производительности и результатов в эксперименте в реальном времени влияют такие факторы как: количество людей и битрейт трансляции.

Как итог, отметим следующие условия применения алгоритмов *AlphaPose* и *OpenPose*, продемонстрированных в таблице 3.

Таблица 3

Условия применения алгоритмов отслеживания движений

Алгоритм	Условия применения
AlphaPose	Спортивный анализ и биомеханика
	Постановка движений для анимации и кинопроизводства
	Медицинские и реабилитационные системы мониторинга
	Распознавание сложных жестов для управления устройствами
OpenPose	Мониторинг толпы и общественная безопасность
	Интерактивные инсталляции и арт-проекты

Условия применения алгоритмов были выбраны методом анализа иерархий. Так, например, для спортивного анализа и биомеханики важнее точность, чем производительность. В то же время, для мониторинга общественной безопасности важен баланс между точностью отслеживания движений, производительностью и надежностью [17-20].

Заключение

Исходя из того, что была поставленная цель – оценить возможности использования работы алгоритмов для распознавания поз человека и последующее отслеживание движение, то в работе для этого было выбрано два алгоритма OpenPose и AlphaPose.

Была рассмотрена архитектура алгоритмов и их математическая модель, исходя из которых был поставлен эксперимент для оценки работ алгоритмов по метрикам PCK, AP, FPS. В рамках сравнения, оба алгоритма продемонстрировали свою актуальность и находят применение в таких сферах как: робототехника, кино, игры, видеонаблюдение, биомеханике.

Проведённое исследование подтвердило, что более сложная архитектура *AlphaPose* обеспечивает высокую точность результатов, хотя и за счёт существенного снижения производительности, ограничивая среднюю частоту обработки динамических изображений до 10-15 кадров в секунду. В следствии чего было проведено сравнение алгоритмических сложностей, в ходе, который выяснили, что лучшая сложность для двух алгоритмов – линейная $\theta(n)$. Средняя сложность для алгоритма OpenPose - $O(p^2)$, а для AlphaPose - $O(n+b\cdot p\cdot r)$. В худшем случае, для алгоритма OpenPose сложность становится - $O(n+p^2)$, а для AlphaPose - $O(f\cdot b\cdot p\cdot r)$.

Исходя из сценариев применения алгоритмов, AlphaPose желательно использовать в сфере деятельности, связанной со спортом, анимацией и кинопроизводства за счёт высокой точности. В то же время, алгоритм OpenPose в большей степени подходит для компаний или служб, занимающихся мониторингом наблюдения на возможность выявления противоправных ситуаций, а также организацией интерактивных инсталляций и арт-проектов.

Литература

1. *Тремасова Л.А., Первухина А.А., Гадасин Д.В.* Использование методов косарайю и k-средних для формирования кластеров // Электросвязь. 2024. № 9. С. 47-55.

2. *Гадасин Д.В., Золотарева П.Ю., Тремасова Л.А*. Влияние кластеризации при обработке сырых данных // Системы синхронизации, формирования и обработки сигналов. 2024. Т. 15. № 3. С. 10-19.

3. *Гадасин Д.В*. Построение бинарного дерева минимальной цены // T-Comm: Телекоммуникации и транспорт. 2024. Т. 18. № 11. С. 38-44.

4. *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. Т. 6. № 1. С. 245-250.

5. *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.

6. *Gadasin D.V., Shvedov A.V., Kuzin I.A*. Reconstruction of a three-dimensional scene from its projections in computer vision systems // 2021 Intelligent Technologies and Electronic Devices in Vehicle and Road Transport Complex, TIRVED 2021 – Conference Proceedings. 2021.

7. *Gadasin D.V., Shvedov A.V., Kuzin I.A.* A model for representing the color and depth metric characteristics of objects in an image // 2021 Systems of Signal Synchronization, Generating and Processing in Telecommunications, SYNCHROINFO 2021 - Conference Proceedings. 2021. С. 9488349.

8. *Zhe Cao, Gines Hidalgo, Tomas Simon, Shih-En Wei, Yaser Sheikh.* OpenPose: Realtime Multi-Person 2D Pose Estimation using Part Affinity Fields // IEEE transactions on pattern analysis and machine intelligence.

9. Hao-Shu Fang, Shuqin Xie, Yu-Wing Tai, Cewu Lu. RMPE: Regional Multi-Person Pose Estimation

10. *Hao-Shu Fang, Jiefeng Li, Hongyang Tang, Chao Xu, Haoyi Zhu, Yuliang Xiu, Yong-Lu Li, Cewu Lu*. AlphaPose: Whole-Body Regional Multi-Person Pose Estimation and Tracking in Real-Time // IEEE transactions on pattern analysis and machine intelligence.

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.

12. *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.

13. *Шульпина П.Д., Гадасин Д.В., Тремасова Л.А*. Взвешивание признаков как предварительная обработка исходных наборов данных // Системы синхронизации, формирования и обработки сигналов. 2024. Т. 15. № 3. С. 40- 47.

14. *Гадасин Д.В., Михайлов М.Р., Чернышов Д.В*. Определение алгоритма структурирования текстовых данных // REDS: Телекоммуникационные устройства и системы. 2024. Т. 14. № 1. С. 4-11.

15. *Mykhaylo Andriluka, Leonid Pishchulin, Peter Gehler, Bernt Schiele*. 2D Human Pose Estimation: New Benchmark and State of the Art Analysis.

16. *Tsung-Yi Lin, Michael Maire, Serge Belongie, Lubomir Bourdev, Ross Girshick, James Hays, Pietro Perona, Deva Ramanan, C. Lawrence Zitnick, Piotr Dollár*. Microsoft COCO: Common Objects in Context.

17. *Шведов А.В., Гадасин Д.В., Коровушкина В.М., Мелькова Е.К.* Интеллектуальное тестирование как способ повышения качества информационной системы // REDS: Телекоммуникационные устройства и системы. 2022. Т. 12. № 2. С. 43-52.

18. *Гадасин В.А., Гадасин Д.В.* Надежность крупномасштабных сетей связи с аддитивной структурой // Автоматика и телемеханика. 1997. № 1. С. 160.

19. *Гадасин В.А., Гадасин Д.В.* Надежность двухполюсных сетей с аддитивной структурой II. Финальная вероятность связи // Автоматика и телемеханика. 1999. № 10. С. 164-179.

20. *Яковенко Н.В., Гадасин Д.В., Коцич Л.* Повышение точности коэффициента влияния ошибок в информационных системах с применением метода обратного распространения ошибки // Системы синхронизации, формирования и обработки сигналов. 2024. Т. 15. № 4. С. 35-42.

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

22. *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

23. *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

24. *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

25. *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

26. *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

27. 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

АНАЛИЗ УГРОЗ И ТРЕБОВАНИЙ К АЛГОРИТМАМ НИЗКОРЕСУРСНОГО ШИФРОВАНИЯ ДЛЯ RFID-МЕТОК

Ткаченко Никита Андреевич
Московский технический университет связи и информатики, студент, Москва, Россия
ntkachenko@rscc.ru

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

Аннотация
В данной работе проведен теоретический обзор RFID-технологий с точки зрения угроз их информационной безопасности и ограниченности ресурсов, рассмотрены требования к алгоритмам низкоресурсной криптографии, применимых в подобных системах, а также описана архитектура разрабатываемой в рамках выпускной квалификационной работы одного из авторов RFID-системы.

Ключевые слова
RFID, RFID метка, Интернет вещей, IoT, информационная безопасность, криптография, низкоресурсная криптография, атака

Введение

Современные технологии активно интегрируются во все сферы жизни, и одной из значимых разработок является радиочастотная идентификация (RFID), под которой мы будем понимать беспроводную коммуникационную технологию, которая использует радиоволны для автоматической идентификации помеченных объектов или вещей [1]. Системы, основанные на данной технологии, позволяют автоматически собирать, передавать и обрабатывать данные, что делает их важной частью логистики, розничной торговли, здравоохранения, умных домов, транспортных систем и Интернета вещей (иначе – IoT). Преимущества RFID включают компактность, низкую стоимость, бесконтактность и обработку данных в реальном времени. Однако широкое применение технологии сопровождается вызовами, главным из которых является обеспечение информационной безопасности.

RFID-метки, которые представляют собой антенны, необходимые для приёма электромагнитных волн ридера (считывателя) и передачи ответного радиосигнала, передают данные, включая чувствительную информацию (идентификационные номера, медицинские записи и т.д.), что делает их уязвимыми для перехвата, подделки или несанкционированного доступа. Для защиты данных требуется шифрование, но традиционные алгоритмы криптографии часто не подходят из-за ограниченных ресурсов RFID-меток: низкой вычислительной мощности, минимальной памяти и ограниченного энергопотребления [2]. Это создает необходимость разработки и использования низкоресурсных алгоритмов шифрования [3, 4], адаптированных для работы в условиях минимальных аппаратных возможностей, при сохранении высокого уровня безопасности.

Целью данной работы является анализ существующих и формулирование требований к перспективным низкоресурсным алгоритмам шифрования для защиты данных RFID-меток в условиях ограниченных ресурсов. Для достижения цели были поставлены такие задачи как изучение существующих подходов к низкоресурсному шифрованию и их применимости в RFID-системах, а также выявление основных угроз информационной безопасности и формулирование требований к подобным алгоритмам;

Данная работа связана с актуальной задачей создания криптографических решений для устройств с минимальными ресурсами, что способствует развитию безопасных RFID-систем и их применению в условиях растущей цифровизации.

Основные угрозы для RFID-меток

RFID-метки широко используются для передачи данных, однако их безопасность остается критически важной проблемой. Среди ключевых угроз современные исследователи выделяют следующие [5]:

1. **Перехват данных.** Сущность этой угрозы заключается в том, что передача данных по радиоканалу может быть перехвачена злоумышленником, особенно если отсутствует информация передается в незашифрованном виде.
2. **Клонирование и подделка.** Сущность этой угрозы заключается в том, что недостаточно стойкие механизмы аутентификации позволяют злоумышленникам создавать копии меток, обходя системы защиты.
3. **Атаки на целостность данных.** Сущность этой угрозы заключается в том, что изменение передаваемой информации может нарушить, к примеру, процессы инвентаризации и учета.
4. **Атаки отказа в обслуживании (DoS).** Сущность этой угрозы заключается в том, что создание помех или перегрузка канала связи может блокировать работу RFID-систем.
5. **Атаки повторного воспроизведения (Replay).** Сущность этой угрозы заключается в том, что записанные сигналы могут быть воспроизведены еще не один раз злоумышленником для обмана системы.
6. **Отслеживание и нарушение конфиденциальности.** Сущность этой угрозы заключается в том, что RFID-метки могут использоваться для слежки за пользователями без их ведома.

Для предотвращения этих угроз требуются эффективные механизмы защиты, включая шифрование, аутентификацию и управление доступом. Однако их реализация осложняется аппаратными ограничениями RFID-меток.

Ограничения аппаратных ресурсов для RFID-меток

RFID-метки массового применения спроектированы с минимальными затратами [6], что накладывает следующие ограничения:

1. **Низкая вычислительная мощность.** Данное ограничение заключается в том, что процессоры меток могут выполнять только простейшие операции.
2. **Малый объем памяти.** Данное ограничение заключается в том, что память метки ограничена несколькими килобайтами, что затрудняет реализацию сложных криптографических алгоритмов.
3. **Ограниченное энергопотребление.** Данное ограничение заключается в том, что энергия для работы метки поступает от радиосигнала считывателя, что исключает использование ресурсоемких алгоритмов.
4. **Задержки при выполнении операций.** Данное ограничение заключается в том, что медленные вычисления ограничивают применение в реальных сценариях.
5. **Физическая уязвимость.** Данное ограничение заключается в том, что простая конструкция меток делает их подверженными физическим атакам.
6. **Стоимость.** Данное ограничение заключается в том, что метки должны быть дешевыми, что ограничивает возможности их модернизации.

Противоречия между информационной безопасности и ограничений ресурсов RFID-меток

Основная проблема при обеспечении информационной безопасности для RFID заключается в поиске баланса между необходимым уровнем защиты данных и ограничениями аппаратных ресурсов. Традиционные криптографические алгоритмы (например, AES, RSA либо отечественный алгоритм Кузнечик) слишком ресурсоемки, а упрощенные подходы часто не обеспечивают должной безопасности. Решением становятся такие специализированные алгоритмы шифрования, такие как низкоресурсные блочные и поточные шифры (PRESENT, Simon/Speck). Новые методы, включая физически неклонируемые функции (PUF) [7], также обещают повышение безопасности [8].

Таким образом, обеспечение надежной защиты RFID-меток требует комплексного подхода: разработки адаптированных алгоритмов, оптимизации энергопотребления и внедрения аппаратных методов защиты. Это позволит повысить устойчивость RFID-систем в условиях современных вызовов [9].

Отметим также такую потенциальную опасность для RFID-систем как квантовый вызов [10]. В связи с ограниченностью ресурсов использование квантовых методов защиты [11] в подобных системах не представляется возможным, да и использование постквантовых методов [12] может быть только ограниченным.

Анализ возможных действий злоумышленника

RFID-метки широко применяются для идентификации объектов и сбора данных в различных сферах, что делает их привлекательной целью для злоумышленников. Несмотря на компактность и простоту конструкции, уязвимости в их системе безопасности создают значительные риски [13]. В данном разделе рассмотрены основные виды атак, которым подвержены RFID-метки, их механизм, последствия и возможные способы противодействия.

Одной из наиболее распространённых угроз или атак является **перехват данных**. Передача данных между RFID-меткой и считывателем осуществляется через радиоканал, который уязвим для прослушивания с помощью недорогого оборудования. Если данные передаются в открытом виде, злоумышленник может:

1. получить доступ к идентификаторам меток;
2. узнать конфиденциальные сведения, такие как информация о товаре или пользователе.

Последствия данной атаки:

- Нарушение конфиденциальности.
- Использование перехваченных данных для дальнейших атак, таких как клонирование метки.

К методам защиты от подобной атаки относятся:

- Применение криптографических протоколов для шифрования передаваемых данных [14].
- Использование динамических идентификаторов, которые изменяются при каждом обмене.

Клонирование и подделка меток происходит, когда злоумышленник копирует содержимое RFID-метки и создает её точный дубликат. Это возможно, если:

1. Метка не имеет встроенной защиты или аутентификации.
2. Используется открытый протокол передачи данных.

Последствия данной атаки:

- Несанкционированный доступ к системам (например, обход турникетов или взлом системы контроля доступа).
- Мошенничество в логистических системах (подмена товаров).

К методам защиты от подобной атаки относятся:

- Реализация механизмов аутентификации меток и считывателей [15].
- Использование уникальных аппаратных идентификаторов (например, физически неклонируемых функций, PUF).

Злоумышленник может модифицировать данные, передаваемые между меткой и считывателем, или встраивать ложную информацию в поток. Такие атаки, именуемые **атаками на целостность данных**, нарушают работу системы и могут привести к:

- Ошибкам в инвентаризации.
- Неправильной идентификации объектов.

Последствия:

- Нарушение логистических процессов.
- Финансовые потери.

К методам защиты от подобной атаки относятся:

- Использование криптографических подписей для проверки целостности данных.
- Внедрение протоколов взаимной аутентификации.

Атаки отказа в обслуживании (DoS) направлены на блокировку взаимодействия между RFID-меткой и считывателем. Злоумышленник может:

- Создавать радиопомехи.
- Перегружать канал связи.

Последствия данной атаки:

- Нарушение работы системы в критически важных приложениях (транспорт, здравоохранение).
- Снижение доверия к технологии.

К методам защиты от подобной атаки относятся [16]:

- Использование защищённых каналов связи.
- Внедрение алгоритмов обнаружения и предотвращения атак DoS.

В ходе **атаки повторного воспроизведения (Replay)** злоумышленник записывает данные, передаваемые между меткой и считывателем, и воспроизводит их для обмана системы. Такие атаки позволяют:

- Получить несанкционированный доступ.
- Внедрить поддельные данные в систему.

Последствия данной атаки:

- Компрометация системы доступа.
- Нарушение работы систем учёта.

К методам защиты от подобной атаки относятся:

- Использование временных меток и одноразовых сессий.
- Применение протоколов взаимной аутентификации с использованием динамических ключей.

RFID-метки могут использоваться для отслеживания передвижений пользователей, что нарушает их право на конфиденциальность. Это становится возможным, если метки передают статический идентификатор, доступный для считывания любым устройством. Подобные атаки именуются **отслеживание и нарушение конфиденциальности.**

Последствия данной атаки:

- Нарушение личной жизни пользователей.
- Неэтичное использование данных со стороны организаций.

К методам защиты от подобной атаки относятся:

- Шифрование идентификаторов.
- Применение протоколов, обеспечивающих анонимность (например, протоколы псевдонимных идентификаторов).

Физическая уязвимость RFID-меток делает их подверженными непосредственным воздействиям злоумышленников, которые называются **физическимм воздействие и атаками на оборудование**. Метки могут быть:

1. Повреждены или уничтожены.
2. Модифицированы для изменения функционала или кражи данных.

Последствия данной атаки:

- Нарушение работы систем, зависящих от RFID-меток.
- Потеря данных и необходимость замены меток.

К методам защиты от подобной атаки относятся:

- Использование защищённых корпусов и устойчивых материалов.
- Внедрение механизмов обнаружения физического вмешательства.

Злоумышленники часто используют комбинацию методов (комбинированные атаки) для усиления эффекта атаки. Например:

1. Сочетание перехвата данных и Replay-атаки.
2. Одновременное создание радиопомех и клонирование меток.

Последствия данной атаки:

- Увеличение сложности обнаружения и противодействия атакам.
- Более серьёзные последствия для системы.

К методам защиты от подобной атаки относятся:

- Комплексный подход к безопасности, включающий защиту данных, оборудования и каналов связи.
- Постоянный мониторинг активности в системе для выявления подозрительных действий.

Атаки на RFID-метки представляют серьёзные угрозы для их использования в системах, где требуется высокая безопасность. Каждая из описанных атак имеет свои особенности, последствия и требует применения соответствующих методов защиты. Разработка и внедрение адаптированных низкоресурсных алгоритмов шифрования, а также протоколов аутентификации и управления доступом, являются ключевыми направлениями для повышения устойчивости RFID-систем. Кроме того, важно учитывать физическую защиту меток и комплексный подход к обеспечению безопасности, чтобы минимизировать риски и расширить области применения RFID-технологий в условиях современных вызовов.

Требования к алгоритмам шифрования для низкоресурсных устройств

RFID-метки являются устройствами с ограниченными вычислительными и энергетическими ресурсами, такими как сенсоры, микроконтроллеры, постоянная память. Безопасность данных играет важнейшую роль, что требует разработки и использования эффективных алгоритмов шифрования. В данном разделе рассмотрены ключевые требования, предъявляемые к алгоритмам шифрования для низкоресурсных устройств.

Одной из основных характеристик низкоресурсных устройств является ограниченный запас энергии, часто связанный с использованием батареек или других автономных источников питания. Алгоритмы шифрования должны быть оптимизированы для минимального энергопотребления как при выполнении криптографических операций, так и при обмене данными.

Снижение энергозатрат достигается за счет:

- Минимизации числа вычислительных операций (например, использование XOR вместо более сложных операций);
- Применения упрощённых арифметических операций, таких как сложение и сдвиги битов;
- Оптимизации структуры алгоритма, включая снижение частоты обращения к памяти.

Многие низкоресурсные устройства обладают ограниченными вычислительными возможностями, включая низкую тактовую частоту процессора и небольшой объём оперативной памяти. Алгоритмы шифрования должны учитывать:

- Минимальный объём памяти не должен превышать 2-4 КБ для хранения ключей и временных данных;
- Низкую временную сложность алгоритмов, к примеру линейную O(n) для большинства операций;
- Возможность реализации на процессорах с ограниченным набором инструкций, таких как ARM Cortex-M0, ALTERA и др.

Примерами алгоритмов, удовлетворяющих этим требованиям, являются такие стандарты, как AES (в лёгкой модификации), SPECK, SIMON. Из отечественных алгоритмов к подобным требованиям близок алгоритм блочного шифрования Магма. Например, SPECK требует значительно меньше ресурсов по сравнению с традиционным AES, сохраняя при этом приемлемый уровень безопасности. В условиях ограниченного объёма памяти устройства критически важна компактность реализуемого кода алгоритма. Это достигается за счёт:

- Оптимизации исходного кода, выраженной в исключение лишних функций и проверок;
- Использования библиотек с минимальным объёмом зависимостей, это библиотеки без использования динамической памяти;
- Внедрения методов сжатия инструкций и данных (например, использование макросов для упрощения операций).

Для примера, реализация SPECK на платформе AVR занимает менее 1 КБ памяти программы, что делает его идеальным выбором для микроконтроллеров.

Даже в условиях ограниченности ресурсов алгоритмы шифрования должны обеспечивать высокий уровень криптографической стойкости, в том числе истойчивость к криптографическим атакам включающую в себя:

- Защиту от атак на основе анализа энергопотребления (side-channel attacks) через внедрение случайных задержек и маскирования данных;
- Устойчивость к методам криптографического анализа, включая дифференциальный и интегральный [17] криптоанализ;
- Возможность адаптации к новым видам угроз, например, добавление дополнительных раундов при необходимости.

Низкоресурсные устройства часто работают в составе более крупных систем или сетей. Это требует:

- Совместимости с существующими стандартами и протоколами шифрования (например, TLS/DTLS);
- Возможности масштабирования алгоритма в зависимости от доступных ресурсов (например, выбор между 64- и 128-битной длиной блока);

- Обеспечения простоты интеграции в программное и аппаратное обеспечение устройства.

Примером может служить протокол DTLS, оптимизированный для устройств IoT, который использует упрощённые шифры, такие как ChaCha20.

Простота реализации является важным фактором для минимизации ошибок при разработке, особенно если алгоритм разрабатывается для устройств с уникальными архитектурными особенностями. Эффективный алгоритм должен быть:

- Легко переносимым между платформами, используя стандартные языки программирования, такие как C, C++, RUST;
- Доступным для реализации как на аппаратном, так и на программном уровне, например, в виде встроенных криптографических модулей. Для примера, многие микроконтроллеры уже имеют аппаратную поддержку AES, что упрощает его внедрение.

Таким образом, алгоритмы шифрования для низкоресурсных устройств должны соответствовать целому ряду требований, включая энергоэффективность, низкую вычислительную сложность, компактность кода, устойчивость к атакам, совместимость и простоту реализации. Эти характеристики позволяют обеспечить надёжную защиту данных, не выходя за рамки ограниченных ресурсов устройства. Разработка таких алгоритмов представляет собой сложную и актуальную задачу, особенно в условиях стремительного роста числа низкоресурсных устройств в различных отраслях.

Описание разрабатываемой RFID системы

В рамках выпускной квалификационной работы один из авторов статьи под руководством другого разрабатывает модель RFID системы. Система состоит из трех основных компонентов: сервера, RFID-метки и ридера.

Сервер является центральным компонентом системы и выполняет следующие функции:

- База данных для хранения информации об объектах, включая их уникальные идентификаторы (ID), статусы, а также секретные ключи для каждой RFID-метки.
- Хранение программного обеспечения для генерации криптографических ключей (открытого и секретного) и шифрования уникальных идентификаторов.
- Записывающее устройство, предназначенное для записи зашифрованного ID и секретного ключа в память RFID-метки. Взаимодействие происходит через NFC.

RFID-метка представляет собой компактное устройство со следующими характеристиками:

- Наличие контроллера STM, криптопроцессора и модуля NFC.
- Объем памяти не превышает 100 МБ.

Функциональность включает хранение зашифрованного ID и секретного ключа, а также обеспечение аутентификации при взаимодействии с ридером.

Ридер предназначен для считывания данных с RFID-меток и передачи информации на сервер. Основные характеристики:

- Включает в себя контроллер STM, криптопроцессор и NFC-модуль.
- Объем памяти также ограничен 100 МБ.

Функции ридера включают считывание зашифрованного ID и закрытого ключа с метки, выполнение аутентификации и отправку данных на сервер.

Процесс работы разрабатываемой системы заключается в том, что на этапе инициализации сервер генерирует уникальный ключ и зашифрованный ID для каждого объекта. Записывающее устройство передает эти данные на RFID-метку.

При идентификации объекта ридер считывает зашифрованный ID и ключ с метки, проводит аутентификацию и передает информацию на сервер.

Сервер обновляет статус объекта в базе данных (например, активация, изменение местоположения или состояния объекта).

Система обеспечивает надежную идентификацию объектов, безопасность данных и может быть адаптирована для использования в различных сферах.

Заключение

В ходе исследования были рассмотрены аспекты применения низкоресурсных алгоритмов шифрования для защиты RFID-меток. Основные угрозы, такие как перехват данных, клонирование меток и атаки на целостность информации, требуют реализации эффективных криптографических решений. Представленная система, включающая сервер, RFID-метки и ридер, в ходе проведенных экспериментов демонстрирует возможности обеспечения безопасной идентификации объектов при ограниченных ресурсах устройств.

Разработка и внедрение адаптированных алгоритмов, таких как низкоресурсные блочные и поточные шифры, позволяет обеспечить баланс между высокой степенью безопасности и ограниченными вычислительными и энергетическими возможностями RFID-меток. Имитационное моделирование и анализ эффективности предложенных решений подтверждают их применимость в реальных условиях.

Предложенная система открывает перспективы для дальнейших исследований в области криптографической защиты данных, а также для практического внедрения в сферы логистики, здравоохранения, IoT и смарт-городов. Реализация представленных подходов позволит повысить устойчивость RFID-систем к современным угрозам и расширить области их применения в условиях цифровизации.

В ходе дальнейшей работы предполагается разработать новую реализацию одного из существующих алгоритмов шифрования, учитывающий аппаратные ограничения RFID-меток, провести оценку производительности, энергопотребления и криптографической стойкости предложенной реализации и выполнить имитационное моделирование для проверки ее эффективности в реальных условиях.

Это расширит применение RFID-меток в безопасных системах передачи данных, включая логистику и IoT.

Предложенная реализация алгоритма может быть внедрена в реальные устройства, повышая их устойчивость к угрозам, таким как перехват, модификация данных и клонирование меток. Она может быть адаптирована для других сфер, включая транспортные карты и розничная торговля.

Отметим, что для подобных систем, как и для систем распределенного реестра, актуальна задача проведения тестирования, верификации и валидации [18], в рамках которых может понадобиться и сертификация [19], которая будет возможна только при использовании стандартизированных криптографических решений. Поскольку в нашей стране подобных низкоресурсных алгоритмов, за исключением Магмы на начало 2025 года нет, требуется проведение специалистами соответствующих глубоких математических исследований (к примеру, как в [20-23])

Литература

1. RFID-технологии. Справочное пособие / Под ред. Д. М. Кузнецова. М.: ДМК Пресс, 2007. 400 с. ISBN 978-5-94074-232-4.

2. *Бельский В.С., Грибоедова Е.С., Царегородцев К.Д., Чичаева А.А*. Безопасность RFID-систем // International Journal of Open Information Technologies. 2021. Т. 9, № 9. С. 1-20. EDN URSLEN

3. *Панков К.Н*. Основные блочные алгоритмы шифрования, предназначенные для обеспечения информационной безопасности в системе интернет-вещей // Технологии информационного общества : Материалы XIII Международной отраслевой научно-технической конференции, Москва, 20-21 марта 2019 г. Том 1. М.: Издательский дом Медиа Паблишер, 2019. С. 458-460. EDN HSNEGU

4. *Панков К.Н*. Основные криптографические алгоритмы для построения систем распределенного реестра в Интернете вещей // Технологии информационного общества : Сборник трудов XIV Международной отраслевой научно-технической конференции, Москва, 18-19 марта 2020 г. М.: Издательский дом Медиа Паблишер, 2020. С. 224-227. EDN VFDNIT

5. *Иманкул М.Н.* Приложения RFID-систем: текущие проблемы и тренды // Инновационное развитие науки и образования : монография. Пенза: "Наука и Просвещение" (ИП Гуляев Г.Ю.), 2019. С. 158-166. EDN YWFPSH

6. RFID-технологии: Справочное пособие / Под ред. И. В. Силова. СПб.: БХВ-Петербург, 2006. 512 с. ISBN 5-94157-789-2

7. *Бельский В.С., Чижов И.В., Чичаева А.А., Шишкин В.А*. Физически неклонируемые функции в криптографии // International Journal of Open Information Technologies. 2020. Т. 8, № 10. С. 10-26. EDN CRXSKM

8. *Федоров М.* Стандарты и тенденции развития RFID-технологий // Компоненты и технологии. 2006. № 1(54). С. 108-110. EDN MTFIPF

9. *Бобков А.С.* Исследование возможностей технологии RFID // Юный ученый. 2021. № S8-1(49-1). С. 1-2. EDN TZUQNO

10. Распоряжение Правительства РФ от 11 июля 2023 г. № 1856-р. Об утверждении Концепции регулирования отрасли квантовых коммуникаций в РФ до 2030 г. // ГАРАНТ.РУ: [сайт]. URL: https://www.garant.ru/products/ipo/prime/doc/407297268/ (дата обращения: 26.01.2025).

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

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

13. *Титов А.* RFID-метки: ультимативный гид по выбору. // Интемс: [сайт]. URL: https://securityrussia.com/blog/rfid-metki.html (дата обращения: 26.01.2025).

14. Криптографическая защита информации в объектах информатизации / Под ред. В. Н. Гостева. М.: Горячая линия – Телеком, 2010. 320 с. ISBN 978-5-9912-0065-9.

15. Современная прикладная криптография: Учебное пособие / Под ред. А. В. Иванова. М.: РУДН, 2008. 218 с. ISBN 978-5-209-03015-6.

16. RFID-технология: описание, применение, работа – 05.06.2023 // Sirius HUB: [сайт]. URL: https://sirius-hub.com/stati/rfid-tekhnologii-kto-kak-gde-i-zachem-ih-ispolzuet/ (дата обращения: 26.01.2025).

17. *Панков К.Н.* Некоторые условия применимости интегрального метода к четырём раундам AES-подобных алгоритмов // Прикладная дискретная математика. Приложение. 2022. № 15. С. 57-62. DOI 10.17223/2226308X/15/15. EDN ZZIIUS

18. *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

19. *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

20. *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

21. *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

22. *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

23. *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.

О НЕЙТРАЛИЗАЦИИ УГРОЗ ОБХОДА АУТЕНТИФИКАЦИИ ВЕБ-ПРИЛОЖЕНИЙ

Комраков Никита Антонович
МТУСИ, студент, Москва, Россия
nikitaakomrakov@yandex.ru

Большаков Александр Сергеевич
МТУСИ, доцент, к.т.н., Москва, Россия
alexbol57@mail.ru

Аннотация
В данной работе проведено исследование сценариев обхода аутентификации с целью выявления признаков нарушения информационной безопасности. В ходе исследования рассмотрены протоколы аутентификации и уделено внимание нейтрализации ключевых уязвимостей, включая SQL-инъекции, LDAP-инъекции и атаке методом перебора паролей. Предложен комплекс защитных мер от ряда уязвимостей, эксплуатируемых атаками согласно OWASP TOP-10, направленных на обход аутентификации. Особое внимание уделено созданию алгоритмов, нейтрализующих наиболее распространенные угрозы, что способствует повышению общей безопасности информационных систем.

Ключевые слова
Аутентификация, Уязвимости, OWASP Top-10, Сценарии атак, Кибербезопасность

Введение

В соответствии с приказами ФСТЭК (Федеральная служба по техническому и экспортному контролю) России [1, 2], касающимися идентификации и аутентификации субъектов доступа, актуальность защиты от атак на аутентификацию становится особенно важной. В условиях увеличения числа киберугроз и утечек данных, соблюдение норм безопасности и защита от потенциальных уязвимостей в системах аутентификации — это не только требование законодательства, но и необходимость для обеспечения конфиденциальности, целостности и доступности информации.

Аутентификация является ключевым элементом системы безопасности любой информационной системы. Однако ошибки в коде приложения могут привести к различным уязвимостям, которые злоумышленники могут использовать для обхода аутентификационных механизмов и получения несанкционированного доступа.

Результаты исследования

1. Формирование сценариев обхода аутентификации

В данной работе основное внимание уделено сценариям обхода аутентификации с использованием актуальных ошибок кода веб-приложений согласно списку литературы.

Определены конкретные техники и методики, которые могут быть использованы злоумышленниками для обхода аутентификации.

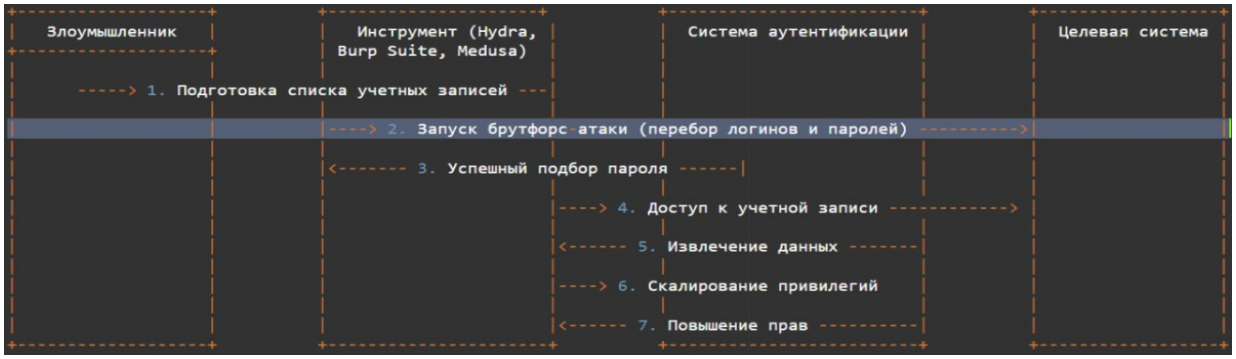

Рис. 1. Сценарий атаки 1

Приведены сценарии, которые описывают, как именно можно использовать уязвимости для получения несанкционированного доступа.

Сценарий 1 реализован на основе техники T1110.001 (рис. 1).

1) Сбор учетных данных. Злоумышленник использует утечки данных, открытые источники, социальные сети, для составления списка учетных записей.

2) Запуск брутфорс-атаки. С помощью ПО (например, Hydra, Burp Suite) злоумышленник автоматизирует подбор учетных данных, как указано в работе [12]. Наиболее распространенными целями для брутфорс-атаки являются такие протоколы, как SSH (Secure Shell, порт 22), FTP (File Transfer Protocol, порт 21), HTTP (HyperText Transfer Protocol, порт 80 или 443 для HTTPS).

3) Получение доступа. После успешного подбора учетных данных злоумышленник аутентифицируется и получает доступ к учетной записи.

4) Извлечение информации. Злоумышленник извлекает конфиденциальную информацию, включая личные и финансовые данные.

5) Эскалация привилегий. Злоумышленник получает административный доступ, что позволяет ему атаковать систему, внедрять вредоносный код или разрушать инфраструктуру.

Внедрение вредоносного кода после эскалации привилегий может происходить через RDP (Remote Desktop Protocol, 3389/TCP(Transmission Control Protocol)), WinRM (Windows Remote Management, 5985/TCP, 5986/TCP), SMB (Server Message Block, 445/TCP), SSH (22/TCP), HTTP/HTTPS (80/TCP, 443/TCP), DNS (Domain Name System, 53/UDP, 53/TCP) и LDAP (389/TCP, 636/TCP). Эти порты используются для загрузки вредоносных файлов, выполнения команд.

Вывод по сценарию использования техники **T1110.001**: Атака, основанная на сборе информации, брутфорсе и дальнейшей эскалации привилегий, показывает, как уязвимости в политике безопасности и недостаточные меры по защите могут привести к серьезным последствиям, включая утечку конфиденциальной информации и полный контроль над системой.

Для предотвращения утечки данных необходимо нейтрализовать атаку на 2 действии злоумышленника.

Сценарий 2 реализован на основе техники T1190 (рис. 2).

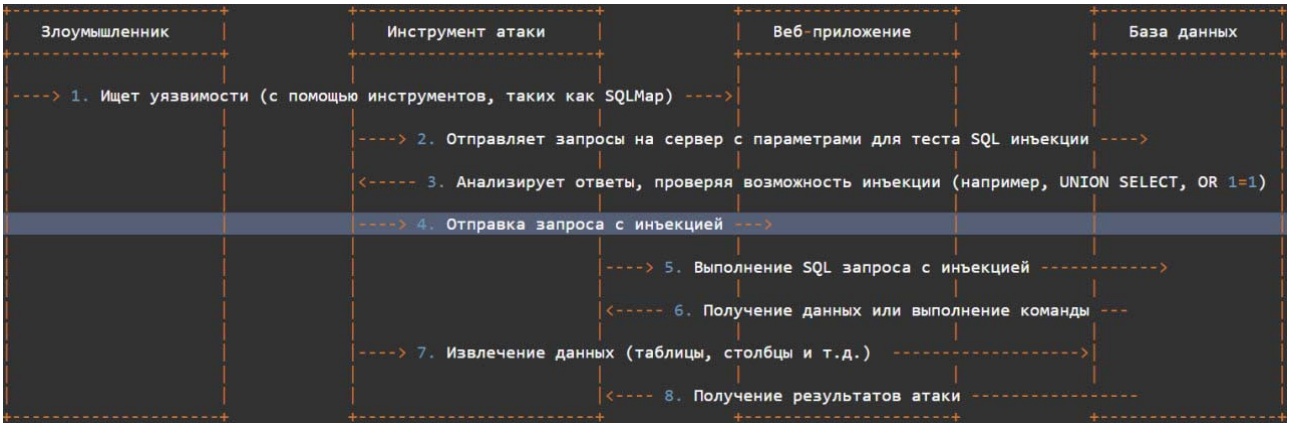

Рис. 2. Сценарий атаки 2

1) Сканирование портов веб-приложения. Злоумышленник использует инструменты (например, SQLMap, Burp Suite) для анализа веб-приложения на наличие уязвимостей SQL-инъекции (CWE-89).

2) Отправка тестовых запросов. Злоумышленник отправляет автоматизированные запросы с потенциально вредоносным кодом (например, ' OR 1=1 --, UNION SELECT NULL) для проверки фильтрации данных, как описано в исследовании [4].

3) Анализ ответов сервера. Анализируются ответы сервера на предмет ошибок базы данных, нестандартных реакций или изменений в контенте страницы.

4) Внедрение вредоносного SQL-запроса. После обнаружения уязвимости злоумышленник отправляет инъекцию с целью доступа к скрытым данным или изменения структуры базы данных.

5) Выполнение команды на сервере. База данных выполняет вредоносный SQL-запрос, что может привести к раскрытию, удалению или модификации данных.

6) Извлечение данных. Злоумышленник извлекает конфиденциальные данные, такие как учетные записи, финансовую информацию или другие чувствительные данные.

7) Получение результатов атаки. Извлеченные данные используются для несанкционированного доступа, шантажа, продажи или дальнейших атак.

Для предотвращения утечки данных необходимо нейтрализовать атаку на 4 действии злоумышленника.

Вывод по сценарию использования техники **T1190**: Атака на веб-приложение, включающая сканирование портов, анализ откликов сервера и внедрение вредоносного SQL-кода, демонстрирует, как отсутствие надёжных механизмов защиты может привести к компрометации данных и несанкционированному выполнению команд на сервере. Данный сценарий подчёркивает критическую важность регулярного мониторинга безопасности и своевременного устранения уязвимостей.

Сценарий 3 реализован на основе техники T1071.001 (рис. 3).

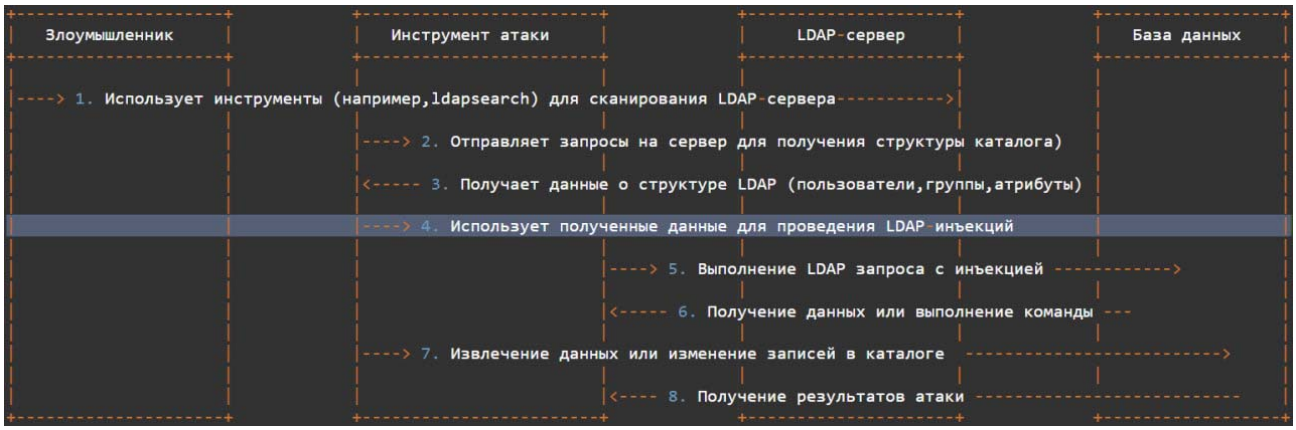

Рис. 3. Сценарий атаки 3

1) Использование инструментов для сканирования LDAP-сервера. Злоумышленник использует инструменты (ldapsearch, Nmap) для обнаружения LDAP-сервера и проверки его открытых портов.

2) Отправка запросов для получения структуры каталога. С помощью анонимных учетных данных злоумышленник отправляет запросы для получения информации о структуре каталога (пользователи, группы, атрибуты).

3) Получение данных о структуре LDAP. Злоумышленник извлекает информацию о пользователях, группах и объектах LDAP, что дает основу для дальнейших атак.

4) Использование данных для LDAP-инъекций или обхода аутентификации. Злоумышленник формирует вредоносные LDAP-запросы для инъекций (CWE-90) или обхода аутентификации.

5) Выполнение LDAP-запроса с инъекцией. LDAP-сервер выполняет вредоносный запрос из-за недостаточной защиты и валидации данных.

6) Получение данных или выполнение нежелательных операций. Злоумышленник может не только получить данные, но и создавать или удалять учетные записи, изменять пароли, повышать привилегии, вносить изменения в группы доступа, модифицировать атрибуты учетных записей и устанавливать бэкдоры, что приводит к компрометации системы и долгосрочному несанкционированному доступу.

7) Извлечение данных или изменение записей в каталоге. Злоумышленник извлекает или модифицирует данные (списки пользователей, хэши паролей) для последующих атак.

8) Получение результатов атаки. Злоумышленник анализирует извлеченные данные или проверяет изменения для дальнейших атак (например, эскалация привилегий).

Вывод по сценарию использования техники **T1071.001.**

Отсутствие защиты LDAP-запросов позволяет злоумышленникам обходить аутентификацию и получать доступ к конфиденциальным данным. Используя сканирование и анонимные учетные записи, они выявляют слабые места системы. Уязвимости, такие как отсутствие ограничений на аутентифи-

кацию (CWE-307), слабые пароли (CWE-521) и некорректная фильтрация ввода (CWE-89), повышают риск атак, ведущих к компрометации данных и изменению привилегий.

Для предотвращения утечки данных необходимо нейтрализовать атаку на 4 действии злоумышленника.

2. Разработка алгоритмов обнаружения техник

Согласно данным таблицы 1 для обнаружения техник обхода аутентификации, таких как:

T1110.001: Brute Force: Password Guessing

T1190: Exploit Public-Facing Application

T1071.001: Application Layer Protocol: Web Protocols

Каждая уязвимость имеет свой уникальный идентификатор в классификаторе Common Weakness Enumeration (CWE). Рассмотрим основные из них:

CWE-307: Неправильное ограничение чрезмерных попыток аутентификации

Уязвимость возникает, когда система не ограничивает количество попыток ввода учетных данных, что позволяет злоумышленнику использовать метод "грубой силы" для перебора паролей.

CWE-521: Слабые требования к паролям

Если система не требует создания сложных паролей, это увеличивает риск успешного подбора пароля злоумышленником.

CWE-89: Неправильная нейтрализация специальных элементов, используемых в SQL-команде.

Эта уязвимость возникает, когда приложение не фильтрует входящие данные должным образом. Злоумышленники могут использовать SQL-инъекции для выполнения произвольных команд в базе данных, что может позволить им обойти механизмы аутентификации.

CWE-90: Неправильная нейтрализация специальных элементов в LDAP-запросах

Если приложение не защищает данные для LDAP-запросов, злоумышленники могут манипулировать запросами для обхода аутентификации и получения доступа к конфиденциальной информации.

Созданы соответствующие алгоритмы работы программ СЗИ (см. рис. 4-6).

Алгоритм обнаружения техники T1110.001 – Brute Force: Password Guessing в сценарии 1 представляет собой процесс мониторинга попыток аутентификации и применения ограничений на количество неудачных попыток ввода учетных данных. Основная цель этого алгоритма – своевременно блокировать попытки атаки методом грубой силы, ограничив возможности для перебора паролей, и одновременно уведомить администратора о возможной атаке, как указано в работе [14] (см. рис. 4).

1) Мониторинг попыток аутентификации:

Каждая попытка аутентификации (включая как успешные, так и неудачные) фиксируется системой.

Для каждой учетной записи или IP-адреса, с которого происходят попытки входа, отслеживаются число неудачных попыток и время последней попытки.

2) Проверка на превышение лимита попыток:

Для каждой учетной записи или IP-адреса система проверяет, сколько неудачных попыток аутентификации произошло за определенный период. Если количество неудачных попыток превышает установленный лимит, например, пять попыток за 15 минут, то включается блокировка учетной записи или IP-адреса.

3) Регистрация блокировки:

После блокировки система записывает событие в логи для последующего анализа и расследования инцидента. Также система может автоматически запустить анализатор, чтобы выявить и заблокировать дополнительные попытки с других IP-адресов или учетных записей, если такие обнаружены.

4) Предотвращение атаки методом грубой силы:

Система применяет время ожидания (например, блокировка на 15 минут) после превышения лимита попыток, чтобы предотвратить дальнейшие атаки с того же IP или учетной записи.

Вместо отображения ошибки «неверный пароль» система может отображать нейтральное сообщение, например, «неправильные учетные данные», чтобы не предоставлять информацию злоумышленнику о том, что ошибка заключается в неправильном пароле.

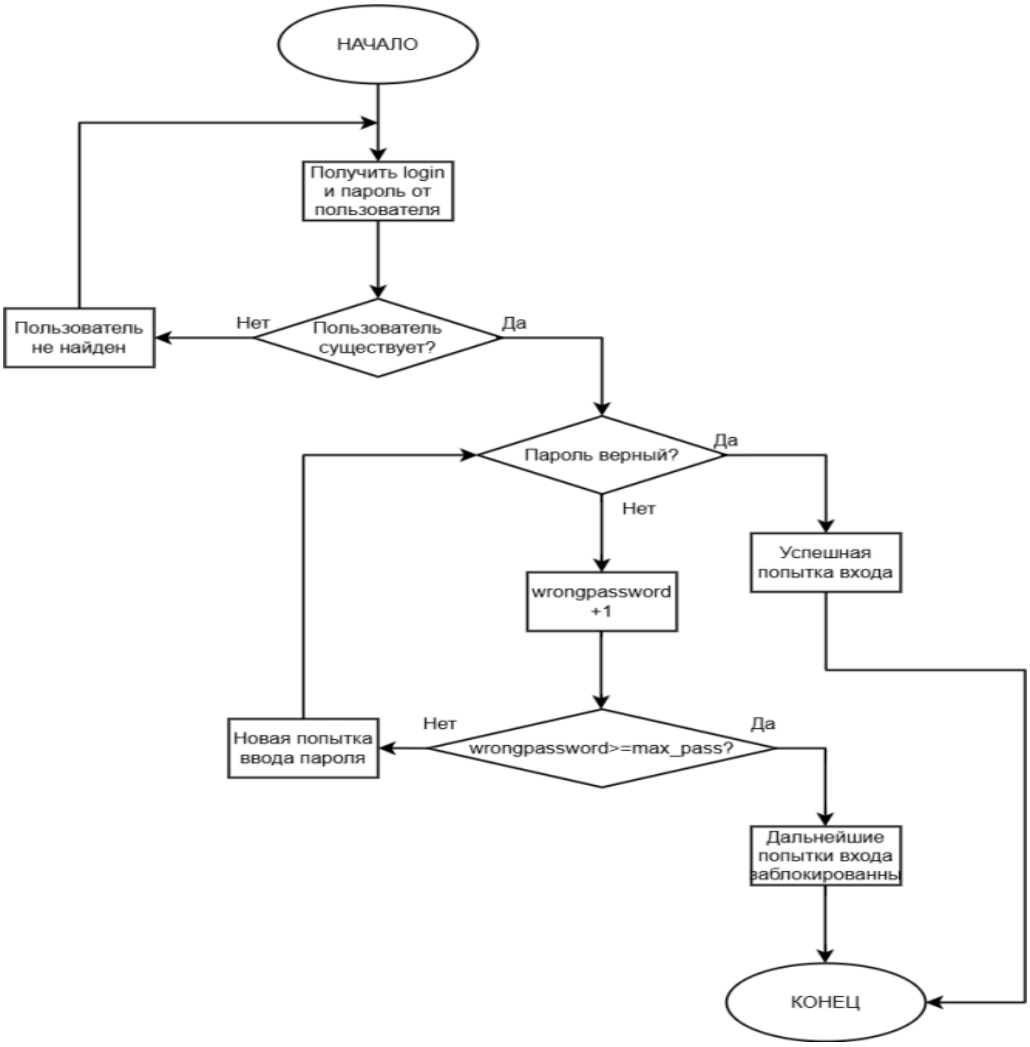

Рис. 4. Блок-схема алгоритма обнаружения техники T1110.001

Алгоритм обнаружения и нейтрализации техники T1190: Exploit Public-Facing Application для защиты от уязвимости CWE-89: Неправильная нейтрализация специальных элементов, используемых в SQL-команде (Structured Query Language), будет включать этапы анализа запросов и обнаружения потенциально опасных паттернов (табл. 1). Задача алгоритма — выявить подозрительные SQL-запросы, которые могут свидетельствовать о попытках использования SQL-инъекций, и предотвратить их выполнение. Основные этапы будут сосредоточены на проверке символов и структуры запросов, как указано в работе [10]. В работе алгоритма используется библиотека re (см. рис. 5).

Таблица 1

Паттерн	Описание
Неэкранированные символы	Использование символов ', ", ;, ` может завершать строковые литералы или выполнять несколько команд в одном запросе.
Использование комментариев	Символы --, /* ... */ позволяют скрывать части запроса, изменяя его логику.
Объединение строк	Символы, используемые для объединения строк в запросах, например: `
Неявное преобразование	Автоматическое преобразование типов в базе данных может приводить к неожиданным результатам и уязвимостям. ' OR 'a' = 'a' (где строка преобразуется в число или булевое значение)
Использование подзапросов	Символы, используемые для создания подзапросов, например: (,)
SQL-функции	Символы, которые могут быть использованы для выполнения SQL-функций, например: *, =, IN, BETWEEN
Регулярные выражения	Символы, используемые для работы с регулярными выражениями в SQL, например: ^, $, ., *, +, []

Рис. 5. Блок-схема алгоритма обнаружения техники T1190

Таблица 2

Этап проверки	Пример запроса
1.Есть ли символы =,1,1 в одной строке?	SELECT * FROM users WHERE username = 'admin' AND password = '' OR 1=1 --';
2.Есть ли опасные символы? (;', --)	SELECT * FROM users WHERE username = 'test'; DROP TABLE users; --';
3.Есть ли вложенные запросы? (SELECT, UNION)?	SELECT * FROM users WHERE id = (SELECT MAX(id) FROM admin_users);

Причина блокировки на этапах проверки (табл. 2):

На этапе проверки 1: Условие 1=1 всегда истинно, что позволяет обойти проверку аутентификации. Всё после -- игнорируется, исключая важные элементы проверки.

На этапе проверки 2: После выполнения SELECT * FROM users WHERE username = 'test', символ ; запускает команду DROP TABLE users;, удаляя таблицу. Комментарий -- игнорирует оставшуюся часть запроса.

На этапе проверки 3: Подзапрос извлекает максимальный id из admin_users и передаёт его в основной запрос, позволяя злоумышленнику получить данные из другой таблицы.

На рисунке 5 представлена блок-схема алгоритма обнаружения техники **T1190.**

Алгоритм обнаружения и нейтрализации техники T1071.001: Application Layer Protocol: Web Protocols для защиты от уязвимости CWE-90: LDAP Injection включает несколько этапов, направленных на анализ и защиту от атак через LDAP-запросы (Lightweight Directory Access Protocol). Важным моментом является выявление опасных символов и конструкций в запросах (табл. 3), а также предотвращение их выполнения в системе как указано в работе [9]. В работе алгоритма используется библиотека re (рис. 6).

Таблица 3

Паттерн	Описание
Неэкранированные символы	Символы, которые могут завершить строку или вызвать ошибку в запросах, например: *,), (, &, `
Использование комментариев	Вставка комментариев, скрывающих часть LDAP-запроса и изменяющих его логику, например: /*, */, --
Объединение строк	Символы, используемые для объединения строк в запросах, например: +, `
Неявное преобразование	Символы, приводящие к неявному преобразованию данных, например: ', ", #
Использование подзапросов	Символы, используемые для формирования подзапросов, например: (,)
LDAP-функции	Символы, которые могут быть использованы для выполнения LDAP-функций, например: *, =
Регулярные выражения	Символы для создания регулярных выражений в LDAP-запросах, например: ^, $, ., *, +, ?, [], `

Таблица 4

Этап проверки	Пример запроса
1.Есть ли операторы (&), (|)?	(&(objectClass=admin)(uid=*))
2.Есть ли опасные символы (*, (,))?	(&(uid=*)(password=*))
3. Есть ли вложенные запросы?	(&(uid=admin)(!(password=*))(&(sn=Smith)(givenName=John)))

Причина блокировки на этапах проверки:

На проверке 1: Условие 1=1 всегда истинно, позволяя обойти аутентификацию. Всё после -- игнорируется, включая важные проверки.

На проверке 2: Команда; DROP TABLE users; запускается после SELECT * FROM users WHERE username = 'test', удаляя таблицу. Остальная часть запроса игнорируется из-за --.

На проверке 3: Подзапрос извлекает максимальный id из admin_users, передавая его в основной запрос, что даёт доступ к данным другой таблицы.

На рисунке 6 представлена блок-схема алгоритма обнаружения техники **T1071.001.**

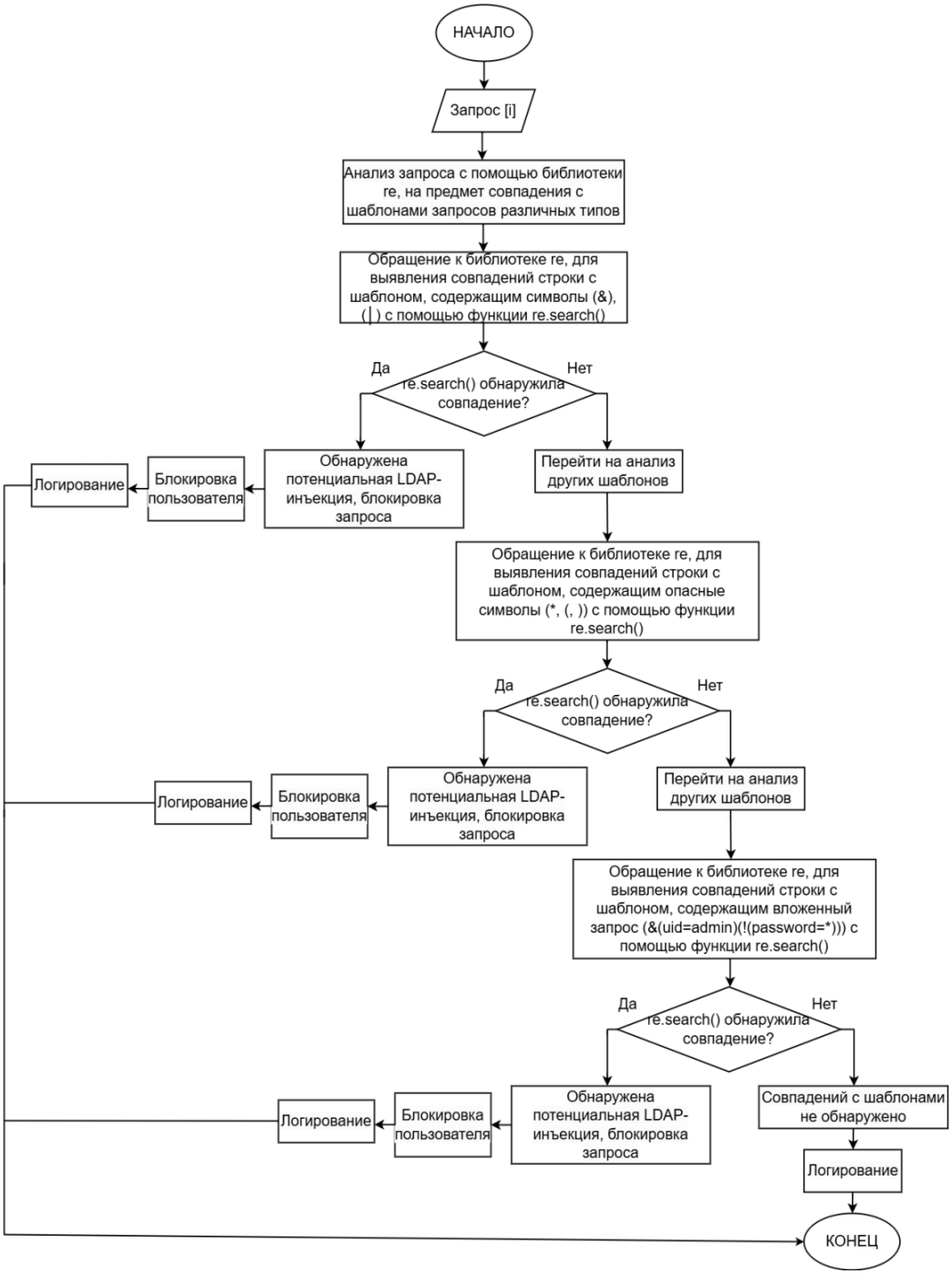

Рис. 6. Блок-схема алгоритма обнаружения техники T1071.001

Все описанные алгоритмы работают в комплексе, формируя многоуровневую систему защиты от атак. Каждый из них нацелен на нейтрализацию специфических техник MITRE ATT&CK, усиливая общую безопасность системы за счёт взаимодействия:

Ограничение попыток аутентификации (T1110.001) и проверка на SQL-инъекции (T1190) совместно блокируют автоматизированные попытки обхода аутентификации.

Фильтрация и экранирование предотвращают выполнение вредоносных SQL- и LDAP-запросов, защищая систему от инъекций и манипуляций.

Каждое решение важно само по себе, но их комплексная реализация создаёт мощную защиту, минимизируя риски обхода аутентификации и работы с запросами.

Заключение

Сформированы типовые сценарии обхода аутентификации на основе техник MITRE ATT&CK и разработаны алгоритмы, направленные на повышение безопасности процессов аутентификации.

Совместное использование предложенных в статье алгоритмов реализации защитных мер направлено на минимизацию рисков, связанных с эксплуатацией вышеуказанных уязвимостей.

Литература

1. Приказ ФСТЭК России от 18 февраля 2013 г. № 21 "Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных". [Электронный ресурс]. URL: https://www.consultant.ru/document/cons_doc_LAW_146520/ (дата обращения: 26.12.2024).

2. Приказ ФСТЭК России от 11 февраля 2013 г. № 17 "Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах". [Электронный ресурс]. URL: https://fstec.ru/dokumenty/vse-dokumenty/prikazy/prikaz-fstek-rossii-ot-11-fevralya-2013-g-n-17 (дата обращения: 24.12.2024).

3. ГОСТ Р 50922-2006. Защита информации. Средства криптографической защиты информации. Общие требования. Введ. 01.01.2007. М.: Стандартинформ, 2006.

4. MITRE. CWE-89: Improper Neutralization of Special Elements used in an SQL Command (‘SQL Injection’). [Электронный ресурс]. URL: https://cwe.mitre.org/data/definitions/89.html (дата обращения: 28.12.2024).

5. InfoWatch. Исследование утечек информации в отраслях за три года. [Электронный ресурс]. URL: https://www.infowatch.ru/analytics/analitika/issledovaniye-utechek-informatsii-v-otraslyakh-za-tri-goda (дата обращения: 18.12.2024).

6. Trend Micro. Avoid LDAP injection attacks [Электронный ресурс]. URL: https://www.trendmicro.com/ru_ru/research/23/c/avoid-ldap-injection-attacks.html (дата обращения: 28.01.2025).

7. MITRE. CAPEC-66: SQL Injection [Электронный ресурс]. URL: https://capec.mitre.org/data/definitions/66.html (дата обращения: 28.01.2025).

8. Positive Technologies. Кибербезопасность в 2023–2024 гг.: тренды и прогнозы. Часть третья [Электронный ресурс]. URL: https://www.ptsecurity.com/ru-ru/research/analytics/kiberbezopasnost-v-2023-2024-gg-trendy-i-prognozy-chast-tretya/ (дата обращения: 30.01.2025).

9. OWASP Cheat Sheet Series. LDAP Injection Prevention Cheat Sheet [Электронный ресурс]. URL: https://cheatsheetseries.owasp.org/cheatsheets/LDAP_Injection_Prevention_Cheat_Sheet.html (дата обращения: 30.01.20

10. OWASP Cheat Sheet Series. SQL Injection Prevention Cheat Sheet [Электронный ресурс]. URL: https://cheatsheetseries.owasp.org/cheatsheets/SQL_Injection_Prevention_Cheat_Sheet.html (дата обращения: 30.01.2025).25).

11. MITRE ATT&CK. Application Layer Protocol: Web Protocols (T1071.001) [Электронный ресурс]. URL: https://attack.mitre.org/techniques/T1071/001/ (дата обращения: 30.01.2025).

12. Atomic Red Team. T1110.001 – Брутфорс: подбор пароля [Электронный ресурс]. URL: https://www.atomicredteam.io/atomic-red-team/atomics/T1110.001 (дата обращения: 30.01.2025).

13. MITRE ATT&CK. T1190 – Эксплуатация публичных приложений [Электронный ресурс]. URL: https://attack.mitre.org/techniques/T1190/ (дата обращения: 30.01.2025).

14. OWASP Cheat Sheet Series. Authentication Cheat Sheet [Электронный ресурс]. URL: https://cheatsheetseries.owasp.org/cheatsheets/Authentication_Cheat_Sheet.html (дата обращения: 30.01.2025).

15. MITRE. CWE-90: Improper Neutralization of Special Elements used in an LDAP Query ('LDAP Injection') [Электронный ресурс]. Режим доступа: https://cwe.mitre.org/data/definitions/90.html (дата обращения: 30.01.2025).

СРАВНИТЕЛЬНЫЙ АНАЛИЗ ОСНОВНЫХ АЛГОРИТМОВ СУММАРИЗАЦИИ ТЕКСТА

Фатхулин Тимур Джалилевич
Московский технический университет связи и информатики, доцент кафедры МК и ИТ, к.т.н., Москва, Россия
t.d.fatkhulin@mtuci.ru

Баринов Константин Александрович
Московский технический университет связи и информатики, студент группы БВТ2302, Москва, Россия

Вотчицева Вероника Михайловна
Московский технический университет связи и информатики, студентка группы БВТ2302, Москва, Россия

Аннотация
Суммаризация текста – одна из ключевых задач обработки естественного языка, которая представляет собой сжатую передачу содержания оригинального текста с сохранением ключевой информации. Цель работы – осуществить сравнительный анализ основных алгоритмов суммаризации текста. В статье проанализированы существующие известные подходы к автоматической суммаризации текста, включая экстрактивные методы TF-IDF и TextRank, и абстрактивные методы, такие как BART. Проведен анализ их производительности, преимуществ и ограничений на основе экспериментальных данных и текущих исследований.

Ключевые слова
Суммаризация, машинное обучение, текст, обработка, естественный язык, экстрактивная суммаризация, абстрактивная суммаризация, нейронные сети

Введение

В настоящее время существует технология машинного обучения, позволяющая осуществлять интерпретацию естественного человеческого языка, понимать и интерпретировать содержание человеческой речи. Эта технология по обработке естественного языка известна как NLP (Natural Language Processing) [1, 9, 10, 13, 18]. В современном информационном обществе, когда любая компания, организация, государственная структура получает и обрабатывает огромное количество текстовых, голосовых, видео-сообщений, электронных писем, новостных лент социальных сетей использование технологии NLP становится крайне актуальным.

Сегодня важно не только получить и обработать информацию, но и максимально ужать ее, сделав ее объем удобным для работы [8, 11-17, 19-21]. Чтобы справиться с растущим объемом данных и при этом не потерять принципиально важную информацию, программное обеспечение должно выполнять поставленную задачу не хуже, чем это делает человек. Автоматическое сжатие или суммаризация текста осуществляется при помощи технологии ATS (Automatic Text Summarization) Получение сжатого содержания объемного документа в повседневной практике трудно переоценить. Кроме экономии времени суммаризация позволяет просканировать и свести воедино внушительный объем информации для ее дальнейшей презентации, обработки, и многофункционального использования [15, 19, 21]. Это определяет актуальность настоящего исследования [1].

Классификация методов суммаризации

Прежде чем приступить к рассмотрению методов и алгоритмов суммаризации текста, необходимо отметить, что автоматическая суммаризация является имитацией схожего процесса в естественном языке. Человек, передавая краткое основное содержание какого-либо текста, осуществляет ряд операций (латентно или осознанно), которые легли в основу подходов автоматической суммаризации. Человек знакомится с текстом, выделяет наиболее существенную информацию, перерабатывает ее,

удаляя ненужные детали, сжимая текст на семантическом уровне, оставляет в новом тексте основные, значимые понятия. Кратко излагая содержание исходного текста, человек может добавить оценочную составляющую к передаваемой информации. При автоматической суммаризации все эти действия раскладываются на отдельные этапы, которые будут раскрыты ниже.

Существует множество классификаций методов суммаризации [5]. Кроме своего назначения, данные классификации отличаются друг от друга по форматам ввода и вывода, а также по степени подробности.

По *формату ввода* методы делятся на основе разных подходов. Подходы Single Document могут принимать на вход только один документ (текст). У этого метода есть существенный недостаток: если документов с похожей темой несколько, он просто не может их обработать. С данной задачей справляются подходы Multi Document, однако реализация алгоритмов в этих методах отличается высокой сложностью, что является их основным недостатком. методов.

По *формату вывода* методы делятся на экстрактивные (extractive) и абстрактивные (abstractive). Экстрактивные подходы (от англ. extract «выделять, вычленять») выделяют в тексте куски, несущие самую существенную информацию и на их основе составляют новый текст с сжатым содержанием исходного. Абстрактивные подходы заново генерируют новый текст, который представляет собой кратко изложенное содержание ключевой информации из исходного текста.

По* подробностям *методы делятся на ориентировочные и информативные. Если человеку необходимо получить лишь самое общее представление о содержании исходного текста, подойдут ориентировочные подходы. Если же необходим обзор исходного текста, лучше подойдут информативные подходы.

По *назначению* методы делятся на направленные на тему и ненаправленные на тему. Направленные подходы имеют определенную тему, поэтому подходят только для текстов (документов), связанных с конкретной темой, в то время как ненаправленные подходы не имеют какой-то конкретной области или темы, поэтому подходят для любого текста и будут показывать результаты лучше направленных методов за исключением той темы, на которую они направлены.

Методы предобработки текста

Предобработка текста – неотъемлемая часть любой задачи обработки естественного языка, включая автоматическую суммаризацию текста [1, 18, 21]. Предобработка необходима для улучшения работы алгоритма суммаризации и повышения точности результатов. Важными *этапами* предобработки являются ниже представленные процессы.

Этап 1. *Токенизация* – процесс разбиения текста на меньшие единицы, называемые токенами. Так как этот метод работает с текстом, не как со строкой, а как с цепочкой отдельных объектов, то преобразование текста в этом случае начинается с деления исходного текста на предложения, а затем на отдельные слова – токены.

Этап 2. *Удаление «стоп-слов»* предполагает изъятие из текста всех незначимых слов, которые не содержат существенной информации, например, частиц, предлогов, артиклей, союзов.

Этап 3. *Нормализация текста* предполагает конвертацию в текстовый формат дат, чисел, приведение к нижнему регистру всех символов. Например: 25 → двадцать пять, расшифровке аббревиатур, например: NLP → Natural Language Processing. Данный метод помогает улучшить работу алгоритма, так как предобработка текста будет производиться без учета различий, вызванных регистрами или опечатками.

Этап 4. *«Лемматизация»* — это приведение однокоренных слов к начальной форме: «печеный» → “печь”, “столбы” → “столб”, “гуляли” → “гулять”.

Этап 5. *«Стемминг»* — это удаление окончаний, префиксов, аффиксов до основы слова, то ест до его неизменяемой части. Например: “лесной” → “лес”, “столовый” → “стол”.

Этап 6. *Удаление пунктуации и специальных символов* – процесс удаления знаков препинания, например: «.», «,», «?», «!» и специальных символов, например: «\», «$», «*», «[«, «]», «^», «&». Данный метод может помочь упростить обработку текста. Однако в некоторых случаях, например, при анализе эмоциональной окраски текста, знаки препинания могут быть важны и их следует учитывать.

Этап 7. *Разметка частей речи* предполагает не только выделение существительных, глаголов, прилагательных, наречий, местоимений и т.д., но и определение их функций в предложении (подле-

жащее, определение, сказуемое, обстоятельство и т.д.) Являясь дополнительным критерием отбора, этот метод указывает и на большую семантическую информативность значимых частей речи по сравнению со служебными (союзами, предлогами, частицами).

Этап 8. *Частотный анализ и выделение признаков* – процесс, направленный на улучшение качества экстрактивной суммаризации, помогающий определить важные слова или фразы на основе частоты их встречаемости в тексте. Например: TF-IDF (Term Frequency-Inverse Document Frequency).

Пример предобработки текста представлен в таблице 1.

Таблица 1

Примеры результатов предобработки текста

Этап предобработки	**Пример текста**
Исходный текст	«Этот текст предназначен для примера предобработки текста в задаче суммаризации.»
Токенизация	[«Этот», «текст», «предназначен», «для», «примера», «предобработки», «текста», «в», «задаче», «суммаризации»]
Удаление «стоп-слов»	[«текст», «предназначен», «примера», «предобработки», «текста», «задаче», «суммаризации»]
«Лемматизация»	[«текст», «предназначать», «пример», «предобработка», «текст», «задача», «суммаризация»]

Сравнительный анализ методов суммаризации

Поведем сравнительный анализ методов суммаризации текста и определим их основные ключевые особенности.

Статистические подходы – одни из первых подходов, которые применялись для решения задачи автоматической суммаризации текста. Например, *TF-IDF (Term Frequency-Inverse Document Frequency)* – это численный признак слова, показывающий как часто слово встречается в предложении и в множестве предложений. TF-IDF рассчитывается по следующей формуле:

$$tfidf(w) = tf(w) * idf(w)$$

где *tf(w) = (сколько раз слово встретилось в предложении) / (число слов в предложении), idf(w) = log(количество предложений / количество предложений со словом «w» в них).*

Чтобы посчитать TF-IDF для всего предложения, достаточно сложить значения TF-IDF слов в этом предложении. Алгоритм суммаризации, основанный на этом методе, будет выглядеть следующим образом:

- загрузить текстовый документ;
- предобработать текст;
- посчитать TF-IDF значения для каждого слова;
- посчитать TF-IDF значения для каждого предложения;
- составить краткое содержание.

Графовые подходы — подходы, которые основаны на графовом представлении предложений текста. Например, *TextRank* — графовый алгоритм, главной идеей которого является “рекомендация”. Каждое предложение выполняет роль вершины направленного графа. Если вершина A соединяется с вершиной B, это значит, что вершина B получила “голос” или “рекомендацию” от вершины A. Чем больше число голосов у вершины, тем больше важность предложения, более того, важность вершины, которая отправляет голос, влияет на важность голоса. Рекомендацию можно определить по-разному. Для задачи суммаризации такой “голос” определяют, как сходство двух предложений.

Алгоритм суммаризации, основанный на этом подходе, будет выглядеть следующим образом:

- загрузить текст (документ);
- предобработать текст (документ);
- составить граф, вершинами которого будут являться предложения;
- получить оценки сходства для каждой пары предложений;
- отсортировать все вершины и составить краткое содержание.

Модели глубокого обучения – подходы, основанные на машинном обучении. При этом выполняется определенный алгоритм и на выходе создается текст, который по своей семантике практически не отличается от естественно языкового текста. Характерной особенностью этих подходов является необходимость обучения модели и его тщательное тестирование, а также существенное количество параметров и данных для обучения модели. Их характерная особенность заключается в том, что содержание текста, полученного в результате выполненного алгоритма, схоже семантически с текстом, составленным человеком. Большие временные затраты и производительность работы данного алгоритма зависят от вышеназванных факторов. Все это влияет на производительность и время работы данного алгоритма. Например, *BART* – шумоподавляющий автоэнкодер, который был натренирован на задании восстановления поврежденных текстов. Предобученные версии этой модели показывают отличные результаты на *Sequence-to-Sequence* (от англ. sequence «последовательность») seq2seq заданиях, когда на вход подается одна последовательность слов или предложений, а на выходе эта последовательность изменяется.

С точки зрения качества суммаризации, современные абстрактивные методы, такие как BART, превосходят экстрактивные подходы. Тем не менее, для специфических задач, где важна точность передачи исходной информации, экстрактивные методы остаются актуальными. Например, алгоритмы на основе TextRank продолжают использоваться для быстрого анализа больших текстовых массивов.

Сравнение методов суммаризации текста представлено в таблице 2.

Таблица 2

Сравнение методов суммаризации текста

Метод	**Тип**	**Преимущества**	**Недостатки**
TF-IDF	экстрактивный	простота реализации, высокая скорость	не учитывает семантический контекст
TextRank	экстрактивный	основан на графовых структурах, гибкость	трудности с длинными текстами
BART	абстрактивный	высокая точность, подходит для сложных задач	требует больших вычислительных ресурсов

Результаты, получаемые методами суммаризации текста

Для оценки производительности алгоритмов используются следующие критерии оценивания [2-7, 21]:

- *ROUGE* (Recall-Oriented Understudy for Gisting Evaluation) — метрика, осуществляющая оценку совпадений между сгенерированным резюме и эталонным текстом.
- *BLEU* (Bilingual Evaluation Understudy) — алгоритм оценки качества текста, который был переведен на машинный перевод с одного естественного языка на другой.
- Читаемость — качество и связность текста, оцениваемое экспертами.
- Время выполнения — время, за которое алгоритм выполняет задачу суммаризации текста. Чем быстрее выполняется алгоритм, там он более эффективен на больших данных.

ROUGE отличается от BLEU в своей оценке, поскольку он вычисляет отзыв, в то время как BLEU вычисляет точность. Это означает, что ROUGE в первую очередь фокусируется на определении того, сколько информации из справочных отрывков содержится в сгенерированном отрывке.

Эксперименты показывают [1,4], что экстрактивные методы, такие как TextRank, достигают высоких значений метрик ROUGE для текстов с четкой структурой. Абстрактивные подходы демонстрируют лучшее качество для текстов с более сложной организацией информации, таких как научные статьи и эссе. Однако их производительность снижается при обработке длинных текстов или текстов с неоднородным стилем.

Для иллюстрации качества работы алгоритмов суммаризации проведем эксперимент, в котором исходный текст будет обработан экстрактивным и абстрактивным подходами. Для оценки результатов будут использоваться метрики ROUGE, BLEU, а также субъективная оценка читаемости.

Исходный текст: *«Технологии машинного обучения нашли широкое применение в бизнесе. Они помогают автоматизировать процессы, анализировать данные и улучшать качество.»*

Результаты работы алгоритма представлены в таблицах 3 и 4.

Таблица 3

Оценка результатов алгоритмов суммаризации текста

Метод суммаризации текста	ROUGE-1	ROUGE-2	BLEU	Читаемость (баллы от 1 до 5)	Время выполнения, с
TF-IDF	0.85	0.72	0.76	4	0.2
TextRank	0.88	0.74	0.79	4.5	0.5
BART	0.92	0.85	0.81	5	1.8

Таблица 4

Результат работы различных методов суммаризации

Метод суммаризации текста	Резюме
TF-IDF	«Технологии машинного обучения нашли применение в бизнесе»
TextRank	«Машинное обучение автоматизирует процессы и улучшает качество»
BART	«Машинное обучение автоматизирует бизнес-процессы и повышает качество»

Заключение

В результате проведенного исследования были проанализированы основные методы сумммаризации текста. Показано, что автоматическая суммаризация текста – активная область исследований, которая продолжает развиваться благодаря появлению новых технологий и методов обработки естественного языка. Экстрактивные методы остаются эффективными и доступными для многих практических задач, однако абстрактивные подходы на основе нейронных сетей открывают новые возможности для создания более качественных резюме.

В ходе работы были представлены экспериментальные данные, которые дают возможность наглядно оценить, как работает тот или иной метод суммаризации текста. Результаты экспериментов систематизированы в соответствующих таблицах.

Будущие исследования должны быть направлены на разработку гибридных методов, которые объединяют преимущества экстрактивных и абстрактивных подходов. Кроме того, требуется улучшение обработки длинных текстов и учет контекста для повышения точности и адекватности суммаризации текста.

Литература

1. *Фатхулин Т.Д., Климов Н.Ю., Гежин С.А.* Анализ нейросетевых технологий, позволяющих генерировать текст // Труды Северо-Кавказского филиала Московского технического университета связи и информатики. 2023. № 1. С. 123-127. EDN MXCTVO

2. *See A., Liu P.J., Manning C.D.* Get to the Point: Summarization with Pointer-Generator Networks // Proceedings of the 2017 Conference on Empirical Methods in Natural Language Processing.

3. *Lewis M., Liu Y., Goyal N.* et al. BART: Denoising Sequence-to-Sequence Pre-training for Natural Language Generation, Translation, and Comprehension // Proceedings of the 58th Annual Meeting of the Association for Computational Linguistics.

4. *Mihalcea R., Tarau P.* TextRank: Bringing Order into Texts // Proceedings of the 2004 Conference on Empirical Methods in Natural Language Processing.

5. *Белякова А.Ю., Беляков Ю.Д.* Обзор задачи автоматической суммаризации текста. https://cyberleninka.ru/article/n/obzor-zadachi-avtomaticheskoy-summarizatsii-teksta/viewer (дата обращения: 24.11.2024).

6. Что такое NLP [Электронный ресурс]. Режим доступа: https://aws.amazon.com/ru/what-is/nlp/ (дата обращения: 01.12.2024).

7. Суммаризация текста: подходы, алгоритмы, рекомендации и перспективы [Электронный ресурс]. Режим доступа: https://habr.com/ru/articles/514540/ (дата обращения: 17.11.2024).

8. *Вострикова П.В., Рыбка С.О., Рыжкова У.С., Фатхулин Т.Д.* Анализ нейросетевых технологий, использующихся для улучшения качества изображений // REDS: Телекоммуникационные устройства и системы. 2024. Т. 14, № 1. С. 57-65. EDN WVBDRN

9. *Фатхулин Т.Д., Смирнов Д.А., Разумов И.В.* и др. Анализ влияния составляемых текстовых запросов (промптов) на качество изображений, генерируемых нейросетевыми технологиями // Системы синхронизации,

формирования и обработки сигналов. 2024. Т. 15, № 2. С. 52-57. EDN TSVMSK

10. *Леохин Ю.Л., Фатхулин Т.Д.* Разработка методов и алгоритма формализации текстового запроса к онлайн-сервисам, генерирующим изображения посредством нейросетевых технологий // Вестник Рязанского государственного радиотехнического университета. 2023. № 85. С. 82-95. DOI 10.21667/1995-4565-2023-85-82-95. EDN PZWYZV

11. *Леохин Ю.Л., Фатхулин Т.Д., Кожанов М.С.* Анализ и исследование применения нейросетевых технологий для генерации программного кода // Вестник Рязанского государственного радиотехнического университета. 2024. № 87. С. 41-53. DOI 10.21667/1995-4565-2024-87-41-53. EDN HKEOFX

12. *Леохин Ю.Л., Фатхулин Т.Д., Ментус М.В.* Разработка и применение методов распознавания зашумленных аудиофайлов посредством нейросетевых технологий // Вестник Рязанского государственного радиотехнического университета. 2024. № 88. С. 65-73. DOI 10.21667/1995-4565-2024-88-65-73. EDN NMXASI

13. *Маслов К.В., Фатхулин Т.Д., Иванов Д.А.* Анализ технологий автоматизации бизнес-процессов и разработки программного обеспечения с использованием low-code платформ // Труды Северо-Кавказского филиала Московского технического университета связи и информатики. 2024. № 1. С. 6-11. EDN HDBOYM

14. *Фатхулин Т.Д., Бойцов К.В.* Анализ функционала программного обеспечения, применяемого для классификации труб на предприятии методами компьютерного зрения // Труды Северо-Кавказского филиала Московского технического университета связи и информатики. 2024. № 2. С. 6-12. EDN FVQYQA

15. *Мяличева А.А., Фатхулин Т.Д.* Анализ методов машинного обучения для прогнозирования дефектов в исходном коде // Труды Северо-Кавказского филиала Московского технического университета связи и информатики. 2024. № 2. С. 16-19. EDN IVJCZF

16. *Фатхулин Т.Д., Леонова В.О., Тремасова Л.А.* Анализ нейросетевых технологий, применяемых для web-разработки // REDS: Телекоммуникационные устройства и системы. 2024. Т. 14, № 2. С. 35-41. EDN SDCNKM

17. *Фатхулин Т.Д., Исаев А.В.* Анализ моделей ARIMA и LSTM, используемых для прогнозирования криптовалют и определения портфеля инвестиций // Труды Северо-Кавказского филиала Московского технического университета связи и информатики. 2024. № 2. С. 20-25. EDN ODWOPA

18. *Фатхулин Т.Д., Фатхулина Г.Г., Ментус М.В.* Разработка методики формирования запроса к нейросети с целью генерации изображений с учетом рекомендаций компьютерной лингвистики // Труды Северо-Кавказского филиала Московского технического университета связи и информатики. 2023. № 1. С. 133-139. EDN PPRTOM

19. *Фатхулин Т.Д., Исаев А.В.* Анализ эффективности использования моделей ARIMA для прогнозирования котировок и определения портфеля инвестиций в области криптовалюты // Труды Северо-Кавказского филиала Московского технического университета связи и информатики. 2024. № 2. С. 26-31. EDN CESRTK

20. *Фатхулин Т.Д., Бойцов К.В.* Оценка эффективности алгоритма на основе YOLO v.8 для классификации труб на предприятии по фото в зависимости от различных условий // Труды Северо-Кавказского филиала Московского технического университета связи и информатики. 2024. № 2. С. 51-55. EDN KWLMYA

21. *Вишневский В.М., Леохин Ю.Л., Фатхулин Т.Д., Занегин А.В.* Методы машинного обучения в решении задачи прогнозирования спроса на отдельные виды товаров // T-Comm: Телекоммуникации и транспорт. 2024. Том 18. №10. С. 34-43.

ИМИТАЦИОННАЯ МОДЕЛЬ АЛГОРИТМА МИЛЛЕРА-РАБИНА ПРОВЕРКИ ЧИСЕЛ НА ПРОСТОТУ

Михалевич Игорь Феодосьевич
Российский университет транспорта, доцент, к.т.н., старший научный сотрудник, Москва, Россия
mif-orel@mail.ru

Савин Лев Андреевич
Российский университет транспорта, студент, Москва, Россия
savin.lev.and@gmail.com

Аннотация
В статье представлена имитационная модель алгоритма Миллера-Рабина проверки чисел на простоту. Она разработана в целях повышения уровня понимания сложной математики, используемой в современной криптографии. Рассмотрены примеры, способствующие восприятию материала. Проведен базовый анализ полученных данных, выявлены ключевые закономерности. Рассмотрены криптографические системы, использующие простые числа.

Ключевые слова
Алгоритм Миллера-Рабина, вероятностный тест, детерминированный тест, имитационная модель, информационная безопасность, криптографическая система, простое число, алгоритм Диффи-Хеллмана, составное число, RSA

Введение

Одна из проблем подготовки специалистов в сфере информационной безопасности – это сложность математической составляющей дисциплины, особенно в области криптографии. Многие студенты сталкиваются с трудностями в освоении этого материала в ограниченные сроки. Это связано не только с его высокой сложностью, но и с большим объемом информации, которая зачастую оказывается неполной или противоречивой.

Трудность в изучение вносит иерархическая система математического материала – упущенный фрагмент значительно усложнит или сделает невозможным освоение дальнейших тем. Это особенно актуально для таких разделов, как криптография, в которых лишь твердое знание предыдущего материала позволит освоить новые понятия. Для облегчения понимания и повышения интереса рекомендуется использовать наглядные примеры, включая создание имитационных моделей (ИМ) систем, что делает материал более доступным и понятным [1].

Выбор моделируемой системы

Многие криптографические протоколы и системы основаны на преобразовании информации, алгоритмы которого зачастую требуют нахождения простых чисел [2-6] – тех, что в качестве делителя имеют только себя и единицу. Среди алгоритмов, которые используют простые числа – Диффи-Хеллмана [7], RSA [8]. Рассмотрим их них более подробно, чтобы разобраться, какие задачи может решать разработанная ИМ.

Выработка ключей в алгоритме RSA

Алгоритм RSA [8] основан на сложности факторизации большого полупростого числа, то есть такого числа, делителем которого является лишь само число, единица и еще два простых числа. В качестве большого числа будем подразумевать число, имеющее больше 300 знаков в десятичной записи [5]. Поиск множества простых чисел для создания полупростого является ключевой задачей для генерации стойкого ключа. Этот процесс требует уверенности в том, что число является простым, и как следствие, применения способа быстрой проверки числа на простоту. Рассмотрим подробнее процесс выработки открытого и закрытого ключей.

Первостепенно выбираются два случайных больших простых числа. Большими числа должны быть в целях криптографической стойкости, чтобы ЭВМ не могла впоследствии быстро разложить полупростое число перебором. Обозначим два таких числа как p и q.

Следующий шаг – вычисление произведения $n = p * q$, которое будет являться модулем для наших открытого и закрытого ключей. Затем вычисляется функция Эйлера от этого модуля, то есть, количество чисел взаимно простых с модулем. Взаимно простые числа – это те, что имеют в качестве единственного общего делителя число 1. В нашем случае модуль будет полупростым, а значит, функция Эйлера будет иметь следующий вид:

$$\phi(n) = (p - 1) * (q - 1) \quad (1)$$

Следующим этапом идет выбор числа, которое будет частью открытого ключа. Обычно берут малое число e: $1 < e < \phi(n)$, - чтобы обеспечить быстроту зашифрования с помощью алгоритма [2]. Затем находится обратное мультипликативное к этому числу по модулю $\phi(n)$, то есть такое d, что $e * d \equiv 1 \pmod{\phi(n)}$. Пара чисел e и n являются открытым ключом, а пара d и n – закрытым ключом. Нетрудно заметить, что если в качестве n будет выбрано не полупростое число, то факторизация станет гораздо проще, и криптографическая стойкость протокола сойдет на нет. ЭВМ сможет быстро найти делители такого числа и получить закрытый ключ [2, 5]. Также следует отметить, что с прогрессом в квантовых технологиях возникает необходимость в увеличении длины ключей и в совершенствовании алгоритмов, чтобы противодействовать взлому систем, использующих современные алгоритмы [9].

Алгоритм выработки ключей Диффи-Хеллмана

Еще одним примером может послужить алгоритм для выработки ключей Диффи-Хеллмана [7]. Подобно алгоритму RSA, он также использует простые числа для генерации ключа, что является его основной задачей [6].

Изначально обе стороны, которые зачастую называют «Алиса» и «Боб», договариваются о двух числах – простом числе p и первообразном корне g. Первообразный корень – это такое число, которое при возведении в степень от 1 до $\phi(p)$ по модулю даст все целые числа от единицы до данного модуля. Это необходимо для того, чтобы обеспечить криптографическую стойкость. Если число g не будет первообразным корнем, выборка ключей значительно снизится, что нарушит требования к безопасной генерации.

Обе стороны выбирают числа, которые будут являться закрытыми ключами. Алиса выбирает число a, а Боб выбирает число b. После этого Алиса вычисляет $g^a \bmod p$, откуда получает свой открытый ключ A. Этот ключ она передает Бобу. Он, в свою очередь, вычисляет $g^b \bmod p$ для того, чтобы получить свой открытый ключ B, который он отправляет Алисе. Затем обе стороны выполняют вычисление общего секретного ключа, выполняя возведение открытого ключа собеседника в степень своего закрытого ключа по модулю простого числа. Таким образом, собеседники делают действие $A^b \bmod p = B^a \bmod p = K$, где K – полученный ключ. В данном случае равенство выполняется из-за свойства степеней. Расписывая, получим следующие формулы:

$$A^b \bmod p = g^{ab} \quad (2)$$

$$B^a \bmod p = g^{ba} \quad (3)$$

$$g^{ab} \bmod p = g^{ba} \bmod p \quad (4)$$

Как можно видеть на этом примере, гарантия того, что число является простым, также является и гарантией того, что мы получим криптографически стойкий ключ при работе алгоритма.

В целях проверки чисел на простоту на практике используют математические алгоритмы, которые упрощают поиск таких чисел, однако не всегда имеют простую для понимания теоретическую основу.

В реальных системах используют два подхода: вероятностный и детерминированный.

Детерминированные способы поиска простых чисел

Детерминированный подход позволяет абсолютно точно утверждать, является ли число простым или составным. Такой способ обычно связан не с проверкой конкретных чисел, а с поиском методами полного перебора делителей числа. Рассмотрим два часто используемых варианта – наивный тест и решето Эратосфена.

Наивный тест является ничем иным, как полным перебором всех чисел до корня из проверяемого числа, то есть $i = 2, 3, \ldots, |\sqrt{(n)}|$, где i – числа, используемые в качестве делителей, n – проверяемое число. Данный тест является очень эффективным для небольших чисел. Он нецелесообразен для применения в криптографических системах из-за больших размерностей чисел, применяемых в них.

Метод решета Эратосфена, в отличие от наивного теста, позволяет найти все простые числа до заданного числа. Изначально выбирается число, являющееся границей для поиска простых, пусть это будет n. Затем, выбирая подряд $i = 2, 3, \ldots, n$, необходимо вычеркнуть все последующие числа, кратные выбранному, а выбранное записать в список простых. После этого необходимо перейти к следующему числу из списка. К примеру, выбрав двойку, мы запишем ее в список простых, и вычеркнем все прочие четные числа, так как они кратны ей. После этого будет выполнен переход к тройке. Данный метод позволяет найти множество простых чисел, но также, как и наивный тест, ввиду использования полного перебора, неэффективен в криптографических системах.

Вероятностные подходы в проверке чисел на простоту

В реальных криптографических системах используют вероятностные подходы. Они позволяют выполнить проверку на простоту для конкретного числа за малое количество шагов. Такие проверки хоть и будут весьма быстры, но не гарантируют простоту числа. Они позволяют с определенной вероятностью утверждать, что число является простым, или гарантированно выявить составной характер числа.

Среди наиболее распространенных тестов три: тест Ферма, тест Соловея-Штрассена и тест Миллера-Рабина [10]. Каждый из них дает свою точность в определении простоты числа.

Тест Ферма основан на малой теореме Ферма, которая вводит необходимое условие простоты числа. Данное условие звучит так. Если n – простое число, то оно удовлетворяет выражению $a^{n-1} \bmod n \equiv 1$, где a – произвольное число от 2 до $n - 2$.

Тест Соловея-Штрассена основан на тесте Ферма, расширенном свойствами символа Якоби. Данный тест, в отличие от теста Ферма, хоть и не повышает точность, однако способен распознать составной характер некоторых чисел, который не может выявить тест Ферма [10]. Такие числа называются числами Карлмайкла. Эти числа являются псевдопростыми и проходят тест Ферма, как простые, хотя являются составными. Тест Соловея-Штрассена решает эту проблему, корректно классифицируя подобные числа, как составные.

На практике же чаще применяется тест Миллера-Рабина [10]. Данный тест основан на тесте Миллера, и, как и предыдущие, использует свойства, позволяющие определить простоту числа. Вероятность ошибки данного теста ниже, что позволяет добиться большей точности при меньшем числе итераций. Для того, чтобы легче понять принцип работы данного теста, было принято решение о построении ИМ. Она позволит легче усвоить материал и разобраться в том, как работает наиболее популярный на данный момент тест простоты.

Описание моделируемой системы

Тест Миллера-Рабина - вероятностный алгоритм проверки числа на простоту, широко используемый в криптографии благодаря простоте реализации и высокой производительности [11]. Он оценивает вероятность простоты числа, зависящую от числа итераций, что требует выбора рационального их количества для баланса между точностью и вычислительными затратами.

На вход тест получает само тестируемое число и количество итераций, которые необходимо провести в целях исследования – является ли число вероятно простым или составным. На выходе тест дает ответ о характере данного числа. Схема алгоритма ИМ теста Миллера-Рабина показана на рисунке 1.

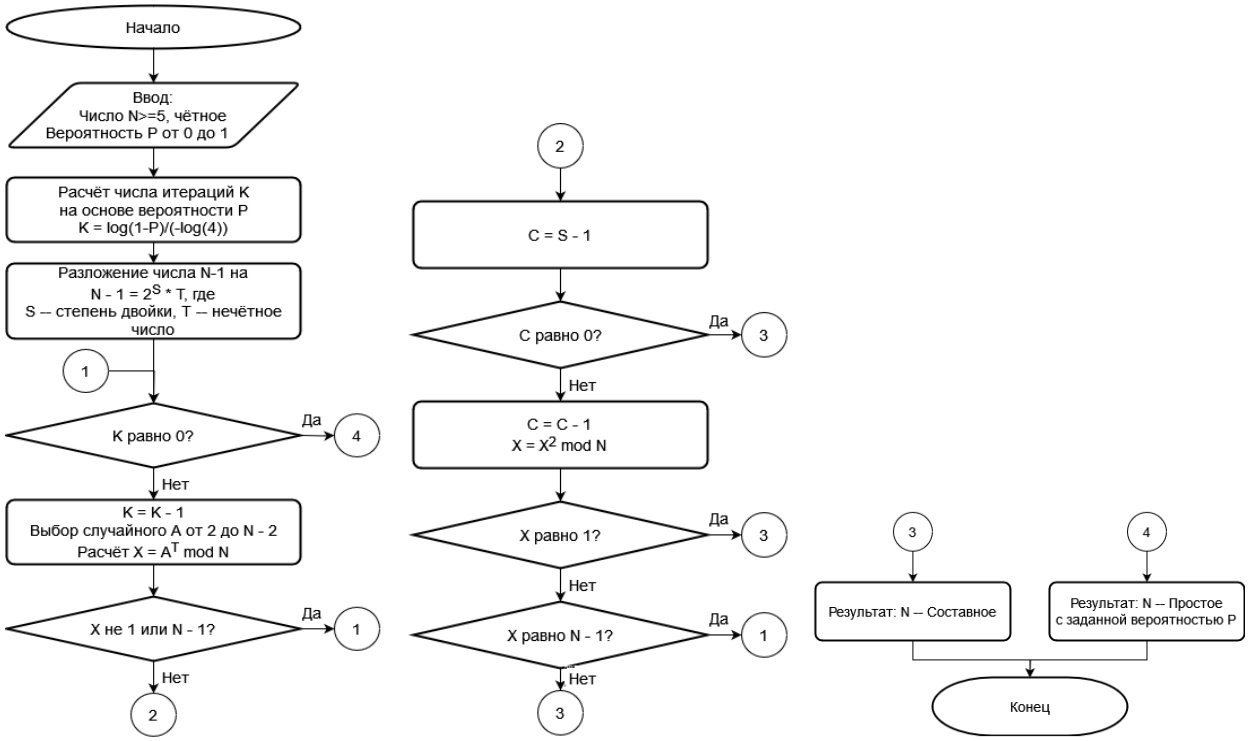

Рис. 1. Схема алгоритма ИМ теста Миллера-Рабина

Имитационная модель реализует измененный алгоритм Миллера-Рабина, который позволяет понять, как выполняется проверка на простоту и как можно дополнить алгоритм, оптимизируя выбор числа итераций.

С целью повышения удобства взаимодействия проведем комплексный анализ зависимости итоговой вероятности простоты числа от количества итераций теста Миллера-Рабина. Рассмотрим как теоретические аспекты метода, включая вывод вероятностных оценок, так и практическую реализацию ИМ. Обратим внимание на тонкости реализации, включая выбор случайных оснований с целью оптимизации вычислений для большеразмерных чисел.

На основе анализа предложим практические рекомендации по выбору числа итераций для различных уровней точности. Результаты проверим экспериментальными данными, которые продемонстрируют влияние числа итераций на частоту ошибок при проверке чисел разной длины.

Расчет рационального числа итераций

В реальных системах следует учитывать точность, которая будет соответствовать точности системы и не будет избыточной. Иными словами, необходимо найти баланс между количеством итераций и точностью, чтобы обеспечить необходимое быстродействие и потребление ресурсов ЭВМ. Так, с ростом числа итераций кратно возрастает точность, однако при этом требуется больше времени и ресурсов на проверку.

Вероятность ошибки при проведении теста Миллера-Рабина для одной итерации со случайно заданным числом составляет 0,25 = 1/4. Вывод зависимости числа итераций от желаемой вероятности точности проведем математически с помощью свойства логарифмов. Сперва формализуем формулу для возможной простоты числа:

$$1 - (¼)^k \geq \varepsilon \tag{5}$$

где $1 - (¼)^k$ — вероятность того, что число является возможно простым, полученная, как разность единицы и $(¼)^k$, а ε – точность, которую мы хотим получить после работы алгоритма. Выполним необходимые переносы:

$$(¼)^k \le 1 - \varepsilon \tag{6}$$

Выполним логарифмирование обоих частей неравенства:

$$\log((¼)^k) \le \log(1 - \varepsilon) \tag{7}$$

Используя правило вынесения степени из логарифма, получим:

$$k * \log(¼) \le \log(1 - \varepsilon) \tag{8}$$

Разложим дробь под логарифмом, используя свойство $\log(a/b) = \log(a) - \log(b)$. Отсюда выйдет следующая формула:

$$k * (\log(1) - \log(4)) \le \log(1 - \varepsilon) \tag{9}$$

Так как $\log(1) = 0$, получим

$$k * (-\log(4)) \le \log(1 - \varepsilon) \tag{10}$$

Выполнив деление, получим итоговую формулу:

$$k \ge \log(1 - \varepsilon)/(-\log(4)) \tag{11}$$

Для полученной формулы произведем несколько расчетов, чтобы наблюдать общую закономерность в росте числа итераций. Примем в качестве значения $\log(4) = 0.60206$, что будет достаточным для удовлетворения нашей потребности в точности и выполним следующие расчеты, при:

$\varepsilon = 0{,}9;\ \frac{\log(1-0{,}9)}{-\log(4)} \approx \frac{-1}{-0{,}60206} \approx 1{,}66 \rightarrow k \ge 2;$

$\varepsilon = 0{,}99;\ \frac{\log(1-0{,}99)}{-\log(4)} \approx \frac{-2}{-0{,}60206} \approx 3{,}32 \rightarrow k \ge 4;$

$\varepsilon = 0{,}999;\ \frac{\log(1-0{,}999)}{-\log(4)} \approx \frac{-3}{-0{,}60206} \approx 4{,}98 \rightarrow k \ge 5;$

$\varepsilon = 0{,}9999;\ \frac{\log(1-0{,}9999)}{-\log(4)} \approx \frac{-4}{-0{,}60206} \approx 6{,}64 \rightarrow k \ge 7;$

$\varepsilon = 0{,}999999;\ \frac{\log(1-0{,}999999)}{-\log(4)} \approx \frac{-6}{-0{,}60206} \approx 9{,}96 \rightarrow k \ge 10$.

Взаимосвязь числа итераций с заданной вероятность уверенности в простоте числа показана в таблице 1.

Таблица 1

Зависимость вероятности простоты числа от числа итераций алгоритма

Требуемая точность простоты	Число итераций
0,9	2
0,99	4
0,999	5
0,9999	7
0,99999	10

Анализ способа выбора основания

Выполним анализ способов выбора числа a, которое используется для проверки внутри алгоритма Миллера-Рабина. Рассмотрим способы выбора путем псевдослучайной генерации, прямого и обратного перебора.

Вариант случайного распределения дает хорошие результаты. В его рамках перебирается множество оснований случайным образом. С ростом числа итераций возрастает уверенность в том, что проверяемое число действительно простое, так как распределение оснований становится равномерным.

Последовательный выбор с начала диапазона имеет свои особенности. Для многих чисел этот метод окажется быстрее, так как перебирает небольшие основания, которые чаще являются делителями больших чисел. При использовании данного метода существует риск того, что числа в начале диапазона будут ложными свидетелями простоты, то есть, при условии составного характера числа будет выполняться условие теоремы Ферма $a^{n-1} \bmod n = 1$, хотя оно должно выполняться только для простых чисел.

Последовательный выбор с конца диапазона имеет ту же проблему, что и метод выбора с начала диапазона.

Таким образом, выбор числа псевдослучайным способом дает хорошие основания полагать, что тест Миллера-Рабина будет пройден корректно, тогда как выбор числа по закономерности может быть быстрее, но дает меньшую уверенность в полученном результате.

Оценка ГПСЧ в C#

В языке программирования C# по умолчанию имеется несколько генераторов псевдослучайных чисел (ГПСЧ). Один из них является линейным конгруэнтным генератором, который выдает последовательность данных на основе генераторных параметров. Данный метод является быстрым, но не криптографически стойким для генерации псевдослучайных чисел.

В языке также имеется библиотека для криптографической генерации псевдослучайных чисел, однако для целей генерации оснований для проверки простоты нет необходимости использовать криптографически стойкий генератор. В сравнении с базовым генератором он работает медленнее, и в данной ситуации лишь замедлит быстродействие ИМ, которая должна наглядно демонстрировать работу теста.

Имитационное моделирование

Для создания ИМ будем использовать язык программирования C#. Он позволит быстро выполнить необходимые для алгоритма расчеты, обеспечит быструю скорость исполнения программы и позволит использовать удобную графическую разработку интерфейса.

Будущее оформление программы будет выполнено в табличной форме, каждая из которых будет отвечать за набор параметров. В ходе исполнения программы некоторые из полей будут подсвечиваться определенным цветом, что позволит проследить ход алгоритма. Описание действий будет производиться в правой части окна ИМ, что также будет способствовать пониманию работы теста Миллера-Рабина.

Общий вид интерфейса ИМ отображен на рисунке 2.

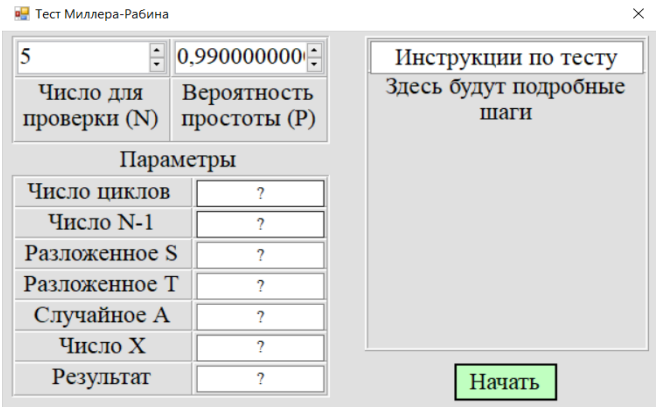

Рис. 2. Интерфейс ИМ теста Миллера-Рабина

Такая реализация ИМ позволяет выполнять тест Миллера-Рабина в интерактивном режиме по шагам. Первостепенно в поля ИМ заносятся данные о числе, которое требуется проверить, и требуемое значение вероятности уверенности в простоте числа, которая требуется для нашей задачи.

После того, как будет введено число и вероятность, ИМ выполнит первый шаг, и поля интерфейса обновятся. Пример состояния окна ИМ после первого шага для числа 17 с заданной вероятностью 0,99 показан на рисунке 3.

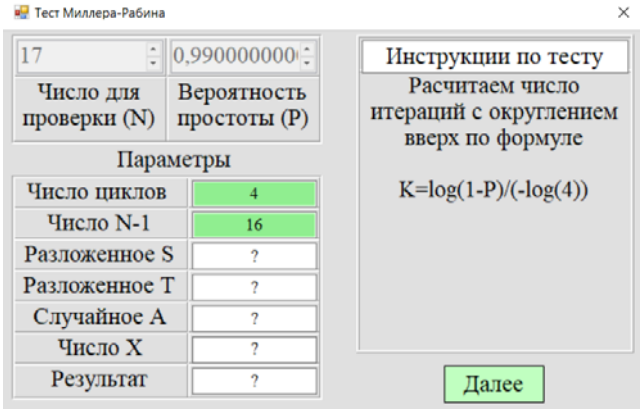

Рис. 3. Первый шаг выполнения ИМ

На перовом шаге будут рассчитаны базовые параметры, которые необходимы для дальнейшей работы. На этом этапе вычисляется необходимое число итераций по формуле (11). Путем нажатий на кнопку «Далее» будет выполняться последовательное разложение числа на степень двойки и нечетное число. По итогу будут сформированы коэффициенты, необходимые для работы алгоритма. Обновленные после разложения параметры приведены на рисунке 4.

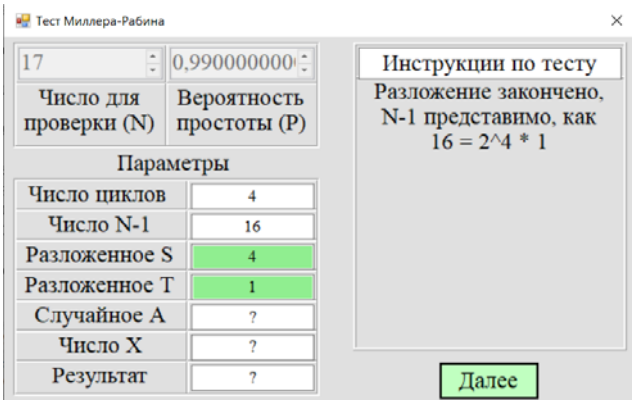

Рис. 4. Параметры ИМ после разложения

Когда разложение завершено, ИМ начнет выполнение итераций алгоритма, что представлено на рисунке 5.

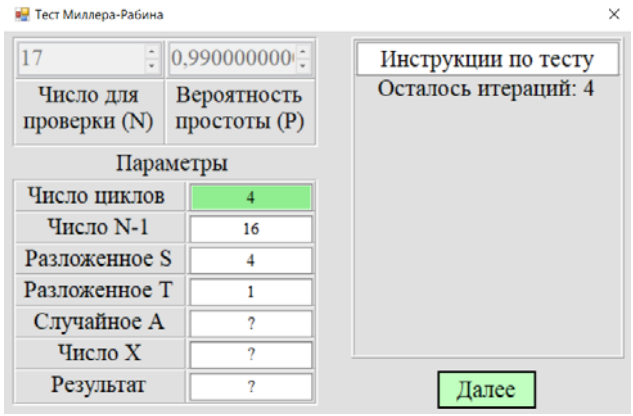

Рис. 5. Начало выполнения итераций

После того, как будет нажата кнопка «Далее», начнется проверка условий теста Миллера-Рабина. Каждый шаг будет отображаться в правой части окна. Также на данном этапе, если необходимо, будет произведен расчет параметров X для внутренних циклов.

На рисунке 6 показан выбор случайного числа для текущей итерации *K*.

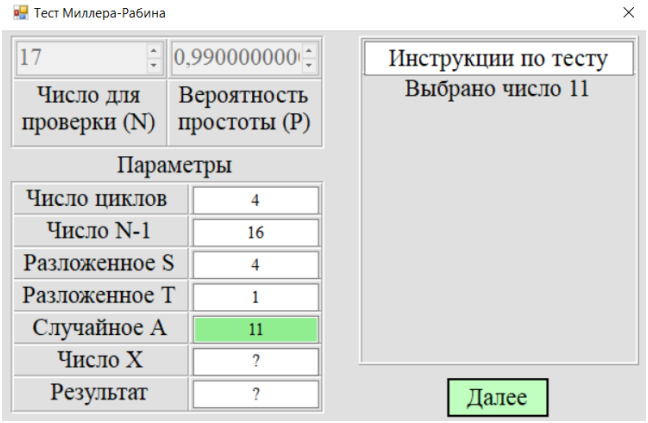

Рис. 6. Выбор случайного числа

Выполнив все итерации для заданного числа, получим результат, который будет отражен в текстовом поле справа и в нижней ячейке параметров, после чего можно завершить работу ИМ (рис. 7).

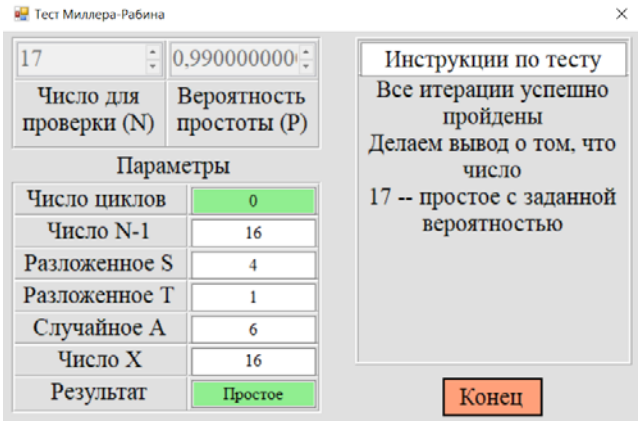

Рис. 7. Итоги работы ИМ

Заключение

В данной статье проанализированы методы проверки чисел на простоту, выявлена важность достоверной генерации простых чисел. Рассмотрены достоинства и недостатки этих методов, области их применения на практике. Проведен анализ результатов в зависимости от метода выбора основания для тестирования числа на простоту алгоритмом Миллера-Рабина. Создана имитационная модель, позволяющая произвести легкое изучение данного теста, понять порядок и этапность производимых шагов на наглядном примере. Выполнен анализ для расчета необходимой точности в различных задачах.

Литература

1. *Михалевич И.Ф., Абызов А.А., Архипов А.М., Басюк С.А*. и др. Имитационная модель SP-сети // REDS: Телекоммуникационные устройства и системы. 2023. № 2. С. 4-12.

2. *Омассон Ж.-Ф*. О криптографии всерьез. Практическое введение в современное шифрование / пер. с англ. А. А. Слинкина. М.: ДМК Пресс, 2021. 328 с.

3. *Фергюсон Н., Шнайер Б*. Практическая криптография. 1-е изд. М.: Диалектика, 2005. 421 с.

4. *David Wong*. Real-World Cryptography. 1-е изд. Manning Publications, 2021. 400 с.

5. *Keith Martin*. Everyday Cryptography. Fundamental Principles and Applications. 2-е изд. Oxford University Press, 2017. 720 с.

6. *Шнайер Б*. Прикладная криптография: протоколы, алгоритмы, и исходный код на С. 2-е юбил. изд.: Пер. с англ. СПб.: ООО “Диалектика”, 2022. 1040 с.

7. *Diffie W., Hellman M.E*. New Directions in Cryptography (англ.) // IEEE Transactions on Information Theory / F. Kschischang. IEEE, 1976. Том 22, 6-е изд. С. 644-654.

8. *Rivest R., Shamir A., Adleman L*. A method for obtaining digital signatures and public-key cryptosystems (англ.) // Communications of the ACM – New York City: Association for Computing Machinery, 1978. Том 21, 2-е изд. С. 120-126.

9. *Джуракулов Т.Х., Евстропов В.А., Петросян А.А., Михалевич И.Ф.* Использование квантовых компьютеров при атаке на RSA // Молодой ученый. 2023. № 23 (470). С. 111-113. URL: https://moluch.ru/archive/470/103926/ (дата обращения: 06.01.2025).

10. *Нестеренко Ю.В*. Глава 4.4. Как отличить составное число от простого // Введение в криптографию / Под ред. В.В. Ященко. Питер, 2001. 288 с.

11. *Алферов А.П., Зубов А.Ю., Кузьмин А.С., Черемушкин А.В*. Основы криптографии: учебное пособие для вузов. М.: Гелиос-АРВ, 2001. 478 с.