Виктор Рулевский
Ректор Томского государственного университета систем управления и радиоэлектроники

ТУСУР

НАЦИОНАЛЬНЫЙ ЦЕНТР МИРОВОГО УРОВНЯ

«БЕЗОПАСНОСТЬ И ЦИФРОВОЕ ДОВЕРИЕ»

Презентация конкурсной заявки

Томск 2025

Цель
Программы развития центра:

Укрепление обороноспособности России в условиях роста гибридных угроз и **обеспечение требуемого уровня противодействия киберугрозам**, за счет создания комплекса суверенных передовых продуктов и систем в области обеспечения информационной и кибербезопасности на основе технологий искусственного интеллекта, квантовой передачи данных, беспилотного транспорта.

Задачи

1. Разработка и исследование на высоком международном научном уровне перспективных моделей, методов, методик и алгоритмов обеспечения безопасности информации и адаптация результатов научной работы для внедрения в практическую деятельность по защите информации и разработке средств защиты информации индустриальных партнеров - лицензиатов ФСТЭК России и ФСБ России.

2. Ускоренный вывод на отечественный и зарубежный рынки полученных научных результатов за счет совместного с индустриальными партнерами формирования технологий, отдельные компоненты которых своевременно проходят апробацию в рамках практической деятельности через передачу прав на разработанные модели и методы.

3. Повышение уровня проведения прикладных научных исследований путем улучшения материально-технической оснащенности Центра за счет внедрения уникальных отечественных аппаратно-программных комплексов квантовой передачи данных, безопасного хранения и обработки данных, а также ускорителей алгоритмов искусственного интеллекта.

4. Привлечение к научным исследованиям Центра большого количества молодых перспективных ученых, аспирантов и студентов через проведение мероприятий (летних и зимних школ, конкурсов, конференций и др.), направленных на популяризацию профильных научных направлений - безопасность квантовых коммуникаций, использование методов искусственного интеллекта в кибербезопасности, создание защищенного программного обеспечения и автоматизированных систем, обнаружение кибератак и уязвимостей в системах критической информационной инфраструктуры.

Запрашиваемый размер субсидии:

1845 млн руб.

ПРИОРИТЕТНОЕ НАПРАВЛЕНИЕ

НАУЧНО-ТЕХНОЛОГИЧЕСКОГО РАЗВИТИЯ

Важнейшие наукоемкие технологии

1. Технологии защищенных квантовых систем передачи данных.
2. Технологии создания доверенного и защищенного системного и прикладного программного обеспечения, в том числе для управления социальными и экономически значимыми системами.
3. Транспортные технологии для различных сфер применения (море, земля, воздух), в том числе беспилотные и автономные системы.
4. Технологии ИИ в отраслях экономики, социальной сферы (включая сферу общественной безопасности) в органах публичной власти.

Участники Центра и индустриальные партнеры

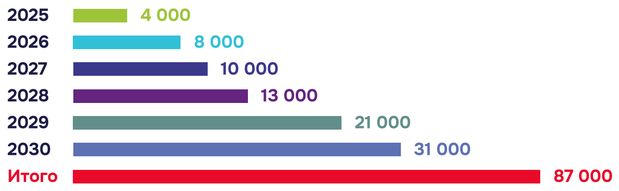
ТУСУР
Координатор центра

СПб ФИЦ РАН, СКФУ
Участники центра

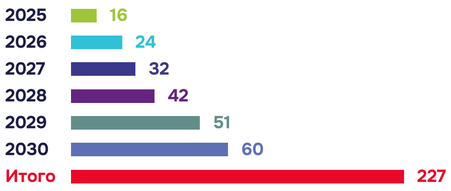
infotecs, ALFAtech, Про Интеграция, КИБЕРПРОТЕКТ, АГРИКО ГРУППА КОМПАНИЙ, УЦСБ
Индустриальные партнеры

Прогнозные значения показателей эффективности центра

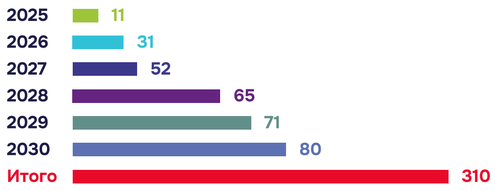
Доход от реализации прав на результаты интеллектуальной деятельности, созданные в результате реализации программы развития центра (тыс.)



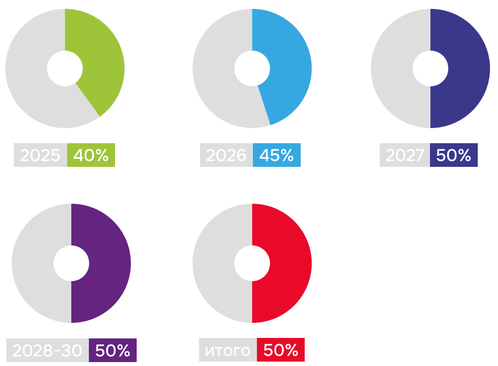
Количество заявок на правовую охрану результатов интеллектуальной деятельности (ед.)



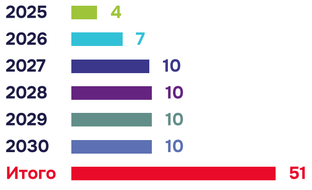
Количество публикаций первого и второго уровня «Белого списка» и на конференциях уровня А* (ед.)



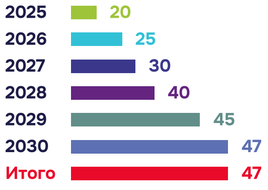
Доля исследователей центра в возрасте до 39 лет в общей численности исследователей центра %



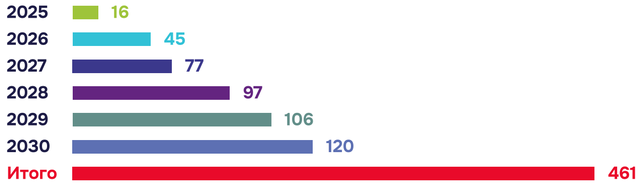
Количество организаций, действующих в реальном секторе экономики, с которыми были заключены соглашения о дальнейшем использовании результатов, полученных в рамках реализации программы развития центра



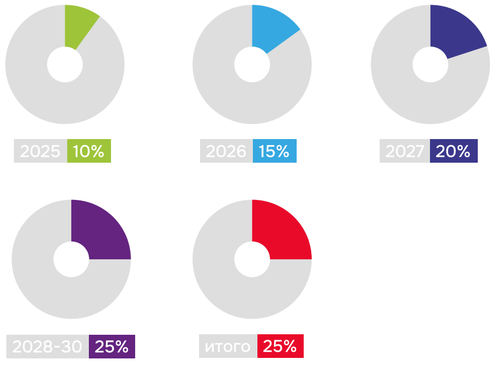
Количество российских и зарубежных ведущих ученых, работающих в центре (чел.)



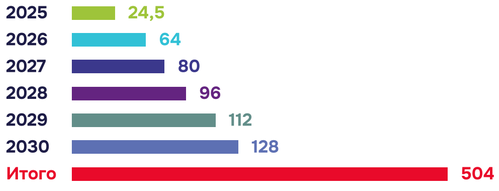
Количество статей в научных изданиях «Белого списка» и (или) в трудах конференций уровня А*, соавторами которых являются работники центра (ед.);



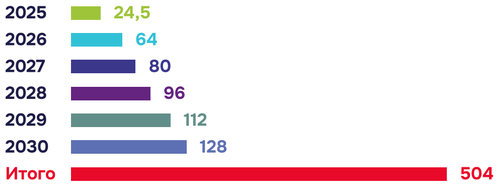
Доля исследований, проводимых центром под руководством молодых (в возрасте до 39 лет) перспективных исследователей %



Размер внебюджетных средств на исследования и разработки центра, (млн руб.)



Количество результатов интеллектуальной деятельности, созданных в результате реализации программы развития центра и переданных по договорам об отчуждении исключительного права или лицензионным договорам с организациями, действующими в реальном секторе экономики, для внедрения в производство, и (или) количество актов о внедрении результатов интеллектуальной деятельности, созданных в результате реализации программы развития центра (ед.)



Научный и технологический задел

2022-2024 гг.

85 сотрудников
коллектив центра

Коллектив центра – **85** сотрудников, из них научных сотрудников – **50**. Количество ведущих ученых – **30** человек.

76
статей

Публикаций 1 и 2 уровней белого списка.

1+
млрд.руб.

Объём выполненных НИР и НИОКТР по профильным ВНТ.

6,49
млн.руб.

Доход организаций от реализации прав на РИД по ВНТ – **6,49 млн.руб.**

180+
мнл.руб.

Уникальное оборудование по квантовым коммуникациям, обнаружению и моделированию кибератак, в т.ч. на объекты КИИ, управлению инцидентами с общей стоимостью – **180+ млн.руб.**

150+
мнл.руб.

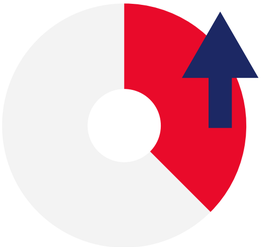
Объемы НИОКТР, выполненных по договорам с квалифицированными заказчиками по направлениям деятельности центра – **105+ млн.руб.**

Планируемые результаты реализации Программы развития центра

Исследования и внедрение их результатов в уникальные высокотехнологичные продукты мирового уровня по следующим направлениям:

- Средство автоматизированного проектирования систем обеспечения информационной безопасности;
- Новое поколение систем квантового распределения ключей, отличающегося применением мультипротокольности сравнимого с мировым уровнем;
- Облачные системы обработки и хранения больших данных, позволяющие обеспечить безопасные распределенные вычисления при построении моделей ИИ;
- Доверенная система хранения и предоставления доступа к наборам данных, используемых при создании систем искусственного интеллекта, и обеспечивающая безопасность информации и моделей на всех жизненных этапах систем и при их взаимодействии;
- Система расследования инцидентов и компьютерных преступлений, отличающаяся применением методов ИИ;
- Разработка продуктов по обнаружению атак и уязвимостей, основанных на принципиально новых подходах на базе искусственного интеллекта;
- Формирование технологического пакета решений по обеспечению противодействия утечкам информации при получении, хранении, передаче и обработке данных.

Реализация Программы обеспечит кумулятивный эффект по обеспечению защищенности национальных информационных ресурсов (в т.ч. Объектов КИИ) от внешних и внутренних киберугроз, окажет значимое и заметное влияние на профильные рынки.



Увеличение объемов, качества и направлений научных исследований и разработок по направлению Computer Science, **повышение узнаваемости и цитируемости** отечественных фундаментальных и прикладных работ в мировом научном сообществе, итоговый рост ежегодного числа публикаций **1 и 2 уровней белого списка** более чем в **2,4 раза**.

Расширение объемов рынка в области информационной и кибербезопасности за счет доведения до высокого уровня готовности **принципиально новых высокотехнологичных продуктов**, конкурентноспособных на мировом уровне, основанных, в том числе, на применении предиктивных подходов.

Формирование совместно с индустриальными партнерами **новых продуктовых направлений** на отечественном и международном рынках **(в т.ч. рынка данных)** в рамках смежных с информационной безопасностью областей – искусственный интеллект, беспилотные системы, квантовые коммуникации.

Появление нового устойчивого рынка телекоммуникационного оборудования на основе квантового распределения ключей, за счет кратного снижения себестоимости продуктов, развитие этого рынка, обеспечит **заданный уровень сетевого суверенитета и информационной безопасности** в информационно-телекоммуникационной сети Интернет.

КА с применением мультипротокольности, что позволит Создание системы направленных на выявление и развитие способностей молодых людей **профессионально ориентированных мероприятий,** людей к проведению научных исследований и практической деятельности в области информационной безопасности, искусственного интеллекта и др.

Планируемые разработки

Технология обеспечения противодействия утечкам информации при получении, хранении, передаче и обработке данных.

2027	2028	2029
1 система с УГТ6	2 системы с УГТ6	3 системы с УГТ6

2029 УГТ6
Языковая модель для поисковых запросов к серверу управления DLP системой

2030 УГТ4
Модули для определения степени конфиденциальности документа с применением ИИ, классификация документов по заданному описанию, с применением языковых моделей

2028 УГТ6
Подсистема анализа событий в целях выявления аномалий поведения пользователей системы

2029 УГТ6
Подсистема анализа событий в целях создания гипотез о потенциальных рисках, создаваемых пользователями

2029 УГТ6
Подсистема определения степени конфиденциальности документа с применением ИИ, классификация документов по заданным образцам

2028 УГТ6
Подсистема выявления некорректного поведения пользователей

2027 УГТ6
Прототип программного комплекса обеспечения безопасности получения, хранения, передачи и обработки документов

Технология малоресурсной обработки сигналов для задач навигации автономных роботизированных систем (ТМОС)	**2028** **УГТ6**	Реализуемая технология является передовым решением, сравнимым с мировым уровнем и направленным на осуществление обработки сигналов на малоресурсных платформах. Подобные решения являются крайне востребованными, в частности, при реализации автономных роботизированных беспилотных систем, функционирующих во всех средах на море, на земле и в воздухе.
Программно-определяемая доверенная система хранения данных (ПОД СХД)	**2029** **УГТ6**	Технология способствует решению задачи безопасной обработки данных от пользователя, при котором в хранилище загружаются сами исходные данные, после чего через внутренний интерфейс они отправляются на обработку на методы машинного обучения, а пользователь получает только конечный результат. При этом исключена возможность оказывать воздействие на хранящиеся данные, а также модели машинного обучения и искусственного интеллекта, что обеспечивает дополнительную безопасность их обработки.
Мультипротокольная система квантового распределения ключей (МПС КРК)	**2030** **УГТ6**	Получаемый прототип реализует комплекс недоступных в настоящее время функций по исследованию эффективности, надежности и совместимости протоколов КРК. Созданный прототип позволит создать реальные отечественные унифицированные мультипротокольные системы мирового уровня КРК.
Система автоматизированного проектирования систем обеспечения информационной безопасности (САПР СОИБ)	**2030** **УГТ6**	САПР СОИБ направлена на повышение безопасности автоматизированных систем различного типа, включая объекты критической информационной инфраструктуры (КИИ). На рынке отсутствует комплексное решение, позволяющее автоматизировать работу по проектированию системы защиты и оценить эффективность разработанного проекта. Результаты проекта будут востребованы при создании систем обеспечения информационной безопасности значимых объектов критической информационной инфраструктуры организациями-субъектами КИИ и организациями-лицензиатами ФСТЭК России.
Технологии проектирования интеллектуальных, отказоустойчивых облачных инфраструктур нового поколения	**2030** **УГТ6**	Разрабатываемые интеллектуальные, отказоустойчивые и безопасные облачные инфраструктуры позволят создать самовосстанавливающиеся системы с интеллектуальным управлением репликацией данных и динамическим балансированием нагрузки с возможностью обнаружения аномалий и предотвращения атак в облачных средах. Это обеспечит создание облачных технологий нового поколения, способных к автономной адаптации, эффективному управлению ресурсами и многоуровневой защите данных.
Технологии проектирования интеллектуальных туманных систем	**2030** **УГТ6**	Разрабатываемые интеллектуальные и безопасные методы передачи, обработки и обучения данных в распределенных туманных и межоблачных средах с доверенными граничными вычислениями позволят производить построение высоконагруженных и критически важных приложений обеспечивающих высокую производительность, минимальные задержки и защиту информации.
Интеллектуальная программная платформа управления, контроля и обеспечения информационной безопасности	**2030** **УГТ6**	Конечный результат, основанный на технологии искусственного интеллекта, обеспечивает возможность защиты социо- и киберфизических систем, которые широко используются в различных отраслях экономики, социальной сфере и в органах публичной власти, от вредоносного воздействия компьютерных атак, вторжений и уязвимостей.
Интеллектуальная программная система оценки защищенности, выбора контрмер и расследования инцидентов информационной безопасности	**2030** **УГТ6**	Система позволят с высокой точностью и полнотой проводить оценку защищенности, выбор контрмер и расследовать инциденты информационной безопасности в российских организациях, что обеспечит уровень защищенности, в том числе, объектов КИИ.

ТУСУР

Рулевский Виктор Михайлович

Ректор, доктор технических наук, профессор

Контакты для связи:

634050, Томск, пр-т Ленина, 40

e-mail: office@tusur.ru

телефон: +7 3822 510530, 907155

Шелупанов Александр Александрович

Директор ИСИБ, доктор технических наук, профессор

Контакты для связи:

г. Томск, ул. Красноармейская, 146

e-mail: ssh@2i.tusur.ru

телефон: 8-953-918-33-20