ISSN 2686-9373

ВЕСТНИК СОВРЕМЕННЫХ ЦИФРОВЫХ ТЕХНОЛОГИЙ

22. 2025 (МАРТ)

Издание включено в перечень ВАК (специальности: 2.3.2, 2.3.6, 2.3.8, 5.2.4)

ВЕСТНИК

СОВРЕМЕННЫХ ЦИФРОВЫХ ТЕХНОЛОГИЙ

НАУЧНО-ПРАКТИЧЕСКИЙ ЖУРНАЛ

№22
МАРТ 2025

www.c3da.org

ISSN 2686-9373

Издатели: *Российский государственный социальный университет*
Ассоциация РКЦФА

Адрес редакции и издателя: 129226, Москва,
ул. Вильгельма Пика, д.4, стр.1
www.c3da.org

РГСУ

Подписано в печать 28.03.2025 г.
Тираж 500 экз.
Подписной индекс в каталоге «Пресса России»: 79111

Свидетельство о регистрации СМИ
ПИ № ФС 77-76187 от 08.07.2019 г.

Журнал включен в перечень рецензируемых научных изданий ВАК, в которых должны быть опубликованы основные результаты диссертаций на соискание ученой степени кандидата наук, на соискание ученой степени доктора наук.
(2.3.2) Вычислительные системы и их элементы
(2.3.6) Методы и системы защиты информации, информационная безопасность
(2.3.8) Информатика и информационные процессы
(5.2.4) Финансы

РЕДАКЦИОННЫЙ СОВЕТ

РЕДАКЦИОННОЕ ПРИМЕЧАНИЕ

Материалы двадцать второго выпуска нашего журнала охватывают как фундаментальные вопросы, касающиеся возможных путей развития цифровых технологий, так и актуальные практические аспекты обеспечения их надежности и применения в качестве инструментов в процессах создания новых и совершенствования существующих цифровых технологий.

Выпуск открывается статьей **«Тринарный процессор как уникальная технология будущего»** Владимира Васильева, в которой описаны принципы работы и архитектура тринарного процессора с уникальными характеристиками, основанного на троичной системе счисления. Развитие этого направления исследований весьма важно для внедрения тринарной логики, разработки систем искусственного интеллекта и искусственного сознания, а также высоконадёжных цифровых вычислителей. Работа может быть полезна и педагогам, занимающимся современной дидактикой высшего образования для дисциплин "прикладная математика", "теоретическая информатика" и "защита информации".

В статье **«Работа двух взаимозаменяемых антивирусных программ с учетом скорости размножения вирусных программ»** коллектива авторов предложен достаточно очевидный механизм поочередного использования двух антивирусных программ для повышения эффективности и отказоустойчивости системы в рамках системы защиты предприятия от компьютерных вирусов. Однако оригинальность работы состоит в теоретико-вероятностном анализе эффективности такой системы при сбоях одной из антивирусных программ и переходе на резервную: анализируется вероятность сбоя антивирусных программ и время восстановления их работы.

Актуальной проблеме использования цифровых сервисов виртуальной реальности для управления сознанием человека посвящена статья Павла Былевского **«Угрозы манипулирования сознанием посредством цифровой виртуальной реальности»**. В качестве одного из основных факторов влияния на развитие проблемы определяется парадигма механистического идеализма, особенности которой автор детально описывает в статье. Отмечается, что развитие цифровых сервисов, основанное на примитивах массовой культуры, и критическое снижение культурного уровня пользователей могут создать условия для замещения реального мира виртуальным. В связи с этим отечественные разработки виртуальной реальности, по мнению автора, должны быть нацелены на социально-культурное развитие общества.

В статье **«О принципиальных проблемах проверки электронной подписи и подтверждения прав»** Андрея Щербакова рассматриваются актуальные вопросы подтверждения неизменности и авторства документов, в частности, принципиальные проблемы ограниченного срока действия сертификата электронной подписи, а также возможный способ их решения. Предлагается алгоритм с использованием удостоверяющей подписи внешнего доверенного сервиса, содержащей метку времени. Другой алгоритм позволяет сформировать цифровые права длительного хранения на некоторый массив информации без применения механизмов электронной подписи.

В статье Сергея Мирзояна **«Применение технологий искусственного интеллекта для повышения качества генераторов псевдослучайных чисел»** изучаются вопросы применения систем искусственного интеллекта для совершенствования и модификации генераторов псевдослучайных чисел. Анализируются особенности традиционных методов анализа, возможности инструментов искусственного интеллекта для улучшения качества случайности, а также проблемы, связанные с их применением: сложность реализации, высокие требования к данным, уязвимости к атакам и этические вопросы. Данные проблемы требуют проведения дополнительных исследований перед внедрением ИИ-моделей в критически важные системы. Статья поднимает важную проблему применения механизмов ИИ для криптографического анализа различных криптографических алгоритмов и протоколов. Призываем автора развивать эту тему в следующих статьях и дискуссиях.

Статья **«Анализ надежности распределенных информационных систем в условиях воздействия внешних угроз: комплексный обзор литературы»** молодого зарубежного ученого Алмали Аайя Аднан Латиф посвящена интересным вопросам оценки надежности, оптимизации и информационной безопасности распределенных информационных систем с позиции противодействия современным внешним угрозам. В ней описываются особенности применения для повышения отказоустойчивости и производительности систем методов нечеткой логики, моделирования Монте-Карло, аппарата цепей Маркова, генетических алгоритмов и моделей на основе искусственного интеллекта. Список реферированной литературы приводится в авторской редакции.

В статье **«Сравнительный анализ инструментов для автоматизированного тестирования мобильного программного обеспечения»** Алексея Маринина представлен анализ современных методов автоматизированного тестирования мобильных приложений с целью выявления основных проблем, решаемых инженерами по тестированию. Публикация позволяет указать на особенности процедуры мобильной кроссплатформенной разработки и провести их анализ, основываясь на передовых направлениях развития мобильных операционных систем. Автор подчеркивает, что для создания качественных приложений при выборе инструментов и методов тестирования необходимо учесть определенные проблемы и сложности, описанные в статье.

СОДЕРЖАНИЕ

УДК: 512, 004.3

Тринарный процессор как уникальная технология будущего

V.I. Vasiliev

Trinary Processor as a Unique Technology of the Future

Abstract. *The article describes the operating principles and architecture of a trinary processor with unique characteristics based on the ternary number system. The theoretical foundations and approaches to the synthesis of practical computing systems that provide continuous hardware control of the data flow are considered. The creation of processors based on the ternary number system is important for the development of computing systems in general, the introduction of trinary logic in artificial intelligence and artificial consciousness systems, for highly reliable digital computers. The results of the presented study can be used in modern didactics of higher education for the disciplines of "applied mathematics", "theoretical computer science" and "information security".*

Keywords: *ternary number system, ternary mirror-symmetric number system, ternary logic, ternary optical computer, highly reliable arithmetic ternary computer, Fibonacci code processor, ternary computing machine "Setun".*

В.И. Васильев
Ведущий инженер-программист встраиваемых микроконтрольных систем.
E-Mail: askfind@ya.ru

Аннотация. *Статья посвящена описанию принципов работы и архитектуры тринарного процессора с уникальными характеристиками, основанного на троичной системе счисления. Рассмотрены теоретические основы и подходы к синтезу практических вычислительных систем, которые обеспечивают непрерывный аппаратный контроль потока данных. Создание процессоров на основе троичной системы счисления важно для развития вычислительных систем в целом, внедрения тринарной логики, в системах искусственного интеллекта и искусственного сознания, для высоконадёжных цифровых вычислителей. Результаты представленного исследования могут использоваться в современной дидактике высшего образования для дисциплин "прикладная математика", "теоретическая информатика" и "защита информации".*

Ключевые слова: *троичная система счисления, троичная зеркально-симметричная система счисления, троичная логика, тернарный оптический компьютер, высоконадёжный арифметический троичный вычислитель, процессор на кодах «фибоначчи», троичная вычислительная машина «Сетунь».*

ВВЕДЕНИЕ

В настоящее время развиваются и широко используются в различных областях техники процессоры, микропроцессоры, универсальные микропроцессоры, сигнальные микропроцессоры, микроконтроллеры и другие аппаратные ускорители цифровых вычислений. В зависимости от области применения требования к процессору меняются и влияют на его внутреннюю архитектуру.

Основное внимание при создании микропроцессоров и микроконтроллеров, как правило, уделялось повышению быстродействия, уменьшению потребляемой мощности и стоимости. Однако недостаточно изучены проблемы повышения информационной надежности, помехоустойчивости, достоверности обрабатываемых данных. Это обстоятельство вызывает тревогу многих известных специалистов в области микропроцессорной техники.

Двоичная система счисления, булева логика, двоичный цифровой элемент используется как основа современных процессоров, основными недостатками которых можно считать то, что они не обеспечивают представления числа со знаком и удовлетворительного округления. «Троянским конём» двоичной системы является ее *нулевая избыточность*. Это делает невозможным осуществление непрерывного контроля цифровых потоков данных в двоичных цифровых вычислителях.

Возрождается интерес к исследованию способов построения вычислительных систем с другими системами счисления. В данной статье рассматриваются перспективные процессоры, микроконтроллеры, использующие троичную систему счисления (с цифрами –1, 0, +1) и зеркально-симметричной арифмитики.

В настоящей работе выполняется обзор исторического наследия учёных Н.П. Брусенцова и А.П. Стахова, которые стали пионерами в области создания уникальных технологий с использованием троичной арифметики и арифметики с кодом «Фибоначчи», излагается теоретический аспект, а также предлагаются пути синтеза высоконадёжного тринарного процессора на основе троичной зеркально-симметричной системы счисления.

НАУЧНОЕ НАСЛЕДИЕ

Обратимся к работам **Николая Петровича Брусенцова**, автора идеологии троичных цифровых элементов и троичной машины "Сетунь", первой в мире троичной машины для научных расчётов [1].

В 1956—1957 гг. под его руководством в Вычислительном центре Московского государственного университета были разработаны троичные элементы для построения цифровых схем, являющихся вариантом магнитных усилителей с питанием импульсами тока. Опыт применения этих элементов в ряде устройств показал, что они могут надежно работать в цифровых схемах с тактовой частотой 200 кгц при нормальных климатических условиях.

Основными достоинствами элементов являются простота устройства и недефицитность используемых деталей (ферритовые сердечники с прямоугольной петлей гистерезиса и германиевые диоды), большой срок службы, незначительное потребление энергии и, как будет здесь показано, возможность с их помощью экономно строить различные логические узлы. В 1961 г. троичные цифровые элементы освоены в серийном производстве.

Конструктивно логические элементы машины выполнены в виде ячеек, смонтированных на пластмассовых платках. В зависимости от количества усилителей, размещенных на одной платке, и от выполняемых ими логических функций ячейки разделяются на 18 типов, использующие магнитные усилители с питанием импульсами тока.

В магнитных усилителях использовали ферритовые кольца с прямоугольной гистерезисной характеристикой, которая сохраняет два различных состояния намагниченности. Логические функции ферритового кольца в электрической цепи можно моделировать двоичным цифровым элементом — триггером. Это позволяет создавать троичные машины, например "Сетунь", на базе цифровых двоичных элементов [2-4]. Для симулятора электронных схем SimulIDE создана библиотека из 18 базовых троичных цифровых элементов «Сетунь».

Построение троичных цифровых элементов на базе двоичных цифровых элементов позволяет использовать все современные технологические достижения в микроэлектронике, а также инструментальное программное обеспечения для синтеза и производства микросхем.

Обратимся также к работам **Алексея Петровича Стахова**, автора технологии процессора Фибоначчи и зеркально-симметричной система счисления.

В докторской диссертации А.П. Стахова (1972 г.) доказана оптимальность так называемых «фибоначчиевых» алгоритмов измерения, которые порождают новый класс позиционных представлений – кодов Фибоначчи.

В 1974 г. опубликована первая статья по арифметике Фибоначчи. В этой статье выдвинута идея, что вся компьютерная технология может быть построена на кодах Фибоначчи и его арифметике, которые являются обобщением и развитием классического двоичного представления и классической двоичной арифметики.

В 1976 г. после доклада по арифметике и компьютерам Фибоначчи на объединенном заседании Кибернетического и Компьютерного обществ Австрии в Советском Союзе, по инициативе посольства СССР в Австрии, началось широкое патентование изобретений в области «компьютеров Фибоначчи» за рубежом. 65 зарубежных патентов (в том числе США, Япония, Англия, Франция, Германия, Канада) являются официальными юридическими документами, которые подтверждают приоритет в этом направлении.

С 1986-го по 1989-й гг. в Специальном конструкторско-технологическом бюро «Модуль» Винницкого технического университета, из инженерных разработок, доведенных до мелкосерийного производства, наибольший интерес представлял «фибоначчиевый» самокорректирующийся 18-ти разрядный аналого-цифровой преобразователь (АЦП), обладающий довольно высокими метрологическими характеристиками. Главная его особенность состояла в том, что впервые в мировой практике был разработан АЦП с «вечными» техническими характеристиками. Благодаря встроенной системе контроля, которая использовала свойство «многозначности» фибоначчиевых представлений, метрологические параметры такого АЦП не зависели от погрешностей технологии, изменения температуры и старения элементов.

Например, при технологической точности изготовления элементов в 5% благодаря самонастройке точность АЦП повышалась в 1000 раз (до 0.005%) и далее сохранялась неизменной независимо от температуры и старения элементов.

В НПО «Научный Центр» (г. Зеленоград) спроектирована и изготовлена первая в истории компьютерной науки «фибоначчиева» микросхема. Микросхема была предназначена для обработки символьной информации и выполнения арифметических операций в кодах Фибоначчи и "золотой пропорции" [5]. В частности, в микросхеме была заложена возможность выполнения следующих операций: запись и чтение информации, свертка, развертка, перемещение, поглощение, приведение к минимальной форме, суммирование, вычитание, реверсивный сдвиг, логическое умножение, логическое сложение и сложение по модулю 2.

Отличительной особенностью микросхемы являлось наличие контрольного выхода, на котором формировалась информация о неправильной работе микросхемы. Одновременно с выдачей сигнала "ошибка" блокировались все информационные

выходы. Если ошибка являлась следствием "сбоя" и при повторении операции сигнал "ошибка" не появлялся, то блокировка выходов снималась. Если же внутри микросхемы происходил "отказ", то это индицировалось с помощью сигнала "ошибка", появляющегося постоянно на контрольном выходе, и в этом случае блокировка информационных выходов оставалась.

Таким образом, в микросхеме обнаруживался сбой любого электронного элемента в момент его возникновения и блокировалась возможность выполнения ложной команды.

В 2005 г. на основе троичного принципа Брусенцова и системы счисления Бергмана создана «золотая» троичная зеркально-симметричная арифметика. Так называемые «симметричные системы счисления» являются дальнейшим развитием идеи позиционного представления чисел. Основная особенность таких систем состоит в использовании отрицательных и положительных цифр для представления чисел. Простейшей из них является «троичная симметричная система счисления». Напомним, что в этой системе счисления в качестве основания используется число 3, а в качестве цифр – троичные цифры 1, 0 и 1 =-1.

Н.П. Брусенцов в статье «Преимущества троичной системы счисления» дает ответ на вопрос, в чем преимущества троичной симметричной системы счисления, которые стали причиной использования этой системы в компьютере «Сетунь».

По мнению Брусенцова, главное преимущество троичного представления чисел перед принятым в современных компьютерах двоичным представлением состоит в том, что с тремя цифрами возможен натуральный код чисел со знаком, а с двумя невозможен. Несовершенство двоичной арифметики и реализующих ее цифровых машин обусловлено именно тем, что двоичным кодом естественно представимы либо только неотрицательные числа, либо только неположительные, а для представления всей необходимой для арифметики совокупности — положительных, отрицательных и нуля — приходится пользоваться искусственными приемами типа обратного или дополнительного кодов, системой с отрицательным основанием или с цифрами +1,-1 и другими способами.

В троичном коде с цифрами +1, 0, 1 имеет место естественное представление чисел со знаком (так называемая симметричная, уравновешенная или сбалансированная система), и «двоичные» проблемы, не имеющие удовлетворительного решения. Это преимущество присуще всякой «симметричной» системе с нечетным числом цифр, но троичная система самая простая из них и доступна для технической реализации. Арифметические операции в троичной симметричной системе практически не сложнее двоичных, а если учесть, что в случае чисел со знаком двоичная арифметика использует искусственные коды, то окажется, что троичная даже проще.

Представление целых чисел в зеркально-симметричной системе счисления

Новая троичная зеркально-симметричная арифметика является оригинальным синтезом троичной симметричной системы счисления, которую использовал Н.П. Брусенцов в своем компьютере «Сетунь», и системы счисления математика Джорджа Бергмана. Самое важное преимущество «зеркально-симметричной арифметики» состоит в том, что свойство «зеркальной симметрии» является «инвариантом» относительно всех арифметических операций над целыми числами, то есть результаты сложения, вычитания, умножения и даже деления всегда представляются в зеркально-симметричной форме. Это означает, что найден новый универсальный способ контроля всех арифметических операций в компьютере, основанный на свойстве зеркальной симметрии троичных представлений. Напомним, что это свойство является справедливым только для случая, когда исходные числа и результаты арифметических операций являются целыми числами.

А.П. Стахов рассматривал создание «троичной зеркально-симметричной арифметики» как своё высшее достижение в области теории систем счисления. Эта система счисления возникла как результат многолетних поисков более эффективных путей построения компьютеров. Новая система счисления основана на «троичном» представлении и сохраняет все основные преимущества классической «троичной» симметричной системы счисления, использованной Н.П. Брусенцовым при создании компьютера «Сетунь».

Однако ее главным достоинством по сравнению с классической симметричной системой счисления является уникальный способ контроля всех основных преобразований информации в компьютере. Этот способ контроля вполне может быть использован для создания самоконтролирующихся процессоров и компьютеров.

А.П. Стахов считал, что вопрос разработки самоконтолирующихся и отказоустойчивых троичных «зеркально-симметричных компьютеров» в дополнение к «троичным» компьютерам Брусенцова может оказаться делом не такого далекого будущего, если учесть, что на современном этапе проблема «трехзначной электроники» считается уже решенной. И если это случится, то это будет еще одним веским доказательством фундаментальности «принципа тринитаризма» в современной науке!

ДВОИЧНАЯ СИСТЕМА

Традиционная (кремниевая) микроэлектроника, выстроенная на двоичной системе счисления, подходит к пределу своих технологических возможностей.

Одним из главных принципов, в перечне Неймановских, считается следующий: машины на электронных элементах должны работать не в десятичной, а в двоичной системе счисления. Основными преимуществами двоичной системы являются: двухпозиционный характер работы электронных элементов, высокая экономичность двоичной системы и простота выполнения арифметических операций с двоичными числами.

К сожалению, этот важнейший принцип – использование двоичной системы как основы современных компьютеров – таит в себе одну «ловушку». Двоичная система обладает «нулевой избыточностью». Это означает, что в классической двоичной системе отсутствует механизм обнаружения ошибок в процессоре и компьютере, которые неизбежно (с большей или меньшей вероятностью) могут возникнуть под влиянием различных внешних и внутренних факторов (прежде всего разнообразных внешних воздействий и помех, действующих в шинах питания и каналах связи).

То есть никакая ошибка не может быть обнаружена в рамках двоичной системы счисления без введения дополнительных контрольных средств. Это является причиной того, что «Неймановские машины», основанные на двоичной системе, являются принципиально ненадежными.

Неадекватность двоичности проявилась при исследовании логико-алгебраических основ информатики. Установлено, что так называемые парадоксы материальной импликации, устранить которые безуспешно пытались виднейшие логики, обусловлены противоестественным “законом исключенного третьего” и составляют неотъемлемую особенность двухзначности. Полноценное содержательное следование, представленное в аристотелевой силлогистике общеутвердительной посылкой “Всякое **x** есть **y**” (“Из **x** с необходимостью следует **y**”), в двухзначной логике непредставимо и вырождено в утратившую смысловую взаимосвязь терминов импликацию, что и обусловило бессодержательность этой логики.

ТРОИЧНАЯ СИСТЕМА

Троичный код является простейшим, позволяющим осуществить симметричную (уравновешенную, сбалансированную) систему счисления, оказывается исключительно важным как в принципе, так и практически. Д.Кнут охарактеризовал уравновешенную троичную систему счисления как “самую изящную”.

Использование троичной сбалансированной (уравновешенной, симметричной) системы счисления имеет существенные достоинства. Практическая ценность троичного кода и троичной логики объясняется следующими свойствами:

- имеет место естественное представление чисел со знаком, т.е. не нужно пользоваться искусственными приемами в двоичной системе счисления, например, прямого, обратного или дополнительного кода представления отрицательного числа;
- знак числа определяется знаком старшей ненулевой цифры и не нужно использовать специальный знаковый бит, как в двоичной системе;
- просто производится операция сравнения модулей чисел;
- операция ветвления по знаку в троичной машине занимает в два раза меньше времени, чем в двоичной;
- усечение длины числа равносильно теоретическому округлению с минимальной погрешностью;
- троичный сумматор может осуществлять вычитание при инвертировании одного из слагаемых, из чего следует, что троичный счетчик автоматически является реверсивным;
- таблицы умножения и деления почти так же просты, как и в двоичной системе, умножение на -1 инвертирует множимое.

Полностью "совместимой" с уравновешенной троичной системой счисления является троичная зеркально-симметричная система счисления, предложенная А. П. Стаховым.

Основные преимущества зеркально-симметричная арифметики:

- представление некоторых иррациональных чисел в виде конечной совокупности троичных разрядов (тритов);
- зеркально-симметричное отображение левой и правой части в записи целых чисел;
- использование указанного выше свойства позволяет контролировать цифровой поток данных всех арифметических действий в вычислительных системах.

ТРОИЧНАЯ ЗЕРКАЛЬНО-СИММЕТРИЧНАЯ АРИФМЕТИКА

Новая троичная арифметика является оригинальным синтезом троичной симметричной системы счисления, которую использовал Николай Брусенцов в своем компьютере «Сетунь», и системы счисления Бергмана. Для пояснения сути нового

троичного способа представления чисел и новой троичной арифметики рассмотрим бесконечную последовательность четных степеней золотой пропорции:

$$\ldots\tau^{6}, \tau^{4}, \tau^{2}, \tau^{0}, \tau^{-2}, \tau^{-4}, \tau^{-6}, \ldots,$$

где $\tau = \frac{1+\sqrt{5}}{2}$ — золотая пропорция.

Ясно, что указанная последовательность представляет собой геометрическую прогрессию с основанием $\tau^2 = \frac{3+\sqrt{5}}{2}$.

Эту последовательность мы будем использовать в качестве весов разрядов для позиционного «троичного» представления чисел, используя троичные цифры 1, 0 и-1 .

Из теории золотого сечения известно следующее интересное тождество, связывающее члены рассматриваемой последовательности:

$$\tau^{2n} + \tau^{2n} = \tau^{2(n+1)} - \tau^{2n} + \tau^{2(n-1)},$$

то есть сумма двух одинаковых четных (2n-x) степеней золотой пропорции равна алгебраической сумме трех четных степеней золотой пропорции, а именно 2(n+1)-й степени, взятой со знаком «плюс», 2n-й степени, взятой со знаком «минус», и 2(n-1)-й степени, взятой со знаком «плюс». На языке «троичных» цифр 1, 0 и -1 указанное тождество имеет следующую кодовую интерпретацию:

1 + 1 = 1 1 1.

Это выражение задает правило сложения положительных единиц в новой системе счисления. Это правило гласит, что при сложении положительных единиц необходимо записать отрицательную единицу 1 в текущий разряд промежуточной суммы и сформировать симметрично относительно текущего разряда две положительные единицы, которые являются переносами в соседние (слева и справа) разряды.

Ясно, что не существует никаких проблем по аналогии записать правило сложения отрицательных единиц:

1 +1 = 1 1 1.

К указанным выше правилам добавим еще четыре правила, которые полностью совпадают с аналогичными правилами сложения в троичной симметричной системе счисления:

0 + 0 = 0; 1 + 0 = 1; 1 + 0 = 1; 1 + 1 = 0.

В результате получается следующая таблица 1 сложения чисел в новой системе счисления. Эта таблица задает правило сложения двух одноименных троичных разрядов $a_k + b_k$.

Таблица 1

Таблица зеркально-симметричного сложения

b_k a_k	1	0	1
1	111	1	0
0	1	0	1
1	0	1	1 1 1

Теперь используем эту таблицу для «конструирования» изображений натуральных чисел в троичной системе счисления, в которой весами разрядов являются четные степени золотой пропорции.

Поскольку $1 = \tau^0$, то число 1 в новой системе счисления мы представим с помощью следующей записи: 1 = 1,0. Заметим, что запятая, стоящая после 1, означает, что 1 относится к нулевому разряду.

Для получения записи числа 2 используем указанное выше правило сложения двух положительных единиц. В соответствии с этим правилом число 2 можно представить в виде следующей записи: 2 = 11,1. Эта запись означает, что число 2 может быть выражено в виде суммы трех четных степеней золотой пропорции: $2 = \tau^2 - \tau^0 + \tau^{-2}$. В этом легко убедиться, если вспомнить, что $\tau^2 = \tau + 1$, $\tau^{-2} = 1 - \tau^{-1}$, а $\tau^{-1} = \tau - 1$.

Добавляя положительную единицу к нулевому разряду кодовой записи числа 2, получим «троичную» запись числа 3 = 10,1. Эта запись означает ни что иное, как сокращенную цифровую запись следующего выражения: $3 = \tau^2 + \tau^{-2}$.

Ясно, что число 4 имеет следующую цифровую запись: 4=11,1, что является цифровой записью следующей суммы: $4 = \tau^2 + \tau^0 + \tau^{-2}$.

Для получения цифровой записи числа 5 добавим 1 к нулевому разряду числа 4. В результате в соответствии с рассмотренным выше правилом сложения положительных единиц на первом шаге сложения в нулевом разряде промежуточной суммы записывается отрицательная единица 1, а из нулевого разряда формируются переносы двух положительных единиц в соседние разряды справа и слева от нулевого разряда.

На следующем шаге сложения в соответствием с тем же правилом в соседних разрядах справа и слева от нулевого записываются отрицательные единицы 1 и из них возникают переносы положительных единиц в соседние разряды. Поскольку при этом в нулевой разряд приходят два переноса положительных единиц (от разрядов справа и слева), то после их суммирования с отрицательной единицей, которую мы записали в нулевой разряд на первом этапе сложения, в нулевом разряде будет записана положительная единица (1 + 1 + 1 = 1). В конечном

итоге мы получим следующее изображение числа 5 = 11 1,1 1.

Продолжая эти рассуждения, мы получим изображения всех натуральных чисел, в частности: 6 = 1 0 1, 0 1; 7 = 100,01; 8 = 101,01; 9 = 111, 11; 10 = 110,11 и т.д.

Таким образом, в результате проведенных рассуждений мы пришли к следующему позиционному представлению целых чисел:

$$N = \sum_{i=-\infty}^{+\infty} c_i \tau^{2i},$$

где c_i – троичные цифры 1 , 0, 1; τ^{2i} – вес i-го разряда.

Основанием системы счисления в данном случае является иррациональное число, равное квадрату золотой пропорции $\tau^2 = \frac{3+\sqrt{5}}{2} \approx 2{,}618$. Таким образом, данная система счисления также относится к классу систем счисления с иррациональными основаниями.

ЭМУЛЯЦИЯ ЗЕРКАЛЬНО-СИММЕТРИЧНОЙ АРИФМЕТИКИ

На языке программирования C реализованы некоторые операции зеркально-симметричной арифметики А.П.Стахова с возможностью достоверного вычисления для каждой арифметической операции [6, 7].

```
/*
*       Filename:       "Ternary_mirror_symmetrical_
arithmetic.c"
 *
 * Project: Демонстрация зеркально-симметричной
арифметики А.П.Стахова
 *
 * Author: Vladimir Vasiley
 * E-Mail: askfind@ya.ru
 *
 * Russia, Saint-Petersburg
 *
 * Create date: 12.02.2025
 * Edit date:   22.02.2025
 * Version:     0.13
 *
 */

#define C_SIZE (7)
#define MSC_SIZE (15)

/*
 * Возведение в степень
 */
double pow_full(double base, int exp)
{
        if (exp == 0)
                return 1;
        if (exp == 1)
                return base;

        if (exp < 0)
        {
                if (exp == INT_MIN)
                {
                return (1 / base) * pow(base, exp + 1);
                }
                base = 1 / base;
                exp =-exp;
        }
        double half = pow(base, exp / 2);
        if (exp % 2 == 0)
        {
                return half * half;
        }
        else
        {
                return half * half * base;
        }
}

/*
 *  Инверсия трита
 */
int INV_trit(int trit)
{
        if (trit > 0)
                return-1;
        if (trit < 0)
                return +1;

        return 0;
}
/*
 *  Сравнение двух тритов
 */
int CMP_trit(int tr1, int tr2)
{
        if (tr1 == tr2)
        {
                return 0; /* равны */
        }
        else
        {
                return 1; /* не равны */
        }
}
```

```
/*
 * Преобразование зеркально-симметричного числа в число с плавающей точкой.
 */
float Mirror_Symmetrical_To_Float(int a[], int len)
{
	int i = 0;
	double res = 0.0;

	int n = len;
	int hn = (int)(n / 2);
	float tt = (float)((3.0 + sqrt(5.0)) / 2.0);

	int j =-hn;
	for (i = 0; i < n; i++)
	{
		float p = (float)(a[i]) * (float)pow_full(tt, (double)j);
		j += 1;
		res += p;
	}

	return res;
}

/*
 * Проверка достоверности вычисления зеркально-симметричного числа
 */
int CHECK_msc(int a[], int len)
{
	int i = 0;
	int hn = (int)(len / 2);
	int p0 = 0;
	int p1 = len- 1;

	for (i = 0; i < hn; i++)
	{
		if (CMP_trit(a[p0], a[p1]) > 0)
		{
			return 1; /* Error */
		}
		p0 += 1;
		p1-= 1;
	}

	return 0; /* Ok' */
}
/*
 * Инверсия зеркально-симметричного числа
 */
int INV_msc(int a[], int len)
{
	int i = 0;
	for (i = 0; i < len; i++)
	{
		a[i] = INV_trit(a[i]);
	}

	return CHECK_msc(a, len);
}
```

Процедура демонстрации зеркально-симметричных вычислений

```
/*
 * Main
 *
 */
int main(int argc, char *argv[])
{
	int check = 0;
	/* MIN mirror_symmetrical codes */
	printf("Example #0----------\n");
	printf("| MIN mirror_symmetrical codes for width 15\n");
	printf("MIN_msc_t15[] := \n");
	int min_t15[MSC_SIZE] =
		{-1,-1,-1,-1,-1,-1,-1,
		-1,
		-1,-1,-1,-1,-1,-1,-1};
	float mind_t15 = Mirror_Symmetrical_To_Float(min_t15, MSC_SIZE);
	check = CHECK_msc(min_t15, MSC_SIZE);
	view_msc(min_t15, mind_t15, MSC_SIZE, check);

	printf("MAX_msc_t15[] := \n");
	int max_t15[MSC_SIZE] =
		{1, 1, 1, 1, 1, 1, 1,
		 1,
		 1, 1, 1, 1, 1, 1, 1};

	float maxd_t15 = Mirror_Symmetrical_To_Float(max_t15, MSC_SIZE);
	check = CHECK_msc(max_t15, MSC_SIZE);
	view_msc(max_t15, maxd_t15, MSC_SIZE, check);

	/* MIN mirror_symmetrical codes */
	printf("Example #0----------\n");
	printf("| MIN mirror_symmetrical codes\n");
	printf("MIN_msc[] := \n");
	int min[C_SIZE] = {-1,-1,-1,-1,-1,-1,-1}; //
	float mind = Mirror_Symmetrical_To_Float(min, C_SIZE);
	check = CHECK_msc(min, C_SIZE);
	view_msc(min, mind, C_SIZE, check);
```

```
        printf("MAX_msc[] := \n");
        int max[C_SIZE] = {1, 1, 1, 1, 1, 1, 1}; //
        float maxd = Mirror_Symmetrical_To_
Float(max, C_SIZE);
        check = CHECK_msc(max, C_SIZE);
        view_msc(max, maxd, C_SIZE, check);

        /* SUM mirror_symmetrical codes */
        printf("Example #1----------\n");
        printf("| SUM mirror_symmetrical codes\n");
        printf("a[] + b[] := c[]\n");
        /*
         * Test 1: for function Float
         */
        int a[C_SIZE] = {-1,-1, 0, 1, 0,-1,-1}; //-24
        float ad = Mirror_Symmetrical_To_Float(a, C_
SIZE);
        check = CHECK_msc(a, C_SIZE);
        printf("a[] :=\n");
        view_msc(a, ad, C_SIZE, check);

        int b[C_SIZE] = {1,-1, 1, 1, 1,-1, 1}; // 15
        float bd = Mirror_Symmetrical_To_Float(b, C_
SIZE);
        check = CHECK_msc(b, C_SIZE);
        printf("b[] :=\n");
        view_msc(b, bd, C_SIZE, check);

        int c[C_SIZE] = {-1, 1, 1,-1, 1, 1,-1}; //-9
        float cd = Mirror_Symmetrical_To_Float(c, C_
SIZE);
        check = CHECK_msc(c, C_SIZE);
        printf("c[] :=\n");
        view_msc(c, cd, C_SIZE, check);

        return 0;
}
```

Данный фрагмент кода реализует основные арифметические операции и может быть использован для тестирования и обучения.

ЗАКЛЮЧЕНИЕ

В настоящей статье рассмотрены теоретические основы синтеза цифровых элементов на основе зеркально-симметричной системы счисления. Полученные результаты позволяют подтвердить, что тринарный процессор является уникальной цифровой технологией будущего, которая может быть создана на основе троичной системы счисления и зеркально-симметричной арифметики [8-10]. Тринарный процессор будет обладать уравновешенной арифметикой и содержательной тринарной логикой, а также высоконадёжным контролем потока цифровых данных в реальном времени.

СПИСОК ЛИТЕРАТУРЫ

1. Брусенцов Н. П., Маслов С. П., Розин В. П., Тишулина А. М. Малая цифровая вычислительная машина «Сетунь».- М.: Изд-во МГУ, 1965. 145 с.

2. Брусенцов Н. П. Использование троичного кода и трёхзначной логики в цифровых машинах // Научный отчёт №24ВТ(378).- М.: Изд-во МГУ, Москва 1969г. 27 с.

3. Вопросы технического и математического обеспечения ЭЦВМ «СЕТУНЬ» и «МИНСК-22»: [Сборник статей] / Под общей редакцией И.У. Солиева. Выпуск 1. Душанбе. 1971. 114 с.

4. Брусенцов Н.П., Владимирова Ю.С., Рамиль Альварес Х. Троичный логико-алгебраический и арифметический процессор // Издательский отдел ВМК МГУ, 2005. С. 184-187.

5. Стахов А.П. Машинная арифметика ЦВМ в кодах Фибоначчи и "золотой" пропорции (Предварит. Публ.). — М. : Б. и., 1981. — 64 с.

6. Байков В.Д., Смолов В.Б. Специализированные процессоры: итерационные алгоритмы и структуры.- М.- изд. Радио и связь. 1985. 288 с.

7. Стахов А.П. Микропроцессоры Фибоначчи — как одна из базисных инноваций будущего технологического уклада, изменяющих уровень информационной безопасности систем. URL: http://www.trinitas.ru/rus/doc/0232/009a/02321212.htm

8. Кушнеров А. Троичная цифровая техника. Ретроспектива и современность. URL: https://www.researchgate.net/publication/331330009_Ternary_digital_technology_Retrospective_and_contemporary_state_in_Russian.

9. Спиридонов А.Н. Троичность, как альтернатива для компьютерных вычислений. Самарский государственный аэрокосмический университет имени академика С.П. Королева.- 2007. 33 с.

10. Васильев В.И. МЭВМ "Сетунь" цифровые элементы на ферритах. URL: http://www.nedopc.org/forum/viewtopic.php?t=18829

УДК: 004.056.57

Работа двух взаимозаменяемых антивирусных программ с учетом скорости размножения вирусных программ

I.V. Atlasov, D.E. Vilkhovsky, V.A. Makeev

Running of Two Interchangeable Anti-Virus Programs With Consideration of the Virus Programs Reproduction Rate

Abstract. *This paper examines the architecture of an enterprise protection system against computer viruses based on two interchangeable antivirus programs. The primary focus is on the efficiency of such a system in the event of a failure of one of the antivirus programs and the transition to a backup. The probability of antivirus program failures and the time to restore their operation are analyzed. Probabilistic methods are used to assess the number of viruses eliminated depending on the system's recovery time. A mechanism for the alternate use of two antivirus programs is proposed to enhance the system's efficiency and resilience.*

Keywords: *antivirus programs, viruses, enterprise protection, resilience, security system, backup protection.*

И.В. Атласов[1]
Д.Э. Вильховский[2]
В.А. Макеев[3]

[1]Доктор физико-математических наук, профессор кафедры естественнонаучных дисциплин учебно-научного комплекса информационных технологий Московского университета Министерства внутренних дел Российской Федерации имени В.Я. Кикотя.
E-mail: atlasov.igor777@gmail.com
[2]Старший преподаватель кафедры информационной безопасности Омского государственного университета имени Ф.М. Достоевского
E-mail: vilkhovskiy@gmail.com
[3]Курсант 4 «И» курса факультета подготовки специалистов в области информационной безопасности Московского университета Министерства внутренних дел Российской Федерации имени В.Я. Кикотя.
E-mail: vova.vackeev2016@yandex.ru

Аннотация. *В статье рассматривается архитектура системы защиты предприятия от компьютерных вирусов на основе двух взаимозаменяемых антивирусных программ. Особое внимание уделяется эффективности такой системы при сбоях одной из антивирусных программ и переходе на резервную. Анализируется вероятность сбоя антивирусных программ и время восстановления их работы. Используются вероятностные методы для оценки количества уничтожаемых вирусов в зависимости от времени восстановления системы. Предложен механизм поочередного использования двух антивирусных программ для повышения эффективности и отказоустойчивости системы.*

Ключевые слова: *антивирусные программы, вирусы, защита предприятия, отказоустойчивость, система безопасности, резервная защита.*

ВВЕДЕНИЕ

Одним из общих требований в отношении антивирусной системы защиты предприятия является требование о стойкой системе самозащиты, которая, в том числе, позволит обеспечить нормальное функционирование системы во время уничтожения вирусов[1]. Однако несмотря на то, что разработчики антивирусных программ существенно продвинулись в вопросах обеспечения их стабильной работы, риски сбоев и отказов работы антивирусных программ не могут быть исключены в полной мере.

Например, в разделе о службе поддержки Лаборатории Касперского размещена статья, с последним обновлением от 04 сентября 2023 г.[2], в которой описано решение проблемы внезапного сбоя их программ, что само по себе уже служит доказательством того, что внезапное прекращения работы антивирусных программ вполне вероятно. Также, интересно отметить, что предлагаемым решением здесь является переустановка программы, что свидетельствует о том, что самостоятельное восстановление антивирусов может происходить не всегда.

Для минимизации последствий сбоев и отказов работы антивирусных программ в условиях высоких требований к отказоустойчивости систем и защите от целевых атак злоумышленников на антивирусную систему необходима разработка архитектуры, способной обеспечить повышение эффективности антивирусной системы, оптимизацию времени работы и восстановления программ.

[1]Антивирусная система защиты предприятия / Лаборатория Dr.Web. 42 с. URL: https://st.drweb.com/static/new-www/files/booklets/antivirus_protection_system/antivirus_protection_system_ru.pdf (дата обращения: 22.01.2025).

[2]Программа «падает», «зависает» или «тормозит», появляется сообщение «При предыдущем запуске программы произошел сбой» / Лаборатория Касперского. 04.09.2023. URL: https://support.kaspersky.ru/common/error/other/14826 (дата обращения: 22.01.2025).

Цель настоящей работы — обосновать целесообразность использования архитектуры системы защиты предприятия от компьютерных вирусов на основе двух взаимозаменяемых антивирусных программ. Для достижения данной цели проводится анализ эффективности такой системы при сбоях одной из антивирусных программ и переходе на резервную, при этом применяются вероятностные методы для оценки количества уничтожаемых вирусов в зависимости от времени восстановления системы.

О ПРИЧИНАХ СБОЯ И ОТКАЗА РАБОТЫ АНТИВИРУСНОГО ПО

Причины сбоя и отказа работы антивирусных программ могут быть различными – от проблем с обновлением баз данных, вызванных, например, недоступностью сервера антивируса из-за настроек провайдера или файрвола, препятствующих обновлению, или повреждением базы данных (причиной может быть прерывание обновления), до уязвимостей непосредственно самих антивирусных программ [1].

Так, согласно данным ФСТЭК, в некоторых антивирусных программах были выявлены следующие уязвимости:

• уязвимость функции VirusEvent службы ClamD из-за непринятия мер по нейтрализации специальных элементов, используемых в команде операционной системы, эксплуатация которой могла позволить удаленно выполнить произвольные команды[3];

• уязвимость модуля разбора данных средств антивирусной защиты, связанная с неограниченным распределением ресурсов, эксплуатация которой могла позволить удаленно выполнить произвольный код[4];

• уязвимость компонента анализа файлов формата OLE2, связанная с возможностью чтения данных за границами буфера в памяти, эксплуатация которой могла удалённо вызвать отказ в обслуживании путём отправки специально сформированного OLE2-файла[5];

• уязвимость, связанная с небезопасным управлением привилегиями, эксплуатация которой могла позволить удаленно приостановить работу защитных модулей в рамках сценариев установки/переустановки продукта[6];

• уязвимость анализатора HTML-кода, связанная с неограниченным распределением ресурсов, эксплуатация которой могла удалённо вызвать отказ в обслуживании[7].

Следовательно, риск сбоя и остановки работы используемого антивирусного ПО, в результате которого система пользователя остается без защиты, действительно существует.

ПРОБЛЕМЫ ОДНОВРЕМЕННОГО ПРИСУТСТВИЯ ДВУХ АНТИВИРУСНЫХ ПРОГРАММ В ОДНОЙ СИСТЕМЕ

Очевидно, что данная проблема не может быть решена при помощи одновременного запуска двух различных антивирусных программ. Во-первых, как и все программы, антивирусы используют значительный объем системной памяти. Следовательно, одновременная работа двух антивирусных программ существенно снижает эффективность всей системы, т.е. неэкономична вследствие выполнения избыточных операций. Во-вторых, установка нескольких антивирусов может привести к конфликтам (поскольку они работают в одних и тех же системных зонах), что может вызвать сбои.

Также отметим, что время, необходимое для восстановления работы антивирусной программы может быть достаточно длительным. За это время вирусы могут существенно размножиться или даже новый вирус может проникнуть в систему [2]. Для

[3]BDU:2024-01734: Уязвимость функции VirusEvent службы ClamD пакета антивирусных программ ClamAV, позволяющая нарушителю выполнить произвольные команды / Федеральная служба по техническому и экспортному контролю России. 07.02.2025. URL: https://bdu.fstec.ru/vul/2024-01734 (дата обращения: 22.01.2025).

[4]BDU:2022-01730: Уязвимость модуля разбора данных средств антивирусной защиты Kaspersky Anti-Virus, Kaspersky Internet Security, Kaspersky Total Security, Kaspersky Small Office Security, Kaspersky Security Cloud, Kaspersky Endpoint Security, позволяющая нарушителю выполнить произвольный код / Федеральная служба по техническому и экспортному контролю России. 07.02.2025. URL: https://bdu.fstec.ru/vul/2022-01730 (дата обращения: 22.01.2025).

[5]BDU:2024-01085: Уязвимость компонента анализа файлов формата OLE2 пакета антивирусных программ ClamAV, позволяющая нарушителю вызвать отказ в обслуживании / Федеральная служба по техническому и экспортному контролю России. 07.02.2025. URL: https://bdu.fstec.ru/vul/2024-01085 (дата обращения: 22.01.2025).

[6]BDU:2024-01525: Уязвимость средства антивирусной защиты Kaspersky Endpoint Security для Windows, связанная с небезопасным управлением привилегиями, позволяющая нарушителю приостановить работу защитных модулей / Федеральная служба по техническому и экспортному контролю России. 07.02.2025. URL: https://bdu.fstec.ru/vul/2024-01525 (дата обращения: 22.01.2025).

[7]BDU:2024-03114: Уязвимость анализатора HTML-кода пакета антивирусных программ ClamAV, позволяющая нарушителю вызвать отказ в обслуживании / Федеральная служба по техническому и экспортному контролю России. 07.02.2025. URL: https://bdu.fstec.ru/vul/2024-03114 (дата обращения: 22.01.2025).

ликвидации этого эффекта на компьютере требуется другая аналогичная антивирусная программа, которая включается в работу, когда первая антивирусная программа перестает работать.

Таким образом, необходимо разработать иной механизм сохранения надлежащего уровня защиты системы от вирусов в случае отказа работы используемого антивируса, обеспечив при этом отсутствие конфликтов антивирусных ПО, а также баланс между защищенностью системы и ее производительностью.

Решение проблемы конфликта двух антивирусных программ

Одним из таких механизмов может являться двойная архитектура антивирусной системы защиты предприятия, основанная на поочередном использовании двух антивирусных программ [3]. Так, изначально работает первая антивирусная программа, тогда так вторая находится в спящем (неактивном) режиме. Программу, которая активно защищает систему, называют основной, а программу, находящуюся в спящем (неактивном) режиме и принимающую на себя функцию защиты лишь в случае отказа основной – резервной.

При сбое и отказе основной программы включается резервная, которая принимает на себя функцию антивирусной защиты системы и переходит в категорию основной программы. Далее, предыдущая программа восстанавливается и переходит в статус резервной программы до момента сбоя или отказа активно действующей программы.

АНАЛИЗ ЭФФЕКТИВНОСТИ ДВУХУРОВНЕВОЙ АНТИВИРУСНОЙ СИСТЕМЫ

При разработке указанного механизма мы исходим из гипотезы, что время между выключением основной антивирусной программы и началом работы резервной антивирусной программы сравнительно мало, а потому в дальнейшем анализе и расчетах этот момент можно не учитывать как существенный фактор. Далее, мы считаем, что работа i программы уничтожает a_i вирусов за единицу времени и уничтожается, когда b_i вирусов атакуют i программу также за единицу времени, $i = 1,2$.

Основная задача состоит в том, чтобы понять, насколько эффективна работа системы из двух программ по сравнению с работой одной программы.

Решать эту задачу будем, вероятностными методами [4-6]. Для этого предположим, что выполнены следующие условия:

1. время безотказной работы i-й программы после k-го восстановления является случайной величиной θ_i^k с функцией распределения $F_i^k(x)$, $i = 1,2$, $k = 0,1,2, \ldots$. Также считаем, что $F_i^k \equiv F_i$, для всех $k = 0,1,2, \ldots$ и $i = 1,2$;

2. длительность k восстановления i-ой программы является случайной величиной η_i^k с функцией распределения $G_i^k(x)$, $i = 1,2$, $k = 1,2, \ldots$. Также считаем, что $G_i^k \equiv G_i$, для всех $k = 1,2, \ldots$ и $i = 1,2$;

3. отказавшая программа сразу отправляется на восстановление и затем находится в резерве.

Рассмотрим следующие новые обозначения:

1. Пусть Θ_0 – количество уничтоженных вирусов за все время работы системы.

2. ξ_0 – общее время работы двух антивирусных программ за все время работы системы.

3. Θ_1 – количество уничтоженных вирусов начиная с времени θ_1^0.

4. ξ_1 – общее время работы двух антивирусных программ за все время работы системы без времени восстановления η_1^1 и $\Psi_1(x)$ – его функция распределения.

5. Θ_2 – количество уничтоженных вирусов за время безотказной работы двух программ, начиная со времени $\theta_1^0 + \theta_2^0$.

6. ξ_2 – общее время работы двух антивирусных программ за все время работы системы без времени восстановления $\eta_1^1 + \eta_2^1$ и $\Psi_2(x)$ – его функция распределения.

7. Θ_3 – количество уничтоженных вирусов за время безотказной работы двух программ, начиная со времени $\theta_1^0 + \theta_2^0 + \theta_1^1$.

8. ξ_3 – общее время работы двух антивирусных программ за все время работы системы без времени восстановления $\eta_1^1 + \eta_2^1 + \eta_1^2 +$ и $\Psi_3(x)$ – его функция распределения.

9. Θ_4 – количество уничтоженных вирусов за время безотказной работы двух программ, начиная со времени $\theta_1^0 + \theta_2^0 + \theta_1^1 + \theta_2^1$.

10. ξ_4 – общее время работы двух антивирусных программ за все время работы системы без времени восстановления $\eta_1^1 + \eta_2^1 + \eta_1^2 + \eta_2^2$ и $\Psi_4(x)$ – его функция распределения.

11. Θ_{2n} – количество уничтоженных вирусов за время безотказной работы двух программ, начиная со времени $\sum_{k=1}^{n}(\theta_1^k + \theta_2^k)$.

12. ξ_{2n} – общее время работы двух антивирусных программ за все время работы системы без времени восстановления $\sum_{k=1}^{n}(\eta_1^k + \eta_2^k)$ и $\Psi_{2n}(x)$ – его функция распределения.

13. Θ_{2n+1} – количество уничтоженных вирусов за время безотказной работы двух программ, начиная со времени $\sum_{k=1}^{n}(\theta_1^k + \theta_2^k) + \theta_1^{n+1}$ без учета расходов во время ремонта устройств.

14. ξ_{2n+1} – общее время работы двух антивирусных программ за все время работы системы без времени восстановления $\sum_{k=1}^{n}(\eta_1^k+\eta_2^k)+\eta_1^{n+1}$ и $\Psi_{2n+1}(x)$ – его функция распределения.

15. Θ – общие количество уничтоженных вирусов за время безотказной работы двух программ и $F_\Theta(x)$ – его функция распределения.

Рассмотрим небольшой чертеж ниже (рис. 1):

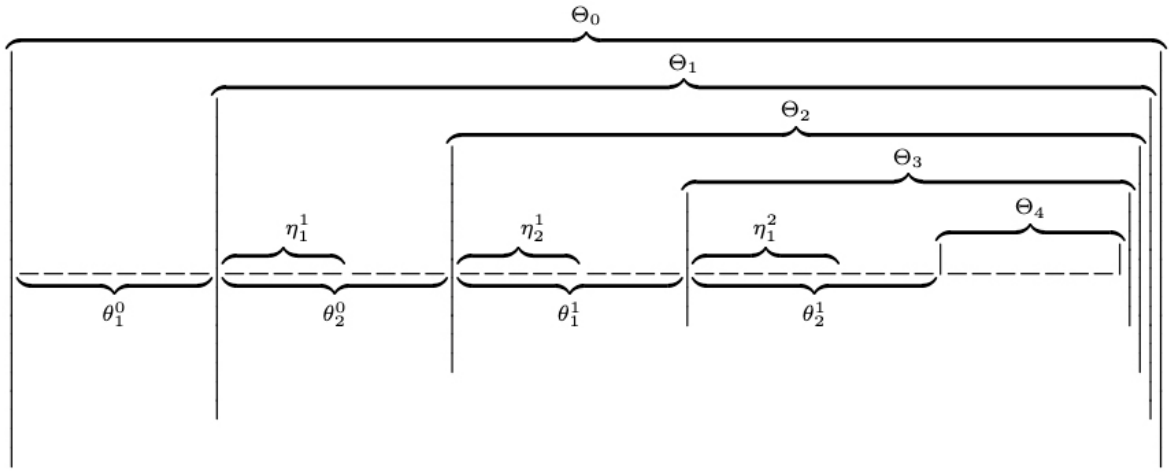

Рис.1. Количество уничтоженных вирусов за различные периоды работы двух антивирусных программ

В дальнейшем будем пользоваться обозначением $\overline{\phi}(x)=1-\phi(x)$ для произвольной функции $\phi(x)$.

1. Время работы

Этот раздел посвящен работе двух антивирусных программ и построению характеристической функции уничтожения вирусов. Как будет видно далее, работа системы включает три этапа. Ниже будем пользоваться обозначением $F_\Theta(x)$ для функции распределения произвольной случайной величины Θ. Символом $\varphi_\Theta(t)$ обозначим характеристическую функцию произвольной случайной величины Θ. Для множества $B\in R^n$ обозначим символом $I_B(x_1,\dots,x_n)$ характеристическую функцию множества B.

1.1 Начало работы двух антивирусных программ

Так как сумма событий $\{a_1\theta_1^0\geq x\}\cup\{a_1\theta_1^0\geq x\}$ – достоверное событие, то

$$\overline{F}_{\Theta_0}(x)=\overline{F}_{\theta_1^0}\left(\frac{x}{a_1}\right)+P\left(\left\{0<\theta_1^0<\frac{x}{a_1}\right\}\{\Theta_1>x-a_1\theta_1^0\}\right)$$

Введем обозначения:

$$B=\left\{(x_1,x_2):\left\{0<x_1<\frac{x}{a_1}\right\}\wedge\{x_2>x-a_1x_1\}\right\}$$

$$B_1=\left\{(x_1):0<x_1<\frac{x}{a_1}\right\}$$

$$B_2=\{(x_1,x_2):x_2>x-a_1x_1\}$$

Несложно видеть, что справедливы равенства

$$\overline{F}_{\Theta_0}(x)=\overline{F}_{a_1\theta_1^0}(x)+\int_0^x\overline{F}_{\Theta_1}(x-y)dF_{a_1\theta_1^0}(y) \quad (1)$$

1.2 Количество уничтоженных вирусов за нечетное число шагов

Возьмем s — натуральное число. Для нечетного числа $k=2s+1$ рассмотрим функцию распределения времени Θ_k. Получим, что функция распределения F_{Θ_k} имеет вид

$$\overline{F}_{\Theta_k}(x)=\overline{F}_2^s\left(\frac{x}{a_2}\right)+P\left(\left\{0<\theta_2^s<\frac{x}{a_2}\right\}\{\Theta_{k+1}>x-a_2\theta_2^s\}\{\eta_1^{s+1}<\theta_2^s\}\right)$$

Построим новые множества

$$B=\left\{(x_1,x_2,x_3):\left\{0<x_1<\frac{x}{a_2}\right\}\wedge\{x_2>x-a_2x_1\}\wedge\{x_3<x_1\}\right\}$$

$$B_1=\left\{(x_1):0<x_1<\frac{x}{a_2}\right\}$$

$$B_2=\{(x_1,x_2):x_2>x-a_2x_1\}$$

$$B_3=\{(x_3,x_1):x_3<x_1\}$$

Несложно доказать, что

$$\overline{F}_{\Theta_{2s+1}}(x)=\overline{P}_{a_2\theta_2^s}(x)+\int_0^x\overline{F}_{\Theta_{2s+2}}(x-y)P_{a_2\eta_1^{s+1}}(y)dP_{a_2\theta_2^s}(y) \quad (2)$$

1.3 Количество уничтоженных вирусов за четное число шагов

Пусть s – натуральное число. Для $k=2s$ рассмотрим время Θ_k.

$$\overline{F}_{\Theta_{2s}}(x)=\overline{F}_{a_1\theta_1^s}(x)+\int_0^x\overline{F}_{\Theta_{2s+1}}(x-y)\cdot F_{a_1\eta_2^s}(y)dF_{a_1\theta_1^s}(y) \quad (3)$$

1.4 Система уравнений для работы

Объединяя равенства (1), (2), (3), получим систему интегральных уравнений

$$\begin{cases} \overline{F}_{\Theta_0}(x) = & \overline{F}_{a_1\theta_1^0}(x) + \int_0^x \overline{F}_{\Theta_1}(x-y)dF_{a_1\theta_1^0}(y) \\ & \dots \\ \overline{F}_{\Theta_{2s}}(x) = & \overline{F}_{a_1\theta_1^s}(x) + \int_0^x \overline{F}_{\Theta_{2s+1}}(x-y)F_{a_1\eta_2^s}(y)dF_{a_1\theta_1^s}(y) \\ \overline{F}_{\Theta_{2s+1}}(x) = & \overline{F}_{a_2\theta_2^s}(x) + \int_0^x \overline{F}_{\Theta_{2s+2}}(x-y)F_{a_2\eta_1^{s+1}}(y)dF_{a_2\theta_2^s}(y) \\ & \dots \end{cases} \quad (4)$$

Для $i = 1,2$ и $k = 0,1,2$ обозначим

$$\begin{aligned} \varphi_{\Theta_k}(w) = & \int_0^\infty e^{-wx}dF_{\Theta_k}(x) \\ \varphi_{a_i\theta_i^s}(w) = & \int_0^\infty e^{-wx}dF_{a_i\theta_i^s}(x) = M\left(e^{-wa_i\theta_i^s}\right) = \varphi_{\theta_i^s}(a_i w) \\ \varphi_{a_2\eta_1^{s+1},a_2\theta_2^s}(w) = & \int_0^\infty e^{-wx}F_{a_2\eta_1^{s+1}}(x)dF_{a_2\theta_2^s}(x) = \int_0^\infty e^{-wa_2\frac{x}{a_2}}F_{\eta_1^{s+1}}\left(\frac{x}{a_2}\right)dF_{\theta_2^s}\left(\frac{x}{a_2}\right) = \\ = & \int_0^\infty e^{-wa_2y}F_{\eta_1^{s+1}}(y)dF_{\theta_2^s}(y) = \varphi_{\eta_1^{s+1},\theta_2^s}(a_2w) \\ \varphi_{a_1\eta_2^s,a_1\theta_1^s}(w) = & \int_0^\infty e^{-wy}F_{a_1\eta_2^s}(y)dF_{a_1\theta_1^s}(y) = \int_0^\infty e^{-wa_1\frac{x}{a_1}}F_{\eta_2^s}\left(\frac{x}{a_1}\right)dF_{\theta_1^s}\left(\frac{x}{a_1}\right) = \\ = & \int_0^\infty e^{-wa_1y}F_{\eta_2^s}(y)dF_{\theta_1^s}(y) = \varphi_{\eta_2^s,\theta_1^s}(a_1w) \end{aligned} \quad (5)$$

Итак, получим систему уравнений

$$\begin{cases} \varphi_{\Theta_0}(w) - \varphi_{\Theta_1}(w)\varphi_{a_i\theta_i^s}(w) = 0 \\ \dots \\ \varphi_{\Theta_{2s}}(w) - \varphi_{\Theta_{2s+1}}(w)\varphi_{a_1\eta_2^s,a_1\theta_1^s}(w) = \varphi_{a_1\theta_1^s}(w) - \varphi_{a_1\eta_2^s,a_1\theta_1^s}(w) \\ \varphi_{\Theta_{2s+1}}(w) - \varphi_{\Theta_{2s+2}}(w)\varphi_{a_2\eta_1^{s+1},a_2\theta_2^s}(w) = \varphi_{a_2\theta_2^s}(w) - \varphi_{a_2\eta_1^{s+1},a_2\theta_2^s}(w) \\ \dots \end{cases} \quad (6)$$

Согласно условиям нашей задачи, случайные величины, являющиеся временем работы θ_i^s и временем ремонта η_i^s, не зависят от s. Далее, их будем обозначать через θ_i и η_i, соответственно.

Поэтому, в случае различных характеристик двух устройств, из последней системы имеем

$$\begin{cases} \varphi_{\Theta_0} - \varphi_{\Theta_1}\varphi_{a_1\theta_1} = 0 \\ \varphi_{\Theta_1} - \varphi_{\Theta_2}\varphi_{a_2\eta_1,a_2\theta_2} = \varphi_{a_2\theta_2} - \varphi_{a_2\eta_1,a_2\theta_2} \\ \varphi_{\Theta_2} - \varphi_{\Theta_1}\varphi_{a_1\eta_2,a_1\theta_1^s} = \varphi_{a_1\theta_1} - \varphi_{a_1\eta_2,a_1\theta_1} \end{cases} \quad (7)$$

Решая ее, согласно (5), имеем

$$\varphi_{\Theta_0} = \varphi_{a_1\theta_1}\frac{\begin{vmatrix} \varphi_{a_2\theta_2} - \varphi_{a_2\eta_1,a_2\theta_2} & \varphi_{a_2\eta_1,a_2\theta_2} \\ \varphi_{a_1\theta_1} - \varphi_{a_1\eta_2,a_1\theta_1} & \varphi_{a_1\eta_2,a_1\theta_1} \end{vmatrix}}{\begin{vmatrix} 1 & -\varphi_{a_2\eta_1,a_2\theta_2} \\ 1 & -\varphi_{a_1\eta_2,a_1\theta_1} \end{vmatrix}} =$$

$$= \varphi_{a_1\theta_1}\frac{(\varphi_{a_2\theta_2} - \varphi_{a_2\eta_1,a_2\theta_2})\varphi_{a_1\eta_2,a_1\theta_1} - (\varphi_{a_1\theta_1} - \varphi_{a_1\eta_2,a_1\theta_1})\varphi_{a_2\eta_1,a_2\theta_2}}{-\varphi_{a_1\eta_2,a_1\theta_1} + \varphi_{a_2\eta_1,a_2\theta_2}} =$$

$$= \varphi_{a_1\theta_1}(w)\frac{\varphi_{a_2\theta_2}(w)\varphi_{a_1\eta_2,a_1\theta_1}(w) - \varphi_{a_1\theta_1}(w)\varphi_{a_2\eta_1,a_2\theta_2}(w)}{-\varphi_{a_1\eta_2,a_1\theta_1}(w) + \varphi_{a_2\eta_1,a_2\theta_2}(w)} =$$

$$= \varphi_{\theta_1}(a_1w)\frac{\varphi_{\theta_2}(a_2w)\varphi_{\eta_2,\theta_1}(a_1w) - \varphi_{\theta_1}(a_1w)\varphi_{\eta_1,\theta_2}(a_2w)}{-\varphi_{\eta_2,\theta_1}(a_1w) + \varphi_{\eta_1,\theta_2}(a_2w)}$$

В случае совпадения характеристик двух устройств, когда случайные величины, являющиеся временем работы θ_i и временем ремонта η_i, не зависят от i, мы их будем обозначать через θ и η, соответственно. Также a_i будем обозначать через a. Поэтому, в случае совпадения характеристик двух устройств, из системы (6) имеем

$$\begin{cases} \varphi_{\Theta_0} - \varphi_{\Theta_1}\varphi_{a\theta} = & 0 \\ \varphi_{\Theta_1} - \varphi_{\Theta_1}\varphi_{a\eta,a\theta} = & \varphi_{a\theta} - \varphi_{a\eta,a\theta} \end{cases} \quad (8)$$

Решив ее, получим

$$\varphi_{\Theta_0}(w) = \varphi_{a\theta}(w)\frac{\varphi_{a\theta}(w) - \varphi_{a\eta,a\theta}(w)}{1 - \varphi_{a\eta,a\theta}(w)} =$$

$$= \varphi_\theta(aw)\frac{\varphi_\theta(aw) - \varphi_{\eta,\theta}(aw)}{1 - \varphi_{\eta,\theta}(aw)}. \quad (9)$$

2 Время восстановления

2.1 Восстановление антивирусной программы для нечетного k

Пусть s – натуральное число и ноль. Для $k = 2s + 1$ рассмотрим время Υ_k.

$$\{\Upsilon_k \geq x\} = \{\Upsilon_k \geq x\}\{b_1\eta_1^{s+1} \geq x\} +$$
$$+ \{\Upsilon_k \geq x\}\{0 < b_1\eta_1^{s+1} < x\} = \{b_1\eta_1^{s+1} \geq x\} +$$
$$+ \{0 < b_1\eta_1^{s+1} < x\}\{\Upsilon_k \geq x\}\{\eta_1^{s+1} > \theta_2^s\} +$$
$$+\{0 <_1 \eta_1^{s+1} < x\}\{\Upsilon_k \geq x\}\{\eta_1^{s+1} \leq \theta_2^s\} =$$
$$= \left\{\eta_1^{s+1} \geq \frac{x}{b_1}\right\} + \left\{0 < \eta_1^{s+1} < \frac{x}{b_1}\right\}\{\Upsilon_{k+1} \geq x -$$
$$- b_1\eta_1^{s+1}\}\{\eta_1^{s+1} \leq \theta_2^s\}.$$

Таким образом,

$$\overline{F}_{\Upsilon_k}(x) = \overline{F}_{\eta_1^{s+1}}\left(\frac{x}{b_1}\right) + P\left(\left\{0 < \eta_1^{s+1} < \frac{x}{b_1}\right\}\{\Upsilon_{k+1} \geq$$
$$\geq x - b_1\eta_1^{s+1}\}\{\theta_2^s \geq \eta_1^{s+1}\}\right).$$

Обозначим

$$B = \left\{(x_1, x_2, x_3): \left\{0 < x_1 < \frac{x}{b_1}\right\} \wedge \{x_2 > x - b_1x_1\} \wedge\right.$$
$$\left. \wedge \{x_3 \geq x_1\}\right\}$$
$$B_1 = \left\{(x_1): 0 < x_1 < \frac{x}{b_1}\right\}$$
$$B_2 = \{(x_1, x_2): x_2 > x - b_1x_1\}$$
$$B_3 = \{(x_3, x_1): x_3 \geq x_1\}$$

В этом случае получаем

$$\overline{F}_{\Upsilon_{2s+1}}(x) = \overline{F}_{b_1\eta_1^{s+1}}(x) + \int_0^x \overline{F}_{\Upsilon_{2s+2}}(x - y) \cdot$$
$$\cdot \overline{F}_{b_1\theta_2^s}(y)dF_{b_1\eta_1^{s+1}}(y) \qquad (10)$$

2.2 Восстановление антивирусной программы для четного k

Пусть s – натуральное число. Для $k = 2s$ рассмотрим время Υ_k.

Обозначим

$$B = \left\{(x_1, x_2, x_3): \left\{0 < x_1 < \frac{x}{b_2}\right\} \wedge \{x_2 > x -\right.$$
$$\left. - b_2x_1\} \wedge \{x_3 \geq x_1\}\right\}$$
$$B_1 = \left\{(x_1): 0 < x_1 < \frac{x}{b_2}\right\}$$
$$B_2 = \{(x_1, x_2): x_2 > x - b_2x_1\}$$
$$B_3 = \{(x_3, x_1): x_3 \geq x_1\}$$

В этом случае

$$\overline{F}_{\Upsilon_{2s}}(x) = \overline{F}_{b_2\eta_2^s}(x) + \int_0^x \overline{F}_{\Upsilon_{2s+1}}(x - y) \cdot$$
$$\cdot \overline{F}_{b_2\theta_1^s}(y)dF_{b_2\eta_2^s}(y) \qquad (11)$$

2.3 Система уравнений для ремонта

Объединяя равенства (11) и (10), получим систему интегральных уравнений

$$\begin{cases} \dots & \dots \\ \overline{F}_{\Upsilon_{2s+1}}(x) = & \overline{F}_{b_1\eta_1^{s+1}}(x) + \int_0^x \overline{F}_{\Upsilon_{2s+2}}(x - y)\overline{F}_{b_1\theta_2^s}(y)dF_{b_1\eta_1^{s+1}}(y) \\ \overline{F}_{\Upsilon_{2s}}(x) = & \overline{F}_{b_2\eta_2^s}(x) + \int_0^x \overline{F}_{\Upsilon_{2s+1}}(x - y)\overline{F}_{b_2\theta_1^s}(y)dF_{b_2\eta_2^s}(y) \\ \dots & \dots \end{cases} \qquad (12)$$

Для $i = 1,2$ и $k = 0,1,2$ обозначим

$$\varphi_{\Upsilon_k}(w) = \int_0^\infty e^{-wx}dF_{\Upsilon_k}(x)$$
$$\varphi_{b_i\eta_i^s}(w) = \int_0^\infty e^{-wx}dF_{b_i\eta_i^s}(x) = M\left(e^{-wb_i\eta_i^s}\right) = \varphi_{\eta_i^s}(b_iw)$$
$$\varphi_{b_1\overline{\theta}_2^s, b_1\eta_1^{s+1}}(w) = \int_0^\infty e^{-wx}\overline{F}_{b_1\theta_2^s}(x)dF_{b_1\eta_1^{s+1}}(x) = \int_0^\infty e^{-wb_1\frac{x}{b_1}}\overline{F}_{\theta_2^s}\left(\frac{x}{b_1}\right)dF_{\eta_1^{s+1}}\left(\frac{x}{b_1}\right) =$$
$$= \int_0^\infty e^{-wb_2y}\overline{F}_{\theta_2^s}(y)dF_{\eta_1^{s+1}}(y) = \varphi_{\overline{\theta}_2^s, \eta_1^{s+1}}(b_1w)$$
$$\varphi_{b_2\overline{\theta}_1^s, b_2\eta_2^s}(w) = \int_0^\infty e^{-wy}\overline{F}_{b_2\theta_1^s}(y)dF_{b_2\eta_2^s}(y) = \int_0^\infty e^{-wb_2\frac{x}{b_2}}\overline{F}_{\theta_1^s}\left(\frac{x}{b_2}\right)dF_{\eta_2^s}\left(\frac{x}{b_2}\right) =$$
$$= \int_0^\infty e^{-wb_2y}\overline{F}_{\theta_1^s}(y)dF_{\eta_2^s}(y) = \varphi_{\overline{\theta}_1^s, \eta_2^s}(b_2w)$$

В итоге получим систему уравнений

$$\begin{cases} \varphi_{\Upsilon_{2s+1}}(w) - \varphi_{\Upsilon_{2s+2}}(w)\varphi_{b_1\overline{\theta}_2^s, b_1\eta_1^{s+1}}(w) = & \dots \\ & \varphi_{b_1\eta_1^{s+1}}(w) - \varphi_{b_1\overline{\theta}_2^s, b_1\eta_1^{s+1}}(w) \\ \varphi_{\Upsilon_{2s}}(w) - \varphi_{\Upsilon_{2s+1}}(w)\varphi_{b_2\overline{\theta}_1^s, b_2\eta_2^s}(w) = & \varphi_{b_2\eta_2^s}(w) - \varphi_{b_2\overline{\theta}_1^s, b_2\eta_2^s}(w) \\ & \dots \end{cases} \qquad (13)$$

Согласно условиям нашей задачи, случайные величины, являющиеся временем работы Υ_i^s и временем ремонта η_i^s, не зависят от s. Далее их будем обозначать через Υ_i и η_i соответственно.

Поэтому, в случае различных характеристик двух устройств, из последней системы получаем

$$\begin{cases}\varphi_{\Upsilon_1} - \varphi_{\Upsilon_2}\varphi_{b_1\bar{\theta}_2,b_1\eta_1} = \varphi_{b_1\eta_1} - \varphi_{b_1\bar{\theta}_2,b_1\eta_1}\\ \varphi_{\Upsilon_2} - \varphi_{\Upsilon_1}\varphi_{b_2\bar{\theta}_1,b_2\eta_2} = \varphi_{b_2\eta_2} - \varphi_{b_2\bar{\theta}_1,b_2\eta_2}\end{cases} \quad (14)$$

Решая ее, получим

$$\varphi_{\Upsilon_1} = \frac{\begin{vmatrix}\varphi_{b_1\eta_1} - \varphi_{b_1\bar{\theta}_2,b_1\eta_1} & \varphi_{b_1\bar{\theta}_2,b_1\eta_1}\\ \varphi_{b_2\eta_2} - \varphi_{b_2\bar{\theta}_1,b_2\eta_2} & \varphi_{b_2\bar{\theta}_1,b_2\eta_2}\end{vmatrix}}{\begin{vmatrix}1 & -\varphi_{b_1\bar{\theta}_2,b_1\eta_1}\\ 1 & -\varphi_{b_2\bar{\theta}_1,b_2\eta_2}\end{vmatrix}} = \frac{\varphi_{b_1\eta_1}\varphi_{b_2\bar{\theta}_1,b_2\eta_2} - \varphi_{b_2\eta_2}\varphi_{b_1\bar{\theta}_2,b_1\eta_1}}{-\varphi_{b_2\bar{\theta}_1,b_2\eta_2} + \varphi_{b_1\bar{\theta}_2,b_1\eta_1}} =$$

$$= \frac{\varphi_{\eta_1}(b_1w)\varphi_{\bar{\theta}_1,\eta_2}(b_2w) - \varphi_{b_2\eta_2}(b_2w)\varphi_{\bar{\theta}_2,\eta_1}(b_1w)}{-\varphi_{\bar{\theta}_1,\eta_2}(b_2w) + \varphi_{\bar{\theta}_2,\eta_1}(b_1w)}.$$

В случае совпадения характеристик двух устройств, когда случайные величины, являющиеся временем работы Υ_i и временем ремонта η_i, не зависят от i, мы их будем обозначать через Υ и η соответственно. Также b_i будем обозначать через b. Поэтому, в случае совпадения характеристик двух устройств, из системы (6) имеем

$$\varphi_{\Upsilon_1} - \varphi_{\Upsilon_1}\varphi_{b\bar{\theta},b\eta} = \varphi_{b\eta} - \varphi_{b\bar{\theta},b\eta} \quad (15)$$

Решая ее, получим

$$\varphi_{\Upsilon_1}(w) = \frac{\varphi_{b\eta}(w) - \varphi_{b\bar{\theta},b\eta}(w)}{1 - \varphi_{b\bar{\theta},b\eta}(w)} = \frac{\varphi_{\eta}(bw) - \varphi_{\bar{\theta},\eta}(bw)}{1 - \varphi_{\bar{\theta},\eta}(bw)} \quad (16)$$

3. Окончание

Пользуясь формулами (9) и (16) найдем математическое ожидание случайной величины $\Theta - \Upsilon_1$.

$$\varphi_{\Upsilon_1}(w) = \frac{\varphi_{\eta}(bw) - \varphi_{\bar{\theta},\eta}(bw)}{1 - \varphi_{\bar{\theta},\eta}(bw)}$$

$$\ln\left(\varphi_{\Upsilon_1}(w)\right) = \ln\left(\varphi_{\eta}(bw) - \varphi_{\bar{\theta},\eta}(bw)\right) - \ln\left(1 - \varphi_{\bar{\theta},\eta}(bw)\right)$$

$$\frac{\varphi^*_{\Upsilon_1}(w)}{\varphi_{\Upsilon_1}(w)} = \frac{\varphi^*_{\eta}(bw) - \varphi^*_{\bar{\theta},\eta}(bw)}{\varphi_{\eta}(bw) - \varphi_{\bar{\theta},\eta}(bw)}b + \frac{\varphi^*_{\bar{\theta},\eta}(bw)}{1 - \varphi_{\bar{\theta},\eta}(bw)}b$$

$$\varphi^*_{\Upsilon_1}(0) = \frac{\varphi^*_{\eta}(0) - \varphi^*_{\bar{\theta},\eta}(0)}{1 - \varphi_{\bar{\theta},\eta}(0)}b + \frac{\varphi^*_{\bar{\theta},\eta}(0)}{1 - \varphi_{\bar{\theta},\eta}(0)}b = \frac{b\varphi^*_{\eta}(0)}{1 - \varphi_{\bar{\theta},\eta}(0)}$$

$$M(\Upsilon_1) = \frac{bM(\eta)}{1 - \varphi_{\bar{\theta},\eta}(0)} = \frac{bM(\eta)}{1 - \int_0^{\infty}\overline{F}_{\theta}(y)dF_{\eta}(y)} = \frac{bM(\eta)}{1 - P(\theta \geq \eta)} = \frac{bM(\eta)}{P(\theta < \eta)}$$

Аналогично,

$$\varphi_{\Theta_0}(w) = \varphi_{\theta}(aw)\frac{\varphi_{\theta}(aw) - \varphi_{\eta,\theta}(aw)}{1 - \varphi_{\eta,\theta}(aw)}$$

$$\ln\left(\varphi_{\Theta_0}(w)\right) = \ln\left(\varphi_{\theta}(aw) - \varphi_{\eta,\theta}(aw)\right) - \ln\left(1 - \varphi_{\eta,\theta}(aw)\right)$$

$$\frac{\varphi^*_{\Theta_0}(w)}{\varphi_{\Theta_0}(w)} = \frac{\varphi^*_{\theta}(aw) - \varphi^*_{\eta,\theta}(aw)}{\varphi_{\theta}(aw) - \varphi_{\eta,\theta}(aw)}b + \frac{\varphi^*_{\eta,\theta}(aw)}{1 - \varphi_{\eta,\theta}(bw)}b$$

$$\varphi^*_{\Theta_0}(0) = \frac{\varphi^*_{\theta}(0) - \varphi^*_{\eta,\theta}(0)}{1 - \varphi_{\eta,\theta}(0)}a + \frac{\varphi^*_{\eta,\theta}(0)}{1 - \varphi_{\eta,\theta}(0)}a = \frac{a\varphi^*_{\theta}(0)}{1 - \varphi_{\eta,\theta}(0)}$$

$$M(\Theta_0) = \frac{aM(\theta)}{1 - \varphi_{\eta,\theta}(0)} = \frac{aM(\theta)}{1 - \int_0^{\infty}F_{\eta}(y)dF_{\theta}(y)} = \frac{aM(\theta)}{1 - P(\eta < \theta)} = \frac{aM(\eta)}{P(\eta \geq \theta)}$$

Без ограничения общности можно считать, что периоды времени восстановления и работы антивирусных программ — абсолютно непрерывные случайные величины и $P(\{\eta = \theta\}) = 0$. В этом случае

$$M(\Theta_0 - \Upsilon_1) = M(\Theta_0) - M(\Upsilon_1) = \frac{aM(\theta) - bM(\eta)}{P(\eta > \theta)}$$

Таким образом, можно сильно увеличить количество уничтоженных вирусов, если обеспечить $P(\eta > \theta)$ близкой к нулю, то есть уменьшить вре-

мя восстановления. Одновременно должно выполняться условие $aM(\theta) - bM(\eta) > 0$. Самый лучший вариант — обеспечить наибольшее положительное значение величины $aM(\theta) - bM(\eta)$, то есть увеличить количество уничтоженных вирусов и уменьшить время восстановления системы из двух программ.

Пример

Пусть обратная к функции распределения случайной величины η имеет показательное распределение, точнее вид $P(\eta > t) = \exp(-\lambda t)$ для некоторого $\lambda > 0$.

Кроме того, обратная к функции распределения случайной величины θ будет иметь показательное распределение, точнее вид $P(\theta > t) = \exp(-\mu t)$ для некоторого $\mu > 0$.

В этом случае из независимости случайных величин η и θ имеем

$P(\eta > \theta) = \int_{-\infty}^{\infty} P(\eta > \theta | \theta = t) f_\theta(t) dt = \int_{-\infty}^{\infty} P(\eta >$

$> t) f_\theta(t) dt = \mu \int_0^{\infty} \exp(-\lambda t) \exp(-\mu t) dt = \mu \int_0^{\infty} \exp(-$

$-(\lambda + \mu)t) dt = \frac{\mu}{\mu+\lambda}$

$$M(\eta) = \frac{1}{\lambda} \qquad M(\theta) = \frac{1}{\mu}$$

Окончательно получим

$$M(\Theta_0 - \Upsilon_1) = \frac{aM(\theta) - bM(\eta)}{P(\eta > \theta)} = \frac{a\frac{1}{\mu} - b\frac{1}{\lambda}}{\frac{\mu}{\mu+\lambda}} = \left(\frac{a}{\mu} - \frac{b}{\lambda}\right) \cdot$$

$$\cdot \left(1 + \frac{\lambda}{\mu}\right) = \left(\frac{a}{\mu} - \frac{b}{\lambda}\right)\left(1 + \frac{\frac{1}{\mu}}{\frac{1}{\lambda}}\right) = (aM(\theta) -$$

$$- bM(\eta))\left(1 + \frac{M(\theta)}{M(\eta)}\right)$$

Отсюда видно, что для того, чтобы сделать величину $M(\Theta_0 - \Upsilon_1)$ достаточно большой, можно выбрать варианты — достигнуть выполнения условий

$$aM(\theta) \gg bM(\eta), \qquad \frac{M(\theta)}{M(\eta)} \gg m$$

для некоторого достаточно большого m. Можно добиться выполнения двух условий, но выполнение второго позволяет достичь гораздо больших результатов, если сделать среднее время $M(\eta)$ близким нулю, не уменьшая среднее $M(\theta)$.

Здесь также отметим, что для получения наиболее качественных оценок математического ожидания на основе экспериментальных данных удобно пользоваться распределением Стьюдента.

ЗАКЛЮЧЕНИЕ

Использование антивирусной системы защиты с двойной архитектурой, когда при остановке основной антивирусной программы резервный антивирус переходит из спящего режима в активный, является целесообразным. Такая архитектура позволит оптимизировать время работы и восстановления программ, что, в свою очередь, позволит обеспечить повышение эффективности антивирусной системы и, в конечном итоге, значительно увеличить количество уничтоженных вирусов.

Следует отметить, что подобная двуслойная архитектура антивирусной системы защиты предприятия может быть особенно необходима в условиях высоких требований к отказоустойчивости систем и защите от целевых атак злоумышленников на антивирусную систему в целом.

СПИСОК ЛИТЕРАТУРЫ

1. Smirnov S.I., Eremeev M.A., Magomedov S.D., Izergin D.A. Критерии и показатели оценивания качества проведения расследования инцидента информационной безопасности при целевой кибератаке // Russian Technological Journal. 2024. Т.12. №3. С.25-36. DOI: 10.32362/2500-316x-2024-12-3-25-36. EDN: LNWLOK.

2. Корчагин И.И. и др. Формализованное представление целевой функции воздействия вредоносного программного обеспечения на операционную среду автоматизированной системы управления специального назначения // Безопасность информационных технологий. 2024. Т.31. №2. С.42–50.

3. Иванов М.А. Стохастические методы защиты информации // Безопасность информационных технологий. Т.31. №3. С.83-93. DOI: 10.26583/bit.2024.3.03. EDN: RWJLVX.

4. Калашников А.О., Бугайский К.А., Аникина Е.В. и др. Применение логико-вероятностного метода в информационной безопасности. Часть 3 // Вопросы кибербезопасности. 2023. №6(58). С.20-34. DOI: 10.21681/2311-3456-2023-6-20-34. EDN: PHUZNU.

5. Калашников А.О., Аникина Е.В., Бугайский К.А. и др. и др. Применение логико-вероятностного метода в информационной безопасности. Часть 4 // Вопросы кибербезопасности. 2024. №3(61). С.23-32. DOI: 10.21681/2311-3456-2024-3-23-32. EDN: BTWVJL.

6. Калашников А.О., Аникина Е.В., Бугайский К.А. и др. Применение логико-вероятностного метода в информационной безопасности. Часть 5 // Вопросы кибербезопасности. 2024. № 4(62). С. 26-37. DOI: 10.21681/2311-3456-2024-4-26-37. EDN: SRDVSA.

УДК: 004.8, 130.2

Угрозы манипулирования сознанием посредством цифровой виртуальной реальности

P.G. Bylevskiy

Threats of Mind Manipulation Through Digital Virtual Reality

Abstract. *The article is devoted to the threats of mind manipulation through digital "virtual reality" services. The sources of threats are unfair competition from the owners of global digital services and the policies of their home countries that are unfriendly to Russia. The methodological basis is idealistic mechanism, the representation of objective reality (nature, society and personality) as techniques of varying degrees of complexity. Such developments, losing in effectiveness to the technical means of classical culture and psychotropic substances, are used for aggressive marketing in order to obtain irrevocable government, corporate and investment financing. A virtual Reality based on the primitives of mass culture can surpass the attractiveness of the real world only with a critical decrease in the cultural level of users. The conclusion is drawn: domestic developments of digital "virtual reality" services should aim at the socio-cultural development of citizens and society based on traditional Russian values.*

Keywords: *virtual reality, digital services, information security, dialectical materialism, mechanistic idealism, cultural technology, computer simulation, socio-cultural development, traditional values.*

П.Г. Былевский
Кандидат философских наук, доцент ВАК 2.3.6. «Методы и системы защиты информации, информационная безопасность», доцент кафедры международной информационной безопасности Московского государственного лингвистического университета, старший преподаватель Российского государственного социального университета
E-mail: pr-911@yandex.ru

Аннотация. *Статья посвящена угрозам манипулирования сознанием посредством цифровых сервисов «виртуальной реальности». Источниками угроз являются недобросовестная конкуренция со стороны владельцев глобальных цифровых сервисов и недружественная России политика стран их базирования. Методологической основой служит механистический идеализм, представление объективной реальности (природы, общества и личности) как техники разной степени сложности. Подобные разработки, проигрывая в эффективности техническим средствам классической культуры и психотропным веществам, используются для агрессивного маркетинга в целях получения безвозвратного государственного, корпоративного и инвестиционного финансирования. Виртуальная реальность, основанная на примитивах массовой культуры, может превосходить привлекательностью реальный мир лишь при критическом снижении культурного уровня пользователей. Делается вывод: отечественные разработки цифровых сервисов «виртуальной реальности» должны нацеливаться на социально-культурное развитие граждан и общества на основе традиционных российских ценностей.*

Ключевые слова: *виртуальная реальность, цифровые сервисы, информационная безопасность, диалектический материализм, механистический идеализм, технические средства культуры, компьютерная имитация, социально-культурное развитие, традиционные ценности.*

ВВЕДЕНИЕ

Компьютерная «виртуальная реальность» как популярный и считающийся перспективным цифровой сервис является социально-культурным феноменом со специфическими рисками информационной безопасности. «Виртуальная реальность» (VR) относится наряду с дополненной (Augmented Reality, AR) и смешанной (Mixed reality, MR) реальностью к расширенной реальности (Extended reality, XR), представленной в решениях Metaverse, Microsoft HapticLinks, Cave, AlloSphere, Teslasuit, VRealizer и др.

Эти разработки глобальных высокотехнологических компаний представляют собой программно-аппаратные комплексы и контент для обмана чувств пользователей интернет-коммуникаций. Пользовательское оборудование включает очки- и шлемы-мониторы, наушники объёмного звучания, перчатки и костюмы-тренажёры с имитаторами прикосновений и внешних воздействий, датчиками движений и встроенными джойстиками, «принтеры» — синтезаторы запахов и вкусов и подобные периферийные устройства.

Разработчики декларировали, что компьютерная «виртуальная реальность» превзойдёт достоверностью и привлекательностью не только прежний мультимедийный контент, компьютерные симуляторы и игры, но и возможности технических средств традиционной культуры, а также объективную реальность как таковую. Виртуальная реальность, таким образом, должна превратиться в «цифровой рай», лучший мир, заменяющий и компенсирующий несовершенства людей, общества, природы и Вселенной в целом.

Но уже в 2022 году наблюдался кризис доверия к компьютерной «виртуальной реальности»: падение массового интереса, отток инвестиций, снижение курсов акций и значительные убытки инвесторов. Проявилась потребность в философско-культурном методологическом анализе реалистичности деклараций и прогнозов разработчиков, реальных возможностей, угроз и рисков компьютерно-сетевых средств сенсорной симуляции и обмана чувств [1].

ЦИФРОВИЗАЦИЯ И ЭВОЛЮЦИЯ ТЕХНИЧЕСКИХ СРЕДСТВ МИРОВОСПРИЯТИЯ

Компьютерную «виртуальную реальность» не случайно относят к технологиям «искусственного интеллекта», поскольку важнейшим результатом применения высоких технологий выступает «сенсорная» имитация, симуляция ощущений, создание иллюзии окружающего мира и, тем самым, виртуализация мировосприятия.

Анализу действительных и мнимых возможностей «виртуальной реальности» помогут соотнесение деклараций разработчиков с практикой применения и сравнение с достижением похожих результатов при помощи других средств, включая «традиционное» искусство, эстрадный иллюзионизм, мошенничество, рекламу и пропаганду. Философско-культурологический анализ цифровой «виртуальной реальности» позволяет выявить несколько «слоёв», уровней имитации действительности, способных использоваться злоумышленниками для извлечения выгоды за счёт нанесения ущерба различным чужим ценностям высоких уровней.

Неожиданные убытки проекта Metaverse, самой масштабной и популярной разработки технологий «виртуальной реальности», за III квартал 2022 года составили $3,7 млрд, а за 9 мес. достигли $9,4 млрд[1]. Публикация отчёта сопровождалась падением курса акций на биржевых торгах на 24%[2].

Разочарование, падение массового интереса и отток инвестиций переживали аналогичные высокотехнологичные разработки Cave, AlloSphere, Teslasuit, VRealizer, Microsoft Haptic Links и др. Обещания разработчиков и оптимистические прогнозы экспертов не реализовались, а усиленная медиа-поддержка проектов цифровой «виртуальной реальности» перестала действовать. Неудачи, преследующие разработки «виртуальной реальности», объясняются не столько технологическими, сколько социально-культурными факторами.

С точки зрения классической философской методологии и теории культуры неудачи были изначально заложены преувеличением возможностей компьютерной симуляции реального мира посредством новых компьютерных спецэффектов, пользовательских интерфейсов, оборудования, программного обеспечения и мультимедийного контента.

Замысел создания компьютерной «виртуальной реальности», решающим образом превосходящей окружающую человека среду, обстановку и объективный мир в целом, изначально содержал критические методологические уязвимости. При этом компьютерная «виртуальная реальность» представляет собой не что иное, как совокупность современных высокотехнологичных средств воздействия на сознание и действия человека, образ жизни людей и сообществ.

Вместе с тем природа сознания, личности и человеческих отношений не техническая и даже не «биологическая», а социально-культурная, необходимо предполагающая саморазвитие и свободу воли. Техника является всего лишь неживой материей, созданной (преобразованной) людьми, используемой человеком как инструмент и предмет труда для удовлетворения своих потребностей. За пределами техники находится мир неживой материи, пока ещё недоступной и необработанной человеком, живые организмы и биосфера в целом, а также сами люди. С помощью технических средств люди могут создавать для себя и других убедительные образы, модели, имитации и иллюзии любых предметов и процессов, осуществляя локально и временно убедительную подстановку, подмену.

Сами по себе технические средства создания иллюзий не способны полностью, убедительно и достоверно заменить единую и целостную объективную реальность, истина которой может проявляться даже в отдельных фактах, событиях и действиях. При наличии конфликтов и антагонизмов разных комбинаций общественных и личностных интересов любые технические средства создания образов, иллюзий и имитации могут использоваться людьми как для созидательной совместной деятельности, так и для обмана, введения в заблуждение, извлечения выгоды нанесением ущерба другим людям.

Критический философско-культурный методологический анализ гипотетических и предполагаемых возможностей, а также реальных применений компьютерной «виртуальной реальности», сопутствующих рисков и социально-культурных последствий позволяет их разделить на ошибочные и ложные.

[1]META After-Hours Quotes. Meta Platforms, Inc. Class A Common Stock (META) / Nasdaq, Inc. 30.10.2022 URL: https://www.nasdaq.com/market-activity/stocks/meta/ after-hours (дата обращения: 25.01.2025).

[2]McQuaid D. Zuck out of luck: Facebook's Meta hit with $3.7bn third-quarter metaverse losses / Capital.com. 27 October 2022. URL: https://capital.com/meta-zuckerberg-metaverse-2022-third-quarter-losses (дата обращения: 25.01.2025).

На основе культурно-исторического и субъектно-деятельностного подходов к человеческим ощущениям, восприятиям, чувствам и эмоциям компьютерную «виртуальную реальность» можно определить в качестве цифрового технического средства для создания, трансляции и потребления мультимедийного (и другого мультимодального) контента. Таким путём может быть решена задача критической оценки возможных угроз и сопутствующих рисков, а также перспектив созидательных применений этого нового высокотехнологичного цифрового массового сервиса.

К традиционным техническим средствам воздействия, позволяющим изменить сознание, расширить познание реально или ложно, иллюзорно, можно отнести неживые предметы и процессы. В этом отношении компьютерные имитации реальности, обстановки, среды и мира в целом находятся в том же ряду, что и технические инструменты, материалы художественного, социального и правового творчества, прессы, педагогики, организации и проведения массовых мероприятий и зрелищ, но также и психотропные препараты и другие предметы, используемые для формирования деструктивных зависимостей.

Как техническое средство воздействия на человека, изменения его сознания, поведения, образа жизни и личности, разработки «виртуальной реальности» полностью соответствуют концепции NBIC(S)-конвергенции, нацеленной на разрешение фундаментальных проблем человечества при приоритете высокотехнологичных исследований, разработок и решений разных направлений (нано-, био, информационных, когнитивных и социальных) [2].

Проект создания компьютерной «виртуальной реальности» с перспективами «переселения» в неё значительной части человечества как пользователей носит фундаментальный смысл, представляющий определённое мировоззрение. Цифровая «виртуализация реальности» посредством публичных массовых интернет-сервисов предполагает специфическое понимание как разработчиками, так и потенциальными пользователями объективной реальности, природы, общества, человека, человеческих отношений, а также целей, путей и средств их развития, преобразования.

Запрос на создание компьютерной имитации «лучшего мира» подменяет и небесный рай религии, и коммунистический «рай на земле», предполагая возможность посредством новой продвинутой техники обеспечить пользователям иллюзию полного тождества «сенсорных ощущений», восприятия с воспринимаемой объективной реальностью.

Невыполнение обещаний разработчиков Metaverse создать убедительную и привлекательную для всех компьютерную «виртуальную реальность», отсутствие роста пользователей, при всей рекламно-маркетинговой поддержке, знаменует неудачу «виртуализации» мировосприятия массовых пользователей и большинства граждан, обнажает критические методологические уязвимости всей концепции NBIC(S)-конвергенции.

Проявилась несостоятельность представлений о возможности решения самых острых и масштабных социально-культурных проблем с помощью только высоких технологий, маскировки общественных имущественных, классовых и международных противоречий, свойственных рыночному глобализму, пренебрежение конкретно-исторической субъектностью человека [3]. Препятствия, казавшиеся разработчикам Metaverse несущественными, оказались гносеологически непреодолимыми, что, с точки зрения классической философии и теории культуры, вполне предсказуемо.

Классическая философская гносеология, не механистическая, а социально-культурная, констатирует невозможность полноценно «обманывать» техническими средствами ощущение и восприятие, имитировать внешние для человека предметы, обстановку, среду, представляющие всю объективную реальность. Успех в подобном может достигаться локально, точечно, кратковременно: в специально созданных лабораторных условиях в отношении доверчивых, внушаемых испытуемых. Наиболее легка имитация ощущений «внешних» органов чувств — зрения, слуха, обоняния, вкуса и осязания, на которые ориентирована компьютерная «виртуальная реальность» [4].

Программно-аппаратные «устройства ввода и вывода данных» созданы только для зрения и слуха — внешних, «дистанционных» чувств, а также для осязания: очки-мониторы стереоизображений и сферического обзора; наушники со стерео, квадро- и др. объёмным звуком; ручные манипуляторы, джойстики, кресла-сидения и «умные скафандры», имитирующие воздействия на внешние предметы, их инерцию и сопротивление.

Компьютерная имитация пока не достигла уровня химического синтеза, применяемого для усиления и имитации вкусов в гастрономии, запахов в парфюмерии [5]. Ещё более в программно-аппаратном плане проблематична полноценная компьютерная имитация осязательных ощущений пользователя [6], не говоря уже о действиях с внешними предметами в «полевых», а не «лабораторных» условиях.

Следующим препятствием успеху компьютерной имитации реальности посредством аппаратно-программных решений выступает сначала принципиальная, а уже потом техническая и финансовая неспособность конкурировать с «традиционными» средствами формирования и «переформатирования» сознания, восприятий и даже ощущений: культурой и искусством, правом, нравственностью и моралью, прессой и межличностным общением. Все эти виды социально-культурной деятельности осуществляются людьми в отношении себя и других людей как посредством только человеческой телесности, так и с использованием «традиционных», «докомпьютерных» технических средств, инструментов и материалов, предметов и документов культуры.

ЗНАЧЕНИЕ КОНЦЕПЦИИ ВИРТУАЛЬНОЙ РЕАЛЬНОСТИ В ПРОЦЕССАХ ГЛОБАЛИЗАЦИИ

Компьютерные технологии любой сложности сами по себе неспособны производить ни знания, ни заблуждения, ни имитации и иллюзии. Их создают и используют только люди для себя или для других людей. Цели, характер и методы использования технических средств могут различаться до полярной противоположности: от солидарной совместной деятельности в общих интересах до противоборства, войны на взаимное уничтожение. Иллюзии и имитации, условности и метафоры могут создаваться и применяться для лучшего понимания и взаимопонимания, художественного и научного познания, моделирования, тренировки и т.п., но также в деструктивных целях обмана, мошенничества, дезинформации, фальсификации, провокаций и т.д.

В настоящий момент лидерами в развитии наукоёмких высоких компьютерных технологий, как и всего комплекса, обозначаемого аббревиатурой NBIC(S)-конвергенции, являются глобальные транснациональные цифровые корпорации, базирующиеся в США. Определение создаваемой компьютерной «виртуальной реальности» (контента и воздействий на пользователей) интересами владельцев, разработчиков и поставщиков этих сервисов и страны их базирования [7] ведёт к тому, что главным критерием успешности оказываются корпоративные прибыли.

В связи с этим компьютерная виртуализация мировоззрения в значительной степени осуществляется для маскировки ухудшения положения и усиления эксплуатации, а не для всестороннего творческого развития пользователей.

Системный кризис однополярного глобализма проявляется в разных сферах: экономике, политике, международных отношениях. «Виртуализации» подвергается сама действительность, повседневная жизнь «массового человека». Происходит снижение уровня жизни, подмена самого необходимого недорогими суррогатами: продвижением престижа «чайлдфри» (бездетности), разрушения семьи и родственных отношений, сокращения рождаемости ниже порога воспроизводства народонаселения, снижения гражданами потребления электроэнергии, подмена натурального питания синтезированным и низкокачественным, вытеснения личной собственности арендой и «пользованием» [8].

С помощью современных технологий многие виды развлечений для современного общества предельно удешевляются, при этом их качество снижается. Ухудшение реальной жизни должна маскировать и «компенсировать» компьютерная «виртуальная реальность», в реальности которой массового пользователя приходится убеждать дополнительно агрессивным маркетингом и рекламой.

«Компьютерная» иллюзорность превращается в многоуровневый феномен, далеко не только компьютерный: для убеждения инвесторов и пользователей разработчики «виртуальной реальности» сильно преувеличивают возможности «мультимедийных тренажёров» имитировать «цифровой лучший мир» как якобы необычайно улучшенную окружающую среду, симулировать небывало сильные приятные ощущения, положительные эмоции и настроения пользователей. Так формируется представление о потребительском «рае для каждого», «цифровой утопии» — жизни без горестей и трудностей, печалей и болезней, полной лишь успеха, развлечений и наслаждений.

Проект цифровой «виртуальной реальности» может быть квалифицирован как квазиутопия или псевдоутопия, поскольку его разработчики и специалисты по маркетингу претендуют на более высокие продуктивность и эффективность, чем первобытные стихии, боги древних мифологий и мировых религий. «Пробниками» «цифрового» искушения выступают преимущества дистанционных интернет-сервисов, мультимедийные развлечения и игры, действительно поглощающие всё больше внимания и времени увеличивающегося количества пользователей.

О ФОРМИРОВАНИИ МЕХАНИСТИЧЕСКОГО ПОДХОДА К СРЕДСТВАМ СОЗДАНИЯ ВИРТУАЛЬНОЙ РЕАЛЬНОСТИ

Декларации разработчиков компьютерной «виртуальной реальности небезупречны, спорны и во

многом уязвимы для критики, поскольку сами являются своеобразным социально-культурным феноменом в контексте далеко не только научно-технических и гуманитарных исследований, но и государственного и корпоративного финансирования, прибылей поставщиков интернет-сервисов, возможностей извлекать выгоду из манипуляций сотнями миллионов пользователей и, косвенно, всем человечеством.

Обоснованно возникает вопрос о степени «искренности» владельцев и разработчиков: о соотношении досадных ошибок, добросовестных заблуждений и циничного расчёта на манипулирование сознанием государственных чиновников, экспертов, инвесторов, пользователей для убеждения их в «подлинности» компьютерной «виртуальной действительности» [9].

Фундаментальной методологической уязвимостью исходных установок рассматриваемых разработок в отношении перспектив создания виртуального «лучшего мира» для человечества является механицизм, представление об объективной реальности — Вселенной, природе, живых организмах, обществе и его истории, о человеке, его способностях — как о неживых предметах и процессах: механизмах, машинах, системах машин, включая электронно-вычислительные сети.

Философскими предшественниками современного «компьютерного» механистического идеализма следует считать концепции Нового времени — И. Ньютона и Р. Декарта, Дж. Беркли и Д. Юма, эмпириокритицизм физика Э. Маха — психиатра Р. Авенариуса на рубеже XIX—XX вв, эмпириомонизм и тектологию А.А. Богданова, теорию систем Л. Берталанфи, «теорию информации» и кибернетику Н. Винера, современную «философию искусственного интеллекта» с «надстройкой» концепции NBIC(S)-конвергенции.

Такое мировоззрение использует как матрицу для понимания всей объективной реальности капиталистическое серийное машинное производство, создающее по единому штампу, шаблону много аналогичных друг другу экземпляров изделия, все из которых являются подлинными.

Улучшение машины, сырья и заготовок, получаемой продукции, создание новых, во всём превосходящих предшествующие, достигаются преимущественно организационно-техническими средствами. Конструктор-производитель механизмов и машин практически всевластен над своими неживыми творениями в локальных, ограниченных во времени и пространстве условиях, наподобие «бога-механика» философии деизма. Создатель «виртуальной реальности» не просто делает новую занятную игрушку, иллюзионный эстрадный номер, но конструирует компьютерный симулятор, как бы превосходящий религиозный рай, построение коммунизма и все прочие попытки улучшить объективный мир.

Развитие с 1940-х годов электронно-вычислительной техники, автоматизации и роботизации промышленных, деловых и социальных процессов в условиях обострения общественных противоречий и противоборства мировых систем социализма и капитализма сопровождалось появлением кибернетики, вскоре заменённой «философией искусственного интеллекта».

ТЕСТ ТЬЮРИНГА: УРОВНИ И ВОЗМОЖНОСТИ

Ключевым, базовым для этой философской школы и связанных научно-технических компьютерных исследований и разработок стал вопрос о том, «способна ли машина мыслить». Критерием «машинного мышления» объявили классический «тест Тьюринга», в ходе которого тестирующий сравнивает письменные ответы на свои вопросы, пытаясь угадать, даны они человеком или сгенерированы компьютером. Неспособность человека, проводящего тест, отличить по письменным ответам автора-человека от компьютерной имитации считается доказательством способности машины «мыслить».

Однако точно так же успех эстрадного иллюзиониста у доверчивой аудитории можно считать достоверным доказательством способности творить чудеса. Тождество образа и изображаемого, иллюзии и реальности, искусной подделки и подлинника возможно, но лишь в узких локальных пространственно-временных границах специфических социально-культурных взаимоотношений доверителя и доверяющего, художника и поклонников, мошенника и жертвы обмана. Электронно-вычислительная машина способна мыслить в воображении того, кто считает такое возможным, приравнивая человека к машине, автомату, неживому предмету, пусть и очень сложно сделанному.

С точки зрения философской методологии диалектического материализма и классической теории культуры «тест Тьюринга» рационально трактуется как состязание тестирующего и «компьютерного иллюзиониста». Электронно-вычислительная машина и программное оборудование являются такими же техническими инструментами соревнования в обмане и его распознавании, как мяч, поле и ворота — средствами игры в футбольном матче.

Дополнительно тестом Тьюринга может проверяться и оцениваться неспособность тестирующего различить человека и неживой предмет, а также мастерство «компьютерных иллюзионистов» в эксплуатации этой уязвимости противника. Отдельно возможно оценить, в какой степени тестирующий был введён в заблуждение, а в какой оказался жертвой самообмана. Подобный самообман может быть свойственен и самим «компьютерным иллюзионистам», и «философам искусственного интеллекта». Нельзя исключить при определённых обстоятельствах добровольного искреннего полного «переселения» в компьютерную «виртуальную реальность» самих её создателей.

По мере развития электромеханической автоматизации различных технических средств, инструментов для удовлетворения всё более обширного перечня человеческих потребностей и развития способностей, тест Тьюринга получал всё новые и новые потенциальные применения. Убедительность, достоверность, правдоподобность, похожесть на настоящее, высокое качество подделки стало можно имитировать с помощью компьютерного оборудования для промышленной продукции, продуктов питания и обстановки, личностей и организаций, социально-культурных ценностей, человеческих мыслей, ощущений и впечатлений, поступков, поведения и образа жизни.

Тест Тьюринга применим для оценки эффективности, правдоподобности, убедительности для целевой аудитории имитации с помощью программно-аппаратных средств не только других людей, но и любых предметов, процессов, обстановки, растений и животных, пейзажей и явлений природы, всей Вселенной [10]. Компьютерные «сенсорные» технологии представляют собой, с одной стороны, оцифровку параметров предметов и процессов, с другой стороны — представление их цифровых кодов с помощью компьютерного оборудования в ощущаемом виде, в чувственно воспринимаемых образах.

К ВОПРОСУ О КОРРЕКТНОСТИ ПРИМЕНЕНИЯ ОСНОВНЫХ ТЕРМИНОВ

Получение, оцифровку, передачу и обработку данных о звуковых, оптических, химических и других процессах стали называть «компьютерными» зрением и слухом, вкусом и обонянием. На техническое средство переносится человеческая способность чувственного восприятия объективной реальности, хотя компьютер способен «видеть» не более, чем лупа или палочка-щуп слепого человека, которым тот проверяет дорогу, по которой идёт.

К простым техническим «сенсорным» средствам можно отнести микроскоп и телескоп, термометр и обычные часы, «визуализирующие» для человека скорость течения времени. Антропоморфные компьютерные аналогии ещё не распространяются на преобразованное представление в чувственно воспринимаемом и понятном для человека виде явлений, непосредственно недоступных органам человеческих чувств без технических инструментов: электромагнитных излучений, радиации и невидимых зон оптического спектра, неслышимых инфра- и ультразвуковых колебаний и т.д. Но их «визуализация» принципиально не сложнее, чем сказочных персонажей.

Сетевые компьютерные программно-аппаратные системы для обработки, структурирования, передачи и хранения данных об объективной реальности, природе, обществе, технике и человеке являются автоматизированными электронными библиотеками, каталогами и реестрами, но причисляются к технологиям «искусственного интеллекта» [11].

В случаях истинного научного познания, допускающего временную неполноту и ошибки, корректно название «автоматизированные электронно-вычислительные технические средства человеческого познания». При использовании в сфере культуры, в искусстве данные технологии правильно обозначать как «компьютеризованные технические средства художественного творчества». «Имитационный» смысл термина «искусственный интеллект» наиболее подходит для обозначения компьютерных инцидентов производства заведомо ложных умозаключений, обмана, манипуляций сознанием, мошенничества, дезинформации, подмены и разрушения традиционных ценностей и социально-культурной идентичности.

Оцифровка с помощью датчиков, разметка и структурирование данных о различных параметрах предметов и процессов (компьютерное «распознавание» изображений, звуков, размеров и формы, скорости и массы, температуры и агрегатных состояний и т.п.) предполагают возможность «распечатки», представления цифровых образов в технических моделях.

Модель оцифрованного предмета представляется пользователю «устройствами вывода данных» — монитором, динамиками и т.п., может быть создана на «принтере» соответствующего профиля: на плоскости и объемно, используя звук, движения, цвет, освещённость, сходный химический состав, температуру и т.п.

Созданная при помощи компьютерного оборудования техническая модель фрагментов объективной реальности будет лишь образом, копией,

как бы отдельной частью исходного предмета (процесса), степень «реальности» которой будет полностью зависеть от особенностей человеческого восприятия. Положительные же результаты теста Тьюринга полностью приравнивают компьютерную имитацию, убедительную подделку к объективной истине, а «виртуальную реальность» — к хрестоматийной «объективной реальности, данной нам в ощущениях».

Компьютерная «виртуальная реальность» действительно способна «превосходить» своей кажущейся иллюзорной подлинностью, привлекательностью объективную реальность для людей, искренне верящих в подобную возможность, предчувствующих и желающих подобного результата.

Архитектура и техническое совершенство программно-аппаратного воплощения в пользовательском оборудовании, подробность имитационной детализации цифрового контента играют сугубо техническую, подчинённую роль. Пределом доверчивости и погружения в компьютерные и прочие деструктивные иллюзии выступает социально-культурная телесность пользователей, чьё чрезмерное погружение в «виртуальную реальность» может быть прервано разочарованием, возвращением в объективную реальность или же гибелью.

Убедительность «компьютерной сказки» может быть использована как в творческих, художественных, созидательных целях, так и в качестве «опиума», маскирующего ухудшение реальной жизни, и как средство обмана, вовлечения в деструктивные сообщества и деятельность.

Пока не обозначаемым, и, возможно, специально не замечаемым разработчиками ограничением служит, как упоминалось выше, социально-культурная спецификация человеческой телесности. Предрасположенное восприятие представляет имитационную чувственную реальность как подлинную или даже лучшую, чем настоящую, и напротив: нежелательные, отвергаемые с порога ощущения подавляются, не превращаясь в восприятия.

Убедительная цифровая «виртуальная реальность», представляемая внешними техническими средствами, не воздействует на пользователя как на механизм, машину, неживой предмет — болванку, заготовку или сырьё. Программно-аппаратная имитация, так же, как изображаемое рисунком, скульптурой или описываемое в книге (простых, не механизированных и не автоматизированных предметах культуры) должна восприниматься пользователем как объективная реальность на основе его внутренних самопроизвольных телесных действий, лежащих в основе ощущений пяти «внешних» чувств.

СОЦИАЛЬНО-КУЛЬТУРНЫЙ ХАРАКТЕР ЧЕЛОВЕЧЕСКОЙ ЧУВСТВИТЕЛЬНОСТИ

Базовая, основополагающая роль самопроизвольных (частично способных осознаваться, пониматься и управляться) движений, мышечных усилий для выработки всех ощущений, включая осуществляемые посредством «дистанционных» органов чувств, просматривается на примере зрения. Малозаметные для внешнего наблюдателя и для самого «зрителя» микросаккады глаз (совершаемое несколькими группами мышц непрекращающееся «ощупывание» форм, размеров, взаимного расположения отдалённых предметов, окружающей среды) является необходимым условием зрительного восприятия.

Зрительные восприятия отдельных предметов и процессов, окружающей среды и представленной в ней всей объективной реальности формируются путём постоянного соотнесения оптических образов на сетчатке глаза и динамичных «слепков» операций с объектами аналогичного вида. В зрительном восприятии участвует весь человеческий организм, его «мышечная память», «слепки действий», распределённые в разной степени и комбинациях между различными телесными органами. Подобно зрительным восприятиям, аналогично формируются слуховые образы внешних процессов и собственных действий, в том числе звуковых, речи [12].

Учитывая органическое единство и целостность человеческого организма, централизацию нервно-мышечной системы, могут быть выявлены взаимосвязанные внутренние действия, воспроизводящие образ применения рассматриваемых дистанционно предметов, при непосредственном телесном контакте или же опосредованном инструментами. Следует помнить, что специализировавшиеся в ходе эволюции «дистанционные» органы зрения и слуха сформировались на основе осязания, контактной чувствительности поверхности тела, кожи к вибрациям, освещению и температуре.

Однако само различение внешнего мира с собой, собственным телом невозможно только на основе ощущений, получаемых с помощью «пассивных», «воспринимающих», «поверхностных» органов чувств. В основе определения предметов как внешних своему телу необходимо находится осознаваемый собственный телесный нервно-мышечный опыт усилий по преодолению их «инерционности», сопротивления изменению [13].

Сложнее всего, практически невозможно технически, с помощью внешних предметов «обманывать» внутренние ощущения, мышечное чувство и

«надстройки» самоощущений, самочувствия и эмоций. Проприоцепция, «тёмное мышечное чувство» (согласно формулировке И.М. Сеченова) неотделима от субъектности — собственных усилий, воздействия на предметность внешнего мира, преодоления его «инерции» и является основой порывов, стремлений и вожделений («аффектов»).

Без самоощущения, внутреннего чувства собственной телесности (боли и удовольствия, голода и насыщения и т.п.), эмоциональных и других психических состояний, желаний и стремлений невозможна достоверность собственного «я», своей личности. Ощущения собственного тела могут быть почти незаметными или невыносимыми; нейтральными, болезненными или приятными и т.п., образуя любые комбинации в разных пропорциях. Чем более они локализованы в определённой точке или зоне тела, тем более воспринимаются как «телесные», а чем шире неопределённо рассредоточены, тем в большей степени представляются «бестелесными», чисто «душевными», образуя основу для широкого спектра самых разных эмоций.

Главным барьером для полноценного успеха технических средств имитации выступает «внутренний настрой», конкретно-историческая социально-культурная субъектность личности. Сознание неотделимо от телесного самочувствия, идентичности личности, не вульгарно-«биологической» [14], но сформированной и осуществляющейся в результате и на основе индивидуального социально-культурного субъектного развития в конкретно-исторических условиях. При отсутствии должного «настроя» личности, другими людьми или собственными усилиями, невозможны «изменённые» состояния ощущений и восприятия, в том числе художественная фантазия, имитация и обман.

Формирование «виртуальных самоощущений» как реальных требует освоения пользователем такого навыка как «надстройки» над уже развитыми способностями представления и воображения. Сама по себе высокотехнологичная, в том числе компьютерная имитация предметов, процессов, их комплексов, обстановки, среды и т.п. не будет восприниматься как имитация без соответствующего социально-культурного «базиса» [15].

Решающую роль играет не дальнейшее повышение качества мониторов, аудиоколонок и наушников и т.д., детализации цифрового представления, разрешения изображения, битрейта звука и т.п., а наличие актуального высокохудожественного, а не гипнотически-убедительного мультимедийного контента, развивающего, а не упрощающего пользователя до «одномерного» примитива.

Полноценная виртуальная реальность потребовала бы компьютерной убедительной имитации для человека его самого, собственной личности во всём бесконечном объёме и перечне осознаваемых внутренних ощущений, желаний, мыслей в живой динамичной, зачастую неожиданной смене их комбинаций.

Внутренние самоощущения необходимо носят субъектный, самодеятельный характер и служат главным, практически непреодолимым барьером для полноценной имитации объективной реальности посредством технической программно-аппаратной «виртуальной реальности». В данном случае «объективной реальностью», как это ни парадоксально может прозвучать, для человека выступает он сам, его собственная телесность, в том числе осознаваемые психические состояния и действия. В основе психических состояний и действий лежит базовое внутреннее чувство проприоцепции, коренное отличие которого от других внешних и внутренних чувств заключается в преимущественно субъектно-практическом характере, неразрывной связи с осознаваемыми действиями человека [16].

Самоощущение является компонентом самосознания, обусловленного местоположением и позиционированием личности в «системе координат» общественных отношений, всей совокупностью непосредственных и опосредованных взаимоотношений с другими людьми. Психические состояния, действия личности представляют собой слабо локализованную, неопределённо рассредоточенную внутреннюю телесную деятельность, непрекращающуюся динамику изменений локализаций, взаимосвязей и последовательностей, «точек» и «зон», в разной степени сочетая произвольность, непроизвольность и самопроизвольность.

О НЕВОЗМОЖНОСТИ ИМИТАЦИИ ЧУВСТВИТЕЛЬНОСТИ ПРОГРАММНО-ТЕХНИЧЕСКИМИ СРЕДСТВАМИ

Инструментальная, программно-аппаратная имитация этой внутренней чувствительности тем же способом, каким представляется компьютерная «виртуальная реальность», потребовала бы внедрения компьютеризованных «устройств ввода и вывода данных» (условных наномикрофонов и нанодинамиков) во все ключевые органы и жизненные системы человеческого организма, в каждую клетку.

Обрисованная принципиальная невозможность имитировать техническими программно-аппаратными средствами внутреннюю чувствительность имеет самое прямое отношение к деятельному

характеру проприоцепции, самоощущениям собственных нервно-мышечных усилий, характер и параметры которых помогают определить и осознать, к каким объектам в какой обстановке они прилагаются. Собственное нервно-мышечное усилие человека неотделимо от его самосознания: инструментальная стимуляция сокращений мышц электрическим импульсом воспринимается не как своё действие, но как непроизвольная судорога.

В проприоцепции просматривается неразрывная связь усилия и ощущения, чувственного восприятия и осознания противоположности себя-субъекта и объекта. Самосознание способно разделять само себя, собственную телесность, на одну часть (субъектную, активную) и другую (выступающую объектом действия) при волевых усилиях, в саморазвитии, самообразовании, занятиях физической культурой и т.д. Проприоцепция как внутреннее «чувство-действие» игнорирует имитирующее инструментальное посредничество, делая принципиально невозможным компьютерную имитацию себя для себя самого.

Таким образом, социально-культурный характер человеческой телесности ставит под сомнение возможности компьютерного «сотворения материи», создания реальности, «параллельной» объективной и «компьютерного я», самого человека как микрокосма.

Компьютерная «виртуальная реальность» является инструментом социально-культурной деятельности, техническим средством познания объективной реальности, природы, общества и человека. В самом широком теоретико-культурном смысле всю деятельность человека, преобразующую мир и его самого, можно назвать создающей «виртуальную» реальность — новую, прежде не существовавшую и понятную лишь человеку.

Преобразованная человеческой исторической деятельностью часть природы является «искусственной», воплощающей человеческие замыслы и смыслы, «рукотворной» по отношению к остальной части Вселенной, пока недоступной для благоустройства человеком. Компьютерная «виртуальная реальность», как и другие, не использующие компьютерные технологии, неавтоматизированные, а простые ручные средства, способна создаваться и применяться для повышения продуктивности познания и преобразования действительности, включая «право на ошибку».

Однако в условиях неразрешимых общественных и личностных антагонизмов компьютерная «виртуализация» природы, общества, человека и самого пользователя она может быть преднамеренно использована для извлечения выгоды одними путём нанесения ущерба другим, превращаясь в средство обмана, маскировки эксплуатации.

Компьютерная «виртуальная реальность» в любом виде, познавательном и вводящем в заблуждение, существует как таковая только для человека. Но не для всякого человека, а для ограниченного круга людей, обладающих не только нужным оборудованием, программным обеспечением, доступом к соответствующим цифровым продуктам, но, что особенно важно, соответствующей потребностью и пользовательскими навыками.

Только человек предрасположен к осознанной практике восприятия объективной реальности, использованию предметов и процессов согласно их социально-культурным предназначениям и смыслам. Использование человеком технических средств любых масштабов, сложности и степени автоматизации коренным образом отличается от механических взаимодействий физических тел и волн.

Применение человеком техники, неживых предметов совершается им для удовлетворения человеческих потребностей, собственных и других людей, выработанным исторически, социально-культурным образом. Предмет культуры характеризуется не только и не столько механическими, физическими, химическими и т.п. свойствами. Указанные характеристики предмета являются частичными, абстрактными сторонами, подчинёнными исторически сформировавшемуся контексту способов употребления: обстоятельствам времени, места, назначения, и, главное, тому, кто, для кого и зачем этот предмет создавал и использует.

Чувственно-эмоциональное восприятие формируется в соответствии с исторической социально-культурной спецификой эпохи и общества, выражая уникальность личности, её «координаты» и позиционирование в системе общественных отношений с другими людьми.

Существование природы до человечества, вне его «контактных» и опосредованных воздействия и преобразований, история общества, предметы культуры, другие люди и сам человек выражаются в конкретной социально-культурной определённости «здесь и сейчас». Объективная реальность воспринимается личностью как таковая образом, сформировавшимся в результате предшествующей чувственно-преобразующей деятельности.

Такова сложная структурно-функциональная особенность культурного бытия личности, её сознания как грани самой себя и всей совокупности человеческих отношений. Это не только непосредственные отношения с «ближними», но и, в разной

степени опосредованные, с «дальними»: всеми современниками и, всё более опосредованно, с предшествующими и последующими поколениями.

Реальность, подлинность, достоверность воспринимаемых объектов определена историческими особенностями, среди которых социально-культурные играют центральную, основополагающую роль, всеобщим образом взаимодействуя с сознанием, восприятиями, чувствами, мыслями и всей деятельной телесностью личности.

КОМПЬЮТЕРНО-СЕТЕВАЯ ИМИТАЦИЯ И ФАЛЬСИФИКАЦИЯ МИРОВОЗЗРЕНИЯ

Предмет культуры, кроме исполнительских искусств, – это физический объект, преобразованный творческой деятельностью автора, но в отношении природы вне человека он является «виртуальным» объектом, воплощая человеческие смыслы и предназначения. Также предмет культуры представляется в большей или меньшей степени «виртуальным» для «непосвящённой» аудитории, не способной его адекватно воспринимать и использовать, в условиях, сильно отличающихся от тех, при которых и для которых был создан. Но для автора и понимающей аудитории, в своём социально-историческом контексте предмет культуры не «виртуален», а более чем реален, и концентрированно представляет всеобщие смыслы современности, прошлого и будущего, используясь как таковой для творческого преобразования природы, общества и человека.

Материал, «технические средства», творческие приёмы и другие особенности видов культурой деятельности (речи и письма, звуковых интонаций, мимики и жестов, действий и передвижений), их использование в музыке, театре, массовых мероприятиях, скульптуре и архитектуре, живописи, художественной фотографии, киноискусстве, современных мультимедийных технологиях и др. определяются различными параметрами и свойствами объективной реальности [17]. Эти элементы «культурной формы» сами по себе могут ничего не значить и оказываться «виртуальными», не действительными; и напротив, обретать и проявлять смысл в соответствующем контексте, представляя бесконечно подробную детализацию единой органической социально-культурной целостности.

За пределами необходимых социально-культурных условий, включающих особенности восприятия, предметы культуры и их элементы могут утрачивать или обретать более глубокие смыслы, обесцениваться, оцениваться по-иному или обретать более высокую ценность. Но локальный конкретный социально-культурный контекст, включая общественные отношения и людей, авторов и аудиторию, также способен и скрыто, и зримо представлять всю бесконечность современности, прошедшего и грядущего, обретая и проявляя созвучия иным местам и временам.

Религиозные воззрения и образы, традиции и ритуалы, правовые, моральные и нравственные нормы, методы и результаты научного познания, произведения художественного творчества для своих времён и мест, условий и людей являются не менее, но чаще всего более реальными, чем природа. Всей предметности мира культуры присуща сложная социально-историческая диалектика условности («виртуальности») и безусловности.

Сами люди также способны в подходяще складывающихся обстоятельствах представать и представляться себе и другим в «условных» социально-культурных статусах и функциях, превосходящих «реализмом» то, что может казаться «физической» механистической достоверностью, точно измеряемой и подсчитываемой. Социально-культурная деятельность создаёт новое смысловое содержание, придавая новую форму в ходе переработки наличного материала: природных и рукотворных (вещества природы, преобразованного прежним творческим трудом) предметов, человеческих взаимоотношений и действий, собственной личности и телесности.

Придание условных, «виртуальных» форм, смыслов и предназначений, свойственно человеческой культуре, начиная с магии, суеверий и религиозных воззрений первобытных обществ. «Искусственной», не природной, «надстроенной» реальностью является сам человек в единстве с миром культуры, динамичной системой взаимосвязанных деятельностей.

В самом общем виде «искусственны», наделены смыслами все предметы культуры, созданные и используемые человеком: от древнейшего камня-зубила раннего палеолита, простого необработанного орудия труда, до современной глобальной автоматизированной сетевой системы электронно-вычислительных машин, рассредоточенной на разных континентах и орбитах искусственных космических спутников Земли.

К техническим предметам культуры, неживым предметам, воплощающим высочайшие, общечеловеческие смыслы и вечные истины, можно отнести шедевры художественного и научного творчества. Будучи наполнена подлинно культурным содержанием, служащим творческому развитию человечества и личности, современная компью-

терная «виртуальная реальность» потенциально может превосходить своей действительностью обыденную предметную обстановку, как и первобытный наскальный рисунок, античная скульптура, готический собор, классический роман, симфония, научный трактат и т.п.

При отсутствии подлинного содержания компьютерная «сенсорная» имитация не будет соответствовать понятию реализма, даже «виртуальной», даже обладая «фотографическим» подобием окружающему миру и убедительно «обманывая чувства». Такая неудача разработчиков неизбежна при имитации, а не условном представлении объективной истины. Верное отображение бесконечно разнообразящейся и многогранной, изменчивой объективной реальности может осуществляться, как показывает история искусства, в самых различных формах художественных условностей, при этом всё же радикально отличаясь от имитации истины в случаях ошибок, заблуждений, лжи и преднамеренного обмана [18].

Масштабы, степень ценности предметов культуры определяются как условиями их создания, так и дальнейшего использования. Глубина научных открытий, художественная сила образов искусства, значение человеческих подвигов и свершений зависят от воплощаемого богатства объективной реальности, непосредственно — исторической, социально-культурной, включающей всё богатство человеческих взаимоотношений. «Условность», «виртуальность» ценностей культуры определяется не отрицательно, по отношению к непосредственному бытию, а положительно — масштабами и глубиной смыслов, ролью в развитии человечества, включая самые отдалённые во времени и пространстве предпосылки, прообразы и последствия.

Существующие локально феномены способны в реальной действительности воплощать, представлять и раскрывать обширные пространственно-временные взаимосвязи, уходящие в бесконечность и вечность, сами обретая значение и смыслы в этой всеобщей взаимосвязи, представляя собой свидетельства далёкого прошлого и предвосхищая отдалённое будущее. Это объективно воплощающееся в предметах культуры значение раскрывается, пересоздаётся творческим трудом созидателей и, чувственно воспринимаясь, воссоздаётся для нового творчества аудиторией, преемниками и продолжателями исторических традиций.

Компьютерная мультимедийность (тексты, изображения, звуко- и видеоматериалы) и мультимодальность (имитация вкусов и запахов, ощущений тактильных и двигательных, а также совершаемых действий и т.д.) как технические средства сами по себе не обеспечивают ни иллюзорного, ни ошибочного, ни истинного характера восприятия объективной реальности аудиторией и пользовательского творчества [19].

Технические средства, применяемые в познавательной и творческой деятельности, являются необходимыми инструментами поиска и представления объективной истины, но не заменяют личности учёного или художника, умений и мастерства, формируемых всей личной жизнью, научными школами и направлениями искусства, драматическими перипетиями социально-исторического процесса.

ВОЗМОЖНОСТИ ВИРТУАЛЬНОЙ РЕАЛЬНОСТИ И СУБЪЕКТНОСТЬ ЧЕЛОВЕКА

Переоценка возможностей технических средств познания и творчества аналогична формализму, отрыву формы от содержания в области художественного творчества и других социально-культурных сферах. Техника и технические приемы сами по себе безразличны к жизненному содержанию, его объективным смыслам и значениям, подобно наукообразности, соблюдению правил формальной логики при написании научных трудов. Другой аналогией является бюрократическая упорядоченность деловой документации, способная создавать иллюзию истинности, убедительности и реальности, подменяя действительное содержание.

Интересы и характер взаимоотношений субъектов, назначение и планируемые результаты применения объектов определяют характер высокотехнологичных разработок компьютерной «виртуальной реальности», архитектуру решений и контент, пользовательскую активность, характер восприятия аудиторией и результаты для всех сторон. Технологии выступают посредниками, неживой средой человеческих взаимоотношений, сочетания и столкновения интересов владельцев, разработчиков, провайдеров и пользователей сервисов, а также других граждан.

Традиционные и новейшие цифровые технические средства могут разрабатываться и использоваться как для повышения творческого мастерства и культурного уровня аудитории, так и для манипуляций сознанием ради извлечения выгоды путём нанесения ущерба другим людям [20]. Подобным высокотехнологичным разработкам может сопутствовать также самообман, ущерб и другие негативные социально-культурные последствия для самих владельцев, создателей и непосредственных пользователей.

Обман чувств с помощью технических средств может быть увлекательной эстрадной или художественной оптической иллюзией, но также может осуществляться для преднамеренного введения в заблуждение жертв, например, при подделке документов, телефонном мошенничестве и дезинформации в ходе психологических спецопераций, для побуждения к деструктивным действиям [21].

Компьютерная «виртуальная реальность» предлагается пользователям как инструмент для обновления, освежения, улучшения картины мира и собственных ощущений, восприятий, впечатлений, эмоций, но без действительного улучшения объективной реальности и самих себя. В таком ракурсе данный феномен можно охарактеризовать как опиум для народа.

Деструктивно изменённое состояние сознания, сиюминутно привлекательное для пользователя, роднит такую компьютерную «виртуальную реальность» не с техническими средствами творческой научной и художественной фантазии, но с игровыми зависимостями, в том числе азартными.

Недооценка социально-культурных факторов при создании компьютерной «виртуальной реальности» обрекает на неудачу стремления убедительно имитировать техническими средствами ощущения и чувственные восприятия пользователем внешнего мира, других людей и себя самого, своей телесности. В этом разработчики проектов цифровой «виртуальной реальности» пока не способны конкурировать с «обычными» способами и средствами изменения сознания, формирующимися с глубокой древности.

В контент «виртуальной реальности» «оцифровываются», в лучшем случае, фрагменты поныне актуального исторического наследия религии, культуры, науки, искусства. Но равным образом могут интегрироваться деструктивные способы воздействия, связанные с традициями обмана и мошенничества, употребления наркотических веществ, вовлечения в деструктивные зависимости, азартные игры и тоталитарные секты.

Таким образом проявляется заведомая несостоятельность деклараций разработчиков создать компьютерную «виртуальную реальность», действительно полностью превосходящую объективный мир. Методологической причиной неудачи служит рудиментарный механистический идеализм, сведение человеческих ощущений к комплексу, сумме «созерцательных» внешних пяти чувств, игнорирование деятельной субъектности человека, его индивидуальности, внутренней телесной чувствительности и самоощущений.

Однако сущность человека совершенно не сводится к механике, вычислениям и алгоритмам, телесно представляя деятельную субъективность совокупности конкретно-исторических социально-культурных взаимоотношений всех людей. Поэтому зарубежные концепции компьютерной «виртуальной реальности» следует трактовать как «виртуальное», имитационное, симулирующее использование новейших цифровых сервисов для манипулирования сознанием, скрытого управления, дезинформации пользователей во всех странах, продвигаемое в собственных интересах их владельцами и разработчиками — глобальными цифровыми корпорациями.

ЗАКЛЮЧЕНИЕ

В современных общественно-политических условиях становится актуальным вопрос активизации отечественных разработок компьютерных симуляторов и массовых публичных цифровых сервисов «виртуальной реальности». Разработчики таких цифровых сервисов должны отказаться от копирования зарубежных и создавать отечественные технологии на основе верной философской методологии и собственных, альтернативных концепций, с учётом социально-культурных аспектов и последствий.

Необходима коррекция описанных недостатков зарубежного механистичного идеализма, некритически транслируемых некоторыми российскими философами, исследователями и разработчиками. При этом максимизация прибыли разработчиков и провайдеров или симуляция благополучия, маскирующая и компенсирующая управляемое ухудшение действительности, не должны быть приоритетными задачами разработки решений компьютерной «виртуальной реальности» [22].

Весьма важное значение имеет развитие национального регулирования доверенных, безопасных и защищённых отечественных разработок компьютерной «виртуальной реальности» и соответствующих интернет-сервисов. Отечественные разработки компьютерной «виртуальной реальности» нуждаются в верной философской методологии, основанной на классической теории культуры и нацеленной на повышение продуктивности использования цифровых решений в области культуры, обучения, образования, общественного и личностного развития, сохранения и развития традиционных ценностей, укрепления семейственности и роста народонаселения, противодействия внешним манипуляциям сознанием.

В области культуры цифровые технологии, включая «виртуальную реальность», могут помочь зна-

чительно расширить доступ к лучшим коллекциям классических шедевров отечественного и мирового искусства, использоваться на публичных платформах и в сервисах массового самодеятельного художественного и социального творчества. Также компьютерная «виртуальная реальность» может применяться как симулятор, тренажёр для формирования и повышения профессиональной и массовой культуры информационной безопасности, для расширения знаний и способностей граждан, улучшения их жизни, благосостояния и благополучия общества в целом.

СПИСОК ЛИТЕРАТУРЫ

1. Былевский П.Г. Культурологические аспекты формирования информационной безопасности граждан // Ярославский педагогический вестник. 2023. № 6(135). С. 232-239. DOI: 10.20323/1813-145X_2023_6_135_232. EDN: XANZER.

2. Лещев С.В. Электронная культура и виртуальная реальность: третья цифровая волна НБИК-парадигмы // Вестник Гуманитарного факультета Ивановского государственного химико-технологического университета. 2014. Т.7. С.5-9.

3. Черкашин М.Д. Виртуальная реальность как феномен культуры: история и современность // Российская наука и образование сегодня: проблемы и перспективы. 2021. №3(40). С.33- 37. EDN: JZGWTZ.

4. Chen S. et al. Metaverse: Perspectives from graphics, interactions and visualization // Visual Informatics. 2022. Vol.6. №1. Pp.56-67. DOI: 10.1016/j.visinf.2022.03.002.

5. Винников Я. Цитологические и молекулярные основы рецепции. Эволюция органов чувств. Л.: Наука. Ленинградское отделение, 1971. 298 с.

6. Escola-Gascon A. New techniques to measure lie detection using COVID-19 fake news and the Multivariable Multiaxial Suggestibility Inventory-2 (MMSI-2) // Computers in Human Behavior. 2021. №3(5). 100049. DOI:10.1016/j.chbr.2020.100049.

7. Aharon D.Y., Demir E., Siev S. Real Returns from Unreal World? Market reaction to Metaverse Disclosures // Research in International Business and Finance. 2022. №63. 101778. DOI: 10.1016/j. ribaf.2022.101778.

8. Li G., Li X., Chen L. Effects of virtual reality-based interventions on the physical and mental health of older residents in long-term care facilities: A systematic review // International Journal of Nursing Studies. 2022. №136: 104378. DOI: 10.1016/j.ijnurstu.2022.104378.

9. Chang J. J. C. et al. Social benefits of living in the metaverse: The relationships among social presence, supportive interaction, social self-efficacy, and feelings of loneliness // Computers in Human Behavior. 2023. Vol.139. Iss.6. 107498, DOI: 10.1016/j.chb.2022.107498.

10. Былевский П.Г. Культурологическая деконструкция социально-культурных угроз ChatGPT информационной безопасности российских граждан // Философия и культура. 2023. №8. С.46-56. DOI: 10.7256/2454-0757.2023.8.43909 EDN: UZDRFW

11. Eloy S., da Silva N. P., Resende R. Robotic construction analysis: simulation with virtual reality // Heliyon. Vol.8. 2022. №10. Pp.1-13. DOI: 10.1016/j.heliyon.2022.e11039.

12. Бурцева Е.П. Этапы развития голосового аппарата при помощи органов чувств / X Кайгородовские чтения. Краснодар, 29 апреля 2010 года. Материалы региональной научно-практической конференции. Вып.9-10. Краснодар: Краснодарский государственный институт культуры, 2010. С.239-241.

13. Barra M. et al. Involvement of visual signals in kinaesthesia: A virtual reality study // Neuroscience Letters. 2022. №786. 136814. DOI: 10.1016/j.neulet.2022.136814.

14. Винников Я.А. и др. Происхождение и эволюция органов чувств (экстерорецепторы). Отчет о НИР №94-04-13255 (Российский фонд фундаментальных исследований). С.-Пб.: Институт эволюционной физиологии и биохимии им. И. М. Сеченова РАН (ИЭФБ РАН), 1994.

15. Былевский П.Г. «Виртуальная реальность» как инструмент глобальных манипуляций социально-культурной идентичностью // Философия и культура. 2024. №2. С.72-83. DOI: 10.7256/2454-0757.2024.2.69843 EDN: TQFKWS.

16. Визитей Н.Н., Манолаки В.Г. Двигательное действие спортсмена: введение в спортивную кинезиологию // Наука и спорт: современные тенденции. 2017. Т.16. №3(16). С.10-19.

17. Соловьев В.М. Виртуальная реальность в контексте ценностно-ориентационного потенциала гуманитарной культуры // Ростовский научный вестник. 2021. №2. С.65-72.

18. Pyasik M., Pia L. Owning a virtual body entails owning the value of its actions in a detection-of-deception procedure // Cognition. 2021. №212. 104693. DOI: 10.1016/j.cognition.2021.104693.
19. Ayal S., Hochman G., Peleg D. Robin Hood meets Pinocchio: Justifications increase cheating behavior but decrease physiological tension // Journal of Behavioral and Experimental Economics. 2021. №92(6). 101666. DOI: 10.1016/j.socec.2021.101699.
20. Norman D. G. et al. Caught Virtually Lying — Crime Scenes in Virtual Reality Help to Expose Suspects' Concealed Recognition // Journal of Applied Research in Memory and Cognition. 2020. Vol.9. №1. Pp.118-127. DOI: 10.1016/j.jarmac.2019.12.008.
21. Савченко А.В., Сегал А.П. Виртуальная реальность — онтология, эпистемология, праксис. Постановка проблем // Искусственные общества. 2020. Т.15. №4. DOI: 10.18254/ S207751800012841-4.
22. Дойч Дэвид. Структура реальности. М., Ижевск: РХД, 2001. 398 с.

УДК: 51, 003.26

О принципиальных проблемах проверки электронной подписи и подтверждения прав

A.Yu. Shcherbakov

On the Fundamental Problems of Verifying Electronic Signatures and Confirming Rights

Abstract. *The article considers the issues of confirming the immutability and authorship of a document, in particular, the fundamental problems of the limited validity period of an electronic signature certificate, as well as a possible way to solve them. An algorithm is proposed using the certifying signature of an external trusted service containing a timestamp. An other algorithm allows to form digital rights for long-term storage of a certain array of information without using electronic signature mechanisms.*

Keywords: *electronic signature, qualified electronic signature, certification authority, payment identifier.*

А.Ю. Щербаков
Доктор технических наук, профессор, заведующий кафедрой когнитивно-аналитических и нейро-прикладных технологий, директор Академического института виртуальной и дополненной реальности Российского государственного социального университета, ведущий научный сотрудник Государственного университета управления.
E-mail: x509@ras.ru

Аннотация. *В статье рассматриваются вопросы подтверждения неизменности и авторства документа, в частности, принципиальные проблемы ограниченного срока действия сертификата электронной подписи, а также возможный способ их решения. Предлагается алгоритм с использованием удостоверяющей подписи внешнего доверенного сервиса, содержащей метку времени. Другой алгоритм позволяет сформировать цифровые права длительного хранения на некоторый массив информации без применения механизмов электронной подписи.*

Ключевые слова: *электронная подпись, квалифицированная электронная подпись, удостоверяющий центр, платежный идентификатор.*

ВВЕДЕНИЕ

В последнее время достаточно часто у практиков применения электронной подписи (ЭП) и квалифицированной электронной подписи (КЭП), особенно в банковской сфере, возникают проблемы потери ***валидности*** подписи. Стоит обратить внимание на *три сценария*, при которых это может произойти.

1. Известны случаи, когда владелец подписи отказывается от факта подписания документа, аргументируя это хакерской атакой, которая привела к похищению ключа подписи. Имеется правоприменительная практика, когда суд становится на сторону владельца ЭП и подписанный документ признается недействительным. Действенных мер, которые могла бы предпринять организация или частное лицо для противодействия такому сценарию, в настоящий момент не найдено, не считая страхования обозначенного риска.

2. При компрометации ключа ЭП его владелец обязан заявить об этом факте в Удостоверяющий центр (УЦ), который выдавал сертификат ЭП. В результате обращения, соответствующий этому ключу ЭП сертификат помещается в список отозванных сертификатов. Обычно проверка ключа ЭП в момент подписания документа происходит с предварительным контролем того, что сертификат не находится в списке отозванных. Однако на размещение скомпрометированного сертификата в списке отозванных требуется некоторое время, в течение которого можно использовать скомпрометированную ЭП для подписания документа, после чего валидность подписанного документа может быть оспорена. Применение данного метода в мошеннических целях также зафиксировано в судебной практике, следствие по таким делам может занимать несколько лет и результат не прогнозируем.

3. По истечению срока действия сертификата ЭП подпись на всех документах, которые подписаны этой ЭП, становится ***невалидной*** (непригодной для подтверждения подлинности документа в суде). Это стратегический недостаток современных систем электронного подписания и проверки ЭП, основанных на сертификатах.

Для проверки ЭП используется подписанный доверенным УЦ открытый ключ, используемый, в свою очередь, для проверки ЭП под входящим документом. При этом сертификаты ЭП имеют ограниченный срок действия, как правило, один год. Удостоверяющие центры по закону не имеют обязанности хранить и предоставлять сертификаты ключа ЭП после истечения срока их действия. Соответственно, проверка подписи документа стандартной про-

цедурой будет выдавать результат "Срок действия ключа электронной подписи истек", даже если на момент подписания документа подпись была валидна. Такая подпись не может быть использована в суде для доказательства подлинности документа.

В качестве примера приведем разъяснения [1] по этому поводу.

Вопрос: что делать, если истекает срок действия сертификата электронной подписи?

Ответ: чтобы электронная подпись оставалась **активной**, её обладатель обязан самостоятельно следить за сроком действия. Рекомендуем подать заявку на продление за две недели до окончания действия сертификата. Если не уложиться в сроки, то придется посещать удостоверяющий центр очно для подтверждения личности.

Вопрос: каков максимальный срок действия сертификата электронной подписи?

Ответ: обычно сертификаты электронных подписей действуют 15 и 12 месяцев. Срок может зависеть и от требований самого удостоверяющего центра, и запроса будущего владельца. Например, УЦ ФНС выдает сертификаты строго на 15 месяцев, а УЦ Контура от 3 до 15 месяцев.

Действие сертификата электронной подписи может завершиться и раньше срока. Это может произойти по желанию владельца, из-за закрытия удостоверяющего центра или по решению суда».

Подписанные ЭП документы, например, в банковской сфере, сфере нотариата и защиты интеллектуальной собственности имеют значительные сроки актуального действия и хранения. Например, устав организации, служащий для составления кредитного досье, может не меняться несколько лет, по прошествии которых проверить ЭП будет невозможно из-за истечения срока действия сертификата. При этом, неизменность и авторство документа, зафиксированные подписью, будут валидны. То же самое остносится к цифровым завещаниям и иным образцам передачи прав через длительные сроки хранения.

ПРОБЛЕМА ОГРАНИЧЕННОГО СРОКА ДЕЙСТВИЯ СЕРТИФИКАТА

Частичным тактическим решением данной проблемы является последовательная простановка ***меток времени*** под документом после проверки ЭП на действующем сертификате (например, каждый год). Метка времени формируется внешним доверенным сервисом и может быть проверена также с его помощью, что делает этот процесс объективным с участием третьей стороны. Для подписания меткой времени предоставляется хеш-функция документа, по которой восстановить содержание документа невозможно, следовательно, риски нарушения конфиденциальности документов в этом случае исключены.

Соответственно, организация должна реализовать на своей стороне особый ***контрольно-удостоверяющий сервис***, который будет дополнительно подписывать все полученные и проверенные документы с ЭП клиента в специализированном внешнем доверенном сервисе, который удостоверит, что ЭП клиента на документе была сделана не позднее текущей даты, когда подпись клиента еще гарантированно валидна. При этом такая удостоверяющая подпись внешнего доверенного сервиса, содержащая метку времени, сама по себе тоже ограничена сроком действия своего сертификата ЭП. Поэтому такой сервис должен отслеживать срок действия всех таких сертификатов, и вовремя переподписывать истекающую по сроку действия подпись внешнего УЦ новой подписью в том же (или в другом) внешнем УЦ, не реже раза в год.

Таким образом, будет создаваться цепочка ЭП, в которой каждая последующая ЭП удостоверяет предыдущую, а самая последняя ЭП всегда остается свежей и проверяемой. В итоге, факт существования ЭП клиента на определенный момент времени в прошлом можно доказать на любую дату в течение периода времени, на протяжении которого у нас имеется цепочка переподписания.

Процедура должна быть отлажена и должна работать без сбоев для всех юридически значимых документов с ЭП на протяжении ***всего срока их востребованности и архивного хранения***. О случаях применения такого рода доказательства в суде или о сложившейся практике принятия решений с их учетом у нас информации на текущий момент информации не имеется, но очевидно, что это дает дополнительный объективный аргумент в суде в пользу подлинности документа.

Ситуация длительного хранения документа

Ещё сложнее ситуация становится, если мы рассматриваем ***документы долговременного хранения***, например, завещание или цифровые образы (ЦО) некоторых персон, которые отправлены на хранение уже сейчас, а "аватарированы" (оживлены) будут через 30-50 лет.

В целом можно констатировать, что система ЭП для длительно хранимых документов в настоящее время себя полностью не оправдывает просто потому, что краткосрочная цель извлечения прибыли, и, как следствие, неверная постановка задачи, часто

приводят к созданию и реализации неработающих решений.

Однако задача состоит в том, чтобы владелец некоторой информации в универсальном формате (например, текста T в человекочитаемом виде или цифровой последовательности M в машиночитаемом формате) доказал свои права на информацию, хранимую длительное время, даже если предположить, что уже нет удостоверяющих центров, частных безымянных фирм, которые этими УЦ владели, учреждений, которые им выдавали разрешения, а также алгоритмов проверок ЭП и сертификатов, исчезнувших за полной коммерческой ненадобностью.

ЦИФРОВЫЕ ИДЕНТИФИКАТОРЫ ДЛИТЕЛЬНОГО ХРАНЕНИЯ

Введем несколько терминов.

Участник проекта (УП) – физическое или юридическое лицо, давшее документальное согласие на участие в длительном проекта, например, создании цифрового образа личности [2].

Основной идентификатор УП (ОИ УП) – цифровая последовательность рекомендованной длины, однозначно описывающая УП и связанная с ним, при этом по ОИ УП должно быть невозможно установление личности и персональных данных УП.

Платежный идентификатор УП (ПИ УП) – цифровая последовательность рекомендованной длины, однозначно описывающая УП в части финансовых операций по обслуживанию операций с ЦО, по ПИ УП должно быть невозможно установление личности УП и ОИ УП.

Предположим, что нам необходимо получить ОИ УП и ПИ УП для некоторого массива M без применения сертификатов и желательно без ЭП.

Допустим, что у нас есть ***хеш-функция H***. Допустим также, что эта хеш-функция алгоритмически описана, например, в виде блок-схемы, математической формулы, текста, фрагмента кода на универсально-понимаемом языке программирования и с ней соединен тестовый пример. ***Тест*** – произвольная последовательность, для которой известен результат ее вычисления ht:

ht = H (Тест)

Без ограничения общности допустим также существование твёрдых человекочитаемых носителей, обеспечивающих ***неизменность*** написанного на них текста Ti и алгоритмов преобразования, которые имеют тестовый результат ht и достаточно компактную запись, описанную выше.

Пусть УП формирует уникальный текст Ti, где i – условный номер УП. Этот текст может описывать УП, например, содержать его имя, псевдоним, дату рождения, номер в системах государственного или корпоративного учета и так далее, причем в любом формате.

Далее при помощи H УП формирует ***hi = H(Ti)***.

Предположим также существование субъекта (организации) «Библиотека» или «Нотариат», который хранит важную для УП информацию, например, его цифровой образ или завещание Mi.

Он вычисляет ***hmi = H(Mi)*** и передает его УП.

УП фиксирует его на носителе (возможно, на том же, где он записал Ti). После чего передает каким-либо образом ранее вычисленный hi библиотекарю или нотариусу, которой хранит Mi и hi необходимое время.

Проверка прав участника проекта происходит следующим образом.

Он предъявляет Ti на носителе (свойства носителя не позволяют изменить Ti, впрочем, если его изменить, то hi не совпадет с тем, который есть у нотариуса или библиотекаря).

Далее проверяется сама хеш-функция H – вычисляется тест, he=H(Тест).

Если he равен ht, то это та самая хеш-функция, которая использовалась вначале фиксации прав УП.

Далее УП демонстрирует вычисление hi на проверенной хеш-функции для Ti, а нотариус проверяет, совпадает ли результат с тем, который хранится у него.

Далее нотариус демонстрирует, что хеш-функция от Mi совпадает с имеющейся у УП.

Таким образом, стороны убеждаются в своих правах и совершают на основе сделанных проверок некие действия, например, «оживляют» Mi.

В текущей деятельности из hi можно сформировать платежный идентификатор, hpi=H(hi), который не позволит определить hi и Ti, но тем не менее, использовать его для совершения уникальных платежных операций от имени УПi.

ЗАКЛЮЧЕНИЕ

Предложенный в статье способ решения проблемы ограниченного срока действия сертификата электронной подписи с использованием удостоверяющей подписи внешнего доверенного сервиса, содержащей метку времени, позволяет убедиться в возникновении некоторых прав у владельцев информации. Таким образом, становится возможным устранение стратегического недостатка современных систем электронного подписания и проверки электронной подписи, основанных на сертификатах.

СПИСОК ЛИТЕРАТУРЫ

1. Срок действия электронной подписи. URL: https://ca.kontur.ru/articles/52807-srok_dejstviya_elektronnoj_podpisi
2. Цифровой образ. Платформа «Вечность». URL: https://birch-league.com/

УДК: 004.8, 130.2, 168

Применение технологий искусственного интеллекта для повышения качества генераторов псевдослучайных чисел

S. A. Mirzoyan

Application of Artificial Intelligence Technologies to Improve the Quality of Pseudorandom Number Generators

Abstract. *This paper explores the use of artificial intelligence (AI) for modifying pseudorandom number generators (PRNGs). We analyze traditional PRNG methods such as the linear congruential method and Mersenne Twister, and investigate the potential of AI, including generative adversarial networks and recurrent neural networks, to improve randomness quality. The application of AI in this field is fraught with several challenges, including implementation complexity, high data requirements, vulnerabilities to attacks, and ethical concerns. Despite the potential benefits, existing challenges and risks highlight the need for additional research before implementing AI models in mission-critical systems.*

Keywords: *pseudorandom number generator, artificial intelligence, generative adversarial network, recurrent neural network, security, randomness quality.*

С. А. Мирзоян
Аспирант, преподаватель кафедры международной информационной безопасности, Московский государственный лингвистический университет.
E-mail: sergey.mirzoyan@bk.ru

Аннотация. *В статье рассматриваются вопросы использования технологий искусственного интеллекта (ИИ) для модификации генераторов псевдослучайных чисел (ГПСЧ). Анализируются традиционные методы ГПСЧ, такие как линейный конгруэнтный метод и алгоритм «вихрь Мерсенна», а также исследуются возможности инструментов ИИ, включая генеративные состязательные сети и рекуррентные нейронные сети, для улучшения качества случайности. Применение искусственного интеллекта в этой области сопряжено с рядом проблем, таких как сложность реализации, высокие требования к данным, уязвимости к атакам и этические вопросы. Несмотря на потенциальные преимущества, существующие проблемы и риски свидетельствуют о необходимости проведения дополнительных исследований перед внедрением ИИ-моделей в критически важные системы.*

Ключевые слова: *генератор псевдослучайных чисел, искусственный интеллект, генеративная состязательная сеть, рекуррентная нейронная сеть, безопасность, качество случайности.*

ВВЕДЕНИЕ

Генераторы псевдослучайных чисел (ГПСЧ) являются важной частью множества технологических систем, от криптографии до моделирования и научных исследований. Традиционные ГПСЧ используют математические алгоритмы для создания последовательностей чисел, которые кажутся случайными, но на самом деле определяются начальным значением. Хотя такие генераторы демонстрируют высокую эффективность в ряде приложений, они не лишены недостатков, таких как предсказуемость и ограниченный диапазон случайных значений.

В последние годы развитие искусственного интеллекта (ИИ) открывает новые возможности для улучшения существующих технологий. ИИ обладает способностью обучаться на больших объемах данных и находить сложные закономерности, что делает его привлекательным кандидатом для модификации ГПСЧ. Однако использование ИИ в этой области не лишено проблем и вызовов, которые требуют глубокого анализа и понимания.

Цель данного исследования заключается в рассмотрении возможностей ИИ для улучшения ГПСЧ, а также в анализе связанных с этим проблем и рисков. Мы рассмотрим принцип работы традиционных ГПСЧ, способы их модификации с помощью ИИ, а также обсудим этические и практические аспекты такого подхода.

ТРАДИЦИОННЫЕ МЕТОДЫ ГПСЧ

Традиционные генераторы псевдослучайных чисел, как указано выше, используют алгоритмы для создания последовательностей чисел, которые выглядят случайными, но на самом деле являются детерминированными и зависят от начального значения, называемого "зерном" (seed). Эти алгоритмы обычно основаны на математических функциях, таких как линейный конгруэнтный метод, Mersenne Twister или XORSHIFT.

Рассмотрим два первых основных метода.

Линейный конгруэнтный метод (Linear congruential generator, LCG) — один из наиболее простых и широко используемых алгоритмов ГПСЧ. Он определяется следующими параметрами: $Xn+1=(aXn+c)modm$ где X — это последовательность псевдослучайных значений, а a, c, и m — констан-

ты, выбираемые таким образом, чтобы обеспечить максимальную периодичность и равномерное распределение чисел.

Вихрь Мерсенна (Mersenne Twister) — более сложный и современный алгоритм, который используется в большинстве языков программирования, таких как Python и R. Этот алгоритм имеет огромный период (2^19937-1) и отличается высокой скоростью и качеством генерации чисел [1].

Преимущества и недостатки традиционных методов

Традиционные ГПСЧ имеют ряд преимуществ и недостатков, которые следует учитывать при их использовании.

Преимущества:

• ***высокая скорость:*** традиционные алгоритмы могут генерировать большие объемы данных за короткое время;

• ***простота реализации:*** большинство алгоритмов легко реализовать и использовать в различных средах;

• ***повторяемость:*** использование одного и того же зерна позволяет воспроизводить одну и ту же последовательность чисел, что полезно для отладки и тестирования.

Недостатки:

• ***предсказуемость:*** поскольку все числа в последовательности зависят от зерна, знание зерна позволяет полностью предсказать всю последовательность;

• ***ограниченный диапазон:*** некоторые алгоритмы могут иметь ограниченный диапазон значений, что может быть проблемой для криптографических приложений;

• ***качество случайности:*** хотя числа кажутся случайными, они не обладают теми же статистическими свойствами, что и истинно случайные числа, что может привести к ошибкам в моделировании и других приложениях.

ПРИМЕНЕНИЕ ТЕХНОЛОГИЙ ИИ ДЛЯ УЛУЧШЕНИЯ ГПСЧ

Возможности ИИ в генерации данных

Искусственный интеллект и машинное обучение предлагают новые подходы к созданию псевдослучайных чисел, которые могут обладать более высоким качеством случайности по сравнению с традиционными методами. Один из таких подходов — использование нейронных сетей для моделирования сложных закономерностей и генерации данных, которые кажутся случайными.

Генеративные состязательные сети (generative adversarial networks, GANs) являются одним из наиболее популярных методов ИИ для создания данных, которые имитируют реальные распределения. GAN состоит из двух частей: генератора и дискриминатора. Генератор создает данные, а дискриминатор пытается различить их от реальных данных. В результате обучения эти две части конкурируют друг с другом, что приводит к улучшению качества генерируемых данных [2].

Пример использования GAN для генерации данных можно найти в области компьютерного зрения. В работе [3] авторы использовали GAN для создания реалистичных изображений лиц людей, которые невозможно отличить от настоящих. Это демонстрирует способность GAN создавать сложные и высоко-качественные данные, которые могут быть адаптированы для других задач, включая генерацию псевдослучайных чисел.

Рекуррентные нейронные сети (recurrent neural network, RNNs) также могут быть использованы для генерации последовательностей данных. Они способны запоминать предыдущие состояния и использовать эту информацию для создания следующих значений, что делает их полезными для задач, требующих долгосрочной зависимости между числами [4]. Например, RNN могут быть использованы для прогнозирования временных рядов или генерации текста на основе ранее наблюдаемых данных.

В контексте ГПСЧ, RNN могут быть использованы для создания последовательностей чисел, которые сохраняют определенную зависимость между элементами, что может быть полезно для специфических приложений, таких как моделирование финансовых рынков или климатические исследования.

Как ИИ может быть использован для модификации ГПСЧ

Применение ИИ для модификации ГПСЧ может происходить несколькими способами:

1. **Улучшение качества случайности:** ИИ может быть использован для анализа статистических свойств генерируемых чисел и их корректировки, чтобы обеспечить лучшее соответствие истинно случайным данным. Например, алгоритмы ИИ могут анализировать распределение чисел и корректировать его таким образом, чтобы оно соответствовало нормальному или равномерному распределению, что важно для многих научных и инженерных приложений.

2. **Адаптивность и персонализация:** ИИ может адаптироваться к конкретным требованиям приложения, например, генерировать числа с определен-

ными статистическими свойствами или удовлетворяющие специфическим условиям безопасности. Например, в криптографии может потребоваться генерация чисел с высокой степенью энтропии, что может быть достигнуто с помощью специально обученных моделей ИИ.

3. **Обучение на больших объемах данных:** ИИ может обучаться на больших объемах данных и находить сложные закономерности, которые невозможно обнаружить с помощью традиционных алгоритмов. Это позволяет создавать более сложные и качественные последовательности чисел. Например, если у нас есть большой набор данных, содержащий примеры реальных случайных событий, мы можем обучить модель ИИ на этих данных, чтобы она могла генерировать числа, которые максимально близко имитируют поведение реальных событий.

Пример использования ИИ в ГПСЧ

Один из примеров применения ИИ для улучшения ГПСЧ — это использование нейронных сетей для генерации ключей шифрования. В работе [5] исследуется возможность использования рекуррентных нейронных сетей для генерации безопасных ключей шифрования, которые демонстрируют высокую степень случайности и устойчивость к атакам. Авторы показывают, что RNN могут быть эффективно использованы для генерации ключей, которые обладают высоким уровнем безопасности и могут быть применены в различных криптографических системах.

Другой пример использования ИИ в ГПСЧ — это генерация данных для тестирования программного обеспечения. В работе [6] авторы предлагают использовать GAN для генерации тестовых данных, которые имитируют реальные пользовательские сценарии. Это позволяет проводить более точные и надежные тесты программного обеспечения, что особенно важно для сложных систем, таких как банковские или медицинские приложения.

ПРОБЛЕМЫ ИСПОЛЬЗОВАНИЯ ТЕХНОЛОГИЙ ИИ В ГПСЧ

Недостатки ИИ как модификатора ГПСЧ

Несмотря на множество преимуществ, использование ИИ для модификации ГПСЧ сопряжено с рядом серьезных недостатков и вызовов:

1. ***Комплексность и сложность реализации:*** модели ИИ, такие как GAN или RNN, требуют значительных вычислительных ресурсов и времени для обучения. Это делает их менее удобными для задач, где требуется быстрая генерация чисел, например, в реальном времени.

Пример: В работе [7] авторы исследуют возможность использования глубоких нейронных сетей (DNN) для генерации случайных чисел. Они обнаружили, что обучение таких моделей требует значительных вычислительных ресурсов. Например, обучение одной модели DNN на наборе данных размером в несколько терабайт заняло около двух недель на кластере из 64 графических процессоров. Для сравнения, традиционный алгоритм Mersenne Twister может генерировать миллионы чисел за доли секунды на обычном персональном компьютере.

2. ***Требования к данным:*** ИИ-модели обычно требуют больших объемов данных для обучения. В случае ГПСЧ это означает, что нам нужно иметь доступ к большим наборам данных случайных чисел, которые могут быть труднодоступными или дорогими в создании.

Пример: В статье [8] рассматривается использование рекуррентных нейронных сетей для генерации псевдослучайных чисел. Авторы отметили, что для достижения приемлемого качества генерируемых чисел им потребовалось собрать огромный набор данных — порядка 10 миллионов уникальных чисел. Это создало значительные трудности с точки зрения хранения и предварительной обработки данных.

3. ***Непредсказуемость поведения:*** ИИ-модели могут демонстрировать неожиданное поведение, особенно если они были обучены на ограниченных или некачественных данных. Это может привести к генерации чисел, которые не соответствуют требованиям приложения.

Пример: В исследовании [9], проведенном командой ученых из Массачусетского технологического института, было показано, что нейронные сети могут "запоминать" шаблоны из обучающих данных. В одном из экспериментов модель RNN была обучена на последовательностях чисел, содержащих определенные закономерности. После обучения модель продолжала генерировать числа, которые содержали те же закономерности, даже если входные данные были полностью случайными. Это значительно снижало качество случайности генерируемых чисел.

Риски и вызовы безопасности

Использование ИИ для модификации ГПСЧ также связано с рядом рисков и вызовов безопасности:

1. ***Уязвимости к атакам:*** ИИ-модели могут быть уязвимы к различным видам атак, таким как атаки на основе противников (adversarial attacks),

когда злоумышленник специально подбирает входные данные для получения желаемого выхода.

Пример: В работе [10] авторы демонстрируют, как можно провести атаку на GAN, используемые для генерации случайных чисел. Злоумышленник может манипулировать входными данными так, чтобы дискриминатор ошибочно принимал сгенерированные данные за реальные. В результате модель начинает генерировать числа, которые не соответствуют требованиям случайности. Например, в одном из экспериментов было показано, что после проведения атаки доля чисел, прошедших тест на случайность, снизилась с 95% до менее чем 50%.

2. ***Зависимость от зерна:*** хотя ИИ может улучшить качество случайности, он все еще зависит от начального значения (зерна), которое используется для инициализации модели. Если злоумышленник сможет узнать это зерно, он сможет предсказать всю последовательность чисел.

Пример: В исследовании [11] команда ученых из Университета Калифорнии в Беркли продемонстрировала, как знание начального значения (зерна) может сделать систему полностью уязвимой к атакам. В рамках эксперимента они использовали методы статистического анализа для восстановления зерна из последовательности сгенерированных чисел. После этого злоумышленник смог предсказать всю последующую последовательность чисел, что делает систему абсолютно небезопасной для криптографических приложений.

Этические вопросы

Этические вопросы также играют важную роль в использовании ИИ для модификации ГПСЧ:

1. ***Прозрачность и объяснимость:*** одной из основных проблем ИИ является его "черный ящик", когда сложно понять, как модель принимает решения. Это может быть особенно проблематично в контексте ГПСЧ, где важно знать, как числа были сгенерированы.

Пример: в работе [12] авторы исследуют вопрос объяснимости ИИ, применяя различные методы для анализа внутренних механизмов работы нейронных сетей. Один из методов, известный как LIME (Local Interpretable Model-agnostic Explanations), позволяет получить локальные интерпретации решений модели. Однако его применение ограничено, особенно для сложных моделей, таких как GAN или RNN. В одном из экспериментов было показано, что LIME способен объяснить только около 30% решений модели, что недостаточно для полной прозрачности.

2. ***Риск злоупотребления:*** Существует риск того, что ИИ-модели могут быть использованы для создания ложных данных или манипуляций, что может привести к серьезным последствиям в различных областях, таких как финансы, медицина или юриспруденция.

Пример: в статье [13] рассматриваются возможности использования GAN для создания фальшивых изображений и видео. Авторы показывают, как такие модели могут быть использованы для создания реалистичных подделок, которые практически невозможно отличить от оригинала. Это представляет серьезную угрозу для общества, поскольку такие подделки могут быть использованы для манипуляций общественным мнением, распространения дезинформации и других негативных действий. Например, в одном из случаев злоумышленники использовали GAN для создания фальшивого видео с участием политического деятеля, что вызвало широкий общественный резонанс.

ПРИМЕРЫ УСПЕШНОГО ПРИМЕНЕНИЯ ТЕХНОЛОГИЙ ИИ В ГПСЧ

1. Генерация ключей шифрования с использованием RNN

Одним из наиболее интересных примеров является использование рекуррентных нейронных сетей (RNN) для генерации безопасных ключей шифрования. В исследовании [14], проведенном группой ученых, в т.ч. из Стэнфордского университета, было показано, что RNN могут быть эффективно использованы для создания ключей, которые демонстрируют высокую степень случайности и устойчивость к атакам. В ходе эксперимента модель RNN была обучена на большом наборе данных, содержащих примеры настоящих ключей шифрования. После обучения она смогла генерировать ключи, которые проходили все стандартные тесты на случайность, такие как тест NIST SP 800-22. Более того, эти ключи показали высокий уровень безопасности при проведении различных атак, включая атаки методом подбора и атаки по времени выполнения.

2. Генерация тестовых данных для программного обеспечения с использованием GAN

В работе [15] авторы предлагают использовать GAN для генерации тестовых данных, которые имитируют реальные пользовательские сценарии. Это позволяет проводить более точные и надежные тесты программного обеспечения, что особенно важно для сложных систем, таких как банковские или медицинские приложения.

Например, в одном из экспериментов модель GAN была обучена на наборе данных, содержащем примеры транзакций в банке. После обучения она

смогла генерировать новые транзакции, которые были практически неотличимы от реальных. Эти данные использовались для тестирования системы обработки транзакций, что позволило выявить несколько ранее неизвестных ошибок и повысить общую надежность системы.

3. Прогнозирование временных рядов с использованием LSTM

В исследовании [16], проведенном командой ученых из Массачусетского технологического института, рассматривается возможность использования долгой краткосрочной памяти (Long short-term memory, LSTM) для прогнозирования временных рядов. Хотя эта задача не напрямую связана с ГПСЧ, она демонстрирует потенциал нейронных сетей для моделирования сложных зависимостей между числами. В рамках эксперимента модель LSTM была обучена на наборе данных, содержащем исторические значения курса акций. После обучения она смогла точно предсказать будущие значения курса, что делает ее полезной для задач финансового моделирования.

Этот подход может быть адаптирован для генерации последовательностей чисел с определенными статистическими свойствами, что может быть полезно для специфических приложений, таких как моделирование финансовых рынков или климатические исследования.

ИССЛЕДОВАНИЯ И РЕЗУЛЬТАТЫ

1. Сравнение качества случайности между традиционными алгоритмами и ИИ-моделями

В статье [17] авторы сравнивают качество случайности, генерируемое традиционными алгоритмами ГПСЧ, такими как Mersenne Twister, и моделями ИИ, такими как GAN и RNN. Результаты показывают, что хотя традиционные алгоритмы демонстрируют высокое качество случайности в стандартных тестах, такие как тест NIST SP 800-22, модели ИИ могут превосходить их в специфических задачах, требующих сложных закономерностей. Например, в одном из экспериментов модель GAN была обучена на наборе данных, содержащем примеры случайных чисел с определенной корреляционной структурой. После обучения она смогла генерировать числа, которые лучше соответствовали требованиям задачи, чем традиционные алгоритмы.

2. Анализ уязвимостей ИИ-моделей в контексте ГПСЧ

В исследовании [18], проведенном командой ученых из Университета Калифорнии в Беркли, анализируются уязвимости ИИ-моделей, используемых для генерации случайных чисел. Авторы показывают, что такие модели могут быть уязвимы к различным видам атак, таким как атаки на основе противников (adversarial attacks). В одном из экспериментов злоумышленник смог манипулировать входными данными так, чтобы дискриминатор ошибочно принимал сгенерированные данные за реальные. В результате модель начала генерировать числа, которые не соответствовали требованиям случайности. Это подчеркивает важность разработки новых методов защиты для ИИ-моделей, используемых в критически важных системах.

3. Этические аспекты использования ИИ для генерации данных

В работе [19] рассматриваются этические аспекты использования ИИ для генерации данных, включая случайные числа. Авторы подчеркивают важность прозрачности и объяснимости ИИ-моделей, особенно в контексте критически важных приложений, таких как криптография и финансы. Они также обсуждают риск злоупотребления такими моделями, который может привести к серьезным последствиям, таким как распространение дезинформации и манипуляции общественным мнением. В качестве примера они приводят случай использования GAN для создания фальшивых изображений и видео, которые были использованы для манипуляций общественным мнением в политической сфере.

ПЕРСПЕКТИВЫ ДАЛЬНЕЙШИХ ИССЛЕДОВАНИЙ

Несмотря на определенный потенциал, использование ИИ для модификации ГПСЧ остается спорным и требует дальнейшего исследования. Существующие проблемы и риски подчеркивают необходимость осторожного подхода и дополнительных исследований перед тем, как внедрять ИИ-модели в критически важные системы.

1. ***Улучшение эффективности и скорости работы:*** одной из основных задач является разработка новых алгоритмов и архитектур нейронных сетей, которые позволят улучшить эффективность и скорость работы моделей ИИ. Однако даже если такие алгоритмы будут разработаны, они все равно могут столкнуться с проблемами, связанными с зависимостью от входных данных и уязвимостями к атакам.

2. ***Разработка новых методов защиты:*** важно разрабатывать новые методы защиты для ИИ-моделей, используемых в критически важных системах. Однако создание действительно надеж-

ных методов защиты может оказаться сложной задачей, особенно в условиях постоянного развития технологий атак.

3. ***Объяснимость и прозрачность ИИ:*** для повышения доверия к ИИ-моделям необходимо разрабатывать новые методы объяснимости и прозрачности. Однако существующие методы, такие как LIME и SHAP, пока не обеспечивают полной прозрачности и могут быть ограничены в своих возможностях.

4. ***Применение ИИ в различных областях:*** существует большой потенциал для применения ИИ-моделей в различных областях, таких как финансы, медицина, криптография и научные исследования. Однако использование ИИ в этих областях требует тщательного анализа и оценки рисков, поскольку любые ошибки или уязвимости могут иметь серьезные последствия.

Таким образом, хотя ИИ имеет потенциал для улучшения ГПСЧ, существующие проблемы и риски делают его применение сомнительным, особенно в критически важных системах. Будущие исследования должны сосредоточиться на разработке новых методов и подходов, которые позволят преодолеть эти вызовы, однако стоит задуматься, действительно ли ИИ является правильным выбором для этой задачи. Возможно, более простые и проверенные временем методы останутся предпочтительнее в ближайшей перспективе.

ЗАКЛЮЧЕНИЕ

В ходе представленного исследования мы рассмотрели различные аспекты использования искусственного интеллекта для модификации генераторов псевдослучайных чисел. Хотя ИИ обладает значительным потенциалом в различных областях, его применение к ГПСЧ вызывает серьезные сомнения. Анализ традиционных методов ГПСЧ, таких как линейный конгруэнтный метод и алгоритм «вихрь Мерсенна», позволяет утверждать, что они проверены временем и широко используются в критически важных системах, таких как криптография и научное моделирование. Однако, несмотря на высокую скорость и простоту реализации, эти алгоритмы часто страдают от предсказуемости и ограниченного диапазона значений.

С учетом данных особенностей мы изучили возможности использования технологий ИИ, в частности, генеративных состязательных сетей (GAN) и рекуррентных нейронных сетей (RNN), в области создания более сложных и качественных последовательностей чисел. Эти модели могут адаптироваться к конкретным требованиям приложения, обеспечивать лучшее качество случайности и обучаться на больших объемах данных. Тем не менее, реальные примеры показывают, что эти преимущества сопряжены с множеством проблем и ограничений.

Один из наиболее очевидных недостатков ИИ-моделей — их сложность и вычислительная трудоемкость. Обучение GAN или RNN требует значительных ресурсов и времени, что делает их малоприменимыми для задач, где требуется быстрая генерация чисел, например, в реальном времени [20]. Кроме того, ИИ-модели сильно зависят от качества входных данных. Если данные некачественные или содержат шаблоны, это может привести к генерации чисел, которые не соответствуют требованиям случайности.

Кроме того, ИИ-модели могут быть уязвимы к различным видам атак, что особенно опасно в контексте криптографии, где любая уязвимость может иметь серьезные последствия. Также серьезными проблемами остаются прозрачность и объяснимость алгоритмов ИИ. Такие методы, как LIME и SHAP, позволяют получить интерпретации решений модели, но их применимость ограничена, особенно для сложных моделей. Также следует учитывать существование риска злоупотребления ИИ-моделями для создания фальшивых данных, которое может привести к дезинформации и манипуляциям общественным мнением.

СПИСОК ЛИТЕРАТУРЫ

1. Matsumoto M., Nishimura T. Mersenne twister: a 623-dimensionally equidistributed uniform pseudo-random number generator // ACM Transactions on Modeling and Computer Simulation (TOMACS). 1998. №8(1). Pp. 3–30. DOI: 10.1145/272991.272995
2. Goodfellow I., Pouget-Abadie J., Mirza M. et al. Generative adversarial nets // Advances in neural information processing systems. 2014. №3. Pp. 2672–2680. DOI: 10.1007/978-3-658-40442-0_9
3. Karras T., Laine S., Aila T. A Style-Based Generator Architecture for Generative Adversarial Networks // 2019 IEEE/CVF Conference on Computer Vision and Pattern Recognition (CVPR). 2019. Pp. 4401–4410. DOI: 10.1109/CVPR.2019.00453

4. Mikolov T., Karafiát M., Burget L. et al. Recurrent neural network based language model // INTERSPEECH 2010, 11th Annual Conference of the International Speech Communication Association, Makuhari, Chiba, Japan, September 26–30, 2010. DOI: 10.21437/Interspeech.2010-343

5. Graves A., Fernández S., Gomez F. et al. Connectionist temporal classification: Labelling unsegmented sequence data with recurrent neural networks // Machine Learning, Proceedings of the Twenty-Third International Conference (ICML 2006), Pittsburgh, Pennsylvania, USA, June 25–29, 2006. Pp. 369–376. DOI: 10.1145/1143844.1143891

6. Zhang H., Cisse M., Dauphin Y. et al. Mixup: Beyond empirical risk minimization. arXiv preprint arXiv:1710.09412. 2017. DOI: 10.48550/arXiv.1710.09412

7. Radford A., Metz L., Chintala S. Unsupervised representation learning with deep convolutional generative adversarial networks. arXiv preprint arXiv:1511.06434. 2015. DOI: 10.48550/arXiv.1511.06434

8. Graves A. Generating sequences with recurrent neural networks / arXiv:1308.0850v5 [cs.NE] 5 Jun 2014. URL: https://arxiv.org/abs/1308.0850 (Дата обращения 2025.03.03).

9. Bengio Y., Simard P., Frasconi P. Learning long-term dependencies with gradient descent is difficult. IEEE Transactions on Neural Networks. 1994. №5(2). Pp. 157–166. DOI: 10.1109/72.279181

10. Kurakin A., Goodfellow I., Bengio S. Adversarial examples in the physical world. arXiv preprint arXiv:1607.02533. 2016. DOI: 10.48550/arXiv.1607.02533

11. Coron J. S., Naccache D., Stern J. P. et al. On the security of RSA padding. In Advances in Cryptology–CRYPTO 2000. 2000. Pp. 1–18. DOI: 10.1007/3-540-44598-6_1

12. Ribeiro M. T., Singh S., Guestrin C. Why should I trust you?: Explaining the predictions of any classifier. In Proceedings of the 22nd ACM SIGKDD International Conference on Knowledge Discovery and Data Mining. 2016. Pp. 1135–1144. DOI: 10.1145/2939672.2939778

13. Thies J., Zollhöfer M., Stamminger M. et al. Deferred neural rendering: Image synthesis using neural textures. ACM Transactions on Graphics (TOG). 2019. №38(4). Pp. 1–12. DOI: 10.1145/3306346.3323035

14. Al-Rfou R., Alain G., Almahairi A. et al. Theano: A Python framework for fast computation of mathematical expressions. arXiv preprint arXiv:1605.02688. 2016. DOI: 10.48550/arXiv.1605.02688

15. Esteban C., Hyland S. L., Rätsch G. Real-valued (medical) time series generation with recurrent conditional GANs. arXiv preprint arXiv:1706.02633. 2017. DOI: 10.48550/arXiv.1706.02633

16. Hochreiter S., Schmidhuber J. Long short-term memory. Neural computation. 1997. №9(8). Pp. 1735–1780. DOI: 10.1162/neco.1997.9.8.1735

17. Panneton F., L'Ecuyer P., Matsumoto M. Improved long-period generators based on linear recurrences modulo 2. ACM Transactions on Mathematical Software (TOMS). 2006. №32(1). Pp. 1–16. DOI: 10.1145/1132973.1132974

18. Papernot N., McDaniel P., Goodfellow I. et al. Practical black-box attacks against machine learning. In Proceedings of the 2017 ACM Asia Conference on Computer and Communications Security. 2017. Pp. 506–519. DOI: 10.1145/3052973.3053009

19. Mittelstadt B. D., Allo P., Taddeo M. et al. The ethics of algorithms: Mapping the debate. Big Data & Society. 2016. №3(2). Pp. 2053951716679679. DOI: 10.1177/2053951716679679

20. Schmidhuber J. Deep learning in neural networks: An overview. Neural Networks. 2015. №61. Pp. 85–117. DOI: 10.1016/j.neunet.2014.09.003

УДК: 004.7

Анализ надежности распределенных информационных систем в условиях воздействия внешних угроз: комплексный обзор литературы

Almali Ahmed Adnan Latif

Analysis Of The Reliability Of Distributed Information Systems Under External Threats: A Comprehensive Literature Review

Abstract. *The article considers current issues of reliability, optimization and information security of distributed information systems from the standpoint of counteracting modern external threats. It describes the features of application of fuzzy logic methods, Monte Carlo methods, Markov chains, genetic algorithms and models based on artificial intelligence to solve the problems of increasing fault tolerance and system performance. It is concluded that to combat cyber threats, including DDoS attacks and malicious intrusions, a prerequisite is the detection of anomalies based on AI and fuzzy trust assessment.*

Keywords: *distributed system, information system, reliability, optimization, information security, fuzzy logic, artificial intelligence, genetic algorithms.*

Алмали Аайя Аднан Латиф
Аспирант Тамбовского государственного технического университета.
E-mail: ayaalmali@outlook.com

Аннотация. *В статье рассматриваются актуальные вопросы надежности, оптимизации и информационной безопасности распределенных информационных систем с позиции противодействия современным внешним угрозам. Описываются особенности применения для решения задач повышения отказоустойчивости и производительности систем методов нечеткой логики, моделирования Монте-Карло, аппарата цепей Маркова, генетических алгоритмов и моделей на основе искусственного интеллекта. Делается вывод о том, что для борьбы с киберугрозами, включая атаки DDoS и вредоносные вторжения, необходимым условием является обнаружение аномалий на основе ИИ и нечеткой оценке доверия.*

Ключевые слова: *распределенная система, информационная система, надежность, оптимизация, информационная безопасность, нечеткая логика, искусственный интеллект, генетический алгоритм.*

ВВЕДЕНИЕ. ОСНОВНЫЕ СВОЙСТВА И ВИДЫ РАСПРЕДЕЛЕННЫХ ИНФОРМАЦИОННЫХ СИСТЕМ

Для представленного обзорно-аналитического исследования используется системный подход к анализу методов, предлагаемых в рамках актуальных исследований в области распределенных информационных систем с учетом их надежности, оптимизации и защищенности.

Распределённые информационные системы (distributed information systems, DIS) — это комплекс программных и аппаратных средств, которые позволяют организовывать совместный доступ к данным и ресурсам, размещённым на различных компьютерах и серверах через сетевую среду. Он обеспечивает эффективное распределение вычислительных задач и работу с большими объёмами информации.

Ключевыми свойствами распределённых информационных систем являются:

- **масштабируемость:** систему можно легко масштабировать, добавляя больше узлов для обработки данных в условиях увеличенной нагрузки;
- **отказоустойчивость:** система продолжает функционировать, несмотря на сбои отдельных узлов;
- **параллельные вычисления:** несколько узлов работают одновременно, параллельно выполняя вычислительные задачи.

Примеры распределённых информационных систем:

- **Облачные вычисления.** Сервисы облачных вычислений: Amazon Web Services (AWS), Microsoft Azure и Google Cloud Platform (GCP) основаны на распределённых системах для предоставления масштабируемых вычислительных ресурсов.
- **Сети доставки контента** (Content Delivery Network, CDN). CDN, такие как Akamai, Cloudflare и Amazon CloudFront, распространяют веб-контент среди пользователей в зависимости от их географического местоположения.
- **Распределённые базы данных** – системы Apache Cassandra, Google Spanner и Amazon DynamoDB, предназначены для обработки больших объёмов данных в нескольких местах.

Изученные автором статьи опубликованы на английском и русском языках и относятся к периоду с 2021-го по 2024-й год. Они были отобраны на основе релевантности их содержания для таких понятий, как устойчивость сети, отказоустойчивость и модели безопасности на основе искусственного интеллекта (ИИ).

Данные были собраны из IEEE Xplore, Springer, Elsevier, Google Scholar и arXiv также с использованием ключевых слов «надежность сети», «оптимизация на основе ИИ» и «нечеткая логика в моделировании надежности». Исследования были классифицированы по методологиям, основным выводам и ограничениям с акцентом на нечеткую логику, моделирование Монте-Карло, цепи Маркова и оценки надежности на основе ИИ.

НЕЧЕТКАЯ ЛОГИКА ДЛЯ АНАЛИЗА РАСПРЕДЕЛЕННЫХ СИСТЕМ

Растущая зависимость от распределенных систем в облачных вычислениях, промышленных сетях и платформах для борьбы со стихийными бедствиями подчеркивает необходимость повышения безопасности и надежности как систем в целом, так и их элементов. Важную роль играет прогнозирование работы таких систем в условиях различных внешних воздействий, в том числе и негативных. Эти системы сталкиваются со значительными проблемами, связанными с кибератаками, сбоями в работе сети и ограничениями ресурсов.

Нечеткая логика может быть использована для указанных систем как надежный подход для улучшения принятия решений, оптимизации производительности сети и усиления мер безопасности. Она эффективно применялась при реагировании на стихийные бедствия и оптимизации сети путем интеграции принятия решений на основе геолокации с применением теории графов и эволюционными алгоритмами.

Такие методы, как алгоритм Форда-Фалкерсона[1] и генетические алгоритмы, использовались для оптимизации распределения полосы пропускания, повышения устойчивости и масштабируемости сети, хотя эти подходы в явном виде не устраняют угрозы информационной безопасности [1]. Интеграция нечеткой логики с методами машинного обучения, такими как самоорганизующиеся карты[2] искусственные нейронные сети (artificial neural networks, ANN), значительно улучшила обнаружение атак типа «распределенный отказ в обслуживании». Такой синтез повышает устойчивость облачных вычислений и сетей IoT за счет снижения рисков уменьшения (истощения) ресурсов сети [2].

Нечеткая логика также применяется в сложных инженерных системах (пример: оценка надежности авиационных двигателей с помощью многоэкстремальной адаптивной нечеткой сети). При интеграции адаптивной нейро-нечеткой системы вывода[3] этот метод повышает точность и вычислительную эффективность в ходе оценки надежности [3]. Кроме того, в двухпродуктовых сетях потоков оптимизация надежности с использованием нечеткого многоцелевого линейного программирования в сочетании с генетическими алгоритмами обеспечивает баланс между эффективностью и ограничениями по времени выполнения, что еще больше усиливает устойчивость системы [4].

Для решения проблемы ухудшения производительности сети, вызванного задержками, изменяющимися с течением времени, были предложены методы синхронизации, запускаемые событиями в нейронных сетях. Эти методы повышают эффективность связи за счет минимизации ненужных передач данных, обеспечивая при этом синхронизацию и надежность в распределенных системах [5]. В киберэнергетических сетях нечеткая структура анализа видов, последствий и критичности отказов[4] улучшает приоритетность рисков, устраняя субъектив-

[1]Алгоритм Форда — Фалкерсона решает задачу нахождения максимального потока в транспортной сети. Идея алгоритма заключается в следующем. Изначально величине потока присваивается значение 0: f(u,v)=0 для всех u,v принадлежащих V. Затем величина потока итеративно увеличивается посредством поиска увеличивающего пути (путь от источника s к стоку t, вдоль которого можно послать больший поток). Процесс повторяется, пока можно найти увеличивающий путь.

[2]Самоорганизующиеся карты (Self-organizing map, SOM) — это тип нейронных сетей, позволяющих выявлять скрытые структуры и закономерности в данных. Они используются для кластеризации, визуализации и понимания данных. Особенностью SOM является способность организовать данные на двухмерной сетке таким образом, чтобы схожие объекты оказывались рядом. Самоорганизующаяся карта Кохонена — это нейронная сеть с обучением без учителя, выполняющая задачу визуализации и кластеризации. Метод был предложен финским учёным Теуво Кохоненом в 1984 году. Применяется также для решения задач моделирования, прогнозирования, выявления наборов независимых признаков, поиска закономерностей в больших массивах данных, разработке компьютерных игр.

[3]Адаптивная нейро-нечёткая система вывода или адаптивная система нечёткого вывода на основе нейронных сетей (adaptive network-based fuzzy inference system, ANFIS) — это разновидность искусственной нейронной сети, основанная на системе нечёткого вывода Такаги — Сугено. Этот метод был разработан в начале 1990-х годов. Поскольку он объединяет нейронные сети и принципы нечёткой логики, он может использовать преимущества обоих подходов в рамках единой системы. Его система вывода соответствует набору нечетких правил "если–то", которые обладают способностью к обучению для аппроксимации нелинейных функций. Следовательно, ANFIS считается универсальным оценщиком. Для более эффективного и оптимального использования ANFIS можно использовать наилучшие параметры, полученные с помощью генетического алгоритма.

[4]Анализ видов, последствий и критичности отказов (Failure mode, effects, and criticality analysis, FMECA) — это метод систематического анализа системы для идентификации видов потенциальных отказов, их причин и последствий, а также влияния отказов на функционирование системы (системы в целом или её компонентов и процессов). FMECA расширяет метод анализа видов и последствий отказов и включает в себя анализ критичности, который используется для сопоставления вероятности отказов в зависимости от серьёзности их последствий. В результате выявляются способы отказа с относительно высокой вероятностью и серьёзностью последствий, что позволяет направить усилия по устранению неполадок туда, где они принесут наибольшую пользу.

ные предубеждения и улучшая процесс принятия решений в критически важных для безопасности инфраструктурах [6].

Интеграция моделирования Монте-Карло (MCS) и генетического алгоритма сортировки без доминирования II[5] обеспечивает комплексный подход к минимизации рисков отключения электроэнергии и обеспечению бесперебойного электроснабжения [7]. Процесс нечеткой аналитической иерархии нечеткий метод анализа иерархий (Fuzzy Analytical Hierarchy Process, FAHP) оказался более эффективным, чем анализ главных компонентов и традиционный анализ рисков при оценке надежности электросетей на основе IoT.

Благодаря динамической корректировке весов индикаторов FAHP усиливает меры безопасности против атак типа «отказ в обслуживании» (Denial-of-service, DoS), увеличивая общую безопасность системы [8]. Также был предложен новый аналитический подход для оценки надежности интеллектуальных микросетей (SMG)[6], включающий сбои и ошибки передачи данных в вероятностную модель на основе графа. Результаты исследования показывают, что сбои в центрах управления микросетями и задержки передачи данных являются наиболее критическими факторами, влияющими на надежность, что подчеркивает необходимость создания устойчивых проектов микросетей [9].

В энергосистемах цепи Маркова и элитные генетические алгоритмы (NSGA-II) используются для оптимизации стратегий обслуживания, сокращения времени простоя и повышения надежности сети. Исследование интегрирует климатологические факторы в планирование обслуживания, достигая до 95% сокращения нераспределенной энергии и значительной финансовой экономии [10].

В исследовании, посвященном анализу избыточности информации в распределенных автоматизированных системах, оцениваются три стратегии эксплуатационной избыточности и две восстановительные с использованием магнитного хранилища. Результаты показывают, что эксплуатационная избыточность увеличивает время безотказной работы, но влечет за собой дополнительные расходы, тогда как восстановительная стратегия, которая объединяет архивные и предыдущие резервные копии, обеспечивает наивысшую устойчивость и надежность [11].

Кроме того, были предложены аналитические методологии и модели для оценки безопасности распределенных информационных систем от киберугроз. Структурно функциональное и вероятностное моделирование используются для выявления уязвимостей и количественной оценки рисков системы, при этом векторы атак классифицируются в соответствии с моделью ISO/OSI. Введена система оценки в реальном времени для адаптации к возникающим угрозам и улучшения стратегий кибербезопасности [12].

НАДЕЖНОСТЬ СИСТЕМ С УЧЕТОМ КИБЕРАТАК

Стабильность и надежность DIS-систем также анализируются с учетом кибератак (в первую очередь – отказа в обслуживании). В этом случае используются математические модели надежности, теория графов и нейронные сети для обнаружения аномалий в сетевом трафике. Результаты подтверждают, что интеграция обнаружения на основе ИИ с традиционными статистическими методами улучшает обнаружение угроз и адаптивные стратегии безопасности [13].

В контексте систем управления информацией (Information Management System, IMS) разработан алгоритм на основе модели Препарата-Метца-Чена для эффективного распределения диагностической нагрузки, снижения потребления энергии и увеличения среднего времени между отказами. Этот алгоритм демонстрирует значительное повышение надежности при крупномасштабных развертываниях систем, содержащих более ста элементов [14].

Что касается электрических сетей, надежность устройств, подключенных к Интернету вещей (IoT), оценивается с помощью процесса нечеткой аналитической иерархии (FAHP). Предлагается многоуровневая система оценки надежности, классифицирующая ключевые показатели, такие как техническая производительность, энергоэффективность, безопасность и эксплуатация. Анализ подтверждает, что FAHP снижает субъективные предубеждения и адаптируется к условиям эксплуатации, повышая надежность распределенных энергосетей [15].

Безопасность в промышленных беспроводных сенсорных сетях (Industrial Wireless Sensor Networks, IWSN) может быть усилена с помощью защищенных

[5]Генетический алгоритм сортировки без доминирования 2 (Non-Dominated Sorting Genetic Algorithm II, NSGA-II). NSGA-II — широко используемый алгоритм для многокритериальной оптимизации. Он известен своей эффективностью при работе с большими популяциями и способностью поддерживать разнообразие среди решений. NSGA-II использует быстрый подход к не доминирующей сортировке, элитизм и механизм дистанции толп, чтобы обеспечить равномерное распределение по фронту Парето.

[6]Интеллектуальные микросети (Smart Microgrid, SMG) — это мелкомасштабные сети, которые объединяют потребителей, традиционные источники энергии, распределённые возобновляемые источники энергии и технологии хранения энергии для формирования гибкой, самодостаточной и экологически полезной системы. В основе микросетей лежит интеллектуальная система управления и технология автоматизации, которая позволяет эффективно контролировать и распределять внутреннюю генерацию и хранение энергии.

протоколов кластеризации с нечеткой оценкой доверия и обнаружением выбросов (secure clustering protocol with fuzzy trust evaluation and outlier detection, SCFTO). Этот подход включает нечеткую логику интервального типа 2 и обнаружение выбросов на основе плотности для идентификации и изоляции вредоносных узлов, смягчая выборочную пересылку и атаки типа «черная дыра» [16].

Нечеткая логика также сыграла важную роль в оптимизации сетей с интегрированным оптоволоконным зондированием и связью. Стратегии неравномерного распределения значительно повышают надежность и устойчивость сети за счет минимизации вероятности отказа [17]. Кроме того, нечетко-возможностные модели используются в беспроводных сенсорных сетях для оптимизации покрытия и энергоэффективности, обеспечивая надежное планирование и устойчивость сети, несмотря на неопределенные условия развертывания [18].

Математическая модель предполагает полностью надежные узлы коммутации, в то время как линии связи характеризуются своей доступностью. Сбои линий связи анализируются как статистически независимые события с использованием вероятностных графиков и диаграмм состояний. Разработан метод расчета сложных метрик надежности, включая время простоя, среднее время между сбоями и время восстановления, с интеграцией данных системы мониторинга [19].

Оценка риска в распределенных энергетических системах была значительно улучшена за счет интеграции FAHP с оптимизацией роя частиц (Particle Swarm Optimization, PSO) и фильтрацией Калмана. Этот гибридный подход эффективно количественно оценивает угрозы, уязвимости и меры безопасности, выявляя ключевые риски, такие как DoS-атаки и вредоносное ПО, тем самым усиливая оценку риска информационной безопасности [20]. Предложена теоретическая основа для оценки надежности сети при периодическом спросе путем количественной оценки ожидаемых потерь полезности.

Стохастические вероятностные модели используются для оценки аномалий и эффектов обслуживания, используя анализ Фурье для обеспечения сходимости результатов к равномерному распределению. Модель применяется к крупномасштабной сотовой сети, и показала, что приблизительно 3,8% трафика теряется из-за аномалий, что способствует стратегиям оптимизации сети [21].

НАДЕЖНОСТЬ СИСТЕМ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА

Надежность системы ИИ повышается за счет интеграции статистических моделей надежности с методами оценки производительности. В работах [22, 23] рассматриваются состязательные атаки и проблемы качества наборов данных, предлагаются стратегии снижения смещения, состязательного обучения и защитной дистилляции. Подтверждается, что сбалансированные наборы данных повышают надежность ИИ, при этом XGBoost превосходит CNN по определенным показателям надежности [22, 23].

Для количественной оценки независимой избыточности в сложных системах вводится метрика степени независимой избыточности, учитывающая факторы единичности на аппаратном, программном и коммуникационном уровнях. Исследование оценивает влияние минимизации самого слабого измерения избыточности, улучшая устойчивость системы при балансировке экономической эффективности и отказоустойчивости [24].

Анализ надежности с высокой размерностью и изменяющейся во времени выполняется по принципу максимальной энтропии (MaxEnt) для реконструкции распределений вероятностей структурных ответов. Эта новая структура оценки вероятности отказа объединяет принципы дробных моментов и энтропии, обеспечивая высокую точность и вычислительную эффективность [25]. Устойчивость объектов информатизации к массированным кибератакам оценивается с использованием методов Монте-Карло. Статистическое моделирование заменяет детерминированные подходы к оценке надежности, интегрируя оценку рисков в планирование информационной и кибербезопасности [26].

Гибридный метод оценки надежности для распределенных сетей объединяет алгоритм выбора колеса рулетки (Roulette Wheel Selection, RWS) с последовательным методом Монте-Карло (Sequential Monte Carlo, SMC). Исследование моделирует как выходную мощность, так и состояния устройств, подтверждая, что интеграция распределенной генерации снижает частоту отключений и увеличивает доступность энергии [27].

Для повышения точности оценки надежности распределительной сети электроснабжения проводится анализ чувствительности, включающий нечеткую логику. Этот подход объединяет анализ блок-схемы надежности (reliability block diagram, RBD) с моделированием Монте-Карло (SMC), уточняя ключевые показатели надежности (SAIFI, SAIDI, ENS) и демонстрируя, что техническое обслуживание трансформатора значительно повышает надежность сети [28].

Кроме того, представлен усовершенствованный метод оценки надежности системы на основе RBD, включающий схему кодирования и алгоритм на основе поиска Tabu для динамической реконфигурации системы. Подход, проверенный с помощью

моделирования, обосновывает применение предиктивного анализа отказов и оптимизацию устойчивости [29].

НАДЕЖНОСТЬ СЕТЕЙ РАСПРЕДЕЛЕНИЯ ЭЛЕКТРОЭНЕРГИИ

Надежность сетей распределения электроэнергии с распределенной фотоэлектрической (Photovoltaic, PV) генерацией также анализируется с помощью моделирования Монте-Карло. Результаты подтверждают, что увеличение проникновения PV повышает надежность за счет сокращения продолжительности отключений и перерывов в подаче энергии [30]. Распределенные системы управления сетями оцениваются с использованием многомерных архимедовых функций для моделирования корреляций производительности пути. Исследование повышает точность оценки надежности за счет интеграции моделирования на основе анализа временных задержек, улучшая оценки в промышленных приложениях в реальном времени [31].

Надежность беспроводных сенсорных сетей (Wireless Sensor Network, WSN) анализируется с помощью кластерной модели с алгоритмом максимизации ожиданий. Подход, учитывающий скрытые данные об отказах, значительно повышает точность прогнозирования отказов, что делает его актуальным для приложений IoT [32]. Надежность интегрированных энергетических систем (Integrated Energy System, IES) оценивается с помощью трехуровневой модели и стратегии оптимального восстановления обслуживания. Этот подход эффективно устраняет частичные отказы и переходные процессы, обеспечивая высокую точность оценок надежности и оптимизации устойчивости [33].

АНАЛИЗ ИНФОРМАЦИОННЫХ АТАК НА МЕЖГРУППОВУЮ КОММУНИКАЦИЮ

Влияние информационных атак на межгрупповую коммуникацию беспилотных летательных аппартов (БПЛА), особенно когда авторизованный БПЛА передает ложные данные из-за неисправностей или злого умысла, анализируется, в частности, в [34]. В статье предложена модель на основе многоагентной системы (Multi-agent system, MAS) для моделирования влияния на координацию, потребление энергии и выполнение задач. Результаты показали, что атаки приводят к повышенному потреблению ресурсов и неоптимальному распределению задач, что подчеркивает необходимость новых стратегий безопасности.

В современной информационной безопасности предлагаются распределенные алгоритмы оптимизации для обеспечения глобальной экспоненциальной конвергенции среди агентов при атаках типа «отказ в обслуживании». Подход основан на градиентном механизме консенсуса, обеспечивающем стабильность, несмотря на периодические сбои в коммуникации [35]. Кроме того, представлена ориентированная на устойчивость структура распределенной оптимизации для многоагентных систем, включающая адаптивные стратегии управления для смягчения внешних помех и враждебных влияний [36].

Для устранения рисков в надежности корпоративных систем представлен систематический подход к управлению рисками, включающий проактивный мониторинг, автоматизированные механизмы отказоустойчивости и архитектурную избыточность [37]. В исследовании особое внимание уделяется непрерывной интеграции, автоматизированному тестированию и структурированной документации для смягчения рисков развертывания. Результаты подтверждают, что внедрение методологий инженерии надежности сайтов (Site Reliability Engineering, SRE), а также разработки и операций (Development and Operations, DevOps) повышает устойчивость системы за счет устранения таких рисков, как внешние атаки, архитектурные недостатки и ухудшение обслуживания.

Оценка надежности является критически важным аспектом в различных областях, от распределения электроэнергии до систем на основе искусственного интеллекта и телекоммуникационных сетей. В исследовании [38] оценивается надежность сетей распределения электроэнергии, особенно тех, которые интегрированы с распределенной генерацией (distributed generation, DG), с использованием анализа режимов и последствий отказов и моделирования Монте-Карло. Результаты подтверждают, что интеграция DG снижает частоту отключений и повышает доступность энергии, хотя повышение надежности зависит от мощности DG, вероятности отказа и возможности островного режима.

Кроме того, предложены методы распределенной оптимизации с византийской отказоустойчивостью для повышения устойчивости системы к состязательным агентам. Исследование объединяет градиентную фильтрацию, избыточные функции стоимости и безопасную агрегацию для смягчения византийских сбоев, обеспечивая устойчивую оптимизацию в состязательных условиях [39].

Надежность системы ИИ повышается за счет интеграции статистических моделей надежности с методами оценки производительности. Исследова-

ние рассматривает состязательные атаки и проблемы качества наборов данных, предлагая стратегии снижения смещения, состязательного обучения и защитной дистилляции. Результаты подтверждают, что сбалансированные наборы данных повышают надежность ИИ, при этом XGBoost превосходит сверточные нейронные сети (Convolutional Neural Networks, CNN) по определенным показателям надежности [40].

ОБЩИЙ АНАЛИЗ ПОДХОДОВ, ПРЕДЛАГАЕМЫХ В ИССЛЕДОВАНИЯХ

В ходе анализа изученной литературы можно выделить ключевые достижения и проблемы в области надежности систем распределенной обработки информации.

Хотя методы на основе ИИ, нечеткая логика и вероятностные модели улучшили обнаружение неисправностей и устойчивость системы, в адаптивных структурах надежности в реальном времени и широкомасштабной проверке остаются значительные проблемы.

В данном обзоре использованы следующие математические выражения и модели:

Моделирование Монте-Карло применяется для оценки надежности с помощью уравнения:

$$R(t) = e^{-\lambda t}$$

Марковские модели используются в области информационной безопасности для оценки надежности программного обеспечения:

$$R = \frac{\mu}{\lambda + \mu}$$

Оценка надежности производится посредством процесса нечеткой аналитической иерархии:

$$w_i = \frac{\sum_{j=1}^{n} a_{ij}}{\sum_{i=1}^{n} \sum_{j=1}^{n} a_{ij}}$$

Генетические алгоритмы применяются для оптимизации надежности:

$$maxR(x) = \sum_{i=1}^{n} \alpha_i R_i$$

Глубокое обучение с подкреплением позволяет добиться оптимизация производительности сети:

$$R_t = \sum_{k=1}^{T} \gamma^k r_k$$

Где:

- R_t = Общее накопленное вознаграждение в момент времени t
- γ = Коэффициент дисконтирования
- r_k = Вознаграждение на шаге k

Общая нечеткая функция надежности [22] определяется по формуле:

$$R_f(t) = e^{-\lambda t}$$

Где λ— нечеткая интенсивность отказов, определяемая по формуле:

$$\lambda = \frac{\sum_{i=1}^{n} \lambda_i}{n}$$

Для распределенных информационных систем используется в моделях планирования для оценки надежности беспроводных сенсорных сетей [18, 19].

Таблица 1

Методы оценки надежности

Методология	Преимущества	Ограничения
Моделирование Монте-Карло (MCS)	Высокая точность при отказе	Вычислительно трудоемко для крупномасштабных DIS
Цепи Маркова	Эффективны для прогнозирования отказа в обслуживании	Проблемы с вычислениями в реальном времени
Модели нечеткой логики	Справляются с неопределенностью и неточностью	Могут быть вычислительно трудоемкими для больших сетей
Генетические алгоритмы	Оптимизируют распределение ресурсов и производительность сети	Не рассматривают в явном виде угрозы безопасности
Модель кибербезопасности на основе ИИ	Высокая точность обнаружения вторжений	Проблемы масштабируемости при внедрении

Таблица 2

Традиционные методы обнаружения неисправностей

Подход	Точность обнаружения неисправностей	Масштабируемость	Адаптируемость
Статистические модели (цепи Маркова, MCS)	Умеренная	Умеренная	Низкая
Нечеткая логика и генетические алгоритмы	Высокая	Умеренная	Высокая
Модели глубокого обучения (CNN, XGBoost , DRL)	Очень высокая	Высокая	Очень высокая

Сильными сторонами современных исследований являются использование расширенных моделей обнаружения неисправностей, которые включают нейро-нечеткие методы, методы машинного обучения и многоцелевой оптимизации, улучшающие мониторинг надежности в реальном времени [3, 4].

Целостная интеграция с вопросами информационной безопасности обеспечена исследованиями по уменьшению последствий DDoS-атак, доверительными моделями безопасности и обнаружением аномалий с помощью искусственного интеллекта [2, 16, 12].

В области устойчивости энергетических систем исследования анализа видов и последствий отказов (failure mode and effects analysis, FMEA), стохастического моделирования и устойчивости интеллектуальных микросетей способствовали повышению надежности распределения электроэнергии [38, 26, 9].

В ходе изучения современных исследований были выявлены следующие проблемы:

• исследования предлагают модели нечеткой оптимизации и отказоустойчивости ИИ, но не решают практические проблемы развертывания в крупномасштабных распределенных системах [8, 20];

• отсутствуют интегрированные модели безопасности и устойчивости системы: хотя киберугрозы и технические сбои рассматриваются по отдельности, не существует комплексного подхода, объединяющего ИИ, кибербезопасность и устойчивость к угрозам окружающей среды [6, 16, 34, 41];

• проблемы масштабируемости в машинном обучении для оценки надежности: не учитывается вычислительная эффективность для общесистемных приложений в реальном времени [8, 20];

• ограниченные исследования в области самовосстанавливающихся сетей и цифровых двойников: будущие исследования должны изучить технологию цифровых двойников для обнаружения сбоев в реальном времени и автоматизированного самовосстановления, интегрируя ИИ для адаптивных фреймворков оценки надежности [40].

Новые тенденции в повышении надежности систем

Рассмотренные исследования выделяют несколько новых тенденций, включая предиктивное обслуживание на основе ИИ, принятие решений на основе нечеткой логики и безопасность на базе квантовых технологий:

• нечеткая логика для реагирования на стихийные бедствия демонстрирует повышение надежности системы на основе геолокации [1];

• нейронечеткие модели обеспечивают динамическую оценку надежности, делая акцент на прогностической аналитике на основе ИИ для обнаружения неисправностей [7 3];

• нечеткие методы принятия решений при распределении ресурсов и оптимизации сети повышают отказоустойчивость в DIS [4, 17];

• квантовые вычисления для кибербезопасности и отказоустойчивости являются новой областью для повышения качества криптографической защиты и исправления ошибок в распределенных сетях [39];

• технология цифровых двойников, интегрированная с прогнозным моделированием на основе искусственного интеллекта, предлагается для прогнозирования сбоев системы в реальном времени и автоматизированных механизмов самовосстановления [40].

ЗАКЛЮЧЕНИЕ

Проведенный анализ литературы, описывающей методы повышения отказоустойчивости и производительности распределенных систем, позволил выявить тенденции, пробелы и новые направления исследований, выделив проблемы в области безопасности и оценки надежности в реальном времени.

В рассмотренных работах освещаются достижения в области повышения надежности, оптимиза-

ции и безопасности DIS, а также в области искусственного интеллекта, применения нечеткой логики и моделировании Монте-Карло, повышающие отказоустойчивость систем.

Нерешенными в настоящее время остались проблемы в области масштабируемости и безопасности, в то время как аналитика на основе ИИ и технология цифровых двойников предлагают более удачные решения. Дальнейшие исследования могут быть сосредоточены в области адаптивных и масштабируемых моделей для повышения устойчивости систем.

СПИСОК ЛИТЕРАТУРЫ [дан в авторской редакции]

1. Синицын А.В., Лисай Н.Ю. Разработка информационных систем с алгоритмами нечеткой логики и оптимизация сети. 2023.

2. Клименко Т.М., Акжигитов Р.Р. Обзор методов обнаружения распределенных атак типа 'отказ в обслуживании' на основе машинного обучения и глубокого обучения // International Journal of Open Information Technologies, ISSN: 2307-8162. Vol. 11, no.6, 2023.

3. Chunyi Zhang, Zheshan Yuan. Multi-Extremum Adaptive Fuzzy Network Method for Dynamic Reliability Estimation Method of Vectoring Exhaust Nozzle. 2023.

4. Ashraf Mohamed Hemeida, Moatamed Hassan, Heba Hamdy. Maximizing Reliability of Two-Commodity Flow Networks with Time Constraint Using Fuzzy Optimization // Aswan University Journal of Sciences and Engineering, Vol. 2, Iss: 2, pp. 14-3, 01 Dec 2022.

5. Bo Yuan, Jun Tao. A Research Study on Methods for Improving the Service Quality of a Network System Based on Time Information. 2024.

6. Andrés A. Zúñiga, João F. P. Fernandes. Fuzzy-Based Failure Modes, Effects, and Criticality Analysis Applied to Cyber-Power Grids // Energies, Vol. 16, Iss: 8, pp. 3346-3346, 10 Apr 2023.

7. Vali Ghanbarimasir. Planning of Distributed Generation Resources to Simultaneously Improve Reliability and Resilience of Distribution Network. doi.org/10.21203/rs.3.rs-2590599/v1, Feb 2023.

8. Xinhong You, Pengping Zhang. FAHP-Based Reliability Evaluation of Distributed IoT Devices in a Distribution Power Grid. 2022.

9. Mehrdad Aslani, Hamed Hashemi-Dezaki. Analytical Reliability Evaluation Method of Smart Micro-Grids Considering the Cyber Failures and Information Transmission System Faults. 2022.

10. Oloulade Arouna. Climate-Multi-Criteria Optimization of the Reliability and Maintainability of a Distribution System by MARKOV Chains and Elitist Genetic Algorithms. 15 Nov 2022.

11. Кульба В., Сомов С., Шелков А. Анализ влияния использования информационной избыточности на показатели надежности распределенных информационных систем. 2022.

12. Баранов В.В., Шелупанов А.А. Методика и алгоритмы расчета защищенности элементов распределенных информационных систем в условиях деструктивного воздействия. 2022, DOI: 10.21293/1818-0442-2022-25-4-88-100.

13. Leontyev A. L., Chumak M. I., Chumak I. V. Use of modern technologies in assessing the stability and vulnerability analysis of information technology systems // IOP Conference Series: Materials Science and Engineering, 2021.

14. Kleiman L. A., Freyman V. I. Improving the functioning reliability of the information management system elements, using built-in diagnostic tools. 2021.

15. Xiao Xue, Yangbing Zheng. Wireless Network Safety Status Prediction Based on Fuzzy Logic. 2023.

16. Liu Yang, Yinzhi Lu. A Secure Clustering Protocol with Fuzzy Trust Evaluation and Outlier Detection for Industrial Wireless Sensor Networks. IEEE Transactions on Industrial Informatics, 20 Jul 2022.

17. Chenlin Zhang, Pan Wang. Fuzzy Logic System Assisted Sensing Resource Allocation for Optical Fiber Sensing and Communication Integrated Network. Sensors. Vol. 22, Iss: 20, pp. 7708-7708, 01 Oct 2022.

18. Boualem Adda, Cyril De Runz. A Fuzzy/Possibility Approach for Area Coverage in Wireless Sensor Networks. 2022.

19. Шерстнева А. А., Шерстнева О. Г. Определение показателей структурной надёжности в распределённых телекоммуникационных системах // Вестник ИжГТУ имени М.Т. Калашникова, 2022. 25(1). С. 100-107.

20. Haiming Li, Chun-Ru Fu. Risk Assessment of Distributed Energy System Based on Fuzzy Analytic Hierarchy Process // Journal of Computer and Communications, Vol. 10, Iss: 11, pp. 56-71, 01 Jan 2022.

21. Ali Maatouk, Fadhel Ayed. A Framework for the Evaluation of Network Reliability Under Periodic Demand. 2023.

22. Shulin Song, Zheng Zhang. Joint Optimization of Age of Information and Energy Consumption in NR-V2X System Based on Deep Reinforcement Learning. 2024.
23. Nima Shahbazi, Abolfazl Asudeh. Reliability Evaluation of Individual Predictions: A Data-Centric Approach. 2024.
24. Hong Su. Quantifying Independence Redundancy in Systems: Measurement, Factors, and Impact Analysis. 2023.
25. Zhou, Yu Hou, Hong Nie. On High-Dimensional Time-Variant Reliability Analysis with the Maximum Entropy Principle. 2022.
26. Воеводин В.А. Метод Монте-Карло для оценки устойчивости функционирования объекта информатизации в условиях массированных компьютерных атак. 2022. https://doi.org/10.24143/2072-9502-2022-2-66-75.
27. Wentao Xu, Siming Zeng. Reliability of Active Distribution Network Considering Uncertainty of Distribution Generation and Load // Electronics, Vol. 12, Iss: 6, pp. 1363-1363, 13 Mar 2023.
28. Mohammed Wadi, Wisam Elmasry. Sensitivity Reliability Analysis of Power Distribution Networks Using Fuzzy Logic. 17 Nov 2022, pp. 190-195.
29. Liu Tianyu, Pan Zhengqiang, Song Guopeng. System Reliability Evaluation and Dynamic Optimization Based on an Improved Reliability Block Diagram. 2023.
30. Azzan Alaskar, Abdulaziz Alkuhayli. Reliability Evaluation of Active Distribution Systems with Distributed Generations. 2022.
31. Longhang Huang, Ying Wang. Reliability Assessment of Distributed Network Control System Based on Time Delay Evaluation. 2023.
32. Jianfeng Yang, Jing Chen. A Novel Cluster-Based Wireless Sensor Network Reliability Model Using the Expectation Maximization Algorithm. 2021.
33. Pan Dai, Li Yang. Data-Driven Reliability Evaluation of the Integrated Energy System Considering Optimal Service Restoration. 2022.
34. Egor Marinenkov, Sergei Chuprov. Study on Destructive Informational Impact in Unmanned Aerial Vehicles Intergroup Communication // Symmetry, 2022, 14(8).
35. Zhi Feng, Guoqiang Hu. Attack-Resilient Distributed Convex Optimization of Linear Multi-Agent Systems Against Malicious Cyber-Attacks over Random Digraphs. 2021.
36. Xuening Xua, Zhiyong Yua, Da Huangb. Distributed Optimization for Multi-Agent Systems with Communication Delays and External Disturbances under a Directed Network // Nonlinear Analysis: Modelling and Control. Vol. 28, Iss: 3, pp. 412-430, 2023.
37. Зоркин А.С. Методы проектирования отказоустойчивых информационных систем. 2024.
38. Ch. V. S. S. Sailaja, Polaki V. N. Prasad. Reliability Evaluation of Distribution System Integrated with Distributed Generation. 2022.
39. Shuo Liu. A Survey on Fault-Tolerance in Distributed Optimization and Machine Learning. 2021.
40. Stine Fleischer Myhre, Olav Bjarte Fosso. Reliability Assessment for Distribution Systems with Embedded Microgrids. 2023.

УДК: 004.42

Сравнительный анализ инструментов для автоматизированного тестирования мобильного программного обеспечения

А.К. Маринин
Главный инженер-программист, ООО «ПСБ Лаб».
ORCID: 0009-0008-0242-8074
E-mail: aleksei.marinin247@gmail.com

Аннотация. *В статье представлен анализ современных методов автоматизированного тестирования мобильных приложений с целью выявления основных проблем, решаемых инженерами по тестированию. В условиях быстро развивающихся технологий и конкурентной борьбы на рынке мобильных приложений эффективные методы и инструменты тестирования позволяют разрабатывать и внедрять актуальные, инновационные мобильные приложения. Материал статьи позволяет указать на особенности процедуры мобильной кроссплатформенной разработки и провести их анализ, основываясь на передовых направлениях развития мобильных операционных систем. Приложения будут высококачественными и востребованными, если правильно выбраны инструменты и методы для их тестирования. При выборе данных инструментов и методов необходимо учесть определенные проблемы и сложности, описанные в статье.*

Ключевые слова: *мобильное приложение, тестирование программного обеспечения, ручное тестирование, автоматизированное тестирование, Robotium, Selendroid, Calabash, Appium, UI Automator.*

A.K. Marinin

Comparative Analysis of Tools for Automated Testing of Mobile Software

Abstract. *The article presents an analysis of modern methods of automated testing of mobile applications in order to identify the main problems solved by testing engineers. In the conditions of rapidly developing technologies and competition in the mobile application market, effective testing methods and tools allow developing and implementing relevant, innovative mobile applications. The material of the article allows us to point out the features of the procedure of mobile cross-platform development and analyze them based on the advanced directions of development of mobile operating systems. Applications will be high-quality and in demand if the tools and methods for their testing are chosen correctly. When choosing these tools and methods, it is necessary to take into account certain problems and difficulties described in the article.*

Keywords: *mobile application, software testing, manual testing, automated testing, Robotium, Selendroid, Calabash, Appium, UI Automator.*

ВВЕДЕНИЕ

На современном этапе развития техники повседневную жизнь трудно представить без информационных технологий, среди которых особую роль играют мобильные технологии, используемые в мобильных устройствах. Статистика свидетельствует о том, что приблизительно половина всех жителей планеты имеют смартфоны. В отчете GSMA[1] сообщается, что в 2023 г. до 55% людей в мире используют смартфоны [1]. Рынок мобильных устройств – один из самых динамичных рынков. Эксперты предполагают, что уже через год количество мобильных устройств приблизится к отметке в 18,22 млрд. [2].

Смартфоны и планшеты – средства поддержания связи с миром, оперативного получения информация, выполнения задач, которое ранее было доступно только на персональном компьютере. Задачи на мобильных устройствах реализуются через мобильные приложения. Именно поэтому последних становится все больше, и сегодня решающим конкурентным преимуществом становится их высокое качество. Разработчики в компаниях всесторонне тестируют собственные мобильные приложения. Данный процесс дает возможность обеспечить их эффективность и потребительскую удовлетворенность продуктом. При этом компании сталкиваются с определенными трудностями, связанными с наличием многообразных платформ, устройств и способов взаимодействия с ними.

Целью настоящего исследования является проведение сопоставительного анализа современных методов автоматизированного тестирования мобильных приложений, а также выявление основных трудностей, с которыми сталкиваются специалисты по тестированию. Технологическая трансформация и конкурентность рынка, на котором предлагаются мобильные приложения, требуют выбора оптимальных методов и инструментов, чтобы проводить тестирование. Правильные методы – залог того, что разработка будет успешной при внедрении и востребованной у потребителей.

Сопоставительный анализ подходов к тестированию ПО будет проведен на основе анализа научных

[1]GSMA (Global System for Mobile Communications Association) – это глобальная ассоциация, объединяющая мобильных операторов и производителей оборудования, которая управляет развитием мобильных технологий и стандартов.

источников, рассматривающих вопросы выбора подходов и методов тестирования ПО, с последующим выявлением ключевых проблем и методов их решения в области тестирования мобильного ПО.

ОСНОВНЫЕ ПОДХОДЫ И МЕТОДОЛОГИИ ТЕСТИРОВАНИЯ ПО

Тестирование является процедурой, при помощи которой проверяется качественность продукта, ПО в целом. Она рассматривается как непрерывный процесс, связанный с любой стадией изготовления продукта. Тестирование — это процесс, в ходе которого ручными или автоматизированными средствами оцениваются системные компоненты с целью определения степени соответствия ожиданиям, в том числе — потребительским [3]. С его помощью проверяется, в каком состоянии находится разрабатываемый продукт, как в процессе сборки, так и по ее завершении. ПО тестируют, чтобы установить ошибки и уязвимости.

Как указано выше, тестирование может осуществляться в ручном или автоматизированном режиме. Последний вариант – наиболее предпочтительный, особенно в случае, когда тестовые сценарии повторяются [4].

Ручное тестирование – процесс тестирования, выполняемый вручную без использования автоматизированных инструментов, что требует значительных временных затрат и может быть подвержено ошибкам.

Для ручного тестирования требуются более значительные временные затраты, здесь также важную роль играет человеческий фактор. Автоматизация при тестировании может исправить ошибки ручного процесса.

Автоматизированное тестирование – процесс проверки программного обеспечения с использованием автоматизированных инструментов и сценариев, что позволяет ускорить тестирование и снизить вероятность ошибок, связанных с человеческим фактором.

Автоматизированное тестирование способствует обеспечению качества мобильных приложений, а это, в свою очередь, ускоряет сам процесс, повышает общую производительность проектов, лояльность потребителей, положительно сказывается на качестве ПО, исключает человеческий фактор возникновения ошибок [5].

Автоматизация для тестирования целесообразна в следующих случаях:

– при разработке комплексных приложений;

– в случае, если тест-кейсы[2] выполнимы со значительными затратами (временными, финансовыми);

– при нагрузочном или стресс-тестировании;

– в случае потребности в сокращении объема тестирования.

Утилиты[3] могут лучше справиться с трудоемкими и ресурсоемкими процедурами. Кроме того, ручные методы не так разнообразны, не всегда оптимальны в конкретном случае. Автоматизированное тестирование в несколько раз быстрее, чем при ручном способе.

Существуют разнообразные методологии и подходы, с помощью которых тестируется мобильное ПО. Рассмотрим самые распространенные из них [6].

Модульное тестирование предполагает, что будет проверяться каждый компонент по отдельности с целью установления его соответствия спецификациям. Элементарный компонент процесса может быть представлен функцией, методом, объектом, модулем, процедурой. Посредством данного метода происходит выявление дефектов в изоляции, упрощается отладка, все части продукта становятся надежнее.

При ***интеграционном тестировании*** появляется возможность оценить, как взаимодействуют между собой модули в мобильном приложении, после того, как проведена интеграция. Таким образом можно выявить дефекты, связанные с совместимостью компонентов.

При ***системном тестировании*** оценивается, как функционируют модули в целом, уровень производительности и функциональности ПО, которое находится в разработке. На этом этапе тестирования приложение рассматривается как самостоятельный продукт, и проверяется в условиях, близких к реальным.

Система управления тестированием – программное обеспечение, которое помогает организовать, планировать и отслеживать процесс тестирования.

Тестовый сценарий – последовательность шагов, описывающая, как провести тестирование определенной функциональности приложения.

Для выявления основных проблем, возникающих в процессе тестирования мобильного ПО, нами были отобраны и проанализированы источники [7-12] Анализ основывался на выявлении специфических сложностей, которые возникают или могут возникнуть при использовании того или иного метода тестирования мобильного ПО. Описание методов тестирования представлено в таблице 1.

[2]Тест-кейс – набор условий и шагов, которые необходимо выполнить для проверки функциональности программного обеспечения.

[3]Утилита — вспомогательная компьютерная программа в составе общего программного обеспечения для выполнения специализированных типовых задач, связанных с работой оборудования и операционной системы.

Таблица 1

Методы тестирования и их краткое описание

Метод	Краткое описание
Локализация[4]	Проведение локализационного тестирования на ранних этапах при разработке мобильного приложения дает возможность понять адекватность внедряемой языковой поддержки, соответствие культурной специфике, менталитету страны. Как правило, мобильные приложения разрабатывают в парадигме интернационализации, это распространенная и простейшая практика, способная многократно увеличить целевую аудиторию. Однако процесс может сопровождаться проблемами, которые типичны для сферы мобильных платформ, в частности, сложностями со свободным пространством для экрана (его нехваткой).
Юзабилити-тестирование[5]	Проведение юзабилити-тестирования – важный аспект в высококонкурентной среде. Понятие удобства является параметром качества, популярности. Это ключевой показатель, который может повысить лояльность потребителя. Как правило, реализуется в качестве бета-тестирования.
Нагрузочное тестирование[6]	Осуществление наблюдения за тем, как используется память и системные ресурсы, их уровень производительности. С помощью нагрузочных тестов выясняется, есть ли утечка памяти, какую производительность имеет программное обеспечение.
Мультиплатформенное[7] и мультидевайсовое тестирование	Важное свойство приложения – работа на устройстве любой конфигурации, что выполняется его разработчиками. Тестируются устройства разного вида, чтобы оценить ту или иную сборку ОС, с различными разрешениями дисплея, функциями и аппаратным обеспечением. Трудоемкая, но важная для дальнейшего продвижения продукта задача.
Лабораторное тестирование	В процессе имитируются реальные условия качества связи и окружающей среды. Выясняется, каким образом реагируют приложения в ситуации, когда сигнал Wi-Fi слабый, или фиксируются сбои сети при передаче данных.
Аттестационное тестирование[8]	Его проведение необходимо, чтобы подтвердить, что приложение соответствует требованиям, изложенным в стандартах, лицензиях и правилах при использовании. Любая платформа подчиняется индивидуальным требованиям, выполнение которых обязательно: только в этом случае она может эффективно проходить ревью, а само приложение окажется размещенным и востребованным.

Классификация проблем может быть представлена следующим образом (рис.1). Проблемы можно сгруппировать следующим образом:

1. Деятельность по выстраиванию процессов при тестировании.

2. Оценка особенностей приложений и видов устройств.

В рамках первой группы решаются задачи, соотносимые с тем или иным типом приложения. В связи с этим важно выбрать подходящие тестировочные инструменты. Вторая группа включает проблемы, связанные с разнообразием и спецификой устройств, сетей, размерности экрана и ограничениями, препятствующими проведению всестороннего тестирования. Таблица 2 содержит ряд направлений, которые могут рассматриваться в качестве решений перечисленных трудностей, выявляемых при тестировании приложений.

[4]Локализация – процесс адаптации программного обеспечения для использования в разных языках и культурах, включая изменение интерфейса и контента.

[5]Юзабилити-тестирование — процесс оценки удобства использования приложения путём наблюдения за реальными пользователями, выполняющими задачи в реальных условиях.

[6]Нагрузочное тестирование – метод тестирования, который оценивает производительность системы под нагрузкой, выявляет узкие места и возможные утечки памяти.

[7]Мультиплатформенное тестирование – тестирование, при котором приложение проверяется на различных платформах (например, iOS, Android) для обеспечения его совместимости.

[8]Аттестационное тестирование – процесс проверки соответствия приложения установленным стандартам и требованиям перед его выпуском на рынок.

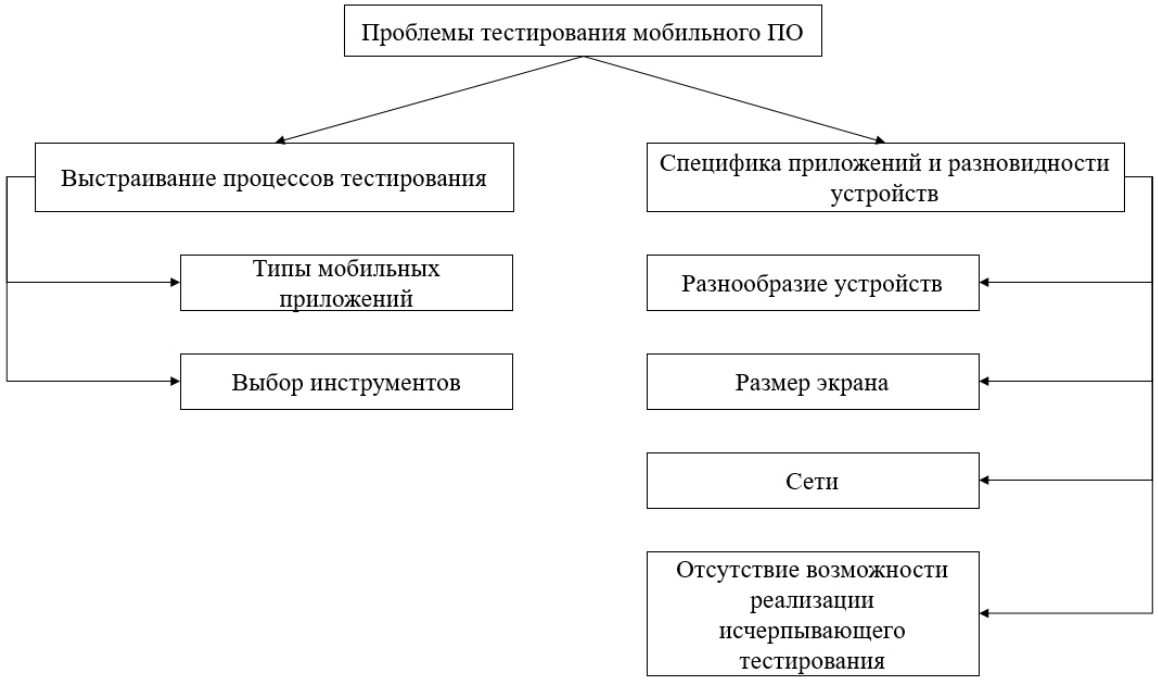

Рис. 1. Классификация проблем тестирования мобильного ПО

Таблица 2

Возможные решения проблем тестирования ПО

Категория проблем	Возможное решение
Выстраивание процессов тестирования	Процессы тестирования должны соответствовать типу приложения. Для этого определяются потребности в процессе тестирования, включая системные ресурсы, которые решают поставленные задачи и соответствуют ожиданиям потребителей.
Специфика приложений и разновидности устройств	Тестирование автоматизируется, появляется возможность выделить классы эквивалентности, с валидными и невалидными значениями, чтобы проверить, каким образом приложение справляется с обработкой граничных значений. Объединение устройств в группы, применение программ, позволяющих симулировать различные виды и состояния сети.

Таким образом, решить проблемы, которые связаны с качеством организации процессов тестирования, можно выстраиванием данных процессов под каждое конкретное приложение.

Важно выбрать подходящие инструменты, чтобы проводить тестирование. Все они обладают определенным функционалом и возможностями. Сам выбор является трудозатратным процессом, ввиду того, что исследование проводится комплексно. Все инструменты должны быть совместимыми. Иногда процесс выбора ограничивается стоимостью работ и инструментов, целями проверки. Как правило, крупная компания выделяет для каждого проекта отдельную команду. Специалисты команды выстраивают тестирование согласно типам приложений. При этом и небольшой бизнес нуждается в правильной организации тестирования с учетом типа приложения, чтобы продукт был качественным.

Весьма часто используют систему по настройке тестовой среды окружения, чтобы получить продукт нужной сборки с необходимыми параметрами в настройках. Для этих целей может использоваться ПО, которое помогает создавать и хранить тест-кейсы и результаты тестирования, а также возможности системы для просмотра отчетов, которые формируются после того, как тесты выполнены.

С помощью автоматизации тестирования решаются проблемы сложных приложений и разнообразия устройств. Могут запускаться автотесты с использованием симулятора или локально, на устройстве.

Далее проведем сопоставительный анализ инструментов автоматизированного тестирования мобильного ПО.

ИНСТРУМЕНТЫ АВТОМАТИЗИРОВАННОГО ТЕСТИРОВАНИЯ

Автоматизированное тестирование мобильного приложения осуществляется с использованием различных инструментов. С их помощью может быть проверен любой аспект продукта. Рассмотрим подробнее некоторые инструменты.

1. ***Robotium*** — платформа, в рамках которой осуществляется автоматизация тестирования с последующим созданием тестовых сценариев по методу «серый ящик». В результате упрощается написание качественных автоматических тестов, рассчитанных на пользовательский интерфейс. Становится доступной реализация различных видов теста, от функциональных до системных, приемочных. Даже если отсутствует исходный код, могут создаваться тестовые сценарии [13].

2. ***Selendroid*** является фреймворком[9] автоматизации тестирования, в котором содержится открытый исходный код, используемый для того, чтобы тестировать нативные и гибридные приложения Android. В его основе — библиотека Selenium WebDriver, располагающая инструментами, которые используются при автоматизации веб-браузера. Selendroid – специальная разработка под Android 4.1 и выше. С ее помощью можно автоматизировать разные задачи, запускать тесты одновременно на нескольких устройствах, тестировать интерфейсы.

Главное преимущество Selendroid – помощь в автоматизации тестов на нескольких устройствах одновременно. Нет необходимости в ручном переключении с устройства на устройство при запуске тестов, работе с разными версиями приложений [14].

3. ***Calabash*** — фреймворк с открытым исходным кодом, разработанный для того, чтобы упростить автоматизированное тестирование приложения. В результате разработчики пишут тесты на специфичном языке cucumber, помогающем в описании пользовательского взаимодействия с тестируемым ПО. Автоматизированное тестирование Calabash дополняется тем, что поддерживает симуляторы[10], эмуляторы[11] и физические устройства [15].

4. ***Appium*** также является фреймворком, посредством которого возможно создание тестовых сценариев для той или иной платформы: iOS, Android и Windows, при использовании одного и того же API (интерфейс программирования приложений – набор правил и протоколов, позволяющих различным программным приложениям взаимодействовать друг с другом). Это означает, что тестовые коды могут использоваться неоднократно, вне зависимости от платформы и набора тестов. Нативные приложения тестируются таким образом, что не требуются последующие SDK (software development kit, от англ. набор инструментов для разработки программного обеспечения) или перекомпиляции. Основная цель его использования – автоматизировать мобильное приложение, при этом язык и среды могут быть любыми, а доступ к API и БД из тестового кода – полный. Появляется возможность для создания тестовых примеров привычными инструментами на любом знакомом языке (от Python до PHP, JavaScript и др.) [16].

5. ***UI Automator*** является многофункциональным инструментом, с помощью которого автоматизируется тестирование ПО для Android. Пригоден для создания сценариев по взаимодействию с устройствами, с имитацией взаимодействия с пользователями. Это часть Android SDK на языке Python, предоставляющая API для доступа к тому или иному аспекту устройств, вкупе с аппаратными компонентами (от GPS, акселерометра до компаса, камеры) [17].

Сопоставительный анализ каждого из представленных инструментов на основании источников [13-17] позволил выделить ряд общих и специфических характеристик каждого инструмента, что дает возможность определить наиболее оптимальный и универсальный вариант для автоматизированного тестирования. Таблица 3 представляет перечень обобщенных результатов, полученных при сравнительном анализе.

Современные средства, используемые разработчиками в процессе тестирования ПО, способствуют повышению эффективности и точности при разработке качественного готового продукта, в связи с чем важно выбирать оптимальные инструменты, чтобы добиться желаемых для специалистов по тестированию результатов.

Анализ приведенных выше положений позволяет сделать следующий вывод. Грамотно выбрать оптимальную платформу для автоматизации тестирования можно только в том случае, если она будет удовлетворять требованиям проекта и ожиданиям разработчика.

[9]Фреймворк – набор инструментов и библиотек, который упрощает процесс разработки и тестирования программного обеспечения.
[10]Симулятор – инструмент, создающий имитацию реальных условий работы приложения, позволяющий тестировать его функциональность в различных сценариях.
[11]Эмулятор – программа, которая имитирует работу другого устройства или системы, позволяя тестировать приложения в среде, похожей на реальную.

Таблица 3

Обобщение результатов сравнительного анализа инструментов для автоматизированного тестирования мобильного ПО

Мобильная платформа	Плюсы	Минусы
1. **Robotium**		
Android	– Совместим с разными версиями Android. – Тестовые сценарии выполняются с хорошей скоростью. – Имеется обширная библиотека, где содержатся тестовые примеры.	– Ограничение – в поддержке только Android. – Ограничение — в поддержке только Java. – Веб-приложения не поддерживаются. – Отсутствует функция записи и воспроизведения.
2. **Selendroid**		
Android iOS Hybrid	– Оказывается поддержка множеству языков: C#, Java, Python, Perl. – Чтобы автоматизировать тестирование, нет необходимости вносить изменения в приложения. – Поддержка быстрого подключения физического устройства для проведения тестирования. – Возможность запуска тестов на разных устройствах и эмуляторах в одно и то же время.	– Часть событий и жестов полностью не поддерживается. – Не предусмотрена автоматизация всплывающего сообщения. – Не предусмотрена автоматизация встроенных приложений (от карт до камеры).
3. **Calabash**		
Android iOS Hybrid	– Располагает активным сообществом и поддерживает его. – Пригоден для поддержки работы эмуляторов. – Тестовые сценарии пишутся на том языке, который предложен разработчиком. – Поддержка использования селекторов CSS (Cascading Style Sheets, от англ. каскадные таблицы стилей).	– Пропуск последующих шагов при тестировании, если один из них не был успешным. – Ограниченность поддержки iOS.
4. **Appium**		
Android iOS Hybrid	– Поддержка множества языков. – Работа на Android и iOS. – Обеспечение автоматизации вне зависимости от того, гибридное это приложение или веб-приложение. – Нет необходимости получать доступ, чтобы работать с исходным кодом. – Совместимость с разными наборами инструментов. – Поддержка встроенных приложений (от камеры до календаря).	– Не сможет помочь в сравнении изображений. – Нужна длительная настройка для Android и iOS. – Отсутствует функция записи и воспроизведения тестового сценария.
5. **UI Automator**		
Android	– Нет необходимости знать исходный код, чтобы создать тестовый сценарий. – Тесты могут быть запущены на реальных устройствах и эмуляторах. – Присутствует функция записи действий, чтобы создавать тестовые случаи.	– Необходимость в переписывании сценария, как только внесено изменение. – Неинформативность документации.

Можно сформулировать следующие обобщенные рекомендации при выборе:

1. Если требуется поддержка лишь Android, при условии, что скорость тестирования первостепенно важна, следует рассмотреть возможности Robotium.

2. Если проекты требуют поддержки разных языков программирования, а тесты могут проводиться без модификации приложения, есть основания сделать выбор Selendroid.

3. Calabash – оптимальное решение при потребности в активном сообществе, а также в случаях, когда тест пишется на языке разработчиков.

4. Appium – универсальное решение, которое поддерживает различные языки. Могут тестироваться гибридные и веб-приложения, даже если отсутствует доступ к исходному коду.

5. UI Automator является инструментом, который может записывать действия, может запускаться на физическом устройстве.

Для определения наиболее универсального и подходящего для широкого спектра задач тестирования инструмента предлагается проведение оценки на основе рейтинговой системы. Критерии оценки представлены в таблице 4 и были сформированы на основе результатов сопоставительного анализа по данным таблицы 3.

Таблица 4

Критерии оценки инструмента тестирования

Критерий	Баллы	Максимум
Поддержка платформ	3 балла: поддержка Android, iOS и Hybrid	3 балла
	2 балла: поддержка только Android и iOS	
	1 балл: поддержка только одной платформы	
Языковая поддержка	2 балла: поддержка нескольких языков программирования	2 балла
	1 балл: поддержка одного языка	
Удобство использования	2 балла: наличие функции записи и воспроизведения тестов	2 балла
	1 балл: отсутствие функции записи и воспроизведения	
Скорость тестирования	2 балла: высокая скорость выполнения тестов	2 балла
	1 балл: средняя или низкая скорость	
Поддержка различных типов приложений	2 балла: поддержка нативных, гибридных и веб-приложений.	2 балла
	1 балл: поддержка только одного типа приложения	
ИТОГО		11 баллов

На основе представленной системы была проведена оценка рассмотренных ранее инструментов для автоматизированного тестирования мобильного ПО (таблица 5).

Таблица 5

Рейтинговая оценка инструментов автоматизированного тестирования мобильного ПО

Инструмент	Поддержка платформ (3)	Языковая поддержка (2)	Удобство использования (2)	Скорость тестирования (2)	Поддержка типов приложений (2)	Общая оценка (11)
Robotium	1	1	1	2	1	6
Selendroid	2	2	1	2	1	8
Calabash	2	1	1	1	1	6
Appium	3	2	1	1	2	9
UI Automator	1	1	2	1	1	6

Таким образом, согласно проведенному анализу, ни один из представленных инструментов не получил максимальную оценку (11 баллов). Наибольшую оценку получили два инструмента: Selendroid (8) и Appium (9). Учитывая, что Appium поддерживает больше платформ и типов приложений, он будет признан оптимальным инструментом для автоматизированного тестирования мобильного ПО.

Резюмируя, можно отметить возможности Appium. Это универсальная платформа, которая работает с различными приложениями, учитывает требования для тестирования.

Следует отметить, что сам проект и ресурсы работающей над ним команды определяют, какой инструмент будет в конечном итоге выбран.

ЗАКЛЮЧЕНИЕ

Высокое качество приложения и потребительский спрос на него во многом обусловлены тем, как разработчики отнесутся к выбору инструментов при его тестировании. При этом процесс выбора может осложняться различными факторами и обстоятельствами, и разработчику следует учитывать, какой инструмент поможет ей достичь поставленной цели с имеющимися ресурсами, в том числе, финансовыми. Для этого целесообразно проведение сравнительного исследования, как работают разные инструменты, предназначенные для тестирования приложения, по методике, сходной с представленной в данной статье. Следует выбирать те инструменты, которые проходят через постоянное обновление, актуализацию. Только в этом случае уровень эффективности и качества разрабатываемых приложении будет обеспечен на долгое время.

Результаты проведенного исследования могут использоваться для усовершенствования подходов при тестировании мобильных приложений.

СПИСОК ЛИТЕРАТУРЫ

1. GSMA: 4.3 billion people now own smartphones [Электронный ресурс] URL: https://www.gsmarena.com/gsma_more_than_half_of_the_world_owns_smartphones-news-60214.php (дата обращения: 15.03.2024).
2. Forecast number of mobile devices worldwide from 2020 to 2025 (in billions) [Электронный ресурс] URL: https://www.statista.com/statistics/245501/multiple-mobile-device-ownership-worldwide/ (дата обращения: 15.03.2024).
3. Pargaonkar S. A Comprehensive Review of Performance Testing Methodologies and Best Practices: Software Quality Engineering // International Journal of Science and Research (IJSR). – 2023. – V. 12. – №. 8. – P. 2008-2014.
4. Thota M.K. et al. Survey on software defect prediction techniques // International Journal of Applied Science and Engineering. – 2020. – V. 17. – №. 4. – P. 331-344.
5. Михалевская К.А., Сергачева М.А. Сравнение инструментов для автоматизации тестирования мобильных приложений на ОС Android // Chronos: естественные и технические науки. – 2020. – №. 2 (30). – С. 45-49.
6. Винокуров А.В., Лавлинская О.Ю. Уровни организации автоматизированного тестирования мобильных приложений для операционной системы Android // Вестник Воронежского института высоких технологий. – 2020. – №. 3. – С. 22-26.
7. Букарев А.В. Актуальные подходы к организации тестирования мобильных приложений // Актуальные проблемы науки и образования в условиях современных вызовов. – 2023. – С. 112-118.
8. Букарев А.В. Особенности и вызовы в современных процессах тестирования мобильных приложений // Colloquium-journal. – Голопристанський міськрайонний центр зайнятості, 2022. – №. 30 (153). – С. 23-27.
9. Винокуров А.В., Лавлинская О.Ю. Уровни организации автоматизированного тестирования мобильных приложений для операционной системы Android // Вестник Воронежского института высоких технологий. – 2020. – №. 3. – С. 22-26.
10. Гуцель Н.В., Брюховецкий А.А. Аудит процессов тестирования мобильных и web-приложений // Мир компьютерных технологий. – 2021. – С. 113-117.
11. Кукушкин Ю.М., Ильина В.Ю. Сравнительный анализ и проблема выбора эмуляторов Android // Конвергентные технологии XXI: вариативность, комбинаторика, коммуникация. – 2020. – С. 262-267.
12. Меликян Р.А. Мобильные приложения Android и методика их тестирования // Современная наука и молодые учёные. – 2020. – С. 20-23.
13. da Silva G., de Souza Santos R. Comparing Mobile Testing Tools Using Documentary Analysis // 2023 ACM/IEEE International Symposium on Empirical Software Engineering and Measurement (ESEM). – IEEE, 2023. – P. 1-6.

14. Li A., Li C. Research on the Automated Testing Framework for Android Applications // International Conference on Computer Engineering and Networks. – Singapore: Springer Nature Singapore, 2022. – P. 1056-1064.
15. Ravelo-Méndez W., Escobar-Velásquez C., Linares-Vásquez M. Kraken 2.0: A platform-agnostic and cross-device interaction testing tool //Science of Computer Programming. – 2023. – T. 225.V. 102897.
16. Tran H.M. et al. Automation Testing with Appium Framework in IP Multimedia Subsystem // 2023 14th International Conference on Information and Communication Technology Convergence (ICTC). – IEEE, 2023. – P. 579-582.
17. Srivastava N., Kumar U., Singh P. Software and performance testing tools // Journal of Informatics Electrical and Electronics Engineering (JIEEE). – 2021. – V. 2. – №. 1. – P. 1-12.

Приглашаем авторов к участию в журнале «Вестник современных цифровых технологий»

ИНФОРМАЦИЯ ДЛЯ АВТОРОВ

Редакция принимает материалы статей, соответствующие тематике журнала, содержащие новые научные результаты, не опубликованные ранее и не предназначенные к публикации в других печатных или электронных изданиях. Проводится независимое внутреннее рецензирование. Статьи в журнале публикуются бесплатно (объем – до 15 тыс. знаков), после получения одобрения Редакционного совета.

Для опубликования статьи в редакцию журнала необходимо направить по адресу *a.shcherbakov@c3da.org, a.ryazanova@c3da.org* **следующие материалы в электронном виде:**

• рукопись статьи в DOC- и PDF-форматах;
• иллюстрации, предоставленные также и отдельными файлами в формате JPG или PNG с разрешением 300 dpi;
• сведения об авторах, содержащие фамилию, имя, отчество, ученые степень и звание, должность, место работы, контактные телефоны или E-mail;
• англоязычную информацию, содержащую название статьи, ФИО авторов, аннотацию и ключевые слова;
• редакция может запросить экспертное заключение о возможности публикации статьи в открытой печати.

ПОСЛЕДОВАТЕЛЬНОСТЬ МАТЕРИАЛОВ ДЛЯ ПУБЛИКАЦИИ:

1. шифр УДК (см. Справочник УДК) в левом верхнем углу;
2. название статьи (полужирным шрифтом по центру) не более 12 слов;
3. инициалы и фамилия автора (полужирным шрифтом по центру), к каждому автору- сноска, содержащая ученое звание, должность, название организации (без сокращений), e-mail;
4. Аннотация, излагающая суть работы и полученные результаты (5-7 строк);
5. ключевые слова (8-10 слов);
6. англоязычная информация по статье (по пп.2-5)
7. текст статьи с учетом указанных далее требований к его оформлению;
8. список литературы, оформленный по ГОСТ Р 7.0.5-2008.

Статья должна быть структурирована, т.е. должна включать разделы с названиями, кратко и точно отражающими их содержание, в том числе:

• введение, содержащее обоснование актуальности и краткий обзор проблематики;
• четкую постановку задачи исследования;
• описание метода решения задачи исследования;
• прикладную интерпретацию и иллюстрацию полученных результатов исследования;
• заключение, включающее обобщение и указание области применения полученных результатов, не повторяющее аннотацию и не ограничивающееся простым перечислением того, что сделано в работе.

С детальными требованиями к рисункам, таблицам, формулам, списку литературы, а также с примерами оформления статьи можно ознакомиться на странице Вестника http://c3da.org/journal.html.

Приглашается к сотрудничеству редактор для работы в редакции журнала по совместительству. Просьба направлять резюме по электронному адресу *accda@c3da.org, info@c3da.org*

ТРЕБОВАНИЯ К РЕДАКТОРУ:

• отличное знание русского языка;
• свободное владение ПК, в том числе специальными текстовыми и графическими программами;
• опыт работы в издательстве.

Высшее техническое образование и знание английского языка являются существенными преимуществами.

ОБЯЗАННОСТИ

Редактор:

• редактирует рукописи, принятые к изданию;
• оказывает авторам необходимую помощь по улучшению структуры рукописей, выбору терминов, оформлению иллюстраций;
• проверяет, насколько учтены авторами замечания по доработке, предъявленные к рукописям;
• подписывает отредактированные рукописи в печать.