

Институт системного программирования
им. В.П. Иванникова Российской академии наук

109004, Москва, улица А. Солженицына, дом 25.
По всем вопросам: scsec@ispras.ru

ОГЛАВЛЕНИЕ

5	ПОСВЯЩАЕТСЯ 85-ЛЕТИЮ В. П. ИВАННИКОВА
9	ИСП РАН 2025: СОБЫТИЯ
11	ЭКОСИСТЕМА ИННОВАЦИЙ
15	2025. ЦЕНТР ИССЛЕДОВАНИЙ БЕЗОПАСНОСТИ СИСТЕМНОГО ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ
17	2025. ИССЛЕДОВАТЕЛЬСКИЙ ЦЕНТР ДОВЕРЕННОГО ИСКУССТВЕННОГО ИНТЕЛЛЕКТА
19	2025. ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ ДЛЯ ПЕРСОНАЛИЗИРОВАННОГО ОПРЕДЕЛЕНИЯ ПОСЛЕДОВАТЕЛЬНОСТИ МРНК-ВАКЦИНЫ ПО ГЕНЕТИЧЕСКИМ ДАННЫМ
22	2025. НАУЧНЫЙ ЦЕНТР МИРОВОГО УРОВНЯ (НЦМУ) «ЦИФРОВОЙ БИОДИЗАЙН И ПЕРСОНА- ЛИЗИРОВАННОЕ ЗДРАВООХРАНЕНИЕ»
27	1. АНАЛИЗ ПРОГРАММ И КИБЕРБЕЗОПАСНОСТЬ
	КОМПИЛЯТОРНЫЕ ТЕХНОЛОГИИ И ВЕРИФИКАЦИЯ
29	AstraVer Toolset: система верификации ключевых компонентов
32	Klever: система автоматической статической верификации Си-программ
34	Masiw: набор инструментов для проектирования ответственных систем
36	MicroTESK: генератор тестовых программ
38	Utopia EDA: система логического синтеза цифровых интегральных схем
40	Buildography: инструмент идентификации реквизитов сборки
42	Безопасный компилятор
47	Svace: статический анализатор исходного кода
52	КЛОС: конфигурируемая линейка операционных систем

- 54 TestOS: окружение для тестирования программного обеспечения
- 56 ANIS: поддержка процессов верификации средств защиты информации на основе формальных моделей управления доступом

АНАЛИЗ БИНАРНОГО КОДА, ФАЗЗИНГ

- 58 Блесна: инструмент динамического анализа помеченных данных
- 60 Платформа для анализа программ на основе эмулятора QEMU
- 63 ИСП Crusher: комплекс динамического и статического анализа бинарного кода
- 69 BinSide: статический анализатор бинарного кода
- 71 Natch: инструмент определения поверхности атаки
- 74 Sydr-fuzz: комплекс гибридного фаззинга и динамического анализа
- 77 LibAFL-DiFuzz: инструмент направленного фаззинга
- 79 ISP Aurora: статический анализатор с технологией искусственного интеллекта
- 80 ISPUaro: композиционный анализ

АНАЛИЗ СЕТЕВОГО ТРАФИКА

- 82 Protosphere: система анализа сетевого трафика
- 85 ML IDS: сетевая система обнаружения вторжений с применением машинного обучения

УПРАВЛЕНИЕ ТРЕБОВАНИЯМИ

- 88 Requality: инструмент управления требованиями

91 2. АНАЛИЗ ДАННЫХ

ИНФРАСТРУКТУРА И ИНСТРУМЕНТЫ РАЗРАБОТКИ ИИ-РЕШЕНИЙ

- 93 Асперитас и другие облачные решения
- 97 Talisman: платформа для построения интеллектуальных информационно-аналитических систем
- 100 Платформа Доверенного Искусственного Интеллекта (ДИИ)
- 102 Colba: система поддержки создания наборов данных

ОБРАБОТКА ЕСТЕСТВЕННЫХ ЯЗЫКОВ

- 104 Lingvodoc: виртуальная лаборатория для документации исчезающих языков

ОБРАБОТКА ДОКУМЕНТОВ

- 107 Dedoc: система извлечения содержимого и структуры текстовых документов
- 109 DocMarking: противодействие анонимности при утечках документов

ПРИКЛАДНЫЕ РЕШЕНИЯ

- 111 EcgHub: интеллектуальный анализ цифровых ЭКГ

113 3. ПРОЧИЕ ТЕХНОЛОГИИ

- 115 VALIDBIM: сервис верификации информационных моделей в архитектуре и строительстве
- 118 DigiTEF: программный комплекс для проведения компьютерного моделирования

ПОСВЯЩАЕТСЯ 85-ЛЕТИЮ В. П. ИВАННИКОВА



АРУТЮН АВЕТИСЯН

академик РАН,
директор ИСП РАН

В этом году исполнилось 85 лет со дня рождения академика РАН Виктора Петровича Иванникова — выдающегося учёного, основателя и первого директора Института системного программирования РАН, ныне носящего его имя.

В 1957 году Виктор Петрович поступил на факультет радиотехники и кибернетики Московского физико-технического института, где оказался в группе, курируемой Институтом точной механики и вычислительной техники АН СССР (ИТМиВТ) — ведущим в те времена исследовательским центром в области вычислительной техники. Его научными руководителями и первыми учителями были основоположники отечественной вычислительной техники Сергей Алексеевич Лебедев и Лев Николаевич Королев.

Принцип Физтеховского треугольника «наука — образование — инновации» стал ярким опытом для Виктора Петровича еще в студенческие годы во время участия в разработке программного обеспечения для центрального управляющего комплекса системы «А». Под управлением этого комплекса, объединявшего несколько ЭВМ, в марте 1961 года был осуществлен первый в мире перехват баллистической ракеты.

После учебы путь становления ведущего специалиста в области операционных систем продолжился в ИТМиВТ, где Виктор Петрович принимал участие в легендарных проектах в качестве ключевого разработчика операционных систем для БЭСМ-6 и многомашинного комплекса АС-6, который использовался в Центре управления полетами и в проекте «Союз — Аполлон». За эти работы он был удостоен Государственной премии СССР.

Виктор Петрович понимал, что системное программирование — это инновационная область, требующая постоянного развития и исследований, возможного лишь при поддержке сильных академических структур. В 1994 году он основал Институт системного программирования

Российской академии наук. В трудный для всей страны период Виктор Петрович, опираясь на опыт открытости и творчества, унаследованный от школы Лебедева, определил стратегию развития Института — он сделал ставку на молодежь и открытые технологии.

Сотрудничая с ведущими вузами (МГУ, МФТИ, ВШЭ и др.), Институт создал свои базовые кафедры, на которых студенты с первых лет обучения вовлекаются в работу над реальными научными задачами от индустрии и госзаказчиков под руководством сотрудников Института.

Свободное ПО стало основой для инноваций, предоставив доступ к глобальным передовым технологиям мирового уровня и выступая мощным образовательным инструментом. При этом открытость кода и участие в исследованиях в рамках международных сообществ повышает видимость и репутацию молодых специалистов на мировом уровне.

Сегодня Институт системного программирования им. В.П. Иванникова РАН — крупнейший научный центр России, который успешно сочетает фундаментальные исследования на переднем крае мировой науки с внедрением их результатов в реальный сектор экономики. Такой подход позволяет не только создавать прорывные технологии, но и получать обратную связь от промышленности, обеспечивая практическую значимость научной работы.

Так, за последнее время, на основе результатов фундаментальных исследований мы развили ряд наукоёмких технологий, в числе которых — полный стек инструментов разработки безопасного программного обеспечения (РБПО) по компилируемым языкам.

Мы начали работать в области доверенного искусственного интеллекта (ИИ), создав инструменты и методы для разработки соответствующих технологий, а также доверенную версию платформы Talisman для построения информационно-аналитических систем и платформу «Асперитас» для проведения ресурсоёмких вычислений и хранения данных.

Сейчас наши инструменты РБПО используют уже более 200 компаний. Технологии для разработки доверенного ИИ и противодействия новым угрозам внедрены в «Лаборатории Касперского» и «ЕС-Лизинг», а доверенная версия платформы Talisman — в МГИМО МИД России, где применяется для интеллектуального анализа данных в области международных отношений. На основе «Асперитас» создана платформа для решения биомедицинских задач.

Продолжается развитие ранее начатых проектов — например, по созданию операционной системы реального времени JetOS совместно с ГосНИИАС и по разработке систем информационного моделирования крупных строительных объектов.

Активно развивается и образование. Мы начали проводить обновление учебных курсов и программ, развивая кибербезопасность как научную специальность. С 2021 г. проводится модернизация бакалаврской программы «Программная инженерия» на факультете компьютерных наук НИУ ВШЭ. В 2022 г. в МГИМО стартовала магистерская программа «Анализ данных и динамика международных процессов».

Развивается наше сотрудничество в рамках совместных лабораторий, открытых в региональных ВУЗах России. Началось наше сотрудничество с Костромским и Саратовским государственными университетами: студенты вовлечены в реальные проекты, пишут дипломы и статьи под руководством наших сотрудников. К лабораториям системного программирования в Великом Новгороде и Ереване прибавились новые: в Орле, в Иркутске (ИДСТУ СО РАН) и в Москве (в РЭУ им. Г.В. Плеханова). С 2020 г. развивается наша стипендиальная программа, которая охватывает студентов МГУ им. М.В. Ломоносова, МФТИ, НИУ ВШЭ, НовГУ и других вузов. Число студентов, вовлечённых в проектную деятельность института, превышает 200 человек, а аспирантов — 50. С 2023 г. мы проводим ежегодную программу «Доверенный искусственный интеллект» в Университете «Сириус» (партнёры — МФТИ, ННГУ, Сколтех, AIRI и Университет Иннополис). В этом году число заявок на участие в нашей программе выросло в три раза.

Необходимость дальнейшего гармоничного развития науки, инноваций и образования естественным образом привела к потребности формирования сообществ, которые значительно повышают продуктивность работы. Один из примеров успешной реализации этой идеи — Центр исследований безопасности системного ПО, созданный при поддержке ФСТЭК России. Поиском уязвимостей в ядре Linux и критических компонентах операционных систем занимаются более 60 компаний и вузов; в основные ветки проектов приняты более 600 исправлений.

Мы собираем сообщества не только для развития существующих технологий, но и для создания новых, объединяя компании и научные организации вокруг Исследовательского центра доверенного ИИ и НЦМУ «Цифровой биодизайн и персонализированное здравоохранение». В 2025 году ИСП РАН вошёл в состав Научно-технологического центра развития мРНК-технологий, объединившего в форме консорциума 17 ведущих научных организаций страны под руководством НИЦ эпидемиологии и микробиологии им. Н. Ф. Гамалеи.

Мы продолжаем выполнять одну из главных академических функций — экспертную. С 2019 г. ИСП РАН является Центром компетенции ФСТЭК России по вопросам безопасной разработки и анализа кода сертифицируемого ПО, а в 2024 г. мы заключили соглашение с Росфинмониторингом — для развития национальной системы противодействия отмыванию преступных доходов. За более

чем 30 лет ИСП РАН стал распределённым центром компетенций по самым актуальным вопросам, связанным с системным ПО и искусственным интеллектом. В планах на ближайшие пять лет — дальнейшее развитие инструментов и сообществ для обеспечения технологической независимости страны.

Время показало, что всё, о чём говорил нам Виктор Петрович, — работает. В ИСП РАН удалось создать экосистему, которая обеспечивает постоянную генерацию кадров и инноваций в области системного программирования. Мы развиваемся, растём, готовим молодых специалистов высшей квалификации, создаём новые технологии.

ИСП РАН 2025: СОБЫТИЯ

- ИСП РАН и Национальный суперкомпьютерный центр в Цзинане (КНР) — один из шести, организованных за последние 15 лет в Китае для развития отрасли, подписали соглашение о создании «Китайско-Российской совместной лаборатории искусственного интеллекта». В рамках лаборатории будут проводиться совместные исследования и разработки в различных аспектах искусственного интеллекта: кибербезопасность и доверенность, медицина и др. Подписание состоялось 4 июня 2025 года в Китае в рамках съезда Международной ассоциации академий наук (МАН).
- ИСП РАН стал одним из семи победителей в конкурсном отборе Министерства экономического развития Российской Федерации на поддержку Исследовательских центров в сфере искусственного интеллекта 3-й волны (Протокол № И-25-139-66879-1-0003 от 30.05.2025).
- 21 мая 2025 года Председатель Правительства Российской Федерации Михаил Мишустин распоряжением №1266-р утвердил ИСП РАН в качестве единственного исполнителя проекта по созданию унифицированной среды разработки безопасного отечественного ПО. Решение принято в рамках проектов «Инфраструктура кибербезопасности» и «Экономика данных». Работа ведется по контракту с Федеральной службой по техническому и экспортному контролю (ФСТЭК России).
- На форуме Kazan Digital Week 2025 ИСП РАН и ПАО «Ростелеком» заключили соглашение о совместной разработке отечественных конвейеров безопасной разработки ПО. На основании данного соглашения, ИСП РАН отвечает за создание методологии и предоставляет собственные инструменты анализа кода — Svace, Crusher, Sydr и Natch. Проект реализуется при поддержке ФСТЭК и основан на наработках, полученных в ходе проекта «Унифицированная среда разработки безопасного отечественного ПО».

- Комплекс моделей искусственного интеллекта и алгоритмов федеративного обучения классификации ЭКГ, разработанный в ИСП РАН, признан одним из ключевых результатов Российской академии наук за 2024 год. Модели демонстрируют высокие показатели чувствительности и специфичности при детектировании 11 распространенных патологий, а алгоритмы федеративного обучения позволяют организациям проводить обучение на распределенных наборах данных без передачи. Созданные модели стали основой готового решения – «Диагностическое ПО для нейросетевого анализа ЭКГ ИСП РАН», которое прошло клинические испытания в НМИЦ имени В. А. Алмазова и зарегистрировано в качестве медицинского изделия III класса риска.

 - ИСП РАН вошёл в состав Научно-технологического центра развития мРНК-технологий (распоряжение № 195-р от 03.02.2025 Председателя Правительства Российской Федерации Михаила Мишустина) и будет вести работы по созданию цифровых конвейеров разработки инновационных препаратов лечения онкологических заболеваний.
- Центр объединяет 17 ведущих научных организаций в форме консорциума под руководством НИЦ эпидемиологии и микробиологии им. Н. Ф. Гамалеи.
- Коллектив ИСП РАН за выдающиеся достижения в научно-исследовательской деятельности, разработку и внедрение инновационных технологий в 2025 году отмечен Благодарностью Президента Российской Федерации (Распоряжение Президента Российской Федерации от 30.09.2025 г. № 377-рп).

ИСП РАН: ЭКОСИСТЕМА ИННОВАЦИЙ

Деятельность ИСП РАН нацелена на внедрение результатов фундаментальных исследований в индустрию. Бизнес-модель института состоит из трёх тесно связанных активностей, которые в совокупности дают синергетический эффект:

- проектно-ориентированные фундаментальные и прикладные исследования в области системного программирования, нацеленные на создание новых технологий (по контрактам с российскими и зарубежными компаниями, Минобрнауки России, программам РАН, грантам РФФИ и т.п.);
- внедрение новых технологий в компаниях-партнёрах и формирование инновационных продуктов после получения обратной связи от индустрии;
- обучение студентов и аспирантов на основе разработанных технологий (с обязательным участием в исследовательских и промышленных проектах института).

Такая модель хорошо известна и применяется в исследовательских лабораториях ведущих университетов (Stanford, MIT, Berkeley, Carnegie Mellon) и промышленных гигантов (IBM, Intel), а также в государственных исследовательских центрах (INRIA, Fraunhofer). При условии эффективной реализации данная модель позволяет решить проблему разрыва между наукой и промышленностью, а также организовать подготовку кадров высшей квалификации.

ФУНДАМЕНТАЛЬНЫЕ ИССЛЕДОВАНИЯ

Фундаментальные исследования и проведение экспериментальных работ — необходимые элементы деятельности института, позволяющие двигаться в русле новейших тенденций в мире IT, а также генерировать собственные идеи для проектов с бизнес-партнёрами. ИСП РАН ведёт большое число научных и образовательных программ и сотрудничает с ведущими российскими и зарубежными научными и университетскими центрами.

Это позволяет обеспечивать высокий уровень результатов исследований, а репутация в академических и универси-

тетских кругах открывает перспективу внедрения отечественных технологий на международных рынках.

В рамках научной деятельности ИСП РАН осуществляет выпуск собственного издания «Труды ИСП РАН» (индексируется в РИНЦ, включён в Russian Science Citation Index (RSCI)). Институт отвечает также за выпуск и редактуру журнала РАН «Программирование». Оба издания входят в перечень ВАК.

ВНЕДРЕНИЕ

ИСП РАН внедряет результаты своих исследований через крупные промышленные и исследовательские организации, которые одновременно используют новые технологии института и продвигают их в широкую практику. Большая часть работ по контрактам ведётся с долговременными партнёрами, в числе главных — «Лаборатория Касперского», «Код Безопасности», «Открытая мобильная платформа», «СберТех», АО «НПО РусБИТех», ГосНИИАС, «Базальт СПО». В настоящее время технологии института используются более чем в 200 компаниях.

Одна из форм организации долгосрочного сотрудничества в ИСП РАН — это совместные лаборатории. При наличии постоянного финансирования они позволяют гибко планировать имеющиеся ресурсы, а также наращивать компетенции во вновь образующихся направлениях системного программирования и организовывать подготовку молодых специалистов с компетенциями в интересующих партнёров областях.

НАУЧНОЕ СОТРУДНИЧЕСТВО

В 2009 г. в институте была открыта совместная лаборатория с Samsung, нацеленная на анализ программ, в том числе на обеспечение безопасности в контексте ОС Android и Tizen, а впоследствии — на применение методов искусственного интеллекта в программной инженерии. В 2019 г. были открыты совместные лаборатории с Huawei. В настоящее время в ИСП РАН успешно функционирует ряд лабораторий, в числе которых:

- Лаборатория цифрового моделирования технических систем, где ведётся разработка ПО для решения сложных промышленных задач;
- Лаборатория «Лингвистические платформы», где совместно с Институтом языкознания РАН и другими организациями проводятся работы по документации исчезающих языков;
- Молодёжная лаборатория по федеративному обучению (при поддержке Минобрнауки России) и др.

ЦЕНТРЫ

Важная миссия института заключается в создании и модерировании сообществ. Развиваются три центра:

- Исследовательский центр доверенного искусственного интеллекта (в рамках федерального проекта «Искусственный интеллект»);
- Центр исследований безопасности системного ПО (создан по инициативе ФСТЭК России);
- Научный центр мирового уровня (НЦМУ) «Цифровой био-дизайн и персонализированное здравоохранение».

ИНТЕЛЛЕКТУАЛЬНАЯ СОБСТВЕННОСТЬ

В бизнес-модели ИСП РАН права на интеллектуальную собственность остаются у института или передаются сообществу разработчиков свободного программного обеспечения (СПО) в рамках специальных соглашений. С учётом специфики данной модели была разработана оригинальная лицензия, базирующаяся не на получении роялти, а на прямом финансировании со стороны заказчика дальнейших исследований и разработок, направленных на развитие технологии. Заказчику передаются неисключительные права по использованию, при этом исключительные остаются за институтом. В отдельных ситуациях решение по управлению правами принимается индивидуально с учётом перспектив долгосрочного развития.

СВОБОДНОЕ ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ (СПО)

Один из важнейших компонентов созданной экосистемы — широкое использование СПО, без которого невозможно представить себе современное системное программирование. СПО рассматривается как:

- инструмент, предоставляющий легитимный свободный доступ ко всем современным технологиям, включая готовые к использованию программные продукты и открытые стандарты;
- возможность вести инновационное развитие без аутсорсинга благодаря взаимодействию с глобальным рынком продуктов и услуг;
- мощный образовательный ресурс: среда и инфраструктура международных СПО-проектов могут использоваться для подготовки специалистов. Научная деятельность подразумевает открытость результата и «видимость» его автора, что часто приходит в противоречие с корпоративной политикой IT-компаний. Для ИСП РАН открытость результатов исследований — это одновременно и стимул к работе, и инструмент продвижения технологий института. Открытость приводит к тому, что каждый молодой исследователь «виден» в международном сообществе IT-специалистов. Его вклад и репутация — это его капитал, и институт делает всё возможное, чтобы этот капитал рос максимально быстро.

ОБРАЗОВАНИЕ

Краеугольный камень экосистемы инноваций ИСП РАН — образовательная деятельность, которая осуществляется по нескольким направлениям:

- Интеграция ИСП РАН с ведущими вузами. Кафедры системного программирования под руководством института работают в МГУ им. М.В. Ломоносова, МФТИ и НИУ ВШЭ. С первого курса студентам читаются лекции по дисциплинам системного программирования, а также проводятся семинары. На третьем курсе, после распределения на кафедры системного программирования, студенты продолжают слушать лекции, посещают спецсеминары, знакомятся с исследовательской тематикой по научным направлениям института, начинают участвовать в проектах и получать специальную стипендию. К моменту выпуска многие учащиеся имеют научные публикации и уже являются специалистами по системному программированию.

Сотрудники ИСП РАН проводят обновление учебных курсов и модернизацию программ, развивая кибербезопасность как научную специальность. В частности, в 2021 г. под научным руководством института началась модернизация бакалаврской программы «Программная инженерия» на факультете компьютерных наук НИУ ВШЭ. Развивается сотрудничество и с другими вузами (например, с МГТУ им. Н.Э. Баумана, Чувашским государственным университетом, Саратовским государственным университетом, Московским авиационным институтом) — по организации совместных учебных программ, семинаров, написанию дипломных работ. В 2022 г. в МГИМО МИД России запущена совместная с ИСП РАН магистерская программа «Анализ данных и динамика международных процессов»; открыта Лаборатория интеллектуального анализа данных, где ведутся работы с использованием платформы Talisman. В 2023 г. на базе Института динамики систем и теории имени В. М. Матросова СО РАН создана совместная с ИСП РАН научно-исследовательская группа. В числе основных направлений деятельности — разработка программных средств анализа электронных документов и обработки естественного языка.

- Стипендиальная программа. В рамках поддержки образовательных процессов институт запустил стипендиальную программу, которая охватывает студентов ряда образовательных организаций, в числе которых МГУ им. М.В. Ломоносова, МФТИ, НИУ ВШЭ, Новгородский государственный университет им. Ярослава Мудрого, Российско-Армянский университет и др.
- Собственная аспирантура ИСП РАН, предусматривающая одновременно накопление практического опыта и изучение новых технологий. Аспиранты активно вовлекаются в процессы обучения: ведут семинарские и практические занятия со студентами, руководят подготовкой курсовых и дипломных работ. Накопив такой опыт, выпускник аспирантуры, как правило, становится руководителем небольшой исследовательской группы.
- Развитие сети лабораторий системного программирования. Активно работают лаборатории в Ереване, в Великом Новгороде, в Орле, а также в Москве — в РЭУ им. Г.В. Плеханова. Лаборатории привлекают к работе успешных студентов и аспирантов, которые занимаются разработкой перспективных технологий в тесном сотрудничестве с индустрией.

КОНФЕРЕНЦИИ

Ежегодно институт проводит ряд мероприятий, в числе которых:

- Международная Открытая конференция ИСП РАН им. В.П. Иванникова: <https://www.isprasopen.ru/>
- Научно-практическая конференция OS DAY (совместно с другими организаторами): <https://www.osday.ru/>
- Международная конференция «Иванниковские чтения»: <https://www.ivannikov-ws.org/>
- Международная научно-практическая конференция «Анализ данных в медицине» (совместно с другими организаторами): <https://digital-med.ru/>
- Весенняя конференция молодых учёных в области программной инженерии: <http://syrcose.ispras.ru/>

2025. ЦЕНТР ИССЛЕДОВАНИЙ БЕЗОПАСНОСТИ СИСТЕМНОГО ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ

СОВМЕСТНО С ФСТЭК РОССИИ
В ПАРТНЁРСТВЕ С ИНДУСТРИЕЙ
PORTAL.LINUXTESTING.RU

ГЛАВНЫЕ ДОСТИЖЕНИЯ 2025 ГОДА:

ОРГАНИЗАЦИОННЫЕ:

- произошла трансформация Консорциума, нацеленная на то, чтобы Консорциум координировал работу Центра не только в части исследования ядра Linux, но и в части других компонентов с открытым исходным кодом;
- к Консорциуму по поддержке Центра присоединились более 70 организаций.

МЕТОДИЧЕСКИЕ:

- подготовлены методики проведения исследования PostgreSQL, Kubernetes, OpenJDK.

Ранее:

- подготовлены рекомендации по конфигурированию ядра с целью повышения его безопасности;
- подготовлены рекомендации по настройке доверенной загрузки ядра;
- подготовлены методики проведения исследования ядра Linux, OpenSSL, NGinx, Qemu, libvirt, podman, .NET Runtime, ASP .NET Core, Node.js, Python, OpenSSH.

ТЕХНОЛОГИЧЕСКИЕ:

- ведётся сопровождение трёх веток ядра Linux, основанных на стабильных версиях 5.10, 6.1 и 6.10;
- проведён анализ более 45 тысяч предупреждений инструмента статического анализа Svace (разработан в ИСП РАН), из которых более 25 тыс. прошли независимую кросс-верификацию;
- подготовлены более 650 исправлений, которые уже приняты в основную ветку ядра, и более 200 исправлений, принятых в основные ветки компонентов OpenSSL, Qemu, libvirt, CPython, Lua, .NET Runtime и др.

ПАРТНЁРЫ ЦЕНТРА:

- ООО «Айдеко»
- АО «Аксиом»
- АО «Актив-Софт»
- АО «Аладдин Р.Д.»
- АО «АЛТЭК-СОФТ»
- ООО «АМИКОН»
- ООО Фирма «АНКАД»
- ООО «АСКОН-Бизнес-Решения»
- ООО «Базальт СПО»
- ООО «БАЗИС»
- АО «БАРС Груп»
- ООО «БИЗон»
- ООО «ВК Цифровые технологии»
- ООО «Газинформсервис»
- ООО «ДАКОМ М»
- ЗАО «ЗЭТ»
- АО «ИВК»
- ООО «Инферит»
- ООО «ИнфоВотч АРМА»
- АО «ИнфоТеКС»
- ООО «ИТБ»
- ООО «Киберпротект»
- ООО «Клауд Солюшенс»
- ООО «КНС ГРУПП»
- ООО «Код Безопасности»
- ООО «Конфидент»
- ООО «Корбит»
- ООО «НПЦ «КСБ»
- АО «Лаборатория Касперского»
- ООО «МТ-Интеграция»
- АО «МЦСТ»
- ООО «Национальный каталог»
- АО «НИЦ ЦТ»
- ООО «НПО «НовоТест-Системы»
- АО «НППКТ»
- ООО «НЦПР»
- ООО «Оператор-ЦРПТ»
- ООО «ОРИОН»
- ООО «Открытая мобильная платформа»
- ООО «ПиЭлСи Технолоджи»
- ООО «ППГ»
- АО «РАСУ»
- ООО «РЕД СОФТ»
- АО «НТЦ ИТ РОСА»
- ООО «РТК ИТ Плюс»
- ООО «РТТ»
- ООО «РусБИТех-Астра»
- ФГУП «РФЯЦ-ВНИИЭФ»
- АО МВП «Свемел»
- ООО «Системные решения»
- ООО «СОЛАР Секьюрити»
- ООО «С-Терра СиЭсПи»
- ООО «ТеконАвтоматика»
- ООО «ТехАргос»
- ООО «ТСС»
- АО «ФИНТЕХ»
- АО «Флант»
- ООО «ЭнджиАр Софтлаб»
- АО «НПО «Эшелон»
- ООО «Юзергейт»
- ООО «ЯНДЕКС.ОБЛАКО»

ОБРАЗОВАТЕЛЬНЫЕ ПАРТНЁРЫ:

- МГУ им. М.В. Ломоносова
- МФТИ
- НИУ ВШЭ
- Вологодский государственный университет
- НИУ «МЭИ»
- МГТУ им. Н.Э. Баумана
- Воронежский государственный университет
- МИРЭА – Российский технологический университет
- Чувашский государственный университет им. И.Н. Ульянова

2025. ИССЛЕДОВА- ТЕЛЬСКИЙ ЦЕНТР ДОВЕРЕННОГО ИСКУССТВЕННОГО ИНТЕЛЛЕКТА

В СОТРУДНИЧЕСТВЕ С МИНЭКОНОМРАЗВИТИЯ РОССИИ;

**С АКАДЕМИЧЕСКИМ СООБЩЕСТВОМ (СКОЛТЕХ, МЕХМАТ МГУ, УНИВЕРСИТЕТ
СИРИУС, НМИЦ ИМ. В. А. АЛМАЗОВА МИНЗДРАВА РОССИИ);**

**С ИНДУСТРИЕЙ (МИД РОССИИ, ПАО «СБЕРБАНК РОССИИ», АО «ЛАБОРАТОРИЯ
КАСПЕРСКОГО», ООО «ТЕЛКОР», ООО «ПРОФИСКОП», ООО «ИНТЕРПРОКОМ»,
ООО НТЦ «ФОБОС-НТ», ООО «СИСТЕМНЫЕ РЕШЕНИЯ»).**

В 2025 ГОДУ БЫЛИ РАЗРАБОТАНЫ:

- Новые версии фреймворков TrustFlow-v2.20.0. (доверенная версия фреймворка TensorFlow) и TrustTorch-v2.8.0. (доверенная версия фреймворка PyTorch);
- Инструмент для выявления дефектов исходного кода или бинарных файлов;
- Инструмент для повышения безопасности генерации изображений с помощью модели генеративного ИИ.

Облачная платформа для создания доверенных ИИ-систем обновлена с учётом требований индустрии. Интегрированные инструменты, основанные на передовых практиках MLOps и методах противодействия новым угрозам, применяются Консорциумом по исследованию безопасности искусственного интеллекта.

ЦЕНТРОМ РАЗРАБАТЫВАЮТСЯ

(завершение запланировано в конце 2026 года):

- комплекс ИИ-решений для повышения эффективности системы здравоохранения и создание многопрофильного медицинского ИИ-помощника для экосистемы заказчика (ПАО «Сбербанк России»);
- доверенная версия большой языковой модели, адаптированной для решения аналитических задач в области внешнеполитической деятельности (МИД РФ);
- программный комплекс для обеспечения доверия к преодобученным LLM при работе с корпоративными данными (АО «Лаборатория Касперского»).

**ЦЕНТР ВЫСТУПАЕТ ПАРТНЕРОМ
ИССЛЕДОВАТЕЛЬСКИХ ЦЕНТРОВ В СФЕРЕ
ИСКУССТВЕННОГО ИНТЕЛЛЕКТА «2-Й ВОЛНЫ»,
ТАКИХ КАК:**

- Исследовательский центр в сфере искусственного интеллекта в здравоохранении НМИЦ онкологии им. Н.Н. Блохина;
- Исследовательский центр в сфере искусственного интеллекта по направлению «Транспорт и логистика» НИЯУ МИФИ;
- Исследовательский центр «Доверенный искусственный интеллект для здравоохранения» ННГУ им. Н.И. Лобачевского;
- Центр искусственного интеллекта и науки о данных СПбГУ.

2025. ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ **ДЛЯ** **ПЕРСОНАЛИЗИРОВАН-** **НОГО ОПРЕДЕЛЕНИЯ** **ПОСЛЕДОВАТЕЛЬНОСТИ** **МРНК-ВАКЦИНЫ** **ПО ГЕНЕТИЧЕСКИМ** **ДАННЫМ**

В СОТРУДНИЧЕСТВЕ

**В ФГБУ «НИЦЭМ ИМ. Н. Ф. ГАМАЛЕИ» МИНЗДРАВА РОССИИ
И ФГБУ «НМИЦ РАДИОЛОГИИ» МИНЗДРАВА РОССИИ**

Цель проекта – разработка экспериментального образца программного комплекса, обеспечивающего выбор наиболее перспективных неоантигенов для персонифицированного лечения онкологических заболеваний с использованием мРНК-вакцин.

В современной онкологии все больше делается упор на персонализированные подходы, где ключевым условием становится точный выбор мишеней для иммунной системы конкретного пациента. Одним из наиболее перспективных направлений является разработка мРНК-вакцин, кодирующих индивидуально подобранные неоантигены – короткие пептиды, возникающие в злокачественных опухолях в результате уникальных для пациента соматических мутаций. Эти пептиды отсутствуют в нормальных тканях и способны вызывать специфический иммунный ответ, направленный против опухоли.

Процесс отбора кандидатов в неоантигены представляет собой сложную вычислительную задачу, требующую комплексной интеграции различных источников данных: данных секвенирования экзома или генома опухоли, данных секвенирования экзома или генома нормальных тканей, данных секвенирования транскриптома. При этом важно учитывать ряд параметров, таких как уровень экспрессии генов, расположение мутации, сила взаимодействия пептида с молекулами главного комплекса

гистосовместимости. Это обуславливает необходимость создания специализированных вычислительных инструментов, обеспечивающих автоматизированный, воспроизводимый и масштабируемый анализ для надежного отбора неоантигенов.

Цель данного проекта заключается в разработке программного комплекса, предназначенного для автоматизированного выбора наиболее перспективных неоантигенов для создания индивидуализированных мРНК-вакцин для лечения онкологических заболеваний.

**В ЧИСЛЕ
ГЛАВНЫХ
ДОСТИЖЕНИЙ
2025 ГОДА:**

РАЗРАБОТАНО ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ ДЛЯ ПЕРСОНАЛИЗИРОВАННОГО ОПРЕДЕЛЕНИЯ ПОСЛЕДОВАТЕЛЬНОСТИ мРНК-ВАКЦИНЫ ПО ГЕНЕТИЧЕСКИМ ДАННЫМ

Разработана Программа для ЭВМ «Базовый экспериментальный образец биоинформатического программного конвейера для автоматизированного поиска неоантигенов» (Свидетельство о государственной регистрации программы для ЭВМ №2025661235 от 05 мая 2025 г.

Программный комплекс для подбора противоопухолевой лекарственной терапии, разработанный в рамках выполнения НИР, объединенной командой ФГБУ «НИЦЭМ им. Н. Ф. Гамалеи», ИСП РАН и ФГБУ «НМИЦ радиологии» Минздрава России и Минздрава России, был зарегистрирован ФГБУ «НМИЦ радиологии» Минздрава России по правилам Постановления Правительства РФ от 24 ноября 2021 г. N 2026 «О незарегистрированных медицинских изделиях для диагностики *in vitro*» (Приказом Росздравнадзора от 06.08.2025 №4720 было предоставлено разрешение на применение незарегистрированного медицинского изделия для диагностики *in vitro* «Набор реагентов с программным обеспечением для подбора противоопухолевой лекарственной терапии, в том числе мРНК вакцин, и других биотехнологических лекарственных препаратов (БТЛП), производимых по индивидуальному назначению на основании результатов генетических исследований (ОнкоБиотехСет-МНИОИ)», производства ФГБУ «НМИЦ радиологии» Минздрава России, № P012-00110-77.02871296, дата предоставления разрешения 06.08.2025).

СОТРУДНИЧЕСТВО В РАМКАХ НАУЧНО- ТЕХНОЛОГИЧЕСКОГО ЦЕНТРА РАЗВИТИЯ МАТРИЧНЫХ РНК-ТЕХНОЛОГИЙ, СОЗДАННОГО ПО РАСПОРЯЖЕНИЮ ПРАВИТЕЛЬСТВА 195-Р ОТ 03.02.2025

Сотрудники ИСП РАН приняли участие в первом (Сириус) и втором (КФУ) заседаниях Научно-технологического Центра развития мРНК-технологий при участии директора НИЦЭМ им. Гамалеи Минздрава России Александра Леонидовича Гинцбурга.

Доклад «Дата-центры и системное ПО как основа разработки диагностических инструментов на основе искусственного интеллекта» директора ИСП РАН академика Арутюна Ишхановича Аветисяна в рамках заседания НТЦ развития мРНК-технологий в Казани.

Сотрудники ИСП РАН приняли участие в проведении дополнительной профессиональной программы повышения квалификации «мРНК-технологии для создания инновационных лекарственных средств».

2025. НАУЧНЫЙ ЦЕНТР МИРОВОГО УРОВНЯ (НЦМУ) «ЦИФРОВОЙ БИОДИЗАЙН И ПЕРСО- НАЛИЗИРОВАННОЕ ЗДРАВООХРАНЕНИЕ»

В КОНСОРЦИУМЕ С СЕЧЕНОВСКИМ УНИВЕРСИТЕТОМ, ИБМХ, НОВГУ
И ИКТИ РАН

**В ЧИСЛЕ
ГЛАВНЫХ
ДОСТИЖЕНИЙ:**

**ОБЕСПЕЧЕНА ВОЗМОЖНОСТЬ РАБОТЫ ОБЛАЧНОЙ
ПЛАТФОРМЫ НЦМУ «ЦИФРОВОЙ БИОДИЗАЙН
И ПЕРСОНАЛИЗИРОВАННОЕ ЗДРАВООХРАНЕНИЕ»
В ФЕДЕРАТИВНОМ РЕЖИМЕ.**

Платформа позволяет наращивать вычислительные ресурсы путем использования ИТ-инфраструктуры внешних организаций, при этом управление ресурсами осуществляется с использованием методов домноспецифичной оркестрации. На текущий момент реализована поддержка оркестратором Michman (входит в состав облачной среды Asperitas) создания виртуальных ресурсов, описываемых на языке OASIS TOSCA, в различных экземплярах развёртываний облачных сервисов на базе Openstack и Yandex Cloud.

Федеративный режим работы обеспечивает централизованное управление распределёнными ресурсами и позволяет передавать задачи на исполнение на соответствующие вычислительные ресурсы в зависимости от установленных правил.

**ВПЕРВЫЕ В РОССИИ ПРОВЕДЁН ЭКСПЕРИМЕНТ
ПО ОБУЧЕНИЮ МОДЕЛИ КЛАССИФИКАЦИИ
12-КАНАЛЬНЫХ ЭКГ С ИСПОЛЬЗОВАНИЕМ
АЛГОРИТМОВ ФЕДЕРАТИВНОГО МАШИННОГО
ОБУЧЕНИЯ**

Федеративное (совместное) обучение предназначено для проектов, где есть несколько участников с собственными наборами данных, или датасетами. Такой подход позволяет участникам коллективно обучать модели,

никому не передавая свои данные. Это открывает новые возможности для партнёрств в сфере искусственного интеллекта.

Яндекс, ИСП РАН и Сеченовский университет, используя федеративный подход, создали нейросеть, которая по данным электрокардиограмм выявляет фибрилляцию предсердий — одну из наиболее распространенных патологий сердца. Технология делает это с высокими показателями чувствительности и специфичности.

Для обучения использовались два независимых датасета с электрокардиограммами: от Сеченовского университета и от ИСП РАН. Оба партнёра провели раунды обучения на своей стороне, а затем передали результаты в общий контур.

За техническую составляющую проекта отвечали инженеры Yandex Cloud и ИСП РАН. В Yandex Cloud продумали этапы реализации, предложили стек технологий, создали унифицированную среду для обучения и рассчитали необходимый объём ресурсов. В ИСП РАН разработали модель и адаптировали её под опенсорсный фреймворк федеративного обучения. Сеченовский Университет дал экспертную оценку качества модели.

Теперь в подобных проектах смогут участвовать компании из отраслей, где работают с чувствительными данными (медицина, финансы и др.).

ПРОВЕДЕНА ПОЛНОМАСШТАБНАЯ ОПЫТНАЯ ЭКСПЛУАТАЦИЯ ПЛАТФОРМЫ.

В 2024 году проведена опытная эксплуатация Платформы с привлечением всех участников Консорциума НЦМУ (ИБМХ, ИКТИ РАН, НовГУ, Сеченовский университет). Приглашены также внешние организации. В ходе опытной эксплуатации с использованием инструментов Платформы решались такие задачи как:

- определение вероятности наличия риска злокачественных новообразований;
- детектирование гипертонической ретинопатии по цифровым изображениям глазного дна;
- обнаружение лимфоваскулярной инвазии рака лёгкого на гистологических скан-изображениях рака лёгкого;
- предсказание уровня экспрессии белков на основании экспрессии транскриптов;
- обнаружение меланомы и рака кожи за счёт анализа дерматоскопических снимков;
- а также другие задачи биомедицинского домена.

Кроме того, на базе Платформы НЦМУ продолжают работы по аннотированию врачами 12-канальных ЭКГ, что в дальнейшем позволит создать качественный набор данных для дообучения нейросетевой модели классификации 12-канальных ЭКГ.

Достижения института в области цифровой медицины получили и международное признание: 2-4 июля 2024 г. в рамках конференции IEEE COMPSAC в Японии прошёл первый семинар по цифровой кардиологии DICAR 2024, организованный ИСП РАН совместно с Сеченовским университетом, ННГУ, Белградским университетом и другими организациями.

РАНЕЕ В РАМКАХ НЦМУ:

СОЗДАНА И ВВЕДЕНА НА УРОВНЕ СЕЧЕНОВСКОГО УНИВЕРСИТЕТА ОБЛАЧНАЯ ПЛАТФОРМА НЦМУ «ЦИФРОВОЙ БИОДИЗАЙН И ПЕРСОНАЛИЗИРОВАННОЕ ЗДРАВООХРАНЕНИЕ».

Разработанная ИСП РАН Платформа НЦМУ обеспечивает предоставление следующих сервисов:

- базовых облачных сервисов (например, виртуальных серверов и блочных устройств по запросу);
- сервисов по сбору, хранению и анализу больших медицинских данных;
- сервисов по разметке медицинских данных и по применению алгоритмов машинного обучения для решения задач биомедицинского домена;
- сервисов поддержки процессов проведения совместных исследований.

Платформа НЦМУ реализована на базе облачной среды Asperitas (ИСП РАН). В 2023 г. в Платформу включен функционал по формированию научной базы знаний в рамках медицинского исследования с использованием технологий сбора и анализа больших данных, реализованный на базе информационно-аналитической системы Talisman (ИСП РАН). Тестирование облачных сервисов осуществлялось на примере web-лабораторий по анализу данных электрокардиограмм и гистологических изображений.

Платформа НЦМУ может быть развёрнута на базе облачной инфраструктуры ИСП РАН или сторонней облачной инфраструктуры для биомедицинских задач, решаемых в рамках НЦМУ, или адаптирована под задачи других медицинских доменов.

ВЫПОЛНЕНА РАБОТА ПО РАЗВИТИЮ И ВНЕДРЕНИЮ НЕЙРОСЕТЕВОЙ МОДЕЛИ КЛАССИФИКАЦИИ 12-КАНАЛЬНЫХ ЭКГ.

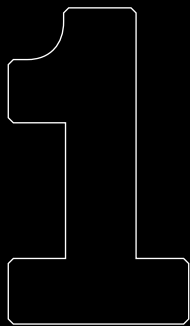
Нейросетевая модель классификации 12-канальных ЭКГ обучена на данных из разных регионов (Республика Татарстан, Москва, Великий Новгород), интегрирована в режиме опытной эксплуатации в систему «Единый Кардиолог» и апробирована на данных ЭКГ Республики Татарстан. Подписано соглашение о сотрудничестве со Станцией скорой и неотложной медицинской помощи им. А.С. Пучкова. Проанализировано несколько десятков тысяч ЭКГ, полученных от Станции. Качество предсказания моделей сравнимо с 10-секундными 12-канальными ЭКГ. Подписаны протоколы тестирования. В настоящее время разработка проходит регистрацию в качестве медицинского изделия.

РЕАЛИЗОВАНА СИСТЕМА РАЗМЕТКИ 12-КАНАЛЬНЫХ ЭКГ.

Качественная стандартизированная разметка по заранее определённому списку патологий помогает достичь высокой степени согласия между экспертами. Система разметки реализована на базе Платформы НЦМУ и врачами функциональной диагностики проведена ее апробация.

ОБУЧЕНА НЕЙРОСЕТЕВАЯ МОДЕЛЬ ДЕТЕКЦИИ КЛЕТОЧНЫХ ЯДЕР ENDONET НА ГИСТОЛОГИЧЕСКИХ ПРЕПАРАТАХ.

Нейросеть обучена на размеченном гистологическом наборе EndoNuke, собранном совместно с партнёрами (РУДН, ГКБ №31, НМИЦ АГП им. В.И. Кулакова, НовГУ и НИИ морфологии человека). Модель детекции ядер встроена в открытую программную платформу для анализа биоизображений QuPath с использованием технологии ИСП РАН Fanlight. Модифицированная платформа QuPath и система разметки изображений с открытым кодом CVAT подготовлены для интеграции в облачную платформу ИСП РАН Asperitas.



АНАЛИЗ ПРОГРАММ И КИБЕР- БЕЗОПАСНОСТЬ

КОМПИЛЯТОРНЫЕ ТЕХНОЛОГИИ И ВЕРИФИКАЦИЯ

- 29 AstraVer Toolset: система верификации ключевых компонентов
- 32 Klever: система автоматической статической верификации Си-программ
- 34 Masiw: набор инструментов для проектирования ответственных систем
- 36 MicroTESK: генератор тестовых программ
- 38 Utopia EDA: система логического синтеза цифровых интегральных схем
- 40 Buildography: инструмент идентификации реквизитов сборки
- 42 Безопасный компилятор
- 47 Svace: статический анализатор исходного кода
- 52 КЛОС: конфигурируемая линейка операционных систем
- 54 TestOS: окружение для тестирования программного обеспечения
- 56 ANIS: поддержка процессов верификации средств защиты информации на основе формальных моделей управления доступом

АНАЛИЗ БИНАРНОГО КОДА, ФАЗЗИНГ

- 58 Блесна: инструмент динамического анализа помеченных данных
- 60 Платформа для анализа программ на основе эмулятора QEMU
- 63 ИСП Crusher: комплекс динамического и статического анализа бинарного кода
- 69 BinSide: статический анализатор бинарного кода
- 71 Natch: инструмент определения поверхности атаки
- 74 Sydr-fuzz: комплекс гибридного фаззинга и динамического анализа
- 77 LibAFL-DiFuzz: инструмент направленного фаззинга
- 79 ISP Aurora: статический анализатор с технологией искусственного интеллекта
- 80 ISPuaro: композиционный анализ

АНАЛИЗ СЕТЕВОГО ТРАФИКА

- 82 Protosphere: система анализа сетевого трафика
- 85 ML IDS: сетевая система обнаружения вторжений с применением машинного обучения

УПРАВЛЕНИЕ ТРЕБОВАНИЯМИ

- 88 Requality: инструмент управления требованиями

ASTRAVER TOOLSET:

СИСТЕМА ВЕРИФИКАЦИИ КЛЮЧЕВЫХ КОМПОНЕНТОВ



AstraVer Toolset — система дедуктивной верификации ключевых компонентов. Позволяет разрабатывать и верифицировать модели политик безопасности, а также проводить доказательство корректности компонентов на языке C. Необходимый инструмент достижения целей семейств доверия ADV_SPM и ADV_FSP, определённых в ГОСТ Р ИСО/МЭК 15408-3-2013.

ОСОБЕННОСТИ И ПРЕИМУЩЕСТВА

AstraVer Toolset — комплекс инструментов, предназначенный для промышленного использования и основанный на многолетних научных исследованиях. Объединяет два подхода к верификации: на уровне моделей и на уровне кода. Включает два отдельных инструмента верификации компонентов на языке C: стабильный транслятор AstraVer, аналогичный Microsoft VCC и Frama-C/WP, но адаптированный для применения к коду ядер ОС, а также перспективный инструмент верификации Isabelle/PLRDF, основанный на новом методе интерактивной абстрактной интерпретации.

AstraVer Toolset — это:

- Комплексный подход к верификации — от формализации требований верхнего уровня до анализа поведения кода.
- Моделирование функциональных требований (формализация функциональных требований к системе, доказательство внутренней согласованности требований и недостижимости небезопасных состояний).
- Тестирование реализации на соответствие функциональным требованиям с использованием формальной модели требований для проверки корректности наблюдаемого поведения в целях оценки качества тестирования и генерации тестов.
- Верификация ключевых компонентов на языке C (формализация требований к ключевым компонентам, доказательство корректности работы компонента на всех возможных входных данных).

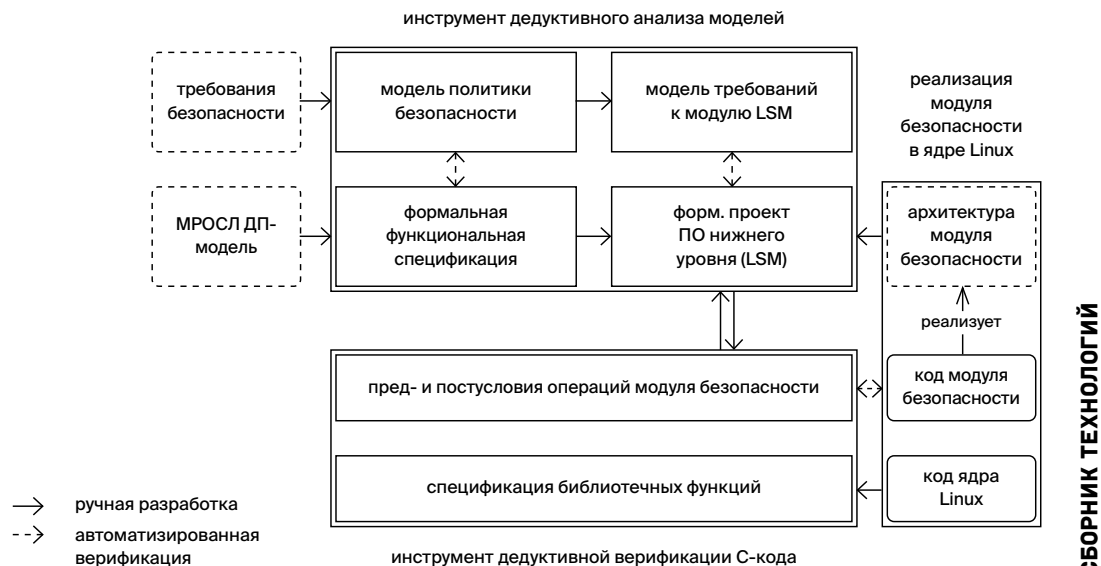
- Поддержка индустриального кода (нестандартные расширения компилятора GCC, арифметические операции с побитовой точностью, адресная арифметика (включая поддержку конструкции `container_of`), функциональные указатели, приведение целочисленных типов к указательным).
- Решение важнейших задач профилей защиты:
 - формальное моделирование политики безопасности;
 - формальное доказательство внутренней непротиворечивости модели политики безопасности и недостижимости небезопасных состояний;
 - разработка полуформальной или формальной функциональной спецификации;
 - формальное или полуформальное доказательство соответствия между моделью политики безопасности и функциональной спецификацией;
 - формальное или полуформальное доказательство соответствия между различными представлениями целевого ПО, такими как функциональная спецификация, проект ПО и его реализация.
- Возможность доработки комплекса под конкретного заказчика (в плане поддержки верификации компонентов на языке C).
- Новый инструмент интерактивной верификации компонентов на языке C Isabelle/PLRDF, который:
 - создан на базе логического ядра Isabelle/Pure системы автоматического доказательства Isabelle/HOL и ее интегрированной среды разработки доказательств Isabelle/PIDE;
 - поддерживает выразительный язык спецификаций, основанный на логике HOL;
 - снижает затраты на верификацию за счет эффективного сочетания автоматических и интерактивных методов композиции и преобразования структурированных спецификаций;
 - реализует концепцию интерактивной двухшаговой абстрактной интерпретации контрактной спецификации вдоль путей выполнения верифицируемого блока кода. Она состоит из шага контекстуализации текущей спецификации в новом состоянии программы с помощью полностью автоматического применения правил из конфигурируемых пользователем наборов доказанных лемм, и шага реабстракции — произвольной модификации пользователем полученной контекстуализированной спецификации с доказательством корректности соответствующих преобразований.

ДЛЯ КОГО ПРЕДНАЗНАЧЕН ASTRAVER TOOLSET?

- Компании, нацеленные на разработку ПО с высокой степенью надёжности и безопасности — как информационной, так и функциональной (ПО для самолётов, АЭС и др.).
- Компании, которые нуждаются в сертификации разрабатываемого ПО в соответствии с ГОСТ Р ИСО/МЭК 15408.
- Испытательные лаборатории средств защиты информации в соответствии с требованиями безопасности.

Система AstraVer Toolset применялась при разработке средств защиты информации ОС Astra Linux Special Edition (АО «НПО РусБИТех»), которая успешно прошла сертификацию на соответствие требованиям безопасности информации ФСТЭК России к операционным системам по профилю защиты «2А». В основу отечественной разработки была положена МРОСЛ-ДП модель безопасности, а реализация её новых возможностей в ОС Astra Linux Special Edition продолжает верифицироваться с помощью AstraVer Toolset.

СХЕМА РАБОТЫ



KLEVER: СИСТЕМА АВТОМАТИЧЕСКОЙ СТАТИЧЕСКОЙ ВЕРИФИКАЦИИ СИ-ПРОГРАММ



Klever — система верификации, которая автоматически строит модели на основе исходного кода на языке программирования Си. Klever позволяет специфицировать различные требования по безопасности и надёжности, а также проверять их выполнение автоматически с заданным уровнем точности. В основе системы верификации лежат методы для покомпонентной верификации, моделирования окружения и спецификации требований, что делает возможным применение формальных методов к исходному коду размером в сотни тысяч и миллионы строк. Klever — это проект с открытым исходным кодом (<https://forge.ispras.ru/projects/klever>).

ОСОБЕННОСТИ И ПРЕИМУЩЕСТВА

Klever — это:

- Масштабируемость. Покомпонентная верификация программ позволяет применять к большому объёму исходного кода наиболее точные методы анализа, такие как верификация моделей и символьное выполнение.
- Возможность адаптации под конкретные нужды заказчиков. Разработка спецификаций моделей окружения целевых программ, а также спецификаций для обнаружения нарушений, специфичных для программ требований, в дополнение к проверке общих правил безопасного программирования на языке Си.
- Обнаружение нетривиальных ошибок. Высокоточный консервативный анализ исходного кода промышленного ПО позволяет выявлять все возможные ошибки искомым видов и доказывать корректность программ при явно заданных предположениях.
- Детализированное представление выявленных ошибок. При обнаружении ошибок система верификации выдаёт подробные трассы ошибок, включающие конкретные значения переменных и аргументов вызываемых функций.
- Удобный многопользовательский веб-интерфейс для подготовки и запуска верификации, а также для выполнения экспертной оценки результатов верификации.

ДЛЯ КОГО ПРЕДНАЗНАЧЕН KLEVER?

- Компании, разрабатывающие ПО с высоким уровнем надёжности и безопасности.
- Испытательные лаборатории и органы по сертификации.

ОПЫТ ВНЕДРЕНИЯ

Система верификации Klever успешно применяется для тщательной проверки ядер и драйверов различных операционных систем. В драйверах устройств ядра Linux удалось обнаружить более 400 ошибок, среди которых:

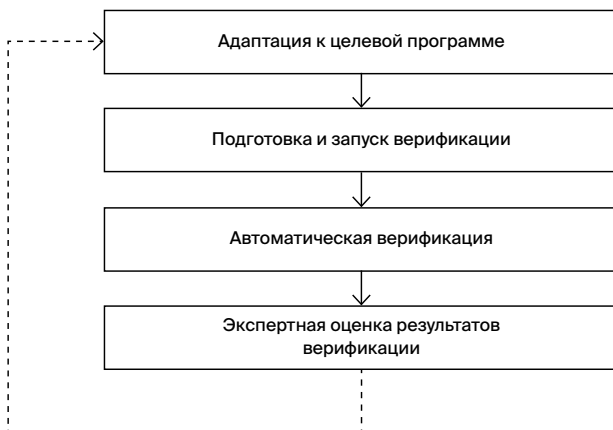
- состояния гонок,
- взаимные блокировки,
- ошибки работы с памятью (выход за границу буфера, утечки и т.д.),
- некорректные вызовы функций в зависимости от контекста,
- некорректная инициализация структур данных ядра Linux.

Данные ошибки были признаны разработчиками ядра Linux.

СИСТЕМНЫЕ ТРЕБОВАНИЯ

Ubuntu 20.04/22.04, не менее 4 процессорных ядер x86-64, 16 ГБ оперативной памяти и 100 ГБ свободного места на диске.

СХЕМА РАБОТЫ



MASIW: НАБОР ИНСТРУМЕНТОВ ДЛЯ ПРОЕКТИРОВАНИЯ ОТВЕТСТВЕННЫХ СИСТЕМ



MASIW — набор инструментов для разработки программно-аппаратных комплексов ответственных систем в сфере авиации, медицины и др. Создан для инженеров-конструкторов комплексов бортового оборудования для авиационных судов, разрабатываемого с применением интегрированной модульной авионики (ИМА). Оперативно адаптируется под другие предметные области.

ОСОБЕННОСТИ И ПРЕИМУЩЕСТВА

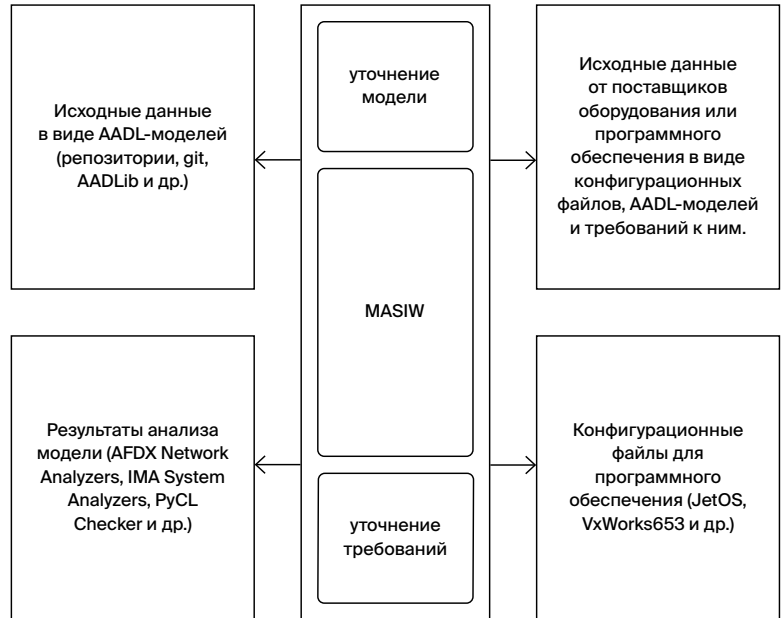
MASIW — технология для оптимизации разработки сложных программно-аппаратных комплексов, а также их верификации. Позволяет провести предварительную оценку качества изделия до появления опытного образца, а также анализ на отказоустойчивость. Снижает риск появления ошибок и дефектов. Разрабатывается совместно с ФГУП «ГосНИИАС». Несмотря на наличие инструмента OSATE на момент начала разработки, на сегодняшний день MASIW превосходит его по функциональности в плане верификации, а также статического и динамического анализа.

MASIW — это:

- Создание, редактирование и управление моделями на языке AADL:
 - создание/редактирование моделей посредством текстового или графического редактора;
 - поддержка командной разработки с возможностью отслеживания и внесения изменений для отдельных элементов модели;
 - поддержка переиспользования AADL-моделей сторонних разработчиков.
- Анализ моделей:
 - анализ структуры программно-аппаратного комплекса (достаточности аппаратных ресурсов, согласованности интерфейсов и т. п.);
 - проверка разрабатываемого программно-аппаратного комплекса на соответствие требованиям;
 - анализ характеристик передачи данных в сети AFDX (времени доставки сообщений от отправителя к получателю, глубины очередей передающих портов и т. п.);

- построение дерева неисправностей и его численный анализ для определения вероятности отказного события верхнего уровня;
- анализ видов и последствий отказов на основе архитектурной модели комплекса бортового оборудования, включая построение таблицы видов и последствий отказов;
- симуляция модели программно-аппаратного комплекса с генерацией пользовательских отчётов по результатам работы симулятора, в том числе совместная симуляция работы прикладных разделов под управлением ОС РВ в эмуляторе QEMU и универсального симулятора AADL моделей.
- Синтез моделей:
 - распределение функциональных приложений по вычислительным модулям с учётом ограничений ресурсов аппаратной платформы и с учётом дополнительных ограничений, касающихся вопросов надёжности и безопасности программно-аппаратного комплекса;
 - генерация распределения вычислительного времени процессора между функциональными приложениями (циклограмма расписания запуска приложений для ARINC-653 совместимых ОС РВ).
- Генерация конфигурационных данных:
 - разработка специализированных инструментов конфигурационных данных на основе предоставляемого программного интерфейса (API);
 - генерация конфигурационных файлов для компонентов КБО.
- Возможность расширения набора инструментов путём создания собственных модулей (благодаря модульной архитектуре в основе технологии).

СХЕМА РАБОТЫ



MICROTESK:

ГЕНЕРАТОР ТЕСТОВЫХ ПРОГРАММ



MicroTESK — реконфигурируемая и расширяемая среда генерации тестовых программ для функциональной верификации микропроцессоров и виртуальных машин. Позволяет автоматически конструировать генераторы тестовых программ на основе формальных спецификаций систем команд. MicroTESK применим для широкого спектра архитектур (RISC, CISC, стековые и регистровые виртуальные машины).

ОСОБЕННОСТИ И ПРЕИМУЩЕСТВА

MicroTESK — комплекс инструментов, включающий в себя средства моделирования (построение модели тестируемой системы по формальным спецификациям) и средства генерации (построение тестовых программ по шаблонам). Распространяется по лицензии Apache 2.0. MicroTESK доступен на сайте ИСП РАН: <https://forge.ispras.ru/projects/microtesk>. Описание технологии — на сайте <http://www.microtesk.org>.

MicroTESK — это:

- Использование формальных спецификаций в качестве источников знаний об устройстве тестируемой системы:
 - спецификации системы команд на языке nML (регистры, память и режимы адресации, логика инструкций, текстовый/бинарный формат инструкций);
 - дополнительные спецификации подсистемы памяти на языке mmuSL (свойства буферов памяти (TLB, L1 и L2), логика трансляции адресов и логика операций чтения и записи).
- Генерация тестовых программ на основе объектно-ориентированных шаблонов:
 - тестовые шаблоны на языке Ruby (описывают способ построения цепочек инструкций и тестовых данных, допускают повторное использование);
 - автоматическая генерация шаблонов по спецификациям;
 - возможность использования разных техник генерации цепочек инструкций и тестовых данных (случайная генерация, комбинаторная генерация, генерация на основе ограничений);
- Генерация вспомогательных инструментов:
 - дизассемблер;
 - эмулятор;
 - тестовый оракул.

- Широкий набор поддерживаемых архитектур микропроцессоров:
 - RISC и CISC (разработаны генераторы тестовых программ для таких архитектур, как RISC-V, ARM, MIPS, PowerPC);
 - регистровые и стековые архитектуры виртуальных машин;
 - многоядерность/многопоточность системы.

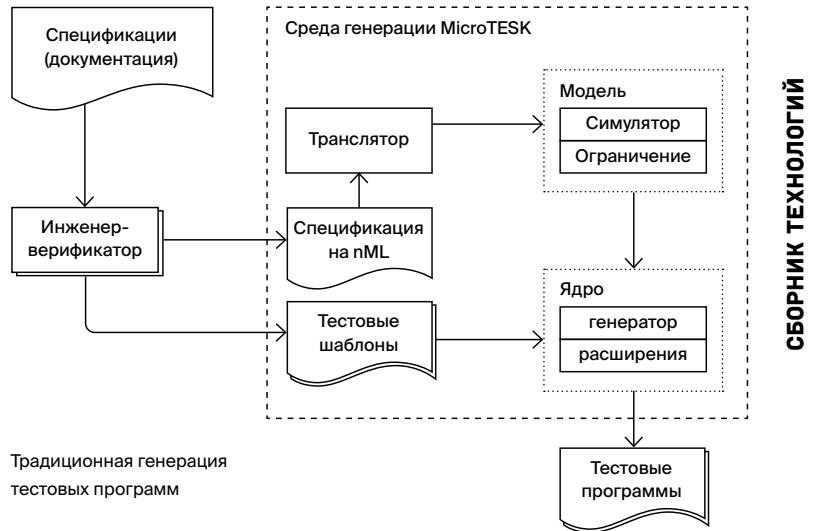
СИСТЕМНЫЕ ТРЕБОВАНИЯ

Java 11, ОС Windows или ОС на базе ядра GNU/Linux.

ОПЫТ ВНЕДРЕНИЯ

MicroTESK разрабатывается с 2007 года. Использовался в российских и международных проектах по разработке современных промышленных микропроцессоров и виртуальных машин (в частности, в промышленных проектах по верификации микропроцессоров ARMv8, MIPS64, RISC-V и виртуальной машины Ark).

СХЕМА РАБОТЫ



UTOPIA EDA: СИСТЕМА ЛОГИЧЕСКОГО СИНТЕЗА ЦИФРОВЫХ ИНТЕГРАЛЬНЫХ СХЕМ



Utopia EDA — открытая расширяемая платформа логического синтеза и верификации цифровой аппаратуры, разрабатываемая в ИСП РАН с 2021 года. Объединяет основные алгоритмы синтеза схем, их оптимизации (на логическом и технологическом уровнях) и проверки логической эквивалентности. Может использоваться как самостоятельный инструмент, так и в качестве основы для построения промышленных систем автоматизированного проектирования (САПР) интегральных схем.

Utopia EDA — это проект с открытым исходным кодом (<https://gitlab.ispras.ru/mvg/utopia-eda>).

ОСОБЕННОСТИ И ПРЕИМУЩЕСТВА

- Поддержка языков описания аппаратуры Verilog и SystemVerilog. Средства синтаксического анализа HDL-описаний базируются на открытых инструментах Yosys и slang.
- Возможность работы с Liberty-спецификациями технологических библиотек. Адаптируемость синтезатора под технологические процессы отечественных и зарубежных фабрик.
- Технологически независимая оптимизация схем по количеству вентиля и/или глубине. Поддержка широкого спектра оптимизирующих преобразований, в том числе rewrite, refactor, resubstitute и balance.
- Технологическое отображение схем с оптимизацией по площади и/или задержке. Возможность задания проектных ограничений и их учета в процессе оптимизации характеристик СБИС.
- Наличие средств проверки логической эквивалентности схем. Контроль корректности процедур синтеза и оптимизации на разных этапах проекта.

ДЛЯ КОГО ПРЕДНАЗНАЧЕНА UTOPIA EDA?

- Разработчики САПР цифровых СБИС (основа для создания инструментов логического синтеза и доверенных маршрутов проектирования).
- Технические университеты (платформа для образовательных курсов по САПР).

ОПЫТ ВНЕДРЕНИЯ

- Проекты по разработке отечественных САПР цифровых СБИС (в том числе проект «Интеллект» Фонда перспективных исследований).
- Учебный курс по проектированию цифровой аппаратуры (ВШЭ МИЭМ).

СИСТЕМНЫЕ ТРЕБОВАНИЯ

Операционная система Linux (Astra Linux, Ubuntu);
не менее 32 Гб оперативной памяти и 100 Гб дискового пространства.

BUILDGRAPHY:

ИНСТРУМЕНТ

ИДЕНТИФИКАЦИИ

РЕКВИЗИТОВ СБОРКИ



Buildography — инструмент для идентификации реквизитов сборки ПО: файлов программ на входных языках, зависимостей (системных библиотек, заголовочных файлов и т.п.), трансляторов и их конфигурационных файлов.

ОСОБЕННОСТИ И ПРЕИМУЩЕСТВА

Buildography — прозрачный и легковесный трассировщик Linux-процессов, ориентированный на сбор информации о выполнении сборки программы для последующего аудита.

Buildography — это:

- Получение структурированной информации о выполнившейся сборке программы в формате JSON.
- Инструменты для анализа полученной информации. Пользователи могут создавать любые анализаторы, опираясь на стабильный формат выходного файла (часть API инструмента). В поставку уже входят инструменты для:
 - установления происхождения результирующих файлов;
 - обнаружения бинарных файлов, не созданных, но использованных в ходе сборки;
 - обнаружения файлов с исходным кодом, использованных в ходе сборки и расположенных вне заданных каталогов;
 - классификации файлов на основе пользовательских правил.
- Независимость от используемых трансляторов или систем сборки.
- Идентификация файлов по хэш-сумме содержимого, вычисленной по ГОСТ Р 34.11-2012.
- Низкие накладные расходы за счёт асинхронного вычисления хэш-сумм в отдельных потоках выполнения, а также применения технологии Seccomp-BPF ядра Linux для фильтрации перехватываемых системных вызовов на стороне ядра.

Buildography отслеживает системные вызовы дочернего дерева процессов с помощью системного вызова ptrace и собирает следующую информацию:

- Аргументы командной строки и рабочие каталоги порождаемых процессов.
- Данные, идентифицирующие вызываемые программы: пути к исполняемым файлам и хэш-суммы их содержимого.
- Данные о файлах, которые открывались в процессе сборки.

**ДЛЯ КОГО
ПРЕДНАЗНАЧЕН
BUILDGRAPHY?**

- Разработчики и вендоры, собирающие ПО из исходных кодов.
- Специалисты по автоматизации процесса разработки безопасного ПО (DevSecOps-инженеры).
- Аудиторы процессов разработки безопасного ПО и компании, желающие пройти сертификацию.

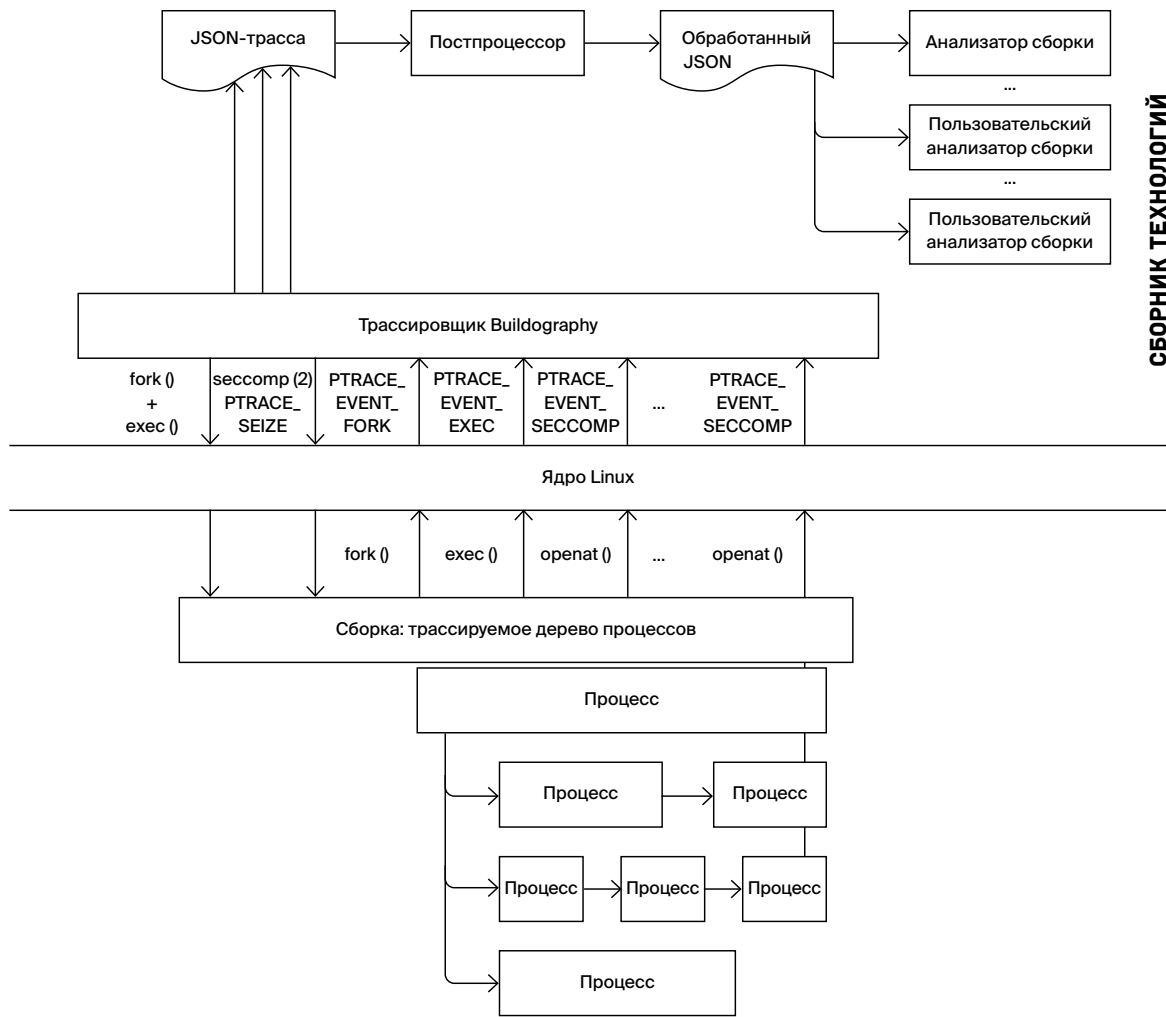
**ОПЫТ
ВНЕДРЕНИЯ**

Buildography используют в компаниях, выстроивших процессы РБПО согласно ГОСТ Р 56939-2024. В частности, применение Buildography позволило сертифицировать внедренные процессы РБПО на соответствие данному ГОСТ.

**СИСТЕМНЫЕ
ТРЕБОВАНИЯ**

- ОС: ядро Linux версии не ниже 4.8.
- Процессорные архитектуры: Intel x86_64, ARM64.

**СХЕМА
РАБОТЫ**



БЕЗОПАСНЫЙ КОМПИЛЯТОР



Безопасный компилятор предотвращает появление уязвимостей в программе при выполнении агрессивных оптимизаций кода (например, в результате использования конструкций, проявляющих неопределённое поведение). Минимально ограничивает выполняемые оптимизации, что позволяет избежать значительного падения производительности по сравнению с полным отключением оптимизаций.

ОСОБЕННОСТИ И ПРЕИМУЩЕСТВА

Разработаны два варианта безопасного компилятора, которые могут быть использованы в качестве замены открытых промышленных компиляторов GCC и Clang (LLVM):

- SAFEC (на основе GCC);
- Safelang (на основе Clang).

Оба компилятора выполняют требования к функциям безопасности из ГОСТ Р 71206-2024 «Защита информации. Разработка безопасного программного обеспечения. Безопасный компилятор языков C/C++. Общие требования».

SAFEC и Safelang — это:

- Доработанные оптимизации компилятора для консервативной обработки конструкций с неопределённым поведением и безопасного доопределения семантики программы.
- Принудительная инициализация неинициализированных автоматических переменных.
- Выдача предупреждений компиляции при обнаружении конструкций с неопределённым поведением.
- Добавление динамических проверок для отдельных классов конструкций в целях исключения появления неопределённого поведения по время работы программы.
- Диверсификация генерируемого кода во время выполнения программы.
- Отсутствие необходимости модифицировать исходный код и файлы системы сборки, что позволяет максимально упростить пользование компилятором.
- Распределение функций безопасности по трём классам, определяющим компромисс между безопасностью генерируемого кода и его производительностью. Самый низкий класс — III, самый высокий — I.

SAFEC и Safelang осуществляют следующие действия:

Согласно III классу:

- Предотвращение возникновения целочисленного переполнения, доступа к объектам через указатель несовместимого типа, разыменования нулевого указателя, замены функций ввода/вывода и работы с памятью стандартной библиотеки на эквивалентные машинные инструкции. Предотвращение перезаписи значений переменных автоматического класса памяти в результате вызова функций семейства `longjmp` (Safelang).
- Обнаружение деления на ноль, некорректности битовых сдвигов, выхода за границы кадра стека, операций загрузки и/или записи в массив за пределами выделенной для него памяти. Обнаружение переменных автоматического класса памяти, которые могут храниться на машинном регистре при вызове функций семейства `longjmp` (SAFEC).

Согласно II классу:

- Анализ аргументов битовых сдвигов; избыточности операций работы с памятью; выравнивания данных при работе с векторными инструкциями; адресной арифметики при оптимизациях, связанных с изменением порядка операций обращения к памяти.
- Инициализация не инициализированных явно переменных автоматического класса памяти нулевыми значениями.
- Остановка процесса трансляции при выдаче определённых предупреждений.

Согласно I классу:

- Диверсификация машинного кода — уникальное распределение кода функций в памяти в ходе динамической компоновки программы или при выполнении статической компиляции. Инструмент диверсификации раньше был частью системы ИСП Обфускатор, а теперь интегрирован в безопасный компилятор.
 - Добавление в программу машинного кода, вызывающего её аварийный останов при обнаружении ситуаций с неопределённым поведением во время выполнения программы:
- 1 Операции с целыми или вещественными типами:
 - загрузка небулевого значения в переменную булевого типа;
 - преобразование значений вещественной переменной, приводящее к целочисленному или вещественному переполнению;
 - операция сдвига, в которой величина сдвига отрицательна либо не меньше ширины типа сдвигаемого значения;
 - операция со знаковыми целыми переменными, результат которой не может быть представлен в нужном типе;
 - целочисленное деление или взятие остатка, в котором значение делителя равно нулю.

- 2 Операции с указателями и массивами:
 - загрузка или запись по некорректно выравненному или нулевому указателю;
 - загрузка или запись в массив по адресу, находящемуся за пределами выделенной для него памяти;
 - передача нулевого указателя в качестве параметра функции, помеченного атрибутом `nonnull`;
 - выполнение операции адресной арифметики, приводящей к целочисленному переполнению;
 - возврат нулевого значения из функции, объявление которой содержит атрибут `returns_nonnull`;
 - выделение в автоматической памяти массива переменной длины с некорректным размером.
- 3 Операции с функциями:
 - вызов по указателю функции, тип которой не соответствует объявленному типу указателя;
 - выход из функции, имеющей возвращаемое значение, без выполнения операции возврата значения;
 - вызов встроенной функции компилятора с недопустимыми значениями аргументов;
 - выполнение точки в программе, отмеченной как недостижимая.

ИНСТРУМЕНТ ДИВЕРСИФИКАЦИИ:

Диверсификация — это защита от массовой эксплуатации уязвимостей, возникающих в результате ошибок или закладок. Если злоумышленник смог атаковать одно из устройств с одинаковым ПО, остальные останутся под защитой благодаря внесённым в код изменениям.

- Позволяет настраивать баланс между степенью запутывания и уровнем производительности (если также требуется защита от обратного анализа). Минимальное замедление работы — в 1,2 раза, максимальное — в 8 раз.
- Применяет оригинальный метод обеспечения целостности потока управления (CFI), который успешно противодействует большинству атак с повторным использованием кода (ROP, JOP, ret-to-plt и др.). Среднее замедление диверсификации из компилятора SAFEC на наборе тестов SPEC CPU2006 составляет около 2%, что заметно ниже, чем у традиционных методов.
- Обеспечивает бесконфликтное совмещение с другими средствами защиты ПО (в том числе с системным механизмом ASLR).
- Реализует два метода — динамическую и статическую диверсификацию.
 - Динамическая диверсификация кода гарантирует один и тот же код на всех устройствах (например, в случае обязательной сертификации) и позволяет перемещать до 98% кода с небольшим увеличением его объёма и ухудшением производительности примерно на 1,5%. Ее преимущества по сравнению с аналогами:
 - перемешивание до функции (в отличие от технологий ASLR и Pagerando, которые перемещают только крупные блоки кода);
 - перемешивание функций во всей системе, кроме ядра, а также отсутствие конфликта с антивирусами (преимущества перед аналогичной технологией Selfrando, разработанной для Tor Browser).

- Статическая диверсификация кода по заданному ключу генерирует при компиляции уникальный исполняемый файл. Ее преимущества:
 - не увеличивается объём бинарного кода (в частности, важно для интернета вещей);
 - ухудшение производительности практически нулевое;
 - благодаря работе внутри компилятора, а не постфактум в компоновщике, можно применять расширенный набор диверсифицирующих преобразований и более гибко его настраивать.

**ДЛЯ КОГО
ПРЕДНАЗНАЧЕНЫ
SAFEC И SAFELANG?**

- Разработчики ОС.
- Компании, разрабатывающие ПО с высокой степенью надёжности и безопасности.

ОПЫТ ВНЕДРЕНИЯ

Безопасный компилятор поставляется в ряд российских компаний и организаций. Инструмент диверсификации как отдельный компонент на базе компилятора GCC внедрен в ОС «Циркон», которую используют МИД и Пограничная служба ФСБ России.

**ПОДДЕРЖИВАЕМЫЕ
ПЛАТФОРМЫ
И АРХИТЕКТУРЫ**

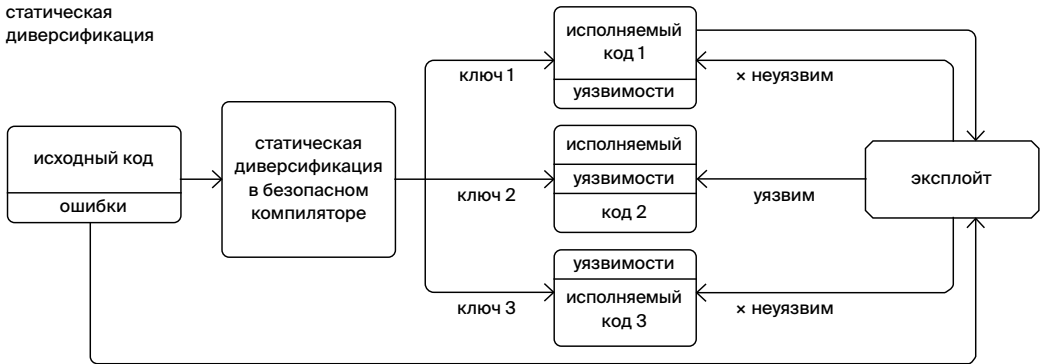
- Целевые ОС: семейство Linux, для SAFEC также Windows (MinGW).
- Целевые процессорные архитектуры: x86 (32/64), armv7, arm64, RISC-V 64.

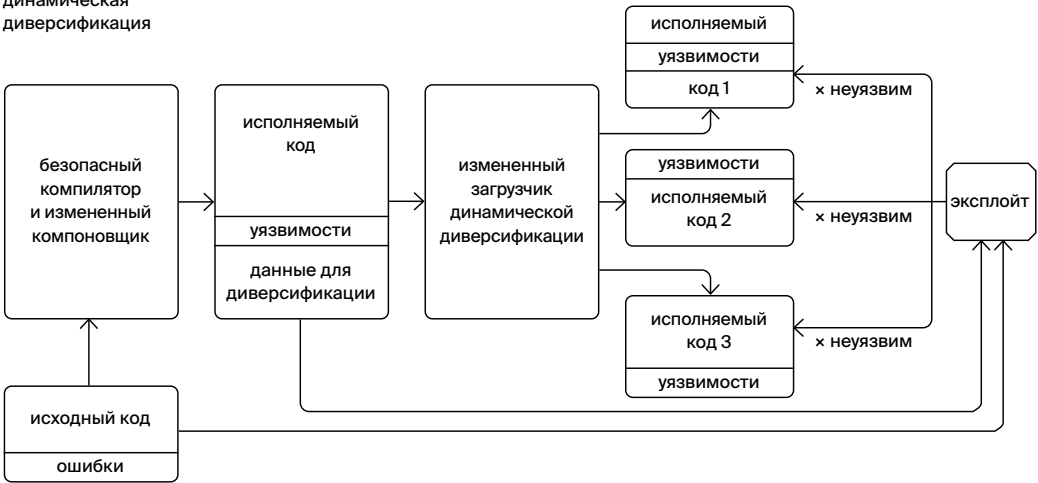
СХЕМА РАБОТЫ

обычная сборка



статическая диверсификация





SVACE: СТАТИЧЕСКИЙ АНАЛИЗАТОР ИСХОДНОГО КОДА



Svace — необходимый инструмент жизненного цикла разработки безопасного ПО, основной статический анализатор компании Samsung. Обнаруживает более 70 классов критических ошибок в исходном коде. Поддерживает языки C/C++, C#, Java, Kotlin, Go, Python, Scala, Visual Basic.NET; в легковесном анализе поддерживает языки JavaScript и Lua. Включён в Единый реестр российского ПО (№4047). Поставляется с web-интерфейсом просмотра предупреждений Svacer (Svace History Server).

ОСОБЕННОСТИ И ПРЕИМУЩЕСТВА

Svace — постоянно развивающийся инновационный продукт, основанный на многолетних исследованиях. Объединяет ключевые качества иностранных аналогов (Synopsis Coverity Static Analysis, Perforce Klocwork Static Code Analysis, Fortify Static Code Analyzer) с уникальным использованием открытых промышленных компиляторов в целях максимальной поддержки новых стандартов языков программирования.

Svace — это:

- Высокое качество анализа:
 - точное представление исходного кода (благодаря интеграции с любой системой сборки);
 - символьное выполнение: полное покрытие всех путей с учетом связей между функциями для поиска сложных ошибок;
 - учёт контекстов вызовов при межпроцедурном анализе, анализ потока данных, анализ чувствительных данных, анализ статистики вызовов;
 - высокий процент истинных срабатываний (60-90%).
- Масштабируемость и высокая скорость:
 - параллельный анализ с использованием всех доступных процессорных ядер;
 - возможность анализировать системы из десятков миллионов строк кода (анализ мобильной ОС Tizen 7 из 57 миллионов строк занимает 7-8 часов основным движком Svace и 9-10 часов всеми движками);
 - поддержка не только полного, но и инкрементального анализа системы (подразумевает быструю повторную проверку недавно изменённого кода), а также поддержка анализа с кэшированием промежуточных результатов (позволяет не повторять анализ не изменившихся частей программы);

- поддержка удаленного анализа, при котором на единый сервер можно отправлять запросы на анализ от разных клиентов. Поддерживаются клиенты и агенты анализа различных версий, а также сбор метрик о ходе анализа в формате Prometheus.
- Автоматическая оценка истинности предупреждений анализатора на основе машинного обучения по структуре исходного кода и данным предыдущей разметки (для языков C, C++, C# и Java).
- Гибкая кастомизация анализа:
 - конфигурация существующих детекторов, а также написание индивидуальных, доступных только данному заказчику;
 - пользовательская настройка истоков и стоков чувствительных данных для точного поиска особо опасных ошибок, важных для заказчика;
 - программный интерфейс для разработки пользовательских детекторов-плагинов.
- Ускоренная адаптация к работе с новым окружением (добавление новых компиляторов в течение 1-2 недель, в сложных случаях — до 2 месяцев).
- Полная совместимость с ГОСТ Р 71207-2024 «Статический анализ программного обеспечения. Общие требования», а также с нормативными документами и требованиями регуляторов (ФСТЭК России).
- Возможность использования для реализации обеспечительных мер ГОСТ Р 56939-2016/2024, а также процедур последних редакций «Методики выявления уязвимостей и недеklarированных возможностей в программном обеспечении» ФСТЭК России (при необходимости сертификации ПО для использования в России).

Swacer — комплексный пользовательский интерфейс просмотра предупреждений, сервер хранения и управления результатами анализа. Поддерживает многопользовательский режим и различные фильтры данных. Swacer — это:

- Разметка и отчёты:
 - широкие возможности сравнения и разметки результатов, навигация по коду и трассе предупреждения, расширенные пользовательские фильтры и управление ими через API;
 - выгрузка отчётов в формате PDF, CSV, JSON;
 - аннотация результатов работы пользовательскими атрибутами и файлами;
 - поддержка разметки различных версий одного проекта;
 - поддержка разметки предупреждений с помощью ИИ (планируется возможность подключать пользовательские ИИ-модели);
 - интеллектуальный перенос разметки между проектами, версиями и ветками проекта, в том числе на основе пользовательских шаблонов переноса;
 - возможность разметки результатов в исходном коде в виде специальных комментариев (режим редактирования), ведение истории работы с комментариями;
 - гибкий пользовательский интерфейс с поддержкой вкладок.

- Совместная работа и управление:
 - богатая ролевая модель, позволяющая гибко настраивать права пользователей и организаций по работе с данными;
 - информационные панели (dashboards) со статистикой по проектам, разметке и активности пользователей;
 - группы проектов и групповые операции с проектами, пользователями, разметкой и др.;
 - поддержка LDAP для аутентификации пользователей;
 - уведомление пользователей о событиях по почте и Telegram;
 - поддержка Web Hooks;
 - доступ ко всем данным через API;
 - поддержка персональных токенов доступа;
 - настройка правил автоматической очистки устаревших данных;
 - импорт и экспорт собранных данных: разметки, исходного кода, комментариев, детекторов (в том числе пользовательских).
- Полнотекстовый поиск по всем предупреждениям, детекторам, комментариям и снимкам (включая пользовательские атрибуты) с поддержкой фильтрации результатов по проектам, веткам и снимкам.
- Веб-среда разработки (IDE) на основе Eclipse/Theia для упрощения работы с кодом.
- Интеграция в CI/CD:
 - предоставление интерфейса командной строки для интеграции в типовые CI/CD-процессы;
 - Поддержка работы в контейнерах.
- Поддержка открытого формата SARIF: позволяет импортировать результаты работы других анализаторов, а также экспортировать результаты вместе с разметкой, комментариями, исходным кодом с учетом таксономии ошибок по классам CWE.

ДЛЯ КОГО ПРЕДНАЗНАЧЕН SVACE?

- Компании, нацеленные на разработку ПО с высокой степенью надёжности и безопасности.
- Компании, которые нуждаются в сертификации разрабатываемого ПО.
- Испытательные лаборатории и органы по сертификации.

ОПЫТ ВНЕДРЕНИЯ

Svace — основной анализатор Samsung с 2015 года. Применяется для проверки собственного ПО компании на базе ОС Android и исходного кода ОС Tizen, которая используется в смартфонах, информационно-развлекательных системах и бытовой технике Samsung. С 2017 года Svace проверяет все изменения, присланные для рецензирования и включения в ОС Tizen. С 2020 года Svace применяется также в компании Huawei.

В России Svace используется более чем в 200 компаниях и лабораториях, в том числе в ОАО «РусБИТех», АО «Лаборатория Касперского», Postgres Professional, ООО «Код Безопасности», МВП «СВЕМЕЛ» и др.

ПОДДЕРЖИВАЕМЫЕ ТИПЫ ОШИБОК

Анализатор Svace находит более 1000 типов ошибок, в том числе более 70 классов критических ошибок (переполнение буфера, работа с некорректными указателями и неинициализированными переменными, использование чувствительных данных, деление на ноль и другие) и множество недостатков кодирования и стилистических недочетов. Полный список ошибок и остальную документацию можно найти на странице <https://svace.pages.ispras.ru/svacewebsite/docs/latest/user-guide.html>.

ПОДДЕРЖИВАЕМЫЕ ПЛАТФОРМЫ И АРХИТЕКТУРЫ

- Платформы, на которых работает анализатор Svace: Linux/x64 (версия ядра 3.10+, версия glibc 2.17+), Linux/ARM 64 (Ubuntu 18.04), Windows (начиная с Windows 7 SP 1 с обновлением KB2533623) и WSL (версий 1 и 2); macOS/x64 (версия 10.10+, языки C# и Visual Basic .NET не поддерживаются); архитектура x86 (только перехват сборки).
- Архитектуры, для которых анализируется исходный код: для C/C++ — Intel x86/x86-64, ARM/ARM64, MIPS/MIPS64, Power PC/Power PC 64, RISC-V 32/64, SPARC/SPARC64, Hexagon (генерация кода через Clang); Эльбрус, AEON, TriCore, HIDS, OpenRISC (генерация кода через одну из предыдущих архитектур); для Go — Intel x86-64 на ОС Linux и Windows; для C#, Java, Kotlin, Scala, Visual Basic. NET — платформы, на которых работает анализатор.
- Платформы и архитектуры, на которых работает Svacer: архитектура x86-64; ОС Linux (версия ядра 3.10+, версия glibc 2.17+), ОС Windows (начиная с Windows 10) и WSL (версий 1 и 2); macOS на x86-64 (начиная с версии 10.12 Sierra).

ПОДДЕРЖИВАЕМЫЕ ЯЗЫКИ И КОМПИЛЯТОРЫ

Для C/C++ (версий до C++20): GCC (GNU Compiler Collection), Clang (LLVM compiler), Microsoft Visual C++ Compiler, RealView/ARM Compilation Tools (ARMCC), Intel C++ Compiler, Elbrus C/C++ Compiler, Wind River Diab Compiler, Keil CA51 Compiler Kit, NEC/Renesas CA850, CC78K0(R) C Compilers, C/C++ Compiler for the Renesas M16C Series and R8C Family, Panasonic MN10300 Series C Compiler, C compiler for Toshiba TLCS-870 and T900 Family, Samsung CalmSHINE16 Compilation Tools, Texas Instruments TMS320C6* Optimizing Compiler, Digital Mars C and C++ Compiler, Green Hills compiler for ARM, TASKING C compiler for TriCore, CEVA Toolbox for CEVA DSP cores, IAR C/C++ Compiler for ARM / Renesas RL78 MCU, CodeWarrior Development Studio for StarCore DSPs, Open Watcom C/C++ compiler, Freescale CodeWarrior, Cadence Tensilica Xtensa C/C++ Compiler.

Для C# (версий до C# 13): Roslyn, Mono.

Для Java (версий до Java 21): OpenJDK Javac Compiler, Eclipse Java compiler.

Для Kotlin: Kotlin 2.0.

Для Go: Go 1.25.

Для Python: Python 3.12.

Для JavaScript: JavaScript ES 6.

Для Lua: Lua 5.4.

СХЕМА РАБОТЫ

1. Сборка

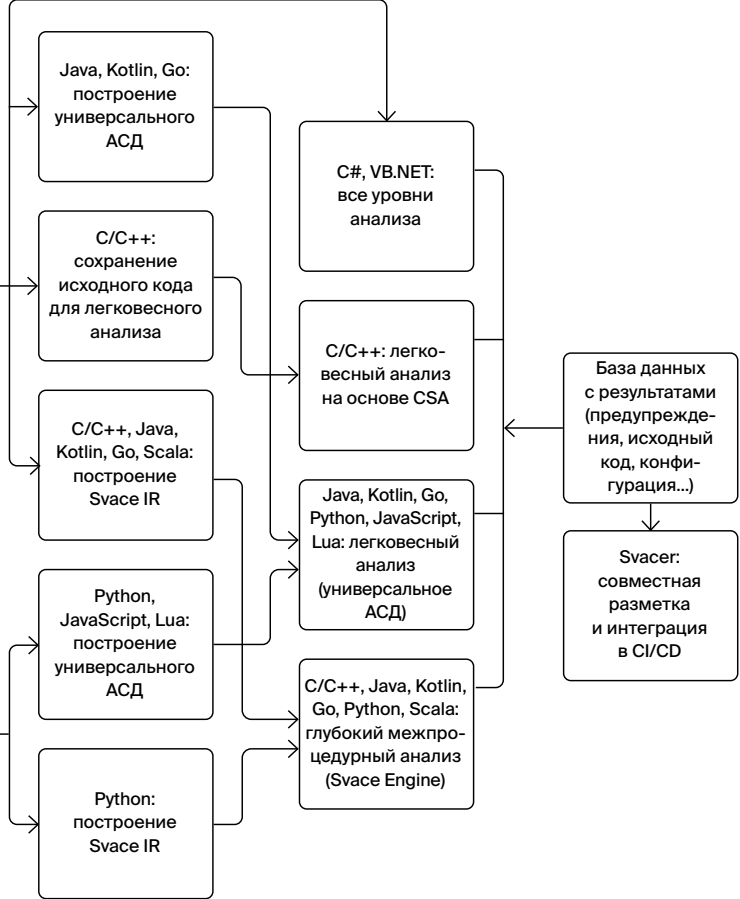
перехват запусков компиляторов / компоновщиков в ходе мониторинга сборки программы

Контролируемая сборка

Сканирование исходного кода

сканирование папок с исходным кодом программ на интерпретируемых языках

2. Анализ



создание внутренних представлений для легковесного анализа (универсальный АСД) и глубокого анализа (Svace IR)

- легковесный анализ синтаксических деревьев программы;
- межпроцедурный анализ (контекстно-чувствительный и чувствительный к путям на основе символического выполнения);
- анализ помеченных данных (пользователь может задать источники и приёмники помеченных данных, в том числе помеченные аргументы функций и поля структур).

- подсветка синтаксиса и навигация по коду;
- просмотр предупреждений (с разметкой на истинные и ложные);
- сравнение результатов анализа и сокрытие ложных предупреждений, найденных на предыдущих запусках;
- групповые операции работы с проектами, пользователями, разметкой;
- доступ ко всем данным через API;
- импорт и экспорт собранных данных.

КЛОС: КОНФИГУРИРУЕМАЯ ЛИНЕЙКА ОПЕРАЦИОННЫХ СИСТЕМ



Семейство операционных систем КЛОС (Конфигурируемая Линейка Операционных Систем) – технология создания микроядерных операционных систем с повышенными требованиями к безопасности и защищённости. На основе КЛОС созданы программные платформы для большинства современных архитектур AArch64, ARM, PowerPC, MIPS, RISC-V и x86, включая операционные системы с жёстким реальным временем для бортовой аппаратуры, реализующие стандарт ARINC 653.

ОСОБЕННОСТИ И ПРЕИМУЩЕСТВА

КЛОС предоставляет гарантии по пространственной и временной изоляции между приложениями, а также стандартизованный механизм обработки отказов, который обеспечивает устойчивую работу приложений даже при отказе или нештатном функционировании других приложений. Данные гарантии подкреплены реализацией требований стандарта ARINC 653 в полном объёме.

Дополнительные возможности изоляции обеспечиваются за счёт принципа микроядерности, положенного в основу КЛОС. Подсистемы сопряжения с аппаратурой, в том числе eMMC, Ethernet, i2c, ONFI NAND, Parallel и SPI NOR, PCI, RTC, SATA, SpaceWire, SPI, VirtIO, ГОСТ Р 52070-2003 (МКИО), UART, SPI NOR могут быть изолированы в отдельных адресных пространствах с пониженными привилегиями, дополнительно повышая защищённость системы от внешних и внутренних угроз.

Накладные расходы со стороны ОС минимизированы за счёт статического конфигурирования памяти и непериодических таймеров с квантованием. Реализована поддержка симметричной (SMP) и асимметричной (AMP) многоядерности для оптимизации производительности и минимизации влияния параллельного кода.

В качестве программного интерфейса предоставляется реализация стандартов ARINC 653 P1 и P2, ISO/IEC 8652 (Ada), 9899 (C), 10514 (Modula 2) и 14882 (C++), GlobalPlatform TEE и других государственных отраслевых стандартов. В комплекте с КЛОС предоставляется

расширенный набор инструментов разработки (РБПО), включающий в себя средства компиляции, отладки, эмуляции аппаратуры, статического и динамического анализа, тестирования, профилирования и сбора покрытия по коду (функции, операторы, ветви, MC/DC).

СИСТЕМНЫЕ ТРЕБОВАНИЯ

GNU/Linux дистрибутив на архитектуре x86_64 (например, Ubuntu 24.04), а также Apple macOS 12 или новее в качестве инструментальной машины.

Целевой вычислитель с ОЗУ не менее 2 МБ на архитектурах:

- AArch64 (Cortex-A53, Cortex-A55);
- ARM (Cortex-A7, Cortex-A9, Cortex-M4), в частности, процессоры i.MX6 или STM32F4;
- PowerPC (e500mc, e500v2, 476FP), в частности, процессоры p1010 или p3041;
- MIPS (MIPS Release 1, MIPS Release 2 / MIPS32, КОМДИВ), в частности, процессоры 1892BM15АФ и K5500BK018;
- RISC-V (RV32 IMA);
- x86 (Intel Prescott и новее).

При необходимости окружение адаптируется к оборудованию заказчика.

ОПЫТ ВНЕДРЕНИЯ

Семейство операционных систем КЛОС (Конфигурируемая Линейка Операционных Систем) является результатом многолетних исследований и разработок коллектива ИСП РАН, которые были начаты академиком В. П. Иванниковым в 70-е годы XX века. Первые статьи по КЛОС были опубликованы в 1977 году, в 1979 В. П. Иванников защитил докторскую диссертацию на основе опыта разработки ОС для ЭВМ АС-6, внедренной в нескольких центрах управления полетами космических аппаратов. В диссертации были изложены принципы построения кластерной операционной системы, что в современной терминологии можно назвать микроядерными ОС. Развитием КЛОС явилась кластерная операционная система для ЭВМ «Электроника ССБИС».

За последние десятилетия ИСП РАН на основе имеющего задела успешно разработал несколько представителей семейства КЛОС, в том числе для нужд аэрокосмической отрасли. Так создаваемая совместно с ГосНИИАС ОСПВ JetOS разрабатывается в соответствии с требованиями отраслевого стандарта КТ-178С (DO-178С) и проходит сертификацию в составе авионики Суперджет Нью (SJ-100) и MC-21.

TESTOS: ОКРУЖЕНИЕ ДЛЯ ТЕСТИРОВАНИЯ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ



TestOS — окружение для модульного тестирования программного обеспечения на целевой аппаратуре, построенное на основе КЛОС. Позволяет проводить отработку программного обеспечения для ответственного применения в целях выполнения сертификационных и иных мероприятий на архитектурах AArch64, ARM, PowerPC, MIPS, RISC-V и x86.

ОСОБЕННОСТИ И ПРЕИМУЩЕСТВА

TestOS позволяет заменить такие средства верификации критических систем, как LDRA, являясь более гибким средством с активной поддержкой отечественных изделий.

С помощью TestOS обеспечивается выполнение тестов на целевой аппаратуре и производится генерация отчётов с трассой по каждому тесту, с информацией по составу и статусу прохождения тестового плана и с покрытием кода тестируемой системы как для одного теста, так и для всего тестового плана. Для разработки модульных тестов для функций на языке C (поддерживается C18 с GNU-расширениями GCC и Clang) предоставляется среда генерации заглушек и обёрток с удобным механизмом написания тестовых сценариев. Построение отчётов осуществляется в формате HTML и TXT. Доступна отладка кода на целевом вычислителе как с использованием, так и без использования JTAG.

С использованием плагинов поддерживаются:

- сбор покрытия функций, операторов и ветвей с помощью GCOV и LLVM Coverage;
- сбор покрытия по MC/DC с помощью GCOV и LLVM Coverage;
- сбор покрытия по MC/DC с помощью COVERest (P-330 по уровню TQL-5);
- проведение статического анализа с помощью статических анализаторов:
 - Clang Tidy;
 - Clang Static Analyzer;
 - Svace.

- динамическое инструментирование кода с помощью инструментария LLVM:
 - AddressSanitizer (выявление ошибок работы с памятью);
 - MemorySanitizer и детерминированная инициализация переменных на стеке (выявление ошибок доступа к неинициализированной памяти);
 - UndefinedBehaviorSanitizer (выявление ошибок арифметики, операций с плавающей точкой и иных проблем, вызванных неопределённым поведением).

СИСТЕМНЫЕ ТРЕБОВАНИЯ

GNU/Linux дистрибутив на архитектуре x86_64 (например, Ubuntu 24.04), а также Apple macOS 12 или новее в качестве инструментальной машины.

Целевой вычислитель с ОЗУ не менее 2 МБ на архитектурах:

- AArch64 (Cortex-A53, Cortex-A55);
- ARM (Cortex-A7, Cortex-A9, Cortex-M4), в частности, процессоры i.MX6 или STM32F4;
- PowerPC (e500mc, e500v2, 476FP), в частности, процессоры p1010 или p3041;
- MIPS (MIPS Release 1, MIPS Release 2 / MIPS32, КОМДИВ), в частности, процессоры 1892BM15АФ и K5500BK018;
- RISC-V (RV32 IMA);
- x86 (Intel Prescott и новее).

При необходимости окружение адаптируется к оборудованию заказчика.

ОПЫТ ВНЕДРЕНИЯ

TestOS разрабатывается с 2019 года. Успешно применяется для модульного тестирования программного обеспечения для аэрокосмической отрасли.

ANIS: ПОДДЕРЖКА ПРОЦЕССОВ ВЕРИФИКАЦИИ СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ НА ОСНОВЕ ФОРМАЛЬНЫХ МОДЕЛЕЙ УПРАВЛЕНИЯ ДОСТУПОМ



ANIS — технология для поддержания процесса динамической верификации средств защиты информации с использованием формальной модели управления доступом. Технология разрабатывается в соответствии с ГОСТ Р 59453.4-2025, «Защита информации. Формальная модель управления доступом, Часть 4. Рекомендации по верификации средства защиты информации, реализующего политики управления доступом, на основе формализованных описаний модели управления доступом» и позволяет выполнять заложенные в документе задачи.

ОСОБЕННОСТИ И ПРЕИМУЩЕСТВА

Не имеющая на данный момент аналогов технология, обеспечивающая поддержку мероприятий по динамической верификации программных систем с использованием формальных моделей, требуемых стандартом ГОСТ Р 59453.4-2025. ANIS включает в себя инструменты:

- разработки формальных моделей;
- импорта и экспорта формальных моделей в другие средства разработки;
- трансляции моделей в программный код для тестовых оракулов;
- интеграции процесса мониторинга целевой системы;
- адаптации собранных трасс исполнения к формату формальной модели;
- анализа собранных трасс исполнения;

- разработки тестов;
- запуска и отладки тестов;
- анализа покрытия по формальной модели;
- генерации отчетов.

Технология в будущем может быть расширена за счет инструментов:

- проверки формальных моделей;
- запуска онлайн-мониторинга целевой системы;
- интеграции нескольких формальных моделей разного уровня абстракции.

При разработке технологии ставилась задача упрощения обучения специалистов элементам формальных методов разработки и верификации программ. В связи с чем, помимо формального языка спецификаций Event-B, технология поддерживает и язык Python, что существенно упрощает ее внедрение в компаниях-разработчиках ПО.

ДЛЯ КОГО ПРЕДНАЗНАЧЕН ANIS

Для компаний, разрабатывающих средства защиты информации и их сотрудников:

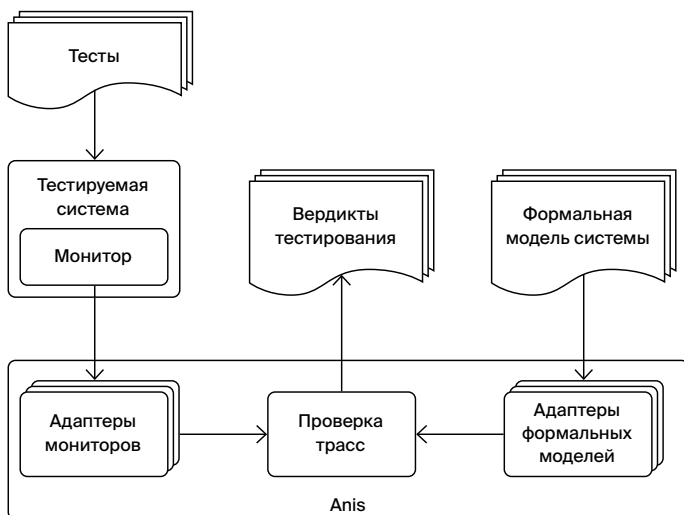
- разработчиков формальных моделей;
- разработчиков тестов;
- инженеров, готовящих систему для сертификации.

ОПЫТ ВНЕДРЕНИЯ

Технология разрабатывалась с учетом формальных моделей управления доступом операционных систем общего назначения, в частности, ОС Linux. Таким образом, была продемонстрирована работоспособность технологии для данного класса моделей. Также данная технология будет применима и для более простых формальных моделей и программных систем.

Разработанные прототипы инструментов используются в компании РусБИТех-Астра для тестирования на основе формальных моделей управления доступом Astra Linux.

СХЕМА РАБОТЫ



БЛЕСНА: ИНСТРУМЕНТ ДИНАМИЧЕСКОГО АНАЛИЗА ПОМЕЧЕННЫХ ДАННЫХ



Блесна — специализированный инструмент, предназначенный для поиска утечек в памяти чувствительных данных, таких как пользовательские пароли и ключи шифрования. Применим для анализа всего программного стека от загрузчика до прикладного ПО. Включён в Единый реестр российского ПО (№13095).

ОСОБЕННОСТИ И ПРЕИМУЩЕСТВА

Блесна проводит точный динамический анализ помеченных данных, проводимый комплексно, для объекта оценки и его программной среды функционирования.

Возможности инструмента опираются на многолетний опыт разработчиков компиляторов и специалистов по информационной безопасности. В отличие от аналогичных научно-исследовательских технологий в области анализа бинарного кода инструмент доработан до промышленного использования.

Блесна — это:

- Автоматизация экспертизы исполняемого кода в части утечек данных с минимальными требованиями к квалификации пользователей.
- Упрощённая подготовка к анализу по типовым сценариям.
- Полносистемный анализ бинарного кода: исследуется весь стек развёрнутого ПО, что позволяет выявлять утечки данных, проходящие через границы виртуальных адресных пространств процессов.
- Глубокий анализ:
 - для анализа достаточно наличия лишь исполняемого бинарного кода и описания сигнатур анализируемых функций;
 - точный анализ потоков данных, учитывающий особенности аппаратуры (конвейер команд, прерывания, трансляция виртуальных адресов, DMA).
- Высокая производительность:
 - параллельный анализ с высокими показателями масштабируемости на многоядерных рабочих станциях;
 - возможность анализа длительных сценариев работы анализируемой системы.

**ДЛЯ КОГО
ПРЕДНАЗНАЧЕНА
БЛЕСНА?**

- Государственные учреждения, в обязанности которых входит экспертиза безопасности программного обеспечения.
- Отечественные компании-разработчики безопасного программного обеспечения.
- Испытательные лаборатории и органы по сертификации.

**УСЛУГИ
С ИСПОЛЬЗОВАНИЕМ
БЛЕСНЫ**

- Исследования программного обеспечения при проведении сертификации на высокие уровни доверия.
- Целевое обучение и повышение квалификации.

**ПОДДЕРЖИВАЕМЫЕ
ПЛАТФОРМЫ
И АРХИТЕКТУРЫ**

- Системные требования инструмента Блесна: ОС Linux x86-64, ОЗУ не менее 16 Гбайт, рекомендуется не менее 2 Тбайт дискового пространства.
- Целевые процессорные архитектуры: x86/x86-64, ARMv7/ARMv8.
- Целевые ОС: семейство Windows, семейство Linux, поддерживается возможность работы с неопознанной ОС и с кодом, работающим вне ОС.

**ОСОБЕННОСТИ
АНАЛИЗА**

- Анализируется целевой сценарий работы программы.
- Программа анализируется совместно со средой функционирования. Для этого подготавливается образ диска QEMU, который содержит анализируемую программу с необходимой ОС и библиотеками.
- Во время выполнения целевого сценария работы программы в эмуляторе QEMU записывается трасса.
- Трасса выполнения содержит последовательность всех машинных команд, выполнившихся на виртуальном процессоре эмулятора QEMU, что позволяет проводить точный анализ.
- Собранная трасса анализируется инструментом Блесна; в ходе анализа происходит выявление утечек помеченных данных.
- Данные помечаются на основе информации о сигнатурах функций, предоставляемой пользователем.
- Для выявленных утечек предъявляется цепочка команд, реализующая утечку с указанием необходимой диагностики: имён функций и модулей, стека вызовов.

ПЛАТФОРМА ДЛЯ АНАЛИЗА ПРОГРАММ НА ОСНОВЕ ЭМУЛЯТОРА QEMU



Платформа ИСП РАН для анализа программ построена на базе открытого эмулятора QEMU, который используется при необходимости кроссплатформенной разработки. Поддерживает механизмы обратной отладки и интроспекции, а также режим полносистемной эмуляции для отладки низкоуровневого ПО.

ОСОБЕННОСТИ И ПРЕИМУЩЕСТВА

QEMU поддерживает более 10 архитектур процессоров (i386 и x86-64, ARM и Thumb, MIPS, PowerPC и др.). Реализует отладку по сетевому протоколу GDB RSP и совместим с IDA Pro, GDB и средами разработки. В режиме полносистемной эмуляции подходит для отладки низкоуровневого ПО, такого как загрузчик и ОС. Исходный код QEMU систематически проверяется двумя статическими анализаторами (Coverity и Svasc), что делает анализ потенциально вредоносного ПО в эмуляторе более безопасным. Эмулятор с поддержкой обратной отладки и интроспекции доступен на GitHub (<https://github.com/ispras/swat>), как и набор инструментов автоматизации (<https://github.com/ispras/qdt>, <https://github.com/ispras/i3s>).

Платформа ИСП РАН на основе QEMU — это:

- Запись и воспроизведение работы виртуальной машины:
 - При каждом воспроизведении виртуальная машина ведёт себя одинаково и точно так же, как при записи. Все воздействия извне зафиксированы и повторяются самим эмулятором. Это упрощает отладку ошибок, связанных с параллельной работой (состояние гонки, взаимные блокировки).
 - На базе воспроизведения реализована GDB-совместимая обратная отладка, которая заключается в откате к предыдущим снимкам состояния виртуальной машины и поиске предпоследнего срабатывания точки останова или предыдущей инструкции.
 - Записывается минимум информации, что позволяет вести длительную запись, необходимую для отладки редко повторяющихся ошибок.
 - Низкое относительное замедление, вносимое записью, позволяет контролировать ПО, взаимодействующее с удалённой неконтролируемой системой в реальном времени.

- Получение высокоуровневой информации о работе гостевой ОС (интроспекция VM) без внесения каких-либо изменений в ядро ОС или установки программ мониторинга:
 - Возможность получить последовательность совершаемых системных вызовов, обращений к именованным функциям в динамических библиотеках, список работающих процессов, список открытых файлов и загруженных в память модулей.
 - Поддержка любого образа виртуальной машины на основе Linux, в том числе — образов встраиваемого ПО различных устройств.
 - Отладка с помощью встроенного в эмулятор сервера WinDbg, что позволяет отображать информацию о гостевом ПО в терминах абстракций ядра Windows. При этом не требуется включение отладочного режима работы гостевой ОС.
- Ускорение разработки расширений для QEMU:
 - Сокращение времени на подготовку средств динамического анализа для образцов кода, требующих специализированной аппаратуры.
 - Автоматизированное добавление процессорных архитектур с использованием генератора декодеров машинных команд и Си-подобного языка описания семантики инструкций.
 - Система автоматического первичного тестирования виртуальной машины. Для работы системы требуются только утилиты GNU Binutils и компилятор языка Си.
 - Автоматизированная разработка моделей устройств.
 - Генерация виртуальной машины (в форме исходного кода модуля QEMU) как из существующих, так и из новых устройств по описанию на языке Python с использованием графического интерфейса пользователя со схематичным изображением системы.
 - API для автоматизации процесса отладки на языке Python по протоколу GDB RSP: отладка гостевого кода, кода эмулятора и обоих одновременно.
- Удобство практического использования:
 - Свободное расширение возможностей QEMU благодаря открытому исходному коду и собственным инструментам ускоренной разработки ИСП РАН.
 - Анализ бинарного кода без внедрения программ в гостевую систему.
 - Модульная структура механизма интроспекции с возможностью расширения за счёт новых плагинов.
 - Удобное API для самостоятельной разработки плагинов интроспекции.
 - Возможность адаптации под конкретные нужды пользователя.
 - Поддержка актуальных версий QEMU с новой периферией и процессорными ядрами.

ДЛЯ КОГО ПРЕДНАЗНАЧЕНА ПЛАТФОРМА НА БАЗЕ QEMU?

- Разработчики загрузчиков, драйверов, ОС и другого системного ПО.
- DevOps-команды (воспроизводимость ошибок, кросс-разработка, масштабирование тестирования в облачной среде).
- Аналитики потенциально вредоносного ПО.
- Специалисты по сертификации ПО.

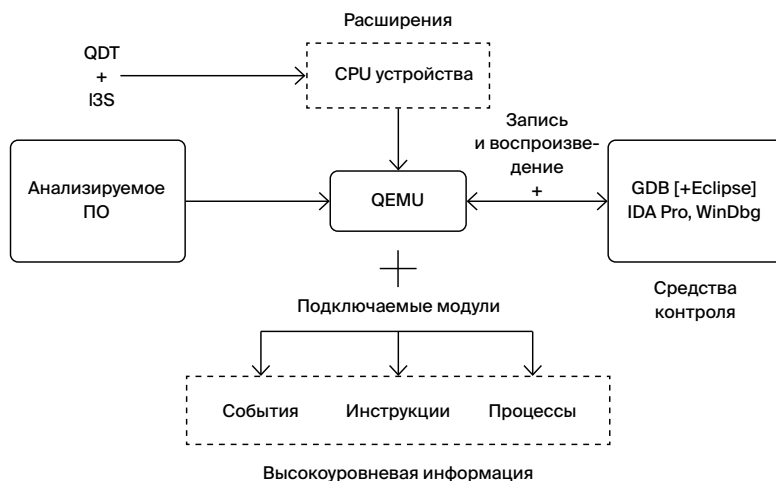
ПОДДЕРЖИВАЕМЫЕ ГОСТЕВЫЕ СРЕДЫ

Эмулируемые платформы: i386, x86-64, ARM, MIPS, PowerPC и другие.
Гостевые системы, поддерживаемые интроспекцией: Windows XP (x86), Windows 10 (x86-64) и Linux 2.x-5.x на платформах x86, x86-64, ARM, AArch64.

ОПЫТ ВНЕДРЕНИЯ

Реализованный механизм воспроизведения принят мировым сообществом разработчиков QEMU и включен в версию 3.1.

СХЕМА РАБОТЫ



ИСП CRUSHER: КОМПЛЕКС ДИНАМИЧЕСКОГО И СТАТИЧЕСКОГО АНАЛИЗА ПРОГРАММ



ИСП Crusher — программный комплекс гибридного анализа, комбинирующий динамический и статический подходы с поддержкой генетического фаззинга и динамического символьного выполнения. ISPCrusher автоматически создает фаззинг-цели и корпус начальных входных данных на основе пользовательских сценариев и тестов, а также внедряет задачи фаззинг-тестирования в уже существующие готовые проекты (GitLab, Jenkins, Jira и т.п.) и тем самым упрощает разработку, помогая выстроить процессы в соответствии с ГОСТ Р 56939-2024 и «Методикой выявления уязвимостей и недекларированных возможностей в программном обеспечении» ФСТЭК России. Включён в Единый реестр российского ПО (№10468).

ОСОБЕННОСТИ И ПРЕИМУЩЕСТВА

ИСП Crusher — первый отечественный продукт в области гибридного анализа ПО, который представляет собой полноценную платформу с автоматическим внедрением в процесс безопасной разработки ПО, выводя участие разработчика в анализе на новый уровень. ISPCrusher обнаруживает дефекты ПО как при наличии, так и при отсутствии исходного кода. Формирует оценку покрытия по строкам исходного кода и по базовым блокам исполняемого кода. Решает те же задачи, что и мировые аналоги (Synopsys Codenomicon, beSTORM, Peach Fuzzer), однако является комплексным решением и более удобен для российских компаний в условиях процесса импортозамещения.

ИСП Crusher — это:

Фаззинг широкого класса ПО:

- пользовательские приложения, ядро и библиотеки;
- ПО встроенных устройств (контроллеры, устройства интернета вещей (IoT)), а также сервисы и СОМ-объекты ОС Windows;
- ОС семейства Linux и Windows;

- приложения на различных языках программирования: C/C++, Java, Python, C#;
- фаззинг-тестирование Enterprise Java-приложений, включая приложения на основе Spring Boot и Spring Framework;
- архитектуры x86/x86_64, ARM, MIPS, RISC-V;
- фаззинг нейронных сетей. Выявляет случаи ошибочных предсказаний нейронных сетей при искажении корректно классифицируемых входных данных, опираясь на анализ карты активации нейронов во время работы нейросетей. Тем самым повышается качество и безопасность ИИ-систем. Функционал позволяет:
 - находить ошибки в работе нейронных сетей для ситуаций, которые изначально не попали в набор данных для обучения;
 - находить возможные закладки и НДВ.
- фаззинг-тестирование через различные источники входных данных: файл, аргументы командной строки, стандартный поток ввода, аргументы переменных окружений, сеть, прямая запись в память;
- возможность проведения анализа серверного и клиентского ПО, работающего по протоколам с состояниями и без состояний;
- фаззинг протоколов с использованием модифицированного клиента: отпадает необходимость написания клиента или его спецификации с нуля для фаззинга сервера (поддерживается и зеркальная схема – с модифицированным сервером);
- широкие возможности для фаззинга ПО встраиваемых устройств с использованием частичной эмуляции и символьного исполнения;
- фаззинг браузеров с гибкой настройкой сценариев через Selenium;
- фаззинг ПО, требующего изоляции, в докер-режиме – каждый экземпляр фаззера работает в отдельном докер-контейнере;
- фаззинг приложений в rootfs в chroot-режиме.

Фаззинг на больших мощностях:

- поддержка многопоточного анализа как на одной машине, так и на распределённых;
- возможность распределения корпуса входных данных между процессами фаззеров для повышения эффективности их работы;
- поддержка дифференциального фаззинга;
- поддержка коллаборативного фаззинга с автоматической балансировкой вычислительных мощностей между различными фаззерами.

Поддержка большого набора типов инструментации:

- статическая (в основном для C/C++): с помощью GCC/LLVM, ISP-Circea;
- статическая инструментация Python-приложений;
- динамическая (в основном для ELF, PE): Qemu (user-mode), TinyInst;
- на основе частичной эмуляции (произвольного кода без необходимости эмуляции периферии устройств с интеграцией динамического символьного выполнения) – Dual-Emu;

- на основе полносистемной эмуляции;
- с использованием Nух-снапшотов и снапшот-API;
- Java-приложений;
- С#-приложений;
- удалённая инструментация (позволяет выполнять фаззинг приложения, работающего на удалённом устройстве).

Автоматизированное управление процессами гибридного анализа с помощью графического интерфейса (MIA):

ИСП-Crusher комбинирует статический и динамический анализ и непрерывно обрабатывает результаты их совместного применения. Пользователь может настраивать все компоненты анализа в графическом интерфейсе или в автоматизированном режиме на основе данных, получаемых в процессе работы. ИСП-Crusher позволяет:

- определять зависимости условных переходов от конкретных значений во входных данных;
- автоматизированно направлять динамический анализ в непокрытые участки программы;
- обнаруживать участки кода, выполнение которых приводит к тому, что анализируемое ПО на одинаковых входных данных выдает разный результат их обработки;
- выполнять девиртуализацию вызовов методов и функций, позволяющую восстанавливать полный граф потока управления (CFG) и использовать эти результаты для уточнения статического анализа;
- отображать найденные предупреждения любых статических анализаторов в формате SARIF (BinSide, Svasc и др.) в графическом интерфейсе с возможностью понимания, какие входные данные от фаззинга проходят через эти дефекты;
- отображать исходный, декомпилированный и ассемблерный код, а также визуализировать граф потока управления (CFG) и отслеживать покрытие;
- отображать информацию об ошибках, выявленных Valgrind;
- отображать семантические ядра в графическом интерфейсе;
- отображать MC-DC покрытие.

Автоматическое внедрение задач фаззинг-тестирования в готовые проекты:

- автоматизированное внедрение фаззинга в процессы CI (GitLab, Jenkins, Jira и т.п.);
- генерация фаззинг-целей и формирование начального корпуса входных данных на основе уже имеющихся пользовательских сценариев и тестов;
- автоматическое обновление фаззинг-целей при любых модификациях в коде.

Возможность интеграции с рядом необходимых инструментов жизненного цикла разработки безопасного ПО, созданных в ИСП РАН:

- Компилятор ISP-Circea
 - автоматически анализирует код программы и аннотирует места переходов между состояниями

- ми, вставляя специальные маркеры, которые при фаззинге направляют Crusher в нужные участки программы, увеличивая покрытие и эффективность;
- инструментирует код, вставляя в места логических выражений MC/DC-датчики, которые во время фаззинга позволяют формировать MC/DC покрытие и отображать его в графическом интерфейсе.
 - автоматизированная подготовка к фаззингу протоколов (ModClient). ISP-Circea позволяет автоматически внедрять мутации переменных состояния в генератор данных (клиент или сервер).
 - Статический анализатор бинарного кода BinSide
 - получение входных данных, на которых проявляются ошибки, размеченных с помощью BinSide в автоматизированном режиме;
 - получение информации о нестабильных участках кода и граничных блоках;
 - Статический анализатор исходного кода Svace
 - отображение трассы последовательности функций, приводящих к аварийному завершению, в Svacer;
 - Инструмент динамического символьного выполнения Sydr
 - получение наборов входных данных для инвертирования условных переходов, обнаруженных во время выполнения программы;
 - Инструмент выявления семантических ядер SemanticExtractor
 - определение семантических ядер (участков кода, реализующих определённую функциональность) в бинарном коде на основе кластеризации функций и генерация описаний функциональности полученных ядер с применением больших языковых моделей;
 - выявление функций-парсеров для определения зависимости условных переходов от конкретных значений во входных данных и направления динамического анализа в непокрытые участки программы.

Интеграция с другими инструментами динамического анализа:

- со сторонними фаззерами: позволяет запускать в рамках одной фаззинг-сессии набор различных фаззеров, между которыми обеспечена синхронизация, что увеличивает эффективность тестирования;
- с инструментами динамического символьного выполнения SymCC и Angr: позволяет получать новые входные данные для увеличения покрытия кода целевого ПО;
- совместная работа с дизассемблером IDA PRO (сохранение покрытия для плагина Lighthouse, которое отображает покрытые базовые блоки в ПО, а также вывод процента покрытых базовых блоков);
- использование фаззера Radamsa для генерации новых данных.

Дополнительный анализ полученных входных данных:

- оценка покрытия по строкам исходного кода и по базовым блокам исполняемого кода;
- предоставление информации об ошибках, включая стек вызовов, состояние системы в момент возникновения ошибки и информацию об утечках памяти;
- оценка критичности найденных аварийных завершений;
- маркирование ошибок, являющихся дубликатами;
- возможность запуска систем динамического анализа на новых входных данных: Valgrind, Dr.Memory, QASan.

Широкие возможности по встраиванию пользовательских расширений:

- возможность добавления пользовательских обработчиков, которые будут автоматически запускаться на новых входных данных;
- возможность добавления пользовательских мутационных преобразований (для генерации новых входных данных и увеличения эффективности тестирования);
- наличие модулей пред- и постобработки входных данных для осуществления константных преобразований над данными перед их отправкой в анализируемое ПО;
- поддержка пользовательских плагинов отправки данных по сети (плагины позволяют осуществлять взаимодействие с клиентским или серверным ПО и отправлять мутированные данные);
- поддержка пользовательских скриптов на языке Python для модификации опций (позволяет избежать конфликтов при одновременном запуске множества процессов фаззинга);
- поддержка пользовательских плагинов на языке Python для управления окружением запуска целевого ПО (позволяет сохранять идентичное окружение на каждом запуске);
- поддержка пользовательских плагинов инструментации (позволяет задавать произвольные правила классификации входных данных на основе поведения целевого ПО: определение нормального и аварийного завершения, зависания);
- поддержка мутаций с учетом формата данных;
- возможность описывать сценарии для фаззинга ПО с пользовательским интерфейсом.

Лёгкая расширяемость и добавление новых методов в рамках существующей инфраструктуры; оперативная адаптация под новые задачи.

ДЛЯ КОГО ПРЕДНАЗНАЧЕН ИСП CRUSHER?

- Компании, нацеленные на разработку ПО с высоким уровнем надёжности и безопасности.
- Компании, разрабатывающие ПО для внедрения на значимых объектах КИИ.
- Компании, отвечающие за аудит или сертификацию ПО.

СИСТЕМНЫЕ ТРЕБОВАНИЯ

Требования к среде выполнения ИСП Crusher:

- операционная система: Ubuntu версии 18.04 и выше, CentOS версии 6.9 и выше, Astra Linux версии 1.5 и выше;
- ядро версии 2.6.32 или выше;
- библиотека glibc версии 2.12 или выше.

Требования к составу технических средств:

Минимальные требования:

- процессор (CPU): Intel Core i7 или аналогичный AMD;
- оперативная память (RAM): 8 Гб.

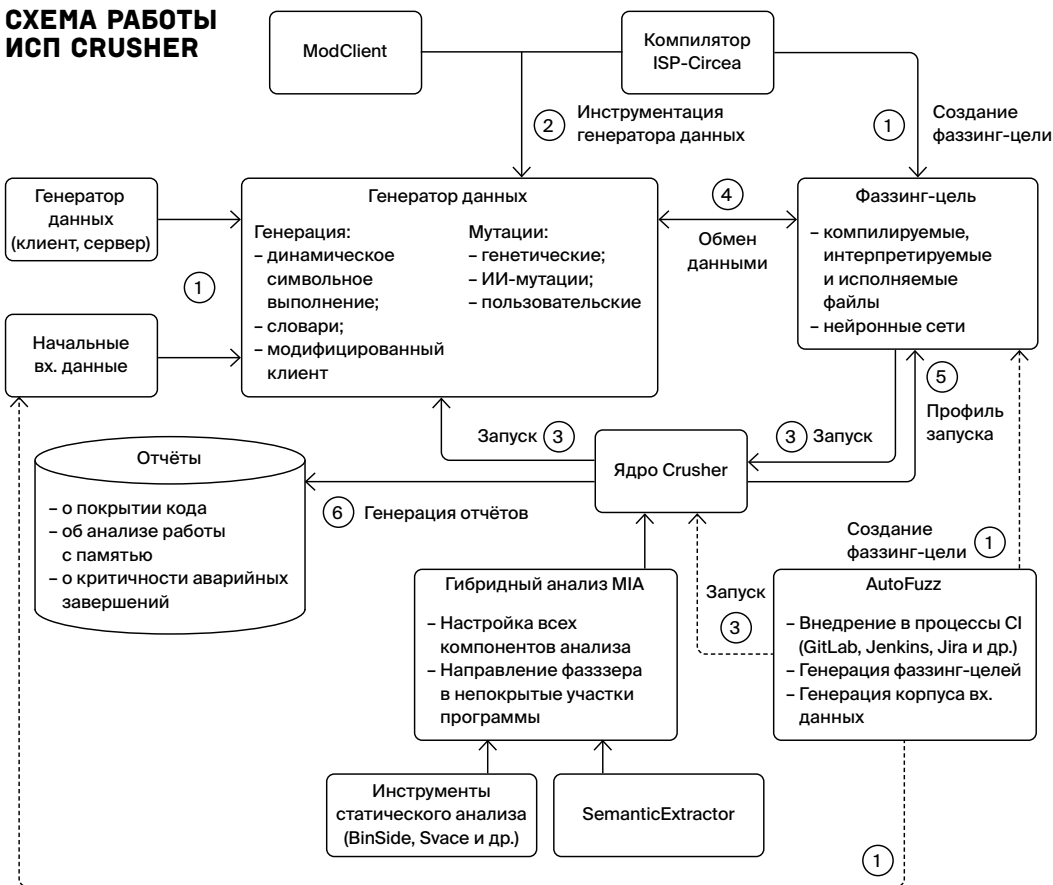
Рекомендуемые требования:

- процессор (CPU): 32-х ядерный и более Intel / AMD (в зависимости от требований к многопоточности фаззинг-тестирования);
- оперативная память (RAM): 32 Гб и более (в зависимости от потребления RAM целевой программой).

ОПЫТ ВНЕДРЕНИЯ

ИСП Crusher в различной комплектации используется более чем в 100 компаниях и лабораториях, в том числе в АО «НПО РусБИТех», ООО «Postgres Professional», ООО «Код Безопасности», МВП «СВЕМЕЛ», АО «СберТех», ООО «Базальт СПО», АО «Лаборатория Касперского», ООО «БАЗИС», Департаменте информационных технологий города Москвы (ДИТ г. Москвы) и др.

СХЕМА РАБОТЫ ИСП CRUSHER



BINSIDE: СТАТИЧЕСКИЙ АНАЛИЗАТОР БИНАРНОГО КОДА



BinSide — платформа обнаружения дефектов в программе методами статического анализа исполняемого кода. Необходима, когда нет доступа к исходному коду (например, при анализе закрытых библиотек).

ОСОБЕННОСТИ И ПРЕИМУЩЕСТВА

BinSide — платформа для анализа исполняемого кода, разрабатываемая на основе фреймворка BinNavi. Исполняемый файл анализируется в представлении IDA PRO или Ghidra. BinSide ищет дефекты, клоны кода, автоматизирует работу аналитика и оптимизирует динамическое тестирование.

Возможности ядра BinSide:

- Лёгкая расширяемость:
 - детекторы ошибок реализованы в виде подключаемых модулей;
 - используется промежуточное представление REIL из 17 инструкций без побочных эффектов (каждая ассемблерная инструкция транслируется в набор из REIL-инструкций);
 - анализ может быть уточнён аналитиком вручную.
- Поддержка анализа исполняемых файлов и библиотек для архитектур x86-64, ARM и MIPS, в том числе драйверов.
- Поиск дефектов следующих типов:
 - CWE-121 (Stack-based Buffer Overflow);
 - CWE-122 (Heap-based Buffer Overflow);
 - CWE-134 (Format String Vulnerability);
 - CWE-415 (Double Free);
 - CWE-416 (Use-After-Free);
 - CWE-77 (Command Injection);
 - CWE-190 (Integer Overflow).
- Выполнение следующих задач:
 - анализ потока данных и управления: восстановление значений и указателей, распространение помеченных данных, определение возможных состояний кучи, определение вычислимых ребёр графа потока управления;
 - межпроцедурный поиск дефектов: поиск дефектов выполняется на основе результатов внутривпроцедурного анализа потока данных и управления, результатов динамического анализа и ручной разметки

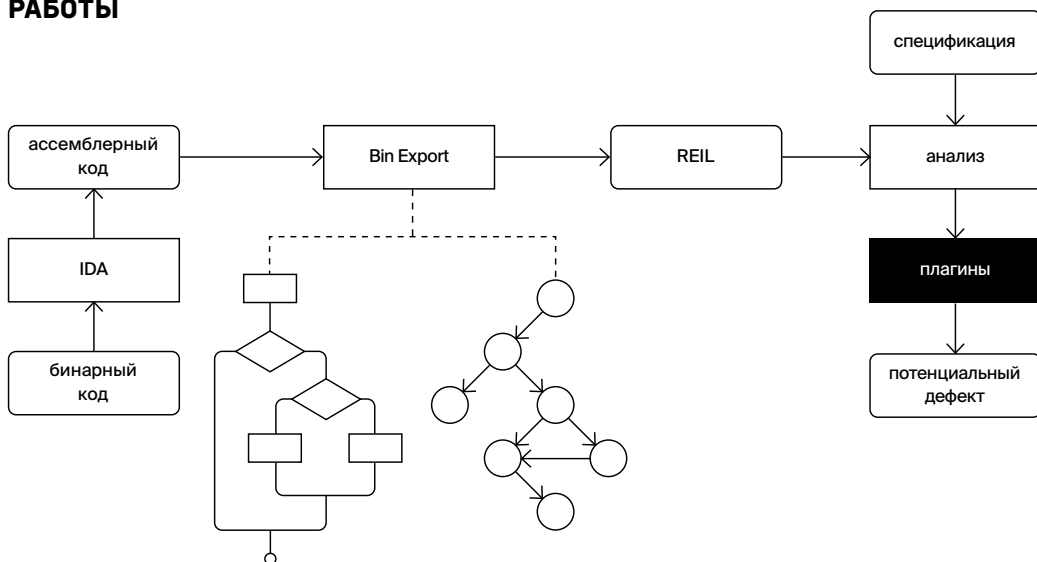
кода аналитиком. Это особенно полезно при анализе комплексного ПО и встраиваемых систем;

- анализ всех путей, независимо от покрытия кода.
- Взаимодействие с технологиями ИСП РАН:
 - с инструментом Svacer (при наличии исходного кода);
 - с инструментом LibraryIdentifier (для поиска клонов кода, например, для идентификации библиотек, с кодом которых был скомпонован исполняемый файл);
 - с инструментом Crusher для гибридного анализа;
 - с инструментом ISPuaro (для поиска клонов кода).

ДЛЯ КОГО ПРЕДНАЗНАЧЕН VINSIDE?

- Компании, которые нуждаются в тщательной проверке стороннего ПО, в том числе при отсутствии доступа к исходному коду.
- Разработчики, которым требуется повысить качество работы инструментов динамического анализа за счёт дополнительных данных, полученных с помощью статического анализа.
- Специалисты по обратной инженерии.
- Компании, отвечающие за аудит или сертификацию ПО.

СХЕМА РАБОТЫ



NATCH: ИНСТРУМЕНТ ОПРЕДЕЛЕНИЯ ПОВЕРХНОСТИ АТАКИ



Natch — это инструмент для определения поверхности атаки, основанный на полносистемном эмуляторе QEMU. Использует технологии анализа помеченных данных, интроспекции виртуальных машин и детерминированного воспроизведения. Включён в Единый реестр российского ПО (№13673).

ОСОБЕННОСТИ И ПРЕИМУЩЕСТВА

Основная функция Natch — получение поверхности атаки, то есть поиск исполняемых файлов, динамических библиотек, а также функций, отвечающих за обработку входных данных (файлов, сетевых пакетов) во время выполнения задачи. Собранные данные визуализируются в графическом интерфейсе SNatch, входящем в поставку инструмента.

Natch построен на базе полносистемного эмулятора QEMU, что позволяет анализировать все компоненты системы, включая ядро ОС и драйверы. Важное преимущество — объединение ключевых возможностей аналогов в одном инструменте.

Построение поверхности атаки может быть встроено в CI/CD для интеграционного и системного тестирования, что позволит повысить эффективность технологий функционального тестирования и фаззинга в жизненном цикле безопасного ПО.

ВОЗМОЖНОСТИ ИНСТРУМЕНТА NATCH

- сбор поверхности атаки: процессов, модулей и функций, которые обрабатывали помеченные данные во время выполнения тестового сценария;
- определение открытых портов, файлов, сокетов и потоков данных через них;
- поддержка анализа для языков C, C++, Go, Python, Java, JavaScript, C#;
- автоматическое скачивание отладочной информации для ядра и системных модулей;
- извлечение отладочной информации из DWARF;
- построение графа потоков помеченных данных через процессы и модули по всей системе;
- сбор лога сетевых пакетов в формате pcap;
- сбор покрытия бинарного и исходного кода;
- сбор корпуса данных для фаззинга выбранных функций (для аргументов простых типов).

СХЕМА ПРИМЕНЕНИЯ NATCH

- Natch записывает сценарий работы аналитика в виртуальной машине;
- аналитик помечает входящий сетевой трафик или обращения к определённым файлам;
- Natch воспроизводит записанный сценарий работы и отслеживает распространение помеченных данных, формирует архив логов операций с помеченными данными и системных событий;
- аналитик загружает полученный архив в графический интерфейс SNatch для изучения.

ВОЗМОЖНОСТИ ГРАФИЧЕСКОГО ИНТЕРФЕЙСА SNATCH

- Граф взаимодействия процессов, работавших с помеченными данными. Позволяет отслеживать потоки данных во времени и упорядочивать элементы схемы удобным для аналитика образом.
- Временная диаграмма процессов, работавших в системе.
- Стеки вызовов помеченных функций с разделением по процессам.
- Стеки вызовов для функций из скриптов при наличии их в объекте оценки.
- Flame-диаграмма процессов с цветовым дифференцированием помеченных и не помеченных функций.
- Просмотр дерева всех процессов, работавших в системе, с возможностью фильтрации только помеченных процессов.
- Просмотр ресурсов, использованных процессами во время работы.
- Просмотр операций чтения и записи для всех файлов и сокетов.
- Подсветка процессов, взаимодействующих с помеченными данными или имеющих повышенные привилегии (например, запущенные с правами root).
- Генерация аннотаций для функций для инструмента Futag.
- Передача отфильтрованного сетевого трафика в Wireshark.
- Удобный поиск по графам, а также сохранение истории перемещений.
- Генерация отчёта с основными аналитиками в формате PDF.
- API для автоматизированного тестирования поверхности атаки.

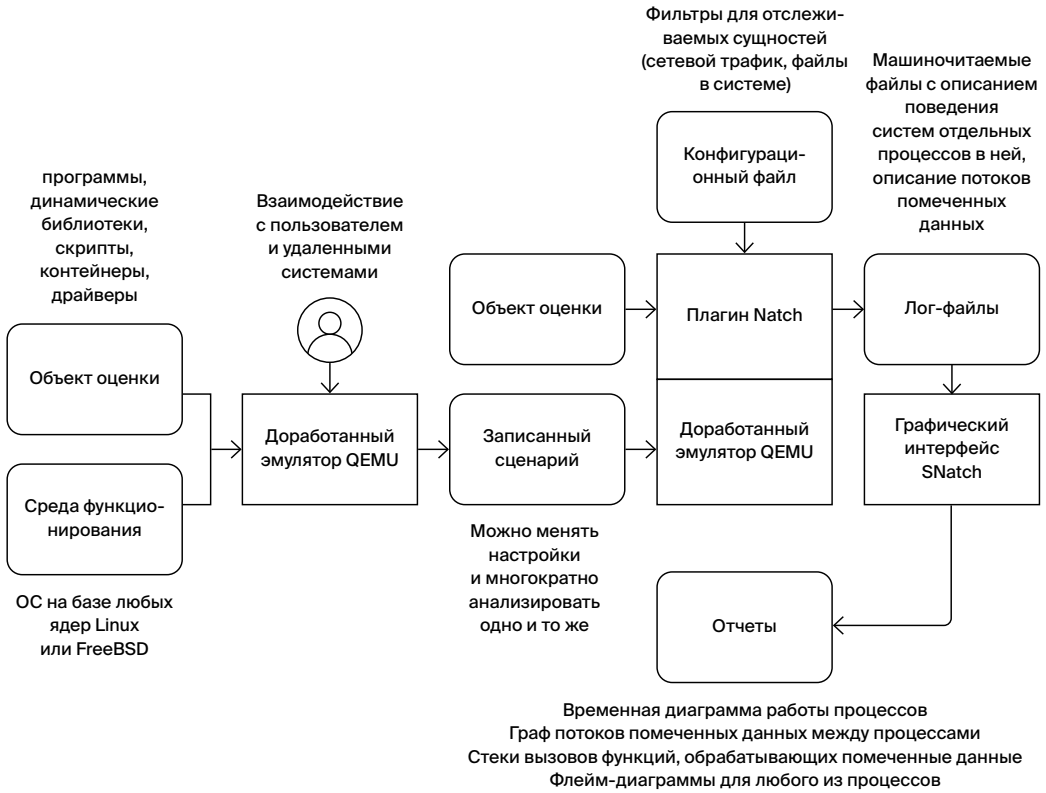
ДЛЯ КОГО ПРЕДНАЗНАЧЕН NATCH?

- Отечественные компании-разработчики безопасного ПО.
- Испытательные лаборатории и органы по сертификации.

ПОДДЕРЖИВАЕМЫЕ ПЛАТФОРМЫ И АРХИТЕКТУРЫ

- Системные требования инструмента Natch: ОС Linux x86-64, ОЗУ не менее 16 Гбайт, рекомендуется не менее 200 Гбайт дискового пространства.
- Целевые процессорные архитектуры: x86-64.
- Целевые ОС: семейство Linux (любые версии ядер), Windows 7-11, FreeBSD последних версий.

**СХЕМА
РАБОТЫ**



SYDR-FUZZ: КОМПЛЕКС ГИБРИДНОГО ФАЗЗИНГА И ДИНАМИЧЕСКОГО АНАЛИЗА

GitHub →
[https://github.com/
ispras/oss-sydr-fuzz](https://github.com/ispras/oss-sydr-fuzz)



Sydr — инструмент динамического символического выполнения бинарных программ, используемый для автоматической генерации тестов с целью увеличения покрытия кода и обнаружения ошибок. Строит математическую модель программы, позволяя фаззеру открывать новые пути выполнения, которые сложно обнаружить классическими методами генетических мутаций. Разработанные методы развивают технологию символического выполнения, представленную в созданных ранее в ИСП РАН инструментах Avalanche и Anxiety. Sydr-fuzz — инструмент динамического анализа программ для безопасного цикла разработки ПО, который реализует гибридный фаззинг с использованием Sydr и современных фаззеров (libFuzzer, AFL++, Honggfuzz), а также автоматизирует этапы сбора покрытия, минимизации корпуса и анализа аварийных завершений. Сайт проекта: sydr-fuzz.github.io.

ОСОБЕННОСТИ И ПРЕИМУЩЕСТВА

В отличие от аналогичных открытых инструментов, Sydr проверяет результаты своей работы на корректность и определяет, действительно ли сгенерированные входные данные приводят к инвертированию целевых переходов. Sydr-fuzz предоставляет возможности для удобной автоматизации пайплайна динамического анализа:

- фаззинг / гибридный фаззинг: `sydr-fuzz run`;
- минимизация корпуса: `sydr-fuzz cmin`;
- поиск ошибок с помощью предикатов безопасности: `sydr-fuzz security`;
- сбор покрытия: `sydr-fuzz cov-report`;
- создание отчётов, дедупликация, кластеризация и оценка критичности аварийных завершений с использованием Casr: `sydr-fuzz casr`.

Sydr-fuzz — это:

- Гибридный фаззинг с помощью Sydr и libFuzzer/AFL++/Honggfuzz проектов на C/C++, Rust, Go, C# (Native AoT).
- Автоматизация фаззинга и всего пайплайна динамического анализа Python/Java/JavaScript/C#/lua проектов с помощью инструментов Atheris/python-afl/Jazzer/Jazzer.jz/SharpFuzz/luzer.
- Эффективность на уровне мировых аналогов: регулярный бенчмаркинг фаззинга (<https://sydr-fuzz.github.io/fuzzbench/>).
- Репозиторий с настроенными проектами под фаззинг: 105 проектов (более 400 уникальных фаззинг-целей) в OSS-Sydr-Fuzz (<https://github.com/ispras/oss-sydr-fuzz>).
- Достижения: Sydr-fuzz нашел 179 новых ошибок в 32 проектах с открытым исходным кодом (<https://github.com/ispras/oss-sydr-fuzz/blob/master/TROPHIES.md>), 30 ошибок найдено с помощью предикатов безопасности.
- Эффективное символьное выполнение программ (concolic execution). Параллельное инвертирование и кэширование условных переходов, слайсинг формул из предиката пути, эвристика оптимистичных решений, высокоуровневое моделирование стандартных функций и использование производительного SMT-решателя Bitwuzla значительно ускоряют анализ. Реализованы алгоритмы по анализу неявных зависимостей (косвенные переходы, jump-таблицы и символьные указатели).
- Удобная автоматизация динамического анализа. Унификация запуска и результатов для различных фаззеров. Удобная настройка фаззинг-кампании с помощью конфигурационного файла. Поддержка параллельного фаззинга, вывод статистики, возможность одновременного запуска Sydr + libFuzzer + AFL++.
- Предикаты безопасности. Поиск ошибок методами символьного выполнения, заключающийся в генерации данных, приводящих к проявлению дефекта: деление на ноль, разыменование нулевого указателя, выход за границы массива, целочисленное переполнение, целочисленное усечение, ошибки форматной строки, внедрение команд.

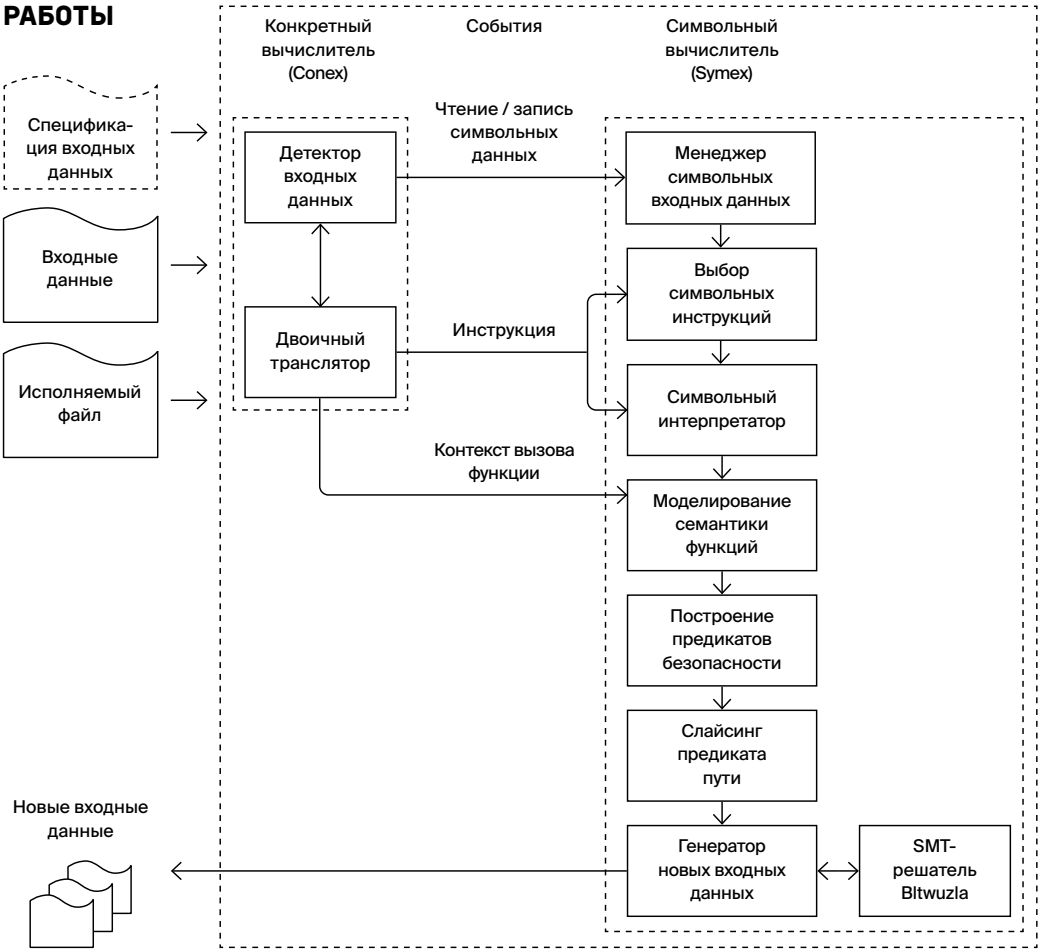
СИСТЕМНЫЕ ТРЕБОВАНИЯ

Запуск на платформах архитектуры x86_64, Aarch64 и RISCv64. Поддержка 64-битных ОС семейства Linux: Ubuntu 18.04/20.04/22.04, Astra 1.7, ALT Workstation 10.0 и аналогов.

ОПЫТ ВНЕДРЕНИЯ

Комплекс Sydr-fuzz включается в состав программного комплекса ИСП Crusher, который в разной комплектации используется более чем в 70 компаниях и лабораториях, в том числе в ОАО «РусБИТех», Postgres Professional, ООО «Код Безопасности», МВП «СВЕМЕЛ» и др. Используется в Исследовательском центре доверенного искусственного интеллекта ИСП РАН.

СХЕМА РАБОТЫ



LIBAFL-DIFUZZ: ИНСТРУМЕНТ НАПРАВЛЕННОГО ФАЗЗИНГА



LibAFL-DiFuzz — это инструмент направленного фаззинга, основанный на модульной архитектуре фаззера LibAFL и инструменте статической предобработки DiFuzz. LibAFL-DiFuzz позволяет выполнять фаззинг-тестирование, фокусируясь на достижении определенных участков кода. Данный вид анализа применяется для анализа патчей, воспроизведения ошибок, верификации предупреждений статического анализа. «Направление» фаззинга задается с помощью одной или нескольких целевых точек в исходном коде программы. Процесс направленного фаззинга начинается со статической предобработки тестируемой программы, в ходе которой формируются специальные метрики для анализа. В процессе фаззинга LibAFL-DiFuzz отслеживает состояние программы и адаптивно распределяет ресурсы для генерирования входных данных. Это значительно увеличивает скорость и вероятность достижения указанных участков кода.

ОСОБЕННОСТИ И ПРЕИМУЩЕСТВА

В отличие от аналогичных открытых инструментов, LibAFL-DiFuzz поддерживает гибкую и удобную конфигурацию, сигнализирует о достижении любой целевой точки в коде (не только аварийные завершения), а также поддерживает направленный фаззинг для нескольких целевых точек одновременно.

Работа LibAFL-DiFuzz организована в три этапа:

Статическая предобработка. Инструмент Difuzz выполняет построение графов и деревьев доминаторов, формирует улучшенные целевые последовательности ETS и рассчитывает контекстные веса.

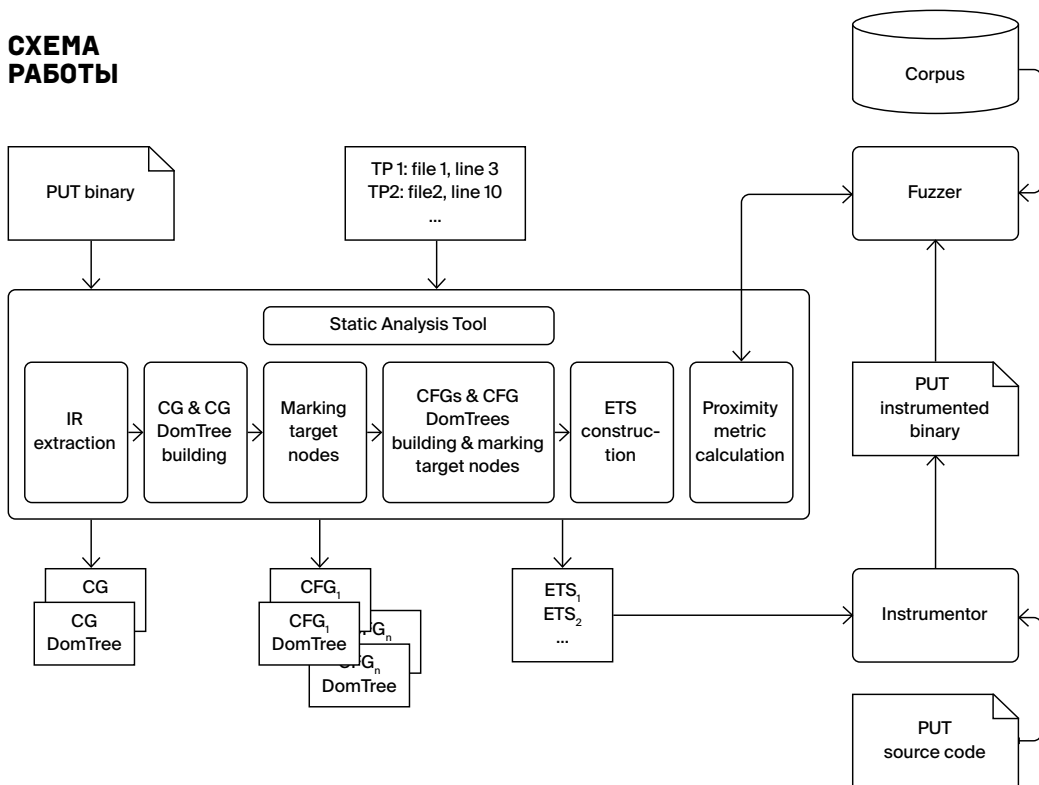
Сборка фаззинг-целей. Специальные компиляторы собирают фаззинг-цели с LibAFL-инструментацией, используя информацию, полученную от Difuzz.

Направленный фаззинг. LibAFL выполняет фаззинг-тестирование и рассчитывает метрику близости к целевым точкам для оценки входных данных. Метрика используется в планировщике энергии для приоритизации генерируемых входных данных.

Основные преимущества LibAFL-DiFuzz:

- метод планирования энергии во время фаззинга основан на алгоритме имитации отжига.
- метрика близости к целевым точкам строится на основе графа доминаторов и улучшенных целевых последовательностях (Enhanced Target Sequences, ETS).
- разрешение неявных вызовов при помощи анализа иерархий наследования.
- использование контекстных весов при построении целевых последовательностей улучшает точность.
- гибридный направленный фаззинг с динамическим символьным исполнением Sydr/Sydr-Fuzz.
- поддержка направленного фаззинга для C/C++/Rust/Go проектов.

СХЕМА РАБОТЫ



ISP AURORA: СТАТИЧЕСКИЙ АНАЛИЗАТОР С ТЕХНОЛОГИЕЙ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА



ISP Aurora — инструмент для выявления дефектов исходного кода и бинарных файлов путем генерации внутреннего представления программы и анализа этого представления большой языковой моделью (LLM).

ОСОБЕННОСТИ И ПРЕИМУЩЕСТВА

ISP Aurora — инструмент для анализа исходного и исполняемого кода, комбинирующий классический подход к анализу кода и подход на основе LLM, направленный на выявление дефектов. Найденные проблемы классифицируются по CWE и оформляются в текстовые отчёты.

Возможности ISP Aurora:

- Анализ кода без компиляции;
- Построение внутреннего представления для целевой программы;
- Автоматическое построение базы знаний о коде;
- Автоматический поиск дефектов в программах на основе статического анализа;
- Наличие расширенного набора детекторов по классификатору CWE;
- Генерация текстовых отчётов о найденных проблемах;
- Поддержка C/C++, Java, Kotlin, C#, Python, JavaScript и др.;
- Возможность использования локальных LLM моделей;
- Интерграция с инструментами Svace, Crusher, BinSide и ISPUaro.

ISPUARO: КОМПОЗИЦИОННЫЙ АНАЛИЗ



ISPUARO — инструмент, предназначенный для автоматизированного анализа компонентов ПО и сопровождающих артефактов с использованием поиска клонов кода, сопоставления бинарных файлов с исходным кодом, а также с собранной базой знаний, дефектами и метаданной. Позволяет построить процесс безопасной разработки в соответствии с ГОСТ Р 56939-2024.

ОСОБЕННОСТИ И ПРЕИМУЩЕСТВА

Инструмент ISPUARO позволяет пользователям проводить инвентаризацию ПО и выявлять возможные дефекты. Предоставляет собственную базу знаний, которая содержит более 500 тысяч исходных и бинарных пакетов Debian и хранит сведения обо всех версиях, начиная с 2010 года. База дополнительно включает актуальную информацию об известных дефектах и соответствующих им версиях ПО.

Загрузка и обработка проектов:

- предоставляет собранную базу знаний с проектами;
- позволяет загружать, обрабатывать, собирать и хранить проекты в базе знаний (в проекте может содержаться как исходный код, так и бинарный, а также метаданная о проекте);
- создает связи между проектами, их версиями, производителями и зависимостями в базе знаний;
- позволяет загружать в базу знаний пользовательские проекты для последующего анализа.

Загрузка и обработка дефектов:

- предоставляет собранную базу знаний с обработанными дефектами из открытых источников (идентификаторы дефектов, а также дефекты, реализующие механизмы контроля доступа и привилегий);
- автоматизированное обновление базы знаний;
- позволяет загружать в базу знаний пользовательские дефекты.

Анализ и поиск клонов:

- проведение анализа компонентов целевого ПО с целью выявления динамических зависимостей и поиска флагов защиты;
- генерация промежуточного представления бинарных компонентов ПО для создания PDG с помощью интеграции статического анализатора BinSide;
- поиск информации о компонентах;

- сопоставление бинарных файлов с исходным кодом;
- поиск клонов кода;
- перенос информации о дефектах из базы знаний в пользовательский проект при помощи результатов поиска клонов кода.

Генерация отчетов:

Генерация отчета об анализе компонентов целевого ПО в стандартизированном формате SBOM (CycloneDX), в котором содержится информация о компонентах, их зависимостях, версиях и дефектах, а также другая метаданная информация.

Пользовательский интерфейс:

Предоставление пользовательского интерфейса, предоставляющего доступ ко всему функционалу ISPUARO.

ДЛЯ КОГО ПРЕДНАЗНАЧЕН ISPUARO?

- компании, которые нуждаются в тщательной проверке стороннего ПО, в том числе при отсутствии доступа к исходному коду;
- компании, нацеленные на разработку ПО с высоким уровнем надёжности и безопасности;
- компании, разрабатывающие ПО для внедрения на значимых объектах КИИ;
- компании, отвечающие за аудит или сертификацию ПО.

PROTOSPHERE:

СИСТЕМА АНАЛИЗА СЕТЕВОГО ТРАФИКА



Protosphere — система глубокого анализа сетевого трафика (DPI). Может встраиваться как компонент в системы мониторинга, классификации, защиты от вторжений и утечек информации. Регистрирует несоответствия между реализацией протокола и фактическим трафиком. Позволяет быстро добавлять поддержку новых (в том числе закрытых) протоколов благодаря универсальности внутреннего представления.

ОСОБЕННОСТИ И ПРЕИМУЩЕСТВА

Protosphere — инновационная система, основанная на научных исследованиях технологий анализа сетевого трафика. Объединяет ключевые особенности иностранных аналогов (Wireshark, Microsoft Message Analyzer, nDPI) с универсальным внутренним представлением, позволяющим быстро расширять возможности анализа.

Protosphere — это:

- Оптимальные возможности ядра системы:
 - универсальная модель представления данных при разборе сетевого трафика;
 - обработка данных, содержащих искажения, потери, перестановки и дублирование пакетов, а также асимметричный трафик;
 - поддержка анализа сжатых и зашифрованных данных;
 - поддержка туннелей произвольной конфигурации;
 - поддержка связанных потоков.
- Поддержка всех этапов анализа сетевой трассы — каждый этап с отдельным компонентом визуализации, все компоненты синхронизированы:
 - локализация одного или нескольких исследуемых сетевых соединений на графе сетевых взаимодействий и в дереве сетевых потоков;
 - детализация выделенных соединений на временной диаграмме;
 - наглядное представление выделенных в сетевых пакетах полей в дереве разбора сетевого потока;
 - выявление несоответствий между реализацией протокола и фактическим трафиком в журнале диагностики;
 - извлечение и анализ данных произвольного уровня (L7+).
- Широкий список поддерживаемых протоколов:
 - Dns, Dhcp, Rip;
 - Tls, Microsoft-Rpc, Postgresql;
 - Ftp, Http, Imap, Smtп, Pop3, BitTorrent;
 - Kerberos, Ntlm;
 - Gre, IpSec, Ppp, OpenVpn, Wireguard;

- Быстрое расширение списка поддерживаемых протоколов:
 - API доступ к результатам разбора;
 - локализация ошибок разбора;
 - декларативное описание форматов сетевых протоколов.
- Поддержка двух режимов работы: на потоке и в отложенном режиме.
- Возможность работы в качестве DPI as Service.
- Продвинутый графический интерфейс, позволяющий выбирать наиболее удобный вариант представления результатов проводимого анализа.
- Возможности по расширению функционала системы:
 - поддержка новых программных интерфейсов;
 - разработка различных механизмов работы с результатами разбора;
 - обавление новых возможностей ядра разбора.
- Адаптация под сетевой канал и доступные вычислительные ресурсы: гибкая система конфигурирования позволяет находить баланс между детализацией/точностью анализа и потребляемыми ресурсами.

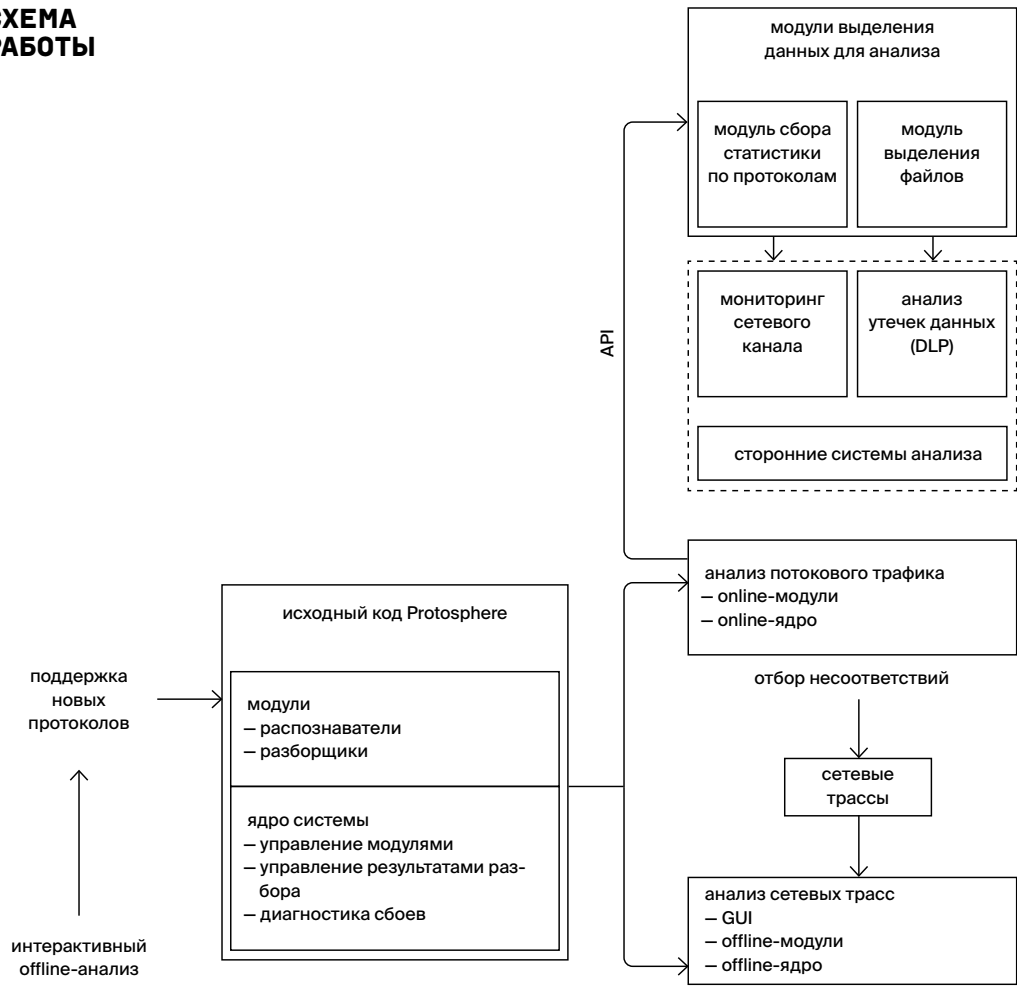
ДЛЯ КОГО ПРЕДНАЗНАЧЕНА PROTOSPHERE?

- Компании, занимающиеся тестированием реализаций сетевых протоколов (в том числе во встраиваемых ОС и сетевой аппаратуре).
- Компании-разработчики средств сетевой безопасности (межсетевых экранов, а также систем обнаружения и предотвращения вторжений, в том числе от атак нулевого дня).
- Компании по производству техники, нуждающейся в повышенном уровне безопасности из-за обязательной сертификации.
- Компании, которым требуется контроль и мониторинг сетевых каналов в режиме реального времени.

ПОДДЕРЖИВАЕМЫЕ ПЛАТФОРМЫ И АРХИТЕКТУРЫ

Архитектуры: Intel x86-64, arm64.
Платформы: ОС Windows, ОС на базе ядра Linux, Apple macOS.

СХЕМА РАБОТЫ



ML IDS: СЕТЕВАЯ СИСТЕМА ОБНАРУЖЕНИЯ ВТОРЖЕНИЙ С ПРИМЕНЕНИЕМ МАШИННОГО ОБУЧЕНИЯ



ML IDS – сетевая система обнаружения вторжений (СОВ), базирующаяся на результатах передовых научных исследований в области применения машинного обучения для обнаружения компьютерных атак. За счёт обобщающей способности используемых моделей машинного обучения система позволяет обнаруживать ранее неизвестные атаки (атаки нулевого дня, zero day).

ОСОБЕННОСТИ И ПРЕИМУЩЕСТВА

ML IDS обнаруживает на сетевом уровне широкий спектр веб-атак на основе анализа признаков сессий. Технология предусматривает работу при использовании как открытого (HTTP), так и защищенного (HTTPS) протокола передачи данных. Инспекция протоколов HTTP/2 и HTTP/3 возможна с применением обратного прокси-сервера в защищаемой сети (например, HTTP роутера nghttpx).

Проведенное тестирование и сравнение ML IDS с сигнатурными средствами обнаружения и предупреждения атак с открытыми исходными кодами показало, что эта система:

- превосходит сигнатурную сетевую систему обнаружения вторжений (NIDS) Suricata по качеству обнаружения атак при работе с зашифрованным трафиком HTTPS;
- сопоставима по качеству с сигнатурным межсетевым экраном для веб-приложений (WAF) ModSecurity в моделируемых условиях.

ML IDS предусматривает возможность использования сигнатурных средств защиты информации как дополнительных источников данных обучения для повышения обобщающей способности модели и качества обнаружения атак.

ML IDS – это:

- Обнаружение атак во времени, близком к реальному.
- Возможность выявления ранее неизвестных атак.
- Выявление атак без анализа содержимого пакетов (возможность работы на зашифрованном трафике).
- Адаптация под меняющиеся условия (возможность дообучения и выбора оптимальной модели).
- Модульная архитектура, позволяющая наращивать производительность.
- Наличие процедуры автоматизированного развёртывания инфраструктуры генерации и сбора обучающего набора данных.
- Удобный веб-интерфейс с результатами работы ML IDS, который может быть легко настроен на отображение необходимых данных.

В текущем исполнении ML IDS обучена и способна выявлять следующие типы веб-атак: XSS, SQL Injection, Command Injection, Brute Force, Web Shell, DoS.

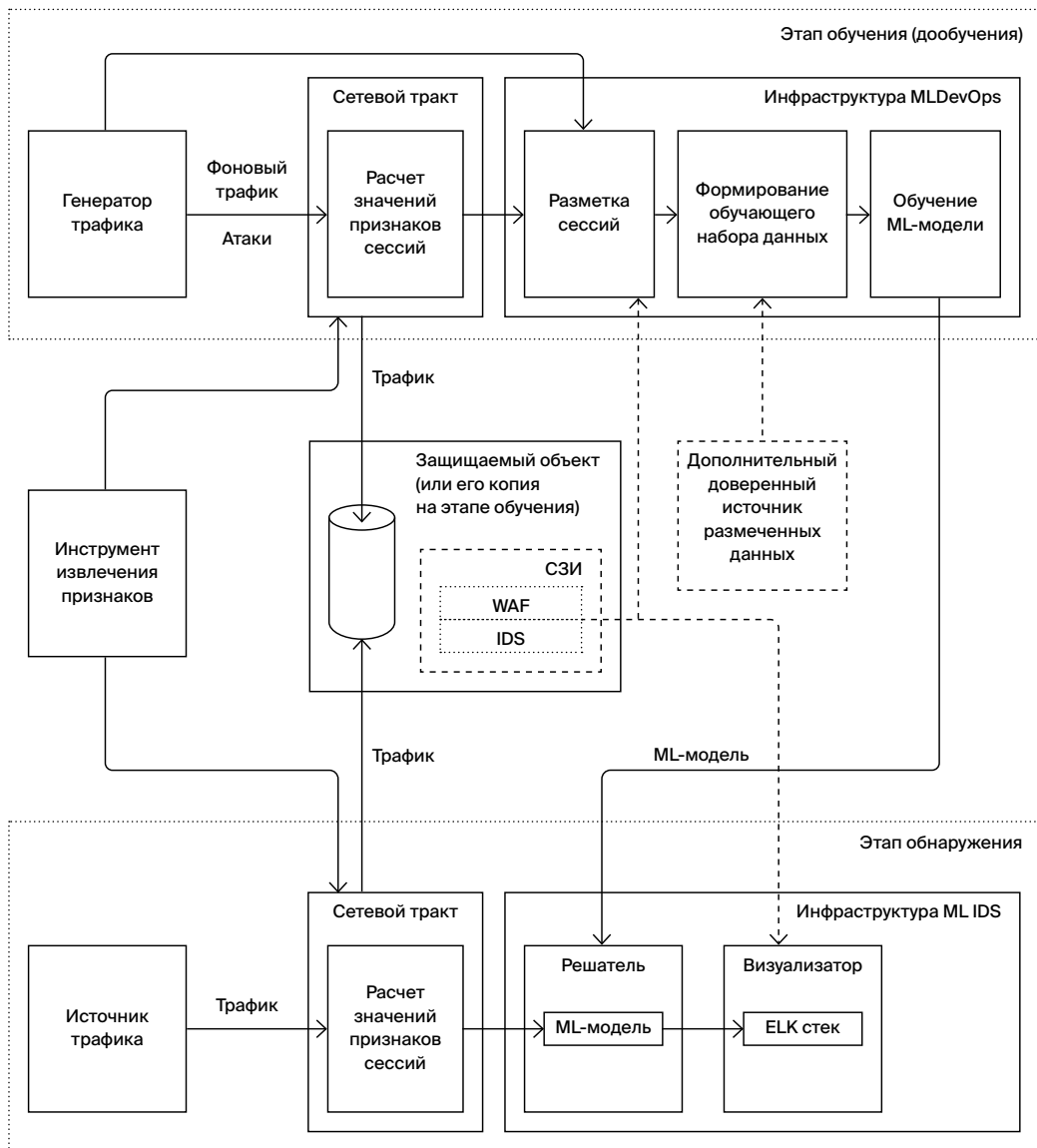
ПОДДЕРЖИВАЕМЫЕ ПЛАТФОРМЫ И АРХИТЕКТУРЫ

Платформы: ОС на базе ядра Linux.
Архитектуры: Intel x86-64.

ДЛЯ КОГО ПРЕДНАЗНАЧЕН ML IDS?

- Компании, которым требуется защита сетевых ресурсов от компьютерных атак.
- Компании-разработчики средств сетевой безопасности (межсетевых экранов, систем обнаружения и предотвращения вторжений).

СХЕМА РАБОТЫ



REQUALITY: ИНСТРУМЕНТ УПРАВЛЕНИЯ ТРЕБОВАНИЯМИ



Requality — расширяемый инструмент для управления требованиями. Позволяет как разрабатывать требования к проектируемым системам с нуля, так и формировать каталоги требований путём разметки существующих документов, сохраняя при этом связи между требованиями и текстовыми фрагментами исходных документов. Поддерживает организацию иерархической структуры требований, трассируемость между требованиями разных уровней, возможность совместной работы над требованиями с использованием системы управления версиями GIT.

ОСОБЕННОСТИ И ПРЕИМУЩЕСТВА

Уникальной возможностью Requality является возможность формирования каталога требований путём разметки существующих документов, при этом у каждого требования сохраняется связь с одним или несколькими текстовыми фрагментами исходного документа.

По другим функциональным возможностям Requality близок к существующим коммерческим аналогам (IBM DOORS, Jama, Polarion) и превосходит ряд имеющихся свободно распространяемых продуктов (aNimble, ProR, RMT00). Инструмент и руководство пользователя доступны на сайте проекта: <https://requality.ru>.

Requality — это:

- Структурирование и хранение каталога требований:
 - каталог требований — это структурированный набор связанных требований и других элементов, хранящийся в рамках единого рабочего пространства. В качестве элементов верхнего уровня выступают проекты, в которых хранятся отдельные наборы требований. Такая возможность используется в том числе для отделения требований верхнего уровня от разработанных на их основе требований нижнего уровня;
 - элементы каталога включают в себя различные виды узлов:
 - требования, содержащие описания возможностей разрабатываемого объекта или накладываемые на него ограничения;

- текстовые узлы, не являющиеся непосредственно требованиями, но обеспечивающие контекст для их понимания (например, описания терминов или примечания);
- документальные представления требований, на основе которых был разработан каталог;
- настройки отчётов и результаты их генерации;
- комментарии.

Набор элементов каталога может быть расширен путем разработки расширений;

- идентификация узлов поддерживается несколькими способами, в том числе с использованием уникального в пределах проекта числового идентификатора и составного удобочитаемого иерархического пути;
- свойства узлов включают в себя как предоставляемые инструментом по умолчанию (описание узла, короткий строковый идентификатор и другие), так и определяемые пользователем параметры, используемые для обозначения характеристик элементов;
- применение HTML-разметки в тексте требований и в других свойствах позволяет использовать различные средства форматирования текста и обеспечивать использование вспомогательных ресурсов, таких как изображения и таблицы.
- Управление связями, трассируемость и анализ покрытия:
 - задание связей между элементами каталога с произвольным именем. Имена связей позволяют определить отношения различных видов;
 - автоматическое построение связей по терминологии путём перечисления списка терминов, используемых в требовании, и установки соответствующего атрибута у узла, который этот термин определяет;
 - задание связи между фрагментом текста и требованием позволяет, с одной стороны, определить источник возникновения отдельного требования, а с другой — предоставляет возможность автоматизированного переноса подобных связей на новые версии документов;
 - сквозная трассируемость представляет собой возможность проследить для отдельного требования как исходные требования, так и разработанные на его основе, а также изучить контекст элемента каталога, в рамках которого его стоит рассматривать;
 - покрытие представляет собой информацию о степени реализации или полноте тестирования каталога требований. Покрытие оценивается по информации о наличии связи между элементами каталога и внешними элементами либо между элементами внутри каталога. В инструменте поддерживается возможность использования внешней информации о покрытии в форме файла определенного формата, а также обеспечивается расширяемый набор источников данных о покрытии.

- Управление изменениями и поддержка совместной работы:
 - в качестве основной системы для совместной работы над каталогом требований поддерживается GIT. В интерфейсе инструмента доступен упрощённый набор команд для отправки изменений и обновления локальной версии проекта;
 - в интерфейсе инструмента доступен просмотр версий как отдельного узла, так и каталога требований в целом с возможностью сравнения отдельных версий;
 - поддерживается возможность сравнения версий проектов, а также переключения на предыдущие версии.
- Генерация отчётов, в частности:
 - формирование различных представлений каталога требований, в том числе для работы с ним вне инструмента, а также для обмена данными каталога требований с другими инструментами или решения нестандартных задач в рамках разработки;
 - предоставление данных о трассируемости для просмотра информации о связях между элементами каталога требований;
 - сравнение версий каталога в целях контроля прогресса работы над каталогом требований путем изучения различий структуры и свойств требований проекта для выбранных версий каталога;
 - анализ покрытия для рассмотрения статуса отдельных элементов каталога с точки зрения информации о покрытии, полученной из выбранного источника;
 - поддержка пользовательских шаблонов с использованием доступной информации относительно каталога, его версий и информации о покрытии.
- Поддерживается программный интерфейс (API) с возможностью изменения хранимых данных и создания новых проектов. В том числе он может быть использован для обмена данными со сторонними инструментами.
- Доступна возможность разработки расширений для задания новых элементов, источников информации о покрытии или для получения новых функциональных возможностей.

СИСТЕМНЫЕ ТРЕБОВАНИЯ

ОС Windows или ОС на базе ядра GNU/Linux, Java Runtime.

ОПЫТ ВНЕДРЕНИЯ

Requality разрабатывается с 2011 года. Использовался для разработки и управления изменениями требований в проекте по разработке операционной системы реального времени в соответствии с процессами, предписанными КТ-178С, а также для каталогизации требований из различных стандартов (в том числе TTCN и POSIX) с целью проведения последующего тестирования совместимых с ними продуктов на соответствие стандарту.

2

АНАЛИЗ ДАННЫХ

ИНФРАСТРУКТУРА И ИНСТРУМЕНТЫ РАЗРАБОТКИ ИИ-РЕШЕНИЙ

- 93 Асперитас и другие облачные решения
- 97 Talisman: платформа для построения интеллектуальных информационно-аналитических систем
- 100 Платформа Доверенного Искусственного Интеллекта (ДИИ)
- 102 Colba: система поддержки создания наборов данных

ОБРАБОТКА ЕСТЕСТВЕННЫХ ЯЗЫКОВ

- 104 Lingvodoc: виртуальная лаборатория для документации исчезающих языков

ОБРАБОТКА ДОКУМЕНТОВ

- 107 Dedoc: система извлечения содержимого и структуры текстовых документов
- 109 DocMarking: противодействие анонимности при утечках документов

ПРИКЛАДНЫЕ РЕШЕНИЯ

- 111 EcgHub: интеллектуальный анализ цифровых ЭКГ

АСПЕРИТАС И ДРУГИЕ ОБЛАЧНЫЕ РЕШЕНИЯ

Асперитас — платформа организации ресурсоёмких вычислений и хранения данных в научных, образовательных и коммерческих целях. Кроме одноимённой облачной среды в состав платформы входят также Michman — оркестратор платформенных распределённых сервисов, основанный на стандарте TOSCA. Кроме того, в число облачных решений ИСП РАН входит Fanlight — платформа для объединения исследований в web-лаборатории и Cotea — системное ПО, предназначенное для программного контроля исполнения сценариев Ansible.

ОБЛАЧНАЯ СРЕДА АСПЕРИТАС



В основе облачной среды Асперитас лежат открытые технологии Openstack и Ceph, которые являются современным стандартом для построения больших частных облачных систем. Дистрибутив поставляется как готовое решение, включающее всё необходимое для настройки, в том числе TUI-установщик.

Другие преимущества Асперитас:

- Отчуждаемость решений: инфраструктура воссоздаётся в изолированной среде с полным контролем над ней за счёт использования открытых стандартов, свободного ПО, научных разработок ИСП РАН, а также изолированного репозитория исходных кодов.
- Высокий уровень безопасности: платформа построена на уменьшенной кодовой базе для сокращения поверхности атаки, а также использует собственные решения по усилению безопасности.
- Стандартные интерфейсы управления виртуальными сетями и вычислительными ресурсами с использованием систем Keystone, Neutron, Nova.
- Блочное хранение данных и расширяемое объектное хранилище на основе распределённой файловой системы Ceph.
- Возможность адаптации платформы под решение задач конкретной предметной области: решение задач механики сплошных сред, анализ больших данных, биомедицина, анализ уязвимости программ и др.

Облачная среда Асперитас включена в Единый реестр российского ПО (№5921), а также имеет сертификат ФСТЭК №4880 по соответствию требованиям доверия 4 уровня и требованиям к средствам виртуализации 4 уровня приказа 187 ФСТЭК.

Асперитас работает в промышленном режиме в НИЦ «Курчатовский институт».

На базе Асперитас также построен коммерческий дистрибутив moncloud (<https://moncloud.ru>) в рамках сотрудничества с ООО «Системные решения».

УНИВЕРСАЛЬНЫЙ ОРКЕСТРАТОР MICHMAN

<https://michman.ispras.ru>



Michman — оркестратор сервисов уровня PaaS для хранения и анализа больших данных, задач машинного обучения, инструментов управления нагрузкой и других. Инструмент позволяет автоматически развёртывать распределённые кластеры в облачной среде с учётом пользовательских требований и настроек. Им предоставляется интерфейс для развёртывания наборов сервисов из заранее настроенных шаблонов и управления их жизненным циклом, в частности:

- кластер для анализа больших данных с системами Apache Spark, Apache Hadoop, настроенными для корректного взаимодействия между собой на произвольном числе вычислительных узлов;
- СУБД различных классов: от классических реляционных до распределённых аналитических;
- система управления ресурсами кластера и планировщик задач Slurm с возможностью использования GPU;
- гибко настраиваемая система оркестрации контейнерных приложений Kubernetes, а также инструменты, работающие поверх неё;
- инструменты для разработки моделей искусственного интеллекта, в частности Jupyter, MLflow, Ray.

Ключевые преимущества оркестратора Michman — это гибкость и расширяемость списка поддерживаемых сервисов за счёт использования языка TOSCA и поддержки следующих механизмов:

- Substitution Mapping, который позволяет унифицировано использовать однотипные ресурсы. Например, этот механизм позволяет описывать возможность развёртывания на различных ресурсах (в приватном или публичном облаке, на выделенных серверах либо с использованием контейнеров). Также с его помощью можно описать интеграцию какого-либо приложения с различными СУБД, подключение различных файловых систем и другое.
- Select, с помощью которого пользователь может переиспользовать созданные ранее ресурсы или использовать сторонние (внешний репозиторий, общая сетевая файловая система).

Кроме того, Michman позволяет консистентно сохранять состояние всех компонентов облачного приложения, масштабировать узлы, управлять отдельными частями приложения, производить обновление запущенных сервисов.

ПЛАТФОРМА FANLIGHT

<https://fanlight.ispras.ru>



Fanlight — платформа по предоставлению виртуальных рабочих столов (DaaS — Desktop as a Service). Позволяет разворачивать SaaS-инфраструктуру для вычислительных web-лабораторий. Создана в результате участия ИСП РАН в программе «Университетский кластер» и в международном проекте Open Cirrus (учреждён HP, Intel и Yahoo!). Fanlight базируется на контейнерных технологиях — в отличие от основных решений данного класса, основывающихся на виртуальных машинах. Изначально платформа базировалась на технологии Docker Compose. Позднее появилась реализация на основе Kubernetes. Поддерживает только приложения, разработанные для ОС на базе ядра Linux. Включена в Единый реестр российского ПО (№6066).

Другие преимущества Fanlight:

- Высокая эффективность работы с облачными вычислениями благодаря использованию контейнеров:
 - комфортная работа с тяжёлыми инженерными CAD-CAE приложениями, требующими поддержки аппаратного ускорения 3D-графики для сложной визуализации;
 - поддержка выполнения MPI, OpenMP, CUDA приложений за счёт доступа к HPC-кластерам, многоядерным процессорам и графическим ускорителям NVIDIA.
- Расширенные вычислительные возможности на уровне PaaS за счёт подключения аппаратных ресурсов (HPC/BigData кластеры, системы хранения, сервера с графическими ускорителями).
- Возможность кастомизации под заданную прикладную область за счёт интеграции специализированных расчётных прикладных пакетов, а также простоты их добавления. В частности, есть опыт внедрения:
 - в области MCC: OpenFOAM, SALOME, Paraview и др.;
 - в области Gas&Oil: tNavigator, Eclipse, Roxar, Tempest и др.
- Работа через любой тонкий клиент (включая мобильные устройства) без вспомогательного ПО.
- Развёртывание на сервере, вычислительной ферме, в облаке (с уровня IaaS), в кластере Kubernetes или в собственном облачном ЦОД. Версия на основе Kubernetes позволяет также использовать различные CRI-движки исполнения контейнеров.

ИНСТРУМЕНТ COTEA

GitHub →
<https://github.com/ispras/cotea>



Cotea — инструмент, позволяющий программно запускать Ansible и контролировать его выполнение (Ansible — одна из самых популярных систем по развёртыванию ПО).

Cotea позволяет:

- программно контролировать выполнения Ansible, итерируясь по составным частям Ansible-сценария;
- встраивать Ansible в другие системы;
- отлаживать выполнения Ansible, в том числе и интерактивно. Переход в интерактивный режим происходит в случае ошибки выполнения task (составной части Ansible-сценария). Примеры функций, предоставляемых в интерактивном режиме:

- перезапустить задание, завершившееся с ошибкой;
- продолжить выполнения сценария Ansible без неудавшегося задания;
- добавить новую переменную Ansible в процессе исполнения;
- добавить новый Ansible task в процессе исполнения.

Интерактивный режим позволяет не начинать выполнение сценария заново в случае возникновения ошибок, что особенно важно при работе с большими сценариями.

На данный момент Cotea используется при развёртывании платформы Асперитас. Grpc-cotea является компонентом Michman и Clouni. Именно grpc-cotea позволяет данным системам оркестрации контролировать процесс развёртывания облачных приложений.

ОПЫТ ВНЕДРЕНИЯ

Вычислительный кластер на базе Асперитас используется для работы ряда технологий ИСП РАН (в частности, для анализа ОС Android с помощью Svace). Реализованы совместный проект с компанией Huawei (анализ больших графов с помощью технологий обработки больших данных) и инфраструктура поддержки жизненного цикла ОС Tizen, позволяющая организовать процесс совместной разработки компонентов ОС и автоматизировать регулярную сборку и тестирование образов. Кроме того, осуществляется ряд работ при участии Минобрнауки РФ. На базе среды Асперитас реализована облачная Платформа НЦМУ «Цифровой биодизайн и персонализированное здравоохранение», а также развёрнута облачная среда в НИЦ «Курчатовский институт».

В рамках соглашения, заключённого в ноябре 2023 года между ИСП РАН и ООО «Системные решения», на основе Асперитас разработано проприетарное коммерческое решение moncloud, ориентированное на бизнес, науку и образование. На момент написания вышла версия 1.5 и проводятся работы по сертификации ФСТЭК.

Возможности платформы Fanlight использовались в ряде совместных проектов по развёртыванию web-лабораторий с ФГУП «РФЯЦ-ВНИИЭФ», ООО «РРС-Балтика», ИПМ им. М.В. Келдыша РАН (разработка технологий для увеличения и эффективного использования ресурсного потенциала углеводородного сырья Союзного государства), а также с Лабораторией механики сплошных сред ИСП РАН (<https://unicfd.ru>).

TALISMAN: ПЛАТФОРМА ДЛЯ ПОСТРОЕНИЯ ИНТЕЛЛЕКТУАЛЬНЫХ ИНФОРМАЦИОННО- АНАЛИТИЧЕСКИХ СИСТЕМ



Talisman — это комплекс взаимосвязанных программных инструментов для автоматизации типовых задач обработки данных, включая их сбор, интеграцию, анализ, хранение и визуализацию. Обеспечивает быструю разработку специализированных многопользовательских интеллектуальных аналитических систем, объединяющих информацию из внутренних баз данных и открытых источников сети Интернет (в том числе из социальных сетей).

ОСОБЕННОСТИ И ПРЕИМУЩЕСТВА

Talisman использует технологии больших данных и передовые методы доверенного искусственного интеллекта для извлечения информации из произвольных источников. Позволяет быстро создавать интеллектуальные аналитические системы, используя подходы Low-code и No-code. Постоянно обучается на результатах работы аналитика, не требуя дополнительных трудозатрат.

Talisman — это:

- Широкий набор переиспользуемых компонентов, каждый из которых обладает программным интерфейсом для удобного управления и взаимной интеграции:
 - Компоненты для получения исходных данных. В частности, это программный комплекс сбора данных из сети Интернет: из соцсетей (Вконтакте, Facebook, Twitter, Instagram, Одноклассники, Youtube, LinkedIn и др.), блогов, СМИ, сайтов mediawiki, порталов разработчиков ПО и др. Кроме того, есть система импорта данных из файловых хранилищ и СУБД.
 - Компоненты автоматического анализа данных. Набор инструментов, позволяющих преобразовать входные данные любых форматов и привести их к единому универсальному представлению (в частно-

- сти, используется разработка ИСП РАН Dedoc). Документы в этом представлении подвергаются анализу с помощью методов машинного обучения. Имеется возможность добавлять собственные обработчики в виде контейнеров с REST API. Управление последовательностью обработки осуществляется системой «Talisman.Поток» (№6045 в Едином реестре российского ПО).
- Компоненты хранения и индексации. Это группа СУБД и информационно-поисковых систем, где хранятся исходные данные, результаты автоматической обработки, а также результаты работы пользователей.
 - Удобный веб-интерфейс, который объединяет все компоненты, предполагающие взаимодействие с пользователями.
 - Гибкая модульная архитектура, позволяющая добавлять новые функции в отдельные компоненты без изменения большинства остальных.
 - Горизонтально масштабируемая архитектура, позволяющая увеличивать объёмы обрабатываемых и хранимых данных без изменения программной части за счёт добавления аппаратных ресурсов.
 - Специализированные подсистемы, которые отвечают за мониторинг состояния компонентов, управление журналом событий, развёртывание, аутентификацию и авторизацию, разграничение прав доступа, а также одностороннюю передачу данных.
 - Инструменты и методики обучения моделей машинного обучения, а также переноса имеющихся моделей и алгоритмов на новую предметную область.
 - Настраиваемая схема предметной области с возможностью внесения изменений оператором в процессе эксплуатации системы.
 - Полная отчуждаемость разрабатываемых систем. Каждая из них может быть развёрнута на площадке заказчика — как на существующем оборудовании, так и в составе программно-аппаратного комплекса.
 - Интеграция с внутренними системами потребителя благодаря наличию программного интерфейса для управления всеми компонентами.
 - Лицензионная чистота благодаря базированию на собственных разработках ИСП РАН и свободном ПО.

ОБЛАСТИ ПРИМЕНЕНИЯ

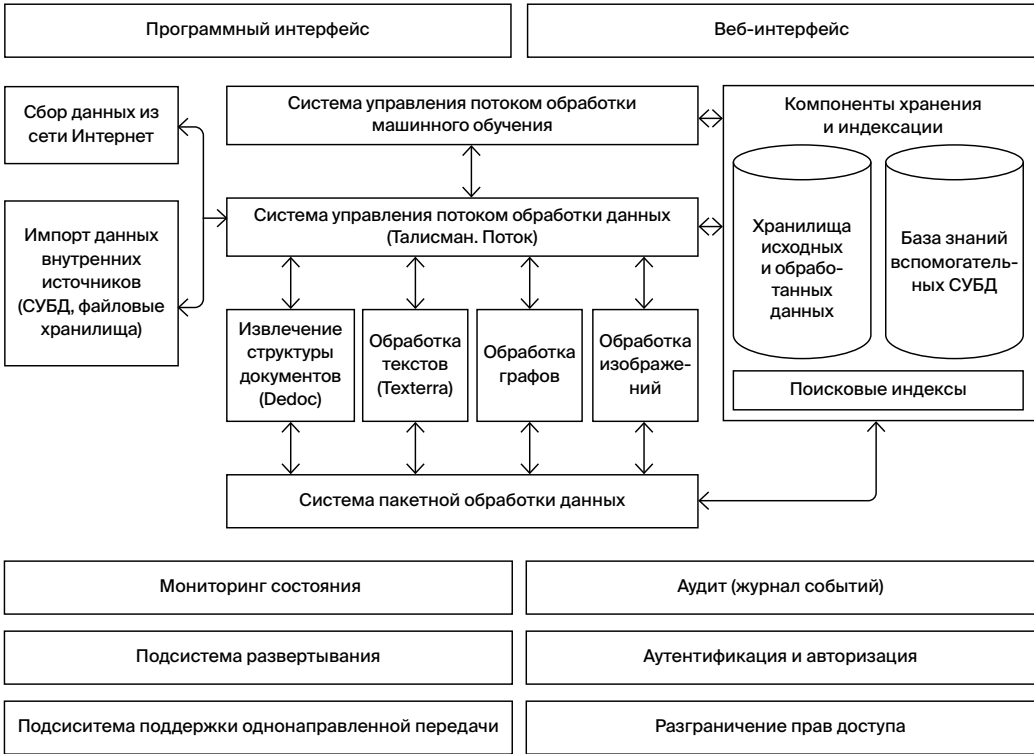
- Talisman позволяет создавать аналитические системы для решения широкого круга прикладных задач. Примеры применения:
- Автоматизация построения базы знаний по интересующей предметной области и обеспечение постоянного мониторинга новой информации об объектах интереса (аналог Palantir Gotham).
 - Проведение конкурентной разведки по открытым данным (OSINT) с целью поиска сведений по объектам интереса (аналог Maltego).
 - Мониторинг СМИ с целью решения аналитических задач (аналог LexisNexis).
 - Оптимизация управления персоналом: эффективный подбор сотрудников, верификация анкетных данных, вы-

- явление некорректного поведения в открытом информационном пространстве (система «Talisman.Биография», №5547 в Едином реестре российского ПО).
- Выявление информационных кампаний, манипулирующих мнением целевой аудитории, а также определение целевой аудитории, на которую направлена кампания.
 - Выявление и анализ особенностей инфраструктуры распространения информации (ресурсы, пользователи, боты), а также анализ типичных ролей членов сообществ в коммуникации (первоисточник, лидер мнения, распространитель, модератор, бот, комментатор).
 - Управление деловой репутацией людей и организаций: мониторинг релевантных сообщений, выявление проблем, вызывающих недовольство, мониторинг утечек и разглашения внутренней информации.
 - Объективная оценка эффективности деятельности, а также тестирование стратегий на целевой аудитории в целях получения обратной связи.
 - Управление точками социального напряжения; обнаружение и своевременное предупреждение эскалации конфликтов.

ПОДДЕРЖИВАЕМЫЕ ЯЗЫКИ

Talisman использует современные искусственные нейронные сети для анализа данных. Используемые инструменты позволяют извлекать информацию более чем из 100 естественных языков.

СХЕМА РАБОТЫ



ПЛАТФОРМА ДОВЕРЕННОГО ИСКУССТВЕННОГО ИНТЕЛЛЕКТА (ДИИ)



Платформа ДИИ — облачная платформа для разработки доверенных систем искусственного интеллекта. Обеспечивает автоматизацию процессов по выявлению и устранению угроз, возникающих на всех этапах жизненного цикла разработки моделей машинного обучения.

ИНФРАСТРУКТУРА

- MLOps ядро платформы;
- инструменты тестирования уязвимости к атакам, защит, интерпретации;
- репозиторий доверенных фреймворков;
- среда анализа безопасности фреймворков;
- бенчмарки для проведения экспериментов.

Платформа ДИИ — это:

- Набор инструментов обеспечения доверия, расширяющийся с появлением новых передовых техник в научной литературе. В набор входят:
 - инструменты проверки уязвимости моделей к распространенным типам атак;
 - инструменты обучения априорно устойчивых и интерпретируемых моделей;
 - инструменты повышения устойчивости моделей к распространенным типам атак;
 - инструменты интерпретации работы моделей.
- API и SDK для встраивания процессов по обеспечению доверия в существующие инструменты разработки.
- Отчуждаемость. Платформа может быть развернута на площадке заказчика — как на существующем оборудовании, так и в составе программно-аппаратного комплекса;
- Гибкая модульная архитектура, позволяющая добавлять новые инструменты, специфичные для прикладных задач заказчика;
- Обновляемые доверенные версии распространенных библиотек и фреймворков машинного обучения (PyTorch, TensorFlow и др.);
- Инфраструктура, обеспечивающая методологию, позволяющую получать доверенные версии необходимых фреймворков и библиотек;
- Прозрачное решение типовых вызовов и проблем, возникающих при разработке моделей машинного об-

учения: версионирование моделей и данных, изоляция и планирование экспериментов, обеспечение воспроизводимости результатов;

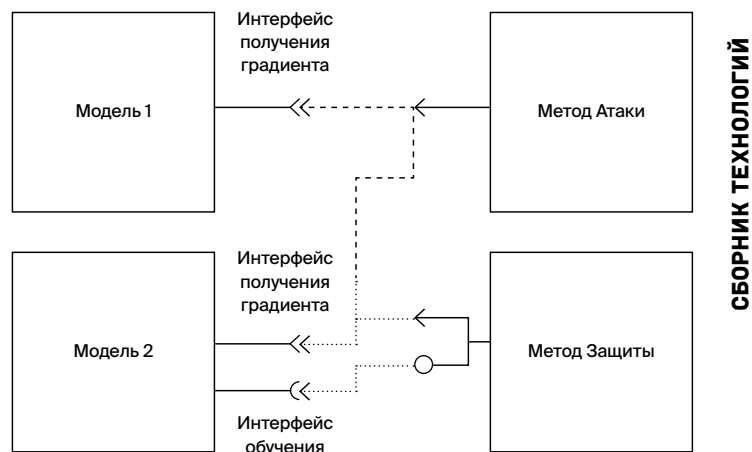
- Инструменты для решения проблемы устаревания моделей и борьбы с дрейфом данных в реальных системах, использующих технологии ИИ.

ДЛЯ КОГО ПРЕДНАЗНАЧЕНА ПЛАТФОРМА ДИИ?

Платформа предоставляет инструменты, полезные следующим группам разработчиков:

- ML-инженерам, решающим прикладные задачи ИИ в критических областях;
- ML-исследователям в области доверенного ИИ — для проведения экспериментов и быстрого внедрения передовых разработок в промышленные процессы;
- MLOps-специалистам для построения инфраструктуры и автоматизации процессов разработки решений, использующих технологии ИИ;
- Специалистам по информационной безопасности, нацеленных на высокий уровень надёжности — для формализации процессов обеспечения безопасности приложений на основе машинного обучения.

СХЕМА РАБОТЫ



COLBA: СИСТЕМА ПОДДЕРЖКИ СОЗДАНИЯ НАБОРОВ ДАННЫХ



Colba — система поддержки создания аннотированных наборов данных для машинного обучения с учителем. Позволяет организатору аннотирования гибко итеративно настраивать постановку задачи для экспертов-аннотаторов, автоматически оптимальным образом распределять задачи и отслеживать качество получаемых аннотаций.

ОСОБЕННОСТИ И ПРЕИМУЩЕСТВА

Colba — инновационная система, созданная с целью оптимизации процесса подготовки аннотированных наборов данных для сложных предметных областей, где проблематично использовать краудсорсинг. Colba захватывает весь процесс подготовки набора данных от выбора варианта постановки задачи до массового аннотирования.

Colba — это:

- Автоматическое распределение задач аннотирования по экспертам:
 - простое равномерное;
 - с учётом согласия;
 - с выявлением научных школ.
- Богатый набор доступных методов подсчета согласия между экспертами:
 - Cohen Kappa и Fleiss' kappa;
 - Krippendorff's alpha;
 - Precision, Recall, F1;
 - IoU.
- Итеративный процесс уточнения постановки задачи.
- Широкий выбор поддерживаемых видов постановки задачи и типов входных данных:
 - бинарная классификация;
 - многоклассовая классификация;
 - многоклассовая многометочная классификация;
 - NERC;
 - сегментация изображений.
- Возможность сфокусированного отбора элементов данных для первоочередного аннотирования.
- Интеграция с привычными экспертам системами разметки.

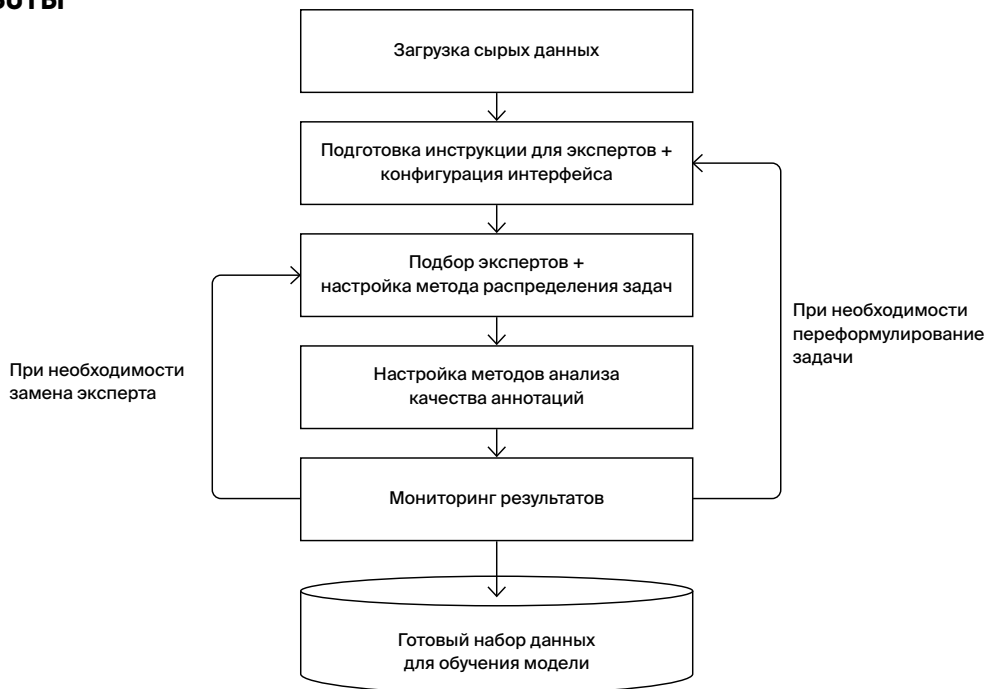
ДЛЯ КОГО ПРЕДНАЗНАЧЕНА COLBA?

- Специалисты по машинному обучению, которым нужны данные для решения прикладной задачи.

ОПЫТ ВНЕДРЕНИЯ

Colba входит в состав платформы НЦМУ для интеллектуального анализа медицинских данных (разрабатывается в ИСП РАН).

СХЕМА РАБОТЫ



LINGVODOC:

ВИРТУАЛЬНАЯ ЛАБОРАТОРИЯ ДЛЯ ДОКУМЕНТАЦИИ ИСЧЕЗАЮЩИХ ЯЗЫКОВ

GitHub →
[https://github.com/
ispras/lingvodoc](https://github.com/ispras/lingvodoc)



ОСОБЕННОСТИ И ПРЕИМУЩЕСТВА

Lingvodoc — система для совместной многопользовательской документации исчезающих языков, создания многослойных словарей и научной работы с полученными звуковыми и текстовыми данными. Совместный проект с Институтом языкознания РАН и Томским государственным университетом. Разрабатывается с 2012 года. Сайт — lingvodoc.ispras.ru.

Lingvodoc — кроссплатформенная система с открытым исходным кодом (<https://github.com/ispras/lingvodoc> и <https://github.com/ispras/lingvodoc-react>), основанная на научных исследованиях.

Lingvodoc — это:

- Совместная работа пользователей над пополнением словарных данных (в отличие от аналогичного проекта Starling, где такая работа не предусмотрена).
- Сохранение полной истории действий пользователей.
- Одновременная работа с аудиотекстовыми корпусами и словарями на основе интеграции с программой ELAN, разработанной Институтом психолингвистики Макса Планка (Нидерланды).
- Расставление однонаправленных и двунаправленных связей между лексическими входами внутри словарей, а также между словарями.
- Запись, проигрывание и хранение звуков с разметкой (в форматах WAV, MP3 и FLAC), а также построение формант гласных с последующей визуализацией.
- Продвинутый поиск, который позволяет искать данные в словарях по множеству параметров (в отличие от аналогичного проекта TypeCraft).
- Возможность поиска данных на карте с автоматическим построением изоглосс.
- Возможность бесконфликтной двусторонней отложенной синхронизации.

- Повышенный уровень автоматизации (по сравнению с аналогичным проектом Kielipankki): возможность проводить автоматический этимологический и фонетический анализ.
- Создание словарей любой структуры, как типичных двуслойных (слой лексических входов и слой парадигм), так и многослойных. Кроме того, существует функция импорта для готовых словарных структур.
- Наличие программ, воспроизводящих работу ученых по фонетическому и этимологическому анализу.
- Возможность уточнения классификации языков и диалектов с построениями графиков в форматах 2D и 3D по глоттохронологии, морфологии, этимологико-фонетическим признакам.
- Возможность размещения корпусов текстов в формате Word и словарей в формате Excel.
- Интерфейс, позволяющий настроить автоматическую работу с параллельными корпусами.
- Встроенные морфологические анализаторы для языков народов России в формате Aperitum.
- Удобный интерфейс для ручного снятия омонимии после работы морфологического анализатора.
- Работа как с привлечением облачных ресурсов ИСП РАН, так и с развёртыванием локальной версии с изоляцией собственных данных.
- Наличие программы для веб-просмотра и десктопной версии.
- Открытая регистрация (с подтверждением).
- Оперативная доработка технологии с расширением набора функций, а также адаптация под другую научную отрасль.

На основе глоссированных корпусов Lingvodoc и программ анализа создана драфтовая версия обучающей платформы edu.ispras.ru, объединяющая 10 000 заданий на 9 языках. Платформа предоставляет возможность:

- создавать упражнения на языках России для любого возраста и уровня владения (любой учитель может создавать свои упражнения, и ему не придётся самому их проверять);
- выполнять упражнения как на родном языке, так и на иностранном, причём каждому ученику программа может подбирать задания индивидуально в зависимости от его ошибок.

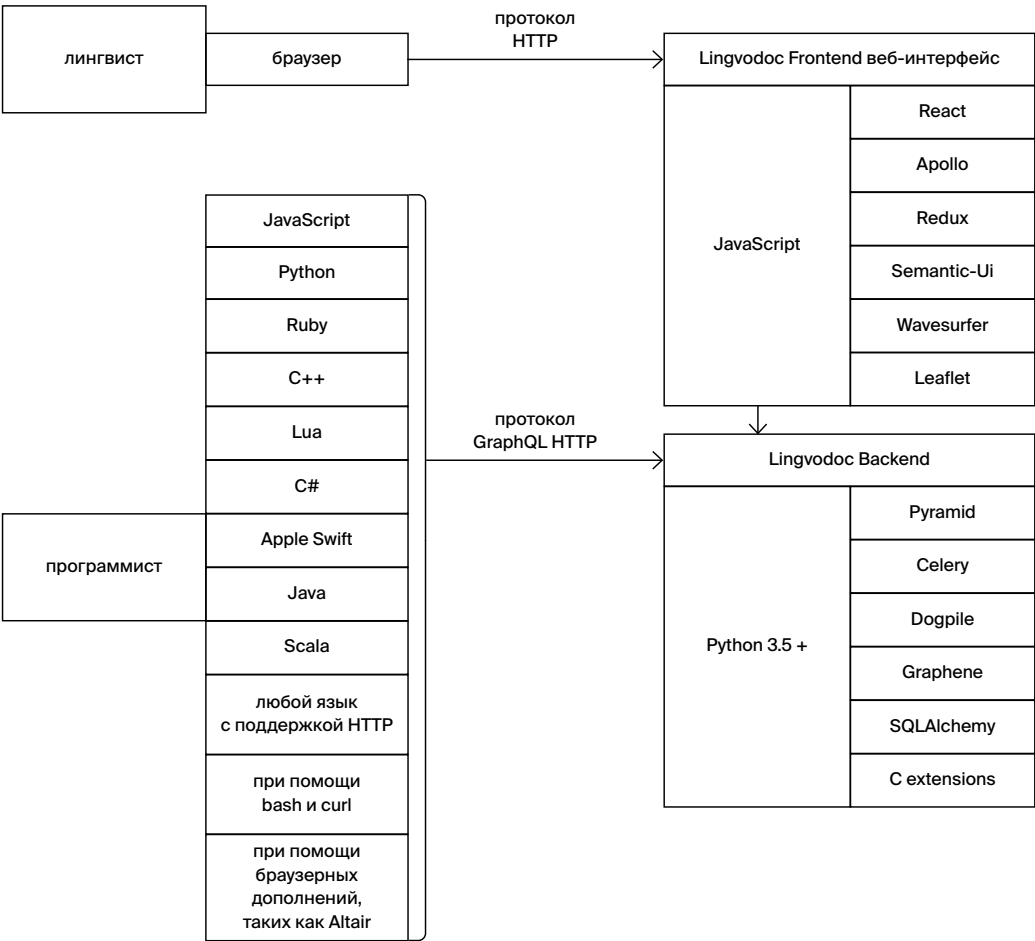
Запущена нейросеть, которая ищет родственные слова в языках. Тесты показывают результаты, которые превосходят те, что были получены ранее с помощью использования статистических программ, и скорость значительно превышает работу исследователя.

ДЛЯ КОГО ПРЕДНАЗНАЧЕН LINGVODOC?

В первую очередь Lingvodoc разработан для лингвистов, ведущих научную работу в сфере документации языков народов России. Однако возможна доработка технологии под другие цели.

Основной функционал Lingvodoc используется филологами из 29 вузов и НИИ из 16 городов. В числе научно-образовательных организаций: Томский государственный университет, Институт филологии СО РАН, Институт истории, языка и литературы Уфимского научного центра РАН, Удмуртский федеральный исследовательский центр УрО РАН, Северо-Восточный федеральный университет, Югорский государственный университет, Институт языка, литературы и истории КарНЦ РАН, Мурманский арктический государственный университет. Специалисты, использующие платформу, готовы к проведению мастер-классов для своих коллег. В 2023 г. четыре потока учёных из нескольких городов России прошли курсы дополнительного образования по направлению «Использование возможностей платформы Lingvodoc в работе лингвистов» (в том числе в Башкирском государственном университете и в РУДН).

СХЕМА РАБОТЫ



DEDOC: СИСТЕМА ИЗВЛЕЧЕНИЯ СОДЕРЖИМОГО И СТРУКТУРЫ ТЕКСТОВЫХ ДОКУМЕНТОВ



Dedoc — универсальная открытая библиотека для приведения документов к единому выходному формату. Автоматически извлекает содержимое, иерархическую структуру, таблицы, форматирование и метainформацию. Содержимое документов представляется в виде дерева, кодирующего заголовки и списки различного уровня вложенности. Dedoc может встраиваться как отдельный компонент в системы анализа структуры и содержимого документов.

ОСОБЕННОСТИ И ПРЕИМУЩЕСТВА

Dedoc реализован на языке Python. Работает со слабо-структурированными форматами данных (DOC*, ODT, XLS/XLSX, CSV, TXT, JSON) и с неструктурированными форматами изображений (PNG, JPG и др.), архивами (ZIP, RAR и др.), PDF, HTML. Извлечение структуры документа проводится в полностью автоматическом режиме вне зависимости от типа входных данных, с извлечением метainформации и разного вида форматирования текста.

Dedoc — это:

- Python-библиотека с открытым исходным кодом (<https://github.com/ispras/dedoc>).
- Расширяемость за счёт гибкого добавления поддержки новых форматов документов и простоты изменения выходного формата данных.
- Поддержка извлечения структуры вложенных документов различных форматов.
- Извлечение разного вида форматирования текста (отступы, шрифты, жирность, размер шрифта и др.).
- Работа с документами различной предметной области (технические задания, нормативно-правовые акты, научные отчёты и статьи) и возможность добавления обработки документов новой предметной области.
- Работа с PDF-документами, содержащими текстовый слой:
 - поддержка автоматического определения корректности текстового слоя.

- Извлечение содержимого и форматирования из PDF-документов с текстовым слоем с помощью разработанного интерпретатора виртуальной стековой машины вывода на печать графики согласно спецификации формата.
- Извлечение табличной информации из DOC*, PDF-документов, HTML, форматов изображений, CSV:
 - распознавание физической структуры и текста ячеек сложных многостраничных таблиц с границами на изображениях с помощью методов контурного анализа.
- Работа со сканированными черно-белыми документами (формата PDF без текстового слоя и с форматами изображений):
 - работа с активно развивающимся движком оптического распознавания символов OCR Tesseract компании Google в совокупности с использованием методов предварительной обработки изображений;
 - использование современных методов машинного обучения для определения ориентации документов, определения одно/многоколоночных документов, полужирного текста и извлечения иерархической структуры на основе классификации строк извлечённых признаков из изображений документов;
 - автоматическая обработка PDF-документов с некорректным текстовым слоем;
 - возможность обработки сканированных документов с подложкой.

ДЛЯ КОГО ПРЕДНАЗНАЧЕНА СИСТЕМА DEDOS?

- Разработчики прикладных систем анализа содержимого электронных документов и документооборота.
- Разработчики интеллектуального анализа текста документов.
- Разработчики систем автоматической обработки текстов.

ПОДДЕРЖИВАЕМЫЕ ЯЗЫКИ

Русский и английский.

СХЕМА РАБОТЫ



DOCMARKING: ПРОТИВОДЕЙСТВИЕ АНОНИМНОСТИ ПРИ УТЕЧКАХ ДОКУМЕНТОВ



DocMarking — уникальная система внедрения цифровых водяных знаков (меток) в текстовые документы. Позволяет создавать едва отличимые от оригинала цифровые и физические копии документов, однозначно идентифицирующие пользователей и их устройства.

ОСОБЕННОСТИ И ПРЕИМУЩЕСТВА

DocMarking базируется на результатах исследований в областях стеганографии, цифровой обработки изображений и машинного обучения. В основе системы маркирования лежат методы поиска и классификации текста на изображениях, используются статистические особенности изображений документов.

По сравнению с аналогичными технологиями DocMarking обладает рядом преимуществ. При извлечении цифровой метки не требуется оригинал документа. Поддерживается повторное маркирование сканированных документов, при этом ранее встроенная цифровая метка стирается.

DocMarking — это:

- Алгоритмы маркирования на основе технологий машинного обучения.
- Поддержка документов любых форматов.
- Работа во всех приложениях.
- Защита документов при отображении на экране монитора и при печати.
- Извлечение цифровых меток в условиях отсутствия оригинальных немаркированных документов.
- Возможность автономной работы на стороне клиента.

ДЛЯ КОГО ПРЕДНАЗНАЧЕНА СИСТЕМА DOCMARKING?

- Государственные и коммерческие учреждения.
- Компании, заинтересованные в соблюдении сотрудниками протокола работы с конфиденциальными документами.

ПОДДЕРЖИВАЕМЫЕ ОС

Windows (32-bit, 64-bit), Linux (64-bit), в том числе Astra Linux SE 1.6/1.7.

СЕРТИФИКАТЫ

- Сертификат №4878 ФСТЭК России – соответствие требованиям доверия (уровень 4) и техническим условиям.
- Регистрация в Реестре российского ПО (№23882).

СХЕМА РАБОТЫ



ECGHub: ИНТЕЛЛЕКТУАЛЬНЫЙ АНАЛИЗ ЦИФРОВЫХ ЭКГ



EcGHub — система разметки 12-канальных ЭКГ и нейросетевые модели классификации патологий. Система позволяет предсказывать наличие или отсутствие ряда патологий, а также выполнять и верифицировать синдромальную разметку ЭКГ на основе специализированного опросника, обеспечивая подготовку качественного набора данных для дальнейшего развития нейросетевых моделей.

ОСОБЕННОСТИ И ПРЕИМУЩЕСТВА

EcGHub базируется на результатах исследований в областях цифровой обработки сигналов и алгоритмов машинного обучения. В основе системы классификации патологий лежат глубокие нейронные сети. Верифицированный экспертами подход обеспечивает получение врачами согласованной разметки ЭКГ для обучения и развития предсказательных моделей скрининга, диагностики сердечно-сосудистых заболеваний.

EcGHub — это:

- Глубокие нейронные сети предсказания патологий для цифровых ЭКГ.
- Непрерывное развитие и доработка нейросетевых моделей, в том числе тонкая настройка для сравнительно небольших наборов данных медицинских учреждений.
- Адаптация обученных нейросетевых моделей для классификации патологий одноканальных ЭКГ (кардиокресло, умные часы), шестиканальных ЭКГ (могут регистрироваться самостоятельно без помощи врача), а также суточных ЭКГ (холтеры).
- Система согласованной синдромальной разметки, позволяющая получать качественные данные для обучения предсказательных моделей.
- Интеграция нейросетевых моделей в цифровой контур заказчика или удаленный доступ к сервису в контуре ИСП РАН.
- Возможность применения системы разметки в процессе обучения современных специалистов функциональной диагностики.
- Развитие автоматизированной системы скрининга населения.
- Зарегистрированное медицинское изделие (№ РЗН 2024/24366) с элементами ИИ (3 класс риска).

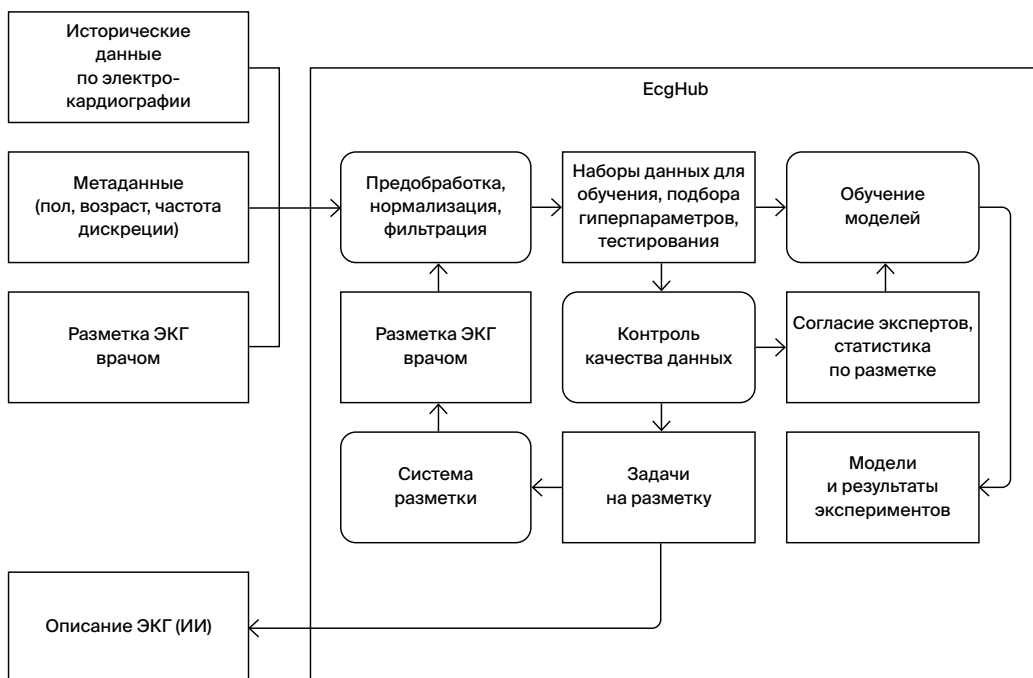
ДЛЯ КОГО ПРЕДНАЗНАЧЕНА СИСТЕМА ECGHUB?

- Медицинские учреждения (результат работы нейросетевых моделей может использоваться в качестве второго мнения).
- Образовательные учреждения (верифицированные наборы данных позволяют оценивать качество работы студентов или начинающих врачей соответствующих специализаций).
- Разработчики устройств и приложений (автономная ЭКГ-диагностика).

ОПЫТ ВНЕДРЕНИЯ

- Нейросетевые модели классификации 12-канальных ЭКГ обучены на данных из нескольких регионов (Республика Татарстан, Москва, Великий Новгород), в том числе данных Скорой помощи Москвы, а также открытых данных.
- Система апробирована в России (Республика Татарстан, Москва, Великий Новгород) и Армении (Ереван).

СХЕМА РАБОТЫ



3

ПРОЧИЕ ТЕХНОЛОГИИ

- 115 VALIDBIM: сервис верификации информационных моделей в архитектуре и строительстве
- 118 DigiTEF: программный комплекс для проведения компьютерного моделирования

VALIDBIM: ТЕХНОЛОГИЯ ИНФОРМАЦИОННОГО МОДЕЛИРОВАНИЯ ДЛЯ УПРАВЛЕНИЯ ТРЕБОВАНИЯМИ В СТРОИТЕЛЬСТВЕ



VALIDBIM — технология, предназначенная для поддержки процессов проектирования, сооружения и эксплуатации в гражданском, промышленном и инфраструктурном строительстве на основе цифровых информационных моделей (ЦИМ). Технология реализует единую концепцию управления требованиями, начиная от анализа нормативной базы и создания цифровых реестров требований на основе машинно-интерпретируемого формата до проверок ЦИМ и визуального анализа выявленных замечаний. Технология составляет основу разработанной Национальной ТИМ платформы, которая предоставляет свободные web-сервисы для решения перечисленных задач российскими проектными организациями и компаниями, экспертными и контролирующими органами, университетами строительного профиля.

ОСОБЕННОСТИ И ПРЕИМУЩЕСТВА

VALIDBIM представляет собой единый стек математических методов, программных компонентов и приложений для решения широкого круга задач управления требованиями на протяжении жизненного цикла объектов капитального строительства. Благодаря поддержке открытых международных информационных стандартов по интероперабельности OpenBIM, включающих IFC (Industry Foundation Classes), IDS (Information Delivery Specification), BCF (BIM Collaboration Format), технология обеспечивает работу с ЦИМ, реестрами требований и журналами замечаний, подготовленными в сторонних системах. Вместе с тем, технология предусматривает формальную спецификацию, математически строгую и полную проверку сложных пространственных, темпоральных, параметрических, геометрических требований, определяемых существующими нормативными документами и сводами правил. Применение технологии в составе Национальной ТИМ платформы способствует повыше-

нию качества проектной документации, представленной в виде ЦИМ, автоматизации и интеллектуализации проведения проверок органами экспертизы и контроля в строительной отрасли.

ФУНКЦИОНАЛЬНЫЕ ВОЗМОЖНОСТИ ТЕХНОЛОГИИ

- Формальная верификация ЦИМ в строительстве на соответствие международным и национальным стандартам IFC (ISO 16739; ГОСТ Р 10.0.02: 2019) и SPF (STEP Physical File – ISO 10303-21; ГОСТ Р ИСО 10303-21: 2002, 2022):
 - Проверка синтаксиса и ссылочной целостности файловых данных модели.
 - Полная и математически строгая проверка семантики данных модели на основе формальной схемы, специфицированной на языке объектно-ориентированного моделирования EXPRESS.
 - Верификация программного обеспечения, для которого декларируется техническая, синтаксическая и семантическая интероперабельность на уровне BIM Level3.
 - Поддержка актуальных версий стандарта IFC, включая IFC 2x3, IFC 4 и IFC 4.3.
 - Журнализация выявленных ошибок и генерация отчета в формате HTML с гиперссылками на разделы стандарта, в которых определены нарушенные правила.
- Просмотр, редактирование, добавление, удаление спецификаций требований, поддерживаемых стандартом IDS:
 - Загрузка файла в формате IDS и проверка на соответствие стандарту.
 - Развитая контекстная помощь для корректного создания спецификаций требований (предусматривается выбор названий типов данных, определенных схемой IFC, а также предопределенных типов элементов, материалов и атрибутов из предлагаемого списка или иерархии).
 - Валидация (проверка корректности) и выгрузка спецификаций требований в виде файла в формате IDS.
 - Полнофункциональная поддержка актуальной версии стандарта IDS 1.0.
- Проверка ЦИМ в формате IFC на соответствие требованиям, представленным в формате IDS с генерацией отчетов в форматах HTML и BCF для дальнейшего анализа.
- Управления замечаниями, представленными в соответствии с открытым стандартом BCF, в проектах гражданского, промышленного и инфраструктурного строительства на всех этапах жизненного цикла:
 - Загрузка и выгрузка журналов замечаний в формате BCF.
 - Поиск, просмотр и редактирование замечаний.
 - Поддержка актуальной версии стандарта BCF 3.0.
 - Загрузка ЦИМ в формате IFC.
 - Управление версиями моделей.
 - 3D-визуализация с интерактивными возможностями навигации по модели, просмотра с заданных ракурсов, отсечений по главным плоскостям, фильтрации по типам элементов, измерения расстояний, локализации замечаний.

ДЛЯ КОГО ПРЕДНАЗНАЧЕНА VALIDBIM?

- Государственные ведомства: создание единого реестра цифровых требований и ведение их версионности.
- Заказчики: возможность создания собственных цифровых требований и их повторного использования.
- Исполнители: проведение внутренних проверок качества и полноты ЦИМ, возможность работы с ними с использованием продуктов от разных производителей, возможность настройки САПР под цифровые требования.
- Органы экспертизы: единая логика требований от разных заказчиков и независимость от ПО.
- Разработчик ПО для ТИМ: следование единым открытым стандартам в существующих и перспективных программных продуктах, создание функционала автоматической верификации ЦИМ.

ОПЫТ ВНЕДРЕНИЯ

Технология составляет основу разработанной Национальной ТИМ платформы, которая предоставляет свободные web-сервисы верификации и валидации цифровых информационных моделей, подготовки спецификаций требований и управления замечаниями. Платформа доступна на сайте <https://bim.ispras.ru> и в настоящее время активно используется российскими проектными организациями и компаниями, экспертными и контролирующими органами, университетами строительного профиля. Имеются свидетельства о государственной регистрации программ для ЭВМ: № 2023667675, № 2024669861, № 2025668968.

DIGITEF: ПРОГРАММНЫЙ КОМПЛЕКС ДЛЯ ПРОВЕДЕНИЯ КОМПЬЮТЕРНОГО МОДЕЛИРОВАНИЯ



DigiTEF — программный комплекс, предназначенный для разработки средств цифрового моделирования, для проведения компьютерного моделирования и инженерного анализа прикладных и научно-технических задач промышленности. Позволяет решать задачи газовой динамики, аэродинамики, гидродинамики, акустики, а также проводить сопряжённые расчеты. Включён в Единый реестр российского ПО (№5377).

ОСОБЕННОСТИ И ПРЕИМУЩЕСТВА

DigiTEF разрабатывается на базе программ с открытым исходным кодом, а также уникальных модулей и библиотек ИСП РАН. Использование собственных разработок позволяет получать для отдельного класса задач решения, точность и достоверность которых превышает уровень мировых аналогов. Сравнительные исследования производительности и точности ядра DigiTEF с ANSYS Fluent и Star CCM+ показали сопоставимые (а в некоторых случаях и более низкие) вычислительные затраты при одинаковой точности.

DigiTEF — это:

- открытый исходный код (позволяет повысить сохранность данных, контролировать и адаптировать реализованные алгоритмы под конкретные задачи);
- понятный графический интерфейс, который при необходимости может быть адаптирован под конкретное предприятие и решаемые задачи;
- отсутствие ограничений на количество пользователей, ячеек расчётной сетки и используемых ядер, что позволяет снизить экономические затраты на вычисления и дальнейшее использование;
- использование современных моделей и алгоритмов за счет синхронизации технологического уровня с международным сообществом;

- наличие средств автоматизации вычислений и интеграции моделей для комплексного исследования технических объектов;
- возможность разработки дополнительных компонентов в соответствии с конкретными требованиями;
- возможность использования высокопроизводительных систем вычислений (суперкомпьютеров и кластеров) для ускорения вычислений.

ДЛЯ КОГО ПРЕДНАЗНАЧЕН DIGITEF?

DigiTEF предназначен для применения в компаниях и на предприятиях ресурсоёмких отраслей промышленности. Использование DigiTEF позволяет повысить эффективность проектирования и рентабельность производства, снизить стоимость и сложность при реализации промышленных проектов.

ОПЫТ ВНЕДРЕНИЯ

DigiTEF используется в ряде проектов в области ветроэнергетики, космонавтики, авиации, кораблестроения, металлургии, а также в нефтегазовой отрасли. Открытые версии модулей DigiTEF успешно применяются в академических, образовательных и промышленных учреждениях мира: Institut Pprime (Франция), Korea Atomic Energy Research Institute (Корея), Universität der Bundeswehr München (Германия), Northwestern Polytechnical University (КНР), Ocean University of China (КНР), Embry-Riddle University (США), California Institute of Technology (США) и др.

СИСТЕМНЫЕ ТРЕБОВАНИЯ

Поддержка ОС семейства Linux (в том числе Astra Linux), а также Microsoft Windows 10. Не менее четырёх процессорных ядер x86-64, 16 ГБ оперативной памяти и 100 ГБ свободного места на диске. DigiTEF также поддерживает параллельные вычисления. Проверенное количество вычислительных ядер — до 1536.

Институт системного программирования
им. В.П. Иванникова Российской академии наук

109004, Москва, улица А. Солженицына, дом 25.
По всем вопросам: scsec@ispras.ru