ДОКУМЕНТАЛЬНАЯ ЭЛЕКТРОСВЯЗЬ

информационно-аналитический журнал

№35 СЕНТЯБРЬ 2025
(Издается с 1999г.)

Выпуск подготовлен при поддержке
АНО «Координационный центр доменов .RU/.РФ»

Журнал является печатным органом
Ассоциации документальной электросвязи

Журнал зарегистрирован в Государственном Комитете Российской Федерации по печати 2 апреля 1999г. Регистрационный номер №018662.

Тираж 5000 экземпляров. Бесплатно.

Полное или частичное воспроизведение или дублирование каким бы то ни было способом материалов, опубликованных в настоящем издании, допускается только с письменного разрешения Исполнительного комитета АДЭ.

АДРЕС:
111024,
г. Москва,
ул. Авиамоторная,
д. 8, стр. 2

КОНТАКТЫ:
8 (495) 532-37-11
info@rans.ru
www.rans.ru
www.адэ.рф

ГЛАВНЫЙ РЕДАКТОР: Янин Егор

РЕДАКТОР: Макарцов Юрий

ДИЗАЙН/ВЕРСТКА: Трусов Сергей

СОДЕРЖАНИЕ

РАЗВИТИЕ ИКТ-ИНФРАСТРУКТУРЫ

2 Ретроспективный обзор и прогнозы развития отрасли связи в России и за рубежом
Анатолий Голомолзин

9 Приземление 2.0: регулирование деятельности иностранных ИТ-компаний в России
Борис Едидин, Алексей Буньков, Антон Куликов

18 Кириллическому домену .РФ 15 лет
Владимир Горжалцан

25 Особенности классификации сетевого трафика в российском сегменте сети интернет
Александр Полунин

31 Совершенствование правового регулирования цифровых рынков как инструмент достижения национальных целей экономического развития
Анатолий Голомолзин

38 Операционные системы для промышленных контроллеров — первый опыт, перспективы и планы
Евгений Синельников, Ольга Юшина

42 Как кроссплатформенные почтовые клиенты меняют отечественный бизнес-ландшафт?
Юлия Денисенко

44 Методология, проблематика и особенности построения зонтичной системы мониторинга и инвентаризации данных в крупных организациях
Илья Ушанов

ОБЕСПЕЧЕНИЕ ДОВЕРИЯ И БЕЗОПАСНОСТИ ПРИ ИСПОЛЬЗОВАНИИ ИКТ

50 Использование искусственного интеллекта для борьбы с фишингом
Лев Лунегов, Никита Немцев

54 Искусственный интеллект в кибербезопасности: новая эра цифровой защиты
Денис Батранков

57 Аспекты внедрения ТС ОРМ у хостинг-провайдеров
Евгений Круглов

66 Двадцать лет инноваций: как Ideco меняет подход Enterprise-компаний к кибербезопасности
Дмитрий Хомутов

69 Киберустойчивость энергетики: стратегия и кадры
Евгений Генгринович

73 Региональный киберполигон как инновационный инструмент подготовки кадров
Сергей Фомин, Александр Фефилов

МЕРОПРИЯТИЯ АДЭ

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

86 Меморандум о необходимости создания полигона содействия разработке и внедрению доверенных решений для КИИ в отрасли связи»

92 ЧЛЕНЫ АДЭ

РАЗВИТИЕ ИКТ-ИНФРАСТРУКТУРЫ



АНАТОЛИЙ ГОЛОМОЛЗИН
к.т.н., советник Президента **АО «ЭР-Телеком Холдинг»** по взаимодействию с органами власти, действительный государственный советник 2 класса

РЕТРОСПЕКТИВНЫЙ ОБЗОР И ПРОГНОЗЫ РАЗВИТИЯ ОТРАСЛИ СВЯЗИ В РОССИИ И ЗА РУБЕЖОМ

ОБ АВТОРЕ

Автор являлся заместителем Министра по антимонопольной политике и поддержке предпринимательства Российской Федерации (2000 – 2004), заместителем Руководителя Федеральной антимонопольной службы (2004 – 2020), первым заместителем Председателя Межгосударственного авиационного комитета (2020 – 2021), возглавлял Штаб по проведению совместных антимонопольных расследований в СНГ при Межгосударственном совете по антимонопольной политике (2006 – 2020).

АННОТАЦИЯ

На стабильных монорынках политика ограничения цен важна для благосостояния потребителей. Для быстро развивающихся многопродуктовых и многосторонних рынков регуляторная политика не должна ориентироваться лишь на краткосрочные эффекты и цели «статической эффективности» (например, директивное удержание цен около порога рентабельности). Приоритет должен быть у «долгосрочной динамической эффективности» (для роста инвестиций, стимулирования инноваций, расширения продуктового предложения и обеспечения международной конкурентоспособности). Сделаны выводы о необходимости устранения разрывов между быстро развивающимися технологиями и бизнес-моделями, с одной стороны, и консервативным и тормозящим развитие регулированием.

КЛЮЧЕВЫЕ СЛОВА:

телекоммуникационная отрасль, цифровые рынки, «цифровые гиганты», антимонопольная политика, цены, быстро развивающиеся многопродуктовые и многосторонние рынки, долгосрочная динамическая эффективность.

РЕТРОСПЕКТИВНЫЙ ОБЗОР ИЗМЕНЕНИЙ НА ЦИФРОВЫХ РЫНКАХ

В России и в мире за последние 30 лет кардинальным образом поменялась техника, аналоговые системы передачи и коммутации каналов заменены цифровыми пакетными системами на базе стека TCP/IP. Появились на рынке новые инновационные технологии предоставления услуг связи, к которым относится IP-телефония, технологии подобные Skype, они позволили значительно удешевить связь, нарастить объёмы оказываемых услуг, повысить их качество, предложить новый спектр услуг. Широкополосный доступ в Интернет (доступ к фиксированной и мобильной связи) стал повсеместным. Есть возможность оказывать весь спектр услуг связи на единой аппаратурной базе, сети стали мультисервисными, архитектура «услуга = сеть» ушла в прошлое. Произошёл переход от аппаратных средств к программному обеспечению, голос уже не дифференцируется от других видов контента и пакетный трафик не различается по типу пакетов.

Технологические изменения сопровождались и кардинальными институциональными изменениями в отрасли связи и ИКТ. С начала 1990-х годов в ходе структурных реформ появлялись новые компании, бизнесы и услуги. Менялись подходы к отраслевому регулированию, государственному тарифному регулированию, мерам антимонопольной политики, защиты и развития конкуренции. Перебалансировка тарифов на услуги фиксированной связи позволила за 5 лет практически устранить перекрестное субсидирование и выйти на уровень тарифов, соответствующий уровню экономически обоснованных расходов и прибыли (в странах организации экономического развития и сотрудничества эти же процессы проходили 8–10 лет). Имел место постоянный рост трафика и качества услуг, предприятия электросвязи превратились в «голубые фишки», а экономика страны получила возможности для устойчивого развития.

В результате этих масштабных изменений были созданы условия для развития конкуренции, для дерегулирования в сфере фиксированной телефонии. Сформировался конкурентный сегмент сотовой связи и внедрились новые услуги, в том числе услуги передачи данных и услуги доступа в Интернет. Сотовая связь и услуги доступа в Интернет были развиты на частные средства за короткое время с «нуля» до грандиозных масштабов, чему способствовали отсутствие жестких административных ограничений и низкие экономические барьеры входа на рынок. Большую роль сыграло антимонопольное регулирование и контроль. Это касалось распределения частотного ресурса, тарифообразования в роуминге, устранения «цифрового неравенства», практики антимонопольных дел в отношении мировых «цифровых гигантов».

За эти годы в России и в мире на рынке связи и информационных технологий утратили позиции доминантов фиксированные операторы, затем на смену сотовым операторам пришли «цифровые гиганты». В основе этих трансформаций или их основным движителем является конкуренция и услуг, и инфраструктур, и экосистем. С опорой на инновационные ключевые активы, новые решения и системы организации бизнеса, появляются новые и трансформируются существующие игроки. Происходит постоянная трансформация и конвергенция услуг и инфраструктур старых и новых игроков.

Инфраструктура фиксированной связи, уступив на определённом этапе сотовой связи и ИТ-инфраструктуре, на современном этапе вновь восстанавливает свою конкурентоспособность. Оптические линии связи обеспечивают опережающее развитие цифровой инфраструктуры, выигрывая в скоростях и качестве, формируя новые условия мобильности, предоставляя новые возможности мониторинга, обработки данных, управления.

В настоящее время стоимость доступа к сети Интернет в России в 1,5 – 2 раза ниже, чем в Китае и СНГ, и в 3 – 4 раза ниже, чем в странах организации экономического сотрудничества и развития. Еще 10 лет назад преобладали скорости доступа в Интернет в равных пропорциях менее 10 Мбит/с и от 10 до 100 Мбит/с, сейчас в России более половины абонентов получают доступ к высококачественному высокоскоростному интернету с показателями более 100 Мбит/с (как правило, 300 – 500 Мбит/с, в режиме коммерческой эксплуатации уже применяются и тарифные планы для домохозяйств со скоростями выше 1 Гбит/с).

Низкая стоимость доступа к сети Интернет в России – следствие высокой конкуренции услуг, инфраструктур и экосистем. Развитая инфраструктура и низкие цены обеспечили бурное развитие интернет-сервисов: онлайн-доступ к СМИ, видео, такси и каршерингу, доставке, маркетплейсам, социальным сетям, сервисам прямого взаимодействия с пользователем (OTT-сервисы), госуслугам. Развитие финтеха (интернет банкинг, брокерское обслуживание в смартфоне, онлайн платежи) также невозможны без надежной и качественной связи[1].

По данным Высшей школы экономики (ВШЭ)[2] совместный вклад отрасли связи (телекома) и ИТ в ВВП России составлял 2,23% в 2013 году. По итогам 2023 года их вклад составил 2,85%. При этом произошло перераспределение вклада телеком-отрасли и ИТ-отрасли. ИТ-отрасль выросла с 0,76% в 2013 году до 1,98% по итогам 2023 года во многом благодаря телеком-

[1] Стратегия отрасли связи на период до 2035г., утв. Распоряжением Правительства Российской Федерации от 24 ноября 2023г. № 3339-р.
[2] Финансово-экономическая модель и прогноз развития отрасли связи на 2025-2027 годы.- Высшая школа экономики (по заказу АНО «Цифровая экономика»). Декабрь 2024г.

инфраструктуре. Кратный рост цифровой экономики и онлайн-сервисов в прошедшие годы был бы невозможен без телеком-инфраструктуры. Следует отметить, что экономические параметры отрасли связи росли существенно медленнее, чем по экономике в целом и в смежной ИТ-отрасли. Доля отрасли связи в ВВП снизилась с 1,47% в 2013 году до 0,87% в 2023 году **(рис.1)**, инвестиции стагнировали даже в текущих ценах.

С 2019 года объем потребления услуг связи (интернет-трафик) растет в России намного быстрее (+26,9% в год), чем реальная плата абонентов и, соответственно, выручка операторов (+3,2% в год). Доходы на единицу трафика непрерывно падают. Динамика выручки от услуг связи ниже темпов индекса потребительских цен (ИПЦ) (+7,4% в год), что привело к накопленному разрыву в 19 процентных пункта (п.п.) в 2023г. относительно 2019г. Одной из ключевых проблем отрасли связи остается стагнация свободного денежного потока и прибыли. Это, в свою очередь, ограничивает инвестиционные возможности российских операторов связи. Падение рентабельности в отрасли связи приводит к снижению её инвестиционной привлекательности. Внедрение новых поколений и технологий связи требует роста инвестиций операторов связи, в том числе в развитие магистральных линий связи. Стратегия отрасли связи на период до 2035г. (далее – Стратегия) устанавливает, что поддержка инвестиционной активности операторов связи – одна из главных задач регуляторов в сфере связи.

С учетом сложившейся и прогнозной структуры денежных потоков операторов связи и при условии неизменности их финансовой политики указанные инвестиционные потребности могут быть обеспечены в основном за счет собственных средств (в том числе амортизационных отчислений и чистой прибыли). В рамках Стратегии рассматривались 2 сценария развития отрасли связи – базовый и целевой (перспективный). В базовом сценарии доходы операторов связи покрывали капитальные расходы на поддержание текущего состояния сетей связи, реализацию текущих проектов при условии не увеличения регуляторных обременений и социальных обязательств[3]. С учетом прогнозного роста цен на оборудование (в том числе при выполнении планов импортозамещения) реализация базового сценария предполагала переход к более высоким темпам роста тарифов на услуги связи, чем те, которые имели место в прошедшие годы, но не выше прогнозной динамики индекса потребительских цен.

Целевой (перспективный) сценарий предусматривал достижение целей Стратегии в полном объеме, развитие сетей связи новых поколений, внедрение новых технологий, реализацию крупных инвестиционных проектов, в том числе в новых сегментах и на новых территориях. Реализация этого сценария возможна при условии привлечения дополнительных инвестиций, в



Рис.1. Россия: ИТ-отрасль успешно росла благодаря телеком-инфраструктуре.

[3] По факту в 2023 - 2025 годах имело место увеличение регуляторных обременений и социальных обязательств.

том числе за счет более быстрого роста тарифов, чем в базовом сценарии, в первую очередь для тех групп потребителей, которые предъявляют повышенные требования к качеству и объему услуг связи. Указ Президента Российской Федерации о национальных целях[4] предопределяет необходимость реализации именно перспективного сценария, с возможностью его дополнения с учетом всего многообразия поставленных задач и целевых установок.

РАЗВИТИЕ ЦИФРОВЫХ РЫНКОВ В БЛИЖАЙШЕЙ И СРЕДНЕСРОЧНОЙ ПЕРСПЕКТИВЕ

Отечественному телекоммуникационному рынку в соответствии со Стратегией предстоит существенно вырасти в условиях растущего спроса. Цели Стратегии России на 2030 год и до 2035 года: темп роста интернет-трафика около 30% в год, скорость мобильного интернета не менее 45 – 60 Мбит/с; покрытие 5G не менее 10 – 15%; гигабитный интернет – обеспечивает возможность подключения домохозяйств на скорости не менее 1 Гбит/сек. Чтобы обеспечить выполнение стратегических установок, ВШЭ по заказу АНО «Цифровая экономика» сделала прогноз потребности в инвестициях. Отмечено, что базовые капитальные затраты обеспечивали поддержание текущей инфраструктуры и растущую нагрузку на сети связи. Кроме того, для реализации показателей Указа Президента Российской Федерации о национальных целях и Стратегии, в том числе в части гигабитного интернета и 5G[5], необходимы дополнительные капитальные затраты (CAPEX).

Целевые задачи для достижения национальной цели «Устойчивая и динамичная экономика» касаются, в частности, вхождения к 2030 году России в число 25 ведущих стран мира по плотности роботизации и увеличению доли креативных (творческих) индустрий в экономике. Целевые задачи для достижения национальной цели «Технологическое лидерство» определены в части обеспечения технологической независимости и формирования новых рынков по таким направлениям, как биоэкономика, сбережение здоровья граждан, продовольственная безопасность, беспилотные авиационные системы, средства производства и автоматизации, транспортная мобильность (включая автономные транспортные средства), экономика данных и цифровая трансформация, искусственный интеллект (ИИ), новые материалы и химия, перспективные космические технологии и сервисы, новые энергетические технологии (в том числе атомные).

Планируемые показатели и задачи для достижения национальной цели «Цифровая трансформация государственного и муниципального управления, экономики и социальной сферы» в т.ч. определяют необходимость достижения к 2030г. «цифровой зрелости» государственного и муниципального управления, ключевых отраслей экономики и социальной сферы; формирования рынка данных, их активное вовлечение в хозяйственный оборот, включая хранение, обмен и защиту; увеличения доли домохозяйств, которым обеспечена возможность качественного высокоскоростного широкополосного доступа к информационно-телекоммуникационной сети Интернет, в том числе с использованием сетей (инфраструктуры) спутниковой и мобильной связи и с учетом роста пропускной способности магистральной инфраструктуры, до 97% к 2030г. и до 99% к 2036г; обеспечения в 2025 – 2030 годах темпа роста инвестиций в отечественные решения в сфере информационных технологий в 2 раза выше темпа роста ВВП; создания системы эффективного противодействия преступлениям, совершаемым с использованием информационно-телекоммуникационных технологий, и снижения ущерба от их совершения; обеспечения сетевого суверенитета и информационной безопасности в информационно-телекоммуникационной сети Интернет.

ВШЭ по заказу АНО «Цифровая экономика» с участием операторов связи актуализировали экономическую модель отрасли связи, подготовленную ранее в рамках Стратегии развития отрасли связи до 2035 года. В частности, была дана оценка текущего состояния по 2024 году и прогноз на 2025 – 2027 годы. Также была учтена совокупность влияющих факторов, включая рост учётной ставки, дополнительные расходы, связанные с отраслевым регулированием, импортозамещением и др. Экономическая модель показывает, что отрасль обеспечивает потребности населения, бизнеса и государства, обеспечивает взрывной рост ИТ, но при этом фиксируется снижение источников финансирования текущей деятельности и развития. ВШЭ был сделан прогноз потребностей в инвестициях и источниках финансирования в рамках обеспечения развития отрасли связи для достижения контрольных цифр Указа о национальных целях[6] и Стратегии.

Основной источник финансирования инвестиций – собственные средства (выручка). Исследователи ВШЭ[7] отмечают, что при росте тарифов по ИПЦ возникает дефицит средств на покрытие капитальных расходов даже от базовых капитальных затрат. Недоинвестирование привело бы к деградации инфраструктуры связи и невозможности выполнения целей и показателей Стратегии. Темп роста тарифов,

[4] Указ Президента Российской Федерации от 7 мая 2024г. «О национальных целях развития Российской Федерации на период до 2030 года и на перспективу до 2036 года».
[5] Финансово-экономическая модель и прогноз развития отрасли связи на 2025-2027 годы.- Высшая школа экономики (по заказу АНО «Цифровая экономика»). Декабрь 2024г.
[6] Указ Президента Российской Федерации от 7 мая 2024 года «О национальных целях развития Российской Федерации на период до 2030 года и на перспективу до 2036 года».
[7] Финансово-экономическая модель и прогноз развития отрасли связи на 2025-2027 годы.- Высшая школа экономики (по заказу АНО «Цифровая экономика»). Декабрь 2024г

который обеспечивает покрытие базовых капитальных затрат, возможен за счёт ликвидации к 2027 году накопленного с 2019 года разрыва между динамикой выручки от услуг связи и ИПЦ **(рис.2)**.

Пролонгация такой тарифной политики отрасли связи на перспективу до 2030 и 2035 года будет способствовать достижению целей Стратегии. С учетом количественных и качественных изменений на рынках услуг связи, фактически в настоящее время имеет место не рост, а постоянное снижение цен (тарифов) – на единицу трафика **(см. рис.3)**, на единицу скоростей передачи данных, на единицу присоединенных устройств абонентов. Достижению целей и задач Стратегии поспособствует детализированная программа мер по ее реализации[8].

Не только в России, но и в мире телекоммуникационная отрасль сталкивается с фундаментальной стратегической проблемой, общей для коммунальных служб и других зрелых отраслей. Сектор предоставляет жизненно важные услуги, на которые полагаются миллиарды потребителей и практически все предприятия. Следует отметить, что трафик ежегодно растет более, чем на 28%, при этом у телеком компаний наблюдается рост затрат, снижение доходности и инвестиционной привлекательности. В значительной степени обусловленное видеотрафиком, глобальное потребление данных в телекоммуникационных сетях почти утроится: с 3,4 миллионов петабайт (ПБ) в 2022 году до 9,7 миллионов ПБ в 2027 году[9] **(см. рис.4)**.

У операторов связи в мире ограничены возможности ценообразования на услуги подключения и передачи данных, доходы от доступа в Интернет вырастут всего на 4% CAGR[10] до 921,6 млрд долларов США к 2027 году. В то же время операторы связи (телекомы) должны вкладывать значительные средства в дорогостоящую инфраструктуру, которая позволит им обслуживать клиентов. По мере продолжения перехода к 5G и внедрения новых технологических стандартов прогнозируется, что телекоммуникационные компании мира инвестируют 342,1 млрд долларов США в свои сети только в 2027 году. Общие капитальные расходы в телекоммуникации выросли на 4,2% в 2022 году до 319,1 млрд долларов США, что больше, чем в любой исторический или прогнозируемый год за десятилетний период. Однако темпы роста инвестиций как в фиксированную широкополосную связь, так и в мобильную широкополосную связь будут снижаться каждый год до 2027 года[11]. Значительно более высокая инфляция и процентные ставки[12] внушают большую



Рис.2. Необходимость ликвидации разрыва инфляции и цен на услуги связи в России.

[8] План мероприятий по реализации Стратегии развития отрасли связи Российской Федерации на период до 2035 года, утверждённый Распоряжением Правительства РФ от 24.05.2025 № 1312-р.
[9] Wilson Chow, Dr. Florian Gröne. Perspectives from the Global Telecom Outlook 2023 – 2027. [Электронный доступ] URL: *https://www.pwc.com/gx/en/industries/tmt/telecom-outlook-perspectives.html*
[10] CAGR (англ. Compound annual growth rate) – совокупный среднегодовой темп роста. Выражается в процентах и показывает, на сколько процентов за год прирастает изучаемый параметр.
[11] Wilson Chow, Dr. Florian Gröne. Perspectives from the Global Telecom Outlook 2023 – 2027. [Электронный доступ] URL: *https://www.pwc.com/gx/en/industries/tmt/telecom-outlook-perspectives.html*
[12] Как можно заметить, такие проблемы имеются даже в стабильных экономиках (примечание автора).



Рис.3. Соотношение роста трафика и выручки от услуг связи в России.



Рис.4. Общемировая проблема телекома.

осторожность в капитальных расходах. В 2026 году капитальные расходы в мобильные сети обгонят инвестиции в фиксированную широкополосную связь. Рост капитальных расходов в телекоммуникациях обусловлен тем, что операторы в США, Европе и Японии развертывают 5G, расширяют свою фиксированную волоконно-оптическую инфраструктуру, переводят системы в облако и изучают сетевые решения с открытым исходным кодом[13].

Телекомы традиционно ориентированы на сокращение расходов, оптимизацию и автоматизацию, при этом компании могут и должны искать точки (направления) роста. Устройства и датчики Интернета вещей (IoT, Internet of Things), решения для коннективности, включая Wi-Fi и Bluetooth следующего поколения, а также ожидания от внедрения сетей и технологий 5G доминируют в основных тенденциях в сфере телекоммуникаций. ИИ влияет на аналитику данных и предлагает различные возможности для автоматизации в секторе телекоммуникаций. Проникновение смартфонов и надежного Интернета приведут к генерированию ещё больших объемов контента высокого разрешения. В дополнение к этим новым тенденциям, телекоммуникационная отрасль также движется в направлении развития облачных и периферийных технологий для обеспечения интеллектуальных промышленных процессов, а также решений для улучшения человеко-машинных и машинно-машинных коммуникаций[14].

Телекоммуникационные компании могут в той мере, в которой у них есть избыточная мощность, развернуть ее для обслуживания быстрорастущих рынков центров обработки данных и облачных вычислений. Дальнейшее развитие получит фиксированная беспроводная домашняя широкополосная связь для домохозяйств, предоставление цифровой инфраструктуры, данных, контента и платформенных услуг, адаптированных к потребностям таких секторов, как развлечения и медиа (E&M), здравоохранение, производство и мобильность.
Телеком являются важнейшей опорой меняющихся высокотехнологичных рынков. Меняются позиции на игровом поле, которые могут занять (или потерять) поставщики услуг связи. Это зависит от вновь формирующихся моделей рынка, стратегий операторов связи, необходимых для достижения успеха, от инструментов, которые есть в их арсенале.

Как отмечалось, низкая стоимость доступа к сети Интернет является следствием высокой конкуренции услуг, инфраструктур и экосистем. Оценки ВШЭ показывают, что в настоящее время, в средней и дальней перспективе в России сформировались факторы роста тарифов, которые в равной мере влияют на всех участников рынка. Такая закреплённая в Стратегии динамика тарифов оправдана и не должна вызывать вопросов у регуляторов.

Также должны измениться условия экономического взаимодействия операторов связи с другими провайдерами услуг на рынке. Некоторые из них являются конкурентами, например, мессенджеры, другие контрагентами. Те и другие являются главными выгодоприобретателями развития цифрового сектора, основанного на использовании телекоммуникационных сетей и инфраструктуры, поэтому должны нести соразмерное бремя поддержания и развития сетей связи и инфраструктуры. На конечных потребителях обсуждаемые изменения условий экономического взаимодействия скажутся незначительно за счет перераспределения доходности между телекомом и ИТ сектором.

ЗАКЛЮЧЕНИЕ

На рынках связи и ИТ произошли серьёзные изменения, включая технологические сдвиги, изменения в деятельности основных игроков и структурные преобразования на рынке, изменения условий конкуренции услуг, инфраструктур, экосистем.

Телекомы создают все условия для цифровой трансформации экономики. Вклад цифрового сектора в мировой и страновой ВВП постоянно растёт, но при этом при росте вклада ИТ, вклад собственно телекома в ВВП снижается. Телекомы не получают достаточных ресурсов для будущего развития цифровых рынков из-за сдерживания развития бизнеса и структурных изменений на рынках, а также недостатков регулирования.

Необходимость реализации задач государственной стратегии отрасли связи на период до 2035 года и достижения целей развития экономики на 2030 и до 2036 года требуют смены акцентов государственного регулирования и целевых его установок от статической к динамической эффективности, уточнения параметров ценовой политики на долгосрочную перспективу, распределения вклада в развитие инфраструктуры связи между телекоммуникационными операторами и другими провайдерами на рынках цифровых услуг.

Необходимы бизнес-модели, которые позволяют сохранить темпы роста и обеспечивать при этом эффективность деятельности операторов связи. Поскольку ставится цель привлечения инвестиций в развитие отрасли в целом и развития инновационной среды, то требуется создание соответствующей перспективной модели регулирования отрасли.

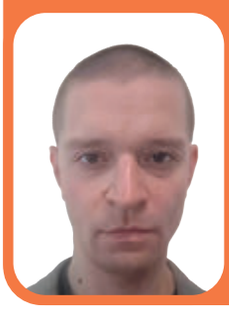
[13] Wilson Chow, Dr. Florian Gröne. Perspectives from the Global Telecom Outlook 2023 – 2027. [Электронный доступ] URL: *https://www.pwc.com/gx/en/industries/tmt/telecom-outlook-perspectives.html*
[14] Discover the Top 10 Telecom Industry Trends in 2024. [Электронный доступ] URL: *https://www.startus-insights.com/innovators-guide/top-10-telecom-industry-trends-innovations-in-2021/*



БОРИС ЕДИДИН
заместитель генерального директора
АНО «ИРИ»



АЛЕКСЕЙ БУНЬКОВ
руководитель направления
АНО «ИРИ»



АНТОН КУЛИКОВ
ведущий юрист-аналитик
АНО «ИРИ»

ПРИЗЕМЛЕНИЕ 2.0: РЕГУЛИРОВАНИЕ ДЕЯТЕЛЬНОСТИ ИНОСТРАННЫХ ИТ-КОМПАНИЙ В РОССИИ

Несмотря на то, что интернет трансграничен, деятельность интернет-компаний тем не менее осуществляется на территории конкретных юрисдикций, и должна соответствовать их законодательству. Одним из инструментов, решающих эту задачу, является так называемое «приземление» – набор требований к компаниям, включающий в себя обычно открытие юридического лица на территории страны и обеспечение прозрачного взаимодействия с регулятором. Различные варианты «приземления» интернет-компаний приняты и действуют во многих странах.

УХОД ИНОСТРАННЫХ ТЕХНОЛОГИЧЕСКИХ КОМПАНИЙ С РОССИЙСКОГО РЫНКА

В Российской Федерации специальные требования к деятельности иностранных интернет-компаний появились в июле 2021 года, когда был принят так называемый «Закон о приземлении»[1].

Закон обязывает иностранных владельцев онлайн-сервисов, доступных для российских пользователей, суточная российская аудитория которых превышает 500 000:

- опубликовать на своём ресурсе форму обратной связи;
- зарегистрировать личный кабинет в системе Роскомнадзора;
- создать филиал/представительство или учредить юридическое лицо на территории России.

Аналогичные требования предъявляются и к провайдерам хостинга, предоставляющим услуги российским клиентам.

Роскомнадзор начал включать компании в перечень попадающих под регулирование субъектов с ноября 2021 года.

В марте 2022 года в связи с началом Специальной военной операции на территории Украины (СВО) зарубежные компании массово объявили об уходе из России[2]. Всего с российского рынка ушло более 1000 компаний[3].

С разной степенью «заботы» о российских клиентах и пользователях с российского рынка ушли: Amazon, PayPal, Cisco, Dell, Ubisoft, Microsoft, Intel, Airbnb, Ericsson и другие[4]. Центр стратегических разработок (ЦСР)[5], проанализировав обстоятельства и действия компаний, которые покинули российский рынок, составил их «репутационный портрет», распределив бренды в красный, желтый и зеленый списки.

В редких случаях компании после объявления об уходе с рынка исполнили перед российскими контрагентами свои обязательства (например, Ericsson), к таким компаниям ЦСР отнёс 2% ушедших из России корпораций. В большинстве же случаев уход с рынка сопровождался неисполнением контрактов, отзывом уже приобретенных лицензий, прекращением поддержки программных продуктов и неисполнением гарантийных обязательств.

[1] Федеральный закон от 1 июля 2021г. № 236-ФЗ «О деятельности иностранных лиц в информационно-телекоммуникационной сети «Интернет» на территории Российской Федерации» // Официальный интернет-портал правовой информации (pravo.gov.ru) 19 августа 2025г. № 0001202107010014.
[2] «Какие зарубежные компании покидают Россию» // www.pnp.ru. URL: *https://www.pnp.ru/top/kakie-zarubezhnye-kompanii-pokidayut-rossiyu.html* (дата обращения: 19.08.2025г.).
[3] «Более 1000 компаний свернули свою деятельность в России» // www.securitylab.ru. URL: *https://www.securitylab.ru/news/533068.php* (дата обращения: 19.08.2025г.).
[4] «ЦСР назвал иностранные компании без шансов вернуться в Россию» // www.forbes.ru. URL: *https://www.forbes.ru/biznes/542446-csr-nazval-inostrannye-kompanii-bez-sansov-vernut-sa-v-rossiu* (дата обращения: 19.08.2025г.).
[5] Один из старейших экспертно-аналитических российских центров, который занимается исследованиями экономики, проводит отраслевую и юридическую экспертизу, анализирует и готовит предложения в области социально-экономической, региональной, регуляторной, технологической и инновационной политик и многих других сферах.

Пример некорректного ухода – австралийский сервис для графического дизайна Canva, который объявил, что блокирует доступ для России в обозримом будущем[6], а также сообщил о распределении 1 миллиона долларов США через Canva Foundation на поддержку Украины[7].

Корпорация Google снижала степень официального присутствия на российском рынке более плавно, однако дружественными её действия назвать затруднительно.

Начиная с марта 2022 года компания начала вывозить сотрудников из России за рубеж[8]. В том же месяце компания сначала ограничила рекомендации для ряда российских государственных СМИ на своих платформах[9], а затем приостановила продажу онлайн-рекламы в России[10].

В октябре 2023 года Арбитражный суд города Москвы признал дочернюю компанию ООО «Гугл» банкротом[11], а в декабре 2024 года магазин Android-приложений Google Play объявил о прекращении финансовых отношений с российскими разработчиками[12].

Принадлежащий компании видеохостинг YouTube по данным Роскомнадзора ограничил доступ к 207 российским каналам[13].

При этом под ограничения попали даже лица, не находящиеся в официальных санкционных списках юрисдикций происхождения сервиса (США и Евросоюза), например, блогеры Артемий Лебедев[14] и Стас Васильев[15].

Сама Google исчисляет количество заблокированных «связанных с Россией» YouTube-каналов в тысячах. Согласно отчётам компании, размещённым в специальном блоге Threat Analysis Group (TAG)[16], с 2020 года и до начала СВО было удалено 504 таких канала, с начала СВО и до начала «замедления» сервиса в августе 2024 года[17] – 8 121 канал, с начала «замедления» и по второй квартал 2025 года – 32 721 канал (подробные данные представлены в **приложении № 1, стр. 15**).

Однако некоторые компании действовали более прагматично. В качестве примера такой практики можно привести американскую компанию Apple, которая исполнила требования «Закона о приземлении» в полном объёме, оплатила антимонопольный штраф[18], удаляет приложения из собственного магазина по требованию российских государственных органов[19].

Компанию Apple ЦСР отнёс к зелёному списку, в который вошли те организации, ограничения со стороны которых были обусловлены санкциями или сопровождались смягчающими действиями – поддержкой персонала, сохранением инфраструктуры, поэтапным выходом.

Прошедший период показал ошибочность принятых решений об уходе с российского рынка. Российские компании смогли адаптироваться к новым обстоятельствам, внедрить собственные решения или воспользоваться глобальным характером многих рынков.

Очевидные экономические просчеты вынуждают иностранные компании пересматривать эмоциональные решения, искать пути возвращения на российских рынок, в том числе рынки онлайн сервисов, рекламы и контента.

Например, в январе 2023 года в СМИ сообщалось о возобновлении возможности скачивать софт Adobe с официального сайта компании из России[20].

[6] «Сервис графического дизайна Canva уходит из России» // iz.ru. URL: *https://iz.ru/1343143/2022-06-01/servis-graficheskogo-dizaina-canva-ukhodit-iz-rossii* (дата обращения: 19.08.2025г.).
[7] «ЦСР провел анализ ушедшего из России иностранного бизнеса» // www.csr.ru. URL: *https://www.csr.ru/ru/news/tssr-provel-analiz-ushedshego-iz-rossii-inostrannogo-biznesa/* (дата обращения: 19.08.2025г.).
[8] «Google вывезла за рубеж большую часть своих сотрудников и прекращает коммерческое присутствие в стране» // habr.com. URL: *https://habr.com/ru/news/666548/* (дата обращения: 19.08.2025г.).
[9] «Google ввела ограничения для российских государственных СМИ» // www.rbc.ru. URL: *https://www.rbc.ru/technology_and_media/01/03/2022/621e82a99a79472f67db77af* (дата обращения: 19.08.2025г.).
[10] «Google приостановила продажу рекламы в России» // www.rbc.ru. URL: *https://www.rbc.ru/business/04/03/2022/622172599a7947e607544f94* (дата обращения: 19.08.2025г.).
[11] «Суд признал банкротом российскую «дочку» Google» // www.interfax.ru. URL: *https://www.interfax.ru/russia/926491* (дата обращения: 19.08.2025г.).
[12] «Google Play прекращает все финансовые отношения с российскими разработчиками» // habr.com. URL: *https://habr.com/ru/news/866182/* (дата обращения: 19.08.2025г.).
[13] «YouTube заблокировал более 200 каналов российских СМИ и деятелей с 2020 года» // tass.ru. URL: *https://tass.ru/obschestvo/21327629* (дата обращения: 19.08.2025г.).
[14] «YouTube заблокировал канал Артемия Лебедева» // www.rbc.ru. URL: *https://www.rbc.ru/rbcfreenews/63f64d0a9a794779baae57ae* (дата обращения: 19.08.2025г.).
[15] «YouTube удалил два канала популярного российского техноблогера» // www.gazeta.ru. URL: *https://www.gazeta.ru/tech/news/2022/12/21/19327951.shtml* (дата обращения: 19.08.2025г.).
[16] «Threat Analysis Group (TAG)» // blog.google. URL: *https://blog.google/threat-analysis-group/* (дата обращения: 19.08.2025г.).
[17] «Россияне сообщили о сбоях в работе YouTube» // www.rbc.ru. URL: *https://www.rbc.ru/society/01/08/2024/66aade959a7947e13d348d20* (дата обращения: 19.08.2025г.).
[18] «ФАС: компания Apple оплатила антимонопольный штраф в размере 1,2 млрд рублей» // fas.gov.ru. URL: *https://fas.gov.ru/news/33033* (дата обращения: 19.08.2025г.).
[19] «Apple объяснила блокировку приложений VPN и СМИ для россиян» // www.rbc.ru. URL: *https://www.rbc.ru/technology_and_media/25/12/2024/676c62aa9a7947d5f9c23cd9* (дата обращения: 19.08.2025г.).
[20] «Встали под загрузку: лицензионный софт Adobe снова можно скачать в России» // iz.ru. URL: *https://iz.ru/1462268/ivan-chernousov/vstali-pod-zagruzku-litcenzionnyi-soft-adobe-snova-mozhno-skachat-v-rossii* (дата обращения: 19.08.2025г.).

В том же году зарегистрировать в Роспатенте товарный знак «Squid Game (Игра в кальмара)» пытался ушедший из России онлайн-кинотеатр Netflix[21]. Как сообщил[22] глава Роспатента Юрий Зубов, «американские агломерации Microsoft и Google традиционно регистрируют бренды IT-продуктов – смарт-часы, электронику, приложения для компьютеров и смартфонов».

В феврале 2025 года крупнейшие российские онлайн-кинотеатры (включая «Кинопоиск», «Okko») возобновили переговоры с голливудскими киностудиями по возвращению их библиотек и доступу к премьерным проектам, сообщалось в медиа[23].

В тот же период начала восстанавливать маркетинговую активность на российском рынке южнокорейская компания Samsung[24].

На пленарной сессии Форума будущих технологий Президент Российской Федерации поручил Правительству России урегулировать возвращение таких игроков рынка, оставляя преимущества для собственных производителей[25].

С учетом данных обстоятельств вопрос регулирования деятельности иностранных онлайн-сервисов в России вновь приобретает актуальность[26]. Российский союз промышленников и предпринимателей подготовил предложения по условиям возвращения иностранных компаний. Одним из актуальных решений может стать совершенствование правил работы зарубежных онлайн-сервисов в России – «Приземление 2.0».

ТЕКУЩАЯ ПРАКТИКА «ПРИЗЕМЛЕНИЯ» В РОССИИ

Перечень попадающих под «приземление» компаний доступен на сайте[27] Роскомнадзора и содержит данные о 26 лицах:

- 14 владельцах онлайн-сервисов;
- 12 провайдерах хостинга.

Как следует из данных Роскомнадзора, полностью исполнили требования закона 6 компаний: Apple, Telegram[28], Likee, Viber, AliExpress и Aviasales.

Частично исполнили требования 4 компании: Google, Twitter (X), Zoom и TikTok зарегистрировали личный кабинет на сайте Роскомнадзора. TikTok также разместил на своём ресурсе форму обратной связи.

Проигнорировали закон Discord, Pinterest, Twitch и Wikipedia, а также все 12 провайдеров хостинга.

Более подробные данные об исполнении закона приведены в таблице **(приложение № 2, стр. 16)**.

Практика показывает, что несмотря на напряжённую политическую обстановку в условиях проведения СВО, многие иностранные компании готовы к контактам с российскими государственными органами.

Следует отметить, что заложенные в Законе «О приземлении» меры понуждения к его исполнению пока применяются Роскомнадзором не в полном объеме и могут быть усилены.

Так, не применялся, например, запрет рекламы на онлайн-ресурсе нарушителя, что было бы актуально для сервисов YouTube и Twitch, а также не применялся запрет платежей в адрес нарушителей.

Одной из возможных причин постепенного применения мер принуждения может быть учет интересов отечественных рекламодателей и целесообразность продвижения товаров и услуг российского бизнеса. Запрет иностранных ресурсов как рекламных площадок может значимо на них повлиять.

По оценкам инфлюенс-агентства Digital Church[29], 40% рекламных бюджетов по итогам 2024 года приходятся на все сервисы VK (VK Video, «Клипы» и текстовые посты), 30% – на YouTube, 15% на Instagram*, около 10% приходится на Telegram, Rutube, «Одноклассники» и Yappy.

При этом отмечается, что *«несмотря на уверенный рост отечественных платформ, они пока не в состоянии*

[21] «Роспатент отказал Netflix в регистрации обозначения Squid Game (Игра в кальмара)» // rapsinews.ru. URL: *https://rapsinews.ru/incident_news/20230816/309136196.html* (дата обращения: 19.08.2025г.).
[22] «Руководитель Роспатента Юрий Зубов: Мировые бренды регистрируют товарные знаки в России в расчете вернуться на наш рынок – RG.RU» // rospatent.gov.ru. URL: *https://rospatent.gov.ru/ru/news/rospatent-04122023* (дата обращения: 19.08.2025г.).
[23] «Онлайн-кинотеатры возобновили переговоры с голливудскими студиями по кино Какие перспективы у российских стримингов» // www.rbc.ru. URL: *https://www.rbc.ru/technology_and_media/19/02/2025/67b496b19a794751c01f89af* (дата обращения: 19.08.2025г.).
[24] «Предпоставочная подготовка» // www.kommersant.ru. URL: *https://www.kommersant.ru/doc/7532247* (дата обращения: 19.08.2025г.).
[25] «Путин поручил проработать механизм возвращения иностранных компаний» // www.vedomosti.ru. URL: *https://www.vedomosti.ru/politics/articles/2025/02/21/1093717-putin-poruchil-prorabotat* (дата обращения: 19.08.2025г.).
[26] Предложения по условиям возвращения иностранных компаний подготовил Российский союз промышленников и предпринимателей.
[27] «Перечень иностранных лиц, осуществляющих деятельность в сети «Интернет» на территории Российской Федерации» // 236-fz.rkn.gov.ru. URL: *https://236-fz.rkn.gov.ru/agents/list* (дата обращения: 19.08.2025г.).
[28] По состоянию на июль 2025 года указано, что создание филиала/открытие представительства Telegram «в стадии согласования», в медиа со ссылкой на источники сообщалось (*https://t.me/lobushkin/5189*), что компания не планирует открытие офиса в России, однако однозначных официальных комментариев на этот счёт на июль 2025 года не последовало.
[29] «Инфлюенсеры хорошо разместились» // www.kommersant.ru. URL: *https://www.kommersant.ru/doc/7516408* (дата обращения: 19.08.2025г.).

* - принадлежит компании Meta, признанной экстремистской и запрещённой на территории России.

обеспечить рекламодателям ту аудиторию, которая доступна на ведущих зарубежных ресурсах».

В исследовании[30] объемов российского рынка блогеров, проведённом Комитетом по инфлюенс-маркетингу Ассоциации коммуникационных агентств России (АКАР) при участии Аналитического центра Российской индустрии рекламы (АЦ РИР), также отмечается лидерство YouTube по объему бюджетов на рекламу у блогеров. На видеохостинг приходится 47,9% рекламных размещений в стоимостном выражении (27,6 млрд руб.)[31].

Остальные рекламные бюджеты распределились по площадкам следующим образом:

- Instagram*– 20% (11,6 млрд руб.);
- Telegram – 19,8% (11,5 млрд руб.);
- VK – 11,2% (6,5 млрд руб.);
- Twitch – 0,6% (0,4 млрд руб.);
- Rutube – 0,5% (0,3 млрд руб.).

Таким образом, доля рекламных бюджетов в блогерском сегменте на российских площадках не превышает 12%, что свидетельствует о сохранении привлекательности отдельных зарубежных интернет-ресурсов для рекламодателей.

Ещё одна проблема правоприменительной практики – отсутствие для «приземлившихся» компаний стимулов, ограждающих сервисы от наиболее суровых рестрикций.

Например, в декабре 2024 года Роскомнадзор ограничил доступ к Viber в связи с нарушением требований российского законодательства к организаторам распространения информации в сети «Интернет»[32], несмотря на то, что ранее компания в полном объеме выполнила требования по «приземлению».

В таких обстоятельствах целесообразность исполнения российского законодательства для крупных международных игроков рынка не очевидна.

Это ставит перед государством дилемму поиска баланса между понуждающими мерами и позитивными возможностями, которые сделали бы привлекательным «приземление» для зарубежных игроков рынка. На основе этого подхода и может быть построено «приземление 2.0».

АКТУАЛЬНАЯ ЗАРУБЕЖНАЯ ПРАКТИКА

Одним из наиболее актуальных кейсов «приземления» за рубежом стал принятый в апреле 2024 года в США закон[33], который предписывал китайской компании ByteDance продать принадлежащей ей видеосервис TikTok, действующий на территории США, американскому лицу при сохранении за компанией аналога на территории Китая – DouYin, иначе сервис будет заблокирован. В мае 2024 года компания ByteDance оспорила положения закона в суде[34], но суд в США отклонил требование компании[35].

Закон вступил в силу 19 января 2025 года, однако президент США Д. Трамп в день вступления в должность 20 января отсрочил исполнение закона на 75 дней[36].

Как отмечается в президентском указе, Д. Трамп планирует *«принять решение, которое защитит национальную безопасность, сохранив при этом платформу, которой пользуются 170 миллионов американцев».*

Продажа зарубежного сервиса местному владельцу под угрозой блокировки – это один из наиболее прямых способов «приземления». Однако принятый закон к назначенному сроку не был исполнен – в апреле 2025 года Д. Трамп продлил отсрочку исполнения до 19 июня 2025 года[37], а затем – до 17 сентября 2025 года[38].

В октябре 2024 уже американская компания – X (ex-Twitter) – возобновила работу в Бразилии после блокировки и судебных штрафов[39].

Как сообщалось в СМИ, юридическое лицо компании в стране действовало до августа 2024 года. В дальнейшем

[30] «Исследование объемов российского рынка блогеров» // akarussia.ru. URL: *https://akarussia.ru/research/issledovanie-obemov-rossijskogo-rynka-blogerov/* (дата обращения: 19.08.2025г.).
[31] «YouTube стал лидером по размещению рекламы у блогеров в 2024 году» // www.vedomosti.ru. URL: *https://www.vedomosti.ru/media/articles/2025/05/13/1109643-youtube-stal-liderom-po-razmescheniyu-reklami* (дата обращения: 19.08.2025г.).
[32] «Роскомнадзор ограничил доступ к Viber» // t.me/rkn_tg/. URL: *https://t.me/rkn_tg/1306* (дата обращения: 19.08.2025г.).
[33] «H.R.815 – Making emergency supplemental appropriations for the fiscal year ending September 30, 2024, and for other purposes.» // www.congress.gov. URL: *https://www.congress.gov/bill/118th-congress/house-bill/815* (дата обращения: 19.08.2025г.).
[34] «TikTok и ByteDance оспорили закон о запрете приложения в суде США» // rapsi-pravo.ru. URL: *https://rapsi-pravo.ru/international_news/20240508/309877449.html* (дата обращения: 19.08.2025г.).
[35] «Суд в США постановил заблокировать TikTok 19 января» // habr.com. URL: *https://habr.com/ru/news/866856/* (дата обращения: 19.08.2025г.).
[36] «APPLICATION OF PROTECTING AMERICANS FROM FOREIGN ADVERSARY CONTROLLED APPLICATIONS ACT TO TIKTOK» // www.whitehouse.gov. URL: *https://www.whitehouse.gov/presidential-actions/2025/01/application-of-protecting-americans-from-foreign-adversary-controlled-applications-act-to-tiktok/* (дата обращения: 19.08.2025г.).
[37] «Extending the TikTok Enforcement Delay» // www.whitehouse.gov. URL: *https://www.whitehouse.gov/presidential-actions/2025/04/extending-the-tiktok-enforcement-delay/* (дата обращения: 19.08.2025г.).
[38] «FURTHER EXTENDING THE TIKTOK ENFORCEMENT DELAY» // www.whitehouse.gov. URL: *https://www.whitehouse.gov/presidential-actions/2025/06/further-extending-the-tiktok-enforcement-delay/* (дата обращения: 19.08.2025г.).
[39] «Musk's X gets OK to resume service in Brazil after bending to top court's demands» // www.reuters.com. URL: *https://www.reuters.com/technology/brazil-attorney-general-backs-reinstating-social-medial-platform-x-2024-10-08/* (дата обращения: 19.08.2025г.).

* - принадлежит компании Meta, признанной экстремистской и запрещённой на территории России.

X закрыла офисы в Бразилии, отказавшись заблокировать некоторые аккаунты в соцсети по требованию суда[40] Бразилии опасаясь ареста сотрудников.

В конечном итоге соцсеть всё же исполнила судебные постановления, заплатив назначенные штрафы, однако, вместо открытия новых офисов назначила своим юридическим представителем адвоката Рэйчел ди Оливейру Вилья Нову, которая представляла интересы компании до ухода из Бразилии.

Решение X выполнить требования государства объясняется наличием в Бразилии порядка 21,5 миллиона пользователей, что делает страну шестым по величине рынком для соцсети. Как отмечалось в СМИ, во время приостановки работы многие пользователи перешли на конкурирующие платформы.

Как видно из вышеприведённого примера, власти Бразилии устроило фактическое исполнение соцсетью обязанностей (блокировка контента и выплата штрафов) и назначение юридического представителя, без открытия дочерних юридических лиц на территории страны.

Один из наиболее свежих регуляторных кейсов – лицензирование зарубежных онлайн-сервисов в Малайзии.

1 января 2025 года Комиссия по связи и мультимедиа Малайзии сообщила[41], что китайская компания Tencent – владелец мессенджера WeChat – получила лицензию на деятельность сервиса в стране.

Регулятор сообщил, что в процессе получения лицензий находятся также Telegram и владелец сервисов Facebook, Instagram и WhatsApp – компания Meta (запрещена в России).

Лицензирование в том числе онлайн-платформ предусмотрено Законом о связи и мультимедиа 1998 года № 588[42].

Согласно принятым во исполнение закона правилам лицензирования[43], по общему правилу иностранные лица не могут получить лицензию поставщика услуг приложения. Однако, министр может *«по уважительной причине или в интересах общества»* разрешить получение лицензий таким лицам.

Таким образом, законодательство Малайзии, допускает деятельность иностранных онлайн-сервисов без открытия представительств на территории страны, используя для «приземления» механизм лицензирования.

Интересный кейс приземления не через введение обязательных требований со стороны государства, а через специальные условия присутствия компании на внутреннем рынке – соглашение о стратегическом партнёрстве между правительством Великобритании и разработчиком ChatGPT – компанией OpenAI, подписанное в июле 2025 года[44].

Компания планирует увеличить штат исследователей и инженеров лондонского офиса, предоставлять техническую информацию Британскому институту безопасности искусственного интеллекта (ИИ), а также поддерживать интеграцию сервисов ИИ в предоставление государственных услуг.

Как отмечает сама OpenAI[45], правительство Великобритании уже создало ИИ-чат-бота на базе ChatGPT, который позволяет получать государственные консультации по вопросам ведения бизнеса.

Кейс иллюстрирует возможность интеграции зарубежных компаний на локальный рынок через определение условий предоставления технологических компетенций государственным учреждениям и развития кадрового потенциала среди граждан.

ВОЗМОЖНЫЕ ВАРИАНТЫ РАЗВИТИЯ РЕГУЛИРОВАНИЯ

Как российская, так и зарубежная практика подтверждает необходимость гибкого регулирования деятельности зарубежных онлайн-платформ на территории страны для достижения баланса интересов государства, общества и бизнеса.

Формальное наличие безальтернативных запретов зачастую не способствует исполнению государственных задач, которые ставятся перед регуляторами, основная из которых – защита прав пользователей.

Рациональным решением представляется создание специальных условий деятельности зарубежных онлайн-сервисов в России, при которых, с одной стороны – будут минимизированы наиболее чувствительные риски, а с другой – согласованы определённые компромиссы.

[40] «X объявила о закрытии офиса в Бразилии из-за угроз судьи» // www.rbc.ru. URL: *https://www.rbc.ru/technology_and_media/17/08/2024/66c0cb049a7947c38f59db76* (дата обращения: 19.08.2025г.).
[41] «FOUR INTERNET MESSAGING AND SOCIAL MEDIA SERVICE PROVIDERS APPLY FOR LICENCE TO OPERATE IN MALAYSIA» // mcmc.gov.my. URL: *https://mcmc.gov.my/en/media/press-releases/four-internet-messaging-and-social-media-service-p* (дата обращения: 19.08.2025г.).
[42] «Communications and Multimedia Act 1998 [Act 588]», Статья 205, // mcmc.gov.my. URL: *https://mcmc.gov.my/en/legal/acts/communications-and-multimedia-act-1998-reprint-200?nid=523* (дата обращения: 19.08.2025г.).
[43] «COMMUNICATIONS AND MULTIMEDIA (LICENSING) REGULATIONS 2000 [P.U.(A) 129/2000]», Статья 23, // mcmc.gov.my. URL: *https://mcmc.gov.my/en/legal/acts/communications-and-multimedia-act-1998-reprint-200/communications-and-multimedia-(licensing)-regulati* (дата обращения: 19.08.2025г.).
[44] «OpenAI to expand UK office and work with government departments to turbocharge the UK's AI infrastructure and transform public services» // www.gov.uk. URL: *https://www.gov.uk/government/news/openai-to-expand-uk-office-and-work-with-government-departments-to-turbocharge-the-uks-ai-infrastructure-and-transform-public-services* (дата обращения: 19.08.2025г.).
[45] «OpenAI and UK Government announce strategic partnership to deliver AI-driven growth» // openai.com. URL: *https://openai.com/global-affairs/openai-and-uk-government-partnership/* (дата обращения: 19.08.2025г.).

В рамках данного подхода иностранные компании – владельцы крупных интернет-сервисов могли бы заключать специальные контракты с регулятором, которые предусматривают условия деятельности в России, в том числе:

1) инвестиции в разработку российских технологических решений (например, искусственного интеллекта, рекомендательных систем и т.д.), либо передача неисключительных прав на такие решения российским партнерским организациям с правом внесения в них изменений, либо проекты по совместной разработке решений, либо интеграция российских решений в сервисы;
2) интеграция с российскими платёжными системами;
3) поддержка российского контента в различных формах, включая финансовые (гранты на производство контента, инвестиции в российские студии разработки видеоигр и др.) и нефинансовые (продвижение российского контента на платформах (например, раздел «Сделано в России» в магазинах приложений, приоритезация российского контента для русскоговорящих пользователей в поисковых выдачах), организация повышения квалификации контентмейкеров (специалистов по созданию разнообразного и привлекательного контента для онлайн-платформ), разработчиков и др.);
4) интеграция с российскими рекламными системами;
5) прозрачная система модерации, ограничение доступа к наиболее опасному контенту, сопряжённому с совершением преступлений (распространение наркотиков, детская порнография и т.д.), восстановление страниц пользователей, заблокированных площадкой, нарушения которых не доказаны, взаимодействие с российскими уполномоченными организациями для рассмотрения обжалований и принятия решений о разблокировке в спорных ситуациях;
6) определение уполномоченного на взаимодействие с государственными органами и общественными организациями лица без физического присутствия на территории России;
7) открытие счёта в российском банке;
8) признание юрисдикции российских судов в спорах с российскими гражданами и организациями;
9) инвестиции в строительство центров обработки данных и других инфраструктурных объектов на территории России.

В качестве нормативных послаблений зарубежным онлайн-ресурсам можно предложить:

1) неприменение мер по полной или частичной блокировке ресурса;
2) учёт специфики работы с данными;
3) частичный учёт политик и правил модерации контента платформ при принятии мер, касающихся удаления спорного контента;
4) вариативность способов исполнения обязанностей организатора распространения информации при условии достижения целей регулирования указанных субъектов;
5) возможность наделения российских компаний и профессиональных участников рынка функциями представления интересов зарубежных корпораций.

Важно предусмотреть возможность гибкой настройки условий для каждой крупной технологической компании, желающей работать в российском правовом поле.

Предлагаемые нормы могут быть закреплены в нескольких актах федерального законодательства, среди которых, например:

- Федеральный закон от 01.07.2021г. № 236-ФЗ «О деятельности иностранных лиц в информационно-телекоммуникационной сети «Интернет» на территории Российской Федерации»;
- Федеральный закон от 31.07.2020г. № 247-ФЗ «Об обязательных требованиях в Российской Федерации»;
- Федеральный закон от 27.07.2006г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;
- Федеральный закон от 09.07.1999г. № 160-ФЗ «Об иностранных инвестициях в Российской Федерации».

Альтернативным вариантом закрепления предлагаемого регулирования, применяемого и к российским технологическим компаниям, может стать установление экспериментального правового режима в сфере цифровых инноваций[46].

Это позволит на время приостановить действие отдельных норм, регулирующих онлайн-пространство в России, оценить последствия такого приостановления для достижения целей развития государства и общества и выбрать наиболее результативную стратегию развития регулирования информационных технологий.

[46] В соответствии с нормами Федерального закона от 31 июля 2020 года № 258-ФЗ «Об экспериментальных правовых режимах в сфере цифровых инноваций в Российской Федерации» // Официальный интернет-портал правовой информации (pravo.gov.ru) 19 августа 2025г. № 0001202007310024.

ПРИЛОЖЕНИЕ №1

Таблица блокировки YouTube-каналов, «связанных с Россией»

№ п/п	Квартал	Количество заблокированных YouTube-каналов, связанных с Россией	Источник
1.	Q1 2020	0	*https://blog.google/threat-analysis-group/tag-bulletin-q1-2020/*
2.	Q2 2020	86	*https://blog.google/threat-analysis-group/tag-bulletin-q2-2020/*
3.	Q3 2020	0	*https://blog.google/threat-analysis-group/tag-bulletin-q3-2020/*
4.	Q4 2020	54	*https://blog.google/threat-analysis-group/tag-bulletin-q4-2020/*
5.	Q1 2021	53	*https://blog.google/threat-analysis-group/tag-bulletin-q1-2021/*
6.	Q2 2021	196	*https://blog.google/threat-analysis-group/tag-bulletin-q2-2021/*
7.	Q3 2021	0	*https://blog.google/threat-analysis-group/tag-bulletin-q3-2021/*
8.	Q4 2021	115	*https://blog.google/threat-analysis-group/tag-bulletin-q4-2021/*
Начало СВО			
9.	Q1 2022	710	*https://blog.google/threat-analysis-group/tag-bulletin-q1-2022/*
10.	Q2 2022	169	*https://blog.google/threat-analysis-group/tag-bulletin-q2-2022/*
11.	Q3 2022	26	*https://blog.google/threat-analysis-group/tag-bulletin-q3-2022/*
12.	Q4 2022	909	*https://blog.google/threat-analysis-group/tag-bulletin-q4-2022/*
13.	Q1 2023	735	*https://blog.google/threat-analysis-group/tag-bulletin-q1-2023/*
14.	Q2 2023	847	*https://blog.google/threat-analysis-group/tag-bulletin-q2-2023/*
15.	Q3 2023	217	*https://blog.google/threat-analysis-group/tag-bulletin-q3-2023/*
16.	Q4 2023	411	*https://blog.google/threat-analysis-group/tag-bulletin-q4-2023/*
17.	Q1 2024	77	*https://blog.google/threat-analysis-group/tag-bulletin-q1-2024/*
18.	Q2 2024	4020	*https://blog.google/threat-analysis-group/tag-bulletin-q2-2024/*
«Замедление» YouTube			
19.	Q3 2024	16 870	*https://blog.google/threat-analysis-group/tag-bulletin-q3-2024/*
20.	Q4 2024	9 429	*https://blog.google/threat-analysis-group/tag-bulletin-q4-2024/*
21.	Q1 2025	4 369	*https://blog.google/threat-analysis-group/tag-bulletin-q1-2025/*
22.	Q2 2025	2 053	*https://blog.google/threat-analysis-group/tag-bulletin-q2-2025/*

ПРИЛОЖЕНИЕ №2

Таблица исполнения «Закона о приземлении»

№ п/п	Компания	Страна	Тип	Форма	Юр. лицо	ЛК РКН	Меры принуждения
1.	Google LLC	США	Онлайн-сервис	–	–	+	Информирование Запрет рекламы сервиса
2.	**Apple Distribution International Ltd.**	Ирландия	Онлайн-сервис	+	+	+	Не применяются
3.	Twitter, Inc. (X)	США	Онлайн-сервис	–	–	+	Не применяются
4.	TikTok Pte. Ltd.	Сингапур	Онлайн-сервис	+	–	+	Информирование
5.	**Telegram Messenger, Inc.**	Британские Виргинские	Онлайн-сервис	+	+	+	Информирование
6.	Zoom Communications, Inc.	США	Онлайн-сервис	–	–	+	Информирование
7.	**Likeme Pte.ltd. (Likee)**	Сингапур	Онлайн-сервис	+	+	+	Не применяются
8.	**Viber Media S.à r.l.**	Люксембург	Онлайн-сервис	+	+	+	Не применяются
9.	Discord, Inc.	США	Онлайн-сервис	–	–	–	Информирование
10.	Pinterest, Inc.	США	Онлайн-сервис	–	–	–	Информирование
11.	Twitch Interactive, Inc.	США	Онлайн-сервис	–	–	–	Информирование
12.	Wikimedia Foundation, Inc. (Wikipedia)	США	Онлайн-сервис	–	–	–	Информирование
13.	**AliExpress CIS Holding PTE. LTD**	Сингапур	Онлайн-сервис	+	+	+	Не применяются
14.	Hetzner Online GmbH	Германия	ПХ	–	–	–	Полная блокировка Запрет поиска Информирование

№ п/п	Компания	Страна	Тип	Форма	Юр. лицо	ЛК РКН	Меры принуждения
15.	Network Solutions, LLC	США	ПХ	–	–	–	Полная блокировка Запрет поиска Информирование
16.	WPEngine, Inc.	США	ПХ	–	–	–	Полная блокировка Запрет поиска Информирование
17.	HostGator.com, LLC	США	ПХ	–	–	–	Полная блокировка Запрет поиска Информирование
18.	Ionos Inc.	США	ПХ	–	–	–	Полная блокировка Запрет поиска Информирование
19.	DreamHost, LLC	США	ПХ	–	–	–	Полная блокировка Запрет поиска Информирование
20.	FastComet, Inc.	США	ПХ	–	–	–	Полная блокировка Запрет поиска Информирование
21.	Amazon Web Services, Inc.	США	ПХ	–	–	–	Полная блокировка Запрет поиска Информирование
22.	GoDaddy.com LLC	США	ПХ	–	–	–	Полная блокировка Запрет поиска Информирование
23.	Bluehost Inc.	США	ПХ	–	–	–	Полная блокировка Запрет поиска Информирование
24.	Kamatera Inc.	США	ПХ	–	–	–	Полная блокировка Запрет поиска Информирование
25.	DigitalOcean, LLC	США	ПХ	–	–	–	Полная блокировка Запрет поиска Информирование
26.	**Go Travel Un Limited (Aviasales)**	Гонконг (Китай)	Онлайн-сервис	+	+	+	Не применяются



ВЛАДИМИР ГОРЖАЛЦАН
советник директора
Координационного центра доменов .RU/.РФ

КИРИЛЛИЧЕСКОМУ ДОМЕНУ .РФ 15 ЛЕТ

1. КАК И КОГДА ЭТО ВСЕ СЛУЧИЛОСЬ

Еще в декабре 1996 году Мартин Дёрст из Университета Цюриха предложил сделать доменные имена доступными для пользователей на их родном языке. Так появилась идея IDN-доменов (Internationalized Domain Names), которые содержат символы национальных алфавитов: китайского, арабского, греческого, кириллицы и других.

Аббревиатура IDN[1] расшифровывается как «интернационализированное доменное имя». IDN — это доменное имя, содержащее символы из набора символов Unicode. Другими словами, интернационализированные доменные имена могут содержать буквы, например, с диакритическими знаками, как того требуют многие европейские языки, или символы нелатинских алфавитов, таких как кириллический, арабский или китайский.

В июне 2008 года в Москве на 10-м Всемирном Конгрессе русской прессы Президент Российской Федерации Д.А. Медведев заявил, что Россия не оставит без реакции попытки притеснения русскоязычных изданий[2]. «Необходимо добиваться появления кириллических доменных имен[3]. "Мы должны сделать все от нас зависящее, чтобы добиться присвоения России доменных имен на кириллице. Это символическая значимость русского языка, и у нас неплохие шансы добиться соответствующего решения».[4]

С 22 по 26 июня 2008 года в Париже проходила 32-я Международная конференция ICANN[5]. На этой конференции было принято решение о введении по ускоренной процедуре «fast track» доменов верхнего уровня на национальных нелатинских алфавитах (IDNs).

Президент ICANN Пол Туми тогда сказал, что желание России получить кириллический домен верхнего уровня .РФ является важным политическим решением руководства страны, которое позволяет утверждать, что России не придется ждать несколько лет до момента окончания разработки общих правил делегирования IDNs. Пол Туми пообещал, что для России делегирование кириллического домена будет сделано по ускоренной процедуре.

Здесь также следует вспомнить, что уже в октябре 2009 года на ежегодном заседании Правления ICANN в Южной Корее в Сеуле прошло одобрение процесса ускоренной регистрации национальных интернационализированных доменов верхнего уровня. Оно позволило странам и территориям подавать запросы в ICANN на домены IDN ccTLD[6], представляющие соответствующие названия стран или территорий на алфавитах, отличных от латинского[7].

И 12 мая 2010 года домен .РФ был делегирован для России в качестве домена верхнего уровня с двухбуквенным кодом страны и стал, таким образом, первым в мире кириллическим доменом.

В отчете для делегирования IANA[8] сделана запись **(см. рис. 1)** о том, что полномочия по данной записи делегирования кириллического домена .РФ для Российской Федерации представляются Координационному центру домена верхнего уровня .RU. Дата регистрации 2010-05-12.

На сегодняшний день в мире делегирован 151 IDN-домен верхнего уровня, за последний год их число не изменилось. Из них 90 относятся к общим доменам, а 61 – к национальным доменам верхнего уровня – 9 из них кириллические **(см. рис. 2)**.

[1] ITU Telecommunication Standardization Sector [Электронный ресурс]. URL: *https://www.itu.int/ITU-T/special-projects/idn/faq.html*
[2] [Электронный ресурс]. URL: *https://web.archive.org/web/20101117152245/http://www.vesti.ru/doc.html?id=187599&cid=1*
[3] [Электронный ресурс]. URL: *https://web.archive.org/web/20220129143703/https://info.nic.ru/st/66/out_2050.shtml*
[4] Открыл Конгресс Дмитрий Медведев, Президент России. Во вступительном слове он затронул и тему возможного делегирования нашей стране кириллического домена .РФ. [Электронный ресурс]. URL: *https://web.archive.org/web/20220129143703/https://info.nic.ru/st/66/out_2050.shtml*
[5] ICANN (Internet Corporation for Assigned Names and Numbers) – «Корпорация по назначению имен и номеров интернета», международная некоммерческая организация, созданная в 1998 году для регулирования вопросов, связанных с доменными именами, IP-адресами и прочими аспектами функционирования интернета, включая стабильность и безопасность. ICANN осуществляет координацию и поддержку функционирования системы имен и адресов в интернете. Одной из основных политик ICANN является расширение адресного пространства за счет создания новых доменов верхнего уровня, в том числе с использованием символов национальных алфавитов.
[6] ccTLD – национальные (страновые) домены верхнего уровня (англ. country-code top level domains, ccTLD) – обозначаемые двухбуквенными именами домены верхнего уровня (двухбуквенный национальный код ISO 3166), выделенные корпорацией ICANN для всех государств и ряда административных территорий мира.
[7] Ускоренная процедура IDN ccTLD [Электронный ресурс]. URL: *https://www.icann.org/resources/pages/fast-track-2012-02-25-en*
[8] IANA (Internet Assigned Numbers Authority) – администрация адресного пространства интернета. На самом деле это не организация, а функция управления пространствами IP-адресов, доменов верхнего уровня, а также регистрирующая типы данных MIME и параметры прочих протоколов интернета.



Рис.1. Запись о домене .РФ на корневых серверах мировой системы доменных имен (DNS), которую IANA разместила 12 мая 2010г.

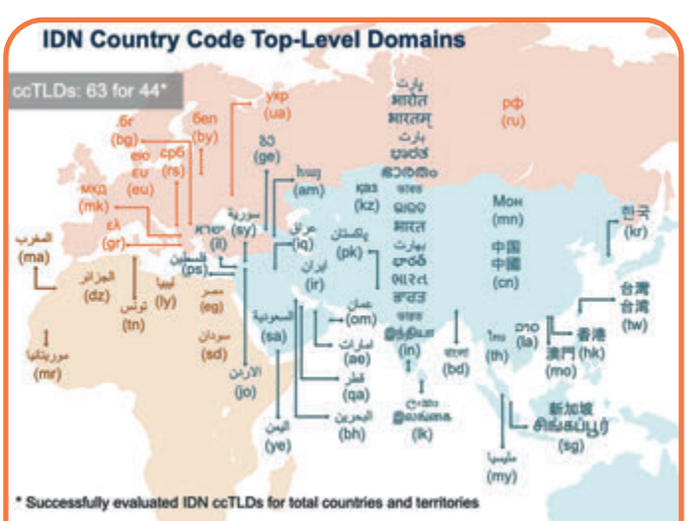


Рис. 2. Интернационализированные национальные домены верхнего уровня (IDN) на карте мира

Кириллические домены способствуют культурной и лингвистической идентификации. Кириллица — это тоже национальный символ, и любая надпись на ней — это национальная идентификация. Национальная идентификация, в том числе и в интернете, позволяет нам расширить наши знания о богатстве национальной культуры.

2. ДЛЯ ЧЕГО ЭТО НАДО (IDN, IDNA, EAI, UA И ПР.)

IDN — это интернационализированное доменное имя, но как реализовать работу таких имён? В 2003 году была разработана первая версия стандарта IDNA (интернационализированные доменные имена в приложениях) — это набор RFC[9], предназначенный для работы с доменными именами, содержащими символы, отличные от ASCII символов. IDNA был разработан рабочей группой IETF (The Internet Engineering Task Force[10]) и существенно переработан к 2008 году. Актуальная на сегодня версия стандарта IDNA 2008г. содержит RFC 5890-5895 и RFC 3492.

Внедрение IDNA не требует внесения изменений в существующую интернет-инфраструктуру и систему доменной адресации DNS. Основная идея заключается в преобразовании символов Unicode, в соответствующие ASCII символы по алгоритму Punycode, который описан в RFC 3492[11] стандарта IDNA 2008г. Такое решение обеспечивает максимальную совместимость с существующей системой DNS, которая поддерживает только домены, использующие символы ASCII.

И только в 2009 году интернет-корпорация ICANN одобрила создание интернационализированных доменов верхнего уровня с кодами стран (IDN ccTLD), использующих стандарт IDNA[12].

В мире существуют множество языков и алфавитов. IDN повышают узнаваемость контента и привлекательность использования интернета на родном языке. Неанглоязычная аудитория использует клавиатуры, на которых доступен национальный алфавит, поэтому, когда они ищут доменное имя, имеет смысл сделать эти домены доступными для них. Для компании также важно иметь идентификаторы бренда не только на английском языке, но и на любом языке мира.

Попробуем сформулировать, что необходимо для того, чтобы реализовать эту задачу. Нужно обеспечить состояние, когда все интернет-приложения, устройства и системы правильно и единообразно принимают, проверяют, хранят, обрабатывают и отображают все

[9] RFC (англ. Request for Comments – букв. «запрос комментариев», «тема для обсуждения») – рабочее предложение, документ из серии пронумерованных информационных документов интернета, которые содержат технические спецификации и стандарты, широко применяемые во всемирной сети и регламентирующие внутреннюю жизнь интернета.

[10] IDNA (интернационализированные доменные имена в приложениях) — это механизм, разработанный для работы с интернет-доменными именами, содержащими символы, отличные от букв/цифр/дефисов (LDH) [Электронный ресурс]. URL: *https://www.itu.int/ITU-T/special-projects/idn/faq.html* Руководящая группа по разработке интернет-технологий (IESG) отвечает за техническое управление деятельностью IETF и процессом разработки интернет-стандартов.

[11] [Электронный ресурс]. URL: *https://mailarchive.ietf.org/arch/msg/rfc-dist/4rKiSjvJh60vcUikYsEFaQ0LUXg/*

[12] «ICANN объединяет языки мира в глобальном Интернете» (пресс-релиз). Интернет-корпорация по присвоению имен и номеров (ICANN). [Электронный ресурс]. URL: *http://www.icann.org/en/announcements/announcement-30oct09-en.htm*

корректные доменные имена и адреса электронной почты. А само состояние называется универсальное принятие (UA, Universal Acceptance)[13]. Универсальное принятие гарантирует, что все доменные имена, включая новые домены верхнего уровня (new gTLD), интернационализированные доменные имена и адреса электронной почты, рассматриваются одинаково и могут использоваться всеми приложениями, устройствами и системами, подключенными к интернету[14].

До настоящего времени проблема универсального принятия остается нерешенной в общем виде. Её решение для России предусматривает предоставление равной поддержки кириллическим доменам и адресам электронной почты, наравне с латинскими во всем российском программном обеспечении, в том числе государственными информационными системами, отечественными социально значимыми проектами и крупными российскими интернет-сервисами. Доступность сетевых технологий для широких слоев населения России сегодня является одним из ключевых векторов цифрового развития государства, поэтому предоставление возможности использования интернета на русском языке, включая не только контент и пользовательские интерфейсы, но и средства интернет-адресации, такие как кириллические доменные имена и адреса электронной почты, способствует повышению доступности интернет услуг для большего числа российских граждан и улучшает пользовательский опыт. Проблема универсального принятия и обеспечения равной поддержки для всех доменных имен, независимо от набора символов (латиницы или символов национального языка), а также адресов электронной почты с их использованием является одним из ключевых сдерживающих факторов, который мешает дальнейшему развитию и популяризации российской национальной доменной зоны.

Вся поддержка интернационализированных доменных имен происходит вне самой системы DNS, т.е. на уровне приложений и пользовательского интерфейса. А задача сводится к трансляции символов Unicode в формат ASCII.

Если посмотреть на то, как используют преимущества IDN, то можно увидеть множество полезных примеров. Так, в России IDN используются для визуального маркетинга. Исследование показало, что человеку требуется немного времени, чтобы распознать и запомнить доменное имя на кириллице, но значительно больше времени, чтобы запомнить адрес на латинице[15]. Многие компании в России начали использовать IDN для этой цели, а затем перенаправлять пользователей на свои сайты на латинице. Таким образом, у людей и компаний появились новые возможности.

ИНТЕРНАЦИОНАЛИЗИРОВАННАЯ ЭЛЕКТРОННАЯ ПОЧТА

Интернационализированная электронная почта появилась благодаря сочетанию интернационализированных доменных имён и интернационализации адресов электронной почты (EAI).

Для полноценного использования электронной почты во всем мире необходимо, чтобы все могли использовать доменные имена, правильно написанные на родном языке и с использованием символов национальных алфавитов, в качестве имен почтовых ящиков в адресах электронной почты[16]. Чтобы использовать интернационализированные адреса электронной почты, нужно обеспечить поддержку как доменной, так и локальной части адресов электронной почты.

Напомним, адрес электронной почты (email) состоит из двух частей: локальной и доменной. Эти части разделены символом «@»[17]. Локальная часть идентифицирует пользователя в почтовом сервисе. Она располагается перед символом «@». Доменная часть указывает на IP-адрес, на котором размещен почтовый сервер. Интернационализированная доменная часть адресов электронной почты может быть преобразована в ASCII по алгоритму Punycode (RFC 3492), а локальная часть — нет. Если имена и инициалы, используемые в адресах электронной почты, смогут быть выражены на родных языках и в системах письменности пользователей, интернет будет восприниматься как нечто более естественное, особенно теми, чей родной язык не написан латиницей.

3. О ЯЗЫКАХ

В мире, по оценкам ЮНЕСКО, существует 8324 языка, из них около 7 тыс. в обращении, остальные уже не используются. Несколько сотен основных языков задействованы в образовательных системах и в госучреждениях, менее сотни — в сфере цифровых технологий. Каждые несколько недель со смертью последнего носителя в мире исчезает один редкий язык, а всего под угрозой исчезновения 40% «языкового запаса» Земли[18]. По подсчетам справочника по языкам мира Ethnologue, более 40% населения Земли (3,6 млрд человек) говорят на 20 ведущих международных языках. Таким образом, активно задействовано лишь 0,3% мирового языкового богатства. Самые распространенные языки — английский и китайский. В десятку ведущих международных языков входит и

[13] Универсальное принятие (UA) — состояние, когда все интернет-приложения, устройства и системы правильно и единообразно принимают, проверяют, хранят, обрабатывают и отображают все корректные доменные имена и адреса электронной почты.
[14] ICANN Universal Acceptance (UA). URL: *https://www.icann.org/ua*
[15] «Как слышится, так и пишется» - видеоролик ролик Координационного центра доменов .RU/.РФ [Электронный доступ]. URL: *clck.ru/3P7kHE*
[16] Обзор и структура интернационализированной электронной почты RFC 4952. URL: *https://datatracker.ietf.org/doc/rfc4952/*
[17] Официальное название знака в соответствии со стандартами ИСО, МСЭ и Юникод — **коммерческое *at*** ([æt]; англ. *commercial at*), такое же название («коммерческое "эт"») закреплено в российских ГОСТах. Кроме того, ранее использовалось название «коммерческий знак "at"».
[18] [Электронный ресурс]. URL: *https://www.kommersant.ru/doc/7497443*

русский. Организация Объединённых Наций так отмечает важность многоязычия в мире:

Многоязычие важно, поскольку оно позволяет добиться того, чтобы люди понимали друг друга; оно помогает нам вместе работать над дальнейшим построением более светлого будущего для всех. Многоязычие способствует укреплению диалога между людьми разного происхождения и обеспечению терпимости в отношениях между странами. Без многоязычия Организация Объединенных Наций не смогла бы эффективно функционировать. Языки связывают наше прошлое, настоящее и будущее; они соединяют все возрастные и этнические группы — всех нас. Многоязычие можно считать одним из основополагающих принципов Организации Объединенных Наций, хотя оно и не упоминается в Уставе Организации[19].

В России, где используются 152 языка, статус менее 10% из них можно назвать благополучным. Остальные языки под угрозой исчезновения, с все меньшим числом говорящих[20]. Официальная оценка этого явления с демографической точки зрения не известна, однако с позиции мультикультурного, языкового многообразия и его наследия полагаем, что это не очень позитивные тенденции. В то же время, бережное отношение, даже к самым небольшим, сохранившимся языковым группам очень важно для сохранения культурного наследия всей России. В Конституции (Основном законе) Российской Федерации в статье 68 написано следующее:

1. *Государственным языком Российской Федерации на всей ее территории является русский язык как язык государствообразующего народа, входящего в многонациональный союз равноправных народов Российской Федерации.*
2. *Республики вправе устанавливать свои государственные языки. В органах государственной власти, органах местного самоуправления, государственных учреждениях республик они употребляются наряду с государственным языком Российской Федерации.*
3. *Российская Федерация гарантирует всем ее народам право на сохранение родного языка, создание условий для его изучения и развития.*
4. *Культура в Российской Федерации является уникальным наследием ее многонационального народа. Культура поддерживается и охраняется государством.*

Таким образом, Конституция Российской Федерации устанавливает:

- Государственный язык - русский;
- Государственные языки субъектов – в республиках Российской Федерации, которых сегодня **24** (Республика Крым — русский язык).

При этом, в одной республике – Дагестане, по Конституции Республики Дагестан государственными на территории республики являются русский язык и все языки народов Дагестана (т.е. - еще **13** языков, кроме русского.)

- Языки с официальным статусом, установленные органами местного самоуправления – всего 10 языков.

Следовательно, обобщая статус государственных языков, имеем следующие наборы государственных языков России **(см. таблицу 1)**.

Итак, роль языка в жизни человека заключается в следующем:

- Коммуникация. С помощью языка люди передают друг другу информацию, делятся знаниями и опытом. Язык позволяет людям сотрудничать, строить сложные общественные структуры и решать коллективные задачи.
- Носитель культуры. Язык отражает уникальную картину мира каждого народа. В его структуре, лексике и идиомах скрыты исторические, культурные и природные особенности. Через язык передаются сказки, легенды, пословицы и поговорки, которые формируют мировоззрение человека с детства.

Таблица 1. Государственные и официальные языки народов России.

Федеральный язык	русский
Языки субъектов федерации	абазинский • аварский • агульский • адыгейский • азербайджанский • алтайский • башкирский • бурятский • даргинский • ингушский • кабардино-черкесский • калмыцкий • карачаево-балкарский • коми • кумыкский • лакский • лезгинский • ногайский • марийский • мокшанский • осетинский • рутульский • табасаранский • татарский • татский • тувинский • удмуртский • хакасский • цахурский • чеченский • чувашский • эрзянский • якутский
Языки с официальным статусом	вепсский • долганский • казахский • карельский • коми- пермяцкий • финский • чукотский • эвенкийский • эвенский • юкагирский

[19] [Электронный ресурс]. URL: *https://www.un.org/sites/un2.un.org/files/2227864r.pdf*
[20] Проект «Языки России», Институт языкознания РАН, Руководитель проекта — ст.н.с., к.ф.н. Коряков Ю. Б., Участники проекта: Т.И. Давидюк, А.П. Евстигнеева, В. В. Иванов, М. А. Каде, А. А. Сюрюн, В. С. Харитонов. Данный проект посвящён языкам России, критериям отбора и составлению их списка. [Электронный доступ]. URL: *https://jazykirf.iling-ran.ru/*

- Основа для передачи знаний и развития науки. На всех этапах обучения язык используется для объяснения, обсуждения и понимания новых концепций.
- Обеспечение связи времён. Язык бережёт опыт народа, накапливает знания и передаёт их от поколения к поколению.

4. О ПИСЬМЕННОСТИ

Письменность, последующий, после языка, этап в эволюции народа, является важнейшим инструментом передачи знаний, культуры и истории, а также одним из главных средств общения и сохранения информации. В случае с русским языком, его письменная традиция тесно связана с развитием культуры и государственной системы. В основе русской письменности лежит алфавит, преимущественно использующий кириллицу, однако, этот путь был долгим и насыщенным различными изменениями[21]. Длинный путь славянской письменности от глаголицы, в девятом веке, до современной кириллицы был пройден за многие сотни лет. Работы первопроходцев от Кирилла и Мефодия до реформатора Петра I и работ Михаила Васильевича Ломоносова над Грамматикой русского языка, других реформаторов XVIII-XIX-го веков вызывают и сегодня большой культурный интерес не только в профессиональной среде.

В современной России пунктом 6 статьи 3 закона Российской Федерации от 25.10.1991г. № 1807-1 (ред. от 13.06.2023г.) «О языках народов Российской Федерации» установлено:
«В Российской Федерации алфавиты государственного языка Российской Федерации и государственных языков республик строятся на графической основе кириллицы. Иные графические основы алфавитов государственного языка Российской Федерации и государственных языков республик могут устанавливаться федеральными законами».

А пунктом 7 статьи 3 того же закона определено, что *«Порядок утверждения норм языков коренных малочисленных народов Российской Федерации, правил орфографии и пунктуации этих языков определяется Правительством Российской Федерации».*

В России до конца XVIII — начала XIX веков большинство народов не имели своей письменности. Старописьменная традиция была у русских, украинцев и белорусов (на кириллице), народов Прибалтики (на латинице), грузин и армян (национальные алфавиты). Мусульманские народы Поволжья, Кавказа и Средней Азии ограничено пользовались арабским письмом[22].

После Октябрьской революции 1917 года начинается активное развитие национальных письменностей. Проходит множество учительских съездов, разрабатывается орфография для бесписьменных в тот момент языков, утверждаются алфавиты. В Москве, а затем и в других городах начинается массовое издание национальных букварей, значительно расширяется издание периодики.

В конце 1970-х годов вновь начинается процесс создания письменности для малочисленных народов СССР. Почти все новые алфавиты создаются на кириллице. Этот процесс продолжается до сих пор.

После распада СССР ряд народов республик бывшего Советского Союза перешёл на латинский алфавит: молдаване, азербайджанцы (в Азербайджане)[23], узбеки, каракалпаки и туркмены.

5. ЧТО ПИСАЛИ СМИ ВЕСНОЙ 2010 ГОДА О КИРИЛЛИЧЕСКОМ ДОМЕНЕ .РФ

Весной 2010 года весть о делегировании кириллического домена .РФ для России облетела многие российские СМИ, информация некоторых СМИ приведена на **рисунке 3**.

6. ЧТО ДЕЛАЕТ КООРДИНАЦИОННЫЙ ЦЕНТР ДОМЕНОВ .RU/.РФ ДЛЯ РЕШЕНИЯ ПРОБЛЕМЫ УНИВЕРСАЛЬНОГО ПРИНЯТИЯ

В Российской Федерации вопросами универсального принятия занимается регистратура национальных российских доменов верхнего уровня – Координационный центр доменов .RU/.РФ, аккредитованные регистраторы и эксперты Российской рабочей группы по универсальному принятию (создана в 2020 году), также Ассоциация Разработчиков Программных Продуктов (АРПП) «Отечественный Софт», вовлечено в это процесс и Минцифры России, в том числе и с проектом о внесении изменений в части включения дополнительных требований по поддержке кириллических средств интернет адресации в Постановление Правительства Российской Федерации от 23 марта 2017 года № 325 (ред. от 07.03.2018г.) «Об утверждении дополнительных требований к программам для электронных вычислительных машин и базам данных, сведения о которых включены в реестр российского программного обеспечения, и внесении изменений в Правила формирования и ведения единого реестра российских программ для электронных вычислительных машин и баз данных».

В рамках работы по данному проекту члены АРПП при

[21] Грамматический метод обучения русскому правописанию. Книга 1. Лекции по орфографии
Наталия Петровна Киреева. Идеальным принято считать алфавит, построенный по фонематическому принципу: количество букв, соответствует количеству фонем языка, причём каждая фонема выражается одной и той же буквой, независимо от позиции, в которую она попадает. Однако, практика показывает, что «идеальных алфавитов в мире нет, а существуют лишь более или менее рациональные».
[22] М. И. Исаев. Языковое строительство в СССР. — М.: «Наука», 1979г. — 352с. — 2650 экз.
[23] В настоящее время для записи азербайджанского языка существуют три официальные графические системы: в Азербайджане — на латинице, в Иране — на арабском письме, в России (Дагестан) — на кириллице.



Рис. 3 Российские СМИ о делегировании кириллического домена .РФ для России.

поддержке Координационного центра реализуют пилотный проект для изучения возможностей по доработке российских программных продуктов в части реализации полного перечня требований по универсальному принятию.

Координационный центр ежегодно проводит исследования для замера уровня поддержки универсального принятия веб-ресурсами и почтовыми серверами. В 2021 году было проведено исследование о поддержке кириллических адресов электронной почты на сайтах социально значимых в Российской Федерации информационных ресурсов. Результаты исследования и предложения по их использованию были направлены в Минцифры России.

В 2025 году домену .РФ исполнилось 15 лет, и за время существования домена множество продуктов и сервисов начало работать с кириллическими доменными именами и почтовым адресами. В настоящее время в доменной зоне .РФ зарегистрировано более 770 тысяч доменных имен, при этом делегировано 725 тысяч имен, что составляет 95,4% от общего количества доменов.

Почти 29% доменных имен ведут на приложения и одностраничные сайты (лендинги, рекламные

объявления и т. д.), 25% указывают на полноценные уникальные веб-сайты, еще 24% находятся на парковке, на 14% расположены исключительно почтовые сервисы и 8% используются для перенаправления на сайты, имеющие адреса и в других доменных зонах. Любопытно, что используют доменные имена .РФ "по назначению", то есть для размещения веб-сайтов, чаще всего вовсе не в Москве или Санкт-Петербурге, а в других регионах России. Так, в Республике Саха (Якутия) веб-сайты размещены на 36,3% зарегистрированных в этом регионе доменных имен в .РФ. Также высокими показателями практического использования домена .РФ могут похвастаться Омская область (34,4%), Севастополь (33,6%), Калмыкия (33,4%) и Еврейская АО (32,6%).

Более 18% доменных имен в .РФ старше 10 лет, а больше всего (почти 40%) имен в домене .РФ имеют возраст от 1 года до 5 лет. Почти 35% имен в .РФ зарегистрированы в Москве и Московской области, также домен .РФ популярен в Санкт-Петербурге (7,1%), Краснодарском крае (3,2%), Свердловской (3%), Челябинской (2,2%) и Новосибирской (2,2%) областях.

А 11 августа 2025 года в российской национальной доменной зоне .РФ стала доступна регистрация интернет-адресов с использованием символов 17 государственных языков республик Российской Федерации. Нововведение значительно расширяет возможности пользователей создавать доменные имена, которые более точно отражают особенности письменности и произношения различных языков народов России. Теперь в именах сайтов могут использоваться буквы абазинского, адыгейского, алтайского, башкирского, бурятского, ингушского, кабардино-черкесского, калмыцкого, коми, марийского, татарского, тувинского, удмуртского, хакасского, чеченского, чувашского и якутского языков. Внедрение этих символов направлено на обеспечение языкового многообразия в цифровом пространстве.

Таким образом, можно констатировать, что за 15 лет существования домена .РФ его востребованность с каждым годом возрастает, повышается доступность интернет услуг населению, оказываемых государственными органами и частными компаниями, в том числе и с использованием национальных языков народов России.

ЗАКЛЮЧЕНИЕ

Кириллица – письменная система, разработанная в IX–X веках н.э. для славяноязычных народов. В настоящее время она используется исключительно, или как один из нескольких алфавитов для более чем 50 языков, в частности, белорусского, болгарского, казахского, киргизского, македонского, черногорского, русского, сербского, таджикского (один из диалектов персидского), туркменского, украинского и узбекского (параллельно с латиницей)[24].

Богатство кириллицы и русского языка и его грамматики до нас донес Михаил Васильевич Ломоносов в одной из своих главных работ, «Российская грамматика» **(рис. 4),** опубликованной в 1755 году тиражом в 1200 экземпляров. В первую годовщину рождения сына Петра Фёдоровича и Екатерины Алексеевны (будущей Екатерины Великой) рукопись «Грамматики» была торжественно поднесена Ломоносовым младенцу великому князю Павлу Петровичу. Это выдающееся произведение российской филологии было отпечатано в Петербурге и затем выдержало подряд пять изданий.

Российская грамматика (отрывок из письма Пресветлейшему государю, великому князю Павлу). 1755г.

Карл Пятый, римский император, говаривал, что ишпанским языком с богом, французским - с друзьями, немецким - с неприятельми, италиянским - с женским полом говорить прилично. Но если бы он российскому языку был искусен, то, конечно, к тому присовокупил бы, что им со всеми оными говорить пристойно, ибо нашел бы в нем великолепие ишпанского, живость французского, крепость немецкого, нежность италиянского, сверх того, богатство и сильную в изображениях краткость греческого и латинского языка.

Михайло Ломоносов.

20 Сентября 1755г.



Рис. 4. Титульный разворот «Российской грамматики» Ломоносова.

Продолжая просветительские традиции Михаила Васильевича Ломоносова, сегодня уже с помощью кириллических доменов в национальной доменной зоне Координационный центр доменов .RU/.РФ способствует культурной и лингвистической идентификации. Кириллица тоже является национальным символом, и любая надпись на ней – это национальная идентификация. С помощью кириллических доменов в интернете мы сможем расширить наши знания и обогатить национальную культуру.

[24] Britannica, Cyrillic alphabet. URL: *https://www.britannica.com/topic/Cyrillic-alphabet*



АЛЕКСАНДР ПОЛУНИН
к.т.н.,
директор Орловского филиала
ООО «ТехАргос»

ОСОБЕННОСТИ КЛАССИФИКАЦИИ СЕТЕВОГО ТРАФИКА В РОССИЙСКОМ СЕГМЕНТЕ СЕТИ ИНТЕРНЕТ

АННОТАЦИЯ
В работе сделана попытка обобщения опыта развития технологий, методов и средств анализа сетевого трафика через призму современного состояния рынка телекоммуникационного оборудования в Российской Федерации. Определены основные вызовы для участников технического сообщества. На основе обзора процессов исторического развития и лучших мировых практик производится классификации актуальных методов анализа трафика. На базе выделенных методов формируется набор алгоритмов идентификации сетевых сервисов и приложений, требования к подбору параметров алгоритмов для решения отдельных прикладных задач. Рассматриваются вопросы реализации механизмов обеспечения гибкости использования решений для глубокого анализа трафика в различных образцах телекоммуникационного оборудования.

КЛЮЧЕВЫЕ СЛОВА:
Классификация сетевого трафика, глубокий анализ пакетов, DPI Engine, методы анализа, признаковое пространство, сетевой сервис, сетевое приложение.

1. ВВЕДЕНИЕ

Вопросы классификации сетевого трафика исторически являются предметом исследования как участников российского и мирового научного сообщества, так и представителей ИТ-индустрии, занимающихся созданием и развитием программно-аппаратных решений для управления трафиком, информационной безопасности и др.

На текущий момент состояние рынка телекоммуникационного оборудования (далее – ТКО) в общем и средств классификации трафика, в частности, в Российской Федерации обусловливается, в том числе следующими факторами:

- жесткая санкционная политика со стороны недружественных государств,
- уход с рынка и, как следствие, прекращение поставок и технической поддержки оборудования ведущими мировыми производителями,
- нехватка и в некоторых случаях полное отсутствие технических решений отечественного производства.

Данные факты вносят значительный вклад в систему угроз информационной безопасности страны и являются причиной постоянной активности участников ИТ-сообщества на всех уровнях: законодательном, административном, техническом.

В настоящих условиях актуальными задачами являются разработка и внедрение критически важных образцов ТКО российскими производителями, ориентированными на собственную разработку. В настоящей работе сделана попытка обобщения опыта разработки решений для глубокого анализа трафика – DPI *(англ. Deep Packet Inspection)* Engine с учетом специфики их применения на сетях связи, относящихся к российскому сегменту сети Интернет, на примере разработанного ООО «ТехАргос» программного комплекса TrACE TA[1] *(англ. Traffic Analysis and Classification Engine)*. TrACE TA – продукт, вышедший на российский рынок и рынок стран СНГ и уже используемый некоторыми производителями DPI и других решений, реализующих в своей основе классификацию сетевого трафика.

2. ОБЛАСТИ ПРИМЕНЕНИЯ СРЕДСТВ КЛАССИФИКАЦИИ СЕТЕВОГО ТРАФИКА

Задача классификации трафика является фундаментальной для построения полноценных DPI решений [1]. Это связано как с постоянной эволюцией самих сетевых сервисов и приложений: использованием новых протоколов и подходов к оптимизации работы сервисов, появлением новых доменных имен, миграцией между сервисами хранения данных и CDN *(англ. CDN, Content Delivery Network)*, так и с растущими темпами использованием средств шифрования и анонимизации. По этой причине функционал глубокого анализа трафика и классификации сетевых потоков *(flow)* реализуется именно в выделенных решениях класса DPI Engine. Традиционными сферами применения DPI Engine являются:

- основные классы решений информационной безопасности (NGFW *(англ. Next Generation Firewall)*, NTA *(англ. Network Traffic Analysis)* и др.);
- решения для операторов мобильной связи, отвечающие за тарификацию трафика абонентов (PCEF (англ. Policy and Charging Enforcement Function) и др.);

[1] Включен в Реестр российского программного обеспечения Министерства цифрового развития, связи и массовых коммуникаций Российской Федерации.

– сетевые устройства, вне зависимости от типа сети, отвечающие за балансировку нагрузки на сеть, управление качеством обслуживания и др.

До недавнего времени решения класса DPI Engine на российском рынке ТКО были представлены в основном зарубежными производителями, прекратившими поддержку своих продуктов:
– Enea Qosmos DPI & Traffic Intelligence [2];
– Rohde&Schwarz PACE 2 [3];
– Sandvine AppIdentifier [4];
– Allot DART engine [5] и др.

В этой связи актуальной задачей является разработка отечественных программных и программно-аппаратных средств идентификации сетевых сервисов и приложений с учетом использования лучших мировых практик для применения в новейших образцах ТКО, отвечающих современным вызовам, обусловленным развитием телекоммуникационной отрасли, законодательными и регуляторными нормами и инициативами, направленными на определение границ государства в киберпространстве и интенсификацию процессов цифровой трансформации Российской Федерации.

3. МЕТОДЫ КЛАССИФИКАЦИИ СЕТЕВОГО ПАКЕТНОГО ТРАФИКА И ОСОБЕННОСТИ ИХ ПРИМЕНЕНИЯ ДЛЯ РЕШЕНИЯ ПРАКТИЧЕСКИХ ЗАДАЧ

3.1. Таксономия методов анализа трафика

В общем случае под классификацией сетевого трафика в сетях передачи данных с коммутацией пакетов будем понимать процесс определения конкретных приложений или действий пользователей на основании анализа сетевых пакетов и/или их последовательностей. Таксономия методов анализа трафика исследуется уже долгое время, предложено большое количество методов, способов и алгоритмов, которые в свою очередь могут быть классифицированы по используемым в них подходам к анализу, обладающим своими достоинствами и недостатками [6]. На **рисунке 1** представлен вариант классификации актуальных, с учетом современного уровня развития телекоммуникаций, методов анализа.

Все перечисленные инструменты анализа сетевого пакетного трафика могут быть положены в основу разработки конкретных методов и алгоритмов классификации и использоваться как самостоятельно, так и в совокупности. Выбор зависит от типа решаемых задач и ограничений по

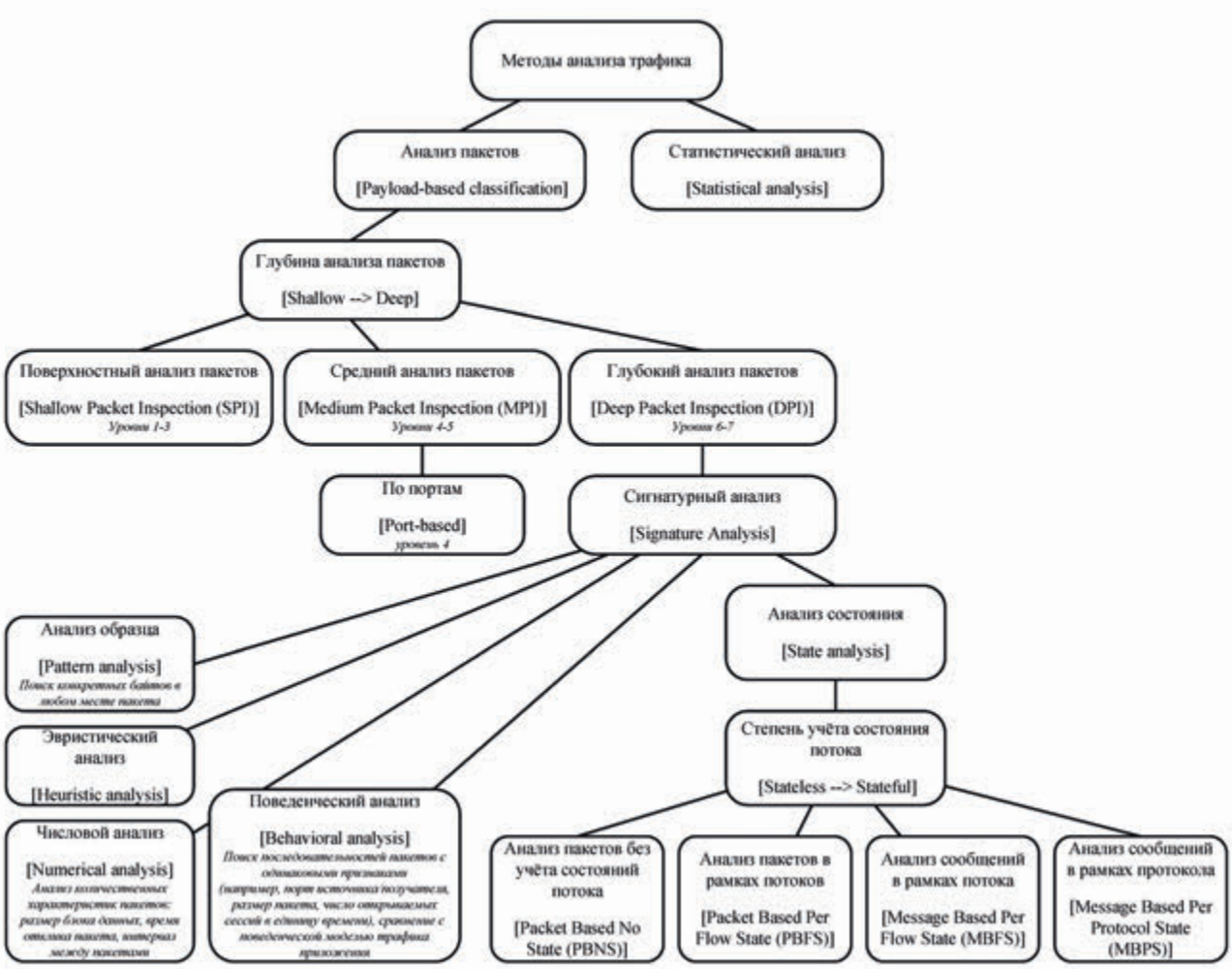


Рис. 1. Методы анализа трафика

ресурсоемкости, скорости принятия решения и пр., накладываемых условиями применения в конечном оборудовании (см. п. 2).

3.2. Реализационные аспекты классификации трафика

Говоря о реализации в конкретных технических решениях тех или иных методов классификации трафика, имеет смысл различать:

- метод классификации – совокупность приемов (способов), позволяющих разделить множество сетевых потоков *(flow)* на отдельные подмножества (классификационные группировки) в соответствии с признаками – чистая логика без привязки к реализации;
- алгоритм идентификации сетевого сервиса/приложения – выделенная из общего алгоритма обработки трафика относительно независимая реализация одного или нескольких методов.

В **таблице 1** представлен набор методов классификации сетевого пакетного трафика, используемых в рассматриваемом решении TrACE TA. Для сохранения общности названия методов приведены в нотации, принятой в ИТ-сообществе [2-5].

Основным предназначением рассматриваемого решения TrACE TA является анализ содержимого сетевых пакетов с целью идентификации протокола или сервиса/приложения, к которому относится анализируемый сетевой поток *(flow)*, а также извлечение метаданных. Результатом процесса идентификации сетевого потока является путь классификации – стек протоколов, содержащий все обнаруженные уровни протоколов/сервисов для обрабатываемого потока (например, *base.ip.tcp.http.google*). Метаданные – это данные,

Таблица 1. Методы классификации сетевого пакетного трафика

№ п/п	Название метода	Краткое описание метода	Комментарий
1.	Explicit	Метод классификации по порту или коду протокола.	Определение номера порта из контекста потока (5-tuple) или поиск явного указания кода протокола в заголовке протокола нижележащего уровня.
2.	Port-based classification over SSL	Метод классификации по ALPN-полям (для SSL/TLS).	Определение имени протокола в полях ALPN заголовка SSL/TLS. Позволяет различать протоколы над SSL/TLS: HTTPS, IMAPS, POP3S и т.д.
3.	Pattern matching	Метод классификации по сигнатурам в пакете.	Синтаксический анализ содержимого пакета – поиск конкретных сигнатур (последовательностей байтов) в самом идентифицируемом пакете.
4.	Protocol Data Signature	Метод классификации по значениям полей в заголовке протокола нижележащего уровня.	Поиск конкретных значений полей и их комбинаций в заголовке протокола нижележащего уровня, таких как server, uri, user_agent (HTTP), page_url (RTMP), common_name (SSL).
5.	DNS Caching	Метод классификации по информации из кэша протокола DNS.	Использование информации, полученной из DNS-обменов и накопленной в кэше в ходе обработки.
6.	Session Correlation	Метод классификации по информации из связанных сеансов.	Использование информации, извлеченной из другого потока, в котором явно анонсировано выделение IP-адреса и порта для открытия идентифицируемого потока.
7.	Session Behavior	Метод классификации по действиям в рамках сеанса.	Анализ метрик потока, специфичных для конкретного приложения (размеры пакетов, время прихода, интервалы и т.д.). Используется, например, для определения типов трафика сервисов мгновенного обмена сообщениями (чат, голос/видео звонок, передача файлов и т.д.), зашифрованного или обфусцированного трафика.
8.	Statistical Protocol Identification	ML-классификация (англ. Machine Learning) трафика на основании структурно-временных характеристик.	Статистическое сравнение с эталонной моделью трафика данного вида.

специфичные для конкретных протоколов, которые могут быть извлечены классификатором в процессе обработки пакета/сетевого потока. Метаданные могут быть двух видов:
- извлекаемые непосредственно из тела пакета/пакетов, например, *http.url*, *ssl.server_name*;
- вычисляемые, например, результаты идентификации типов трафика для OTT сервисов *(англ. Over the Top)*: Whatsapp *(принадлежит компании Meta, признанной экстремистской и запрещённой на территории Российской Федерации)*, Telegram, Viber, Skype (чат, голос/видео, передача файлов) или *http.rtt*.

Классификатор использует различные, базирующиеся на представленных в **таблице 1** методах, проприетарные алгоритмы идентификации потоков: часть протоколов/сервисов может быть идентифицирована по сигнатурным признакам, часть по связанным потокам, часть по некоторым комбинациям признаков. При этом все алгоритмы используют одни и те же признаки классификации. В этой связи возникает задача качественной подготовки признакового пространства: формирование исчерпывающих наборов признаков и их разбиение на классификационные группировки в соответствии с моделями функционирования тех или иных сетевых сервисов и приложений.

Приоритизация признаков классификации

Не всегда алгоритм классификации дает однозначный ответ о принадлежности сетевого потока *(flow)* тому или иному сервису. Например, ИТ-компания *VK* объединяет сервисы *vk*, *vk_video*, *odnoklassniki*, *ok_video* и другие, поэтому существует априорная неопределенность:
- в используемых наборах признаков есть принадлежащие одновременно к нескольким классификационным группировкам (классам); это корректно – отражает существующее разбиение на классы (они определены так, что могут пересекаться, в том числе быть вложенными друг в друга);
- алгоритмы классификации, реализованные в обработчиках разных сервисов, не проектируются как взаимоисключающие, поэтому «конкурируют» между собой – разные обработчики могут среагировать на одну и ту же совокупность параметров трафика.

В ряде сценариев выбор результирующего пути классификации может осуществляется непрозрачно, но, по крайней мере, детерминировано, а в ряде сценариев даже случайно. Однако в контексте прикладных задач (см. п. 2), в частности, тарификации трафика абонентов или реализации функции идентификации приложений в межсетевых экранах, классификатор должен давать однозначный ответ о принадлежности потока конкретному сервису. С этой целью в рассматриваемом решении TrACE TA реализован набор механизмов исключения неопределенности результата на этапе подготовки признакового пространства, в частности, учёт приоритетов признаков, заданных аналитиком либо на основании эвристических правил.

Решение TrACE TA применяет следующий набор механизмов исключения неопределенности результата.

1. **Исключение дубликатов** – на этапе подготовки наборов признаков исключаются дубликаты признаков типа *url* и *ip-address* согласно заданным настройкам приоритетов:
   - исключаются дубликаты, имеющие более низкий приоритет источника получения признака;
   - исключаются дубликаты (с максимальным приоритетом источника), которые найдены в сервисах, относящихся к одному метасервису (экосистеме) – признак соотносится с классом самой экосистемы (например, один и тот же признак, найденный в классификационных группировках *vkontakte* и *vk_music*, будет отнесен к классу *vkontakte*, отмеченному как *primary*).
2. **Приоритет доменных имён по длине совпадения** – на этапе обработки при конфликте признаков типа *domain_name* в качестве сработавшего будет выбран признак, полностью совпадающий с выделенным из потока значением, либо один из признаков с наибольшей длиной совпадения. Например, для значения *«music.service155.aws.com»* из имеющихся в наборе признаков:
   - *«*.service155.*»* – длина 12 (все символы без "*"),
   - *«*.service{1,4}.*»* – длина 12 (вместо {1,4} подставляем 155 из встреченного значения),
   - «music.service155.aws.com» – длина 24

   всегда будет выбран признак, полностью совпадающий со встреченным в трафике значением. Если же полностью совпадающего признака нет, то будет выбран (случайно) один из признаков с наибольшей длиной совпадения.

3. **Приоритет конкретного IP-адреса перед маской** – на этапе обработки при конфликте конкретного *ip-address* и содержащей его маски подсети будет выбран конкретный адрес. Например, если из контекста потока получен адрес 24.105.0.1, при этом в наборе признаков найдены адрес 24.105.0.1 и маска 24.105.0.0/18, то в качестве сработавшего признака будет выбран адрес 24.105.0.1;

4. **Приоритет между масками** – на этапе обработки при конфликте двух вложенных подсетей будет выбрана более длинная маска (вложенная подсеть). Например, если из контекста потока получен адрес 24.105.0.1, при этом в наборе признаков найдены маски 24.105.0.0/18 и 24.105.0.0/20, то в качестве сработавшего признака будет выбрана подсеть 24.105.0.0/20.

Категоризация трафика приложений

Как отмечено ранее, во многих случаях один и тот же признак классификации может относиться одновременно к разным классификационным группировкам (классам). С учетом состояния развития современных информационных экосистем это является нормой – классы пересекаются или входят один в другой согласно своему определению. Например, *Yandex Stream* (один из сервисов компании «Яндекс») входит в *Yandex* (это вся экосистема «Яндекса») и при этом частично пересекается с *Kinopoisk* (Кинопоиск

пользуется сервисом *Yandex Stream*). На **рисунке 2** представлена обобщенная модель трафика, генерируемого пользовательскими приложениями.

В **таблице 2** приведено описание основных типов (категорий) трафика, генерируемого современными пользовательскими приложениями в процессе осуществления сеансов сетевого взаимодействия. Данная модель может быть избыточной для некоторых утилитарных приложений, но, в то же время, не может является исчерпывающей. Тем не менее, основываясь на опыте использования решения TrACE TA, можно утверждать, что оно применимо к 90% современных информационных экосистем.

В качестве примера в **таблице 3** приводится структура трафика для *Yandex Music* – музыкального стримингового сервиса компании «Яндекс».

На основании представленной модели разработана система тегирования – присвоения элементам признакового пространства повторяющихся категорий и параметров. Этот механизм предоставляет пользовательскому приложению, эксплуатирующему DPI Engine TrACE TA, гибкость в использовании результатов классификации, например, при реализации опций для бесплатных и тарифицируемых приложений в абонентских тарифных планах операторов связи и пр. Решение обеспечивает стабильно высокий уровень качества классификации трафика за счёт постоянного обновления признаков и правил классификации, поставляемых внутри библиотек, «бесшовно» обновляемых без необходимости прерывания выполнения пользовательского приложения. Актуализация признаковых пространств и механизмов категоризации трафика производится собственной лабораторией анализа сервисов и протоколов сети Интернет.

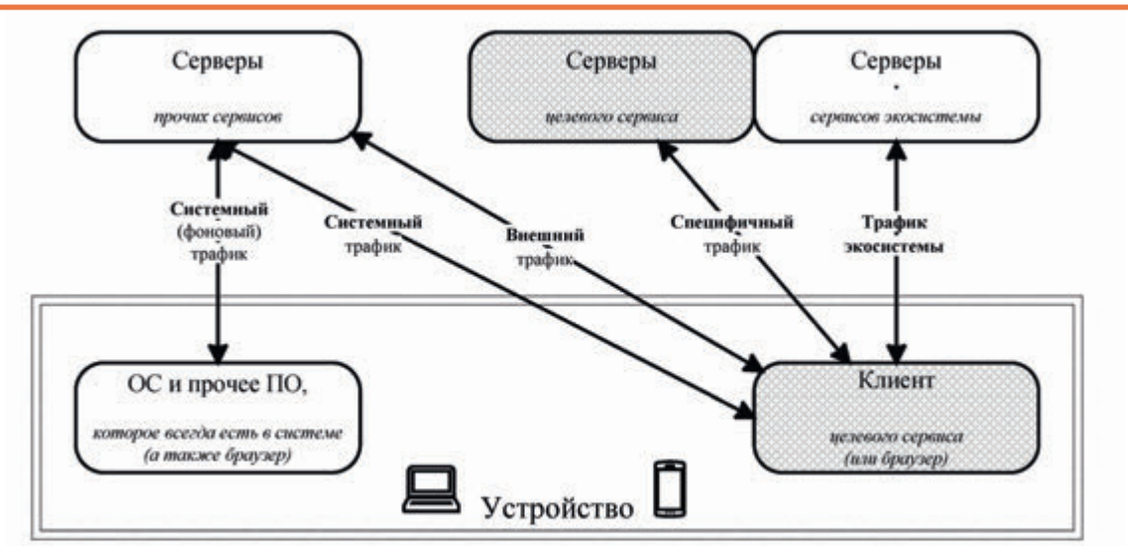


Рис. 2. Обобщенная модель трафика приложения

Таблица 2. Категории трафика сетевых приложений

Категория трафика	Описание
А. Специфичный трафик	Собственно трафик, специфичный для конкретного приложения и имеющий специфические функции, тесно связанные с основным предназначением приложения / сервиса.
Б. Трафик экосистемы	Определение имени протокола в полях ALPN заголовка SSL/TLS. Позволяет различать протоколы над SSL/TLS: HTTPS, IMAPS, POP3S и т.д.
В. Системный трафик	Синтаксический анализ содержимого пакета – поиск конкретных сигнатур (последовательностей байтов) в самом идентифицируемом пакете.
Г. Внешний трафик	Поиск конкретных значений полей и их комбинаций в заголовке протокола нижележащего уровня, таких как server, uri, user_agent (HTTP), page_url (RTMP), common_name (SSL).
Д. Прочий трафик	Использование информации, полученной из DNS-обменов и накопленной в кэше в ходе обработки.

Таблица 3. Структура трафика сервиса *Yandex Music*

Категория трафика	Доля трафика	Содержание	
А. Специфичный трафик	55,7 %	PROTO_YANDEX_MUSIC: прослушивание музыки	
Б. Трафик экосистемы	23,7 %	PROTO_YANDEX: общие ресурсы, превью видео на странице браузера, прослушивание подкастов в браузере, прослушивание музыки в бета-версии для Windows	
		PROTO_YANDEX_ID: авторизация	
		PROTO_YANDEX_PAY: оплата услуг, «Яндекс.Плюс»	
		PROTO_YANDEX_STREAM: просмотр видеоклипов, прослушивание подкастов в мобильных приложениях.	
В. Системный трафик	13,4 %	PROTO_DNS	PROTO_FCM
		PROTO_APNS	PROTO_FIREFOX
		PROTO_APPLE_ICLOUD	PROTO_GOOGLE_APIS
		PROTO_APPLE	DPI_PROTO_OPERA
Г. Внешний трафик	5,5 %	PROTO_VK: поделиться треком в социальной сети «ВКонтакте»	
		PROTO_TWITTER: поделиться треком в социальной сети Twitter	
		PROTO_ODNOKLASSNIKI: поделиться треком в социальной сети «Одноклассники»	
Д. Прочий трафик	1,7 %	PROTO_APPSFLYER PROTO_CRASHLYTICS PROTO_MEDIASCOPE	PROTO_YANDEX_ADS PROTO_YANDEX_METRICA

4. ЗАКЛЮЧЕНИЕ

Из приведённого обзора отдельно взятого решения DPI Engine TrACE TA можно сделать ряд выводов. Необходимо констатировать, что особенности современного этапа развития инфраструктуры сетевых сервисов в целом и функционирования цифровых экосистем в российском сегменте сети Интернет в частности определяют для участников технического сообщества ряд вызовов. Процессы разработки и внедрения программных и программно-аппаратных средств классификации сетевого трафика не ограничиваются исключительно поиском инновационных методов анализа, требуют подбора конкретных параметров алгоритмов для отдельных прикладных задач и реализации механизмов обеспечения гибкости использования решений. По сути, синтез востребованного на рынке решения (продукта) заключается в поиске баланса, который сводится к решению оптимизационных задач по обеспечению требуемых полноты и качества анализа, производительности и возможности кастомизации – реализации функций под фактические нужды потенциальных потребителей.

Программный комплекс TrACE TA включен в Реестр российского программного обеспечения Министерства цифрового развития, связи и массовых коммуникаций Российской Федерации (реестровая запись №24378 от 18.10.2024). Решение востребовано на рынке и применяется на сетях крупных российских операторов связи. Опыт применения ПК TrACE TA показывает возможность его использования для классификации трафика большинства современных информационных экосистем, включая VK, Яндекс и Сбербанк.

СПИСОК ЛИТЕРАТУРЫ

1. Что такое DPI Engine? [Электронный ресурс] – Режим доступа: URL: *https://habr.com/ru/articles/889082/* (11.07.2025)
2. Next-Generation DPI Engine. [Электронный ресурс] – Режим доступа: URL: *https://www.enea.com/solutions/deep-packet-inspection-traffic-intelligence/dpi-engine/* (11.07.2025)
3. DPI engine R&S PACE 2. Advanced protocol and application classification with metadata extraction for application-aware networking. [Электронный ресурс] – Режим доступа: URL: *https://www.ipoque.com/products/deep-packet-inspection-for-software-vendors/dpi-engine-rs-pace-2-for-application-awareness* (11.07.2025)
4. App Identifier. Proactively Analyze and Enhance App Categorization Performance. [Электронный ресурс] – Режим доступа: URL: *https://www.applogicnetworks.com/products/app-identifier* (11.07.2025)
5. Network Traffic Identification and Classification. [Электронный ресурс] – Режим доступа: URL: *https://www.allot.com/network-intelligence/technology/traffic-identification/* (11.07.2025)
6. А.И. Гетьман, Е.Ф. Евстропов, Ю.В. Маркин. Анализ сетевого трафика в режиме реального времени: обзор прикладных задач, подходов и решений. Препринт ИСП РАН, 28, 2015г., стр. 1-52.



АНАТОЛИЙ ГОЛОМОЛЗИН
к.т.н., советник Президента АО «ЭР-Телеком Холдинг» по взаимодействию с органами власти,
действительный государственный советник 2 класса

СОВЕРШЕНСТВОВАНИЕ ПРАВОВОГО РЕГУЛИРОВАНИЯ ЦИФРОВЫХ РЫНКОВ КАК ИНСТРУМЕНТ ДОСТИЖЕНИЯ НАЦИОНАЛЬНЫХ ЦЕЛЕЙ ЭКОНОМИЧЕСКОГО РАЗВИТИЯ

ОБ АВТОРЕ

Автор являлся заместителем Министра по антимонопольной политике и поддержке предпринимательства Российской Федерации (2000 – 2004), заместителем Руководителя Федеральной антимонопольной службы (2004 – 2020), первым заместителем Председателя Межгосударственного авиационного комитета (2020 – 2021), возглавлял Штаб по проведению совместных антимонопольных расследований в СНГ при Межгосударственном совете по антимонопольной политике (2006 – 2020).

АННОТАЦИЯ

В контексте совершенствование правового регулирования цифровых рынков с целью достижения национальных целей экономического развития даны предложения по совершенствованию отраслевого законодательства, его систематизации и кодификации. Даны предложения по поправкам в действующее законодательство, обеспечивающие переход от старой к новой бизнес-модели рынка телекоммуникаций и ИТ в условиях цифровой трансформации; описания возможных положений Цифрового кодекса России; предложения по развитию конкуренции и совершенствованию правового и методического обеспечения антимонопольного контроля.

КЛЮЧЕВЫЕ СЛОВА:

телекоммуникационная отрасль, цифровые рынки, бизнес-модели, «цифровые гиганты», антимонопольная политика.

СОВЕРШЕНСТВОВАНИЕ ОТРАСЛЕВОГО И ОБЩЕЭКОНОМИЧЕСКОГО РЕГУЛИРОВАНИЯ

Вопросы государственной политики и оценки её эффективности в условиях цифровой трансформации в явном виде сформулированы в Указе Президента Российской Федерации от 7 мая 2024 года «О национальных целях развития Российской Федерации на период до 2030 года и на перспективу до 2036 года» (далее – Указ). Все нормы Указа, касающиеся целеполагания, являются взаимно обусловленными.

Достижение целевых установок, касающихся:

1. экономического развития, основанного на честной конкуренции, предпринимательстве и частной инициативе,
2. обеспечения устойчивого экономического и социального развития Российской Федерации,
3. открытости внешнему миру,
4. высокой эффективности и технологичности,

- способствуют и достижению целеполагания, касающегося:

5. обеспечения безопасности государства и общественной безопасности,
6. укрепления государственного, культурно-ценностного и экономического суверенитета,
7. увеличения численности населения страны и повышения уровня жизни граждан.

Одним из основных инструментов реализации государственной политики является нормотворчество. Здесь важно, как создавать правовые рамки стремительно развивающемуся сектору экономики, так и избегать излишней зарегулированности, препятствующей экономическому росту и выходящему за рамки изначально заявленных целей создания справедливых правовых рамок.

Существует разнообразный зарубежный опыт законодательного регулирования, как в рамках консолидации и кодификации законодательства, так и специализации законодательства. За рубежом процессы консолидации и кодификации законодательства в сфере информационных отношений находятся на разных стадиях, при стремлении к систематизации законодательства.

Предметом законодательной систематизации за рубежом являются:

- обработка цифровых данных и цифровых записей, в том числе их защита;
- обработка персональных данных, в том числе их защита;
- цифровая трансформация государственного управления;
- управление информационно-коммуникационными технологиями;
- управление телекоммуникационными сетями и связью;
- электронная (цифровая) подпись;
- обработка информационных ресурсов, в том числе сайтов и приложений;
- создание свободного потока обезличенных данных;
- правовое регулирование цифровых сервисов, технологических систем, цифровых экосистем;
- информационная безопасность;

- электронная коммерция;
- государственное управление в информационной сфере;
- искусственный интеллект.

В России продолжается работа по совершенствованию законодательства в направлении его систематизации с возможным акцентом на кодификацию. В краткосрочной перспективе обсуждаются изменения, направленные на обеспечение соответствия нормативно-правового регулирования темпам развития отрасли связи и на устранение административных барьеров.

Как представляется, на данном этапе в законодательстве должны быть определены правовые рамки и условия перехода от старой к новой бизнес-модели сектора телекоммуникаций, формирующейся в условиях цифровой трансформации[1]. Старую бизнес-модель, к примеру, TM-Forum[2] относит к активо-центричной, а новую бизнес-модель телекома – к решение-центричной. Требуется уточнить понятийный аппарат и условия взаимодействия «провайдера коннективности», «провайдера сети», «провайдера физической инфраструктуры», «провайдеров облачных сервисов и вычислений», маркетплейсов дополняющих решений, «провайдеров платформ», платформ инноваций и решений, «провайдеров решений». Необходимо также сформулировать условия перехода от старой бизнес-модели к новой.

В среднесрочной и долгосрочной перспективе речь идёт о систематизации отраслевого законодательства посредством приведения его в единую логически цельную и согласованную правовую систему. Долгосрочная Стратегия Правительства Российской Федерации[3] оптимальным видом правового акта называет Цифровой кодекс Российской Федерации, обеспечивающий комплексное регулирование развития и использования информационных технологий, сетей связи и инфраструктуры связи. В Правительстве Российской Федерации и экспертами обсуждаются следующие задачи проекта Кодекса:

- определение единых принципов регулирования информационных отношений, включая систематизацию понятийного аппарата;
- установление правового статуса субъектов информационных отношений, в том числе закрепление полномочий органов государственной власти в области информационных отношений;
- обеспечение соблюдения прав и свобод личности, установление механизмов их защиты в информационном пространстве;
- определение правовых основ регулирования информационных отношений, включая формы, виды и категории информации, а также:
  - правовой статус данных, регулирование отношений по обработке данных в отдельных видах правоотношений, специальные (отраслевые) принципы обработки цифровых данных, особенности обработки данных с использованием технологий больших данных и интернета вещей,
  - правовое регулирование основ обработки и защиты персональных данных, основ создания и функционирования цифрового профиля;
- установление правовых основ регулирования создания и применения информационно-коммуникационных (в том числе цифровых) технологий:
  - установление правовых основ создания, развития и эксплуатации информационных систем, в том числе государственных,
  - установление правовых основ регулирования использования новых цифровых технологий, в том числе определение правовых основ создания, развития и эксплуатации цифровых платформ, облачных сервисов и цифровых услуг, основ регулирования искусственного интеллекта;
- установление правовых основ регулирования отношений в области связи;
- установление регулирования основ защиты информации, правовое обеспечение информационной безопасности;
- установление правовых основ регулирования объектов критической информационной инфраструктуры и требований по обеспечению их информационной безопасности.

Для того, чтобы обеспечить динамичное развитие рынков и поддержание на них справедливых условий, происходит смещение правого регулирования от отраслевого в сторону общеэкономического и антимонопольного. Современный уровень обмена информацией и цифровая трансформация в условиях минимальных транзакционных издержек делают рынки многосторонними, взаимоувязанными и глобальными. Поставка и потребление наличных товаров осуществляется исходя из решений, принятых в виртуальном мире. Чтобы оценивать ситуацию на рынках и перспективные изменения на них, мы начинаем говорить в терминах экономики внимания и впечатлений, данных и цифровых алгоритмов, платформенной, нарративной и виртуальной экономики и т.п. Появились методы оценки процессов цифровой трансформации и достижения приемлемого уровня цифровой зрелости. Работу по развитию бизнеса, цифровой экономики, обеспечения при этом прав и свобод потребителей и предпринимателей важно проводить с применением современных инструментов и с опорой на фундаментальные ценности и правила[4].

[1] CEO Playbook: Reigniting telecoms growth: TM Forum's CEO Playbook // Sangeet Paul Choudary, Anthony Rodrigo, Nik Willets, Dean Ramsay.- 2023
[2] TM Forum (англ. Tele Management Forum) — отраслевая некоммерческая ассоциация, объединяющая предприятия электросвязи и их поставщиков с целью выработки стандартов, рекомендаций и моделей для информационных технологий в телекоммуникационной отрасли.
[3] Стратегия отрасли связи на период до 2035г., утв. Распоряжением Правительства Российской Федерации от 24 ноября 2023г. № 3339-р.
[4] Голомолзин А.Н. «О конкуренции и регулировании: теория, история, практика, перспективы».- М: РГ-Пресс, 2021.- 176с.

На федеральном портале проектов нормативно – правовых актов обсуждается проект федерального закона «О платформенной экономике в Российской Федерации»[5] и иные, связанные с ним законопроекты[6,7]. Деятельность в условиях платформенной экономики нуждается в системном правовом регулировании, призванном упорядочить работу цифровых платформ, устранить пробелы и дисбаланс в законодательстве, обеспечить требования к безопасности товара, защитить права более экономически слабых участников рынка, правообладателей и потребителей. В законопроекте под платформенной экономикой понимается совокупность имущественных отношений, складывающихся в результате взаимодействия неограниченного круга лиц посредством цифровых платформ для осуществления предпринимательской деятельности или в иных целях. При этом законопроектом вводятся термины «цифровая платформа» и «посредническая цифровая платформа». Предлагаемое регулирование определяет правовые отношения, возникающие между операторами лишь посреднических цифровых платформ, их партнеров и пользователей. Ранее, на этапах обсуждения законопроекта «О платформенной экономике», Российский союз промышленников и предпринимателей предлагал для большей взаимосвязанности дополнительно соотнести между собой название законопроекта, предмет регулирования и применяемый в нем понятийный аппарат, конкретизировать сферу применения.

О МЕРАХ ПОВЫШЕНИЯ ЭФФЕКТИВНОСТИ ЗАЩИТЫ КОНКУРЕНЦИИ НА ЦИФРОВЫХ РЫНКАХ

Антимонопольная политика наряду с политикой в сфере защиты прав потребителей должна быть взаимно обусловлена и промышленной, и секторальной (отраслевой) политикой. Также антимонопольная политика должна быть одним из инструментов обеспечения экономической безопасности государства. Политика в области прав интеллектуальной собственности должна не противопоставляться, а взаимно дополняться антимонопольной политикой. Глобализация выдвигает новые требования к проведению скоординированной антимонопольной политики в рамках двустороннего и многостороннего международного сотрудничества[8].

В числе основополагающих принципов государственной политики по развитию конкуренции Указом Президента Российской Федерации[9] устанавливаются положения по совершенствованию антимонопольного регулирования в условиях развития цифровой экономики и ее глобализации в целях эффективного пресечения нарушений антимонопольного законодательства, носящих трансграничный характер, и повышения конкурентоспособности российских компаний на мировых рынках.

В результате принятия пятого «цифрового» антимонопольного пакета[10] была повышена объективность принимаемых решений при контроле экономической концентрации: предусмотрен институт заключения об обстоятельствах ходатайства, если антимонопольный орган придет к предварительному выводу о том, что сделка приведет (может привести) к ограничению конкуренции; введено очное рассмотрение ходатайств о совершении сделок с участием заинтересованных сторон; для заявителей по сделкам устанавливается право заявлять о добровольных обязательствах для обеспечения конкуренции на рынке. Был введён новый критерий, по которому сделки должны совершаться с согласия Федеральной антимонопольной службы (ФАС России) – это превышение цены сделки 7 млрд рублей. Использование только традиционных критериев, основанных на сумме выручки участников сделок или величине их активов, могут не отражать подлинную ценность компании и возможного влияния на рынок совершаемых сделок слияний и/или приобретений с её участием. Появилась возможность привлечения экспертов при рассмотрении сделок экономической концентрации, а также в рамках контроля исполнения предписаний, что важно для высокотехнологичных рынков. При этом предписания ФАС России к участникам сделок слияний или приобретений могут касаться передачи технологий, интеллектуальной собственности, которые требуют экспертных знаний. В ряде случаев исключительно на экспертном уровне возможно оценить, исполнено предписание или нет.

В целях пресечения нарушений со стороны цифровых платформ установлена совокупность условий, при наличии которых владелец цифровой платформы может оказывать решающее влияние на условия обращения товара, злоупотреблять своим положением. Было введено понятие «сетевой эффект», который может приводить к барьерам входа на рынок новых цифровых платформ и новых участников рынка. Проблема в том, что конкретно эти новации являются узко технологическими, они не отражают специфики и широты общей проблематики цифровых рынков.

Можно сказать, что пока не удалось в полной мере достичь целей совершенствования антимонопольного

[5] «О платформенной экономике в Российской Федерации» // regulation.gov.ru. URL: *https://regulation.gov.ru/projects#npa=152517*
[6] «О внесении изменения в Кодекс Российской Федерации об административных правонарушениях» // regulation.gov.ru. URL: *https://regulation.gov.ru/projects#npa=152633*
[7] О внесении изменений в отдельные законодательные акты Российской Федерации в связи с принятием Федерального закона «О платформенной экономике в Российской Федерации» // regulation.gov.ru. URL: *https://regulation.gov.ru/projects#npa=152635*
[8] Голомолзин А.Н. Государственная антимонопольная политика в цифровую эру.- Конкуренция и антимонопольное регулирование в Евразийском экономическом союзе.- № 01, 2023.- с.5 -18.
[9] Указ Президента Российской Федерации от 21 декабря 2017г. № 618 «Об основных направлениях государственной политики по развитию конкуренции».
[10] Федеральный закон от 10 июля 2023 № 301-ФЗ о внесении изменений в Закон «О защите конкуренции».

регулирования в условиях развития цифровой экономики и ее глобализации в целях эффективного пресечения нарушений антимонопольного законодательства, носящих трансграничный характер, и повышения конкурентоспособности российских компаний на мировых рынках. В том числе, не удалось учесть в полной мере и опыт ФАС России, и мировой опыт.

ФАС России является одним из немногих антимонопольных органов в мире, который применяет антимонопольное законодательство в отношении «цифровых гигантов». Имеется обширная практика в отношении таких компаний, как Apple, Google, Microsoft и других, по результатам которых в рамках дел пресечены нарушения антимонопольного законодательства, восстановлены условия справедливой конкуренции, взысканы штрафы о нарушениях антимонопольного законодательства. В ФАС России есть и практика рассмотрения крупных сделок слияний и приобретений, например, Monsanto/Bayer, Яндекс.Такси/Uber, которая также относится к лучшим примерам правоприменения. Необходимо продолжить подобную практику, особенно в условиях одностороннего санкционного давления, ведущего к ограничению конкуренции на глобальных и национальных рынках.

На примере сделки между Amazon и iRobot, о которой впервые было объявлено в августе 2022 года, можно показать, что мировой опыт является далеко не однозначным и говорит о необходимости выработки более адекватных подходов. Данная сделка получила одобрение от антимонопольного органа Великобритании в июне 2023 года, а в ноябре 2023 года Еврокомиссия сочла, что планируемая сделка может ограничить конкуренцию на рынке роботов-пылесосов. Еврокомиссия заявила, что многие конкуренты iRobot продают свои устройства в интернет-магазине Amazon, и комиссия обеспокоена тем, что Amazon может исключить их из каталога товаров или уменьшить заметность, что ограничит конкуренцию и «приведёт к более высоким ценам, снижению качества и меньшему количеству инноваций для потребителей». В Европейском союзе считают, что данная сделка ведет к нарушению конкуренции на рынке, так как слияние с производителем роботов-пылесосов может позволить Amazon усилить свое доминирование на онлайн-площадках.

Логика конкурентного ведомства США – Федеральной торговой комиссии (ФТК) является более сложной. Во-первых, ФТК уже давно проводит полномасштабное расследование монополизации Amazon. Федеральная торговая комиссия США с 2019 года присматривается к Amazon в связи с антимонопольными проблемами, связанными с ее розничным бизнесом и подразделением облачных вычислений. Во-вторых, ведомство намеревалось проверить, не приведёт ли упомянутая сделка к незаконному увеличению доли Amazon на рынке «подключаемых устройств» и «розничном рынке в целом». В-третьих, ФТК оценивала последствия расширения модельного ряда смарт-устройств Amazon, в который входят камеры видеонаблюдения Ring и голосовой помощник Alexa, за счёт поглощения iRobot. И в-четвёртых, по порядку, но не по важности, вопрос, рассматриваемый ФТК в ходе расследования, связан с возможными преимуществами, которые относительно других розничных продавцов может получить Amazon за счёт обработки данных о домах потребителей, собираемых пылесосами iRobot Roomba. Подробные карты домов владельцев роботов-пылесосов могут использоваться для продажи им мебели и других интерьерных предметов, подобранных с учётом планировки помещений.

Представляются целесообразными дальнейшие изменения в Федеральный закон Российской Федерации «О защите конкуренции». В частности, обсуждается вопрос об исключении иммунитетов на запреты, установленные применительно к злоупотреблениям и антиконкурентным соглашениям и согласованным действиям на рынке, а также при контроле сделок слияний и приобретений. Предлагается рассмотреть вопрос о внесении изменений и дополнений в закон с целью отражения особенностей цифровых товарных рынков в понятии «доминирующего положения». Требуется обеспечить общность подходов при анализе рынков, включая определение доминирующего положения на рынке и его использование, а также при контроле монополистических действий и при контроле экономической концентрации.

Кардинальные изменения на цифровых рынках поставили вопрос и о доработке документов по методологии анализа товарных рынков. Так, применяемый в рамках процедур анализа рынка тест «гипотетического монополиста» далеко не всегда применим к цифровым рынкам ввиду более сложных схем монетизации доходов – услуги могут оказываться клиентам и бесплатно, но зарабатывают компании при этом, например, на рекламе. Кроме этого, этот тест, а также ряд других процедур анализа рынка, отражают теоретические условия изменения ситуации на рынках. Фактические же изменения на рынках в условиях пандемии, санкций, институциональных изменений влияют (могут влиять) на продуктовые и географические границы в гораздо более широких параметрах, а фактические параметры изменений условий обращения товаров на рынках значительно превосходят теоретические гипотезы.

Недостаточно оценивать положение на рынке исходя только из анализа ситуации по отдельным элементам производственных цепочек национального рынка. Так, Приказом Федеральной службы по тарифам Российской Федерации (ФСТ России) № 481-э[11] определяется порядок анализа рынка естественно монопольных сфер

[11] Приказ ФСТ России от 13.10.2010 № 481-э. «Об утверждении Порядка рассмотрения документов, представляемых для принятия решения о введении, изменении или прекращении регулирования деятельности субъектов естественных монополий, и перечня таких документов».

деятельности, включая услуги общедоступной связи. В соответствии с этим устаревшим приказом расчет коэффициента рыночной концентрации на услугу «предоставление внутризоновых телефонных соединений» на территории соответствующего субъекта Российской Федерации определяется исходя из «числа операторов сети фиксированной телефонной связи, оказывающих услугу «предоставление внутризоновых телефонных соединений» в пределах соответствующего субъекта России. Такой подход противоречит принципу технологической нейтральности, а ограничения географических границ административными противоречат реальной экономической ситуации, фактически имеющимся условиям конкуренции фиксированных и мобильных операторов связи, мессенджеров, VPN операторов и др. Очевидно, что созрели условия отмены Приказа ФСТ России № 481-э. Все сферы деятельности должны анализироваться в соответствии с общим порядком, установленным Приказом ФАС России № 220[12], но и в него должны быть внесены изменения и дополнения, в том числе отражающие условия цифровой трансформации экономики, её глобализации.

При анализе рынка необходимо рассматривать совокупности глобальных цепочек поставок, должно анализироваться фактическое и потенциальное участие отечественных и зарубежных компаний и на национальном, и на мировых рынках. В современных условиях стираются границы между международными и национальными рынками, оптовыми и розничными рынками, онлайн и офлайн торговлей. В индустриальном мире в силу высоких транзакционных издержек всеединство материального мира лишь угадывалось. Современный уровень обмена информации и цифровая трансформация в условиях минимальных транзакционных издержек делают глобальность и взаимоувязанность рынков понятным каждому. Понятным, но пока ещё не закрепленным в методологии анализа товарного рынка.

Предлагается ввести в Порядок ФАС России по проведению анализа состояния конкуренции на товарном рынке новый раздел «Обзор рынка» с оценками границ единых рынков (тест на всеединство), который должен предшествовать применению последующих процедур анализа рынка. В рамках данного раздела предлагается проводить оценку всех возможных условий взаимозаменяемости и взаимодополняемости товаров и условий их оборота в широких временных (на десятки и более лет в ретроспективе и перспективе) и географических (вплоть до глобальных) границах с оценкой и прогнозом изменений на рынках. Целесообразно также дополнить раздел X этого приказа «Особенности проведения анализа конкуренции на товарных рынках» особенностями современных сложно устроенных и динамично меняющихся рынков. К таковым могут быть отнесены особенности рынков, отражающих процессы цифровизации, применения платформенных ИТ-решений и цифровых алгоритмов ценообразования и выбора; аспекты применения организованной (биржевой) торговли; использования (пулов) прав интеллектуальной собственности; специфику финансовых рынков и рынков финансовых технологий; поведения потребителей в условиях цифровизации; структурных реформ, мер планирования и стратегического развития и др.

О МЕРАХ ПО РАЗВИТИЮ КОНКУРЕНЦИИ НА РЫНКАХ ТЕЛЕКОММУНИКАЦИЙ И ИТ

Указом Президента Российской Федерации от 21 декабря 2017г. № 618 (далее – Указ № 618) установлены основные направления государственной политики, Национальный план как перечень первоочередных мероприятий по защите и развитию конкуренции, определены направления действий системы органов власти. Указ № 618 постулирует, что активное содействие развитию конкуренции в Российской Федерации является приоритетным направлением деятельности органов власти всех ветвей и уровней. Принятая во исполнение Указа № 618 Дорожная карта по развитию конкуренции на 2018 - 2020 годы[13] предложила ряд мер, направленных на развитие конкуренции на рынках телекоммуникаций и информационных технологий.

Дела и решения ФАС России по «отмене роуминга» внутри России (национальный и внутрисетевой роуминг) в отношении «большой четвёрки» российских операторов связи обеспечили исполнение Национального плана по развитию конкуренции. При этом ведомство стало победителем в конкурсе Всемирного банка – Международной Конкурентной Сети в номинации «Развитие конкуренции в секторе цифровой инфраструктуры, цифровых платформ и цифровых финансов» с проектом «Отмена национального и внутрисетевого роуминга»[14]. Особенность дел состояла в признание того факта, что в условиях единого рынка услуг связи, стоимость услуг связи в роуминге по технологическим и экономическим основаниям не может сколь-нибудь существенно отличаться от стоимости услуг связи внутри регионов деятельности каждого из этих операторов – по принципу «в роуминге как дома». В результате по итогам рассмотрения дел произошло не только снижение

[12] Приказ ФАС России от 28 апреля 2010г. «Об утверждении Порядка проведения анализа состояния конкуренции на товарном рынке» (в ред. Приказов ФАС РФ от 03.02.2012 № 65, от 12.03.2013 № 143/13, от 30.01.2015 № 33/15, от 23.11.2015 № 1132/15, от 20.07.2016 № 1000/16, от 12.03.2020 № 261/20).

[13] Распоряжение Правительства Российской Федерации от 16.08.2018 № 1697-р «О плане мероприятий («дорожной карте») по развитию конкуренции в отраслях экономики Российской Федерации и переходу отдельных сфер естественных монополий из состояния естественной монополии в состояние конкурентного рынка на 2018 - 2020 гг.

[14] Отмена роуминга в России признана лучшим делом ФАС // FAS.GOV.RU. URL: *HTTPS://FAS.GOV.RU/NEWS/27753*.

тарифов на услуги связи в роуминге от 2,5 до 10 раз, но также имел место и соразмерный рост трафика. От применения рыночного уровня тарифов выиграли и операторы связи, и потребители услуг связи – ситуация, которую в учебниках называют Win – Win.

Одной из эффективных мер Дорожной карты 2018 – 2020 годов в части обеспечения справедливых условий конкуренции российским разработчикам программного обеспечения (ПО) с зарубежными на единых цифровых рынках стало принятие нормативно-правовых положений о предустановке отечественного ПО. Во исполнение закона от 21 ноября 2019 года № 425-ФЗ «О внесении изменения в статью 4 Закона Российской Федерации «О защите прав потребителей» Правительством Российской Федерации[15] были утверждены перечень отдельных видов технически сложных товаров с предварительно установленными российскими программами для электронных вычислительных машин (ЭВМ), порядок составления и ведения перечня российских программ для ЭВМ, которые должны быть предварительно установлены на отдельные виды технически сложных товаров, и порядок их предварительной установки. Потребителям обеспечена возможность использования предварительно установленных российских программ для ЭВМ при покупке отдельных видов технически сложных товаров.

Важным стало предусмотренное Дорожной картой 2018 – 2020 годов внесение изменений в законодательство Российской Федерации по недискриминационному доступу операторов связи и иных лиц, размещающих сети связи и (или) инфраструктуру для размещения сетей связи операторов связи, к объектам общедомовой собственности многоквартирных жилых домов в целях размещения сетей связи для обеспечения оказания услуг связи жильцам. Федеральный закон от 06 апреля 2024г. № 67 «О внесении изменений в статью 6 Федерального закона «О связи» и Жилищный кодекс Российской Федерации» (далее – 67-ФЗ) позволяет улучшить положение граждан, обеспечив им доступ к высококачественным услугам связи, а также создать при этом благоприятные условия для ведения бизнеса. Правительством Российской Федерации приняты Правила взаимодействия оператора связи и лица, осуществляющего управление многоквартирным домом (управляющие компании и товарищества собственников жилья (УК/ТСЖ), при монтаже, эксплуатации и демонтаже сетей связи на объектах общего имущества в многоквартирном доме[16] (далее – Правила № 1055).

Эти меры направлены на достижение национальных целей, установленных Указом Президента Российской Федерации от 7 мая 2024 года «О национальных целях развития Российской Федерации на период до 2030 года и на перспективу до 2036 года» в части обеспечения доступа населения к высококачественным услугам связи, в том числе увеличения домохозяйств с доступом в Интернет до 97% к 2030 и 99% к 2036 году. Но пока в среднем лишь 30 – 40 процентов всех условий взаимодействия между Управляющими компаниями и операторами связи приведены в соответствие с принятыми Правилами № 1055. По данным Минцифры России за период с сентября 2024 года по январь 2025 года поступило 334 обращения (жалобы) от операторов связи и абонентов по конкретным проблемным ситуациям препятствования доступа в многоквартирные дома (МКД). В силу п.47 Правил № 1055 обжалование подобных действий (бездействий) осуществляется в порядке, установленном антимонопольным законодательством. У ФАС России имеются соответствующие полномочия, но отсутствуют нормы права, наделяющие ФАС России соответствующей компетенцией, которой ведомство предлагается наделить в рамках дополнений в ст.9.21 КоАП.

Для обеспечения недискриминационного доступа операторов связи к инфраструктуре для размещения сетей связи приняты Правила недискриминационного доступа к инфраструктуре для размещения сетей электросвязи, утвержденные постановлением Правительства Российской Федерации от 22.11.2022 № 2106, а также Методические рекомендации по установлению цен (тарифов) на предоставление доступа к инфраструктуре для размещения сетей связи, утвержденные приказом Федеральной антимонопольной службы от 18.05.2023 № 289/23. С принятием этих актов ситуация с доступом к инфраструктуре постепенно нормализуется, но пока имеет место значительное количество разбирательств в ФАС России и в судах.

Дорожной картой на 2018 – 2020 годы предусмотрено внесение изменений в нормативные правовые акты Российской Федерации, предусматривающих закрепление унифицированного порядка доступа хозяйствующих субъектов к объектам государственной и муниципальной собственности для целей размещения сетей связи. Но эта мера пока не нашла нормативно-правового закрепления, продолжаются обсуждения данного вопроса заинтересованными органами власти и организациями.

Дорожная карта по развитию конкуренции на 2021 - 2025 годы[17] включает меры по обеспечению равных

[15] Постановление Правительства Российской Федерации от 18 ноября 2020 г. № 1867 «О перечне отдельных видов технически сложных товаров с предварительно установленными российскими программами для электронных вычислительных машин, порядке составления и ведения перечня российских программ для электронных вычислительных машин, которые должны быть предварительно установлены на отдельные виды технически сложных товаров, и порядке их предварительной установки».

[16] Постановление Правительства Российской Федерации от 06.08.2024 № 1055 «Об утверждении Правил взаимодействия оператора связи и лица, осуществляющего управление многоквартирным домом, при монтаже, эксплуатации и демонтаже сетей связи на объектах общего имущества в многоквартирном доме».

[17] Распоряжение Правительства Российской Федерации от 02.09.2021 № 2424-р «Об утверждении Национального плана («дорожной карты») развития конкуренции в Российской Федерации на 2021 - 2025гг.».

условий деятельности на конкурентных рынках для компаний с государственным участием и организаций частной формы собственности, унификации и систематизации государственных и муниципальных преференций хозяйствующим субъектам, замене мер государственного регулирования экономических отношений на меры экономического стимулирования.

Система развития конкуренции в России включает в себя федеральный проект «Развитие конкуренции», Национальный план развития конкуренции на 2026-2030 годы, а также Стандарт развития конкуренции в субъектах Российской Федерации. Основной задачей федерального проекта является повышение экономической эффективности и конкурентоспособности хозяйствующих субъектов. Для определения показателей федерального проекта ФАС России планируется утверждение Методики оценки уровня развития конкуренции на товарных рынках, а также проведение мониторингов уровня развития конкуренции. В настоящее время разработан и находится на стадии межведомственного согласования проект Национального плана («дорожной карты») развития конкуренции в Российской Федерации на 2026-2030 годы[18].

ЗАКЛЮЧЕНИЕ

Вопросы государственной политики и оценки её эффективности в условиях цифровой трансформации в явном виде сформулированы в Указе Президента Российской Федерации от 7 мая 2024 года «О национальных целях развития Российской Федерации на период до 2030 года и на перспективу до 2036 года», а также в Стратегии отрасли связи на период до 2035г., утв. Распоряжением Правительства Российской Федерации от 24 ноября 2023г. № 3339-р. Стоящие перед Россией задачи в сфере обеспечения технологического суверенитета, реализация национальных целей по достижению технологического лидерства, цифровой трансформации государственного и муниципального управления, экономики и социальной сферы[19] требуют формирования соответствующей законодательной среды, направленной на стимулирование инноваций, снижение барьеров, поддержку инвестиций в создание прорывных технологических решений в сфере информационных и коммуникационных технологий, включая искусственный интеллект.

Условия формирования и стремительного развития единого цифрового рынка требуют изменения подходов отраслевого регулирования. Сформировался запрос на систематизацию законодательства, включая движение в направлении кодификации, связанного с созданием благоприятных условий для развития новых технологий и рынков, защитой прав потребителей, обеспечения безопасности, и других аспектов, важных для цифровых рынков.

Требуется смещение правового регулирования от отраслевого в сторону общеэкономического и антимонопольного. В том числе в рамках законодательства о платформенной экономике в Российской Федерации происходят процессы, направленные на упорядочение деятельности цифровых платформ, устранение пробелов и дисбалансов в законодательстве, обеспечение требований к безопасности товаров, защите прав более экономически слабых участников рынка, правообладателей и потребителей.

Должно меняться и антимонопольное законодательство. Традиционные процедуры анализа рынков должны дополняться тестом «на всеединство», позволяющим адекватно оценивать географические и продуктовые границы рынков в условиях цифровой экономики. Требуется адекватный учет институциональных особенностей, отражающий кардинальные изменения на только на стороне предложения, но и на стороне спроса на современных цифровых рынках. Также должны меняться процедуры и правила контроля защиты конкуренции, в сочетании с мерами по развитию конкуренции.

Важной является работа по развитию конкуренции, осуществляемая в рамках доработки проекта «дорожной карты» Правительства Российской Федерации на 2026-2030 годы. Целесообразно включить в неё предложения по выработке новых концептуальных подходов, обусловленных изменениями моделей бизнеса в сфере телекоммуникаций и ИТ, изменениями в потребительском сегменте в связи с кардинальными процессами цифровой трансформации, изменениями в парадигме и подходах антимонопольного контроля, отраслевого и общеэкономического регулирования.

Важно и дополнить «дорожные карты» на уровне субъектов Российской Федерации с целью общей организации совместной работы бизнеса и власти, направленной на развитие конкуренции на местах. Это может касаться вопросов доступа операторов связи в многоквартирные дома, к объектам государственной и муниципальной собственности, к объектам инфраструктуры, мониторинга достижения показателей Национальных целей и Национального плана по конкуренции.

[18] [Электронный ресурс]. URL: *https://fas.gov.ru/news/34003*

[19] Указ Президента Российской Федерации от 7 мая 2024г. «О национальных целях развития Российской Федерации на период до 2030 года и на перспективу до 2036 года».



ЕВГЕНИЙ СИНЕЛЬНИКОВ
руководитель саратовского обособленного подразделения
«Базальт СПО»



ОЛЬГА ЮШИНА
ведущий редактор
«Базальт СПО»

ОПЕРАЦИОННЫЕ СИСТЕМЫ ДЛЯ ПРОМЫШЛЕННЫХ КОНТРОЛЛЕРОВ — ПЕРВЫЙ ОПЫТ, ПЕРСПЕКТИВЫ И ПЛАНЫ

Уже несколько десятилетий большинство средств промышленной автоматизации в России — импортные. В последние годы появились проблемы с поставками импортного оборудования, в том числе промышленных компьютеров (в частности, программируемых логических контроллеров, ПЛК). Возникают сомнения и в безопасности импортной техники, особенно при использовании программного обеспечения (ПО) с закрытым кодом.

Поэтому предприятия обратили внимание на отечественных производителей, которые до 2022 года занимали небольшую долю рынка и в основном работали в узких нишах.

ОСНОВНЫЕ ПОТРЕБНОСТИ ЗАКАЗЧИКОВ

Когда спрос на отечественные контроллеры вырос, производителям потребовался новый инструментарий для создания прошивок российского производства и с гарантированной поддержкой.

Несколько производителей обратились в нашу компанию – «Базальт СПО»[1] с предложением разработать такой инструментарий.

Их цель — иметь возможность лицензировать операционную систему при создании собственных решений – программно-аппаратных комплексов (ПАК). Промышленные контроллеры (специализированные промышленные компьютеры) широко используются в критической информационной инфраструктуре (КИИ). Поэтому им требуется продукт, входящий в Единый реестр российских программ для ЭВМ и БД (далее – Реестр), а в перспективе — и с сертификатом ФСТЭК России, что позволит сертифицировать ПАК как средство защиты информации.

У «Базальт СПО» есть включенная в Реестр операционная система (ОС) «Альт Сервер»[2] (рег. № 1541 от 05.09.2016) и сертифицированная ФСТЭК России ОС «Альт СП»[3] (рег. № 4305, сертификат № 3866 от 10.08.2018), которые могут стать базой для создания подобного продукта.

Основные требования к продукту:

- поддержка конкретных аппаратных изделий, как правило, разработанных заказчиком;
- возможность генерации прошивок с предустановленной операционной системой в объёме и качестве, достаточном для промышленного использования;
- доступность инструментов разработчика для сборки, тестирования и отладки специализированных приложений под целевую платформу;
- стабильность рабочего и сборочного окружений при длительной эксплуатации генерируемых прошивок;
- возможность создавать прошивки, работающие в мягком и жестком реальном времени[4];
- поддержка промышленных протоколов и стандартов, таких как OPC UA[5], MQTT (IoT)[6], Modbus TCP/RTU[7].

[1] [Электронный ресурс]. URL: *https://www.basealt.ru/*
[2] [Электронный ресурс]. URL: *https://www.basealt.ru/alt-server/*
[3] [Электронный ресурс]. URL: *https://www.basealt.ru/altsp/*
[4] ОС реального времени — это системы, выполняющие задачи в строго определенный момент, для них задается допустимая задержка, измеряемая миллисекундами (в зависимости от задачи). Применяются на встроенных устройствах. ОС мягкого реального времени используют там, где превышение заявленного времени реакции нежелательно, но не фатально. ОС жесткого реального времени — там, где превышать время реакции строго запрещено.
[5] OPC Unified Architecture — спецификация, определяющая передачу данных в промышленных сетях и взаимодействие устройств в них.
[6] MQTT (Message Queuing Telemetry Transport) — протокол обмена данными, разработанный для Интернета вещей (IoT).
[7] Modbus — открытый протокол для обмена данными в промышленных системах автоматизации. Modbus RTU применяется для последовательного подключения, Modbus TCP / IP — в сетях Ethernet.

ПРАКТИЧЕСКОЕ ВОПЛОЩЕНИЕ

Первой задачей было провести сравнительный анализ работы изделия на базе чипа RK3528 одного из наших партнеров в режиме реального времени.

У нас уже был опыт запуска ОС «Альт» на различных одноплатных компьютерах. Адаптация ядра обеспечивалась за счет включения в него дополнительных модулей, а работа периферийных устройств — доработкой описателя дерева устройств (DTB) без изменения исходного кода ядра.

В случае с контроллерами мы адаптировали инструментарий генерации образов для одноплатников и на основе специальной редакции операционной системы «Альт Сервер» сформировали новый продукт, который получил рабочее название «Альт Контроллер». В «Базальт СПО» были созданы и опробованы на конечном изделии две прошивки — на стандартном ядре и ядре реального времени.

Затем были проведены по 9 серий измерений для различных конфигураций на стандартном ядре и ядре с уменьшенным временем задержки (параметр PREEMPT_RT), в каждой серии снято по 100 осциллограмм, которые совмещены наложением в один файл и позволяют судить о разбросе времени реакции **(рисунок 1)**.

Тесты показали, что операционная система «Альт Контроллер» на целевом изделии позволяет обеспечить необходимый отклик в 50 мкс даже при высокой нагрузке на процессор, причем с большим запасом и допустимым временным разбросом (jitter).

В итоге партнер получил тестовый образ «Альт Контроллера» и результаты тестирования изделия с нашими ядрами в различных режимах, а мы решили продолжить работу в данном направлении.

АРХИТЕКТУРНЫЕ ДЕТАЛИ СОПРОВОЖДЕНИЯ КОНЕЧНЫХ ИЗДЕЛИЙ

ОС «Альт Контроллер» — особая редакция операционной системы «Альт Сервер», она проектируется под OEM-установку. Это основной способ поставки ПО на специализированное встраиваемое оборудование.

Чтобы превратить опытный образец в продукт, распространяемый на рынке, необходимо разработать технологию его производства, внедрения и сопровождения.

Сначала требуется разработать технологию доработки и сборки «прошивок» под конкретные аппаратные изделия, используемые заказчиком.

Затем необходимо автоматизировать сборку под различные виды сопровождаемых изделий и сформировать «каркасный» образ корневой файловой системы в виде архива или iso-образа (для

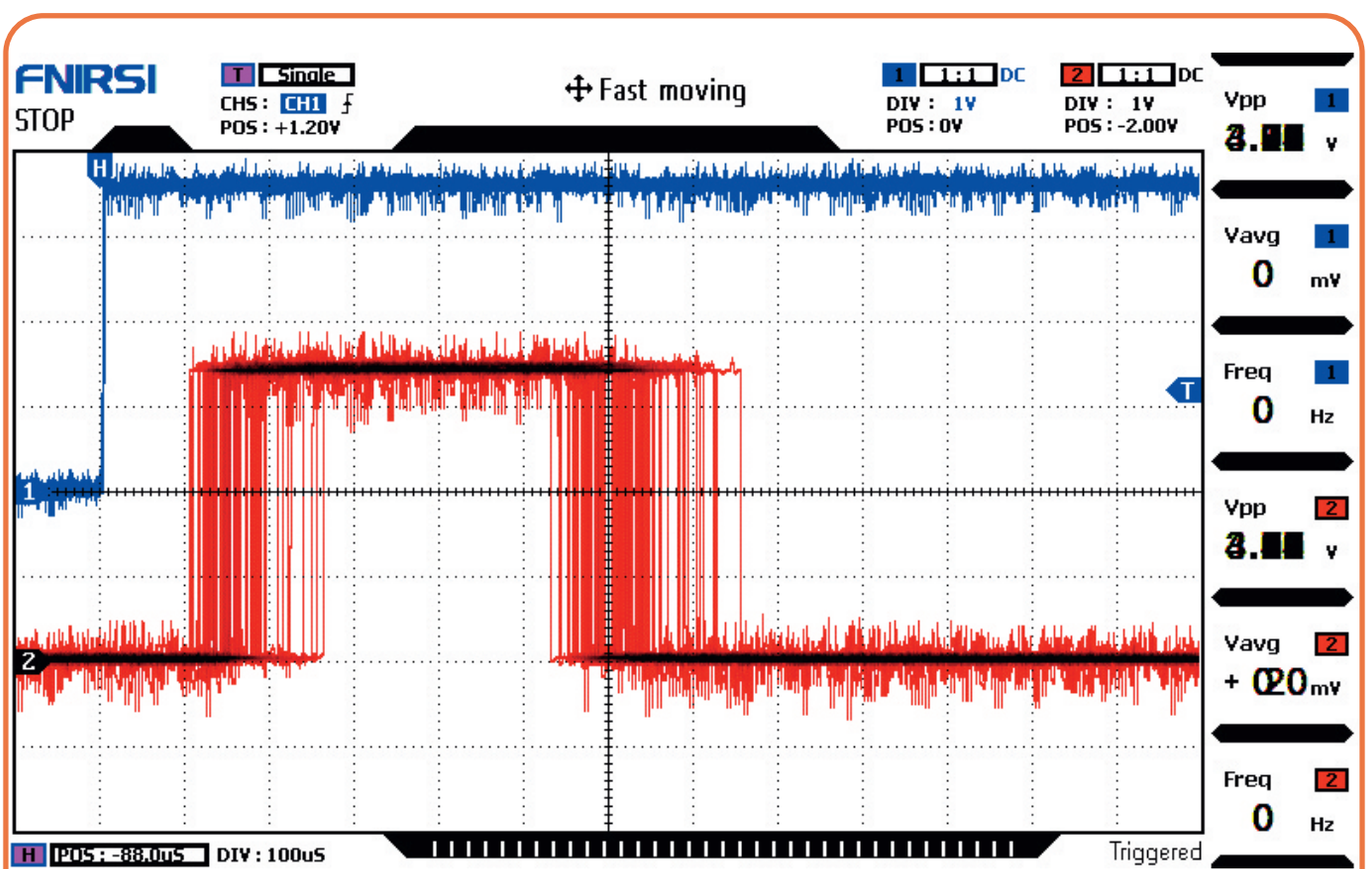


Рис. 1. Результаты экспериментов.

сертифицированных продуктов). Эти артефакты становятся первоисточником для генерации «прошивки» под конкретное изделие. Схематично этот процесс показан на **рисунке 2**.

Далее запускается полноценный жизненный цикл разработки, включающий в себя:
- **регулярный выпуск обновлений** первичного «каркасного» образа корневой файловой системы;
- **подготовку инструментария** для генерации прошиваемого в изделие предустанавливаемого варианта образа при появлении новых сопровождаемых типов оборудования;
- **поддержку инструментария**, созданного ранее, во избежание регрессий;
- **формирование** предустанавливаемого варианта образа.

При подготовке прошивки в предустанавливаемом варианте образа должны быть обеспечены:
- таблица разделов под целевое изделие;
- корректное размещение загрузчика;
- файл с описанием device tree (dtb-файла), исключающий конфликт загрузчика и ядра;
- возможность обновлять ядро и корневую файловую систему на конечном изделии штатными средствами;
- интеграция дополнительного «вендорского» программного обеспечения.

КЛЮЧЕВЫЕ ОСОБЕННОСТИ «АЛЬТ КОНТРОЛЛЕРА»

«Альт Контроллер» по состоянию на август 2025 года находится в разработке, но его основные особенности уже можно назвать:
- сопровождаемая по безопасности пакетная база, включая ядро, с возможностью сертификации в дальнейшем (сертифицированная ветка);
- поддержка работы ядра в режиме мягкого реального времени;
- возможность бесшовного переноса на контроллер программных доработок из рабочих окружений разработчика;
- системная поддержка многоядерности в рамках единой пакетной базы;
- поддержка современных версий ядра Linux;
- возможность обеспечить поддержку различных архитектур: x86_64, aarch64, loongarch64, riscv64, e2k;
- работа с изделиями промышленной автоматики на базе современных 64-разрядных микропроцессоров.

СРАВНЕНИЕ «АЛЬТ КОНТРОЛЛЕРА» СО СВОБОДНЫМИ И ПРОПРИЕТАРНЫМИ ИНСТРУМЕНТАМИ ДЛЯ ПРОМЫШЛЕННЫХ КОМПЬЮТЕРОВ

Российские производители по различным причинам вынуждены отказываться от проприетарного ПО зарубежных производителей, в том числе от ПО для промышленных компьютеров в пользу свободных или отечественных решений.

Для генерации прошивок для промышленных компьютеров можно использовать популярный инструмент buildroot, но он имеет свои особенности, препятствующие его использованию при длительном сопровождении и внедрении практик безопасной разработки. Многие производители планируют сертифицировать свои продукты во ФСТЭК России, в подобных случаях применять инструмент buildroot также нежелательно.

Buildroot собирает прошивку с нуля, по сути, формируя уникальную операционную систему. В результате ответственность за все компоненты операционной системы в итоговом образе ложится на того, кто создаёт собственное решение – ПАК.

При использовании ОС «Альт Контроллер» и других систем, основанных на подобном принципе, производитель ПАК отвечает только за часть собственного кода времени исполнения (runtime), который разрабатывается в рамках ПАК. При этом системные компоненты операционной системы, включая ядро, остаются, если это возможно технически, в компетенции разработчиков ОС «Альт Контроллер».

Кроме того, в buildroot применяется кросс-компилляция. С одной стороны, это удобно для разработки в режиме Host-Target, когда архитектура хоста, на котором происходит компиляция, и целевого изделия отличаются. С другой стороны, при этом приходится сопровождать сборку множества библиотек и других системных компонентов, которые доступны в дистрибутивах Linux «из коробки».

ПО на базе Linux может занимать больше места на диске и содержать избыточные библиотеки, загруженные по зависимостям. Гибкое разбиение пакетной базы ОС «Альт», содержащей множество отдельных подпакетов, существенно снижает издержки такой избыточности.

ОС «Альт Контроллер» превосходит, по нашему мнению, привычные проприетарные инструменты по ряду параметров:
- открытый код обеспечивает полный доступ к ОС и возможность компоновки программно-аппаратных решений из сопровождаемых и проверяемых на безопасность модулей (пакетов);
- операционные системы «Альт» интегрированы с российским ПО;
- в качестве инструментов разработки можно использовать универсальные языки (C/C++, Python) вместо узкоспециализированных;
- нет привязки к конкретному вендору – можно выбрать различные поддерживаемые контроллеры и периферию;
- прозрачность системы – нет «черных ящиков», как в проприетарных решениях;
- поддержка единого стека технологий на рабочем месте разработчика и на конечном изделии (Self-Hosted вместо Host-Target).

ПЛАНЫ И ПЕРСПЕКТИВЫ

Первый опыт показал, что ОС «Альт Контроллер» может стать востребованным продуктом.

У разработчиков промышленных контроллеров есть требования и ожидания. Часть этих ожиданий мы уже реализовали и наметили план развития в соответствии с



Рис. 2. Инструменты и артефакты разработчика.

их потребностями. Итак, чего ждут от ОС «Альт Контроллер» наши заказчики?

Наличие инструментов разработки «под ключ»
- Приложения для графического программирования – создания лестничных диаграмм и т.п.
- Текстовые языки для сложных алгоритмов (C/C++ и Python) – уже реализовано.
- Системные инструменты для командной работы – уже реализовано.

Наличие различных ядер реального времени
- Мягкое реальное время (Soft RT) с типовыми задержками до 50 мкс для критичных процессов (управление двигателями, датчиками) в оптимизированных системах, благодаря применению патчей PREEMPT_RT.
- Жесткое реальное время (Hard RT) с поддержкой Xenomai, обеспечивающей доли микросекундных задержек (например, для робототехники).

Поддержка различных процессорных архитектур
«Базальт СПО» имеет большой опыт выпуска сборок операционных систем под различные процессорные архитектуры: x86_64, aarch64, loongarch64, riscv64, e2k (Эльбрус). «Альт Контроллер» при необходимости может быть адаптирован под любую из них.

Наличие драйверов
В системе должны быть драйверы для промышленных шин (EtherCAT, CANopen), датчиков, модулей ввода-вывода (например, Advantech, ОВЕН) и средства разработки драйверов под нестандартное оборудование.

Локальная и удалённая отладка
Требуется возможность локальной отладки на симуляторе промышленного контроллера с визуализацией сигналов и трассировка задач в реальном времени, а также удалённая отладка изделий, подключенных по сети, на рабочем месте разработчика контроллеров.

Удаленный мониторинг
Встроенный интерфейс для просмотра состояния системы.

Интеграция с системами мониторинга для сбора данных и их наглядного представления.

Безопасность и надежность
- Возможность изоляции критичных процессов и проприетарных драйверов в контейнерах.
- Шифрование данных на уровне ОС.
- Автоматический перезапуск «упавших» задач.
- Сторожевой таймер (watchdog) для предотвращения зависаний.

ВЗАИМОДЕЙСТВИЕ С ПАРТНЕРАМИ

Помимо самого продукта, производителям контроллеров важно, чтобы вендор реагировал на запросы, помогал на этапе внедрения и на первых этапах использования, инициативно вносил улучшения в продукт. Поэтому команда «Базальт СПО»:
- проводит технический анализ на совместимость и оперативную адаптацию с целью длительной поддержки конкретных изделий;
- осуществляет отладку ядра для сопровождаемых изделий;
- предоставляет системный инструментарий сопровождения прошивок;
- обеспечивает безопасную разработку в рамках репозитория.

Для успешной разработки и сопровождения такого продукта как ОС «Альт Контроллер» необходимо тесное партнерское взаимодействие с производителями промышленных компьютеров. Поэтому мы – команда «Базальт СПО», приглашаем к сотрудничеству вендоров, заинтересованных в появлении надежного и безопасного российского продукта с открытым исходным кодом.



ЮЛИЯ ДЕНИСЕНКО
генеральный директор
АО «Иридиум»

КАК КРОССПЛАТФОРМЕННЫЕ ПОЧТОВЫЕ КЛИЕНТЫ МЕНЯЮТ ОТЕЧЕСТВЕННЫЙ БИЗНЕС-ЛАНДШАФТ?

Сегодня кроссплатформенные почтовые клиенты важны для бизнеса как никогда. В условиях импортозамещения российские разработчики создают аналоги зарубежных решений. В результате отечественные решения становятся всё более конкурентоспособными и востребованными на рынке, открывая новые возможности. Однако, какой эффект это оказывает на бизнес?

ОЦЕНКА РОССИЙСКОГО РЫНКА

Развитие отечественных кроссплатформенных почтовых клиентов — важный тренд в российском бизнесе. Они помогают компаниям снижать зависимость от иностранных решений, повышать безопасность данных и оптимизировать внутренние процессы. В целом, многие российские разработки способны конкурировать с иностранными на рынке благодаря высокой технологической базе, гибкости интеграции и постоянному совершенствованию архитектуры.

Тем не менее несмотря на очевидные преимущества отечественных решений, многие заказчики пока не спешат полностью переходить на российские системы. Они занимают выжидательную позицию, что формирует отложенный спрос. Такой подход позволяет бизнесу оценить новые возможности без риска, а потом менять устоявшиеся решения.

По нашим оценкам, этот спрос рано или поздно активизируется: только по итогам 2024 года объем рынка почтовых решений России составил чуть более 4,5 миллиарда рублей (прирост относительно 2023 года +36%), а к 2030 году он может достигнуть около 18 миллиардов рублей.

Кроме того, рынок виртуализации демонстрирует еще больший потенциал — по нашим прогнозам, он может достигнуть до 57 миллиардов рублей к 2030 году.

Это свидетельствует о высокой востребованности современных российских технологий в сфере инфраструктурных решений.

РАЗВИТИЕ ОТЕЧЕСТВЕННЫХ РЕШЕНИЙ: ПРИМЕР DEEPMAIL

Одним из ярких примеров отечественных решений является платформа DeepMail[1], разработанная компанией «Иридиум»[2]. DeepMail – это почтовый сервер-клиент, позволяющий осуществлять коммуникационное взаимодействие между сотрудниками.

История создания этого продукта началась еще в 2008 году, задолго до официальных мер по импортозамещению. Тогда команда под руководством главного конструктора «Иридиума» Игоря Коптелова создала криптозащищенный «почтовик», ориентированный на безопасный обмен письмами с использованием криптошифрования. Изначально решение позиционировалось как платформа для обмена электронными сообщениями, включавшая календари и возможность подключения IP-телефонии.

Проведенный специалистами компании «Иридиум» анализ статистики показал, что более 60% обращений клиентов связаны не только с электронной почтой, но и с календарями, бронированием ресурсов, делегированием прав и управлением общими ящиками.

Сегодня DeepMail – это универсальное корпоративное средство управления рабочим временем и коммуникациями. Пользователи могут иметь до 12 делегированных календарей[3] и 20 почтовых ящиков, что делает систему мощным инструментом для крупных

[1] Подробнее о DeepMail: *https://iridium-soft.com/docmail*
[2] Подробнее о компании: *https://iridium-soft.com/*
[3] Делегированный календарь – это возможность одного пользователя управлять календарем другого пользователя. Например, когда секретарь руководителя имеет возможность ставить, изменять и удалять встречи у руководителя. При этом, и секретарь и руководитель сохраняют возможность управлять своими личными календарями.

организаций. DeepMail входит в Реестр российского программного обеспечения (номер реестровой записи № 6199[4]) и в настоящее время проходит сертификацию ФСТЭК России.

Кроме того, один сервер поддерживает до 250 доменов, что позволяет создавать единую экосистему коммуникаций с возможностью видеть время занятости сотрудников разных компаний (из разных доменов). Это особенно актуально группам компаний или холдинговым структурам, ведущим тесное коммуникационное взаимодействие друг с другом, поскольку позволяет без лишних звонков и переписок оптимизировать время на согласование встреч и совещаний, что, в свою очередь, существенно сокращает транзакционные издержки компаний.

НОВЫЙ СЕРВЕР DEEPMAIL

Недавняя полная переработка серверной архитектуры позволила увеличить пропускную способность почтового решения с 20 тысяч до 45 тысяч запросов (любых команд в почте – например, отправка, получение письма, создание и изменение собрания) в минуту – это около 64 миллионов сообщений в сутки, а доставка писем адресатам достигает 5 тысяч сообщений в минуту. Такое масштабное обновление существенно повышает эффективность работы крупных предприятий, использующих платформу.

Теперь каждый из сервисов почтового клиента можно конфигурировать через административное приложение с возможностью использования различных профилей настроек, что обеспечивает гибкое управление и адаптацию системы под текущую ИТ-инфраструктуру компании. Внедрение современных технологий позволяет не только повысить эффективность корпоративных коммуникаций, но и укрепить технологический суверенитет страны. В условиях глобальных вызовов такие решения становятся важнейшим инструментом для устойчивого развития отечественного бизнеса.

ПЕРСПЕКТИВЫ

На фоне усиления внутреннего спроса и постепенного перехода бизнеса на отечественные программные продукты, перспективы рынка кроссплатформенных почтовых клиентов выглядят весьма оптимистично. Это обусловлено тем, что компаниям выгодно приобретать лицензии на отечественный продукт, так как это удобно на период перехода с импортных операционных систем в тех случаях, когда на одном предприятии может использоваться сразу несколько решений. Это позволяет обеспечить гибкость коммуникаций сотрудников.

Однако на текущий момент есть большая проблема, о которой не принято громко говорить со стороны вендоров – быстрое устаревание решений и наличие множества различий в их функциональных характеристиках, что вызывает серьезную озабоченность и тот самый отложенный спрос со стороны заказчиков. В компании «Иридиум» уже нашли выход из этой ситуации – сейчас идет активная доработка DeepMail, которая позволит выровнять функциональные возможности между решениями.

Таким образом, внедрение новой кроссплатформенной версии клиента DeepMail в организациях заказчиков позволит выполнить требования по импортозамещению, предусмотренных такими нормативными документами, как например, Указ Президента Российской Федерации от 30.03.2022 года № 166 «О мерах по обеспечению технологической независимости и безопасности критической информационной инфраструктуры Российской Федерации», постановление Правительства Российской Федерации от 16 ноября 2015 года № 1236 «Об утверждении Правил формирования и ведения единого реестра российских программ для электронных вычислительных машин и баз данных и единого реестра программ для электронных вычислительных машин и баз данных из государств – членов Евразийского экономического союза, за исключением Российской Федерации», Приказ Министерства связи и массовых коммуникаций Российской Федерации от 29 июня 2017 года № 334 «Об утверждении методических рекомендаций по переходу федеральных органов исполнительной власти и государственных внебюджетных фондов на использование отечественного офисного программного обеспечения, в том числе ранее закупленного офисного программного обеспечения» и многими другими. Также это обеспечит устойчивое развитие компаний и цифровой инфраструктуры России. При этом будет поддерживаться и улучшаться качество использования продукта и оказания услуг при гарантированном уровне безопасности и надежности.

В совокупности перечисленные факторы создают благоприятную среду для дальнейшего роста рынка отечественных почтовых клиентов, что позволит укрепить технологическую независимость страны и повысить уровень информационной безопасности российского бизнеса.

[4] [Электронный доступ]. URL: *https://reestr.digital.gov.ru/reestr/307549/*



ИЛЬЯ УШАНОВ
генеральный директор
ООО «Геларм»

МЕТОДОЛОГИЯ, ПРОБЛЕМАТИКА И ОСОБЕННОСТИ ПОСТРОЕНИЯ ЗОНТИЧНОЙ СИСТЕМЫ МОНИТОРИНГА И ИНВЕНТАРИЗАЦИИ ДАННЫХ В КРУПНЫХ ОРГАНИЗАЦИЯХ

ЧТО ТАКОЕ ЗОНТИЧНАЯ СИСТЕМА МОНИТОРИНГА ДАННЫХ?

Зонтичная система мониторинга – термин, который часто вызывает дискуссию, потому что существуют разные трактовки того, каким же должен быть мониторинг, а тем более зонтичный, в организации. Поэтому мы раскроем суть данного термина и далее перейдем к вопросам миграции с западных на российские решения, проблематике этих решений и другим аспектам. Прежде всего, нужно разграничить мониторинг для малых и средних организаций и мониторинг в крупном бизнесе. Для первой группы компаний разумной достаточностью является использование open source[1] решений или программного обеспечения (ПО) с невысокой производительностью, без онлайн контроля метриковой информации, параметров SLA[2] и прочего. Все меняется в крупных, в том числе территориально-распределенных, ИТ-инфраструктурах, особенно если они принадлежат к сегменту критической информационной инфраструктуры (КИИ). Зонтичный мониторинг здесь – это система, собирающая и обрабатывающая огромные массивы данных со всего оборудования в контуре компании, ПО, процессов, датчиков, а также умеющая коррелировать события между собой и определять корневую причину сбоя или простоя в любом месте инфраструктуры компании. Использование разрозненных систем мониторинга, open source решений или ПО с неподходящей производительностью гарантировано принесет компании экономические потери из-за несвоевременного и/или не верного реагирования на инцидент/простой. В текущих социально-экономических реалиях это еще и грозит высокими рисками в сфере безопасности. Тем не менее, существует опасное заблуждение, что зонтичный мониторинг – это исключительно «картинки» с информацией работает/не работает, упускающее из виду большую сложность в определении именно корневых причин проблем. Для того, чтобы обезопасить бизнес от простоев производства, финансовых и репутационных потерь, рисков в области безопасности, необходимо построить полноценную зонтичную систему мониторинга, обязательно опирающуюся на зрелую систему инвентаризации данных. Есть ли сейчас на российском рынке решения, способные решить данную задачу?

Сегмент решений мониторинга и инвентаризации данных в России за последние годы претерпел существенные изменения. Во-первых, из-за полномасштабного ухода ключевых западных игроков, таких как IBM Tivoli, а во-вторых, из-за того, что появился ряд российских компаний, способных в той или иной мере заменить покинувшие рынок решения. Можно констатировать факт, что большой просадки этот сегмент избежал, но общая проблема ИТ-рынка, а именно недостаток информации об имеющихся возможностях в области мониторинга и инвентаризации данных, а также методологии перехода с западных решений на российские, безусловно присутствует.

КАК ПОСТРОИТЬ И ИЗ ЧЕГО ДОЛЖНА СОСТОЯТЬ ПОЛНОЦЕННАЯ ЗОНТИЧНАЯ СИСТЕМА МОНИТОРИНГА ДЛЯ КРУПНОГО БИЗНЕСА?

При построении системы мониторинга важно понимать, что в фундаменте всегда должна лежать автоматически пополняемая инвентарная база инфраструктуры предприятия, которая содержит в себе описания всех объектов инфраструктуры, включая их свойства и взаимосвязи, а также сервисы, которые эти элементы предоставляют. Важно отметить, что ручной труд для наполнения такой базы должен быть сведён практически к нулю, так как для корректной работы процессов управления инцидентами, корреляции и обогащения событий мониторинга, требуется высокий уровень актуальности инвентарных данных.

Вторым элементом для построения качественной системы мониторинга является система управления инцидентами, так как по факту основная задача мониторинга – получить события, определить корневую причину с симптомами, завести инцидент и проконтролировать его решение. Жизненный цикл события представлен на **рис. 1**. Все функции работы пользователя по предупреждению аварии лежат в системе управления инцидентами. Мониторинг может предоставлять только дополнительные функции для диагностики проблемы.

[1] Open source (с английского – «открытый исходный код») – это модель разработки программного обеспечения, при которой исходный код доступен для просмотра, изменения и распространения любым желающим.
[2] SLA (англ. *Service Level Agreement* – соглашение об уровне предоставления услуги) – это соглашение между поставщиком услуги и клиентом, определяющее уровень предоставляемых услуг, их качество и ответственность сторон в случае нарушений.



Рис. 1. Жизненный цикл события

Важно отметить, что система управления инцидентами и мониторинг должны существовать в единых координатах справочников, и это обеспечивает система инвентаризации. К примеру, в систему мониторинга пришло событие, которое обогащается идентификатором элемента (КЕ). При заведении инцидента из системы мониторинга помимо информации об аварии также передаётся идентификатор КЕ, так как к этому идентификатору в системе управления инцидентами уже привязаны ответственные сотрудники и необходимые процессы эскалации.

Таким образом, при построении системы мониторинга важно понимать, что в ее основе лежит автоматически пополняемая база конфигурационных элементов, учитывающая связи между ними. Она служит фундаментом для инцидент менеджмента и именно она обеспечивает важнейший процесс – корреляцию событий. Прежде чем придавать статус «работает/не работает» необходимо четко настроить процесс сбора и анализа данных о том, что реально происходит в ИТ-инфраструктуре, где произошло корневое событие и какие у него последствия. В этом процессе особую роль играет использование правильного набора метрик и корректная обработка событийной информации. Для крупных сетевых инфраструктур необходимо собирать огромное число метрик и обрабатывать миллионы событий, что является нетривиальной математической задачей, но без этой работы корректная корреляция событий невозможна. Также для грамотной корреляции событий при построении системы мониторинга нужно создать и/или настроить релевантную базу конфигурационных элементов, включающую оборудование, программное обеспечение и сервисы со всеми связями, чтобы предельно точно настроить процесс обработки инцидента.

КАКИЕ ПРОБЛЕМЫ СУЩЕСТВУЮТ У РОССИЙСКИХ СИСТЕМ МОНИТОРИНГА И ИНВЕНТАРИЗАЦИИ ДАННЫХ?

На данный момент на российском рынке представлен ряд вполне зрелых систем мониторинга, но отсутствует система инвентаризации данных enterprise уровня[3], включающая в себя базу конфигурационных элементов для целей мониторинга. Вместе с этим, отсутствует и полноценный автодискаверинг[4], который обязательно должна содержать зрелая система инвентаризации. Меры для решения этой проблемы на рынке принимаются, и разработчики программных продуктов, вероятно, смогут в обозримом будущем предоставить удовлетворяющее потребности заказчиков решение.

Точкой роста в развитии отечественных систем мониторинга и инвентаризации данных сейчас является возможность практического использования алгоритмов искусственного интеллекта (ИИ) для автоматического создания сценариев корреляции событий, т.е. выявления корневой аварии и её симптомов. На данный момент такая задача решается путём ручного формирования сценариев корреляции. В текущей ситуации все события, которые не попали под правила корреляции, попадают на консоль оператору, и он осуществляет их ручную обработку с возможностью создания нового сценария корреляции. Для примера, средний поток событий в сутки у оператора мобильной связи в России равен 800 000 000. Если у оператора связи высокий уровень зрелости системы мониторинга, то около 99,99% событий обрабатываются автоматически, а 0,01%

[3] Enterprise-уровень – это крупномасштабные программные решения, предназначенные для удовлетворения сложных и многоуровневых бизнес-потребностей крупных организаций или многонациональных корпораций.
[4] Автодискаверинг – это система автоматической инвентаризации, которая позволяет собирать информацию об установленных и используемых экземплярах программного обеспечения (ПО) с различных типов клиентов.

приходится обрабатывать вручную и формировать по ним сценарии корреляций для дальнейшего совершенствования системы. Но даже 0,01% это существенная нагрузка для специалистов операторов связи, так как приходится обработать вручную около 80 000 событий. Для решения данной проблемы целесообразно использовать современные алгоритмы ИИ. Операторы связи накопили уже достаточно большой массив данных для обучения моделей ИИ, что открывает дорогу для внедрения данной технологии в практической сфере.

Компания Gelarm исторически работает с операторами связи и накопила существенный объем данных (datasets), что обеспечивает возможность проводить исследовательские работы и разработку (research&development) по направлениям использования алгоритмов ИИ для автоматического создания правил корреляции событий и использования алгоритмов ИИ для автоматического создания правил заведения инцидентов. В планах компании на 2025-2026 годы подобрать алгоритмы сегментации данных и собрать стенд для отработки теоретических моделей, а затем создать прототип обучаемой модели для обкатки решения в инфраструктуре заказчиков.

КАКИЕ КЛЮЧЕВЫЕ ОСОБЕННОСТИ СИСТЕМ МОНИТОРИНГА И ИНВЕНТАРИЗАЦИИ ДАННЫХ В КРУПНОМ БИЗНЕСЕ?

Эталонными инфраструктурами в части построения мониторинга и инвентаризации данных являются ИТ-инфраструктуры операторов связи, так как в них в сутки непрерывно обрабатываются сотни миллионов событий и метрик от миллионов единиц оборудования и программного обеспечения. Инфраструктура операторов связи находится на пике технологий, и в части решений для инвентаризации или мониторинга стоит обратиться к операторскому опыту и посмотреть какое ПО и какие подходы при внедрении они используют.

Для решения задач подобного уровня сложности необходимо, чтобы система обладала гибкими настройками для глубокой интеграции с бизнес-процессами, такими как управление SLA и прочими. Другим важным моментом при построении или миграции системы мониторинга в масштабных, в том числе территориально распределённых ИТ-инфраструктурах, является наличие шины для интеграции данных. В решении GIMS этот функционал выполняет блок GIMS Automation, способный получать данные из различных источников, обрабатывать их и загружать в любые типы хранилищ, реализуя автоматизацию процедур ETL, а также может применяться для интеграции различных приложений между собой. Для распределенной инфраструктуры очень важно иметь возможность создания множества выносов для реализации опроса объектов мониторинга в различных сетевых сегментах с асинхронной обработкой данных, что также реализуется с помощью GIMS Automation.

МИГРАЦИЯ ИЛИ НОВАЯ СИСТЕМА МОНИТОРИНГА, ВОТ В ЧЕМ ВОПРОС.

На данный момент самой насущной задачей и проблемой отечественного ИТ-рынка в части мониторинга и инвентаризации данных является импортозамещение распространенных западных решений, таких как IBM Tivoli и HP OpenView, и этот тренд на рынке сохранится еще 3-5 лет. Долгие годы российский рынок был занят западными решениями, и проблема заключается в том, что у большинства отечественных производителей отсутствует методология перехода с западных решений на российские. Некоторые компании идут по пути построения новой системы мониторинга, параллельно действующей на западных решениях. Такой подход имеет большие риски, поскольку проект по созданию системы мониторинга в крупной компании занимает 2-3 года, а затем необходимо провести незаметный «переезд», что практически невозможно сделать безупречно и незаметно. Другим методом является поэтапная замена элементов западного решения на российские компоненты. Для такого сценария миграции необходимы четкая методология миграции и совместимость российского решения с используемым западным. При этом, методология миграции без обеспечения совместимости нереализуема. Компания Gelarm предлагает решение GIMS, которое позволяет выполнять поэтапное замещение западных решений российским, по нашему мнению, наиболее эффективно. Структура решения GIMS, удовлетворяющего жестким требованиям высоконагруженных ИТ-инфраструктур, представлена на **рис. 2**.

Более того, позиция компании Gelarm представляется наиболее выигрышной, т.к. решение GIMS архитектурно максимально близко к лидирующему в мире IBM Tivoli и способно бесшовно заменять его в ИТ-ландшафте любого, самого крупного заказчика.

КОМПОНЕНТЫ СИСТЕМЫ МОНИТОРИНГА И ИНВЕНТАРИЗАЦИИ GIMS

Несмотря на то, что Gelarm – достаточно молодой вендор, команда экспертов, создавших компанию и программный продукт GIMS, хорошо известна в области проектирования и разработки систем мониторинга, управления ИТ-инфраструктурой и технологическими процессами предприятий. Долгое время специалисты Gelarm внедряли и поддерживали решения по мониторингу и инвентаризации данных в компаниях-операторах связи, что и продолжают делать, используя уже собственный продукт, учитывающий все особенности внедрения, миграции и поддержки систем мониторинга и инвентаризации данных в крупных компаниях. Решение Gelarm Infrastructure Management System, во многом превосходящее мировые аналоги в сфере мониторинга, инвентаризации данных и управления корпоративным хранилищем данных, состоит из трех модулей:

- GIMS Automation – система для интеграции различных информационных систем между собой. Система обеспечивает подключения к различным источникам данных, сценарии обработки информации, триггеры для запуска сценариев обработки информации.

- GIMS Monitoring – система мониторинга сервисов организации. Система обеспечивает сбор и корреляцию событий сервисов, сбор метрик производительности и качества сервисов.
- GIMS Inventory – система инвентаризации оборудования, программного обеспечения и объектов инфраструктуры. Система обеспечивает построение топологий инфраструктуры, создание моделей данных описывающих классы объектов, связей и их атрибуты.

ПРИМЕР ПОЭТАПНОЙ ЗАМЕНЫ ЗАПАДНЫХ ПРОДУКТОВ РЕШЕНИЕМ КОМПАНИИ GELARM

Компания Gelarm предлагает метод поэтапной замены элементов западного решения на российские компоненты. Для такого сценария миграции необходимы четкая методология миграции и обеспечение совместимости российского решения с ушедшим западным. При этом, методология миграции без совместимости нереализуема. Решение GIMS позволяет выполнять такое поэтапное замещение, поэтому позиция компании Gelarm, полагаем, наиболее выигрышная на рынке.

Рассмотрим пример реализации такого проекта в компании оператора связи.

Описание объекта автоматизации:

- Количество объектов мониторинга: более 2 млн.
- Сегменты объектов мониторинга: сеть радиодоступа, транспортная сеть, инженерное оборудование, системы электропитания, системы контроля и учёта доступа, ИТ инфраструктура.
- Инфраструктура разделена на 8 филиалов.
- Поток событий в сутки: более 500 млн.
- Протоколы интеграции: SNMP, SYSLOG, CORBA, HTTPS, JDBC, ICMP, SFTP, IMAP.
- Система мониторинга построена на базе продуктов IBM Tivoli по трёхуровневой модели (сбор, агрегация, отображение) с отдельно выделенным слоем автоматизации обработки событий (корреляция, обогащение, автодиагностика и т.д.). Система развивалась более 10 лет.

Этапы реализации проекта:

Этап 1. Замещение слоя автоматизации обработки событий. Продолжительность этапа 8 месяцев.

Этап 2. Замещение слоя сбора и предварительной обработки событий. Продолжительность этапа 8 месяцев.

Этап 3. Замещение слоя агрегации событий. Продолжительность этапа 2 месяца.

Этап 4. Замещение слоя отображения или пользовательского портала. Продолжительность этапа 4 месяца.

Предлагаемая методология позволяет мигрировать функционал системы, которая развивалась в течении 10 лет без потери функций, минимизировать

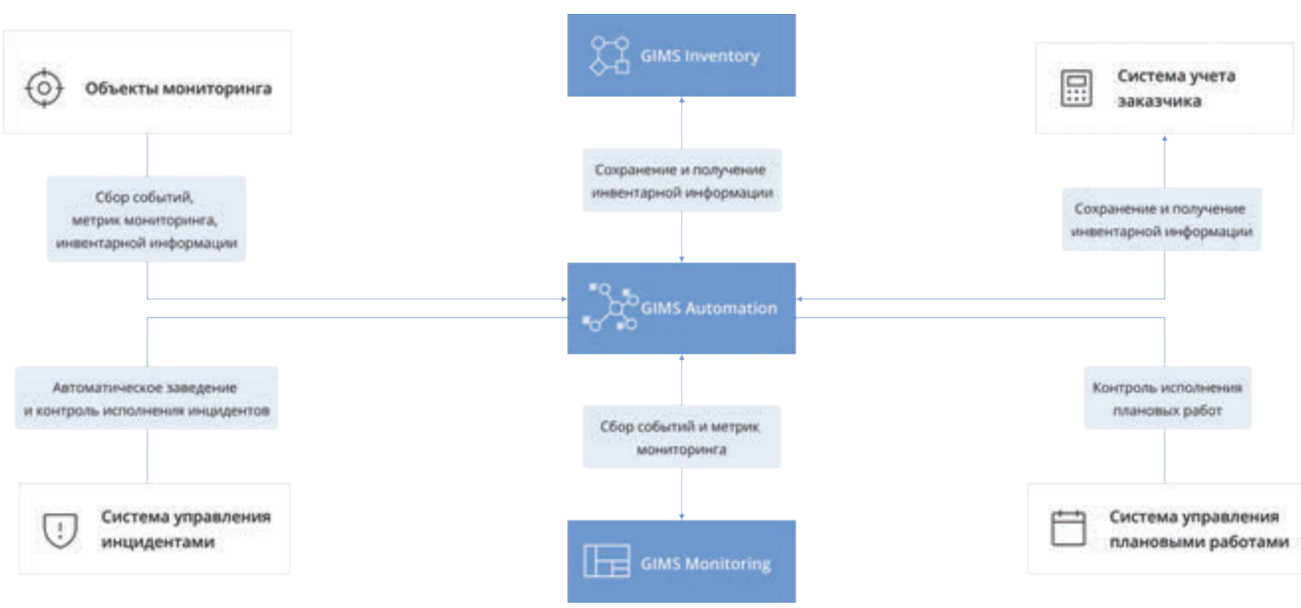


Рис. 2. Общая архитектура системы мониторинга на примере использования продуктов линейки GIMS от компании Gelarm

пользовательский негатив за счёт постепенного перехода, минимизировать финансовые риски, т.к. инвестиции выполняются короткими этапами с чётким и понятным результатом. При таком подходе можно довольно быстро выявить пригодность выбранного продукта и команды для реализации поставленной задачи. Это является не маловажным фактом при внедрении отечественных решений, имеющих маленькое портфолио.

ОСНОВНЫЕ ТОЧКИ РОСТА В РАЗВИТИИ ОТЕЧЕСТВЕННЫХ СИСТЕМ МОНИТОРИНГА

С учетом рассмотренных в статье положений рассмотрим основные точки роста в развитии отечественных систем мониторинга. Как отметили ранее, одно из самых популярных направлений – возможность практического использования алгоритмов ИИ для автоматического создания сценариев корреляции событий, т.е. выявления корневой аварии и её симптомов. Использование современных алгоритмов ИИ и накопленного операторами связи достаточно большого массива данных для обучения моделей ИИ будут способствовать внедрению данной технологии в практической сфере.

Второе важное направление развития систем мониторинга – высокоскоростные хранилища, позволяющие хранить большие объёмы событий и метрик. Данные хранилища должны позволять быстро оперировать наборами данных на любую историческую глубину и по различным параметрам сегментации данных. Это необходимо для предсказательной аналитики, для обучения алгоритмов ИИ, а также для удовлетворения кратного роста объёма данных мониторинга от инфраструктуры за последние годы.

Третье направление – стандартизация протоколов мониторинга и инструментов для описания правил обработки событий и метрик. Прошло то время, когда многие производители ПО и оборудования старались сделать закрытый протокол для того, чтобы привязать заказчика к своим решениям. Это создавало массу не нужных прослоек при построении зонтичной системы мониторинга, в результате заказчик нёс дополнительные затраты как при внедрении решения, так и при его эксплуатации. Также такой подход плохо сказывался на надёжности решения, т.к. использовались избыточные компоненты.

Четвертое направление – разработка методологий для учёта и мониторинга сервисов организаций. Это обширное направление, о котором можно написать отдельную статью.

ВЫБОР ВСЕГДА ДЕЛАЕТ ЗАКАЗЧИК

Резюмируя все вышесказанное, хотелось бы отметить, что первым вопросом в процессе принятия решения о построении/миграции системы зонтичного мониторинга должен быть вопрос о ее назначении в компании. После того, как ИТ-специалисты и руководство компании-заказчика определят цели функционирования такой системы, можно приступать к выбору и анализу продуктов на рынке. Лучше всего это делать при помощи нагрузочного тестирования с 10-20 тысячами объектами мониторинга. Если объектов меньше, то такая система просто не нужна. Если объектов больше, то тестирование покажет возможности того или иного решения. Цена ошибки при выборе не соответствующей ИТ-инфраструктуре и бизнес-задачам системы мониторинга и инвентаризации данных может быть очень большой.

ОБЕСПЕЧЕНИЕ ДОВЕРИЯ И БЕЗОПАСНОСТИ ПРИ ИСПОЛЬЗОВАНИИ ИКТ



ЛЕВ ЛУНЕГОВ
ведущий технический аналитик
ФГБУ «НИИ «Интеграл»



НИКИТА НЕМЦЕВ
технический аналитик
ФГБУ «НИИ «Интеграл»

ИСПОЛЬЗОВАНИЕ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА ДЛЯ БОРЬБЫ С ФИШИНГОМ

ВВЕДЕНИЕ

Активная цифровизация всех сфер жизни создала широкие возможности не только для развития, но одновременно и для киберпреступности. Злоумышленники получили доступ к мощным инструментам, позволяющим проводить атаки с высокой эффективностью и в глобальном масштабе. Фишинг[1], как одна из самых распространенных угроз, значительно эволюционировал: современные атаки используют персонализацию, механизмы обхода систем обнаружения и другие методы, способствующие повышению доверия пользователя.

[1] Фишинг – это методика обмана пользователей путем имитации легитимных ресурсов с целью неправомерного получения конфиденциальных сведений для их последующего использования в совершении преступлений.

Традиционные средства защиты, основанные на статических правилах и черных списках, часто не справляются с новыми, быстро адаптирующимися тактиками злоумышленников [1]. В этих условиях искусственный интеллект (ИИ) становится критически важной технологией для противодействия фишингу, алгоритмы машинного обучения способны анализировать огромные объемы данных в реальном времени, выявлять сложные схемы мошенничества и адаптироваться к новым угрозам.

ПОЧЕМУ ЭФФЕКТИВНОСТЬ ТРАДИЦИОННЫХ МЕТОДОВ СНИЖАЕТСЯ

Несмотря на долгую историю борьбы, классические подходы к выявлению фишинговых сайтов все чаще оказываются неэффективными перед лицом современных тактик мошенников. Ключевая слабость классических подходов – статичность и реактивность в условиях динамично меняющейся угрозы [2]. Сигнатурный анализ, основанный на сравнении кода страниц или их фрагментов с базами известных вредоносных шаблонов, бесполезен против постоянно обновляемых или совершенно новых фишинговых ресурсов. Злоумышленники легко обходят его, применяя простую обфускацию кода[2] [3]: меняют структуру HTML, добавляют случайные комментарии или пробелы, используют разные скрипты для достижения одной цели, чтобы код страницы не совпал с известной сигнатурой. Даже если сигнатура создана для нового шаблона, всегда существует критическая задержка между обнаружением угрозы, созданием сигнатуры и ее обновлением на всех защищенных устройствах пользователей, которой успешно пользуются фишеры.

Черные списки доменов и URL – еще один столп традиционной защиты – имеют критический недостаток, они всегда отстают. Фишинговые кампании сегодня используют одноразовые сайты: массово создаются новые домены или используются дешевые хостинги и легитимные, но скомпрометированные веб-ресурсы для размещения фишинговых страниц. Эти страницы существуют считанные часы или дни, собирают данные жертв и исчезают задолго до того, как их URL-адрес или домен успеют внести в блоклисты [4]. Злоумышленники мастерски используют визуально похожие домены, заменяя буквы похожими символами или применяя символы идентичные латинским, которые на первый взгляд выглядят легитимно и не вызывают подозрений у систем, опирающихся только на списки запрещенных адресов [5]. Широко распространена маскировка конечного вредоносного URL-адреса через сервисы сокращения ссылок или сложные цепочки перенаправлений через легитимные, но уязвимые, или нейтральные промежуточные сайты. Пользователь видит в адресной строке или при наведении курсора безопасный короткий URL, который в итоге ведет на фишинговую страницу, и черные списки бессильны против такой маскировки.

Статические эвристические правила, пытающиеся искать на страницах подозрительные ключевые элементы, легко обходятся. Фишеры заменяют эти слова синонимами, используют изображения с текстом вместо самого текста, или просто копируют дизайн и стиль легитимных сайтов до мельчайших деталей, избегая явных ключевых фраз. Более сложные правила, применяемые при анализе структуры страницы, также ненадежны: легитимные формы ввода данных выглядят аналогично, а фишинговые страницы могут искусно маскироваться под них. Главная же проблема статических правил – их неспособность оценить контекст и правдоподобность сайта в целом. Они не могут понять, что сайт идеально копирующий дизайн банка, но расположенный на странном домене или без валидного SSL-сертификата известного центра сертификации, является подделкой [6]. Они не улавливают тонкие несоответствия в логотипах, шрифтах или общем ощущении подлинности, которые может заметить человек или более интеллектуальная система.

Ручной анализ и верификация сайтов специалистами безопасности не могут масштабироваться под поток новых подозрительных URL-адресов. Физически невозможно вручную в режиме реального времени проверить каждый потенциально опасный ресурс в сети Интернет или каждый сайт, на который пытается перейти пользователь. Время реакции критически велико, а нехватка экспертов делает этот подход непрактичным для массовой защиты. В итоге, все эти методы уязвимы из-за своей фундаментальной реактивности и статичности. Эти методы настроены искать некачественно сделанные мошеннические сайты или очень явные признаки подделки, но совершенно не способны проактивно выявлять новые, ранее неизвестные фишинговые ресурсы, особенно те, что искусно маскируются под легитимные. Они не могут анализировать комплексные факторы: репутацию домена в реальном времени, валидность и цепочку SSL-сертификатов, историю создания домена, визуальное сходство с брендом, поведенческие сценарии на странице – и делать выводы на основе совокупности слабых сигналов. Экономика атаки выгодна злоумышленникам: создание нового фишингового сайта или клона обходится дешево и происходит быстро, в то время как поддержание актуальности и эффективности традиционных защитных механизмов требует постоянных и значительных затрат ресурсов. Эта растущая пропасть между изощренностью и скоростью создания фишинговых сайтов и возможностями старых методов защиты делает необходимым переход к принципиально новым подходам – интеллектуальным, адаптивным, способным обучаться и анализировать

[2] Обфускация кода — это метод преобразования исходного кода приложения, который делает его трудным для понимания и анализа.

сайты комплексно, оценивая множество параметров для выявления подделок. Именно такие возможности предоставляют технологии искусственного интеллекта и машинного обучения [7].

ИСПОЛЬЗОВАНИЕ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА

Осознавая ограничения традиционных подходов, ФГБУ «НИИ «Интеграл» разработало и внедрило специализированное решение на основе искусственного интеллекта, направленное на эффективное выявление фишинговых веб-ресурсов. Была проведена масштабная работа по обучению модели машинного обучения, ставшей основой программного модуля, предназначенного для глубокого анализа сайтов. Этот модуль не ограничивается поверхностной проверкой; он проводит всестороннее исследование всех доступных данных, связанных с подозрительным веб-ресурсом. Анализ начинается с тщательного изучения самого URL-адреса, выявляя паттерны, характерные для поддельных или вредоносных ссылок. Информационная система мониторинга фишинговых сайтов ИС «Антифишинг» (далее – Система) агрегирует и обрабатывает обширные данные о домене: срок его существования, информацию о регистраторе и владельце, репутационные показатели. Однако ключевая сила решения заключается в глубинном сканировании и оценке самого содержимого и поведения сайта. Модуль анализирует структуру HTML-страницы, выявляя подозрительные схемы расположения элементов, а также оценивает сценарии поведения: наличие необычно агрессивных или скрытых запросов данных пользователя, злонамеренных полей ввода, маскирующихся под легитимные, или скриптов, специально разработанных для обхода средств обнаружения, например, обфускация кода, динамическая подгрузка вредоносного контента, проверка на наличие анализатора. Для оценки самодостаточности или, наоборот, зависимости от внешних ресурсов, Система рассчитывает сложные метрики, такие как процент внутренних ссылок и процент контента, подгружаемого со сторонних, потенциально небезопасных источников. Исследуются все исполняемые скрипты на странице с целью выявления потенциально вредоносных функций или попыток эксплуатации уязвимостей браузера. Важным аспектом архитектуры Системы является то, что ИИ-модуль не действует как полностью автономный «черный ящик», выносящий окончательный и безоговорочный вердикт, вместо этого он выполняет функцию интеллектуального ассистента аналитиков. На основе комплексного анализа параметров и выявленных аномалий ИИ-модель формирует обоснованное заключение о характере ресурса и присваивает ему потенциальный уровень угрозы. Эта оценка поступает в Систему, такой подход кардинально меняет рабочий процесс операторов и аналитиков Системы. Им больше не требуется тратить значительное время на ручное, детальное изучение каждого поступающего в систему подозрительного ресурса. Система, благодаря высокой точности анализа, предварительно оценивает очевидно легитимные или, наоборот, явно вредоносные сайты, существенно сужая область для ручной проверки и фокусируя внимание специалиста на наиболее критичных моментах. Это позволило ФГБУ «НИИ «Интеграл» добиться значительного сокращения времени обработки каждого инцидента в Системе, повысить пропускную способность анализа и оперативность реагирования на новые фишинговые угрозы в веб-пространстве, переложив основную нагрузку по первичной, трудоемкой оценке на обученные алгоритмы искусственного интеллекта.

Дополнительным инструментом, реализованным ФГБУ «НИИ «Интеграл» на базе обученной ИИ-модели, стал автоматизированный источник данных в Систему, работающий с ресурсами, вызывающими подозрения у пользователей сети Интернет. Механизм работает следующим образом: модуль собирает данные о веб-сайтах, на которые пользователи жалуются через различные общедоступные каналы как на потенциально мошеннические или фишинговые. Эти ресурсы, часто являющиеся еще не попавшими в фокус профессиональных аналитиков, автоматически поступают для анализа в программный модуль, основанный на искусственном интеллекте. Модуль оперативно сканирует и анализирует каждый такой сайт по всем ранее описанным параметрам. Ключевым моментом является то, что модуль не просто анализирует, а применяет свою обученную модель для оценки уровня угрозы. Если по результатам этого сайт получает оценку как опасный, он автоматически, без обязательного ручного подтверждения аналитиком на первом этапе, заносится в Систему через специальный канал. Это создает принципиально новый источник обнаружения угроз. Теперь Система получает информацию не только о ресурсах, напрямую выявленных или поступивших через официальные каналы обращений, но и о тех фишинговых сайтах, с которыми уже столкнулись и на которые пожаловались пользователи в сети Интернет, даже если эти пользователи не направляли официальное обращение непосредственно. Это позволяет значительно расширить охват Системы, оперативно включать в защиту актуальные, только что появившиеся или активно используемые мошенниками ресурсы, на которые уже обратили внимание жертвы, и блокировать их распространение на более широкую аудиторию.

ПЕРСПЕКТИВЫ СОЗДАНИЯ НОВЫХ МЕХАНИЗМОВ ПРОТИВОДЕЙСТВИЯ НА ОСНОВЕ ИИ

Опыт успешного применения ИИ-модуля для анализа сайтов открывает новые горизонты для разработки еще более совершенных инструментов, и в данный момент проводится активная разработка двух ключевых проектов. Первый проект – система предиктивного распознавания доменных имен – нацелен на выявление доменов, которые с высокой вероятностью будут использованы для фишинга, еще до начала активной фазы атаки. Используя машинное обучение для анализа паттернов, система предиктивного распознавания доменных имен сможет проактивно идентифицировать потенциально опасные ресурсы, позволяя повысить эффективность мониторинга на самом раннем этапе. Второй проект – система аналитики фишинговых сайтов на основе ИИ – предназначен для

решения задачи консолидации разрозненных инцидентов. Алгоритмы будут глубоко анализировать технические характеристики, контент, скрипты и инфраструктуру множества обнаруженных фишинговых ресурсов, выявляя скрытые связи и общие черты. Это позволит автоматически объединять отдельные сайты в целостные фишинговые кампании, выявляя преступные группы, их инструменты и тактики. Такая кластеризация критически важна для понимания полной картины угрозы, пресечения деятельности преступных групп на системном уровне и прогнозирования их следующих шагов, что выводит борьбу с фишингом на качественно новый уровень стратегического противодействия.

ЗАКЛЮЧЕНИЕ

Борьба с фишингом перешла в эпоху, где скорость, масштаб и изощренность атак сделали традиционные, реактивные методы защиты недостаточными. Как показано в статье, искусственный интеллект стал не просто дополнением, а стратегическим императивом в этой непрекращающейся битве. Его способности анализировать колоссальные объемы данных в реальном времени, выявлять сложные, скрытые паттерны и адаптироваться к новым тактикам злоумышленников предлагают принципиально иной уровень противодействия – проактивный, контекстный и масштабируемый.

Практический пример – разработки ФГБУ «НИИ «Интеграл». Внедренный ИИ-модуль для комплексного анализа сайтов значительно ускорил обработку инцидентов в информационной системе мониторинга фишинговых сайтов ИС «Антифишинг». Модуль выносит предварительную оценку угрозы, фокусируя внимание аналитиков на наиболее критичных случаях. Автоматический источник данных на основе ИИ-анализа сайтов, отмеченных в пользовательских жалобах, оперативно включает в защиту актуальные угрозы, с которыми уже столкнулись пользователи.

Таким образом, технологии ИИ показывают свою ключевую роль в борьбе с фишингом, предлагая не просто обнаружение, а проактивную, масштабируемую защиту. Развитие интеллектуальных систем в настоящее время – необходимое направление для обеспечения безопасности в цифровой среде.

СПИСОК ЛИТЕРАТУРЫ

1. Гордиенко В. В., Жданов Д. М. МЕТОДЫ ЗАЩИТЫ ОТ СОЦИАЛЬНОЙ ИНЖЕНЕРИИ И ФИШИНГА. ИХ ДОСТОИНСТВА И НЕДОСТАТКИ // Auditorium. 2024. №2 (42). URL: *https://cyberleninka.ru/article/n/metody-zaschity-ot-sotsialnoy-inzhenerii-i-fishinga-ih-dostoinstva-i-nedostatki* (дата обращения: 09.06.2025).

2. Архипова А. Б., Нечаев Д. А. ТЕХНОЛОГИЯ ФОРМИРОВАНИЯ ИНТЕГРИРОВАННОЙ АНТИФИШИНГОВОЙ СИСТЕМЫ В ЦИФРОВОМ ОБЩЕСТВЕ // Вестник СибГУТИ. 2023. №2. URL: *https://cyberleninka.ru/article/n/tehnologiya-formirovaniya-integrirovannoy-antifishingovoy-sistemy-v-tsifrovom-obschestve* (дата обращения: 09.06.2025).

3. Войнов А. С. ИССЛЕДОВАНИЕ УЯЗВИМОСТЕЙ И УГРОЗ В МОБИЛЬНЫХ ПРИЛОЖЕНИЯХ: СТРАТЕГИИ ПРОТИВОДЕЙСТВИЯ // Вестник науки. 2023. №9 (66). URL: *https://cyberleninka.ru/article/n/issledovanie-uyazvimostey-i-ugroz-v-mobilnyh-prilozheniyah-strategii-protivodeystviya* (дата обращения: 09.06.2025).

4. Корнюхина С. П., Лапонина О. Р. ИССЛЕДОВАНИЕ ВОЗМОЖНОСТЕЙ АЛГОРИТМОВ ГЛУБОКОГО ОБУЧЕНИЯ ДЛЯ ЗАЩИТЫ ОТ ФИШИНГОВЫХ АТАК // International Journal of Open Information Technologies. 2023. №6. URL: *https://cyberleninka.ru/article/n/issledovanie-vozmozhnostey-algoritmov-glubokogo-obucheniya-dlya-zaschity-ot-fishingovyh-atak* (дата обращения: 10.06.2025).

5. Данько О. С., Медведева Т. А. ИССЛЕДОВАНИЕ ТЕХНИК ФИШИНГА И МЕТОДОВ ЗАЩИТЫ ОТ НЕГО // Молодой исследователь Дона. 2021. №3 (30). URL: *https://cyberleninka.ru/article/n/issledovanie-tehnik-fishinga-i-metodov-zaschity-ot-nego* (дата обращения: 10.06.2025).

6. Афанасьева Н. С., Елизаров Д. А., Мызникова Т. А. КЛАССИФИКАЦИЯ ФИШИНГОВЫХ АТАК И МЕРЫ ПРОТИВОДЕЙСТВИЯ ИМ // ИВД. 2022. №5 (89). URL: *https://cyberleninka.ru/article/n/klassifikatsiya-fishingovyh-atak-i-mery-protivodeystviya-im* (дата обращения: 10.06.2025).

7. Баратбаев И. З. ПРИМЕНЕНИЕ МАШИННОГО ОБУЧЕНИЯ В ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ // In The World Of Science and Education. 2025. №15 март ТН. URL: *https://cyberleninka.ru/article/n/primenenie-mashinnogo-obucheniya-v-informatsionnoy-bezopasnosti* (дата обращения: 10.06.2025).



ДЕНИС БАТРАНКОВ
директор по развитию
ГК «Гарда»

ИСКУССТВЕННЫЙ ИНТЕЛЛЕКТ В КИБЕРБЕЗОПАСНОСТИ: НОВАЯ ЭРА ЦИФРОВОЙ ЗАЩИТЫ

ОТ ТЕОРИИ К ПРАКТИКЕ — ИИ В ДЕЙСТВИИ

Если еще вчера искусственный интеллект (ИИ) в кибербезопасности звучал как абстракция, то сегодня он стал по-настоящему прикладным инструментом, который применяется в продуктах, процессах и даже фигурирует в регуляторных нормах. Интеллектуальные системы (ИС) уже работают в антифрод-сервисах банков, системах мониторинга промышленных сетей, решениях для мониторинга облачной безопасности и даже в call-центрах, где ИИ может не только идентифицировать клиента по голосу, но и заметить эмоциональные аномалии в его речи.

Характерный пример — внедрение ИИ-алгоритмов в таких системах мониторинга и защиты, как SIEM и XDR[1]. Раньше для настройки правил корреляции событий информационной безопасности (ИБ) нужно было вручную прописывать десятки условий. Сегодня система сама выявляет, например, что запрос от бухгалтерии в 3 часа ночи к серверу инженерного отдела — аномалия. И делает это без участия человека.

В настоящей статье под термином «искусственный интеллект» мы будем иметь в виду технологию создания интеллектуальных машин, особенно интеллектуальных компьютерных программ.

ИИ В ЗАЩИТЕ КРИТИЧЕСКОЙ ИНФРАСТРУКТУРЫ

Для объектов критической информационной инфраструктуры (КИИ) ИИ становится не просто удобством, а насущной необходимостью. Цена ошибки для таких объектов может быть измерена не только в деньгах, а, в первую очередь, в рисках для здоровья граждан, экологии и безопасности страны.
Применение ИИ в КИИ позволяет:

- выявлять попытки вмешательства в SCADA-системы[2];
- анализировать технические журналы в режиме реального времени;
- строить модели нормального поведения оборудования и быстро реагировать на отклонения.

Ряд российских решений уже показал эффективность в этом сегменте. Отечественные решения особенно необходимы при работе в условиях импортозамещения, когда традиционные западные средства стали недоступны или не соответствуют требованиям российского законодательства.

ИИ ПРОТИВ УГРОЗ НУЛЕВОГО ДНЯ И ПОДДЕЛЬНЫХ СООБЩЕНИЙ

Одна из самых грозных категорий угроз — уязвимости нулевого дня (zero-day). Речь идет о проблемах в программном обеспечении, о которых еще не знают разработчики и которые не успели устранить. В этот момент злоумышленники могут воспользоваться уязвимостью раньше всех — до того, как появится какое-либо обновление или защита. Такие атаки особенно опасны именно потому, что системы не готовы к ним: ни антивирусы, ни специалисты по безопасности не знают, чего ожидать. Обнаружить их традиционными средствами почти невозможно. Но ИИ в силах изменить правила игры: он может анализировать поведение системы, искать отклонения и даже предсказывать векторы, по которым возможна атака.

Пример из практики: в одном из проектов ИБ-команда использовала модель машинного обучения для анализа сетевого поведения IoT-устройств[3]. После месяца обучения система заметила странную активность от «умной» камеры — ее IP-адрес начал устанавливать соединения с неизвестными IP-адресами в Восточной Азии. Проверка подтвердила факт заражения. Без ИИ эту активность могли бы заметить через недели — уже после утечки данных.

Есть и обратная сторона медали: злоумышленники все

[1] SIEM (англ. Security Information and Event Management) — система управления событиями информацией безопасности. Предназначена для сбора, анализа и корреляции данных из различных источников безопасности в организации, что позволяет выявлять и реагировать на инциденты безопасности.
XDR (англ. Extended Detection and Response) — система для обнаружения и реагирования на сложные угрозы и целевые атаки. Обеспечивает более широкое представление об инцидентах, чем традиционные решения и позволяет быстрее и точнее реагировать на сложные атаки.
[2] SCADA (англ. Supervisory Control And Data Acquisition) — система диспетчерского управления и сбора данных для автоматизации и мониторинга промышленных и инженерных процессов. Позволяет собирать информацию с датчиков и оборудования, обрабатывать ее и представлять в удобном для оператора виде, а также управлять оборудованием.
[3] IoT-устройство – физическое устройство – например, камера, принтер, чайник – включенное в Интернет вещей (англ. Internet of Things, IoT). Интернет вещей – концепция сети передачи данных между физическими объектами («вещами»), оснащенными встроенными средствами и технологиями для взаимодействия друг с другом или с внешней средой.

чаще комбинируют технические атаки с психологическим воздействием, применяют поддельные аудио- и видео-сообщения (deepfake) в комплексе с методами социальной инженерии. По данным Bugcrowd[4], 71% хакеров в 2024 году заявили, что новые технологии ИИ помогают им в атаках. Для сравнения: в 2023 году таких хакеров было всего 21%. Сегодня даже простые инструменты позволяют сделать реалистичное фейковое видео- или аудиосообщение, способное обмануть не только пользователя, но и систему.

В противовес хакерам, специалисты создают современное программное обеспечение (ПО) и онлайн-сервисы, которые помогают отслеживать deepfake. По данным анализа обзора Unite.AI[5], полагаем, что реально заслуживают внимания следующие решения:

- Deepware Scanner – приложение на смартфоне, которое анализирует аудио и видео. Удобно для быстрой проверки, но часто дает ложные срабатывания — рекомендуется относиться критично.
- Sensity AI — один из лидеров среди профессиональных платформ. Проверяет видео, фото, аудио — всё в одном. Работает на базе обученной нейросети, широко используется в банках и корпорациях.
- DeepFake-o-meter и Reality Defender — экспериментальные сервисы, иногда даже бесплатные, которые способны выявлять базовые подделки, но сложные современные фейки иногда пропускают.

Важно понимать, что ни один из этих инструментов не дает 100% гарантии. Даже лучшие алгоритмы иногда не справляются с новыми, глубоко обученными дипфейками. Мошенники учатся быстрее, чем обновляется защита.

Что часто упускается:

- алгоритмы детекторов чаще выявляют уже устаревшие варианты фейков, а новейшие deepfake-модели пока обходят большинство фильтров;
- все чаще применяются гибридные схемы: фейк-видео с поддельным голосом, deepfake-аватары в Zoom — и здесь традиционные алгоритмы уже бессильны.

В итоге решающее значение по-прежнему имеет человеческий фактор. Тренированный взгляд специалиста иногда замечает подделку быстрее любой нейросети: например, по сбоям синхронизации губ, артефактам на коже или странным бликам в глазах.

ИИ способен помочь, но нельзя полностью полагаться только на его алгоритмы. Именно сочетание автоматических инструментов и обученного человека дает устойчивую защиту — особенно в условиях, когда граница между реальностью и фейком все более размыта.

ЭТИКА И «ПРАВА МАШИНЫ»: НОВЫЙ УРОВЕНЬ ДИСКУССИИ

С ростом влияния ИИ на защитные процессы возникает вопрос — а кто несет ответственность за действия системы, если она ошиблась? Как трактовать решение ИИ, если оно привело к блокировке бизнеса или допустило утечку данных?

Пока эти вопросы остаются в серой зоне, но их надо решать. В ближайшие годы, по мнению экспертов, для обеспечения решений таких вопросов появятся новые инструменты:

- четкие нормы аудита ИИ-решений в ИБ (в том числе в рамках ФСТЭК России и Центра мониторинга угроз);
- обязательные требования к прозрачности принятия решений (explainable AI);
- протоколы «вмешательства человека» при возникновении неоднозначных инцидентов.

Подобные инициативы уже начинают обсуждаться на уровне регуляторов и в этом процессе особенно важно участие профессионального сообщества.

ОБУЧЕНИЕ ПРОТИВОСТОЯНИЮ: ЧЕЛОВЕК КАК СЛАБОЕ ЗВЕНО

ИИ — мощный инструмент, но в руках неподготовленного пользователя он бесполезен, поэтому человек остается самой уязвимой частью системы.

Важно не только использовать ИИ для защиты, но и обучать специалистов и граждан его возможностям и ограничениям:

- регулярные тренировки и симуляции фишинговых атак;
- разбор реальных кейсов с deepfake;
- использование ИИ-помощников для повышения осведомленности о киберугрозах.

РОССИЙСКИЙ ВЕКТОР: ИИ КАК ДРАЙВЕР СУВЕРЕННОСТИ

В условиях санкционного давления и стремительного ухода иностранных вендоров российский ИИ в кибербезопасности перестал быть «запасным

[4] Отчет Bugcrowd «Inside the Mind of a Hacker 2024» [Электронный доступ]. URL: *https://www.bugcrowd.com/press-release/bugcrowd-report-71-of-hackers-believe-ai-technologies-increase-the-value-of-hacking-compared-to-only-21-in-2023/*

[5] Статья 7 лучших инструментов и методов обнаружения дипфейков (август 2025) [Электронный ресурс]. URL: *https://www.unite.ai/ru/best-deepfake-detector-tools-and-techniques/*

вариантом». Это уже флагман. Интеграция собственных моделей в продукты, развитие обучающих датасетов, создание центров компетенций — все это идет параллельно с реальным внедрением.

Пример — в продукте «Гарда NDR» ИИ используется для анализа сетевого трафика и определения аномалий, что позволяет точно и быстро находить подозрительные действия и останавливать злоумышленников на раннем этапе атаки.

ВЗГЛЯД В БУДУЩЕЕ: ИИ КАК СТРАТЕГИЧЕСКИЙ ЭЛЕМЕНТ КИБЕРСУВЕРЕНИТЕТА

По всему миру 44% организаций используют машинное обучение для борьбы с кибератаками. В России около половины компаний планируют внедрить интеллектуальные системы, а еще 40% хотят расширить их применение. Согласно прогнозу Gartner[6], шесть из десяти ключевых технологических трендов 2025 года напрямую связаны с ИИ. К таким трендам относится защита неструктурированных данных, которая становится критичной на фоне роста генеративных моделей: компании должны научиться классифицировать такие данные, контролировать доступ к ним и внедрять политики безопасного использования. Также в фокусе разработчиков и производителей решений снижение человеческого фактора через автоматизацию, интеллектуальный анализ поведения и системы реагирования на инциденты. Улучшается и мониторинг в гибридных и мультиоблачных средах: ИИ обеспечивает сквозную видимость и корреляцию событий. Отдельное внимание уделяется интеллектуальному выявлению рисков: от предиктивной аналитики до интеллектуальных систем обнаружения вторжений. Генеративный ИИ становится инструментом для автоматизации отчетности, упрощения представления данных и создания дашбордов. И, наконец, ИИ все глубже встраивается в бизнес-процессы: от разработки до соблюдения нормативных требований.

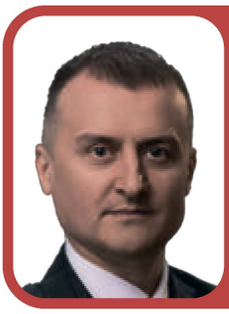
Результаты впечатляют. Некоторые NDR[7], XDR и SIEM-системы интегрированы с ML-технологиями[8], например, GigaChat. Благодаря этому, время реагирования на инциденты сократилось на 70%[9], точность анализа выросла на 30%, а операционные расходы снизились на 40%. Согласитесь, эти цифры говорят сами за себя.

До 2028 года рынок ИИ в кибербезопасности изменится, полагаем, кардинально:

- алгоритмы будут не просто реагировать, а действовать проактивно, например, изолируя узел в сети еще до начала атаки;
- генеративный ИИ будет использоваться для создания сценариев ответных действий, имитируя мышление опытного аналитика;
- расширится применение моделей «цифровых двойников» — для прогнозирования последствий инцидентов до их фактического наступления;
- будут проводиться киберучения с участием ИИ — когда обороняющаяся и атакующая стороны управляются нейросетями, обученными на реальных кейсах.

Важно понимать, в этой технологической гонке ИИ будет ни хорошим, ни плохим — все зависит от того, в чьих он руках, для каких целей применяется и какие задачи решает. И если мы хотим сохранить цифровой суверенитет страны, то должны научиться использовать ИИ как инструмент, а не бояться его как угрозу.

[6] Отчет Gartner Top 10 Strategic Technology Trends for 2025 [Электронный доступ]. URL: *https://www.gartner.com/en/articles/top-technology-trends-2025*
[7] NDR (англ. Network Detection and Response) — система сетевой безопасности, которая отслеживает трафик в корпоративной сети, анализирует его на наличие подозрительной активности и предоставляет инструменты для оперативного реагирования на инциденты.
[8] ML-технологии (от англ. machine learning, ML) — класс методов искусственного интеллекта, характерной чертой которых является не прямое решение задачи, а обучение за счет применения решений множества сходных задач. Позволяет компьютерным моделям обучаться без прямого программирования.
[9] Новость ИИ-ассистент GigaChat усилил российскую SIEM-систему Security Capsule [Электронный ресурс]. URL: *https://companies.rbc.ru/news/HQlGe4M23u/ii-assistent-gigachat-usilil-rossijskuyu-siem-sistemu-security-capsule/*



ЕВГЕНИЙ КРУГЛОВ
начальник отдела
региональных продаж
ООО Цитадель

АСПЕКТЫ ВНЕДРЕНИЯ ТС ОРМ У ХОСТИНГ-ПРОВАЙДЕРОВ

СТАТЬЯ ДОСТУПНА В ПЕЧАТНОЙ ВЕРСИИ ЖУРНАЛА



ДМИТРИЙ ХОМУТОВ
директор
ООО «Айдеко»

ДВАДЦАТЬ ЛЕТ ИННОВАЦИЙ: КАК IDECO МЕНЯЕТ ПОДХОД ENTERPRISE-КОМПАНИЙ К КИБЕРБЕЗОПАСНОСТИ

За 20 лет Ideco, пройдя путь от стартапа до лидера в корпоративной кибербезопасности, не только адаптировалась к быстро меняющемуся ландшафту угроз, но и определяет будущее защиты для Enterprise-сегмента[1], преобразуя подходы к цифровой безопасности. Вместе с директором Ideco Дмитрием Хомутовым разбираемся в перспективах российского рынка NGFW[2].

ПОЧЕМУ ENTERPRISE-КОМПАНИИ ПРЕДЪЯВЛЯЮТ ПОВЫШЕННЫЕ ТРЕБОВАНИЯ К NGFW СЕГОДНЯ

С каждым годом количество и уровень сложности кибератак на объекты государственного сектора и критической информационной инфраструктуры (КИИ) продолжают расти. В 2024 году на них пришлось 64% всех зафиксированных инцидентов, а 68% атак были высококритичными[3], что на 10% больше по сравнению с предыдущим годом. Эти данные подчеркивают, насколько важна защита объектов КИИ и государственной инфраструктуры.

Промышленность оказалась самой уязвимой отраслью, на которую пришлось 31% всех атак и 28% высококритичных[3] инцидентов. С увеличением применения искусственного интеллекта для реализации атак, киберугрозы будут только усложняться. Ожидается, что в 2026 году более 80% атак[4] будут использовать искусственный интеллект (ИИ), что приведет к повышению их эффективности и автоматизации.

В 2025 году тенденция повышенности степени угроз на госсектор и объекты КИИ сохраняется, и новые виды кибератак появляются с ускоренной скоростью. При этом объекты КИИ остаются приоритетной целью для хакеров. Значительная часть атак приходится именно на промышленную инфраструктуру, где высокая степень автоматизации и подключенные устройства создают многочисленные уязвимости. Это дает хакерам дополнительные возможности для эксплуатации слабых мест в защите инфраструктуры предприятий. Поэтому безопасность объектов КИИ, включая государственные и промышленные объекты, должна быть приоритетом в контексте современных киберугроз.

Ответом на эти угрозы стали новые решения в области информационной безопасности, которые стремятся повысить уровень защиты объектов КИИ. В частности, внедрение технологий NGFW, системы защиты от DNS-атак и шифрования данных помогают существенно улучшить безопасность периметра госсектора и объектов критической важности и предотвратить утечки информации. Применение таких технологий делает объекты КИИ более защищенными от внешних и внутренних угроз.

Межсетевой экран — неотъемлемый компонент комплексной системы безопасности сети. Корректная настройка и использование межсетевого экрана обеспечивают надежную защиту от взломов и утечек данных, гарантируя сохранность информации и соответствие требованиям регуляторов. Растущее осознание важности кибербезопасности в России, отраженное в национальной статистике и исследованиях, поддерживает спрос и дальнейшее развитие технологий межсетевого экранирования.

Основная задача NGFW экрана — обеспечение безопасности компьютерных сетей или отдельных узлов путем предотвращения несанкционированного доступа. Выполняя роль фильтра, он анализирует сетевые пакеты и блокирует те, которые не соответствуют заданным правилам безопасности. Более того, аналитики из Центра стратегических исследований (ЦСР) прогнозируют[5], что к 2027 году доля российских производителей на рынке кибербезопасности Российской Федерации достигнет 531 млрд рублей. Этот рост стимулируется указом Президента Российской Федерации № 250 «О дополнительных мерах по обеспечению информационной безопасности Российской Федерации», который меняет подход к кибербезопасности на ключевых российских предприятиях и в государственных структурах. Указ возлагает ответственность за обеспечение информационной безопасности на заместителей руководителей организаций и устанавливает личную ответственность руководителей компаний.

[1] Enterprise-сегмент – это крупные компании и организации, которым нужны сложные и масштабируемые решения для бизнеса.
[2] NGFW – это комплексное решение для защиты сети, которое объединяет традиционные функции брандмауэра с расширенными возможностями по контролю трафика и предотвращению угроз.
[3] [Электронный доступ]. URL: *https://clck.ru/3PG72s*
[4] [Электронный доступ]. URL: *https://www.apn.ru/index.php?newsid=47766*
[5] [Электронный доступ]. URL: *https://www.csr.ru/ru/research/prognoz-razvitiya-rynka-kiberbezopasnosti-v-rossiyskoy-federatsii-na-2023-2027-gody/*

Таким образом, несмотря на развитие технологий информационной безопасности, растущее количество и сложность кибератак на госсектор и КИИ требуют постоянного совершенствования мер защиты. Внедрение новых решений и технологий, а также переход на отечественные разработки, являются ключевыми шагами в обеспечении надежности и безопасности критической инфраструктуры.

ЧТО ПОД КАПОТОМ NGFW

NGFW перестал быть просто «межсетевым экраном», это сложный программно-аппаратный комплекс, и его архитектура напрямую влияет на эффективность защиты. Современные NGFW строятся на модульном фундаменте, где каждый компонент развивается независимо, обеспечивая гибкость и масштабируемость, необходимые для защиты разветвленных корпоративных сетей.

Такой подход требует многоуровневой фильтрации, выходящей за рамки простого анализа пакетов. Речь идет о глубокой инспекции трафика, анализе прикладного уровня и, что особенно важно, инспекции зашифрованного трафика, чтобы предотвратить проникновение угроз, скрытых в безопасных на первый взгляд соединениях. Архитектура безопасности должна быть встроена в само «ДНК» NGFW, обеспечивая интеграцию с SIEM-системами[6], поддержку Zero Trust[7] и автоматизацию реагирования на инциденты. И, конечно, современный NGFW обязан органично вписываться в гибридную инфраструктуру, будь то локальные сети, облачные среды или их комбинация.

В силу своей сложности, NGFW требует серьезного подхода к разработке. Строгое применение SDL[8] становится критически важным. SDL начинается с тщательного анализа требований безопасности, формализации угроз и определения зон риска. На этапе проектирования, NGFW должен создаваться с *security by design*[9] – с самого начала закладываются принципы многоуровневой защиты. И, наконец, постоянная обратная связь от пользователей и эффективный инцидент-менеджмент позволяют быстро исправлять уязвимости и реагировать на реальные угрозы. Базы сигнатур постоянно пополняются новыми записями о вредоносных паттернах, эксплойтах и объектах, создавая постоянно обновляемый щит. Механизмы автоматического обновления обеспечивают оперативную доставку этих сигнатур на все инсталляции, позволяя реагировать даже на самые свежие, нулевые угрозы. Однако, современный NGFW не ограничивается простым сопоставлением с известными сигнатурами. Интеллектуальные системы анализа, использующие эвристики и машинное обучение, способны выявлять ранее неизвестные угрозы, не попадающие под формальные описания.

В том числе NGFW с IPS[10] больше не является обособленным модулем, а представляет собой интегрированную часть общей архитектуры безопасности. Глубокая инспекция пакетов DPI[11] анализирует не только заголовки, но и содержимое пакетов на всех ключевых уровнях, выявляя подозрительные активности. Корреляция событий позволяет обнаруживать сложные, скоординированные атаки (например, APT[12]), формируя контекстную картину для автоматического реагирования на угрозы. Самообучающиеся политики, основанные на поведенческом анализе, позволяют IPS самостоятельно адаптироваться к новым типам атак и минимизировать количество ложных срабатываний.

20 ЛЕТ, ЗАЩИЩАЯ БИЗНЕС.
ЮБИЛЕЙ IDECO В СФЕРЕ КИБЕРБЕЗОПАСНОСТИ

Компания Ideco, основанная в 2005 году выпускниками Уральского федерального университета, прошла путь от стартапа до признанного игрока на рынке NGFW и UTM-решений[13].

В фокусе Ideco всегда были решения актуальных задач, стоящих перед корпоративными заказчиками. Ключевым этапом стало создание Ideco ICS, обеспечивающего контроль и фильтрацию трафика. Получение сертификата ФСТЭК России в 2021 году подтвердило[14] соответствие продукта высоким стандартам безопасности и позволило Ideco занять прочные позиции в сегменте сертифицированных решений.

Сейчас компания ориентирована на разработку инновационных и надежных продуктов в сфере цифровой безопасности, адаптированных к потребностям российского enterprise рынка. Флагманский продукт, Ideco NGFW, предлагает широкий

[6] SIEM-система – это комплексное решение в сфере информационной безопасности, предназначенное для централизованного сбора, анализа и реагирования на события безопасности в ИТ-инфраструктуре организации.
[7] Zero Trust (нулевое доверие) – это модель кибербезопасности, основанная на принципе «никогда не доверяй, всегда проверяй». Вместо доверия к пользователям и устройствам, находящимся внутри или вне сети, Zero Trust требует строгой верификации каждого запроса на доступ к ресурсам, независимо от его местоположения.
[8] SDL – жизненный цикл разработки программного обеспечения.
[9] *security by design* – это принцип архитектуры безопасности, гарантирующий, что системы и возможности разработаны с учётом их фундаментальной безопасности.
[10] IPS – это программно-аппаратные комплексы сетевой безопасности, которые в режиме реального времени обнаруживают и блокируют несанкционированную активность, вредоносные атаки и нарушения безопасности.
[11] DPI – это технология глубокой инспекции пакетов, которая позволяет анализировать содержимое сетевых пакетов данных для их классификации, фильтрации, мониторинга и регулирования трафика.
[12] APT-атака – это долговременная атака с использованием изощренных технологий взлома, в результате которой хакеры получают доступ к системе компании.
[13] UTM-решения – это аппаратные или программные устройства безопасности, объединяющие несколько функций защиты сети (антивирус, брандмауэр, антиспам, VPN, веб-фильтрация, IDS/IPS) в одном устройстве.
[14] [Электронный доступ]. URL: *https://ideco.ru/sobytiya/tpost/a46otkmgk1-ideco-utm-poluchil-sertifikat-sootvetstv*

спектр функциональных возможностей, включая обнаружение и предотвращение хакерских вторжений, и базируется на глубокой экспертизе в области сетевой безопасности.

Ideco продолжает инвестировать в развитие продуктов, интегрируя передовые технологии для повышения эффективности защиты от современных угроз. Компания стремится обеспечить клиентам комплексную защиту, позволяющую эффективно противодействовать постоянно меняющемуся ландшафту киберугроз.

NGFW NOVUM: БУДУЩЕЕ КОРПОРАТИВНОЙ ЗАЩИТЫ НАЧИНАЕТСЯ СЕГОДНЯ

Ideco NGFW Novum — это решение нового поколения для построения масштабируемой и надёжной сетевой безопасности. Благодаря микросервисной архитектуре, собственной реализации сетевого стека на базе VPP[15] и фильтрации трафика на скоростях до 200 Гбит/с, Ideco NGFW Novum обеспечивает гибкость, производительность и отказоустойчивость, соответствующие требованиям современных ИТ-ландшафтов.

В отличие от устаревших NGFW-продуктов, Ideco NGFW Novum предлагает не просто фильтрацию трафика, а комплексную платформу безопасности с поддержкой DPI, WAF[16], IPS/IDS, ZTNA[17], инспекцией TLS 1.3[18] и централизованным управлением через Ideco Center. Решение легко встраивается в существующую инфраструктуру, поддерживает отказоустойчивые кластеры и полностью соответствует российским регуляторным требованиям.

Ideco обеспечивает заказчику полную **прозрачность и контроль над сетевой активностью и действиями администраторов** благодаря централизованному журналированию событий NGFW, настраиваемым панелям мониторинга в реальном времени, детальному анализу трафика, визуализации загруженности ресурсов и экспорту данных во внешние SIEM-системы (Zabbix, ELK, Graylog, Splunk и др.). NGFW Novum также предоставляет инструменты аудита административных действий и политик безопасности, разграничение прав доступа и конструктор отчетов, которые централизованно управляются через Ideco Center, упрощая выполнение политик безопасности, ускоряя расследование инцидентов и повышая готовность к аудиту.

Novum обеспечивает контроль и защиту пользовательских сессий в терминальных серверах и VDI[19], позволяя применять индивидуальные политики безопасности к каждой сессии, предотвращая несанкционированный доступ, благодаря поддержке многопользовательских сессий с динамическим разделением, привязке политик безопасности (контроль доступа, контент-фильтр, приложения, антивирус, межсетевой экран), контент-фильтрации и инспекции зашифрованного трафика (TLS/SSL), централизованному аудиту и журналированию, что делает его идеальным решением для защиты данных и контроля доступа, особенно при работе с подрядчиками и в распределенных инфраструктурах, снижая риски утечек и обеспечивая удобное масштабирование.

Также это централизованное решение **для контроля веб-доступа** сотрудников, блокирующее нежелательный и вредоносный контент с помощью прозрачного и явного прокси-сервера, контент-фильтра с более чем 70 категориями, инспекции HTTPS-трафика (SSL-Interception/TLS 1.3), интеграции с антивирусом и антиспам-фильтрами, контроля приложений (L7 DPI) и гибких политик доступа, что позволяет соблюдать корпоративные политики безопасности, повышать производительность и вести детальное журналирование посещений с возможностью экспорта данных в SIEM и SkyDNS для дополнительной фильтрации.

В условиях всё более изощренных кибератак, когда даже незначительная брешь может обернуться катастрофическими последствиями, NGFW Novum становится незаменимым щитом для вашей сети, обеспечивая **первую линию обороны против взломов, вредоносного трафика, DDoS-атак** и других современных угроз, включая фишинг и эксплойты, а также эффективно предотвращая их распространение внутри инфраструктуры благодаря высокопроизводительному сетевому стеку, L7 DPI, IDS/IPS Suricata с базами Kaspersky, веб-антивирусу, контент-фильтру, DNS Security с интеграцией SkyDNS и WAF, что позволяет не только отражать атаки, но и проактивно выявлять потенциальные уязвимости, гарантируя надежную защиту данных и непрерывность бизнес-процессов.

IDECO NGFW NOVUM — ОТВЕТ НА ЗАПРОСЫ КРУПНОГО БИЗНЕСА

Ideco NGFW Novum создавался для компаний, которые нуждаются не в очередной «чёрной коробке», а в инструменте, который можно контролировать, адаптировать и масштабировать. Система не требует отдельного SOC[20] или штатных специалистов по информационной безопасности — достаточно базовых компетенций ИТ-отдела. При этом компания-заказчик получает глубокую интеграцию с SIEM, DLP, AD и другими сервисами, прозрачную политику лицензирования и поддержку на всех этапах — от пилота до промышленной эксплуатации.

[15] VPP (платформа векторной обработки пакетов) – расширяемая платформа, которая обеспечивает готовые функциональные возможности коммутатора или маршрутизатора. Это высокопроизводительный стек обработки пакетов, который может работать на обычных процессорах.
[16] WAF – это межсетевой экран для веб-приложений, который фильтрует и анализирует HTTP/HTTPS-трафик, чтобы выявлять и блокировать вредоносные запросы и защищать веб-приложения от различных киберугроз
[17] Zero Trust Network Access (ZTNA) – это технология, которая предоставляет безопасный доступ к корпоративным приложениям и сервисам на основе строгой аутентификации и авторизации, без необходимости доступа к всей корпоративной сети.
[18] Инспекция TLS 1.3 – это функция сетевой безопасности, позволяющая просматривать и анализировать трафик, зашифрованный с помощью протокола TLS версии 1.3, несмотря на его сильное шифрование.
[19] VDI – это технология, которая размещает операционные системы и приложения на центральном сервере, а не на физическом устройстве пользователя.
[20] SOC – это централизованная функция или группа, ответственная за улучшение состояния кибербезопасности организации, а также за предотвращение, обнаружение и реагирование на угрозы.



ЕВГЕНИЙ ГЕНГРИНОВИЧ
советник генерального директора
АО «ИнфоТеКС»

КИБЕРУСТОЙЧИВОСТЬ ЭНЕРГЕТИКИ: СТРАТЕГИЯ И КАДРЫ

В контексте цифровой трансформации автоматизированных систем управления технологическими процессами (АСУ ТП) все чаще наряду с информационной безопасностью (ИБ) обсуждается тема киберустойчивости[1]. Этот аспект актуален для всех отраслей, которые отнесены к критической инфраструктуре. Многие предприятия в значительной степени зависят от цифровых систем управления, что приводит к слиянию ИТ-инфраструктуры с АСУ и АСУ ТП. Это способствует росту производительности и снижению влияния человеческого фактора, что, в свою очередь, повышает эффективность бизнеса. Но одновременно появляются новые угрозы – кибератаки и инциденты, которых ранее не существовало.

ПОИСК БАЛАНСА: ГДЕ ПРОХОДИТ ГРАНИЦА МЕЖДУ БЕЗОПАСНОСТЬЮ И ЭФФЕКТИВНОСТЬЮ

В современных условиях компаниям приходится балансировать между двумя важными группами требований. Первые касаются аспектов, от которых напрямую зависит безопасность людей, окружающей среды и, в отдельных случаях, даже национальной инфраструктуры. Это зона, где компромиссы недопустимы: соблюдение всех предписаний строго контролируется надзорными органами.

Вторая категория требований отражает интересы самой компании. Речь идет про эффективность бизнес-процессов, прибыльность и устойчивость к внутренним и внешним рискам. Здесь важна точность оценки: если затраты на безопасность начинают превышать реальные угрозы, бизнес может столкнуться с падением рентабельности.

Эти два подхода не противоречат друг другу – напротив, они дополняют систему управления. Формальное соответствие нормативам позволяет пройти проверки и избежать санкций, но этого недостаточно. Без перехода к риск-ориентированному управлению компания может потерять контроль над критическими процессами. Один из тревожных сигналов – когда ИТ-инфраструктура становится непрозрачной для управленцев, а влияние киберугроз на производственные и финансовые показатели перестает быть очевидным. На практике речь идет не о бесконечных инвестициях в обеспечение ИБ, а о взвешенном анализе рисков и поиске оптимального решения.

Нередко можно услышать: «Сначала запустим систему, а потом пригласим специалистов по ИБ – пусть обеспечивают защиту». Такой подход оборачивается высокой стоимостью и низкой эффективностью. Внешний эксперт не сможет в большинстве случаев адаптировать технологический процесс к устойчивости – кибербезопасность должна быть учтена еще на этапе проектирования.

Цифровая трансформация порождает любопытный парадокс: с одной стороны, цифровизация действительно усиливает безопасность производства – операторы могут управлять процессами дистанционно, не подвергаясь риску в опасных зонах, а с другой – она открывает принципиально новые уязвимости. Преодолеть это противоречие можно только с помощью системного подхода. Устойчивость достигается путем проектирования системы таким образом, чтобы отказы были разделены. Если одна функция выходит из строя, это не должно приводить к отказу других функций, и в проекте должны быть альтернативные способы выполнения отказавшей функции, которые можно вызвать автоматически, немедленно и надежно. Добавляется физическая или логическая избыточность для элементов и взаимосвязей, что обеспечивает переходы к альтернативным элементам и соединениям при необходимости. Тестирование должно проводиться для нормальных и ненормальных сценариев и изучаться на предмет того, может ли злоумышленник намеренно нарушить комбинацию компонентов. Программное обеспечение также должно иметь возможность перехода на альтернативные функции, реализации, конфигурации, местоположения или сегменты сети, которые могут иметь другие слабые стороны, чтобы те же угрозы и опасности не были столь разрушительными для возможностей замены. Тогда меры защиты органично интегрируются в производственный процесс, а не накладываются позже, как дорогостоящая надстройка.

КАК ОБЕСПЕЧИТЬ КИБЕРУСТОЙЧИВОСТЬ В АСУ ТП

В отечественной практике пока нет единства в терминологии: «кибериммунные системы», «конструктивная безопасность», «киберустойчивые решения» – эти понятия используются параллельно, но общепринятого стандарта не существует. Это порождает неоднозначности и затрудняет формирование четких и универсальных требований.

[1] Киберустойчивость – это способность системы поддерживать приемлемый уровень обслуживания в условиях информационных воздействий.

Примечательно, что в аппаратной части прогресс заметен гораздо сильнее. Разработчики АСУ ТП давно учитывают физические аспекты защиты: от использования экранированных корпусов до соблюдения температурных норм и ограничений физического доступа к узлам. Однако в области обеспечения киберустойчивости микропроцессоров и программного обеспечения, по-прежнему сохраняется серьезный пробел – как в технической компетенции разработчиков, так и в формулировке задач со стороны заказчиков.

Основная трудность заключается в разрыве взаимодействия между регулятором, заказчиком и производителем. Пока нормативные документы прямо не предписывают включать киберустойчивость в проектные фазы, изменения будут идти медленно. Тем не менее, позитивные сдвиги уже происходят. Производители, ориентированные на долгосрочную работу в отрасли, начинают добровольно внедрять принципы безопасной разработки, включая сертифицированные средства криптографической защиты в архитектуру устройств. Постепенно меняется и подход заказчиков: все чаще инвестиции в киберустойчивость воспринимаются не как излишние расходы, а как необходимый инструмент повышения надежности и снижения эксплуатационных издержек.

Этот процесс можно сравнить со сборкой сложного механизма: сначала необходимо понять функции каждой детали, затем установить каждую из них на свое место. Сегодня отрасль как раз проходит стадию осмысления. Пусть темпы пока отстают от вызовов времени, но направление очевидно: будущее за системным подходом, в котором устойчивость, защищенность и безопасность закладывается в проект, а не добавляется в последнюю очередь.

ФОРМИРОВАНИЕ НОВОЙ КОРПОРАТИВНОЙ КУЛЬТУРЫ КАК СПОСОБ НАУЧИТЬ ЭНЕРГЕТИКОВ ОСНОВАМ ИБ

Регуляторные нормы, касающиеся безопасности и надежности эксплуатации, продолжают развиваться. Однако им пока недостает четких положений, отражающих цифровую специфику. Кроме того, непосредственно на объектах эксплуатации часто наблюдается нехватка экспертизы: специалисты-технологи не всегда обладают достаточными знаниями в области современных ИТ-систем.

Для преодоления данной проблемы необходимо начать формирование новой корпоративной культуры, в которой станет аксиомой: инженер-технолог, не обладающий базовыми знаниями в сфере ИТ и ИБ, оказывается неэффективным звеном, неспособным обеспечить надежную эксплуатацию современных цифровых решений. На этапе перехода, пока вузы еще не выпускают специалистов с такими компетенциями в должном объеме, оптимальным решением должно стать – создание эксплуатационных подразделений нового формата. В них будут работать ИТ и ИБ-специалисты совместно с технологами, которые понимают тонкости производственных процессов.

Стоит также развеять распространенное заблуждение, будто современный инженер-технолог не в состоянии дополнительно осваивать вопросы ИТ и ИБ из-за высокой нагрузки. В действительности, в цифровой инфраструктуре таких специалистов потребуется немного – на уровне крупной корпорации достаточно команды из 4-5 человек. Основную работу в процессе эксплуатации смогут выполнять технологи со среднеспециальным образованием, используя готовые решения, без необходимости глубокого технического понимания, подобно тому, как мы ежедневно пользуемся смартфонами, не вникая в их внутреннее устройство.

С развитием централизованных платформ для управления и обеспечения безопасности, появлением цифровых двойников и киберполигонов, станет возможным оперативно анализировать причины сбоев и устранять их с помощью удаленных подключений или действий специалистов на местах. А в перспективе следующего технологического этапа таких исполнителей все чаще будут заменять автоматизированные системы и роботы.

Для наглядности представим типовое устройство в составе АСУ ТП. При его разработке инженеры могли бы использовать минимально соответствующую слабую микросхему и простой пластиковый корпус. Но они выбирают защищенную оболочку, устойчивую к электромагнитным помехам, и мощный чип, способный выдерживать перегрузки, например, при скачке напряжения или ударе молнии. То есть закладываются элементы, повышающие надежность. Такой же принцип должен применяться и к информационным системам: как производители, так и заказчики должны осознавать, что без защиты от киберугроз достичь требуемого уровня устойчивости и безопасности практически невозможно.

ГДЕ ГОТОВЯТ СПЕЦИАЛИСТОВ ПО РАЗРАБОТКЕ ЗАЩИЩЕННЫХ ИНТЕЛЛЕКТУАЛЬНЫХ СИСТЕМ УЧЕТА ЭЛЕКТРОЭНЕРГИИ

Электроэнергетическая отрасль переживает масштабные изменения, требующие переосмысления подходов к подготовке специалистов. Сегодня одного лишь профильного образования в энергетике уже недостаточно – требуется понимание сетевых технологий и основ кибербезопасности. Компания «ИнфоТеКС»[2] совместно с Центром НТИ МЭИ[3] подготовили специальный учебный курс «Введение в разработку защищенных Интеллектуальных систем учета электроэнергии (ИСУЭ) и АСУ ТП с

[2] [Электронный ресурс]. URL: *https://infotecs.ru/*
[3] [Электронный ресурс]. URL: *http://nti.mpei.ru/*

использованием ViPNet SIES»[4], который объединяет накопленный опыт в области криптографической защиты информации и создания отечественных программно-аппаратных комплексов для обеспечения кибербезопасности объектов электроэнергетики. Курс проходит на базе НИУ МЭИ.

Курс имеет глубокую практическую направленность, при освоении курса слушатели учатся развертывать инфраструктуру решения ViPNet SIES[5], встраивать криптографический модуль ViPNet SIES Core[6] в устройства нижнего уровня ИСУЭ и АСУ ТП, интегрировать программный комплекс ViPNet SIES Unit[7] с системами верхнего уровня ИСУЭ и АСУ ТП, обеспечивать реализацию резервированной защищенной связи между устройствами верхнего и нижнего уровня, а также удаленно управлять и обслуживать встроенные средства криптографической защиты информации.

Действующие разработчики устройств и программного обеспечения компаний-производителей систем промышленной автоматизации, систем коммерческого учета электроэнергии, систем релейной защиты и противоаварийной автоматики – все они реальные и потенциальные слушатели курса.

КАДРОВАЯ ПОЛИТИКА В НОВЫХ УСЛОВИЯХ: ВЫЗОВЫ И ПЕРСПЕКТИВЫ

Обучение специалистов – лишь часть общей задачи подготовки кадров. Куда сложнее оказывается их включение в действующую эксплуатационную систему у заказчика. Молодые выпускники с современными, комплексными знаниями нередко сталкиваются с недопониманием и недооценкой со стороны работодателей. В результате складывается парадокс: отрасль остро нуждается в компетентных кадрах, но при этом подготовленные профессионалы часто остаются невостребованными.

Чтобы преодолеть этот разрыв, необходим комплексный подход. Крупным энергокомпаниям целесообразно формировать центры компетенций – небольшие, но квалифицированные команды из 10-15 человек, работающие на стыке энергетики, ИТ и ИБ. В то же время на местах достаточно технического персонала с базовой подготовкой. Для достижения требуемого результата ключевым моментом становится необходимость трансформации самой корпоративной культуры – от методов эксплуатации до системы мотивации. Цифровизация требует не только новых технологий, но и новой философии управления кадрами. Без этого даже самые передовые решения останутся нереализованными.

Особенно обидны случаи, когда подготовленный для работы в области электроэнергетики инженер по релейной защите, освоивший ИТ и ИБ, вынужден уходить в банковскую или другую отрасль. Между тем общение с магистрами НИУ «МЭИ», защитившими работы на пересечении цифровизации и надежности энергосистем, показывает: перед нами действительно уникальные кадры. Их ценность в том, что они одинаково хорошо разбираются как в технических процессах, так и в цифровых технологиях.

Самое важное – донести до молодых специалистов, насколько перспективен этот путь. Ведь именно они в будущем будут определять цифровую архитектуру критически важных секторов экономики.

ПРЕДЛАГАЕМЫЕ ПУТИ РЕШЕНИЯ

Зрелая культура обеспечения киберустойчивости энергокомпаний, полагаем, должна включать:

- Принятие решений с учетом рисков на этапе внесения изменений, а не только после их внедрения.
- Обучение инженеров оценке уровня киберустойчивости во время ввода в эксплуатацию, закупок и запросов на изменение.
- Совместную ответственность специалистов ИТ, ИБ, АСУ/АСУТП и технологами, при этом киберустойчивость должна рассматривается как условие утверждения проекта и подтверждения эксплуатационной готовности.

Например, процессы ввода в эксплуатацию будут включать вопросы киберустойчивости в качестве стандартной практики:

- Как эта новая система подключается к сети?
- Кто управляет логическим доступом после развертывания?
- Какие меры безопасности предусмотрены для доступа поставщика?
- Поддаются ли все точки удаленного доступа аудиту и контролю?

Эти вопросы не теоретические; они отражают реальные точки входа для злоумышленников и должны стать частью повседневных инженерных решений.

В процедурах проектирования и закупок необходимо сформировать практику контроля:

- наличия программы и методики испытаний на киберустойчивость от поставщиков;
- проведения испытаний на виртуальных моделях, симулирующих реальную инфраструктуру;
- представления периодичности и методики проведения плановых проверок, включающих корректировки программного обеспечения, проверку учетных данных и аудит журнала доступа;
- оценки киберустойчивости и её соответствия нормам в качестве предварительного условия для ввода – запуска в эксплуатацию.

[4] [Электронный доступ]. URL: *http://nti.mpei.ru/course-vipnetsies/*
[5] [Электронный доступ]. URL: *https://infotecs.ru/solutions/zashchita-isue/*
[6] [Электронный доступ]. URL: *https://infotecs.ru/products/vipnet-sies-core/*
[7] [Электронный доступ]. URL: *https://infotecs.ru/products/vipnet-sies-unit/*

При практической интеграции в инженерные рабочие процессы организациям следует предусматривать приведение в соответствие существующих эксплуатационных процессов с новым цифровым окружением. Многие инженерные рабочие процессы уже включают в себя этапы обеспечения безопасности, качества и соответствия. Поддержка киберустойчивости может быть внедрена путем целенаправленных, высокоэффективных изменений, включая оценку киберустойчивости существующих процессов.

ФОРМИРОВАНИЕ КОРПОРАТИВНОЙ КУЛЬТУРЫ

Корпоративная культура формируется посредством повторения, прозрачности и закрепления. Руководители по безопасности давно осознали важность регулярных процедур – инструктажей на рабочем месте, производственных обходов и коротких собраний по безопасности, которые внедрили важность управления рисками в повседневную работу.

Эти подходы помогают развить чувство сопричастности и необходимости личного вклада к достижению поставленных задач у сотрудников и укрепить идею о том, что кибербезопасность, как и устойчивость, является ответственностью каждого.

Для поддержания культурных изменений требуются практические инструменты, которые закрепляют желаемое поведение. Вместо строительства новых систем с нуля, организации могут адаптировать существующие ресурсы и процессы, с учетом нового цифрового окружения.

Необходимо добавить тему киберустойчивости в стандартные программы обучения в вузах, колледжах, при переподготовке и повышении квалификации специалистов, а также при инструктажах на предприятиях и в организациях. Следует также разработать и внедрить в энергокомпаниях панели мониторинга для отслеживания ключевых показателей уровня киберустойчивости (например, количество активов с проверенными контролями доступа, процент систем с обновленной прошивкой), создать рабочие инструкции по обеспечению киберустойчивости, которые помогут инженерам выявлять распространённые уязвимости (например, открытые порты, пароли по умолчанию, неуправляемый удалённый доступ).

Простые, последовательные подсказки в нужных местах помогают командам формировать привычки, а привычки стимулируют изменения в корпоративной культуре эксплуатации.

ЗАКЛЮЧЕНИЕ

Цифровая трансформация индустрии, безусловно, значительно повысит ее эффективность и безопасность. Цифровые решения обеспечат сокращения сроков смены технологических циклов. Но необходимо проявлять осторожность, должную предусмотрительность и мудрость, чтобы гарантировать, что технологические достижения в конечном итоге не обойдутся нам слишком дорого. Существует ограниченный период — окно возможностей — когда мы можем разработать целостную концепцию безопасности, которая будет базироваться на киберустойчивых устройствах и решениях, реализует безопасную связь между конечными точками и обеспечит управление киберустойчивостью и ее мониторинг. Этому должны способствовать культурные стимулы, структурные изменения зон ответственности, прозрачность принятия решений руководством и постоянное повышение квалификации специалистов на соответствующих курсах и при работе на местах.

Интеграция цифровых решений в существующие рабочие процессы, электронные реестры, закупки, ввод в эксплуатацию и обслуживание, гарантируют, что киберустойчивость станет частью повседневной деятельности.



СЕРГЕЙ ФОМИН
начальник отдела информационной безопасности управления информационной безопасности и связи
Минцифры Кузбасса



АЛЕКСАНДР ФЕФИЛОВ
руководитель учебно-методического направления
АО «Перспективный мониторинг»

РЕГИОНАЛЬНЫЙ КИБЕРПОЛИГОН КАК ИННОВАЦИОННЫЙ ИНСТРУМЕНТ ПОДГОТОВКИ КАДРОВ

Сфера информационной безопасности испытывает острый дефицит кадров. Согласно исследованию Центра стратегических разработок «Северо-Запад», представленному на Петербургском международном экономическом форуме – ПМЭФ-2024, в 2023 году потребность рынка труда в специалистах информационной безопасности (ИБ) составляла 150 тысяч человек при уровне дефицита в 50 тысяч специалистов. Согласно прогнозам, к 2027 году совокупная потребность российского рынка в специалистах в сфере информационной безопасности может достичь 260 тысяч человек. Увеличение масштабов подготовки кадров и внедрение автоматизированных решений позволят удовлетворить значительную часть этого спроса. Тем не менее, ожидаемая занятость в отрасли составит максимум 200 тысяч человек, то есть на четверть меньше, чем требуется рынку.

Кроме того, остается актуальной проблема оттока молодых специалистов из регионов. Для решения этой задачи предпринимается ряд шагов как со стороны государства, так и со стороны бизнеса и образовательных учреждений. Так, Минобрнауки России в 2024/2025 учебном году выделило региональным университетам больше бюджетных мест. С 2025 года реализуется национальный проект «Экономика данных и цифровая трансформация государства», в рамках которого предусмотрена программа «Кадры для цифровой трансформации», включающая шаги по развитию цифровой грамотности: обучение школьников, студентов и профессионалов. Формируются новые образовательные программы, цель которых – подготовить топ-специалистов в сфере ИТ, которые смогут решать сложные задачи и быстро развиваться в профессии.

В целом система высшего и среднего образования ежегодно выпускает 10-15 тысяч новых специалистов ИБ. Однако рынку требуется узкая специализация, в связи с чем повышается актуальность дополнительного обучения и развития узконаправленных навыков выпускников, отвечающих современному динамичному ландшафту цифрового пространства.

Недостаток современных инструментов и технологий компенсируется интеграцией в учебный процесс интерактивных тренировочных платформ, которые могут помочь в работе преподавательского состава. Такой подход позволит специалистам получить необходимые профессиональные навыки и компетенции в процессе освоения специальности, а также повышать квалификацию специалистам в рамках обучения на курсах дополнительного профессионального образования. Так, для специалистов по информационной безопасности важным является практический навык защиты информационных систем от компьютерных атак, который требуется поддерживать на высоком уровне, в том числе за счет регулярных тренировок на учебном полигоне.

РЕГИОНАЛЬНЫЙ КИБЕРПОЛИГОН

В масштабах субъекта Российской Федерации кадровые задачи могут решаться комплексно: путем создания регионального киберполигона – платформы для практико-ориентированной подготовки специалистов по информационной безопасности, работающей на мощностях регионального министерства цифрового развития и связи. Для эффективного решения задач доступ к нему должны иметь все подразделения региональной администрации и образовательные учреждения региона.

В данной статье мы рассмотрим построение Регионального киберполигона Кемеровской области – Кузбасса[1] на основе программного комплекса Ampire[2] –

[1] Министерство цифрового развития и связи Кузбасса. Киберполигон [Электронный ресурс]. URL: *https://digital42.ru/deyatelnost/informatsionnye-sistemy-i-servisy/kuberpoligon.php*
[2] Киберполигон Ampire [Электронный ресурс]. — URL: *https://ampire.team/*

учебно-тренировочной платформы для отработки навыков обнаружения, анализа и устранения последствий компьютерных атак.

Идея такого проекта пришла «снизу»: в 2023 году вузы Кузбасса обратились к губернатору Кузбасса с просьбой: решить проблему недостатка практической подготовки специалистов по ИБ. Губернатор поддержал идею создания регионального киберполигона, выделил финансирование, и до конца 2023 года проект был успешно реализован.

В рамках методической подготовки проекта был выработан регламент подключения пользователей к региональному киберполигону, в соответствии с которым вся бюджетная сфера Кузбасса имеет возможность получить доступ к киберполигону. График киберучений Кузбасс может формировать самостоятельно, независимо от разработчика. Первыми пользователями регионального киберполигона стали органы государственной власти Кузбасса, Кузбасский государственный технический университет (КузГТУ), Кемеровский государственный университет (КемГУ), учебные заведения среднего общего и профессионального образования региона. Федеральное государственное казенное общеобразовательное учреждение «Кемеровское президентское кадетское училище» в Кузбассе – первое в России, имеющее доступ к киберполигону и возможность готовить специалистов с уклоном на кибербезопасность.

За год функционирования регионального киберполигона было проведено 193 тренировки, из которых 10 – для сотрудников органов государственной власти Кузбасса. За год киберучения прошли более 60 специалистов по информационной безопасности. Команда Кемеровского государственного университета стала двукратным чемпионом соревнований Ampire Trophy, опередив 29 команд других учебных заведений России **(Рис. 1)**. В июле 2025 года проект Министерства цифрового развития и связи Кемеровской области «Региональный киберполигон Кузбасса» был удостоен Кубка информационной безопасности регионов в номинации «За распространение знаний в сфере информационной безопасности» как способствующий развитию цифровой грамотности населения и распространению знаний в сфере информационной безопасности.

ОБРАЗОВАНИЕ ПО ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В ШКОЛАХ

Количественный и качественный рост кибератак требует расширения границ образования по информационной безопасности за пределы профильных направлений в вузах. Базовыми знаниями цифровой гигиены должны обладать работники без специальной подготовки, а начинать обучение



Рис 1. Награждение команды КемГУ на соревнованиях Ampire Trophy 24 апреля 2025 года

киберграмотности требуется еще на уровне школы, что также позволит увеличить количество абитуриентов в вузы и ссузы на специальности, связанные с информационной безопасностью.

Эту потребность также может удовлетворить киберполигон, который должен отвечать следующим требованиям:

1. Тренироваться на киберполигоне должно быть интересно.
2. Должны раскрываться детали работы в информационной безопасности.
3. Должна быть видимая польза от каждой тренировки прямо сейчас.
4. Киберполигон должен давать возможность почувствовать себя в профессии.

Киберполигон Ampire может использоваться для проведения практических уроков по цифровой грамотности в рамках школьной программы. Школьники на практике изучают основы безопасной работы с компьютерами и мобильными устройствами, учатся определять вредоносные действия и защищать себя от негативного воздействия, а персональные данные – от кражи. Такие уроки позволяют прививать базовые навыки работы с программным и аппаратным обеспечением.

Кроме того, в школах могут проводить внеурочные занятия для углубленного изучения информационной безопасности. На киберполигоне такие занятия могут проходить как очно, так и онлайн.

Важным аспектом просвещения в области цифровой грамотности являются олимпиады и соревнования по информационным технологиям и информационной безопасности в различных форматах. Соревновательный элемент способствует повышению мотивации и вовлеченности, а также снижению барьера вхождения в профессию. Такие соревновательные форматы занятий Ampire также поддерживает.

Однако отдельно взятая школа не всегда может позволить себе приобретение платформы. В такой ситуации проявляется еще одно достоинство регионального киберполигона – удаленный доступ к ресурсу. В Кузбассе все школы региона имеют возможность подключиться к программному комплексу, при этом персональные данные пользователей остаются в безопасности, так как платформа размещена внутри защищенного периметра Центра обработки данных информационных систем Кузбасса. Такой подход делает работу по повышению уровня цифровой грамотности населения региона системным, а занятия – регулярными. Методисты «Перспективного мониторинга» уже приступили к обучению педагогов региональных средних общеобразовательных школ работе с киберполигоном Ampire и его отдельным модулем для школьников Ampire Junior.

КИБЕРПОЛИГОН КАК РЕШЕНИЕ ПРОБЛЕМЫ НЕДОСТАТКА ПРАКТИЧЕСКОЙ ПОДГОТОВКИ СТУДЕНТОВ НАПРАВЛЕНИЙ, СВЯЗАННЫХ С ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТЬЮ

Тренировки на киберполигоне включаются в учебные программы университетов в качестве инструмента практической отработки полученных ранее теоретических знаний. Для того, чтобы удовлетворять потребностям учебного процесса, киберполигон должен содержать:

- актуальные практические задачи;
- методические материалы для преподавателей и обучаемых;
- задачи разного уровня сложности;
- средства моделирования киберугроз;
- современные средства защиты информации;
- подсистему взаимодействия между участниками;
- опции проведения индивидуальных и групповых занятий.

Киберполигон также должен позволять преподавателю самостоятельно готовить комплекс к занятию, организовывать непрерывный учебный процесс, защищать элементы комплекса от повреждений и самостоятельно развивать полигон.

Киберполигон Ampire позволяет проводить практические занятия на двойнике реальной инфраструктуры организации, поддерживает различные форматы обучения – образовательный, тренировочный, соревновательный. Обучение проходит на автоматизированных сценариях атак на основе реальных инцидентов, взятых из практики пентестеров[3] и экспертов центра мониторинга компьютерных атак компании «Перспективный мониторинг» (входит в ГК «ИнфоТеКС»). Такой подход преодолевает разрыв между теоретической подготовкой и практическими требованиями профессии, позволяет предоставить студентам доступ к реальной «боевой» работе, которая проходит в безопасной среде, при этом партнерам вуза – бизнесу и государственным организациям – не требуется предоставлять обучаемым доступ к своей инфраструктуре и средствам защиты информации.

Преподаватель может сам настроить все параметры тренировки: выбрать шаблон инфраструктуры, виртуальные машины с предустановленным ПО, содержащим определенные уязвимости, проложить путь злоумышленника, действиям которого должны будут

[3] Пентестер (от англ. *pentester*, специалист по *penetration testing* — «тестированию на проникновение») — эксперт по информационной безопасности, который исследует системы и сети, моделируя действия злоумышленников, чтобы выявить и оценить уязвимости до того, как ими смогут воспользоваться и нанести ущерб.

противостоять обучающиеся. Содержание, этапы и статистика киберучений во время их проведения содержатся на дашборде **(Рис. 2)**.

Киберполигон содержит шаблоны инфраструктуры, средства защиты информации, сценарии атак, а также конфигуратор собственных сценариев. Актуальность обеспечивают ежеквартальное обновление и наполнение платформы новыми уязвимыми узлами и сценариями. На сегодняшний день платформа содержит 58 готовых сценариев, 94 уязвимых узла, 320 уязвимостей и последствий. Ampire включает набор учебно-методических материалов, которые помогают обучаемым и преподавателям снизить порог входа. Все сценарии атак могут конфигурироваться преподавателем под различный уровень сложности. Этот принцип помогает преподавательскому составу применять тренировки на платформе в течение всего периода обучения, постепенно усложняя задания и помогая учащимся сразу применять получаемые знания на практике и переводить их из теории в умения и навыки.

Применение регионального киберполигона позволяет добавлять в учебный процесс соревновательную составляющую для стимулирования мотивации обучающихся. Региональные соревнования на киберполигоне между командами вузов и ссузов могут стать примером такой практики. Данные соревнования также могут стать точкой притяжения для представителей регионального бизнес-сообщества, находящихся в поисках молодых специалистов ИБ. Это позволит эффективно закрывать потребность в кадрах и удерживать молодых специалистов внутри региона.

КИБЕРПОЛИГОН ДЛЯ ПОВЫШЕНИЯ КВАЛИФИКАЦИИ ДЕЙСТВУЮЩИХ СПЕЦИАЛИСТОВ

Для построения эффективной защиты критической инфраструктуры региона важно постоянно повышать квалификацию сотрудников, отвечающих за информационную безопасность. Обязательность проведения практических тренировок со специалистами в сфере ИБ определена различными приказами и нормативно-правовыми актами. Так, например, Приказом ФСБ России №282 от 19 июня 2019г. «Об утверждении Порядка информирования ФСБ России о компьютерных инцидентах, реагирования на них, принятия мер по ликвидации последствий компьютерных атак, проведенных в отношении значимых объектов критической информационной инфраструктуры Российской Федерации» определено, что организации, имеющие значимые объекты критической информационной инфраструктуры (КИИ), должны организовывать и проводить тренировки по отработке мероприятий плана реагирования на компьютерные инциденты и принятия мер по ликвидации последствий компьютерных атак не реже одного раза в год. Приказы ФСТЭК России № 235 от 21 декабря 2017г. «Об утверждении Требований к созданию систем безопасности значимых объектов критической информационной инфраструктуры Российской Федерации и обеспечению их функционирования» и № 239 от 25 декабря 2017г. «Об утверждении Требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации» содержат нормы по информированию и обучению работников субъектов КИИ.

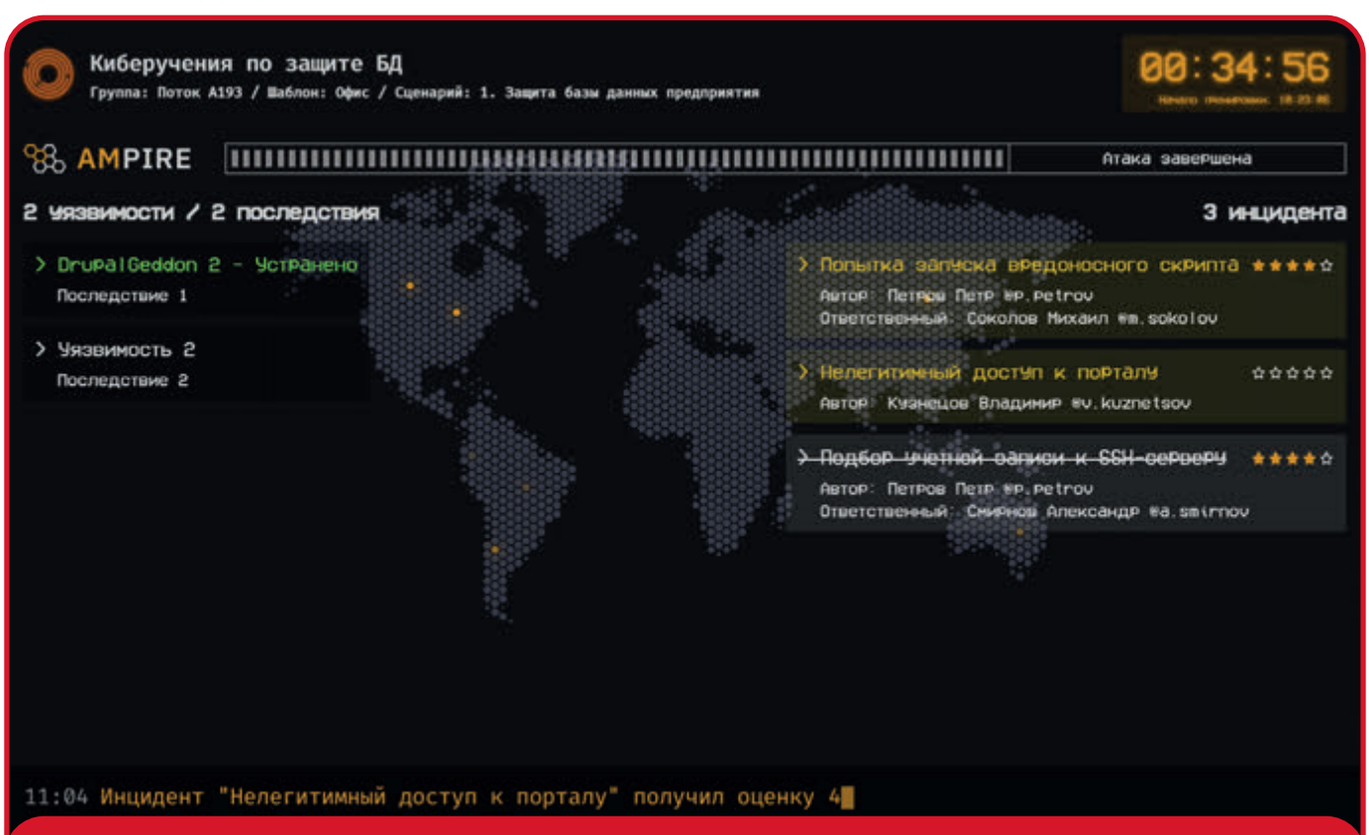


Рис 2. Дашборд киберполигона Ampire, отображающий статистику текущих киберучений

Обученные сотрудники быстрее реагируют на киберугрозы благодаря большей осведомленности о типах угроз, методах и инструментах злоумышленников, механизмах защиты. Это позволяет сэкономить до 50% времени, затрачиваемого на устранение последствий компьютерных атак. Подводя итоги интенсивного курса практических тренировок на платформе Ampire, преподаватели «Перспективного мониторинга» отмечают, что сотрудники после обучения на 70% чаще правильно распознают вредоносные вложения и ссылки, выявляют артефакты и ликвидируют последствия компьютерных атак.

Проведение регулярных киберучений **(Рис. 3)** централизованно и системно на уровне региона упрощает процесс их организации и повышает результативность. Наличие в субъекте регионального киберполигона создает условия для проведения межрегиональных киберучений специалистов государственных организаций. Такие киберучения становятся площадкой для обмена опытом и повышения защиты чувствительных данных по всей Российской Федерации.

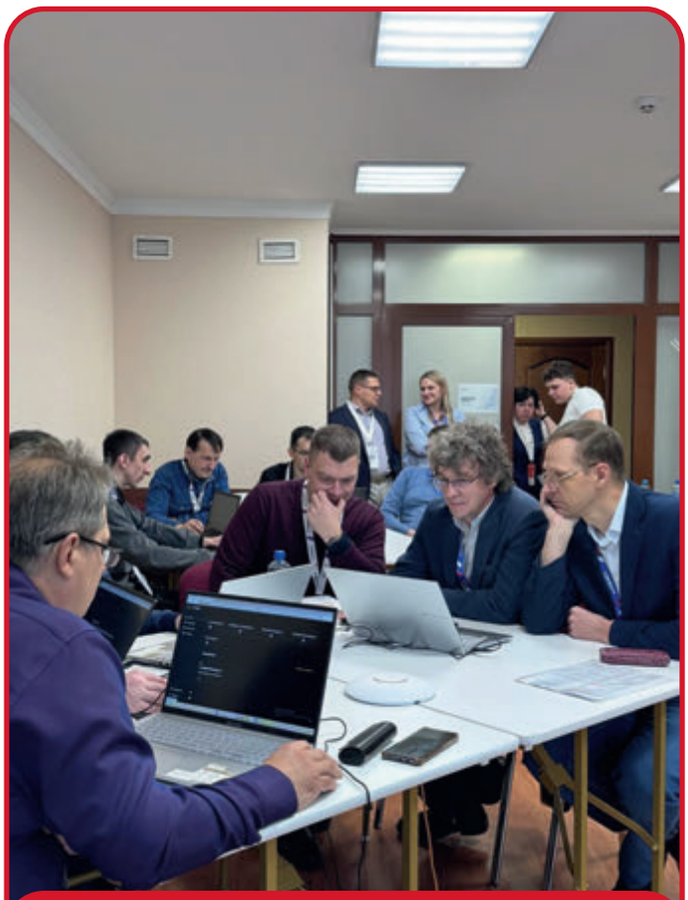


Рис 3. Киберучения специалистов ИБ на киберполигоне Ampire в Кузбассе

ВЫВОД

Создание регионального киберполигона – это один из инструментов, позволяющих перейти от фрагментарного подхода к системному развитию практической подготовки в сфере информационной безопасности. Он помогает решать сразу несколько задач:

- содействие восполнению дефицита кадров;
- обеспечение регулярного обучения сотрудников госструктур;
- повышение уровня цифровой грамотности заинтересованного населения;
- улучшение качества подготовки специалистов в учебных заведениях;
- обеспечение межрегионального взаимодействия.

Региональные инициативы в этом направлении особенно значимы, поскольку именно на уровне субъектов Российской Федерации возможна более эффективная координация всех заинтересованных сторон – от вузов и колледжей до школ и органов власти. Региональный киберполигон создает базу, на которую могут опираться как образовательные учреждения, так и организации, отвечающие за кибербезопасность в регионе.

Ключевую роль играет сотрудничество региональных властей с бизнесом, в данном случае между Министерством цифрового развития и связи Кузбасса и АО «Перспективный мониторинг», которое также было закреплено соглашением о сотрудничестве в области информационных технологий. Такой диалог позволяет производителю платформы ИБ учитывать реальные потребности пользователей, адаптировать решение к техническим и организационным условиям конкретного региона, а также обеспечить устойчивость проекта в долгосрочной перспективе. Важно, что участие бизнеса не ограничивается поставкой технологии – речь идет о включении в образовательный процесс, методической поддержке, помощи в обучении преподавателей и развитии инфраструктуры. Регион, в свою очередь, может выстроить необходимые нормативные и организационные рамки, обеспечить финансирование и масштабирование решения.

Использование отечественного решения в таких проектах критически важно: оно обеспечивает соответствие требованиям по защите данных и локализации, снижает технологическую зависимость от внешних поставщиков, позволяет адаптировать платформу под конкретные задачи региона и развивать ее функциональность по мере необходимости. Кроме того, поддержка и документация на русском языке, а также возможность локального размещения платформы без обращения к облачным решениям делают такие системы более управляемыми и безопасными.

Опыт Кузбасса показывает, как регион может самостоятельно инициировать и реализовать проект, востребованный всеми участниками образовательного и административного процесса. Подготовленные методические материалы и регламенты уже доказали свою эффективность и могут быть использованы другими регионами. Готовность делиться этим опытом – важный шаг к формированию устойчивой и практико-ориентированной системы подготовки специалистов по информационной безопасности в масштабах страны.

МЕРОПРИЯТИЯ АДЭ

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» (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.



Рис 1. Открытие конференции

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.

Ведущий: Торбенко Е.Б., ФСТЭК России.

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

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



Рис 2. Заседание круглого стола № 1 «Приоритетные задачи нормативного регулирования отрасли ИКТ»



Рис 3. Заседание круглого стола № 2 «Актуальные вопросы категорирования объектов КИИ отрасли ИКТ»

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).

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.



Рис 4. Заседание круглого стола № 3 «Роль и место надзорной и разрешительной деятельности в области связи в обеспечении доверия»



Рис 5. Заседание круглого стола № 4 «Безопасность разработки, распространения и использования контента»

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.

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

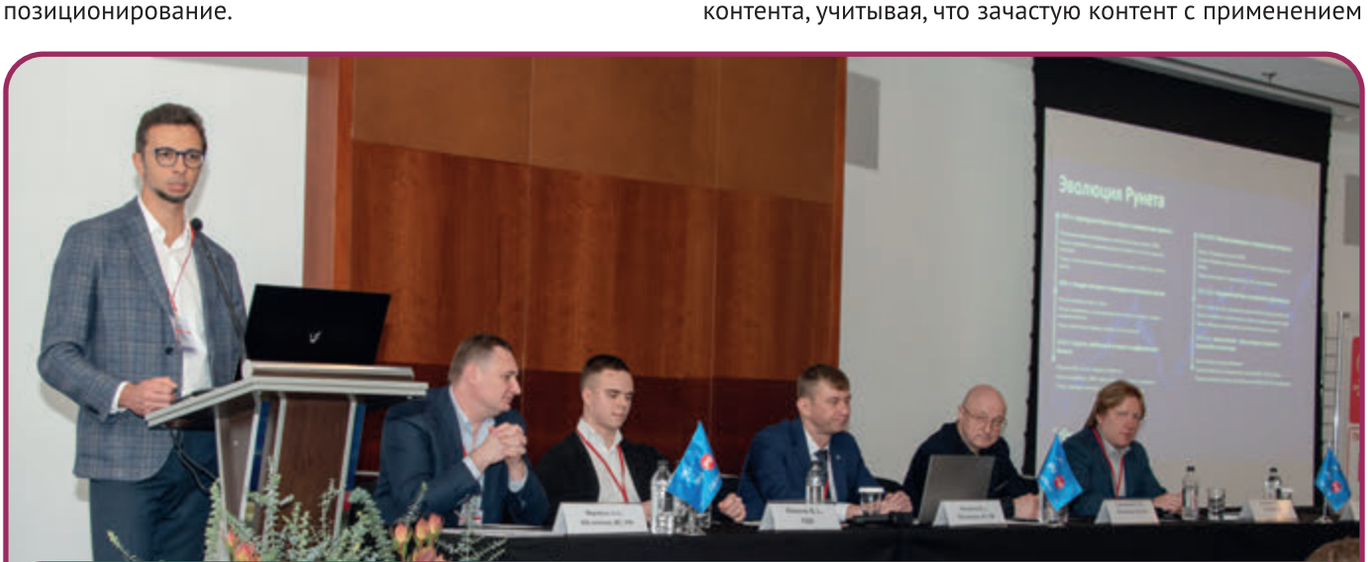


Рис 6. Заседание круглого стола № 5 «Обеспечение доверия и безопасности при развитии и использовании российского сегмента сети Интернет»

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.

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.

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.



Рис 7. Заседание круглого стола № 6 «Обеспечение требуемой функциональности оборудования NGFW»



Рис 8. Заседание круглого стола № 7 «Национальные интересы и международное взаимодействие в сфере ИКТ»

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.

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.

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.



Рис 9. Заседание круглого стола № 8 «Эффективное использование возможностей современных сетей связи: перспективы регулирования и вопросы безопасности при оказании услуг связи (на примере ВАТС)»



Рис 10. Заседание круглого стола № 9 «Содействие разработке и внедрению программного обеспечения для отечественных архитектур микропроцессоров»

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.

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.

МЕМОРАНДУМ О НЕОБХОДИМОСТИ СОЗДАНИЯ ПОЛИГОНА СОДЕЙСТВИЯ РАЗРАБОТКЕ И ВНЕДРЕНИЮ ДОВЕРЕННЫХ РЕШЕНИЙ ДЛЯ КИИ В ОТРАСЛИ СВЯЗИ»

18 апреля 2025 года под руководством заместителя министра цифрового развития, связи и массовых коммуникаций Российской Федерации, члена Исполкома АДЭ Александра Михайловича Шойтова состоялось совещание по вопросу создания на базе АДЭ Полигона доверенных решений для критической информационной инфраструктуры в отрасли связи (далее – Полигон).

На совещании присутствовали представители ФОИВ, операторов связи, разработчиков ПО и технических средств.

По итогам заседания АДЭ была предложена реализация подготовительных и организационных мероприятий, в том числе — задача по консолидации отраслевых организаций, заинтересованных в формировании и участии в деятельности Полигона.

В рамках выполнения поставленной задачи был подготовлен Открытый меморандум «О необходимости создания полигона содействия разработке и внедрению доверенных решений для критической информационной инфраструктуры в отрасли связи» (далее – Меморандум). Меморандум содержит принципы и определяет цели и задачи работы Полигона на базе АДЭ. Целью работы Полигона является содействие реализации государственной политики в сфере разработки и внедрения ПАК для КИИ отрасли связи. Полигон обеспечит экспертное взаимодействие участников, проведение тестирований, формирование требований к ПАК и продвижение лучших отечественных практик и технологических решений в этой сфере, отвечающих требованиям безопасности, технологической зрелости и совместимости.

К Меморандуму могут присоединиться организации отрасли связи, разделяющие цели и задачи инициативы и заинтересованные в своевременном переходе на доверенные программно-аппаратные комплексы на принципах безопасности и технологической зрелости.

По состоянию на 29 сентября 2025 года к Меморандуму присоединились ПАО «Ростелеком», АО «Эр-Телеком Холдинг», ПАО «Мобильные ТелеСистемы», ООО «Т2 Мобайл».



Рис 1. Совещание по вопросу создания на базе АДЭ Полигона доверенных решений для критической информационной инфраструктуры в отрасли связи

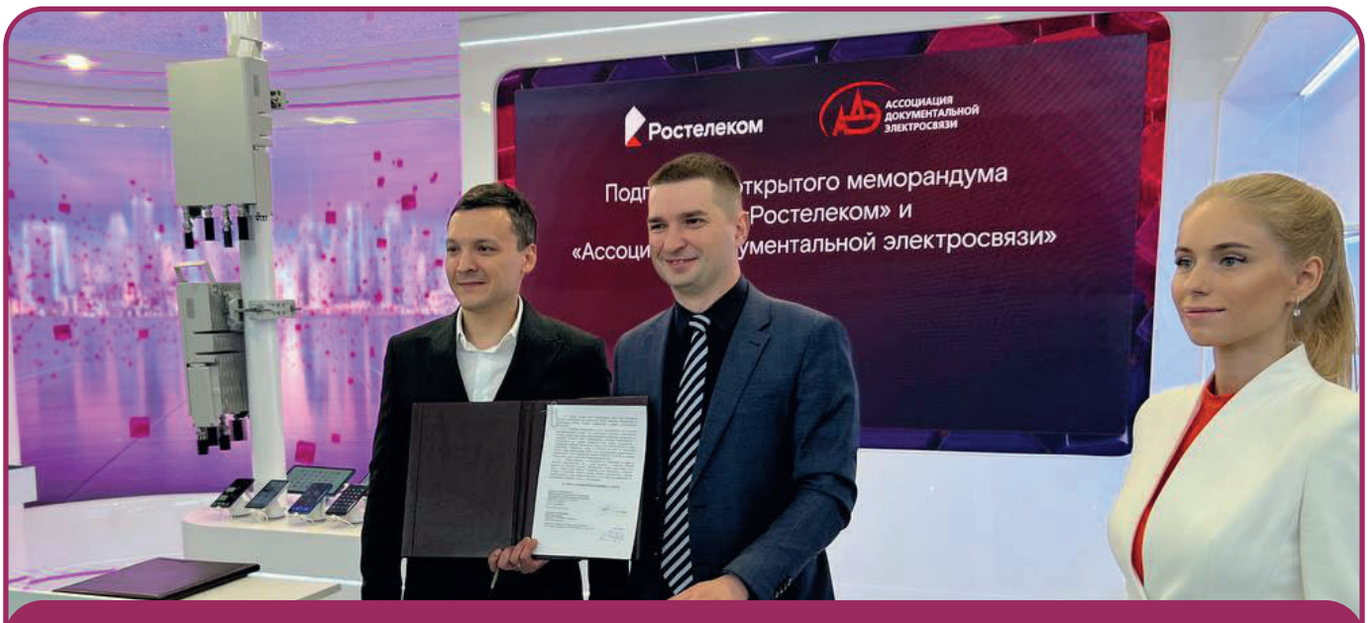


Рис 2. Подписание Меморандума с ПАО «Ростелеком»

ОТКРЫТЫЙ МЕМОРАНДУМ

«О НЕОБХОДИМОСТИ СОЗДАНИЯ ПОЛИГОНА СОДЕЙСТВИЯ РАЗРАБОТКЕ И ВНЕДРЕНИЮ ДОВЕРЕННЫХ РЕШЕНИЙ ДЛЯ КРИТИЧЕСКОЙ ИНФОРМАЦИОННОЙ ИНФРАСТРУКТУРЫ В ОТРАСЛИ СВЯЗИ»

г. Нижний Новгород **«2» июня 2025г.**

В соответствии с Указами Президента Российской Федерации от 30 марта 2022 г. № 166 «О мерах по обеспечению технологической независимости и безопасности критической информационной инфраструктуры Российской Федерации» и 01 мая 2022 г. № 250 «О дополнительных мерах по обеспечению информационной безопасности Российской Федерации» объекты критической информационной инфраструктуры до 2030 года должны перейти на доверенные программно-аппаратные комплексы (далее – «ПАК»).

Мы, представители организаций отрасли связи, заинтересованные в своевременном переходе на доверенные программно-аппаратные комплексы на принципах безопасности и технологической зрелости, обеспечивая непрерывное функционирование и деятельность субъектов критической информационной инфраструктуры (далее совместно именуемые – «Стороны», а по отдельности – «Сторона»), подписали настоящий Открытый меморандум (далее – «Меморандум», о нижеследующем:

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Меморандум содержит принципы и определяет цели и задачи работы Полигона

содействия разработке и внедрению доверенных решений для критической информационной инфраструктуры (далее – «КИИ») отрасли связи на базе общественно-государственного объединения «Ассоциация документальной электросвязи» (далее – «Полигон»).

1.2. Сотрудничество Сторон осуществляется в соответствии с принципами равенства Сторон, их добросовестности, защиты взаимных интересов, соблюдения требований законодательства Российской Федерации.

1.3. Меморандум является открытой декларацией намерений о сотрудничестве в целях создания, развития и поддержания работы Полигона. Организация отрасли связи, разделяющая цели, задачи и принципы работы Полигона, может присоединиться к Меморандуму.

1.4. Цели и задачи Полигона:

Целью работы Полигона является содействие реализации государственной политики в сфере разработки и внедрения ПАК для КИИ.

Задачами Полигона являются:

– Изучение, комплексирование и распространение лучших отечественных компетенций, практик и ресурсов в управлении развитием функциональности и обеспечением информационной безопасности при разработке и внедрении ПАК для КИИ;

– Определение перечня специфического отраслевого оборудования в связи для объектов критической информационной инфраструктуры;

– Формирование функциональных требований, а также требований совместимости и безопасности к специфическим отраслевым программно-аппаратным комплексам (далее – «ПАК»);

– Тестирование и апробация совместимости ПАК в сфере связи;

– Подтверждение соответствия отраслевых ПАК требованиям участников рынка отрасли связи;

– Принятие необходимых мер по обеспечению информационной безопасности и целостности функционирования доверенных ПАК для КИИ с использованием отечественной криптографии;

– Подготовка и реализация образовательных программ и учебных дисциплин по разработке и внедрению ПАК для КИИ в интересах работодателей.

2. ПРЕДМЕТ МЕМОРАНДУМА

2.1. Стороны выражают заинтересованность в сотрудничестве по направлениям, перечисленным в пункте 1.4 Меморандума, но не ограничиваясь ими.

2.2. Стороны будут стремиться оказывать содействие друг другу в достижении взаимных целей, прямо или косвенно вытекающих из условий настоящего Меморандума.

2.3. Сотрудничество между Сторонами будет осуществляться на основе равенства, доброй воли, взаимовыгодного партнерства, уважения и доверия.

2.4. Стороны при исполнении настоящего Меморандума осуществляют свою деятельность в соответствии с действующим законодательством Российской Федерации.

3. УСЛОВИЯ ВЗАИМОДЕЙСТВИЯ И СОТРУДНИЧЕСТВА

3.1. В рамках Меморандума Стороны осуществляют взаимодействие и сотрудничество в следующих формах:

– обмен опытом и информацией по вопросам, относящимся к предмету Меморандума и представляющим взаимный интерес;

– проведение в целях реализации Меморандума совещаний рабочих и экспертных групп;

– использование инфраструктуры Полигона для разработки, портирования, отладки, оптимизации программного обеспечения под отечественные архитектуры микропроцессоров (по согласованию с владельцем инфраструктуры);

– использование инфраструктуры Полигона для тестирования и демонстрации возможностей программного обеспечения и ПАК (по согласованию с владельцем инфраструктуры);

– направление представителей Сторон для участия в мероприятиях, проводимых другой Стороной по направлениям деятельности, связанным с предметом Меморандума;

– проведение совместных мероприятий (конференций, совещаний и иных мероприятий);

– оказание взаимной поддержки в освещении в средствах массовой информации совместных мероприятий.

3.2. Сотрудничество Сторон может осуществляться также и в иных взаимосогласованных формах.

3.3. В целях осуществления оперативного взаимодействия в рамках Меморандума Стороны вправе назначить ответственных лиц и направить другой Стороне информацию о контактных данных таких лиц. Стороны подтверждают намерение своевременно информировать друг друга об изменениях контактных данных ответственных лиц.

3.4. Деятельность Сторон по реализации Меморандума регулируется путем проведения двухсторонних переговоров, рабочих встреч, заседаний, консультаций и иных мероприятий, которые оформляются протоколом соответствующего мероприятия.

4. ОТВЕТСТВЕННОСТЬ СТОРОН И КОНФИДЕНЦАЛЬНОСТЬ

4.1. Конфиденциальными являются условия настоящего Меморандума и всей информации, переданной в качестве конфиденциальной.

4.2. Стороны обязуются не разглашать конфиденциальные сведения производственного и коммерческого характера, которые стали известны в процессе совместной деятельности, а также не будут выступать с публичными заявлениями об их сотрудничестве в рамках настоящего Меморандума без предварительного согласования с другими Сторонами.

4.3. Стороны оказывают друг другу помощь в охране патентов и других исключительных прав в защите от недобросовестной конкуренции со стороны третьих лиц.

4.4. Стороны обязуются передавать друг другу все материалы, необходимые для рекламы и предоставления своих услуг, каталоги, фотоматериалы, слайды, рекламные образцы и т.д.

5. РАЗРЕШЕНИЕ СПОРОВ

5.1. Все споры и разногласия, которые могут возникнуть в ходе исполнения Меморандума, будут в преимущественном порядке решаться путем переговоров между сторонами.

5.2. В случае неурегулирования споров и разногласий путем переговоров разрешение разногласий производится в суде по месту нахождения Ответчика.

6. ВСТУПЛЕНИЕ В СИЛУ, ПРИСОЕДИНЕНИЕ К МЕМОРАНДУМУ

6.1. Настоящий Меморандум вступает в силу 02 июня 2025 и действует до достижения цели Меморандума.

6.2. Стороны вправе в одностороннем внесудебном порядке прекратить своё участие в Меморандуме, письменно уведомив об этом другие Стороны не менее чем за 10 (Десять) календарных дней до предполагаемой даты расторжения.

6.3. Стороны пришли к соглашению о том, что решение о присоединении других организаций к настоящему Меморандуму принимает общественно-государственное объединение «Ассоциация документальной электросвязи» (далее – «АДЭ»).

6.4. Для присоединения к Меморандуму потенциальный участник направляет в АДЭ заявление о намерении присоединиться к Меморандуму и заполненную анкету потенциального участника. Документы, подписанные уполномоченным лицом или представителем уполномоченного лица собственноручно, передаются по адресу фактического местонахождения АДЭ: г. Москва, ул. Авиамоторная, д.8, стр.2. В случае если от имени участника заявление направляет не лицо, имеющее право действовать от его имени без доверенности, к заявлению прилагается надлежащим образом оформленная доверенность. Документы, подписанные усиленной квалифицированной электронной подписью участника или уполномоченного представителя участника (в случае если от имени участника заявление направляет не лицо, имеющее право действовать от его имени без доверенности, к заявлению прилагается машиночитаемая доверенность либо доверенность в виде электронного образа документа, заверенного усиленной квалифицированной электронной подписью) направляются по адресу электронной почты info@rans.ru. Форма заявления и анкеты участника установлены в Приложении №1 к Меморандуму, являющемуся его неотъемлемой частью.

6.5. АДЭ в течение 30 (тридцати) календарных дней с момента получения документов от потенциального участника, указанных в пункте 6.4. настоящего Меморандума, проверяет правильность заполнения документов, а также актуальность и достоверность содержащихся в них сведений посредством открытых источников информации. После успешного прохождения проверки потенциальный участник считается присоединившимся к условиям Меморандума, о чем уведомляется посредством электронных каналов связи. Потенциальному участнику может быть отказано в присоединении к Меморандуму без объяснения причин.

6.6. Информация о Сторонах настоящего Меморандума (наименование, ИНН, основной вид деятельности, сайт в сети Интернет) размещается АДЭ в открытом доступе в сети Интернет.

6.7. Настоящий Меморандум составлен в одном экземпляре и хранится в АДЭ. Текст Меморандума АДЭ публикует на своём сайте в сети Интернет rans.ru.

7. ПРОЧИЕ УСЛОВИЯ

7.1. Меморандум не является предварительным договором, офертой соглашением о порядке ведения переговоров, договором простого товарищества. Меморандум не налагает на Стороны финансовых, имущественных и иных обязательств, за исключением обязательств, предусмотренных п. 7 Меморандума.

7.2. Ни одна из Сторон не будет действовать в качестве агента другой Стороны без заключения соответствующих отдельных соглашений.

7.3. Каждая Сторона будет самостоятельно нести свои собственные расходы, возникающие при выполнении условий настоящего Меморандума, за исключением случаев, отдельно оговариваемых в рамках соответствующих соглашений.

7.4. Положения Меморандума не могут рассматриваться как создающие благоприятствующие условия для деятельности отдельного хозяйствующего субъекта, которые могут иметь своим результатом ограничение конкуренции или ущемление интересов иных хозяйствующих субъектов. Взаимодействие и сотрудничество при решении конкретных задач должны осуществляться с соблюдением требований Федерального закона от 26.07.2006 № 135-ФЗ «О защите конкуренции», Федерального закона от 05.04.2013 № 44-ФЗ «О контрактной системе в сфере закупок товаров, работ, услуг для обеспечения государственных и муниципальных нужд», Федерального закона от 18.07.2011 № 223-ФЗ «О закупках товаров, работ, услуг отдельными видами юридических лиц».

7.5. Стороны признают, что Меморандум не ограничивает их права по принятию самостоятельных мер в своих интересах в отношении областей деятельности, указанных в разделе 1 Меморандума. Стороны имеют право, в том числе, в период срока действия Соглашения, вести переговоры и заключать договоры и соглашения, предметом которых является сотрудничество с любыми третьими лицами в любых сферах деятельности, в том числе, без ограничения, по направлениям, указанным в пункте 3.1 Меморандума.

ЧЛЕНЫ АДЭ

ОРГАНИЗАЦИИ - ЧЛЕНЫ АССОЦИАЦИИ ДОКУМЕНТАЛЬНОЙ ЭЛЕКТРОСВЯЗИ

ПО СОСТОЯНИЮ НА 25 СЕНТЯБРЯ 2025 ГОДА

- Айдеко
- Айтулабс
- Академия ФСО России
- Базальт СПО
- ВАС Экспертс
- ВымпелКом
- Геларм
- ГЛОНАСС
- ГРЧЦ
- Институт государства и права РАН
- Институт развития интернета
- Информационная внедренческая компания
- ИнфоТеКС
- КНС ГРУПП
- Координационный центр доменов .RU/.РФ
- Космическая связь
- МВД России
- МегаФон
- Межрегиональный Транзит Телеком
- Министерство промышленности и торговли Российской Федерации (Минпромторг России)
- Министерство цифрового развития, связи и массовых коммуникаций Российской Федерации (Минцифры России)
- Министерство энергетики Российской Федерации (Минэнерго России)
- МИФИ
- Мобильные ТелеСистемы
- Московский государственный лингвистический университет
- МТУСИ
- МЦСТ
- НИИ Интеграл
- НИЦ ЦТ
- НоваКард
- Норси-Транс
- НТЦ Вулкан
- НТЦ ИТ РОСА
- НТЦ Модуль
- НТЦ Протей
- НТЦ СОТСБИ
- Пенсионный фонд Российской Федерации
- Российская Академия Наук
- Российские сети вещания и оповещения
- Ростелеком
- РТ-Иридиум
- РТРС
- Санкт-Петербургский государственный университет телекоммуникаций им. проф. М.А.Бонч-Бруевича
- СИГНАЛТЕК
- Сигнатек
- Системы и Решения
- Специальные технологии
- СТАРТЕЛЕКОМ
- Стек Софт
- Т2 Мобайл
- Телкор
- ТехАргос
- Труконф
- УК Гарда
- Федеральная служба безопасности Российской Федерации (ФСБ России)
- Федеральная служба охраны Российской Федерации (ФСО России)
- Федеральная служба по надзору в сфере связи информационных технологий и массовых коммуникаций (Роскомнадзор)
- Федеральная служба по техническому и экспортному контролю (ФСТЭК России)
- Центр компетенции информационно-телекоммуникационных сетей
- Центр Хранения Данных
- Цитадель
- ЭР-Телеком Холдинг