Итоговый документ
21-й ежегодной конференции
«Обеспечение доверия и безопасности при использовании ИКТ»,
15-16 марта 2023 года

15-16 марта 2023 года в Москве состоялась 21-я ежегодная конференция «Обеспечение доверия и безопасности при использовании ИКТ», организованная общественно-государственным объединением «Ассоциация документальной электросвязи».

В работе конференции приняли участие более 120 представителей, в том числе руководители и ведущие эксперты органов государственной власти, поставщиков и производителей оборудования, операторов связи, контент-провайдеров, регистраторов, компаний в области обеспечения информационной безопасности, а также преподаватели и студенты профильных вузов.

Конференция включала в себя 8 заседаний. В рамках круглого стола № 1 **«Состояние и перспективы регулирования ИБ в отрасли ИКТ»** при участии представителей Минцифры России, ФСБ России, Минэнерго России обсуждались актуальные вопросы совершенствования нормативной базы развития ИКТ-инфраструктуры и обеспечения доверия и безопасности при её использовании.

На заседании круглого стола предложено:

1. Продолжить обеспечение и поддержку важной роли АДЭ как связующего звена между органами власти и бизнес-сообществом в целях дальнейшей консолидации и объединения усилий общественных организаций, органов власти и бизнеса для достижения решения задач обеспечения доверия и безопасности.
2. Поддержать деятельность АДЭ в части содействия обеспечению практической технологической независимости и информационной безопасности страны, применения отечественных программно-аппаратных средств в образовательной деятельности и при реализации инфраструктурных проектов с сохранением требуемой функциональности.
3. Отметить важную роль Ассоциации и базовой кафедры АДЭ в обеспечении подготовки востребованных специалистов отрасли ИКТ, положительный опыт привлечения к преподаванию ведущих экспертов из числа организаций-членов АДЭ.
4. Создавать доверенные системные и прикладные программные продукты, способные работать на отечественных архитектурах микропроцессоров, и размещать их в технологически независимый репозиторий свободного и проприетарного программного обеспечения с возможностью безопасной разработки, отладки, сопровождения и поддержания жизненного цикла ПО.
5. Отметить целесообразность развития стандартизации информационной безопасности на национальном уровне и значимость участия в международном развитии ИКТ, необходимость быть активными участниками в работе доступных и значимых международных и региональных организаций.

В рамках круглого стола № 2 **«Взаимодействие экспертного сообщества и органов государственной власти в рамках пилотной зоны отечественного репозитория»** обсуждались вопросы формирования технологически независимой инфраструктуры разработки, сборки, отладки и сопровождения свободного и проприетарного программного обеспечения, которое может исполняться, в том числе, на отечественных аппаратных платформах.

В соответствии с Протоколом заседания секции по проблемам информационной безопасности Научного совета при Совете Безопасности Российской Федерации №4 от 23.12.2021 №А216-815 рабочая группа общественно-государственного объединения «Ассоциация документальной электросвязи» (АДЭ) разработала проект Стратегии создания российского репозитория программных пакетов и библиотек, находящегося в юрисдикции и на территории Российской Федерации (прилагается, далее – проект Стратегии). В процессе прошедших обсуждений в проект Стратегии внесены доработки и исправления по замечаниям Минцифры России, ФСБ России и ФСТЭК России. В соответствии с предложением ФСБ России, Исполнительным комитетом АДЭ на заседании 22.12.2022 принято решение о целесообразности проверки положенных в основу проекта Стратегии принципов в рамках постоянно действующей пилотной зоны отечественного репозитория, разворачиваемой на базе АДЭ с использованием ресурсов всех организаций, заинтересованных в открытом и профессиональном изучении и обобщении лучших практик ведения безопасной разработки, отладки и сопровождения свободного и проприетарного программного обеспечения (далее - ПО) с целью создания востребованных программных приложений для граждан, бизнеса и органов государственной власти, способных работать на отечественных средствах вычислительной техники.

В рамках пилотной зоны предлагается решать следующие основные задачи:

- создание инфраструктуры разработки и поддержки полного жизненного цикла российского программного обеспечения, в том числе, для отечественных аппаратных платформ;
- формирование экосистемы российских кроссплатформенных продуктов с использованием свободного и проприетарного программного обеспечения, совместимых друг с другом и с отечественными аппаратными архитектурами, независимыми от зарубежных решений;
- создание национальной экосистемы разработки безопасного системного и прикладного программного обеспечения;
- содействие обеспечению устойчивости и безопасности функционирования объектов информационной инфраструктуры Российской Федерации;
- вовлечение максимально широкого круга специалистов в индустрию российских разработок ПО для национального и мирового рынков (частные лица, сообщества, коммерческие разработчики, учебные заведения, отраслевые научные учреждения, коммерческие потребители ПО, организации в области ИБ);
- повышение конкурентоспособности российского программного обеспечения за счет формирования экосистемы совместимых российских кроссплатформенных продуктов: средств разработки программного обеспечения, операционных систем, прикладного программного обеспечения.
- содействие участию российских компаний в международных проектах по разработке свободного программного обеспечения с учетом национальных интересов.

Вопросы развертывания и функционирования пилотной зоны предлагается обсуждать на конференциях АДЭ, проводимых 2 раза в год. Являясь общественно-государственным объединением, АДЭ готова организовывать работу пилотной зоны российского репозитория в соответствии с указаниями Минцифры России, содействуя реализации государственной политики в области развития ИКТ-инфраструктуры и обеспечения доверия и безопасности при её использовании.

Представляется целесообразным провести обсуждение предложения по возможной интеграции проводимых работ по созданию репозитория СПО и пилотной зоны в рамках Ассоциации, учитывая нацеленность проекта АДЭ на выявление и использование российских достижений в создании безопасной инфраструктуры разработки, комплексирования, отладки и сопровождения практически значимых приложений на базе свободного и проприетарного ПО, которые могут использоваться для отечественных архитектур микропроцессоров. При этом важно учесть имеющиеся в стране отечественные решения, используемые в отрасли, а существующий задел на создание технологической независимости необходимо использовать и развивать. Примером такого задела является ПАК «МАРС», успешно функционирующий на отечественном процессоре «Эльбрус» под ОС «Альт».

Также участниками была отмечена целесообразность предлагать к использованию отечественным разработчикам решений отечественных компаний (например, репозиторий «Сизиф»), так как использование библиотек и пакетов, над которыми нет возможности контроля и анализа, приводит к проблеме отсутствия контроля над кодом ПО при контейнеризации.

В настоящее время в рамках поручения Правительства Российской Федерации выполняются работы в части создания Отечественного репозитория СПО («аналог GitHub»). На данный момент существуют следующие актуальные задачи:

- локализация разработчиков на едином ресурсе;
- вовлечение большего количества заинтересованных людей в разработку;
- обеспечение ИБ платформы, предоставление всех необходимых условий операторам ИБ;
- исключение противоречий и нарушений, проверка на соответствие ФСТЭК России.

При функционировании пилотной зоны репозитория на базе Ассоциации представляется важным обеспечить согласованность и интеграцию проводимых работ, учитывая нацеленность проекта АДЭ на выявление и использование российских достижений в создании безопасной инфраструктуры разработки, комплексирования, отладки и сопровождения практически значимых приложений на базе свободного и проприетарного ПО, которые могут использоваться для отечественных архитектур микропроцессоров.

В рамках круглого стола № 3 **«Безопасный контент»** рассмотрены вопросы использования современных способов коммуникации в работе органов власти, в том числе, правоохранительных органов и бюджетных организаций; развитие критичных для импортозамещения новых коммуникационных интернет-технологий (НКИТ).

Учитывая сложившуюся внешнеполитическую ситуацию, необходимость развития цифровых технологий, обеспечивающих технологическую независимость России и безопасность граждан страны в информационной среде, сформулированы следующие предложения:

1. Предусмотреть развитие технических и организационных инструментов выявления фейков и дипфейков, нормативных механизмов санкций к физическим и юридическим лицам, использующим недостоверный контент в деструктивных целях. Обеспечить оказание в приоритетном порядке государственных мер поддержки отечественным компаниям, создающим решения, обеспечивающие создание и выявление фейков и

дипфейков, развитие организационных и технических инструментов реагирования на информационные угрозы.

2. Поддержать установление оборотных штрафов в отношении компаний, допускающих утечку персональных данных, усиление ответственности за их незаконный оборот и иные нарушения законодательства в области персональных данных.
3. Продолжить разработку организационных и технических механизмов, исключающих бесконтрольное использование технологическими компаниями пользовательских данных, в том числе, персональных.
4. Обеспечить создание условий для обмена опытом, развития программ подготовки и массового обучения сотрудников органов власти, в том числе, правоохранительных органов, а также сотрудников бюджетных учреждений современным способам коммуникации в публичном пространстве (работе с соцсетями, продвижением контента, рекомендательными сервисами), в том числе с использованием лучших практик и компетенций АНО «Диалог Регионы» и образовательного проекта «Мастерская новых медиа».
5. В целях обеспечения безопасности использования контента продолжить развитие подходов к сквозной идентификации и авторизации пользователей в различных отечественных сервисах.
6. Для поддержки научных исследований в сфере коммуникационных технологий сформировать пул критичных наукоемких задач с крупными премиями за их решение (по аналогии с семью математическими «Задачами тысячелетия» Математического института Клэя).
7. Поручить профильным органам власти и организациям актуализировать требования по информационной безопасности коммуникационных технологий и процедуры сертификации средств защиты информации с целью повышения скорости проведения сертификации и снижения ее стоимости.
8. Провести оценку потребности в проактивном регулировании «метавселенных» как в техническом, так и в этическом аспекте.
9. В целях создания условия для продвижения российских решений за рубежом, предусмотреть при развитии отраслевых стандартов в сфере коммуникационных технологий обеспечение обратной совместимости отечественных решений с решениями, используемыми на мировом рынке (в том числе, со свободным программным обеспечением).
10. В целях повышения доли российского контента на отечественном рынке:
    - расширить меры поддержки разработчиков профессионального контента, сервисов и платформ, предусмотрев софинансирование государством крупных видеопроектов, и в целом создание позитивного контента;
    - рассмотреть возможность создания государственной компании, предоставляющей в аренду технику и технологии (возможно, в формате технопарков и коворкингов) для производства высококачественного видео, анимационного и игрового контента.
11. Предусмотреть механизмы поощрения граждан, использующих легальные ресурсы для просмотра видеоконтента. Обеспечить создание условий для льготного доступа к отечественным видеосервисам либо определенным видам контента на них для отдельных категорий лиц (школьники, студенты, многодетные семьи и другие).

В рамках круглого стола №4 **«Обеспечение доступности, доверия и безопасности в российском сегменте сети Интернет»** обсуждались современные вызовы и решения в части обеспечения доступности, доверия и безопасности инфраструктуры российского сегмента сети Интернет, а также возможные сценарии дальнейшего развития.

На заседании круглого стола сформулированы следующие предложения:

1. Представляется целесообразным расширить поддержку российской национальной доменной зоны в части расширения использования кириллических интернет-идентификаторов (доменных имен и адресов электронной почты) и решения проблем по их интеграции в отечественные программные решения и почтовые сервисы. Обеспечение поддержки интернет идентификаторов на русском языке необходимо учитывать при разработке законодательных инициатив, национальных программ и проектов в области цифровизации, импортозамещения ПО и дальнейшего развития ИКТ в России. Координационный центр доменов .RU/.РФ разработал рекомендации по внедрению в программном обеспечении поддержки кириллических доменных имен и адресов электронной почты в домене .РФ, которые могут использоваться участникам ИКТ отрасли при разработке новых и доработке существующих программных продуктов и сервисов.
2. Представляется целесообразным создание авторитетного сервера имен системы DNS на базе отечественных аппаратно-программных средств, так как используемые в российском сегменте сети Интернет серверы и компоненты в DNS построены на зарубежном ПО и «железе». В целях обеспечения технологической независимости и безопасности функционирования системы DNS в стране, предлагается разработать доверенное ПО для сервера DNS на отечественной аппаратной платформе, что соответствует приоритетным направлениям деятельности (стратегии развития) Координационного центра доменов .RU/.РФ на период до 2025 года. Соответствующая заявка на выполнение работ готовится со стороны АНО «ЦКС» в Общее собрание учредителей КЦ доменов .RU/.РФ. Техническое задание на проведение работ согласовано с ООО «Технический центр Интернет».
3. В связи с угрозой приостановки выдачи удостоверяющим центром GSMA сертификатов для eSIM для российских операторов связи, целесообразно рассмотреть возможность реализации средств национальной среды доверия, подобного структуре GSMA, на базе одного из имеющихся в России корневых удостоверяющих центров и административной структуры в виде некоммерческой организации. В качестве такой административной структуры наиболее подходящей выглядит АДЭ как ассоциация, объединяющая в себе и заинтересованные органы государственной власти, и операторские компании, и производителей оборудования. Предложено на ближайшем заседании Исполнительного комитета АДЭ рассмотреть вопрос о создании новой рабочей группы по вопросам национальной среды доверия.

В рамках круглого стола № 5 **«Международное сотрудничество в обеспечении доверия и безопасности при использовании ИКТ»** обсуждался опыт международного сотрудничества в развитии ИКТ-инфраструктуры и обеспечении доверия и безопасности при ее использовании, а также новые задачи, которые предстоит решить в этой сфере.

На заседании круглого стола сформулированы следующие предложения:

1. Содействовать участию российских представителей в деятельности специального комитета ООН по разработке конвенции по борьбе с информационной преступностью и рабочей группы открытого состава по безопасности использования ИКТ.
2. Содействовать созданию реестра контактных пунктов государств-членов (инициатива нацелена на совместное взаимодействие и сотрудничество государств в расследовании информационных преступлений).
3. Содействовать формированию внутренних ресурсов, способных в максимальной степени обеспечить технологическую независимость, информационную безопасность

и выстроить цифровой суверенитет России. Целесообразно межведомственно консолидировать усилия, в том числе, в части подготовки квалифицированных кадров, четко понимающих задачи, стоящие перед государством, способных реализовать имеющийся в стране научно-технический потенциал.

4. Через АНО «Центр по глобальной ИТ-кооперации» всем заинтересованным российским экспертам внести свой вклад в выработку консолидированной позиции в проект Глобального цифрового договора (инициатива Генсека ООН) до завершения срока открытых консультаций - 30 апреля 2023 года.
5. С целью продвижения отечественных технологий на рынках дружественных стран целесообразно рассмотреть возможность создания «единого окна» для обеспечения взаимодействия с соответствующими министерствами (МИД, Минпромторг, Минцифры). Российские производители готовы предложить множество зрелых и уникальных решений, востребованных за рубежом (решения в области информационной безопасности, финансовой сферы, офисного ПО, инженерного ПО, логистики и других), целесообразно развивать кредитование зарубежных заказчиков, поддерживать, а там, где это нужно, создавать компании-интеграторы для внедрения как отдельных российских решений, так платформенных решений (общесистемного и прикладного ПО).

В рамках круглого стола № 6 **«Актуальные задачи операторских компаний связи по обеспечению ИБ и пути их решения»** обсуждались вопросы обеспечения безопасности объектов критической информационной инфраструктуры сети связи общего пользования и импортозамещения средств защиты информации в отрасли ИКТ.

На заседании круглого стола сформулированы следующие предложения:

1. Устранить противоречие между требованиями к безопасности объектов КИИ и необходимостью обеспечить функциональную устойчивость и развитие сети связи общего пользования.
2. В целях повышения уровня защищенности КИИ РФ и обеспечения функциональной устойчивости и развития ССОП целесообразно изменить парадигму отнесения объектов к КИИ в сторону усиления защиты объектов КИИ, которые используются при управлении критически важными объектами (далее – КВО) с высоким потенциальным ущербом из-за нарушения их функционирования, и снижения количества объектов относимых к КИИ, если не создаются высокие риски техногенных, экологических и других катастрофических последствий из-за их отказа; в частности, предлагается:
    - установить требование к построению объектов КИИ 1 категории значимости только с «закрытой» архитектурой, с использованием российского программно-аппаратного обеспечения и без подключения к ССОП; в случае необходимости подключения объектов КИИ к ССОП (например, из-за невозможности исключения иностранной технической поддержки) установить специальные требования к защите и контролю взаимодействия (2 категория значимости); 3 категорию значимости целесообразно устанавливать для объектов КИИ с высокими рисками, но которые могут функционировать только с «открытой» архитектурой и должны использовать ССОП, например, для автоматизированных систем управления беспилотным транспортом, для систем, предоставляющих государственные электронные услуги и т.п.;

- установить в НПА единую шкалу оценки потенциального ущерба на основе методических подходов МЧС России, использовать эту шкалу в качестве критерия для отнесения объектов управления КВО к объектам КИИ;
- внести изменения в Постановление Правительства РФ от 08.02.2018 № 127, исключить социальные, экономические и иные критерии отнесения объектов к КИИ, если из-за отказа объекта управления не наносится критический ущерб КВО и функционирование может быть восстановлено в установленные нормативами сроки, например, исключить из КИИ некоторые объекты ССОП.

3. Разрабатывать информационные технологии с изначально безопасной архитектурой («secure by design»), которая позволит обеспечить высокий уровень доверия пользователей к программно-аппаратному обеспечению, в том числе за счет исключения недекларированных функций, позволяющих производителям и возможным нарушителям безопасности получать несанкционированный доступ к информации.

В рамках круглого стола № 7 **«Роль и место Отраслевого центра ГосСОПКА отрасли связи для повышения безопасности информации операторов мобильной связи»** обсуждались вопросы взаимодействия между операторами мобильной связи, регуляторами и разработчиками средств ГосСОПКА с целью подготовки и сопровождения продвижения обобщенных предложений отрасли связи по совершенствованию нормативного, организационного и методического обеспечения функционирования ГосСОПКА на объектах мобильной связи.

На заседании круглого стола сформулированы следующие предложения:

1. Необходимо распространять лучшие практики и применять рекомендации для сохранения надлежащего уровня предупреждения, выявления и блокирования атак через сигнальные сети на стороне оператора связи:
   - своевременно оценивать эффективность инструментов выявления атак через сигнальные сети;
   - SS7 и Diameter, что позволяет своевременно обнаруживать атаки на отдельных абонентов мобильной связи и инфраструктуру оператора;
   - проводить периодические внешние аудиты безопасности сигнальных сетей;
   - в случае выявления уязвимых мест, оперативно осуществлять модернизацию настроек телекоммуникационного оборудования, например, запрещать сигнальные сообщения, которые не используются для организации связи между операторами, но могут применяться при проведении атак на сети операторов связи;
   - отрабатывать процедуры с применением инструментов безопасности, позволяющих оперативно блокировать атаки через сигнальные сети;
   - регулярно проводить киберучения с целью проверки уровня защищенности сигнальных сетей.
2. Целесообразно рассмотреть возможность создания в Российской Федерации нормативной базы и единой системы сбора и аналитической обработки информации об атаках через сигнальные сети на инфраструктуру и абонентов мобильных операторов связи, а также подключение ее к ГосСОПКА.
3. Целесообразно распределить компетенции по специализированным отраслевым центрам, которые занимались бы мониторингом в рамках своего направления.

В рамках круглого стола № 8 **«Базовая кафедра АДЭ: возможности компаний по эффективному увеличению своего интеллектуального капитала»** обсуждались вопросы функционирования базовой кафедры АДЭ «Технологии электронного обмена данными» в Московском университете связи и информатики, а также научные и исследовательские направления, в которых принимают участие сотрудники и обучающиеся кафедры.

Участниками заседания отмечено, что базовая кафедра АДЭ – уникальная образовательная среда, в которой студенты получают знания от преподавателей-экспертов отрасли. Более 400 студентов ежегодно проходят обучение по дисциплинам кафедры. В соответствии с Постановлением Правительства №1632 от 27 сентября 2021 года Ассоциации документальной электросвязи выделена субсидия в целях осуществления подготовки специалистов, обладающих знаниями и умениями, необходимыми для представления интересов Российской Федерации в основных международных организациях, занимающихся развитием инфраструктуры информационно-коммуникационных технология и обеспечением доверия и безопасности при её использовании. В рамках реализации мероприятия на кафедре созданы уникальные учебно-исследовательские лаборатории по развитию ИКТ-инфраструктуры и обеспечению доверия и безопасности при ее использовании, базирующиеся на отечественных программно-аппаратных средствах.

В период с 21 по 24 февраля текущего года студенты второго курса магистерской программы по профилю подготовки «Информационная культура цифровой трансформации» под руководством и.о. заведующего базовой кафедрой АДЭ «Технологии электронного обмена данными» (ТЭОД) в МТУСИ Милашевского Игоря Анатольевича приняли участие в заседании Исследовательской комиссии 17 «Безопасность» сектора Стандартизации Международного Союза Электросвязи (МСЭ) в составе делегации Администрации связи Российской Федерации, получив практический опыт представления и защиты российских интересов на международной площадке.

Кафедра принимает активное участие в научных исследованиях, в том числе и в рамках Академии программирования для архитектуры «Эльбрус», образованной АДЭ, МЦСТ и ИВК. Сотрудники, совместно с магистрами и аспирантами кафедры, участвуют в создании новой учебной дисциплины «Инфраструктура создания ПО для отечественных архитектур микропроцессоров» и подготовке материалов по системе безопасных вычислений.

Базовая кафедра АДЭ приглашает всех заинтересованных членов ассоциации к совместному участию в подготовке профессиональных и востребованных кадров для отрасли.