Итоговый документ
22-й ежегодной конференции
«Состояние и перспективы развития ИКТ-инфраструктуры»

12-13 октября 2022 года

12-13 октября 2022 года в Москве состоялась 22-я ежегодная конференция «Состояние и перспективы развития ИКТ-инфраструктуры», организованная общественно-государственным объединением «Ассоциация документальной электросвязи».

В конференции приняли участие представители федеральных органов государственной власти, поставщиков и производителей оборудования, операторов связи, контент-провайдеров, регистраторов и студенты профильных вузов России.

Более 150 участников конференции обсуждали вопросы совершенствования нормативной правовой базы цифрового развития, обеспечения технологической независимости, вопросы качества услуг связи и других тем области ИКТ-инфраструктуры.

В программу конференции были включены заседания по актуальным направлениям развития ИКТ-инфраструктуры, в разработке и реализации которых участвует общественно-государственное объединение «Ассоциация документальной электросвязи».

Конференция включала в себя 8 заседаний (круглых столов).

Конференцию открыл ведущий первого круглого стола **«Правовое и техническое регулирование развития ИКТ-инфраструктуры»** В.А. Кутуков - заместитель Председателя Исполкома АДЭ, генеральный директор компании АО «Стек Софт», который торжественно поприветствовал всех участников мероприятия и поблагодарил партнеров конференции.

Представитель Администрации Президента Российской Федерации Т.В. Матвеева рассказала об актуальности проблемы сфабрикованного аудиовизуального контента.

Особое внимание было уделено широкому распространению технологии DeepFake в рамках текущих информационных войн, ее активного использования для влияния на пользователей. Татьяна Владимировна отметила приоритетное направление для решения данной проблемы – изучение возможности анализа подобного контента и дальнейшего выявления измененного материала.

Заместитель Министра промышленности и торговли Российской Федерации В.В. Шпак отметил, что в рамках реализации Постановления Правительства РФ от 23 августа 2021 г. № 1380 («Об утверждении Правил предоставления субсидий из федерального бюджета российским организациям на финансовое обеспечение части затрат на разработку конкурентоспособных нишевых аппаратно-программных комплексов для целей искусственного интеллекта») и Постановления Правительства РФ от 24 июля 2021 г. № 1252 («Об утверждении Правил предоставления из федерального бюджета субсидий российским организациям на финансовое обеспечение части затрат на создание электронной компонентной базы и модулей») ведутся активные работы для обеспечения надежной основы импортонезависимости в отрасли связи и ИКТ-инфраструктуры.

Представитель ФСБ России А.И. Самойлов отметил важность создания российского репозитория программных пакетов и библиотек, одной из основополагающих целей которого является формирование условий устойчивого развития отечественной отрасли информационных и телекоммуникационных технологий, а также обеспечение целостности,

безопасности и устойчивости функционирования объектов критической информационной инфраструктуры Российской Федерации (далее – КИИ), включая объекты военного и государственного управления. Он добавил, что остро стоит вопрос создания высококвалифицированной кадровой базы, способной ставить перед собой амбициозные задачи по решению актуальных проблем в области информационных технологий. Одним из путей достижения данной цели является реализация базовой кафедрой АДЭ при МТУСИ программы профессиональной переподготовки «Информационная культура цифровой трансформации». В рамках обучения по этой программе осуществляется подготовка всесторонне развитых специалистов, способных применять в своей дальнейшей работе знания в сферах технологического развития ИКТ-инфраструктуры и обеспечения доверия и безопасности при ее использовании, а также обладающих знаниями и умениями, необходимыми для представления интересов Российской Федерации в основных международных организациях, занимающихся развитием инфраструктуры информационно-коммуникационных технологий и обеспечением доверия и безопасности при ее использовании.

Директор Департамента развития облачных сервисов и управления данными Минцифры России П.И. Бурлаков сделал доклад о реализации проекта облачного хранилища – ГосОблако, анонсировал переход государственных и муниципальных органов на единую систему хранения данных. Петр Игоревич отметил заявленные показатели: качества услуг - 100%; доступности - 99,9%.

Представитель Администрации Президента Российской Федерации В.А. Костеев отметил необходимость регулирования контента. На основании Федерального закона «Об информации, информационных технологиях и о защите информации» от 27.07.2006 № 149-ФЗ социальные сети и медиаплощадки обязаны самостоятельно мониторить контент на наличие противоправной информации (149-ФЗ, статья 10). В свою очередь, определение запрещенной информации дано в статье 15 данного ФЗ. Выступающий подчеркнул, что не соблюдение закона влечет за собой ограничение доступа к площадке по размещению контента.

В.А. Костеев отметил, что на сегодня актуально следующее:

- остро встал вопрос допуска на рынок легального контента (в связи с отзывом лицензий на легальный контент альтернатива останется только за пиратством, что является нежелательным);
- борьба с пиратством, разработка методов борьбы с ним (особо остро стоит вопрос распространения заказной противоправной информации на пиратских сервисах);
- внесение изменений в законодательство об обязательном ведении организациями официальных страниц в социальных сетях;
- развитие закона о форме обратной связи для своевременного реагирования и ответа на обращения к регуляторам в сети «Интернет».

Генеральный директор АО «Глонасс» И.А. Милашевский рассказал, что компания уделяет особое внимание построению общего пространства доверия, отметив большое значение обеспечения доверия при использовании ИКТ. АО «Глонасс» - оператор государственной информационной системы «ЭРА-ГЛОНАСС» с защищённой сетью связи, которая обеспечивает максимальное покрытие. Сегодня в системе зарегистрировано свыше 9 миллионов абонентов. «Среди них нет ни одного физического лица, это все материальные, подвижные объекты, транспортные средства», - добавил Игорь Анатольевич.

Заместитель Министра цифрового развития, связи и массовых коммуникаций Российской Федерации А.М. Шойтов обратился к участникам конференции и пожелал им продуктивной работы, отметив важность разработки и использования в ИТ-индустрии доверенной среды, которую необходимо активно распространять.

В рамках круглого стола № 2 **«Стратегия создания российского репозитория программных пакетов и библиотек»** 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.

Представленные доклады как нельзя вовремя охарактеризовали состояние развития отечественной отрасли информационных технологий в контексте ее способности обеспечить технологическую независимость объектов КИИ. Выступления касались как собственно методологического подхода к созданию отечественного репозитория для сборки технологически независимых отечественных программных продуктов, так и предложений по использованию уже существующей инфраструктуры для безопасной разработки программ и программных пакетов в отечественной инфраструктуре разработки - репозитории СИЗИФ. Как возможный вариант программного пакета для включения в отечественный репозиторий была представлена отечественная система управления базами данных «Глобал». Система«Глобал» была позиционирована в качестве возможной для использования в виде отечественной платформы для хранения больших объемов данных для широкого профиля информационных систем, в том числе и для информационных систем транзакционного типа. Участники круглого стола отметили необходимость создания экосистемы прикладного и системного ПО на базе архитектуры процессора «Эльбрус».

На круглом столе № 3 **«Российский сегмент сети Интернет»** обсуждались вопросы поддержки и администрирования корневого пространства доменных имен, безопасности и надежности доменной инфраструктуры российского сегмента сети Интернет, а также вопросы связности сети, устойчивости и её безопасности в новых условиях. Также в ходе круглого стола рассматривались современные проблемы и вызовы Рунета, а также пути для их решения.

В рамках круглого стола было отмечено, что каждый день в сеть заходят почти 90 миллионов россиян. Для обеспечения непрерывности, безопасности и повышения надежности российского сегмента сети Интернет по результатам обсуждений сформированы следующие предложения:

1. Российская интернет-инфраструктура находится в критической зависимости от зарубежных центров сертификации. Данная проблема касается в том числе и TLS-сертификатов, и сертификатов для электронной почты, и сертификатов для подписи кода. Для решения этой проблемы предлагается создать в России распределенную систему, включающую в себя не один государственный, а несколько корневых центров сертификации, так как это позволит повысить отказоустойчивость и надежность всей системы.

   На текущий момент в России существует два центра сертификации: Национальный удостоверяющий центр при Минцифры и Центр сертификации ТЦИ. Центр сертификации ТЦИ позволяет выпускать TLS-сертификаты как ECDSA, так и ГОСТ, а также S/MIME-сертификаты для электронной почты. В настоящий момент ведутся работы над функционалом по выпуску сертификатов для подписи кода и созданием корпоративного центра сертификации.

2. АО «РСИЦ» (RU-CENTER) совместно с КЦ, Минцифры России, ФСБ России и другими ведомствами участвует в пилотном проекте по подключению информационной системы регистратора к ЕСИА для идентификации администраторов. В настоящий момент АО «РСИЦ» получило сертификат от УЦ НИИ «Восход» для подключения к ЕСИА и перешло к этапу опытно-промышленной эксплуатации. Координационный центр предложил на основании опыта АО «РСИЦ» по подключению ИС регистратора к ЕСИА использовать наработки АО «РСИЦ» в качестве основы для методологических материалов по подключению регистраторов. АО «РСИЦ» готово предоставить все необходимые сведения и собственные шаблоны, не составляющие коммерческую и служебную тайну, по запросам заинтересованных органов и компаний. Основные этапы подключения информационной системы АО «РСИЦ» (RU-CENTER) к ЕСИА:
    - актуализация модели угроз и её согласование с ФСБ России;
    - получение одобрений регуляторов для подключения к ЕСИА;
    - организация защиты персональных данных с применением криптографических средств;
    - организация защищенного канала до ЕСИА и инфраструктуры работы с цифровой подписью класса КВ2.
3. КЦ предлагает в рамках НИР КЦ совместно с уполномоченными компетентными организациями продолжить исследования, направленные на изучение методик проактивного подхода выявления вредоносных регистраций доменных имен.

В рамках круглого стола № 4 **«Процедурные и технологические меры по созданию новых каналов распространения информации»** обсуждались: организационные и технические меры по импортозамещению контента в сети Интернет, новые каналы распространения информации; современные технологии генерации фейков и противодействие им; поддержка отечественных интернет-технологий.

Начальник Управления контроля и надзора в сфере электронных коммуникаций Роскомнадзора Е.Ю. Зайцев сообщил, что на сегодняшний день приобретают знаковость деструктивные формы информационного воздействия на российских граждан для дестабилизации обстановки внутри страны. Мониторинг РКН фиксирует возросшее количество деструктивного и противоправного контента. Также идет прямое воздействие на традиционные ценности граждан России с целью разложения моральных основ общества. РКН ведет активную борьбу с нелегальным контентом, уже зафиксировано и заблокировано свыше 85 тыс. сайтов, распространявших запрещенную информацию. Касательно иностранных крупных компаний также принимались меры по удалению материалов, нарушающих законодательство Российской Федерации. Все подобные действия по блокировкам были вынужденной мерой в связи с нежеланием зарубежных компаний самостоятельно модерировать контент.

Участниками круглого стола были рассмотрены проблемы влияния пограничного и деструктивного контента, а также способы противодействия его распространению. Так, например, С.П. Маклаков отметил важность систематического повышения уровня медиаграмотности и развития навыков критического мышления среди населения. В качестве способов борьбы прозвучало предложение о маркировке потенциально опасного контента и фейковых новостей. Чтобы популяризировать борьбу с фейками и повышение уровня медиаграмотности, АНО «Диалог Регионы» запустила первую в России фактчекинговую платформу «Лапша». В рамках проекта любой желающий может отправить на проверку

команде профессиональных фактчекеров сомнительную информацию. В.В. Ампелонский в своей речи поведал о влиянии деструктивного контента на молодежь и детей. Объем знаний ребенка об окружающем мире не позволяет ему критически оценивать ту информацию, которая поступает через различные медийные каналы. Помочь обезопасить информационную среду могут общественные организации и экспертные комиссии, которые производят мониторинг и фильтрацию поступающей информации в Сеть. Немаловажную проблему в сфере развлекательного контента отметила С.Т. Митрофанова. Индустрия столкнулась с отсутствием качественных иностранных фильмов и сериалов при условии малого количества отечественных. Работа в этом направлении осложняется оттоком работников индустрии, способных производить качественный контент.

В рамках круглого стола № 5 «**Развитие инфраструктуры программирования для отечественных архитектур микропроцессоров»** обсуждались вопросы оказания научной, технологической, организационной, методологической и образовательной поддержки в создании и развитии инфраструктуры разработки и внедрения ПО для отечественных архитектур микропроцессоров.

На заседании экспертами АДЭ было анонсировано создание консультационных материалов по теме «Особенности разработки программного обеспечения для процессоров Эльбрус и вычислительных комплексов на базе процессоров Эльбрус», на основе которых будет разработана новая учебная дисциплина «Инфраструктура разработки отечественного программного обеспечения», предназначенная для студентов бакалавриата 3 и 4 курсов. Данный проект призван обеспечить подготовку кадров, которые будут способны самостоятельно разрабатывать, портировать, оптимизировать и тестировать отечественное ПО.

В дискуссиях на круглом столе были подняты текущие проблемы, вызовы и способы их преодоления, которые стоят перед специалистами в области создания отечественного программного и аппаратного обеспечения.

На круглом столе № **6 «Обеспечение качества инфокоммуникационных сервисов»** были представлены доклады о перспективных решениях по обеспечению качества инфокоммуникационных сервисов.

Отмечено, что требования к обеспечению QoS (Quality of Service, качество обслуживания) в сети связи должны быть стандартизованы на всем протяжении сетевого соединения и учитываться разработчиком информационных услуг. Показатели качества услуги/сервиса должны учитывать реальные ценности абонента/пользователя.

В ходе круглого стола был представлен проект «ЛИНКМЕТР» - комплекс продуктов по измерению характеристик каналов связи сетей передачи данных. Продукт разработан в целях замещения импортных решений (Ookla SpeedTest).

В ходе дискуссий были озвучены следующие предложения:

- провести исследования целесообразности и необходимости создания в ГСОЕИ РФ группы исходных эталонов единиц величин для Минцифры России, что позволит с заданной погрешностью формировать, хранить и передавать объем данных (информации), а также в последующем получать эталонные скорости передачи и другие производные величины;

- повысить доверие к средствам обеспечения качества инфокоммуникационных сервисов, которые должны подтверждаться на основании процедур сертификации;
- актуализировать описание содержания услуг ИКТ, включая их перечень;
- синхронизировать наименования и содержание услуг во всех нормативных правовых и нормативных документах, в дальнейшем использовать при разработке иных документов.

В дискуссии приняли участие Бабкин В.А., МТС; Викулин В.Н., Трилайн; Горкавенко Д.В., КС ЦОД; Еременко В.А., МТС; Кондрашов С.Ф., ТК 480; Мальянов С.А., Вымпелком; Одинцов Д.В., Труконф.

На заседании круглого стола № 7 **«Практика реализации указов Президента №166 и №250»** рассматривался практический опыт обеспечения технологической независимости и безопасности информационной инфраструктуры Российской Федерации в соответствии с указами Президента от 30.03.2022 № 166 и от 01.05.2022 № 250.

Актуальность импортозамещения и обеспечение информационной безопасности в последнее время не только возросла, но и практически оказалась первостепенной задачей. В результате исполнения рассматриваемых указов возникли различные результаты и взгляды к подходу по их реализации. Была обозначена возможная проблема: категорирование всей инфраструктуры целиком, как объект КИИ, что привело к требованию реализации на всех уровнях вплоть до конкретного устройства. Каждый мелкий элемент был назван самостоятельным объектом КИИ, для которого необходимо всё разработать и защищать его следует отдельно. Этот процесс весьма дорогой и неудобный.

Краеугольным камнем обсуждения стала ответственность за обеспечение информационной безопасности, возлагаемая на организации. Участники круглого стола подчеркнули важность распределения ответственности между ведомствами во избежание ее перекладывания и возникновения финансовых и репутационных рисков.

В целях обеспечения импортонезависимости предлагается участие и ведение на региональном уровне совместных проектов, что связано с изоляцией страны от крупных международных ИТ-площадок. Предлагается региональным органам исполнительной власти рассмотреть в сфере импортозамещения единые проекты в сфере связи, взамен большого количества разрозненных нормативных документов.

В рамках круглого стола № 8 **«Базовый уровень информационной безопасности операторов связи»** обсуждались вопросы обеспечения СОРМ, безопасности КИИ, противодействия вредоносному ПО, устойчивости функционирования ССОП, взаимодействия с 17-ой Исследовательской комиссией МСЭ-Т и иные вопросы по данной тематике.

В ходе докладов были отмечены ключевые риски и зафиксированные инциденты безопасности опорных сетей мобильных операторов. В их числе:

- отказ в обслуживании - неработоспособность сети и отдельных сервисов;
- отключение от сети и сервисов отдельных абонентов и групп абонентов;
- перехват пользовательского трафика - голосовых вызовов и SMS;
- компрометация персональных данных и «цифровой личности» абонентов, в т.ч. публичных персон и государственных служащих;
- получение данных о местоположении абонента, статистики его звонков и т.д.;

- кража денег со счетов абонентов и у оператора.

Было также подчеркнуто, что отсутствие адекватного реагирования на возросшие угрозы безопасности может привести к массовой реализации инцидентов, связанных с нарушением работоспособности опорной сети и компрометацией данных абонентов.

Прозвучало предложение о том, что в Российской Федерации необходимо создание 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.

Специалистами «Лаборатории Касперского» была затронута тема защищенности корпоративных систем и представлена актуальная статистика киберугроз бизнеса. В качестве их профилактики предложено следующие:

- регулярно работать с пользователями, персоналом;
- ввести или актуализировать сегментацию (ограничить доверительные отношения между доменами, усилить по возможности их изоляцию), использовать минимально необходимый набор портов и протоколов для сетевого обмена;
- ввести двухфакторную аутентификацию для доступа к конфиденциальной информации и критически важным системам;
- при необходимости удалённого доступа между сетевыми сегментами организовывать демилитаризованные зоны (DMZ), а сам удалённый доступ осуществлять через терминальные серверы;
- разработать и внедрить политику резервного копирования.

Более подробно с материалами мероприятия можно ознакомиться на сайте: https://ict22.rans.ru

Мероприятие состоялось при поддержке организаций-членов АДЭ.

Генеральные партнеры

НОРСИ-ТРАНС Закрытое акционерное общество

Специальные технологии

Координационный центр доменов .RU/.РФ

Партнеры конференции

АО ГЛОНАСС

ONYMA

TrueConf

Партнеры заседаний

infotecs

base alt

ROSA