РЕЦЕНЗИЯ

на заявку Федерального государственного бюджетного учреждения науки Института системного программирования им. В.П.Иванникова Российской академии наук (ИСП РАН)
на разработку комплексного научно-технического проекта полного инновационного цикла «Инструментальная платформа выявления уязвимостей и дефектов в программно-аппаратных решениях на всех этапах жизненного цикла»

Представленная заявка предлагает развернуть комплексный проект по разработке новых средств инструментальной платформы выявления уязвимостей и дефектов в программно-аппаратных решениях на всех этапах жизненного цикла. Кроме того, предлагается развернуть мероприятия по обучению кадров и созданию условий для широкого использования новых технологий при создании программных систем критичных с точки зрения информационной безопасности.

Из перечня угроз, которые перечислены в описании данного приоритетного направления научно-технического развития России, самыми близкими по теме являются угрозы терроризма и киберугрозы для общества экономики и государства. Косвенно угрозы кибербезопасности связаны со всеми видами угроз от нарушения информационной безопасности, в частности, это может быть потеря технологического суверенитета страны в целом. Цель комплексного научно-технического проекта в целом и его отдельных направлений (развитие технологий и инструментов, подготовка кадров в области кибербезопасности, внедрение новых технологий в практику) являются важными и актуальными для Российской Федерации особенно в свете сложного международного положения в настоящее время.

Перечень задач, которые предлагается решить в рамках данного проекта, представляет собой комплекс мероприятий, являющихся важными, своевременными, реализуемыми и обещающими дать значительный эффект в плане укрепления информационной безопасности, технологической независимости и повышения технологической культуры ИТ-индустрии в стране в целом. Особенно следует отметить комплексность предложенного подхода. В рамках проекта предлагается решать не только научные и инженерные задачи создания и развития технологий, но и задачи образования и внедрения новых технологий.

Цели и задачи проекта полностью отвечают требованиям директивных документов ОГВ, а также учитывает большие вызовы для общества, государства и науки, указанные в Стратегии научно-технологического развития Российской Федерации, утвержденной Указом Президента Российской Федерации от 1 декабря 2016 г. №642 «О Стратегии научно-технологического развития Российской Федерации» и Указ Президента Российской Федерации от 21 июля 2020 г. №474 «О национальных целях развития Российской Федерации на период до 2030 года».

Задачи проекта включают формирование научно-технического задела, разработку новых технологий и создание наукоемкой конкурентоспособной продукции, а их решение направлено на создание условий для проведения исследований и разработок, соответствующих современным принципам организации научной, научно-технической, инновационной деятельности и лучшим российским и мировым практикам.

Решение задач будет содержать научную и (или) научно-техническую новизну технологий, продуктов и услуг, в том числе на фоне зарубежных разработок, и демонстрировать роли науки и технологий как основополагающих элементов решения многих национальных и глобальных проблем. Результаты решения задач (программные инструменты и услуги) будут востребованы в экономике России, так как рынок средств защиты информации постоянно расширяется.

Цели и задачи проекта отвечают всем основным критериям оценки для заявок на тему КНТП:

- проект нацелен на реализацию важной комплексной задачи по данному приоритету научно-технологического развития Российской Федерации;

- проект ставит масштабную и научно значимую комплексную задачу, в том числе для развития перспективных технологий и создания наукоемкой продукции в различных отраслях и секторах экономики Российской Федерации;

- важнейшим следствием реализации проекта будет улучшение ситуации в направлении подготовки кадров для различных отраслей и секторов экономики;

- реализация проект будет иметь мультипликативный (синергетический) эффект от использования технологий, создаваемых в результате решения комплексных задач, входящих в состав комплексных научно-технических задач как минимум за счет повышения технологической культуры в компаниях-разработчиках программного обеспечения для государственных нужд;

- возможно увеличение объема экспорта наукоемкой продукции, полученной по результатам решения задач, если на уровне правительств будут заключены соответствующие соглашения в рамках стран ОДКБ и БРИКС;

- значимость решения комплексных задач, входящих в состав комплексных научно-технических задач для обеспечения национальной безопасности Российской Федерации и борьбы с терроризмом велика в силу важности обеспечения информационной безопасности, особенно для критической информационной инфраструктуры страны;

- обеспечение импортонезависимости Российской Федерации как результат решения задач КНТП.

В заявке представлен подробный аннотированный список технологий и инструментов анализа, верификации и разработки доверенного программного обеспечения. Работы разбиты на этапы, отдельно выделены фазы по фундаментальным и экспериментальным разработкам. Хорошо увязаны между собой работы по созданию и развитию технологий и работы по обучению кадров по новой специальности «кибербезопасность». Организационная работа по налаживанию сотрудничества с университетами позволит на их базе проводить не только учебные занятия, но и вести научно-инженерные разработки.

Важнейшими заказчиками КНТП являются: Министерство промышленности и торговли Российской Федерации, Министерство науки и высшего образования Российской Федерации, Минэнерго, Министерство экономического развития Российской Федерации, Министерство цифрового развития, связи и массовых коммуникаций Российской Федерации, ГК «Ростех», ГК «Роскосмос», ГК «Росатом», ГК «Роснано». На более детальном уровне заказчиками являются компании-партнеры ИСП РАН, которые уже

сейчас используют инструменты кибербезопасности. Таких предприятий более сотни, по этой причине можно заключить, что потенциальных заказчиков много, и рынок средств кибербезопасности будет стабильно растущим весьма долго. В настоящее время объем рынка уже значительно больше тех цифр, которые упомянуты в заявке.

Рынок доверенного программного обеспечения растет как в нашей стране, так и за рубежом – это общая тенденция, которая связана со все большим распространением цифровизации, внедрении цифровых технологий во все сферы жизни. Показано, что рынок уже измеряется миллиардами рублей, гарантирован рост этого рынка на долгую перспективу. Предлагаемые технологии и инструменты будут востребованы в этом сегменте рынка, так как они одновременно и существенно упрощают подготовку к сертификации и позволяют поднять качество и надежность средств защиты информации.

У ИСП РАН имеется все необходимое оборудование и другие ресурсы, которые могут понадобиться в ходе выполнения проекта.

ИСП РАН обладает всеми необходимыми ресурсами. Институт обладает хорошей материальной базой, высококвалифицированными кадрами, имеется уникальный задел в форме научных публикаций, инструментов и технологий, разработанных в ИСП РАН, защищенных объектов интеллектуальной собственности. Все необходимые ресурсы для выполнения проекта есть.

В заявке в качестве соисполнителей указано более 10 университетов, включая: МГУ им. М.В. Ломоносова, МФТИ, НИУ ВШЭ, НИУ МЭИ, МГТУ им. Н.Э. Баумана, РТУ МИРЭА, НИЯУ МИФИ, РЭУ им. Г.В. Плеханова, а также индустриальные партнеры: АО РусБИТех (AstraLinux), АО «Лаборатория Касперского», АО «НПО «Базальт». Со всеми этими организациями у института многолетние связи, по этой причине можно рассчитывать на то, что партнерство, включая софинансирование этого проекта, организовать удастся.

По итогам рассмотрения материалов заявки ИСП РАН считаю, что заявка на разработку комплексного научно-технического проекта полного инновационного цикла «Инструментальная платформа выявления уязвимостей и дефектов в программно-аппаратных решениях на всех этапах жизненного цикла» заслуживает поддержки и самой высокой оценки.

Рецензент,
главный научный сотрудник
ИПМ им.М.В.Келдыша РАН,

д.ф.-м.н., проф. В.А.Галактионов

Рецензия на заявку на разработку КНТП

«Инструментальная платформа выявления уязвимостей и дефектов в программно-аппаратных решениях на всех этапах жизненного цикла».

Представленная заявка полностью соответствует действующим нормативно-правовым актам, определяющим форму заявки.

Предложенный проект направлен на достижение следующих целей:

готовых решений, на основе которых предприятия ИТ отрасли смогут строить свои защищенные решения (доверенные ядра операционных систем, доверенные библиотеки, доверенная инфраструктура облачных вычислений и др.);

технологий и инструментов моделирования и анализа требований безопасности, анализа проектов аппаратуры, исходного и бинарного кода программ для выявления и минимизации рисков эксплуатации уязвимостей, адаптированных к требованиям современных и перспективных государственных регламентов разработки, верификации и сертификации программных средств критичных в плане кибербезопасности.

Цели проекта соответствует приоритетным направлениям научно-технологического развития Российской Федерации в части противодействия техногенным и биогенным источникам опасности для общества, экономики и государства, а также, в области перехода к передовым цифровым, интеллектуальным и производственным технологиям.

Задачами комплексного проекта являются:

- адаптация уже имеющихся технологий и инструментов к конкретным программно-аппаратным платформам и особенностям видов и классов программных систем критичных в плене кибербезопасности, что потребует усилий по внедрению и анализу обратной связи от потребителей созданных продуктов;

- подготовка квалифицированных кадров для разработки и сертификации доверенного программного обеспечения разработка образовательных программ в области кибербезопасности, построение партнерства с университетами и другими образовательными центрами;

- собственно научные исследования и разработки в области кибербезопасности - создание технологий и инструментальных средств, нацеленных на минимизацию угроз безопасности, связанных с ошибками в программно-аппаратном обеспечении.

Комплексные задачи, на решение которых направлены комплексный проект, и входящие в их состав научно-технические задачи полностью соответствуют требованиям и критериям, утвержденным постановлением правительства РФ от 09 октября 2021 года № 1715.

Обеспечение информационной безопасности становится сквозной технологией цифровой экономики и информационного общества. Вызовы, связанные с конфиденциальностью, целостностью, доступностью данных и защитой коммерческой тайны и частной жизни, возникают во всех областях информационных технологий. Данный КНТП предназначен найти системный ответ на возникающие вызовы и строить более надёжные и безопасные системы.

Особую значимость данная тема приобретает в свете задач обеспечения технологической независимости и технологического суверенитета России. В настоящее время многие программные технологии, нацеленные на выявление дефектов и потенциальных уязвимостей становятся недоступными отечественным программистам.

Информационная безопасность является неотъемлемым свойством программно-аппаратной системы. Требования информационной безопасности должны закладываться в архитектуру системы ещё на этапе проектирования, анализ и поиск ошибок должны осуществляться на протяжении всего цикла разработки. Так как современные системы, по большей части, создаются из повторно-используемых компонентов или библиотек, то безопасность системы в целом в значительной мере определяется безопасностью и надёжностью используемых компонентов.

Таким образом, актуальность предложенного проекта является бесспорной, от его реализации ожидается значимый социально-экономический эффект как в виде повышения информационной безопасности Российской Федерации, так и в виде создания новых рабочих мест и увеличения налоговых отчислений.

Рыночный потенциал планируемых результатов предложенного комплексного проекта является высоким.

У заявителя имеются следующие научные заделы и научно-технические результаты, которые могут быть использованы для достижения целей, предлагаемых к разработке комплексного проекта:

за последние пять лет выполнено более 70 научных и технологических проектов по тематике заявляемого исследования;

с 2017 по 2021 год сотрудниками заявителя получен 1 патент и более 100 свидетельств о регистрации программ для ЭВМ, в том числе по тематике заявляемого исследования более 90.

Заявитель полностью обеспечен высококвалифицированными кадрами: более 15 докторов наук (из них 1 академик РАН, и 1 профессор РАН, 7 имеют ученое звание профессор), более 30 кандидатов наук и более 400 программистов-исследователей и инженеров-программистов.

Заявленные цели проекта являются реалистичными. Уверенность в достижимости поставленных целей обусловлена наличием значимого задела, в том числе, уже готовых к внедрению доверенных компонентов программных систем и наличием квалифицированного коллектива исследователей и инженеров ИСП РАН. Важным факторами также являются опыт создания и функционирования центров компетенции, созданных на базе ИСП РАН при поддержке ФСТЭК России и большое число индустриальных партнеров института, которые используют технологии ИСП РАН и участвуют в их развитии и адаптации к нуждам реальных комплексов программ ответственного назначения.

План реализации предложенного комплексного проекта детально проработан, необходимость проведения заявленных НИР не вызывает сомнений, запрошенные финансовые ресурсы обоснованы.

В качестве соисполнителей проекта планируется привлечь ведущие российские организации в области информационных технологий, в том числе:

- ФГБОУ ВО «Московский государственный университет имени М.В. Ломоносова» (МГУ им. М.В. Ломоносова),
- ФГАОУ ВО «Московский физико-технический институт (государственный университет)» (МФТИ - Московский физико-технический институт),
- НИУ ВШЭ (Высшая школа экономики, факультет компьютерных наук),
- НИУ МЭИ (Московский энергетический университет),
- ФГБОУ ВО «Московский государственный технический университет им. Н. Э. Баумана» (МГТУ им. Н. Э. Баумана),
- ФГАОУ ВО «Национальный исследовательский университет «МИЭТ» (НИУ МИЭТ - Московский институт электронной техники),
- ФГБОУ ВПО «Московский государственный технический университет радиотехники, электроники и автоматики» (РТУ МИРЭА),
- НИЯУ МИФИ «Московский инженерно-физический институт»,
- Российский экономический университет им. Г.В. Плеханова,
- ФГБОУ ВО Новгородский государственный университет имени Ярослава Мудрого,
- Чувашский государственный университет им. И.И.Ульянова,
- ФГУ ФНЦ НИИСИ РАН (Научно-исследовательский институт системных исследований),
- Математический институт им. В.А.Стеклова РАН.

Потенциальными заказчиками проекта являются крупные компании сектора информационных технологий, такие как АО РусБИТех (AstraLinux), АО «Лаборатория Касперского», АО «НПО «Базальт».

Исходя из вышесказанного, предложенный проект рекомендуется поддержать.

К.т.н., заместитель директора
ИБХ РАН по научной работе,
Руководитель Центра
научно-технологической инициативы ИБХ РАН  Исаев А.И.

РЕЦЕНЗИЯ

на заявку Федерального государственного бюджетного учреждения науки Института системного программирования им. В.П.Иванникова Российской академии наук (ИСП РАН)
на разработку комплексного научно-технического проекта полного инновационного цикла «Инструментальная платформа выявления уязвимостей и дефектов в программно-аппаратных решениях на всех этапах жизненного цикла»

Заявка ИСП РАН выдвигает идею развития инструментальной платформы выявления уязвимостей и дефектов в программно-аппаратных решениях на всех этапах жизненного цикла, которая позволить повысить защищенность отечественных программных систем. Также в заявке предлагается инициировать работы по подготовке кадров по новой специальности «Кибербезопасность» и мероприятия по внедрению новых технологий в процессы разработки и сертификации ПО. Данные работы непосредственно связаны с реализацией целей приоритетного направления научно-технического развития России по преодолению угроз в области терроризма и нарушения информационной безопасности.

В заявке справедливо отмечается, что обеспечение информационной безопасности становится сквозной технологией цифровой экономики и информационного общества. Вызовы, связанные с конфиденциальностью, целостностью, доступностью данных и защитой коммерческой тайны и частной жизни, возникают во всех областях информационных технологий. Особую значимость данная тема приобретает в свете задач обеспечения технологической независимости и технологического суверенитета России. В настоящее время многие программные технологии, нацеленные на выявление дефектов и потенциальных уязвимостей, становятся недоступными отечественным программистам.

Такую сложную проблему можно решить только при помощи комплекса мероприятий, тщательно спланированных и проводящихся на систематической основе. Именно такой план предлагается в данной заявке. Научно-технический и технологический задел, которым обладает инициатор заявки, дают уверенность, что все цели проекта будут успешно достигнуты.

Задачи КНТП соответствуют следующим требованиям:

- они направлены на решение комплексных задач и входящих в состав комплексных задач научно-технических задач направлено на реализацию приоритетов научно-технологического развития Российской Федерации, а также учитывают большие вызовы для общества, государства и науки, указанные в Стратегии научно-технологического развития Российской Федерации, утвержденной Указом Президента Российской Федерации от 1 декабря 2016 г. № 642 "О Стратегии научно-

технологического развития Российской Федерации". Результаты КНТП будут способствовать достижению национальных целей развития Российской Федерации, определенных пунктом 1 Указа Президента Российской Федерации от 21 июля 2020 г. № 474 "О национальных целях развития Российской Федерации на период до 2030 года".

Задачи проекта нацелены на эффективное использование человеческого потенциала и разработку новых технологий и создание наукоемкой конкурентоспособной продукции, а их решение направлено на создание условий для проведения исследований и разработок, соответствующих современным принципам организации научной, научно-технической, инновационной деятельности и лучшим российским и мировым практикам.

Заявка тщательно проработана по составу работ и срокам. Предлагается привлекать к работе кадры из университетов и индустриальных партнеров. Оба пути доступны для Заявителя, так как ИСП РАН имеет многолетние связи в этих областях с известными образовательными и научно-техническими центрами. Представленный график работ хорошо структурирован, предусматривает различные фазы НИР и ОКР. Остались незабытыми фундаментальные исследования, работа по созданию и апробации новых образовательных программ, мероприятия по внедрению новых технологий. ИСП РАН имеет хорошую материальную базу, включая облачные хранилища данных, географические распределенные серверы для хранения данных. Риски, которые могли бы препятствовать успешному выполнению проанализированы, предусмотрены все необходимые мероприятия, чтобы минимизировать возможные потери.

Потенциальными заказчиками являются компании-разработчики ПО ответственного назначения, сертификационные лаборатории и образовательные центры. Среди этих компаний есть несколько весьма крупных структур, например, Ростех и Росатом, но наряду с такими гигантами есть и много предприятий разного размера, чей бизнес связан с разработкой и сертификацией доверенного ПО. К таким предпритиям относится, например, РусБИТех (Группа компаний «Astra Linux»), «Базальт СПО» и др. То есть индустриальных партнеров и потенциальных заказчиков и ИСП РАН в рамках данной инициативы достаточно много. Вероятно, имеет смысл объединить эти компании в консорциум, чтобы представлять общие интересы. Члены консорциума могут взять на себя часть работ по адаптации технологий и инструментов к нуждам конкретных программных систем или консолидировать средства выполнения задач проекта. Несмотря на то, что к заявке не приложены письменные согласия потенциальных заказчиков, можно быть уверенным, что следующих фазах подготовки проекта такие согласия появятся.

В ИСП РАН есть все необходимая материальная и научно-технической база. Кадровое обеспечение проекта и квалификация потенциальных участников высокие. Институт обеспечивает себя специалистами, которые выпускаются его базовыми кафедрами в МГУ, МФТИ и ВШЭ. Кроме того, институт активно сотрудничает и с

другими университетами страны. У института много научных и научно-технических результатов, подтверждающих квалификацию его сотрудников, включая патенты, зарегистрированные программы и научные публикации.

У ИСП РАН большой опыт кооперации как в сфере образования, так и в сфере индустриального партнерства. В заявке приводится внушительный список партнеров-университетов и партнеров-представителей бизнес-сообщества. Большая часть партнеров имеет долгосрочные договора сотрудничества в области технологий разработки доверенного ПО. На этом основании можно утверждать, что вопросы кооперации в рамках будущего проекта будут решены, включая и вопросы софинасирования.

Считаем, что заявка ИСП РАН на разработку комплексного научно-технического проекта полного инновационного цикла «Инструментальная платформа выявления уязвимостей и дефектов в программно-аппаратных решениях на всех этапах жизненного цикла» заслуживает самой высокой оценки.

Директор по развитию и стратегии Карпов Роман Дмитриевич

ООО «БЕЛЛСОФТ» 07.11.2022

Руководитель комитета по информационной

безопасности АРПП «Отечественный софт»

Руководитель технического комитета АНО «Открытый код»

Советник министра цифрового развития РФ по системному ПО

РЕЦЕНЗИЯ

на заявку Федерального государственного бюджетного учреждения науки Института системного программирования им. В.П.Иванникова Российской академии наук (ИСП РАН)
на разработку комплексного научно-технического проекта полного инновационного цикла «Инструментальная платформа выявления уязвимостей и дефектов в программно-аппаратных решениях на всех этапах жизненного цикла»

Проект ИСП РАН посвящен созданию и внедрению инструментальной платформы выявления уязвимостей и дефектов в программно-аппаратных решениях на всех этапах жизненного цикла, проведению масштабных мероприятий по обучению кадров в области кибербезопасности, а также внедрению новых технологий в промышленности.

В заявке предлагается интенсифицировать работы по созданию инструментальных средств анализа, разработки и верификации программных и аппаратных систем, критичных по надежности и безопасности. Заявленная цель напрямую отвечает данному приоритетному направлению, так как информационная безопасность и защита критической информационной инфраструктуры являются главными задачами в области кибербезопасности. Как отмечается в тексте заявки, помимо собственно развития технологий и инструментов кибербезопасности важно вкладывать значительные усилия в обучение кадров в области кибербезопасности упрощать внедрение новых технологий в практику разработки программ. Эти цели также важны в рамках приоритетного направления, без их достижения общая цель кибербезопасности на средне- и длинно-срочной перспективе достигнута быть не может.

Заявка ставит комплексную задачу, которая полностью соответствует декларированной цели. Комплекс задач соответствует трем направлениям: Развитие технологий и инструментов, подготовка кадров и адаптация технологий и инструментов под нужды предприятий промышленности, в том числе, создание типовых доверенных решений, которые практически без изменений могут использоваться в комплексах доверенного ПО за счет того, в рамках плана работ по КНТП будут выполнены работы по исследованию важнейших компонентов в контексте оценки уровня их доверия при помощи новейших методик и поддерживающих их инструментов.

Предлагаемый КНТП направлен на реализацию приоритетов научно-технологического развития Российской Федерации, а также учитывает большие вызовы для общества, государства и науки, указанные в Стратегии научно-технологического развития Российской Федерации, утвержденной Указом Президента Российской Федерации от 1 декабря 2016 г. №642 «О Стратегии научно-технологического развития Российской Федерации».

Решение комплексных задач и входящих в состав комплексных задач научно-технических задач способствует достижению национальных целей развития Российской Федерации, определенных пунктом 1 Указа Президента Российской Федерации от 21 июля 2020 г. №474 «О национальных целях развития Российской Федерации на период до 2030 года».

Комплексные задачи и входящие в состав КНТП являются системными, включают формирование научно-технического задела, разработку новых технологий и создание наукоемкой конкурентоспособной продукции, а их решение направлено на создание условий для проведения исследований и разработок, соответствующих современным принципам организации научной, научно-технической, инновационной деятельности и лучшим российским и мировым практикам.

Заявка отвечает всем основным критериям к КНТП, в том числе критериям:

- масштабности и научной значимости комплексных задач и входящих в состав комплексных задач научно-технических задач, для развития перспективных технологий и создания наукоемкой продукции практически во всех отраслях экономики России;
- создание и внедрение по результатам решения комплексных задач новых образцов продукции и технологий в различных отраслях и секторах экономики;
- обеспечения развития по результатам решения комплексных задач мероприятий по подготовке кадров для различных отраслей и секторов экономики;
- реализуемости и важности для устойчивого развития прорывных научных достижений;
- обеспечения перспективы успешной коммерциализации результатов решения задач;
- создания по результатам решения задач результатов интеллектуальной деятельности, подлежащих правовой охране.

ИСП РАН имеет необходимый научно-технический задел в данной области. Многолетний опыт проведения крупных НИР и ОКР в интересах как государственных заказчиков, так и коммерческих предприятий, устойчивые связи с университетами и крупнейшими научными центрами как в нашей стран, так и за рубежом позволили в концентрированном виде представить хорошо проработанный план работ по всем трем направлениям: технологии, кадры, внедрение. Работы по созданию и развитию инструментов и технологий кибербезопасности разбиты на этапам, выделены фазы проведения фундаментальных и поисковых исследований и фазы продуктизации и внедрения.

Представленная заявка показывает, что рынок для технологий и инструментов кибербезопасности уже сейчас составляет несколько миллиардов рублей в год с тенденцией ускоренного роста, в частности в связи с режимом санкций и

усложнением международной обстановки. Кроме того, постоянно ужесточаются требования регуляторов по обеспечению информационной безопасности, особенно для систем из критической информационной инфраструктуры. В число потенциальных заказчиков создаваемых технологий и инструментов входят практически все госкорпорации, а также компании, создающие программные комплексы ответственного назначения и нуждающиеся в соответствующей сертификации.

В число таких предприятий-заказчиков входят РФЯЦ-ВНИИЭФ, ПАО «Сбербанк», компании таких госкорпораций как Ростех, Роскосмос и др. Часть рынка будет обеспечена сертификационными лабораториями ФСТЭК и других регуляторов. Также немалую долю рынка будут составлять университеты (специальность «Кибербезопасность» со временем будет присутствовать практически во всех университетах, выпускающих ИТ-специалистов).

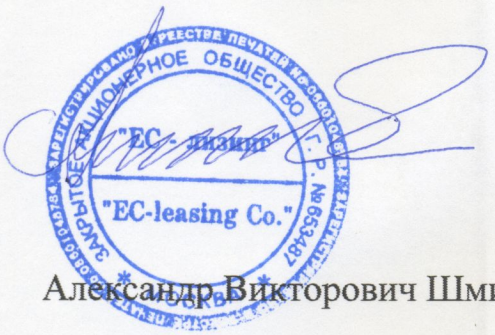
В заявке имеется краткий анализ рынка. Показано, что еще пять-десять лет назад рынок измерялся миллиардами рублей. Однако в последние годы спрос на доверенное ПО и на технологии независимые от зарубежных поставщиков устойчиво растут.

ИСП РАН имеет несколько базовых кафедр в ведущих университетах России. Сейчас в институте трудится большой коллектив квалифицированных специалистов, больше половины из которых составляют молодые ученые и инженеры. У института большой задел: сотни публикаций в отечественных и зарубежных изданиях, инструменты и технологии, патенты и зарегистрированные программы. Институт располагает необходимой материальной базой включая рабочие станции, серверы и облачные хранилища.

ИСП РАН имеет многолетние научные и производственные связи с ведующими научно-техническими центрами страны. В число партнеров ИСП РАН входят промышленные компании: Лаборатория Касперского, Positive Technologies, РусБИТех, Базальт СПО, СКБ Сухого, СКБ Лавочкина, НТЦ Модуль, МЦСТ, НТЦ Фобос-НТ; университеты: МГУ, МГТУ, СПбПУ, ИТМО, МФТИ, МИФИ; научно-исследовательские институты: ГосНИИАС, НИИСИ РАН, ИНЭУМ и другие. Со многими предприятиями и учреждениями у института заключены рамочные договоры о партнерстве в области разработки, анализа и верификации доверенного ПО. У ИСП РАН большой опыт выполнения НИР с индустриальными партнерами, которые обеспечивали софинансирование в заданным объемах. В ИСП РАН разработана дифференцированная лицензионная политика, в соответствии с которой осуществляется передача прав на использование разработанных программных продуктов. Дифференциация позволяет предоставлять существенные скидки образовательным и бюджетным учреждениям, за счет чего образовательные программы, подготовленные в ИСП РАН достаточно легко внедряются во многих университетах страны.

Среди недостатка заявки отметим отсутствие письменного согласия ответственного исполнителя-координатора, однако постановка задачи и все остальные части заявки находятся в полном соответствии с целями и задачами Министерства науки и высшего образования РФ, что позволяет надеяться на поддержку этой заявки министерством. Письменные согласия потенциальных заказчиков к проекту заявки не приложены, однако наличие долгосрочных связей с предприятиями-индустриальными партнерами ИСП РАН указывает на то, что заинтересованность индустриальных партнеров велика, и, соответствующие письма-согласия обязательно появятся позже.

Несмотря на указанный недостаток, считаю, что заявка Федерального государственного бюджетного учреждения науки Института системного программирования им. В.П. Иванникова Российской академии наук на разработку комплексного научно-технического проекта полного инновационного цикла «Инструментальная платформа выявления уязвимостей и дефектов в программно-аппаратных решениях на всех этапах жизненного цикла» заслуживает поддержки.



Александр Викторович Шмид

Д.т.н., профессор

Президент ЗАО «ЕС-лизинг»