Итоговый документ
23-й ежегодной конференции
«Обеспечение доверия и безопасности при использовании ИКТ»

02-03 апреля 2025 года

02-03 апреля 2025 года в Москве состоялась 23-я ежегодная конференция «Обеспечение доверия и безопасности при использовании ИКТ», организованная общественно-государственным объединением «Ассоциация документальной электросвязи» (далее – АДЭ).

В работе конференции приняли участие более 150 специалистов, представляющих органы государственной власти, операторские компании связи, разработчиков средств и оборудования связи и информационной безопасности, контент-провайдеров, регистраторов, а также преподаватели и студенты профильных вузов. АДЭ выражает благодарность составу программного комитета, который сгруппировал основные направления деятельности АДЭ в сфере обеспечения доверия и безопасности при использовании ИКТ в 9 тематических круглых столах, в рамках которых с докладами и предложениями выступили более 50 экспертов.

Конференцию открыл председатель Исполнительного комитета АДЭ А.В. Иванюк, ведущий первого круглого стола **«Приоритетные задачи нормативного регулирования отрасли ИКТ»**. В обращении к участникам мероприятия ведущий поблагодарил организации, оказавшие партнерскую поддержку конференции. На заседании руководители органов государственной власти и бизнес-компаний обсуждали актуальные задачи нормативного правового и нормативного технического регулирования обеспечения доверия и безопасности при использовании ИКТ.

Ведущий: Иванюк А.В., АДЭ.
Выступили: Гореславский А.С., ИРИ; Ивашко А.М., ФСБ России; Ковалев О.В., Роскомнадзор; Мицкевич Ф.В., Минэнерго России; Сизоненко Г.Е., ИВК; Торбенко Е.Б., ФСТЭК России; Шойтов А.М., Минцифры России.

На заседании круглого стола сформулированы следующие предложения:

1. В рамках реализации перспективных задач Минцифры России включить отдельные инициативы со стороны отрасли ИКТ по вопросам противодействия мошенничеству в работу профильных комитетов и рабочих групп АДЭ.
2. Проработать предложение о создании на базе АДЭ отраслевого Полигона доверенных решений для КИИ в отрасли связи, с учетом принятия необходимых мер по обеспечению информационной безопасности и целостности их функционирования с использованием отечественной криптографии, определить готовность участия в работе Полигона профильных организаций из числа членов АДЭ.
3. Поддержать деятельность АДЭ по организации сотрудничества и взаимодействия органов государственной власти, отраслевого сообщества и бизнеса по актуальным вопросам нормативного регулирования отрасли ИКТ.
4. При координирующей роли государства и участии профильных Регуляторов для обеспечения технологической независимости Российской Федерации в рамках деятельности АДЭ оказать содействие в продвижении российских ИКТ-решений, в том числе на зарубежные рынки.

В рамках круглого стола № 2 **«Актуальные вопросы категорирования объектов КИИ отрасли ИКТ»** обсуждались вопросы совершенствования и реализации подготовленных рабочей группой АДЭ документов по категорированию и обеспечению безопасности объектов КИИ в отрасли связи, обеспечения технологической независимости и ключевые аспекты перехода на доверенные программно-аппаратные комплексы (ПАК) на значимых объектах КИИ.

Ведущая: Торбенко Е.Б., ФСТЭК России.
Выступили: Раевский А.Н., НКЦКИ; Рудзик А.С., Минцифры России; Савельев М.С., Ростелеком; Генгринович Е.Л., ИнфоТеКС.

Представитель ФСТЭК России Е.Б. Торбенко представила результаты реализации требований по обеспечению безопасности критической информационной инфраструктуры (КИИ), сделав акцент на отрасли связи. Е.Б. Торбенко отметила заметный прогресс в части категорирования объектов и поддержания актуальности сведений о них, а также отметила наличие системных вопросов, требующих решения: многие отраслевые организации по-прежнему не выполняют в полной мере требования законодательства, допускают нарушения при обеспечении защиты объектов, включая использование незащищённых каналов удалённого доступа и эксплуатацию уязвимых средств защиты информации. Участникам конференции была доведена информация о готовящихся изменениях в нормативно-правовую базу, которые должны упростить процедуру категорирования за счёт введения типового перечня объектов КИИ и документов об отраслевых особенностях категорирования, а также было сообщено о согласовании подготовленных рабочей группой АДЭ Методических указаний по категорированию объектов критической информационной инфраструктуры, принадлежащих субъектам критической информационной инфраструктуры, осуществляющим деятельность в отрасли связи. Е.Б. Торбенко подчеркнула необходимость усиления контроля за деятельностью подрядчиков, оперативного устранения выявляемых недостатков до момента проведения проверок, отметив важную роль АДЭ во взаимодействии между бизнесом и регуляторами.

Представитель НКЦКИ А.Н. Раевский подвёл итоги 9-летнего применения федерального закона «О безопасности критической информационной инфраструктуры Российской Федерации» от 26.07.2017 №187 (далее – №187-ФЗ) и отметил ключевую роль этого закона в повышении устойчивости функционирования КИИ. А.Н. Раевский сообщил, что накопленный опыт частично учли в новых нормативных актах, включая Указ Президента Российской Федерации «О дополнительных мерах по обеспечению информационной безопасности Российской Федерации» от 01.05.2022 г. №250. А.Н. Раевский уделил особое внимание мониторингу защищённости, а также пояснил, что организации обязаны предоставлять данные о своих сетевых ресурсах для удалённого анализа и очных проверок. Представитель НКЦКИ отметил системную проблему с безопасностью подрядчиков, подчеркнув, что их уязвимости часто становились причиной инцидентов, и анонсировал планы по законодательному закреплению требований к их защищённости. Также А.Н. Раевский рассказал о готовящихся изменениях в №187-ФЗ, которые обяжут субъекты КИИ сообщать не только об инцидентах, но и о компьютерных атаках.

Представитель Минцифры России А.С. Рудзик рассказала о работе министерства по обеспечению безопасности объектов критической информационной инфраструктуры в сфере связи. Выступающая подчеркнула, что все операторы связи относятся к субъектам КИИ и обязаны соблюдать соответствующие требования законодательства. А.С. Рудзик сообщила, что Минцифры России проводит мониторинг предоставления организациями актуальных

данных о категорировании объектов КИИ, а также оказывает им методическую поддержку. В выступлении отмечено, что, основываясь на результатах проведенного мониторинга за 2024 год, 67% поступивших ответов и предоставленных данных указывают на возможные нарушения законодательства в области безопасности КИИ, и всего 33% показали положительный результат. По итогам мониторинга были выявлены типичные нарушения: отсутствие комиссий по категорированию; случаи, когда организации, имеющие лицензию на деятельность в сфере связи, заявляют, что не осуществляют её в качестве основного или дополнительного вида деятельности, то есть не рассматривают объекты применительно к отрасли связи; отсутствие актов категорирования. Для решения этих проблем Минцифры России совместно с ФСТЭК России и АДЭ разработало перечень типовых объектов КИИ в сфере связи, а также ведёт работу по утверждению проекта приказа «Об утверждении порядка проведения в отношении субъектов КИИ в сфере связи оценки актуальности и достоверности сведений о категорировании объектов КИИ». В заключение А.С. Рудзик сообщила о планах по скорому утверждению методических указаний по категорированию.

М.С. Савельев, представитель Ростелекома и рабочей группы АДЭ по КИИ, поделился практическим опытом в области обеспечения информационной безопасности и призвал операторов связи активнее участвовать в деятельности рабочих групп АДЭ. Выступающий подробно остановился на методологических подходах к категорированию объектов КИИ, подчеркнув опасность формального следования отраслевому перечню без анализа реального влияния систем на оказание услуг.

Е.Л. Генгринович, представитель ИнфоТеКС, обратил внимание слушателей на важность учета информационных угроз при расследовании технологических аварий, отметив, что современные системы требуют принципиально новых подходов к обеспечению надежности. Выступающий подчеркнул, что интеграция промышленных и корпоративных систем создает новые уязвимости, а традиционные методы оценки рисков в таких случаях становятся неэффективными, и сообщил о необходимости проектирования систем с учетом возможных компьютерных атак, включая применение встроенных механизмов защиты и оперативного реагирования.

На заседании круглого стола сформулированы следующие предложения:

1. Субъектам КИИ в рамках обеспечения безопасности объектов КИИ усилить контроль выполнения требований по безопасности подрядчиками, с которыми осуществляется взаимодействие.
2. Поддержать деятельность АДЭ по организации сотрудничества и взаимодействия органов государственной власти и отраслевого сообщества по актуальным вопросам категорирования объектов КИИ отрасли ИКТ в рамках профильных рабочих групп.
3. Рассмотреть возможность разработки отдельных требований, регламентирующих обеспечение надежности, защищенности, устойчивости и безопасности при развитии функциональности систем, на которые отрасль планирует переход в процессе импортозамещения.

В рамках круглого стола № 3 **«Роль и место надзорной и разрешительной деятельности в области связи в обеспечении доверия»** обсуждались вопросы обеспечения безопасности и устойчивости российского сегмента сети «Интернет» и взаимодействия с отраслью: проблематика и практика взаимодействия с операторами связи, провайдерами хостинга и иными лицами (участниками централизованного управления).

Ведущий: Глазунов Д.В., ГРЧЦ.

Выступили: Шорохов О.С., ГРЧЦ; Диянский О.В., ГРЧЦ; Панышев Д.О., ЦХД (Ростелеком-ЦОД).

Ведущий круглого стола довел до участников конференции основные задачи Центра мониторинга и управления сетью связи общего пользования (ЦМУ ССОП), и рассказал о ключевых системах этого центра. Д.В. Глазунов поделился со слушателями статистикой работы национальной системы противодействия DDoS-атакам за 2024 год и статистикой применения национальной системы доменных имён (НСДИ), отметив востребованность хостинг-провайдеров в НСДИ во время атак на их DNS-сервера.

О.С. Шорохов подробно рассказал о реестре провайдеров хостинга и обратил внимание на необходимость соблюдения новых требований, предусматривающих использование данных GeoIP (система учета географической принадлежности IP-адресов) о местоположении сетевых адресов. Выступающий отметил, что ряд компаний до сих пор игнорирует эти требования, даже несмотря на наличие информации, предоставляемой ЦМУ ССОП.

Д.О. Панышев в своем выступлении подчеркнул важность совершенствования регулирования в сфере хостинговых услуг. Он отметил, что для развития отрасли необходимо уточнить понятийный аппарат в законодательстве, оптимизировать систему реестрового учета и выработать эффективные механизмы взаимодействия между участниками рынка. Выступающий отметил проблематику, связанную с определением термина «провайдер хостинга». Одной из проблем является дублирование информации в реестре: определение «провайдер хостинга», приведенное в Федеральном законе «Об информации, информационных технологиях и о защите информации» от 27.07.2006 №149, позволяет отнести к ним не только владельцев вычислительных мощностей, но и лиц, которые занимаются их перепродажей. В процессе оказания услуг одна организация (первичный поставщик) реализует услуги хостинга, которые затем перепродаются другой организацией (вторичный поставщик). В результате обе организации подлежат регистрации в Реестре и должны исполнять требования, предусмотренные законодательством. Так как обе организации функционируют на одной и той же инфраструктуре, то происходит дублирование, а возможно и многократного повторение сведений в Реестре, что приводит к излишнему административному бремени для субъектов бизнеса (включение в Реестр накладывает определенные требования на провайдеров), но и затрудняет мониторинг и регулирование данного сегмента рынка. Отдельно Д.О. Панышев выделил и техническую проблему использования данного определения: другой особенностью установленного регулирования является ситуация, когда провайдер облачной услуги, предоставляющий инфраструктуру для размещения государственной информационной системы (ГИС), включенный в Перечень провайдеров хостинга для ГИС, обязан предоставлять сведения (контентная информация), которой владеет исключительно сам владелец ГИС, а провайдер не имеет доступа к ней, что затрудняет выполнение требований по оперативно-разыскным мероприятиям.

На заседании круглого стола сформулированы следующие предложения:

1. На площадке АДЭ продолжить обсуждение вопросов, касающихся совершенствования регулирования в сфере хостинговых услуг, с участием заинтересованных сторон для выработки сбалансированных решений.
2. Провести анализ целесообразности уточнения понятия «провайдер хостинга» в Федеральном законе «Об информации, информационных технологиях и о защите информации» от 27.07.2006 №149.

В рамках круглого стола № 4 **«Безопасность разработки, распространения и использования контента»** обсуждалось развитие технологий создания контента с использованием ИИ в креативных индустриях, их влияние на искусство и культуру, вопросы авторских прав, персонализации контента и регулирования дипфейков, а также роль России в международных проектах и регулировании использования ИИ в контенте.

Ведущий: Буньков А.В., ИРИ.
Выступили: Полянчинков И.Н., МТС; Хренов С.Н., МегаФон; Бурцева Ж.С., Т2 Мобайл; Алферов П.В., ВымпелКом; Велигодский С.С., Сбербанк.

Участники круглого стола отметили, что, продолжая рассмотрение вопросов обеспечения когнитивной независимости развития общества и государства в Российской Федерации, необходимо создание среды для развития отечественных платформ и производителей контента. Это позволит обеспечивать сохранение и трансляцию следующим поколениям традиционных ценностей, национальной культуры и истории, создать безопасное, содействующее личностному и общественному развитию информационное пространство для всех россиян.

В части существующей проблематики в сфере контента, генерируемого с применением искусственного интеллекта (ИИ) участники отметили его важное место во многих индустриях, таких как кинопроизводство, разработка видеоигр, анимация, социальные сервисы и многих других, в которых он используется для позитивных целей. В связи с этим необходимо соблюсти баланс между защитой от рисков, связанных с дипфейками, и поощрением законного использования контента, генерируемого с применением ИИ.

На заседании круглого стола сформулированы следующие предложения:

1. В целях популяризации отечественного контента за рубежом целесообразно обеспечить создание «единой витрины» его представления в других странах, что позволило бы более эффективно обеспечивать продвижение и позиционирование.
2. В части борьбы с дипфейками целесообразно основные усилия направить на образовательные и просветительские инициативы в сфере цифровой гигиены с использованием широкого спектра информационных каналов, ориентированные на разные группы населения (дошкольники, школьники, студенты, взрослые и пожилые люди, родители). Такие меры должны обеспечивать формирование критического мышления, навыков распознавания недостоверного, мошеннического и деструктивного контента и понимания уровня достоверности и качества, который может быть достигнут дипфейками.
3. Разработать профессиональные стандарты в сфере технологий ИИ.
4. Поддерживать и предусмотреть в профильных программах развития мероприятия, направленные на создание на базе отечественных вузов лабораторий по Научно-исследовательским и опытно-конструкторским работам в сфере ИИ, в том числе в креативных индустриях.
5. Придерживаться общих принципов регулирования контента, учитывая, что зачастую контент с применением ИИ становится неприемлемым не в силу использования технологий, а потому что создавался с деструктивными целями.
6. Разделение в законодательном поле контента, генерируемого с применением ИИ и дипфейков (деструктивного контента, созданного с помощью ИИ). Это позволит развивать и поддерживать необходимые технологии для целей создания позитивного контента.

7. Маркировку и модерацию контента, созданного с помощью технологий ИИ, на первых этапах целесообразно вводить путем распространения лучших практик среди интернет-платформ и иных форм саморегулирования.

8. Представляется нецелесообразным полный отказ от участия человека в модерации контента на онлайн-платформах. Необходима возможность апеллирования к человеку (уполномоченному представителю платформы) для разрешения сложных или нетипичных случаев. Соответствующие нормы могут быть закреплены в том числе законодательно.

9. Выработать комплекс мер по регулированию использования технологий ИИ в образовательном процессе, закрепив основные принципы в нормативных актах в сфере образования.

В рамках круглого стола № 5 **«Обеспечение доверия и безопасности при развитии и использовании российского сегмента сети Интернет»** обсуждались вопросы дальнейшего повышения доступности, эффективности, качества и безопасности функционирования и использования, а также интеграции российского сегмента сети Интернет в национальную ИКТ-инфраструктуру и обеспечения возможности безопасного функционирования российского сегмента сети Интернет в составе международной ИКТ-инфраструктуры.

Ведущий: Воробьев А.А., КЦ доменов .RU/.РФ.
Выступили: Морозов Е.Н., MSK-IX; Георгиевский Г.Ю., КЦ доменов .RU/.РФ; Михайлов В.А., КЦ доменов .RU/.РФ; Новиков Н.А., ТЦИ; Кускевич Е.Г., РосНИИРОС.

Представитель MSK-IX Е.Н. Морозов поделился информацией о поэтапной локализации сети Интернет в России и об эволюции Рунета. Отдельное внимание выступающий уделил созданному глобальному DNS-облаку в России и привел при этом статистику по количеству запросов к авторитетным DNS RU серверам в России за сутки.

Во время своего выступления представитель Координационного центра Г.Ю. Георгиевский сообщил о ключевых изменениях на российском рынке регистраторов доменных имён: происходит перераспределение клиентов между существующими регистраторами доменных имён, клиенты активнее ведут поиск выгодных предложений на рынке, появляются новые регистраторы доменных имён на рынке и вместе с этим отмечается рост уже существующий, а также выступающий рассказал о новой системе взаимодействия с партнёрами.

Представитель Координационного центра В.А. Михайлов рассказал присутствующим о новых тенденциях в сфере альтернативных систем доменной адресации, акцентировал внимание на реестрах доменов верхнего уровня на основе блокчейна и привел в пример, набирающий популярность Ethereum Name Service, работающий на технологии блокчейна Ethereum. В.А. Михайлов отметил, что не смотря на перспективность подобных систем, они имеют явные проблемы с точки зрения безопасности. В.А. Михайлов подчеркнул, что новые технологии не только открывают возможности, но и создают новые угрозы, что требует современных методов защиты.

Представитель ТЦИ Н.А. Новиков в своем выступлении привел анализ текущего состояния рынка TSL-сертификатов в России. Он отметил значительные изменения, произошедшие после 2022 года, когда большинство иностранных центров сертификации покинули российский рынок. Это создало серьезные риски для безопасности интернет-соединений в российском сегменте сети Интернет. Выступающий подчеркнул важность развития отечественных решений в области TSL-сертификации. Он рассказал о мерах,

предпринятых ТЦИ для создания устойчивой инфраструктуры, включая автоматизацию процессов выпуска сертификатов и интеграцию с российскими операционными системами. Особое внимание было уделено работе по повышению доверия к отечественным сертификатам среди пользователей.

На заседании круглого стола сформулированы следующие предложения:

1. Продолжить работу по локализации трафика сети Интернет в России, для обеспечения более стабильной и надёжной работы сети и обеспечения дальнейшего развития и популяризации отечественных решений в области TSL-сертификации.

В рамках круглого стола № 6 **«Обеспечение требуемой функциональности оборудования NGFW»** обсуждались требования по функциональности к межсетевым экранам нового поколения (NGFW) как к средству связи и подходы к подтверждению соответствия таким требованиям.

Ведущий: Хасин Е.В., Минцифры России.
Выступили: Коктышев К.М., Интер РАО; Меджлумов М.А., BI.Zone; Пайсаев Р.У., Айдеко; Кадер М.Ю., Positive Technologies; Иванюк А.В., АДЭ.

В ходе обсуждения рынка межсетевых экранов нового поколения (NGFW) выступающие рассказали о комплексе проблем, с которыми сталкиваются как разработчики, так и заказчики. Многие тесты, проводимые сегодня в испытательных лабораториях, не учитывают специфику конкретных инфраструктур, что приводит к расхождению между лабораторными результатами и практической эксплуатацией. Отмечалось, что массовый приход новых российских разработчиков на рынок после 2022 года, хотя и создал конкуренцию, но осложнил выбор для заказчиков, так как из десятков вендоров лишь единицы могут предложить решения, готовые к масштабному внедрению.

Выступающие сообщили, что несмотря на отставание от зарубежных аналогов, отмечается положительная динамика в развитии отечественных NGFW решений. Отмечалось, что для ускорения прогресса необходима системная работа – формирование единых программ и методик испытаний, учитывающих отраслевую специфику (например, различия между требованиями банков, телекоммуникационных компаний или промышленных предприятий), а также создание прозрачной системы подтверждения соответствия. Такой подход позволит заказчикам опираться не на маркетинговые заявления производителей, а на проверенные данные, подтвержденные независимыми экспертами. Важным аспектом стало обсуждение роли регуляторов. Выступающие подчеркнули, что доверие к предлагаемым на отечественном рынке решениям невозможно без координации усилий между государственными органами, бизнес-структурами и экспертным сообществом. Примером может стать разработка «профилей защиты» — наборов требований для разных сценариев использования NGFW (например, для ЦОД или удаленного доступа), которые упростят выбор заказчикам. Кроме того, была отмечена необходимость открытости данных: публикация результатов испытаний, включая параметры производительности и стабильности, что должно помочь избежать дублирования усилий и обеспечить стимулирование здоровой конкуренции.

На заседании круглого стола сформулированы следующие предложения:

1. Минцифры России с возможным привлечением профильных комитетов и рабочих групп АДЭ проработать вопрос разработки программы и методик испытаний NGFW как средства связи. Рассмотреть возможность использования системы добровольной

сертификации «Связь-эффективность», функционирующей на базе АДЭ, для подтверждения соответствия требований по функциональности NGFW как средства связи.

В рамках круглого стола № 7 **«Национальные интересы и международное взаимодействие в сфере ИКТ»** обсуждалось формирование и функционирование системы международной информационной безопасности, вопросы выстраивания международного взаимодействия в сфере ИКТ, роль и шаги Российской Федерации в этой области, а также задачи базовой кафедры АДЭ по обеспечению комплексной гуманитарно-технологической подготовки экспертов для представления интересов страны в международных организациях.

Ведущий: Мирошников Б.Н., УК Гарда.
Выступили: Петров А.А., Совет Безопасности Российской Федерации; Люкманов А.Р., МИД России; Иванов А.В., НКЦКИ; Григорьев Д.И., НАМИБ; Стрельцов А.А., НАМИБ; Бородин А.С., РСС; Глущенко В.В., Центр компетенций по глобальной ИТ-кооперации; Фролов Д.Б., РТРС; Захарова С.А., Администрация президента Российской Федерации.

Представитель Совета Безопасности Российской Федерации А.А. Петров рассказал о том, что глобальное противостояние между Западом и Россией в информационной сфере усугубляется международными системными угрозами: двойные стандарты в регулировании киберпространства, политизация атрибуции кибератак и милитаризация информационного пространства. В ответ Россия делает ставку на международно-правовые механизмы в рамках Конвенций ООН, укрепление межгосударственного диалога и сотрудничество в рамках БРИКС и ШОС. Приоритетом при этом является формирование системы международной информационной безопасности, основанной на равной безопасности всех государств с учетом их национальных интересов и особенностей.

Представитель МИД Российской Федерации А.Р. Люкманов сообщил о важности международного регулирования кибербезопасности и искусственного интеллекта в рамках Конвенций ООН. А.Р. Люкманов подчеркнул, что Россия выступает за техническое регулирование передовых технологий в рамках МСЭ. Он отметил, что разработчики искусственного интеллекта из иностранных государств могут намеренно предоставлять недостоверную информацию, манипулируя общественным мнением и создавая угрозы другим государствам.

Представитель Национального координационного центра по компьютерным инцидентам А.В. Иванов сообщил о возросшем количестве кибератак на различные секторы Российской Федерации с момента начала специальной военной операции. Координация противодействия кибератакам включает в себя взаимодействие с другими странами в рамках «Глобального межправительственного реестра контактных пунктов для обмена информацией о компьютерных атаках/инцидентах», который был создан по инициативе России в рамках ООН, что позволило повысить безопасность российского информационного пространства. Ещё одной важной составляющей является заключение меморандума о взаимопонимании между НКЦКИ и соответствующими полномочными органами в иностранных государствах. А.В. Иванов отметил большой запрос со стороны партнёров из дружественных стран на обучение, предоставлений информационных технологий и технологий средств защиты информации.

Представитель Национальной ассоциации международной информационной безопасности (НАМИБ) Д.И. Григорьев рассказал о деятельности Центра координации государственно-частного партнёрства в области международной информационной

безопасности – дочернего подразделения НАМИБ по реализации мероприятий государственно-частного партнёрства в области продвижения продукции российских кампаний ИТ-сектора на зарубежных рынках дружественных государств.

Представитель НАМИБ А.А. Стрельцов затронул проблемные вопросы международного сотрудничества в ИКТ-среде. Было отмечено, что наиболее актуальной проблемой сотрудничества в области международной информационной безопасности с дружественными государствами является формирование системы мер установления и поддержания доверия в области применения норм и принципов международного права.

Представитель Регионального содружества в области связи А.С. Бородин отметил, что в условиях глобальных кризисов критически важно четко определять национальные интересы, интегрируя их в стратегии международного сотрудничества. Для преодоления вызовов необходимы изменение кадровой политики, импорт образования в дружественные страны, преодоление языковых барьеров. А.С. Бородин подчеркнул, что успех зависит от отказа от иллюзорной солидарности и учета уникальных интересов всех участников, а не конфронтации.

Представитель Центра глобальной ИТ-кооперации В.В. Глущенко представил ход подготовки юбилейного 20 Форума по управлению интернетом, который пройдёт в июне 2025 года, рассказал про ключевые сессии и тематики Форума.

Представитель Российской телевизионной и радиовещательной сети Д.Б. Фролов акцентировал внимание на том, что в рамках гибридных войн большинство военных действий происходит в информационной сфере, в том числе в виде атак на медийную сферу: атаки на радиостанции, телевещание, дипфейки.

Представитель администрации президента Российской Федерации С.А. Захарова сообщила о готовящемся глобальном цифровом форуме, в рамках которого планируется подписание стратегических соглашений с иностранными государствами, что позволит продемонстрировать Россию как технологически независимого и открытого партнёра, готового делиться экспертизой в области инноваций и информационной безопасности.

На заседании круглого стола сформулированы следующие предложения:

1. Активнее использовать возможности АДЭ в комплексной гуманитарно-технологической образовательной деятельности по подготовке экспертов, способных представлять интересы страны в международных организациях, работающих в сфере обеспечения доверия и безопасности при использовании ИКТ.
2. В рамках общественно-государственного партнерства продолжить гармонизацию представления национальных интересов страны в сфере ИКТ на международной арене.

В рамках круглого стола № 8 **«Эффективное использование возможностей современных сетей связи: перспективы регулирования и вопросы безопасности при оказании услуг связи (на примере ВАТС)»** обсуждались необходимые регуляторные и технические требования к средствам связи, обеспечивающие возможность расширения функциональности услуг, оказываемых операторами связи на ССОП, и комплекс мер по обеспечению их безопасности, подготовленные в рамках рабочей группы АДЭ.

Ведущий: Мальянов С.А., ВымпелКом.
Выступили: Антипкин Р.Б., РГ АДЭ по СОРМ; Власов И.И., Минцифры России; Ермоленко О.В., МТТ; Королев Д.И., ВымпелКом; Лачинов А.Р., ВымпелКом.

Участники круглого стола отметили необходимость внедрения перспективных решений, создаваемых на основе конвергенции существующих сетей связи, а также их востребованность субъектами экономики страны. Наличие технических возможностей операторов связи по эффективной реализации таких возможностей при необходимости обеспечения безопасности при оказании услуг связи с использованием виртуальных телефонных станций (далее – ВАТС), требуют соответствующего отраслевого регулирования.

Отмечено, что нормами статьи 9 Федерального закона от 01 апреля 2025 года №41-ФЗ «О создании государственной информационной системы противодействия правонарушениям, совершаемым с использованием информационных и коммуникационных технологий, и о внесении изменений в отдельные законодательные акты Российской Федерации» (далее – 41-ФЗ) определено место ВАТС в сети связи общего пользования как средства связи. Таким образом, 41-ФЗ заложена правовая основа для регулирования использования ВАТС как средства связи на уровне подзаконных актов.

Выступающими отмечено, что своевременный запуск обсуждения в рамках рабочей группы АДЭ вопросов реализации услуг ВАТС, нумерации, сертификации цифровых сервисных платформ ВАТС и требований СОРМ к ним, позволило прийти к согласованному пониманию представителями отрасли роли и места ВАТС на сети связи общего пользования включая, в том числе функции, задачи и оказываемые услуги. Рабочей группой АДЭ подготовлена схема решения СОРМ при оказании услуг связи с использованием ВАТС. Указанная схема обеспечивает системное понимание работы ВАТС, необходимых решений по обеспечению безопасности оказания услуг связи и взаимодействию с системой оперативно-разыскных мероприятий и, соответственно, подходов к их регулированию.

Участниками круглого стола отмечено, что дальнейшие усилия рабочей группы должны быть направлены на подготовку проектов подзаконных нормативных правовых актов, направленных на реализацию ст.41 и ст.44 Федерального закона от 07 июля 2003 года № 126 «О связи».

Представителями рабочей группы АДЭ сформулированы предложения по содержанию Технических заданий для Правил применения, которые необходимо разработать. Отмечено, что в Правилах применения ВАТС в обязательном порядке должны быть четко обозначены границы ВАТС, регулируемыми Правилами исходя из общей нормы в ст.9 41-ФЗ.

На заседании круглого стола сформулированы следующие предложения:

1. Обеспечить системный подход и более тесное взаимодействие рабочей группы АДЭ с Минцифры России при обсуждении и подготовке проектов нормативных правовых актов для реализации оказания услуг связи с использованием виртуальных телефонных станций при необходимости обеспечения безопасности этих услуг.

2. В рамках совещаний рабочей группы АДЭ подготовить и представить в Минцифры России проекты нормативных правовых актов, в том числе:

- включение ВАТС в Перечень средств связи, подлежащих обязательной сертификации, утвержденный постановлением Правительства Российской Федерации от 04 февраля 2022г. № 113;
- правила применения ВАТС;
- правила применения оборудования СОРМ при использовании ВАТС;
- предложения по внесению изменений и дополнений в Правила оказания услуг телефонной связи, утвержденные постановлением Правительства Российской Федерации от 09 декабря 2014г. № 1342, в части оказания услуг связи с использованием ВАТС.

В рамках круглого стола № 9 **«Содействие разработке и внедрению программного обеспечения для отечественных архитектур микропроцессоров»** обсуждались технологические, организационные, процедурные, образовательные и нормативные аспекты содействия разработке и внедрению ПО для отечественных архитектур микропроцессоров, применение взаимодополняющих понятий обеспечения доверия и безопасности при решении взаимодополняющих задач развития функциональности и безопасности отечественных ПАК, а также создание на базе АДЭ отраслевого центра компетенций по разработке и внедрению отечественных ПАК.

Ведущий: Смирнов А.В., Базальт СПО.
Выступили: Сундеев П.В., Сириус; Новоселов М.Е., НТЦ ИТ РОСА; Шереметьев А.В., МТУСИ; Иванюк А.В., АДЭ.

Представитель Сириус П.В. Сундеев представил комплексный анализ проблемы доверия в контексте обеспечения информационной безопасности и национальной стабильности. Он поддержал широкое понимание «обеспечения доверия» как управление осведомлённостью о функционировании системы и отметил проблему разночтений в трактовке термина «доверие» разными нормативно-правовыми документами (приказ ФСТЭК России от 02.06.2020г. №76, постановление Правительства Российской Федерации от 14 ноября 2023г. №1912, стандарт ТК167 ПНСТ 05-2023), что затрудняет правоприменительную практику данного термина. П.В. Сундеев сообщил, что ранее доверие к системам обеспечения информационной безопасности зависело от их типа (программные, аппаратные, программно-аппаратные), но современные стандарты относят к «доверенным» все компоненты системы, что размывает границы между защищёнными и уязвимыми элементами. П.В. Сундеев подчеркнул необходимость единого подхода к стандартизации терминов, связанных с функциональной безопасностью, стабильностью и защитой информации, чтобы избежать путаницы и коллизий при применении различных нормативных правовых актов.

Представитель Базальт СПО А.В. Смирнов отметил значительные изменения в нормативной базе, касающиеся совместимости прикладного и системного ПО с отечественными процессорами. Готовятся изменения в нормативно-правовую базу, которые позволят внести дополнительные требования к ПО из реестра российского программного обеспечения и предоставить преференции в госзакупках отечественным продуктам при их соответствии дополнительным требованиям, включая совместимость с отечественными процессорами. Если продукт не будет соответствовать этим требованиям, он останется в реестре, но потеряет приоритет перед решениями, поддерживающими отечественные процессоры. Это создаст «мягкое принуждение» для разработчиков: сохраняя текущие льготы, они рискуют уступить в конкурентной борьбе тем, кто адаптирует свои продукты под отечественные процессоры.

Представитель НТЦ ИТ РОСА М.Е. Новоселов подчеркнул важность создания экосистемы, в которой разработчики процессоров, производители плат и конечного оборудования взаимодействуют, упрощая процесс разработки. Докладчик сообщил о проблеме, связанной с доступностью оборудования, реализованного на отечественных процессорах «Эльбрус», при этом отметил, что данную проблему помогает решить пилотная зона на базе АДЭ, которая предоставляет разработчикам необходимую экспертизу и доступ к оборудованию с отечественными процессорами для разработки, портирования, тестирования и отладки ПО. Несмотря на встречающийся скепсис в отношении отечественных процессоров и их преимущественное использование в госзаказах, М.Е. Новоселов отметил положительную

тенденцию развития отрасли в части содействия разработке и внедрению ПО для отечественных архитектур микропроцессоров, подчеркнув необходимость дальнейшей государственной поддержки.

Представитель МТУСИ А.В. Шереметьев отметил важность участия аккредитованных ИТ-компаний в деятельности вузов. Он обратил внимание на ключевую проблему - нехватку квалифицированных специалистов, способных сразу после обучения выполнять сложные задачи. Как отраслевой университет, МТУСИ активно взаимодействует с индустриальными партнерами, однако большинство вузов слабо вовлечены в такое сотрудничество. А.В. Шереметьев сообщил, что Минцифры России разработало показатели взаимодействия ИТ-компаний с вузами, включая стажировки студентов, разработку дисциплин и участие экспертов отрасли в преподавании. Проект начнет реализовываться с 1 августа 2025 года, при этом уже сейчас ощущается нехватка времени для выстраивания полноценного сотрудничества. А.В. Шереметьев выделил основные вопросы требующие проработки: недостаточная информированность отрасли и вузов об инициативе, неясность механизмов проверки соответствия требованиям: кто будет проводить проверки и какие данные запрашивать.

Председатель Исполкома АДЭ А.В. Иванюк сообщил о поручении заместителя Министра цифрового развития, связи и массовых коммуникаций Российской Федерации А.М. Шойтова по созданию на базе АДЭ Полигона доверенных решений для КИИ в отрасли связи. Докладчик обозначил ключевые предпосылки к данному поручению – недостаток ПО для отечественных архитектур микропроцессора, риски использования зарубежной инфраструктуры для разработки ПО и отсутствие системной подготовки квалифицированных кадров, способных разрабатывать и внедрять доверенные ПАК для значимых объектов КИИ отрасли связи. АДЭ обладает необходимыми компетенциями для решения этих задач благодаря участию бизнеса, научного сообщества и Регуляторов, а также имеющейся инфраструктуре – с 2018 года на базовой кафедре АДЭ в МТУСИ ведется преподавание исключительно с использованием отечественного оборудования и ПО. А.В. Иванюк отметил, что на базовой кафедре АДЭ активно разрабатываются и внедряются дисциплины, связанные с обеспечением технологической независимости и разработкой ПО для отечественных архитектур микропроцессоров. Кроме того, с сентября 2025 года планируется обучение студентов по новой магистерской программе «Доверенные программно-аппаратные средства для обеспечения безопасности КИИ». Докладчик отметил необходимость повышения значимости вовлечения ИТ-компаний в деятельность базовых кафедр в рамках оценки участия бизнеса в образовательной деятельности.

На заседании круглого стола сформулированы следующие предложения:

1. Провести анализ целесообразности уточнения термина «доверие» в контексте содействия обеспечению информационной безопасности для решения проблемы разночтений в трактовке.
2. Проработать вопрос о введении единого стандарта для терминов и определений в области функциональной стабильности, информационной безопасности и защиты информации для всех отраслей.
3. Пригласить операторов связи и разработчиков телекоммуникационного оборудования к участию в деятельности созданного на базе АДЭ Полигона доверенных решений для КИИ в отрасли связи.

4. Пригласить отраслевые организации принять участие в целевом наборе студентов по новой магистерской программе «Доверенные программно-аппаратные средства для обеспечения безопасности КИИ» на базовой кафедре АДЭ в МТУСИ.