Сведения о важнейших научных результатах ЦРКЦФА за 2019 г.

1. Директору научного учреждения РАН, находящегося под научно-методическим руководством ОНИТ РАН, представить руководителям соответствующих секций (список распределения учреждений по секциям прилагается) (isokolov@ipiran.ru, gulyaev@cplire.ru, vpanch@rfbr.ru)и в ОНИТ РАН (nanoitdep@presidium.ras.ru) (!): важнейшие результаты исследований в 2019 году, расположенных в порядке значимости (не более 2-х с указанием названия результата, научной организации, фамилий авторов и сведений об опубликовании. Текст по каждому результату объемом строго 7-15 строк должен отражать его сущность, новизну и значимость, при этом значимость результата должна быть понятной и для неспециалиста. Результаты обязательно сопроводить иллюстративными материалами (таблицы, графики, схемы) в форматах jpeg, png с разрешением не менее 600 dpi. Общий объем материала на каждый результат, включая иллюстрации, – до 1 страницы машинописного текста (интервал одинарный, шрифт 12 Times New Roman)

2. Привести (если имеются) краткие сведения о важнейших исследованиях и разработках в 2019 году, готовых к практическому применению. По каждой разработке дать краткое (не более 1 страницы текста) описание с указанием: института-разработчика; краткой характеристики основных технических параметров; области возможного использования; степени готовности разработки к практическому применению; возможного технического и/или экономического эффекта от внедрения; сравнительных характеристик с известными разработками; сведений о патентоспособности и патентной защите разработки

1. В настоящее время в условиях действующих международных санкций весьма актуальна фундаментальная математическая и криптографическая задача построения системы распределенных реестров, обладающих высоким транзакционным быстродействием и использующих симметричные криптографические алгоритмы, а также обеспечивающих минимальное или регулируемое разглашение данных об архитектуре системы и проводимых в ней транзакциях. В течение 2019 г. в рамках государственного задания ЦРКЦФА ВИНИТИ РАН занимался решением данной задачи. Для решения указанной задачи сформулировано понятие технологий “информационного чёрного

ящика” для системы, утройство которой таково, что внешний наблюдатель не имеет никакой информации о ее участниках и данных, хранимых и обрабатываемых в ней. На основе системно-аналитического подхода, формулирования модели нарушителя и выделения существенных требований к распределенному реестру решена проблема создания универсального доверенного распределенного реестра, устойчивого к внешним атакам, включая трекинг транзакций, и обеспечивающего неразглашение данных об архитектуре реестра. Сформулированная концепция создания доверенного защищенного распределенного реестра может являться методологической основой для формулирования ведомственных или национальных регулирующих требований в области цифровой экономики, а также послужить технической основой для разработки конкретных проектов в области защищенных систем, использующих распределенные реестры в сфере государственного управления, финансов и учетно-сервисных систем.

Результаты отражены в следующих публикациях:

1. Гостев С.С., Гриняев С.Н., Щербаков А.Ю., Правиков Д.И. К РАЗВИТИЮ МЕТОДОЛОГИИ СОЗДАНИЯ ДОВЕРЕННЫХ И ЗАЩИЩЕННЫХ ИНФОРМАЦИОННЫХ СИСТЕМ, ПОСТРОЕННЫХ С ИСПОЛЬЗОВАНИЕМ ТЕХНОЛОГИИ РАСПРЕДЕЛЕННЫХ РЕЕСТРОВ // Современная наука: актуальные проблемы теории и практики. Серия: Естественные и технические науки, 2019. № 3-2. С. 10-15.

2. Касперская Н.И., Кузьменко В.В., Хайретдинов Р.Н., Щербаков А.Ю.О ПОДХОДАХ К СОЗДАНИЮ УНИВЕРСАЛЬНОГО ДОВЕРЕННОГО РАСПРЕДЕЛЕННОГО РЕЕСТРА, ОБЕСПЕЧИВАЮЩЕГО НЕРАЗГЛАШЕНИЕ ДАННЫХ О СИСТЕМЕ // Безопасность информационных технологий, 2019. Т. 26. № 2. С. 95-108. DOI: http://dx.doi.org/10.26583/bit.2019.2.01

2. В рамках научно-технического сотрудничества с Концерном «Гранит» ЦРКЦФА принял участие в разработке и сертификации в ФСБ РФ системы распределенных реестров «Купол», обеспечивающей защиту конфиденциальной информации (включая персональные данные), не составляющей государственную тайну. По результатам работы получен сертификат СФ/СЗИ-0308 от 30.10.2019 (графический файл прилагается). Решение готово к внедрению и патентованию.