НАУЧНЫЕ ИССЛЕДОВАНИЯ И РАЗРАБОТКИ 2019 ГОДА

Материалы международного
научно-исследовательского конкурса

(28 декабря 2019)

УДК 004.02:004.5:004.9
ББК 73+65.9+60.5
К64

Н34 НАУЧНЫЕ ИССЛЕДОВАНИЯ И РАЗРАБОТКИ 2019 ГОДА: материалы международного научно-исследовательского конкурса (28 декабря 2019г., Саратов) Отв. ред. Зарайский А.А. – Издательство ЦПМ «Академия Бизнеса», Саратов 2019. - 176с.

978-5-907199-56-9

Сборник содержит научные статьи и тезисы ученых Российской Федерации и других стран. Излагается теория, методология и практика научных исследований в области информационных технологий, экономики, образования, социологии.

Для специалистов в сфере управления, научных работников, преподавателей, аспирантов, студентов вузов и всех лиц, интересующихся рассматриваемыми проблемами.

Материалы сборника размещаются в научной электронной библиотеке с постатейной разметкой на основании договора № 1412-11/2013К от 14.11.2013.

ISBN 978-5-907199-56-9

УДК 004.02:004.5:004.9
ББК 73+65.9+60.5

УДК 004.3/.8

Четвертков Е.В.
студент 2 курса
Терехов Д.А.
студент 2 курса
Меленюк А.В.
студент 2 курса
Институт информационных технологий
и автоматизации систем
кафедра Прикладных информационных технологий и программирования
ФГБОУ ВО «СибГИУ»
научный руководитель: Моисеенко Т.Г.
доцент
Россия, г. Новокузнецк

РАЗВИТИЕ НЕКОТОРЫХ НАПРАВЛЕНИЙ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ В СОВРЕМЕННОМ ИНФОРМАЦИОННОМ ОБЩЕСТВЕ

Аннотация:

В статье рассматриваются некоторые направления информационных технологий в современном информационном обществе такие как криптография, нейронные сети и теория языков программирования. Криптография имеет большое значение во многих сферах жизни современного информационного общества, где необходима защита той или иной информации. В то время как нейронные сети помогают людям обрабатывать большие объемы данных и находить сложные решения для широкого спектра проблем. Также без языков программирования нельзя представить себе современные информационные технологии — это инструмент, который улучшается и модифицируется под нужды времени.

Ключевые слова: информационные технологии, криптография, нейронные сети, языки программирования, динамический хаос, парадигма программирования.

Chetvertkov E.V.
Student
2 course, Institute of information technology and systems automation
Department of applied information technologies and programming
Federal state budgetary educational institution of higher education
«SibSIU»
Russia, Novokuznetsk
Terekhov D.A.
Student
2 course, Institute of information technology and systems automation

Department of applied information technologies and programming
Federal state budgetary educational institution of higher education
«SibSIU»
Russia, Novokuznetsk Melenyuk A.V.
Student
2 course, Institute of information technology and systems automation
Department of applied information technologies and programming
Federal state budgetary educational institution of higher education
«SibSIU»
Russia, Novokuznetsk Scientific adviser: Moiseenko T.G.
Docent

DEVELOPMENT OF SOME DIRECTIONS OF INFORMATION TECHNOLOGIES IN THE MODERN INFORMATION SOCIETY

Abstract:

The article discusses some areas of information technology in the modern information society such as cryptography, neural networks and the theory of programming languages. Cryptography is of great importance in many areas of modern information society, where it is necessary to protect this or that information. While neural networks help people process large amounts of data and find complex solutions to a wide range of problems. Also, without programming languages, it is impossible to imagine modern information technology — a tool that is improved and modified to meet the needs of time.

Keywords: informational technologies, cryptography, neural networks, programming languages, dynamic chaos, programming paradigm.

Развитие информационных технологий — непрерывный процесс. Практически каждый год появляются новые или усовершенствуются старые области и направления информационных технологий.

По всему миру ведутся разработки в обширной области информационных технологий. Разрабатываются новые методы защиты информации, всевозможные алгоритмы, нейронные сети, создаются и улучшаются языки программирования и т.д.

В представленной статье отмечаются направления развития в криптографии, нейронных сетях и теории языков программирования.

Защита данных — задача, важность которой сложно переоценить. В современном же информационном обществе защита данных попросту необходима. Ведь владение информацией в современном информационном обществе может являться, пожалуй, решающим фактором и залогом успеха во множестве предприятий.

Стоит, кроме того, отметить, что в настоящее время криптография является, возможно, единственным инструментом для обеспечения достоверности, конфиденциальности и целостности передаваемой информации [1].

Итак, в современном информационном обществе особо остро стоит

вопрос защиты данных. Большинство традиционных криптографических методов на данный момент потеряли актуальность, так как существуют подходы, способные эффективно противостоять этим методам [2].

И потому в этом контексте важным и жизненно необходимым является разработка все новых и новых методов шифрования или улучшение уже существующих.

Развитие технологий и повсеместное распространение сети Интернет позволило передавать с большой скоростью не только текстовые файлы, но и мультимедиа-файлы.

В частности, одной из важнейших проблем современной криптографии является защита медиа-файлов. Большинство существующих алгоритмов шифрования разработаны в основном для защиты информации, представленной в виде текста. Потому они не дают удовлетворительных результатов при работе с изображениями и звуковыми файлами.

Наряду с этим все большую популярность приобретает криптография с использованием систем динамического хаоса [3]. Главное преимущество систем, основанных на хаосе, состоит в том, что выходные данные таких систем никогда не повторяются, и ни один внешний источник не может располагать информацией для расшифровки закодированных с помощью хаотической системы информации.

На деле же, хаотическая система передает необходимые для шифрования изображения данные в специальную подчиненную систему, таким образом, только владелец подчиненной системы может дешифровать изображение для желаемой цели.

При создании новых криптографических методов важно учитывать их практическую применимость. Для количественной оценки качества и надежности методов шифрования существует целый ряд критериев.

Основное качество любой криптосистемы — надежность, ее устойчивость к различным атакам. В настоящее время на практике применяются линейные и дифференциальные атаки, кроме того, распространены атаки с использованием «грубой силы».

Атака грубой силой в общем случае нейтрализуется благодаря большому пространству возможных ключей. Хаотические системы с заметной легкостью способны обеспечить генерацию пространства ключей, способного справится с атакой грубой силой.

Немаловажным количественным критерием устойчивости криптографического метода является лавинный критерий и строгий лавинный критерий. Эти критерии показывают, насколько алгоритм шифрования чувствителен к открытому тексту, и являются количественной оценкой лавинного эффекта — значительного изменения битов зашифрованной информации при незначительном изменении битов открытого текста [1].

Лавинный критерий требует изменения в среднем половины битов зашифрованного файла при изменении каждого отдельно взятого бита

исходного файла. В то время как строгий лавинный критерий требует изменения каждого отдельно взятого бита выходного значения с вероятностью одна вторая при изменении каждого отдельного бита входного значения.

Еще одним важным критерием надежности криптографического метода является информационная энтропия — количественная мера неопределенности. Для зашифрованной информации данный критерий доложен иметь максимально возможное значение, это в определенной степени затрудняет расшифровку [2].

Кроме того, существуют определенные специфические критерии надежности методов шифрования. Так в криптографии изображений существуют свои уникальные критерии оценки надежности алгоритма шифрования, например: процент пикселей, изменивших значение (Number of Pixels Change Rate (NPCR)) и среднее изменение интенсивности (Unified Average Changing Intensity (UACI)) [1].

Для криптографического метода важно, однако не только его стойкость. Так самым важным показателем практического применения алгоритма шифрования является его быстродействие. Алгоритм шифрования, обеспечивающий сверхнадежную защиту от взлома, но шифрующий информацию критически медленно не получит широкого применения.

При прохождении по реальным каналам связи закодированный файл может подвергнуться воздействию многих видов шумов. Поэтому чтобы метод шифрования была применима на практике, алгоритм дешифрования должен быть устойчив к шумам и выдавать максимально близкий к открытому тексту результат.

Для оценки криптосистемы к шумам существуют определенные критерии: пиковое отношение сигнал/шум (PSNR) — количественная оценка качества декодированного файла после воздействия на него шума и MSE — это среднеквадратичная ошибка между исходной и восстановленной информацией [2].

Итак, создание криптографических систем, которые удовлетворяют указанным критериям и при том способных эффективно работать с информацией, представленной как в текстовом формате, так и в одном из медиа форматов является необходимой задачей не только криптографии, но и в целом важным направлением информационных технологий.

Огромную роль в современном информационном обществе играют нейронные сети. Они нашли свое применение в работе с большими данными. Нейронные сети облегчают работу медикам, аналитикам, лингвистам и многим другим.

Основными областями применения нейронных сетей на данный момент являются автоматизация процессов классификации, автоматизация прогнозирования, автоматизация процессов распознавания, автоматизация процессов принятия решений; управление различного рода информацией.

Нейронные сети активно развиваются и проникают во все области жизни современного общества [4].

Одной из задач, для решения которой применяются нейронные сети, является определение лингвистической сложности текста и дальнейшее его упрощение.

Так нейронные сети, упрощающие текст [5], помогают ряду групп: тем, кто имеет языковые ограничения, тем, кто имеет низкий уровень образования, людям, страдающим заболеваниями, ограничивающими языковые функции и т.д.

Нейронные сети активно используются в других направлениях информационных технологий, в частности, нейронные сети служат основой при разработке компьютерного зрения, искусственного интеллекта и т.д.

Например, нейронные сети используются для создания систем автоматического управления транспортными средствами, такими как автомобили. Особо стоит отметить, что нейронные сети могут применятся при кодировании и декодировании информации, то есть в криптографии.

Здравоохранение является одним из основных направлений, которое может позволить выйти на эффективный уровень развития искусственного интеллекта на базе нейронных сетей. Так нейронные сети применяются в США, Южной Корее, Монголии и других странах для назначения лечения некоторым группам пациентов [6].

Нейронные сети стали практически неотъемлемой частью экономики, маркетинга и аналитики. Нейронные сети применяются при исследовании спроса, потребностей рынка, нейронные сети участвуют в ценообразовании и управлении производством.

Перечень применения нейронных сетей в современном информационном обществе можно продолжать бесконечно долго.

Практическую пользу применения нейронных сетей сложно переоценить. Современное информационное общество уже невозможно представить без искусственного интеллекта в общем и нейронных сетей, в частности. Это направление является перспективным и в будущем будет развиваться и проникать во все новые области нашей жизни.

Пожалуй, самым важным элементом информационных технологий являются языки программирования. Это в первую очередь мощный инструмент, без которого уже невозможно представить работу в каждой из отраслей информационных технологий.

Как и любой инструмент, языки программирования развиваются и улучшаются. С момента своего появления языки программирования прошли долгий путь: от громоздких машинных кодов до современных языков программирования с легким синтаксисом.

С развитием языков программирования связано еще и развитие парадигм программирования: машинно-ориентированная, процедурная, объектно-ориентированная, логическая и функциональная [7].

Языки программирования традиционно рассматриваются как

принадлежащие к конкретным парадигмам, однако понятия парадигм и ориентации программирования являются неточными [8].

При развитии языков программирования выработалась устойчивая модель, которой в той или иной степени придерживаются все современные языки программирования независимо от парадигмы.

Во-первых, в подавляющем числе языков программирования присутствует система типов. Системы типов служат трем связанным целям в языках программирования: классифицировать значения, определять их применимые операции и сообщать компилятору, сколько памяти выделить для хранения значения данного типа. На первый взгляд, тип — это ограничение, которое определяет набор допустимых значений, которые ему соответствуют. Также типы являются абстрактными спецификациями функциональности, которые определяют законные контексты использования для значений, которые они описывают.

Попытка выполнить недопустимую операцию со значением известна как ошибка типа, которая может быть обнаружена либо во время компиляции, либо во время выполнения. В языке без типов «должно быть так, что каждое значение может использоваться в любом контексте».

Во-вторых, важной особенностью многих языков программирования является «возможность ассоциирования значений с символами для последующего их получения». Эта категория объектов связана с символьно-ценностными ассоциациями, которые после создания не могут быть изменены, например, константы.

Кроме того, в последнее время популярность приобретает явный параллелизм, то есть ряд действий, которые могут чередоваться в любом порядке или выполняться параллельно, как это определено базовой платформой в соответствии с количеством доступных ядер центрального процессора.

Хотя декларативные программы часто могут распараллеливаться автоматически компилятором или интерпретатором, многие языки также определяют функции для явной поддержки одновременного выполнения программ, которые зависят от изменчивого состояния или императивного управления. Взаимодействие между явно параллельными действиями может поддерживаться в нескольких различных стилях связи.

В контексте объектно-ориентированной парадигмы важна модульность, декларативность. Особенности модульности позволяют разделить систему на «согласованные части, которые можно разрабатывать и обслуживать отдельно», а затем, при необходимости, повторно использовать как внутри компании, так и за ее пределами, для получения выгоды.

Декларативность в программирование по своей сути является разделением логики и контроля. Программист создает логический компонент, состоящий из декларативных выражений, которые «определяют, каким должен быть результат алгоритма». Компонент управления частично или полностью предоставляется компилятором или интерпретатором.

Итак, на данный момент языки программирования по сути своей стагнируют, они имеют устоявшуюся рабочую структуру. Сегодня языки программирования не предлагают ничего кардинально нового, а лишь улучшают что-то уже существующие, что называется, добавляют «синтаксический сахар».

Информационные технологии важная часть современного информационного общества. Помимо криптографии, нейронных сетей и языков программирования существует множество перспективных и важных направлений развития информационных технологий. В данной статье рассмотрена лишь малая часть из них.

Использованные источники:

1. Сидоренко А. В., Жуковец Д. А. Элементы дифференциального и линейного криптоанализа алгоритма шифрования с использованием динамического хаоса // Системный анализ и прикладная информатика. - 2015. - №3. - С. 48-54.
2. A new algorithm for the colored image encryption via the modified Chua's circuit // ScienceDirect URL: https://doi.org/10.1016/j.jestch.2019.09.001 (дата обращения: 20.10.2019).
3. Сидоренко, А. В., Жуковец, Д. А. Блочный алгоритм шифрования на основе динамического хаоса // Вестник БГУ. Серия 1, Физика. Математика. Информатика. - 2015. - №3. - С. 34-39.
4. Тихонов Алексей Анатольевич Большие данные и глубокое машинное обучение в искусственных нейронных сетях // Наука и образование сегодня. 2018. №6 (29). URL: https://cyberleninka.ru/article/n/bolshie-dannye-i- glubokoe-mashinnoe-obuchenie-v-iskusstvennyh-neyronnyh-setyah (дата обращения: 26.12.2019).
5. Evaluation of Text Complexity in Italian Language: a Representation Point of View // ScienceDirect URL: https://doi.org/10.1016/j.procs.2018.11.108 (дата обращения: 20.10.2019).
6. Гусев А.В. Перспективы нейронных сетей и глубокого машинного обучения в создании решений для здравоохранения // Врач и информационные технологии. 2017. №3. URL: https://cyberleninka.ru/article/n/perspektivy-neyronnyh-setey-i-glubokogo-mashinnogo-obucheniya-v-sozdanii-resheniy-dlya-zdravoohraneniya (дата обращения: 26.12.2019).
7. Голицина О.Л., Попов И.И. Программирование на языках высокого уровня: учебное пособие. – М.: ФОРУМ, 2010.
8. Howell J., Goetz B., John N., Andrew B., Rem C. A feature model of actor, agent, functional, object, and procedural programming languages // Science of Computer Programming. - 2015. - №98 part 2. - С. 120-139.

Научное издание

НАУЧНЫЕ ИССЛЕДОВАНИЯ И РАЗРАБОТКИ 2019 ГОДА

Материалы международного
научно-исследовательского конкурса
28 декабря 2019

Статьи публикуются в авторской редакции
Ответственный редактор Зарайский А.А.
Компьютерная верстка Чернышова О.А.