14 марта 2024 г. в ИРЭ им. Котельникова РАН в очном формате и в формате видеоконференции состоялось заседание Научного Совета РАН «Фундаментальные проблемы создания и функционирования телекоммуникационных систем» по теме «Проблемы информационной безопасности».

В повестке дня:

1. *«Инфраструктура технической защиты информации. Технологическая независимость, доверенность и импортозамещение», д.т.н. Конявский Валерий Аркадьевич, ЗАО «ОКБ САПР», зав. кафедрой защиты информации МФТИ;*
2. *«Безопасность передачи информации в телекоммуникационных сетях», д.т.н., профессор РАН Мещеряков Роман Валерьевич, Институт проблем управления им. В.А. Трапезникова РАН;*
3. *«Базис Отрасли Связь», Фрейнкман Владимир Анатольевич, Общество с ограниченной ответственностью «Научно-Технический Центр Протей»);*
4. *«Разработка и облик национальной гибридной системы связи», Кургузов Роман Юрьевич, АО «Информационные спутниковые системы» имени академика М.Ф. Решетнева» (АО «РЕШЕТНЁВ»).*

Выступающие:
Борисов В.И., Конявский В.А., Мещеряков Р.В., Фрейнкман В.А., Кургузов Р.Ю., Аджемов А.С., ак. Никитов С.А., ак. Сойфер В.А., Цым А.Ю., Кренделин В.Б., Урличич Ю.М.

Заслушав доклады и выступления участников совещания, а также предложения по перспективам развития телекоммуникаций в России, с учетом необходимости гарантий национального суверенитета в этой области, Совет отмечает:

1. Закрытым акционерным обществом «Особое конструкторское бюро систем автоматизированного проектирования» (ЗАО «ОКБ САПР») при методологическом участии МФТИ разработана принципиально новая архитектура компьютера (новая Гарвардская архитектура), отличающаяся тем, что за счет управляемой ее изменяемости обеспечивается доверенность на всех этапах ее применения, включая высокий уровень вирусного иммунитета. В ОКБ САПР разработан и серийно выпускается целый ряд средств защиты информации (средства доверенной загрузки, средства защиты от несанкционированного доступа, защищенные носители информации и др.), применение которых позволяет блокировать такие угрозы как: архитектурная уязвимость от вредоносного действия вирусов, несанкционированные действия злоумышленников извне и т.п. На этой базе создано и серийно выпускается большое количество доверенных решений, в том числе для значимых объектов критической инфраструктуры, для управления локомотивами, для управления беспилотными летательными аппаратами, для защиты финансовых коммуникаций, биометрии, а также смартфон, позволяющий использовать услуги связи в специальных условиях. Результаты опытного тестирования и эксплуатации в органах государственной власти и организациях (Минтранс России, ФТС

России, Росавиация, Минпромторг, Росатом, Роскосмос, кредитно-финансовая сфера и др.) показали возможность обеспечения выполнения всех необходимых требований по обеспечению достаточного уровня доверия. Совет высоко оценивает уровень прикладных работ ОКБ САПР: в области обеспечения защищенности государственных информационных систем (включая системы, обрабатывающие информацию, содержащую сведения, составляющие государственную тайну), информационных систем персональных данных, объектов критической информационной инфраструктуры; в решении задач технологической независимости от зарубежных компаний (решения защищены рядом патентов); в обеспечении импортозамещения (разработка выполнена полностью на отечественной базе и элементах производства КНР); в создании отечественного производства высокотехнологичного оборудования в сочетании с высокой степенью информационной защищенности. Совет рекомендует ОКБ САПР продолжить развитие перспективных решений, направленных на повышение защищенности информационных систем, при этом учитывать результаты фундаментальных и прикладных исследований РАН в области информационной безопасности, в частности – в вопросах развития и эксплуатации доверенных телекоммуникационных систем.

2. Современное состояние телекоммуникационных систем требует непрерывного обеспечения безопасности на всех этапах жизненного цикла их функционирования и во всех (не только аппаратных) элементах телекоммуникационных систем. Особое внимание необходимо уделить сохранению свойств информации, которая передается по телекоммуникационным сетям: конфиденциальность, целостность и доступность. Телекоммуникационные сети представляют собой сложные гетерогенные системы, и их развитие идет за счет увеличения количества устройств в сети, каналов передачи, пропускной способности, протоколов и других характеристик. Вычислительные возможности оконечных устройств не позволяют использовать сложные алгоритмы защиты информации, что существенно влияет на безопасность передаваемой информации и безопасность всей системы в целом. Основные направления обеспечения безопасности передачи информации в телекоммуникационных сетях следующие: совершенствование систем поведенческого анализа (технологичные системы обнаружения угроз информационной безопасности при помощи анализа поведения пользователей компьютерных систем и объектов); использование технологий искусственного интеллекта, биометрии; технологий стеганографии, стегоанализа и цифровых водяных знаков; совершенствование квантовых технологий, постквантовой криптографии и квантового распределения ключей. Совет отмечает высокий уровень научных исследований в области безопасности передачи информации в телекоммуникационных сетях, проводимых Институтом проблем управления им. В.А.Трапезникова РАН.

3. Основное мировое направление развития телекоммуникаций – многотысячные группировки спутников на низких орбитах, вследствие чего услуги спутниковой связи становятся сопоставимы, по качественным характеристикам, с услугами операторов фиксированной и мобильной связи, но при этом имея существенное преимущество в глобальности охвата и низких операционных затратах. Разработка «Национальной гибридной системы связи Российской Федерации» (проект АО «РЕШЕТНЁВ») с целью создания взаимоувязанной инфраструктуры для предоставления современных доверенных услуг связи в глобальном масштабе и технологическом экспорте обеспечит: полное покрытие территории РФ услугами связи в стандарте LTE и 5G; предоставление высокоскоростной передачи данных и голосовых услуг в населённых пунктах РФ и для

наземного, надводного и воздушного транспорта в любой точке планеты; предоставление услуг связи NTN (Non-Terrestrial Network – не наземные сети), URLLC (Ultra-Reliable Low-Latency Communications — предоставление высоконадёжного соединения с низкой задержкой передачи данных), eMBB (enhanced mobile broadband - расширенная мобильная широкополосная связь - высокая скорость обмена данными, до нескольких гигабит в секунду) , eMTC (enhancements for Machine-Type Communications - коммуникации между различными механизмами и устройствами, такими как IoT, M2M и др.) в стандарте 5G; предоставление доверенной связи для силовых структур и федеральных органов исполнительной власти. Совет отмечает важность и актуальность прикладных и фундаментальных научных исследований для реализации гибридной системы связи, отмечает особую значимость реализации гибридной системы связи для всех отраслей экономики, обороноспособности страны и безопасности государства. Совет поддерживает предложение АО «РЕШЕТНЁВ» по облику национальной гибридной системы связи, поддерживает предложение АО «РЕШЕТНЁВ» по преимущественному применению в бортовом оборудовании космического сегмента этой системы использование отечественного электронной компонентной базы при ее технологической готовности, а также рекомендует АО «РЕШЕТНЕВ» учесть результаты научно-исследовательских работ РАН при проектировании и создании этой системы.