ДОКУМЕНТАЛЬНАЯ ЭЛЕКТРОСВЯЗЬ

информационно-аналитический журнал

№36 СЕНТЯБРЬ 2026
(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:
+7 (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 Рунет переходит на новую модель: как меняется доменная отрасль с 1 сентября 2026 года
Андрей Воробьев

5 Применение технологий машинного обучения в вопросах классификации сетевого трафика
Александр Полунин

14 Экономика отказоустойчивости цифровой инфраструктуры: риск-ориентированный подход
Дмитрий Петров

18 Российский рынок видеоигр и игрового ПО: актуальные тенденции развития
Алексей Буньков, Наталья Саранкина

22 35 лет Региональному содружеству в области связи: стратегические ориентиры цифрового развития и укрепление межгосударственного сотрудничества
Мария Большакова, Владимир Горжалцан

25 Трансфер технологий: в какой момент «чужое» становится «своим»?
Анатолий Корсаков

ОБЕСПЕЧЕНИЕ ДОВЕРИЯ И БЕЗОПАСНОСТИ ПРИ ИСПОЛЬЗОВАНИИ ИКТ

30 Практическая подготовка персонала к киберинцидентам: возможности современных киберучений
Александр Фефилов, Наталия Кабакова, Наталья Киселева

35 Одноюнитовая крейтовая модульная система для критической информационной инфраструктуры
Максим Орлов

39 Имитатор ТС ОРМ «Импульс 374». Реализация новых НПА. Сертификация.
Евгений Громыхин

42 ViPNet QRNG квантовый генератор случайных чисел: обзор архитектуры, принципов работы и сравнительный анализ
Олег Иванов

46 Многоуровневая защита периметра в межсетевых экранах следующего поколения (NGFW)
Александр Моисеенко

МЕРОПРИЯТИЯ АДЭ

52 Итоговый документ 24-й ежегодной конференции «Обеспечение доверия и безопасности при использовании ИКТ»

58 Соглашение о сотрудничестве между Минпромторгом России и АДЭ

64 ЧЛЕНЫ АДЭ

РАЗВИТИЕ ИКТ-ИНФРАСТРУКТУРЫ



АНДРЕЙ ВОРОБЬЕВ
директор
АНО «Координационный центр национального домена сети Интернет»

РУНЕТ ПЕРЕХОДИТ НА НОВУЮ МОДЕЛЬ: КАК МЕНЯЕТСЯ ДОМЕННАЯ ОТРАСЛЬ С 1 СЕНТЯБРЯ 2026 ГОДА

В 2026 году Координационный центр доменов .RU/.РФ (АНО «Координационный центр национального домена сети Интернет», КЦ) отмечает 25-летие, встречая эту веху на пороге масштабной трансформации всей доменной отрасли. В эксклюзивном интервью для журнала АДЭ «Документальная электросвязь» директор КЦ Андрей Воробьев рассказывает о ключевых этапах эволюции организации и новых правилах игры, вступающих в силу с 1 сентября 2026 года. Обязательная идентификация через Единую систему идентификации и аутентификации (ЕСИА), регулярная перепроверка аккредитации регистраторов и новая роль КЦ как специализированного регистратора для госсектора – как эти изменения сделают Рунет прозрачнее и безопаснее? Поговорим о том, как рынок адаптируется к новым требованиям, почему это не создаст барьеров для добросовестного бизнеса и какую роль доменные имена будут играть в эпоху искусственного интеллекта и Web 3.0.

За 25 лет Координационный центр прошел путь от небольшой координационной группы до лидера цифровой инфраструктуры России. Какие, на ваш взгляд, ключевые этапы можно выделить в 25-летней истории организации, и что характеризует каждый из них?

Я бы выделил три таких этапа. Первый – создание в начале 2000-х годов единых правил и распределенной системы регистрации. Второй – запуск кириллического домена .РФ в 2010 году, после которого Координационный центр стал администратором двух национальных доменов и одним из лидеров развития многоязычного интернета. Третий – усиление роли центра в обеспечении безопасности и устойчивости Рунета. Сегодня этот этап выходит на новый уровень: полномочия центра расширяются, а отрасль переходит к новой модели регулирования.

2026 год станет годом серьезных перемен в доменной индустрии. Какие изменения ждут администраторов доменов и регистраторов после 1 сентября?

Вступление в силу новых Правил регистрации доменных имен[1] (Постановление Правительства Российской Федерации от 31.08.2026 № 1119) с 1 сентября 2026 года — это важнейшая веха для всего Рунета, для всей отрасли начнется переход к новой, более прозрачной и безопасной модели работы.

[1] https://cctld.ru/files/pdf/docs/rules_gov.pdf

Теперь любые операции с доменом требуют подтверждения личности через Единую систему идентификации и аутентификации (ЕСИА), а для сохранения права администрирования вводится требование о прохождении обязательной ежегодной идентификации. Единый механизм подтверждения данных поможет защитить домены от угона. Изменится и работа регистраторов: им потребуется интегрировать свои системы с ЕСИА и привести процессы в соответствие с новыми требованиями.

В результате рынок станет более прозрачным, а регистрация доменов на вымышленные или чужие данные и другие злоупотребления будут существенно затруднены.

Одновременно меняется сама модель регулирования отрасли: Правила регистрации доменных имен в национальных зонах утверждены Правительством Российской Федерации, оно также утвердило Правила формирования и ведения перечней юридических лиц, осуществляющих регистрацию доменных имен[2] (Постановление Правительства Российской Федерации от 31.08.2026 № 1120). Одно из ключевых требований к регистраторам – техническая готовность работать с ЕСИА.

Поэтому наша первоочередная задача – обеспечить плавный переход на новую модель всех участников отрасли: регистраторов, администраторов доменов, государственных организаций и других участников рынка. Важно сохранить стабильность системы, в которой сейчас в России работают 185 регистраторов и более 2,5 миллиона администраторов.

Не станет ли переход к регистрации доменных имен через ЕСИА критическим для дальнейшего развития российских национальных доменов?
Ни в коем случае, я бы назвал этот переход давно назревшим шагом, который приведет к серьезной и позитивной трансформации всей доменной индустрии.

К сожалению, текущая ситуация позволяет злоумышленникам регистрировать домены на поддельные или вымышленные данные для создания фишинговых ресурсов. Поэтому идентификация администраторов через ЕСИА должна рассматриваться в первую очередь как эффективный инструмент защиты пользователей и добросовестного бизнеса.

Для обычных пользователей регистрация доменов станет не сложнее, а проще благодаря автоматизации процессов через портал Госуслуг. Мы не ставим целью создание искусственных барьеров, наша задача — выстроить правильную «цифровую гигиену» и найти баланс между безопасностью и доверием в сети.

А как на это событие реагируют аккредитованные регистраторы?
Регистраторы реагируют на эти изменения прагматично и конструктивно, понимая, что регулирование доменного пространства объективно движется в сторону максимальной прозрачности. Мы тесно взаимодействуем с отраслью, чтобы сделать этот переход максимально безболезненным. Показательным примером нашего совместного решения стало недавнее внеочередное Общее собрание учредителей КЦ (решение ОСУ № 05-42), на котором была утверждена новая редакция Соглашения об аккредитации[3], вступившая в силу 10 сентября 2026 года.

Для регистраторов это, безусловно, серьезная организационная и финансовая нагрузка: им необходимо обеспечить интеграцию своих систем с ЕСИА и пройти процедуру включения в новые официальные перечни юридических лиц. Однако мы предусмотрели комфортный переходный период, чтобы рынок не испытал шока: заключенные ранее соглашения с действующими регистраторами прекратят свое действие либо с даты включения компании в новые перечни, либо с 18 января 2027 года — в зависимости от того, какое событие наступит ранее. Это позволит регистраторам продолжать бесперебойно обслуживать своих клиентов и принимать заявки в период выполнения всех необходимых действий для подтверждения своего нового статуса.

Координационный центр доменов .RU/.РФ с 1 сентября также примеряет на себя роль регистратора — насколько это сложно для национальной регистратуры?
Здесь важно сделать принципиальное уточнение: Координационный центр не выходит на розничный рынок, чтобы конкурировать с коммерческими компаниями за массового пользователя или частный бизнес. Согласно Федеральному закону № 569-ФЗ[4], с 1 сентября 2026 года мы берем на себя функцию специализированного регистратора исключительно для определенных законом категорий организаций. Речь идет о регистрации и обслуживании доменных имен для государственных органов, органов местного самоуправления, ГУПов, МУПов, государственных и муниципальных учреждений, а также государственных и публично-правовых компаний.

С организационной и технологической точек зрения для нас это масштабный, но абсолютно решаемый проект. Чтобы исключить любой конфликт интересов с функцией национальной регистратуры, мы создаем выделенную структуру — «Регистратор КЦ в доменах .RU/.РФ».

[2] https://cctld.ru/files/pdf/docs/rules_form-reg.pdf
[3] https://cctld.ru/files/docs/accr_sogl.pdf
[4] Федеральный закон от 29 декабря 2025 г. № 569-ФЗ "О внесении изменений в Федеральный закон "Об информации, информационных технологиях и о защите информации" и отдельные законодательные акты Российской Федерации";
https://www.garant.ru/products/ipo/prime/doc/413278488/

Для государственных заказчиков процесс выстроен максимально прозрачно и состоит из трех обязательных шагов:

- Заключение договора на услуги напрямую с Координационным центром.
- Перенос существующих доменов в зонах .RU и .РФ на обслуживание к нам от текущих коммерческих регистраторов.
- Регистрация всех новых доменных имен для определенных законом категорий организаций теперь будет осуществляться исключительно у Регистратора КЦ в доменах .RU/.РФ.

Ключевым элементом нашей новой системы станет полная интеграция с ЕСИА. Регистрация заказчиков и все операции с доменами будут осуществляться исключительно через идентификацию на портале Госуслуг. Это не только защищает госсектор от мошенничества, но и упрощает бюрократические процедуры. Однако это требует от самих госструктур определенной подготовки: мы рекомендуем им заранее актуализировать профили своих организаций на Госуслугах и обязательно добавить туда подтвержденные учетные записи сотрудников, уполномоченных работать с доменными именами.

Главная сложность здесь кроется не в технологиях — инфраструктура у нас мощная — а в выстраивании новой архитектуры бизнес-процессов и обеспечении бесперебойного переноса тысяч государственных доменов от других регистраторов к нам в переходный период. Сейчас идет работа над всеми необходимыми нормативными актами, после чего Регистратор КЦ в доменах .RU/.РФ сможет начать полноценную работу.

Мы живем в эпоху стремительного развития цифровых технологий — искусственный интеллект, блокчейн, Web 3.0. Как, по вашему мнению, будет эволюционировать доменная система в ближайшие 5-10 лет, и какую роль в этом сыграет Координационный центр?

На мой взгляд, в ближайшие 5-10 лет домены не исчезнут, но станут менее заметны пользователю. Люди будут все чаще искать информацию и обращаться к сервисам через нейросети, ИИ-агентов и другие интерфейсы, а домены постепенно перейдут на уровень базовых цифровых идентификаторов. Блокчейн и Web 3.0 могут расширить сценарии их использования, например, связать доменные имена с криптокошельками и смарт-контрактами, но вряд ли заменят традиционную DNS.

Наша задача в этих условиях – обеспечивать устойчивость национальной доменной инфраструктуры, развивать защиту от злоупотреблений и адаптироваться к новым технологиям и рискам. Каким бы ни стал интернет будущего, в его основе должна оставаться надежная, безопасная и понятная система цифровых адресов.

Каким будет дальнейшее развитие Координационного центра? Какие задачи стоят перед организацией на ближайшие годы?

Можно без преувеличения сказать, что сейчас мы стоим на пороге нового этапа. Полномочия центра расширяются, а вместе с ними растут масштаб задач и уровень ответственности.

Координационный центр остается ключевой площадкой взаимодействия государства, регистраторов и других участников рынка. Наша задача – поддерживать постоянный диалог, находить баланс интересов и совместно вырабатывать решения, необходимые для дальнейшего развития отрасли.

Также мы продолжим укреплять безопасность и устойчивость доменной инфраструктуры, развивать механизмы противодействия злоупотреблениям в DNS, расширять поддержку языков народов России и повышать цифровую грамотность пользователей.

В конечном счете наша главная цель и задача – сделать Рунет безопасным и надежным пространством, в котором пользователи будут чувствовать себя уверенно и защищенно, а бизнес сможет запускать новые проекты и развивать онлайн-сервисы.



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

ПРИМЕНЕНИЕ ТЕХНОЛОГИЙ МАШИННОГО ОБУЧЕНИЯ В ВОПРОСАХ КЛАССИФИКАЦИИ СЕТЕВОГО ТРАФИКА

АННОТАЦИЯ
В работе рассматриваются прикладные аспекты классификации сетевого трафика с использованием методов машинного обучения. Описываются процессы формирования наборов данных – адаптированной матрицы признаков классификации для обучения моделей машинного обучения. Рассматриваются различные реализации алгоритмов машинного обучения для задачи классификации сетевого трафика. На основе результатов практических исследований моделей приводятся результаты анализа наиболее эффективных методов обучения, оценка их эффективности с использованием известных метрик классификации: точности, полноты, F-меры и матрицы ошибок. Основное внимание уделяется вопросам реализации механизмов анализа структурно-временных характеристик потоков сетевых пакетов с учётом требований к качеству при отсутствии снижения скорости классификации.

КЛЮЧЕВЫЕ СЛОВА:
Классификация сетевого трафика, сетевой сервис, методы машинного обучения, случайный лес, градиентный бустинг.

1. ВВЕДЕНИЕ

Технологии классификации сетевого трафика исторически играют важную роль в решении прикладных вопросов управления потоками трафика, улучшения тактико-технических и эксплуатационных характеристик телекоммуникационного оборудования (далее – ТКО), обеспечения информационной безопасности, поскольку позволяют не только идентифицировать конкретный сетевой сервис или приложение, являющееся источником потоков данных, но и определять его структуру. Традиционными сферами применения средств классификации трафика являются решения для операторов связи, отвечающие за тарификацию трафика абонентов, сетевые устройства, вне зависимости от типа сети, отвечающие за обеспечение требуемого качества обслуживания клиентов, оптимизацию предоставляемых сервисов и балансировку нагрузки на сеть и др. С точки зрения обеспечения требований к функциям информационной безопасности информационных систем, классификация сетевого трафика может использоваться как инструмент контроля сетей связи и передаваемого по ним трафика: управления параметрами передачи или блокировки определенных сетевых протоколов/сервисов/приложений, детектирования компьютерных атак и др.

В [1] рассматриваются методы, способы, алгоритмы и прикладные вопросы разработки решений для глубокого анализа трафика – DPI (англ. Deep Packet Inspection) Engine на примере разработанного ООО «ТехАргос» программного комплекса TrACE TA[1] (англ. Traffic Analysis and Classification Engine). Вместе с тем традиционные методы классификации сетевого трафика (по порту или коду протокола, по значениям полей в заголовках протоколов или по сигнатурам в пакете) оказываются неприменимы в условиях существенного роста объемов, видов и сложности сетевых протоколов, сервисов и приложений, широкого распространения технологий шифрования и обфускации трафика, средств анонимизации и обхода блокировок, не позволяющих использовать для классификации служебную информацию и содержимое полезной нагрузки. Соответственно и технологии классификации должны эволюционировать вместе с глобальными изменениями в устройстве трафика.

В этой связи одним из перспективных направлений классификации сетевого трафика является использование поведенческих моделей Session Correlation (метод классификации по информации из связанных сеансов), Session Behavior (метод классификации по действиям в рамках сеанса) [1], а также статистических методов и технологий машинного обучения – ML-классификации (англ. Machine Learning) трафика, основанных на выявлении и анализе структурно-временных характеристик. Степень проработанности темы на сегодняшний день достаточно высока, многие вопросы исследования методов классификации трафика с помощью ML рассматривались в [2-4]. Однако в данных работах не получили достаточного отражения практические вопросы классификации IP-трафика сетевых сервисов и приложений в условиях жестких требований к качеству (точности) при отсутствии снижения скорости классификации при потоковом режиме обработки данных.

[1] Включен в Реестр российского программного обеспечения Министерства цифрового развития, связи и массовых коммуникаций Российской Федерации (https://reestr.digital.gov.ru/reestr/2735118/?sphrase_id=24912811).

В настоящих условиях актуальными задачами являются разработка и внедрение технологий ML-классификации в новейших образцах ТКО, предназначенных для классификации потоков сетевых пакетов, например, в составе программно-аппаратных комплексов глубокого анализа пакетов (DPI). В работе сделана попытка обобщения опыта разработки подобного решения на примере программного комплекса TrACE TA. 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. МЕТОДЫ МАШИННОГО ОБУЧЕНИЯ В ЗАДАЧАХ КЛАССИФИКАЦИИ СЕТЕВОГО ТРАФИКА

Задача классификации трафика является фундаментальной и может рассматриваться как задача обучения с учителем. Для её решения применимы соответствующие методы машинного обучения:

- наивный байесовский классификатор (англ. Naive Bayesian Classifier);
- метод опорных векторов;
- метод k-ближайших соседей;
- деревья принятия решений (с разными алгоритмами построения: CART, C4.5, C5.0);
- методы бэггинга (случайный лес, англ. Random Forest);
- методы бустинга (Adaboost, XGBoost);
- нейронные сети различных видов.

Основные характеристики, теоретические основы и особенности использования каждого из данных методов рассмотрены в [2], где классификация рассматривается только для применения в моделях вне режима реального времени. Качество такой классификации напрямую зависит от глубины анализа (количества анализируемых пакетов), используемой ML-модели и множества анализируемых структурно-временных характеристик. Более глубокий анализ и сложные модели требуют значительных вычислительных ресурсов, что в условиях высокой интенсивности поступления потоков сетевых пакетов на классификатор приводит к снижению скорости обработки и потенциальным потерям данных.

Настоящая статья посвящена поиску компромисса между качеством классификации и производительностью реализующей её вычислительной системы в контексте уменьшения входного объема данных модели классификации. Предварительно стоит отметить, в рамках проводимых экспериментов исследовалось большинство перечисленных выше методов. Вместе с тем бэггинг на деревьях и бустинг показали лучшую точность среди всех рассмотренных алгоритмов, обеспечивая при этом высокую производительность, хотя и требуют больше времени для обучения. Это связано с их способностью комбинировать несколько моделей для улучшения предсказательной силы. Именно данные группы методов рассматриваются в настоящей статье подробно.

3. ML-КЛАССИФИКАЦИЯ МУЛЬТИМЕДИЙНОГО ТРАФИКА СЕРВИСОВ МГНОВЕННОГО ОБМЕНА СООБЩЕНИЯМИ

Для проведения эксперимента были выбраны следующие сервисы мгновенного обмена сообщениями: Amazon Chime, Discord[2], Google Meet, Jitsi, МТС Линк, Одноклассники, SaluteJazz (Jazz by Sber), Signal, Skype (Microsoft Teams), Slack, Snapchat, Telegram, Viber, VK Мессенджер, WB Мессенджер, Webex, Whatsapp[3], Яндекс Телемост.

3.1. ПОДГОТОВКА НАБОРОВ ДАННЫХ

Исходные данные: записи дуплексных UDP-потоков сервисов мгновенного обмена сообщениями, содержащие минимум 1 минуту полезной медиа-нагрузки. Матрица признаков – статистические данные (структурно-временные характеристики информационного обмена) рассчитываются в двух режимах: «посекундном» и «попакетном».

Режимы «посекундный» и «попакетный» принципиально отличаются. Попакетная статистика накапливается в общей таблице отдельно для каждого симплексного направления и обновляется с каждым следующим пакетом. Обнуление статистики (как в случае «посекундного» режима) не производится – на каждом новом пакете производится пересчет статистики в этом симплексе.

Пример матрицы признаков для обучения модели приведен на **рисунке 1**.

	service	sumNp	sumL	mL	stdL	Lbin[0]	Lbin[1]	Lbin[2]	Lbin[3]	Lbin[4]	...	Tb[7]	Tb[8]	Tb[9]	Tb[10]	Tb[11]	Tb[12]	Tb[13]	Tb[14]	Tb[15]	Tb[16]
0	amazon-chime	7.0	344.0	49.0	50.0	15.0	23.0	30.0	38.0	45.0	...	0.0	0.0	2.0	0.0	0.0	0.0	0.0	0.0	0.0	1.0
1	amazon-chime	7.0	344.0	49.0	50.0	15.0	23.0	30.0	38.0	45.0	...	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	1.0
2	amazon-chime	7.0	344.0	49.0	50.0	15.0	23.0	30.0	38.0	45.0	...	0.0	0.0	0.0	0.0	2.0	0.0	0.0	0.0	0.0	1.0
3	amazon-chime	7.0	344.0	49.0	50.0	15.0	23.0	30.0	38.0	45.0	...	0.0	0.0	0.0	0.0	0.0	0.0	0.0	2.0	0.0	1.0
4	amazon-chime	7.0	344.0	49.0	50.0	15.0	23.0	30.0	38.0	45.0	...	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	2.0	1.0
...	...	...	...	...	...	...	...	...	...	...	...	...	...	...	...	...	...	...	...	...	...
2741	ya-telemost	7.0	786.0	112.0	34.0	96.0	100.0	104.0	108.0	112.0	...	0.0	0.0	0.0	0.0	1.0	0.0	0.0	0.0	0.0	1.0
2742	ya-telemost	7.0	655.0	93.0	37.0	58.0	65.0	71.0	78.0	84.0	...	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	1.0	1.0
2743	ya-telemost	7.0	655.0	93.0	37.0	58.0	65.0	71.0	78.0	84.0	...	0.0	0.0	0.0	0.0	0.0	1.0	0.0	0.0	1.0	1.0
2744	ya-telemost	7.0	754.0	107.0	40.0	58.0	65.0	71.0	78.0	84.0	...	1.0	0.0	1.0	0.0	0.0	0.0	0.0	1.0	0.0	1.0
2745	ya-telemost	7.0	632.0	90.0	18.0	55.0	58.0	61.0	65.0	68.0	...	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	1.0

Рис. 1. Пример набора данных для обучения модели

[2] Сервисы Discord, Signal, Snapchat, Viber, Whatsapp, Telegram (частично) заблокированы на территории России в соответствии с предписаниями Роскомнадзора на основании ст. 15.1-15.4 ФЗ № 149 от 27.07.2006 за нарушение российского законодательства.
[3] Продукт компании Meta Platforms Inc., признанной в России экстремистской организацией.

В **таблице 1** показаны признаки (англ. feature set), извлеченные из каждой дуплексной сессии информационного обмена (значения признаков обрезаны по границам: 1 минута для посекундной статистики и 100 пакетов одного из симплексов (направлений передачи) для попакетной статистики).

Табл. 1. Матрица признаков – формализованный набор признаков для классификации

№ п/п	Признак	Описание (посекундная статистика)	Описание (попакетная статистика)
1.	service	Имя сервиса (целевая переменная)	Имя сервиса (целевая переменная)
2.	sumNp[0]	Усредненная величина «число пакетов за 1 секунду»	–
3.	sumL[0]	Усредненная величина «сумма длин пакетов за 1 секунду» (скорость в бит/с)	Усредненная величина «накопленная сумма длин пакетов в симплексной сессии»
4.	mL[0]	Усредненная величина «среднее длин пакетов за 1 секунду»	Усредненная величина «накопленное среднее суммы длин пакетов»
5.	stdL[0]	Усредненная величина «СКО длин пакетов за 1 секунду»	Усредненная величина «накопленное СКО длин пакетов»
6.	Lbin[0][0]… Lbin[0][16]	Границы бинов (интервалов) для гистограммы длин пакетов	Границы бинов (интервалов) по накопленным данным
7.	L[0][0]…L[0][16]	Значение гистограммы длин пакетов, 17 бинов (число фиксировано)	Значение гистограммы по накопленным данным
8.	sumNp[1]	*для встречного направления*	*для встречного направления*
9.	sumL[1]	*для встречного направления*	*для встречного направления*
10.	mL[1]	*для встречного направления*	*для встречного направления*
11.	stdL[1]	*для встречного направления*	*для встречного направления*
12.	Lbin[1][0]… Lbin[1][16]	*для встречного направления*	*для встречного направления*
13.	L[1][0]…L[1][16]	*для встречного направления*	*для встречного направления*
14.	sumTb[0]	Усредненная величина «сумма интервалов между пакетами за 1 секунду»	Усредненная величина «накопленная сумма интервалов между пакетами в симплексной сессии»
15.	mTb[0]	Усредненная величина «среднее интервалов между пакетами за 1 секунду»	Усредненная величина «накопленное среднее интервалов между пакетами»
16.	stdTb[0]	Усредненная величина «СКО интервалов между пакетами за 1 секунду»	Усредненная величина «накопленное СКО интервалов между пакетами»
17.	Tbbin[0][0]… Tbbin[0][16]	Границы бинов для гистограммы интервалов между пакетами	Границы бинов для гистограммы интервалов между пакетами по накопленным данным
18.	Tb[0][0]…Tb[0][16]	Значение гистограммы интервалов между пакетами, 17 бинов (число фиксировано)	Значение гистограммы интервалов между пакетами по накопленным данным
19.	sumTb[1]	*для встречного направления*	*для встречного направления*
20.	mTb[1]	*для встречного направления*	*для встречного направления*
21.	stdTb[1]	*для встречного направления*	*для встречного направления*
22.	Tbbin[1][0]… Tbbin[1][16]	*для встречного направления*	*для встречного направления*
23.	Tb[1][0]…Tb[1][16]	*для встречного направления*	*для встречного направления*

3.2. ОБУЧЕНИЕ МОДЕЛИ RANDOM FOREST

В качестве базовой модели используется случайный лес, поскольку данная модель не требует нормализации признаков.

Разделение набора данных на обучающую и тестовую выборки производится в пропорции 80:20 со стратификацией по целевому параметру *service*. Количество деревьев решений, которые составляют ансамбль – параметр *n_estimator*, является ключевым гиперпараметром, который напрямую влияет на качество и ресурсоёмкость модели случайного леса. Его выбор – это всегда компромисс между точностью и скоростью вычислений. В рамках эксперимента значение параметра *n_estimator=20* (для «посекундной» статистики) и *n_estimator=13* (для «попакетной» статистики) предварительно было подобрано в Knime Analytics [5] **(рисунок 2)**.

3.3. ИССЛЕДОВАНИЕ МОДЕЛИ

Процесс исследования модели начинается с оценки результативности матрицы признаков – определения вклада каждого из элементов feature set в итоговый результат классификации **(рисунок 3, таблица 2)**.

На основании проведенного анализа вклада признаков в результат классификации сформированы оценки их индивидуальной и накопленной значимости **(рисунок 4)**.

Для достижения порога 95% важности влияния количества признаков на результат классификации необходимо учитывать верхнюю часть списка из 48 признаков, на последующих этапах исследования нижняя часть ранжированного списка может быть исключена из модели.

В качестве основных метрик исследуемой модели используются:

- *accuracy* (точность) – метрика, измеряющая долю правильных предсказаний модели от общего числа всех предсказаний (отношение количества верно классифицированных наблюдений к общему количеству наблюдений);
- *precision* (точность) – доля объектов, действительно принадлежащих классу, относительно всех объектов, которые модель отнесла к этому классу;
- *recall* (полнота) – доля объектов класса, которые модель правильно определила, относительно всех объектов этого класса;
- *F1-score* – гармоническое среднее между *precision* и *recall*.

На **рисунках 5, 6** показаны результирующие метрики исследуемой модели и их зависимость от длительности наблюдения трафика.



Рис. 2. Зависимость точности от размерности модели и числа узлов в листе

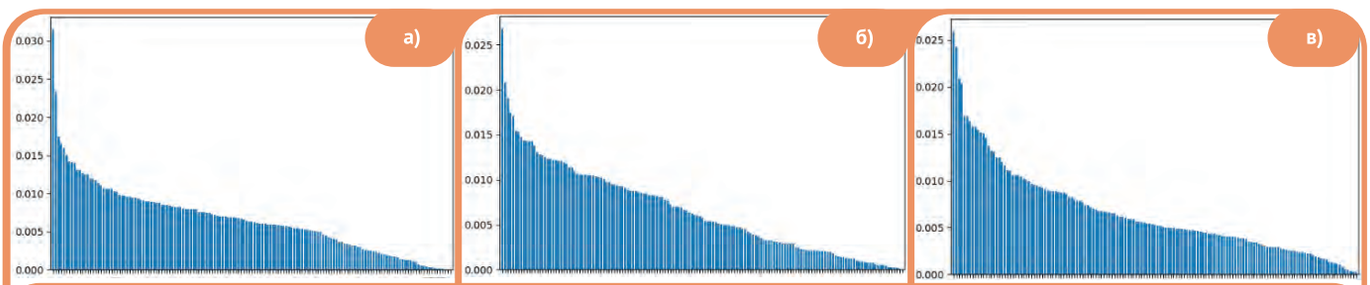


Рис. 3. Ранжирование матрицы признаков по вкладу в результат классификации для посекундной – а), попакетной – б) и попакетной статистики для раздельных симплексов – в).

Табл. 2. Ранжирование признаков по вкладу в результат классификации (top 10)

№ п/п	Посекундная статистика		Попакетная статистика		Попакетная статистика для раздельных симплексов	
1.	mL[0]	0.031551	mL[0]	0.026825	sumNp[1]	0.025946
2.	L[0][16]	0.023381	Lbin[0][0]	0.020772	stdL[0]	0.024246
3.	sumNp[1]	0.017452	L[0][1]	0.019019	Lbin[0][11]	0.020922
4.	sumL[1]	0.016621	L[1][16]	0.017405	Lbin[0][16]	0.020396
5.	Lbin[0][0]	0.015992	Lbin[1][16]	0.017062	Lbin[0][1]	0.016946
6.	stdL[1]	0.015045	Lbin[0][11]	0.015426	sumL[0]	0.016817
7.	mL[1]	0.014173	Lbin[0][7]	0.015339	Lbin[0][4]	0.016294
8.	L[1][16]	0.014130	Lbin[0][6]	0.014731	mL[0]	0.015861
9.	sumNp[0]	0.014058	sumL[0]	0.014354	Tbbin[1][0]	0.015773
10.	Tb[0][0]	0.013083	sumL[1]	0.014336	L[0][1]	0.015473

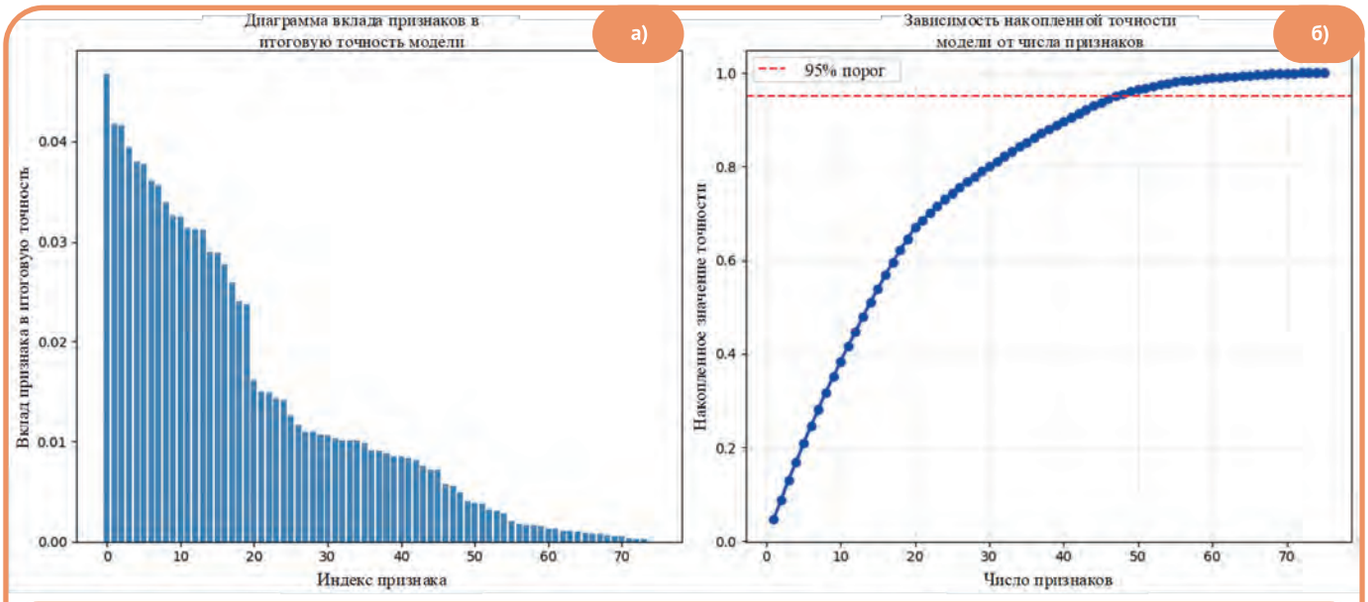


Рис. 4. Индивидуальная – а) и накопленная – б) значимость признаков.

а)

ОЦЕНКА МОДЕЛИ НА ТЕСТОВЫХ ДАННЫХ

Accuracy: 0.9082
Precision: 0.9136
Recall: 0.9082
F1-score: 0.9076

Детальный отчет по классам:

	precision	recall	f1-score	support
amazon-chime	0.86	1.00	0.92	24
discord	0.89	0.97	0.93	32
google-meet	1.00	1.00	1.00	12
isq	0.95	0.95	0.95	20
jitsi	0.91	0.91	0.91	23
mts-link	1.00	0.97	0.98	32
odnoklassniki	1.00	0.75	0.86	8
sber-jazz	0.87	0.87	0.87	15
signal-ows	1.00	0.89	0.94	9
skype	1.00	0.64	0.78	11
slack	1.00	0.83	0.91	12
snapchat	0.93	1.00	0.97	14
telegram	0.92	0.92	0.92	25
viber	0.78	0.88	0.83	33
vk-messenger	0.80	0.71	0.75	17
wb	0.97	0.97	0.97	32
webex	0.90	0.92	0.91	39
whatsapp	1.00	0.83	0.91	24
ya-telemost	0.79	0.90	0.84	21
accuracy			0.91	403
macro avg	0.92	0.89	0.90	403
weighted avg	0.91	0.91	0.91	403

б)

ОЦЕНКА МОДЕЛИ НА ТЕСТОВЫХ ДАННЫХ

Accuracy: 0.9073
Precision: 0.9103
Recall: 0.9073
F1-score: 0.9054

Детальный отчет по классам:

	precision	recall	f1-score	support
amazon-chime	0.81	0.92	0.86	24
discord	0.88	0.96	0.92	48
google-meet	1.00	1.00	1.00	12
isq	1.00	0.95	0.97	20
jitsi	0.85	0.92	0.88	24
mts-link	0.97	1.00	0.99	33
odnoklassniki	0.60	0.50	0.55	12
sber-jazz	0.93	0.87	0.90	15
signal-ows	1.00	0.77	0.87	13
skype	0.94	0.85	0.89	39
slack	0.88	0.58	0.70	12
snapchat	1.00	1.00	1.00	18
telegram	0.82	0.99	0.90	75
viber	0.89	0.84	0.86	38
vk-messenger	0.78	0.67	0.72	21
wb	1.00	0.97	0.98	32
webex	1.00	0.90	0.95	39
whatsapp	0.95	1.00	0.97	54
ya-telemost	1.00	0.86	0.92	21
accuracy			0.91	550
macro avg	0.91	0.87	0.89	550
weighted avg	0.91	0.91	0.91	550

в)

ОЦЕНКА МОДЕЛИ НА ТЕСТОВЫХ ДАННЫХ

Accuracy: 0.8994
Precision: 0.8980
Recall: 0.8994
F1-score: 0.8968

Детальный отчет по классам:

	precision	recall	f1-score	support
amazon-chime	0.78	0.93	0.85	43
discord	0.92	0.91	0.92	92
google-meet	0.96	1.00	0.98	24
isq	0.82	0.92	0.87	39
jitsi	0.83	0.94	0.88	47
mts-link	0.95	0.92	0.93	62
odnoklassniki	0.59	0.54	0.57	24
sber-jazz	0.88	0.70	0.78	30
signal-ows	0.82	0.67	0.74	21
skype	0.94	0.94	0.94	77
slack	0.83	0.65	0.73	23
snapchat	1.00	0.94	0.97	35
telegram	0.94	0.97	0.95	148
viber	0.88	0.87	0.87	76
vk-messenger	0.74	0.56	0.64	41
wb	0.94	0.97	0.95	64
webex	0.97	1.00	0.99	78
whatsapp	0.92	0.97	0.95	107
ya-telemost	0.90	0.84	0.87	43
accuracy			0.90	1074
macro avg	0.87	0.85	0.86	1074
weighted avg	0.90	0.90	0.90	1074

Рис. 5. Экспериментально полученные метрики модели для посекундной – а), попакетной – б) и попакетной статистики для раздельных симплексов – в).

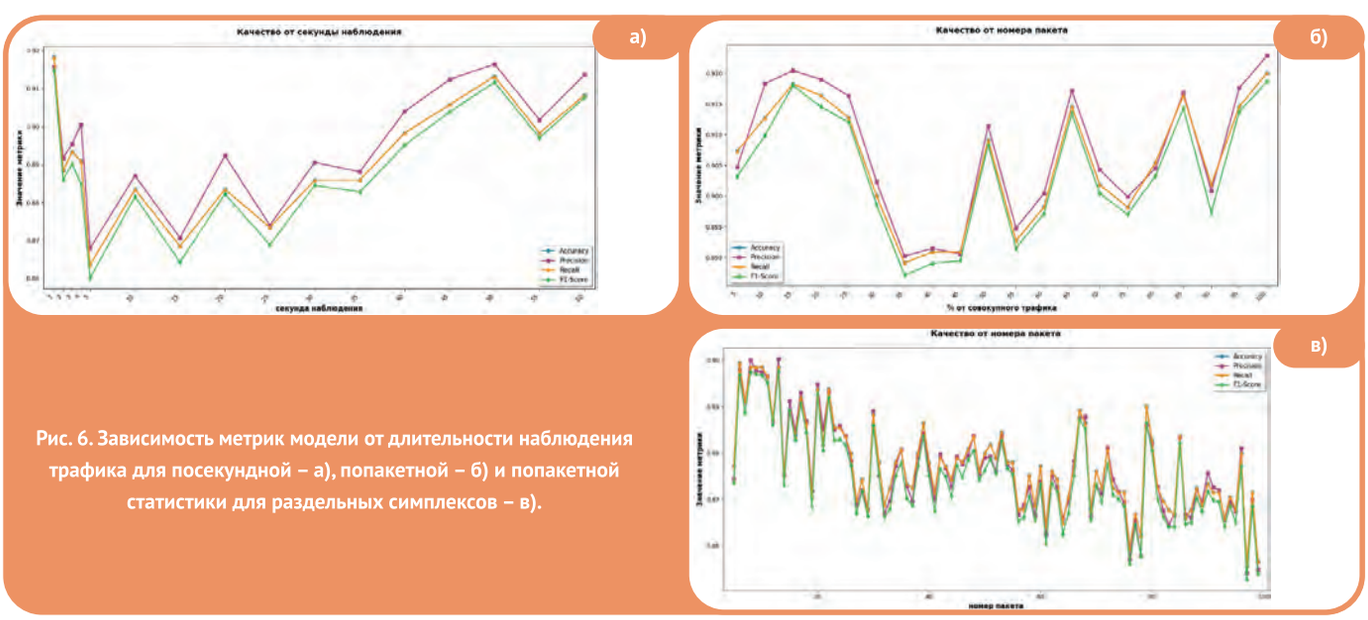


Рис. 6. Зависимость метрик модели от длительности наблюдения трафика для посекундной – а), попакетной – б) и попакетной статистики для раздельных симплексов – в).

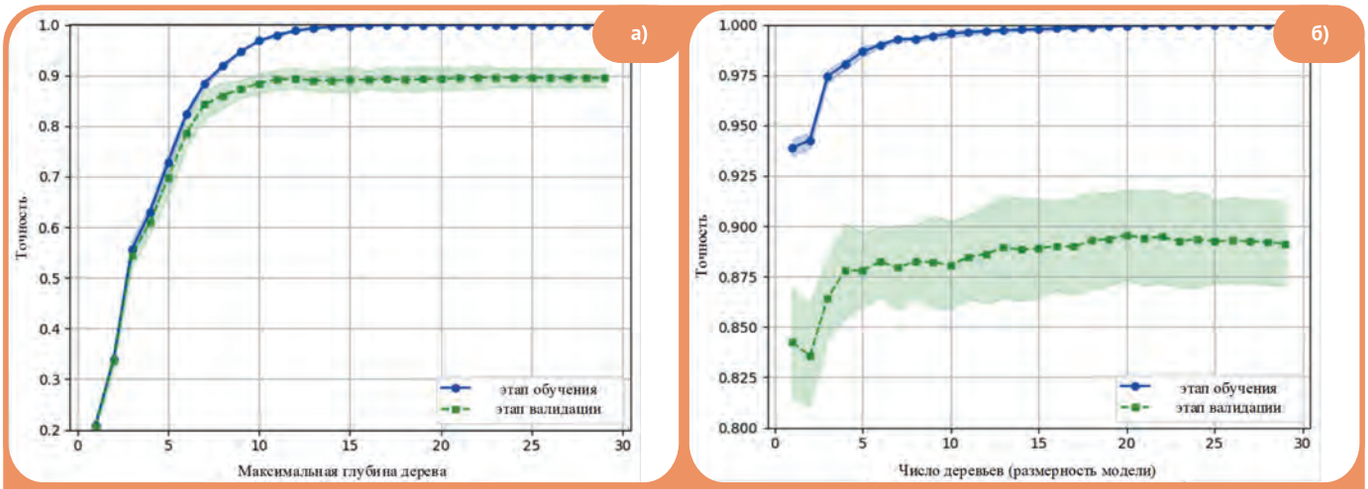


Рис. 7. Зависимость точности от глубины деревьев при n_estimators=20 – а) и от числа деревьев при max_depth=22 – б).

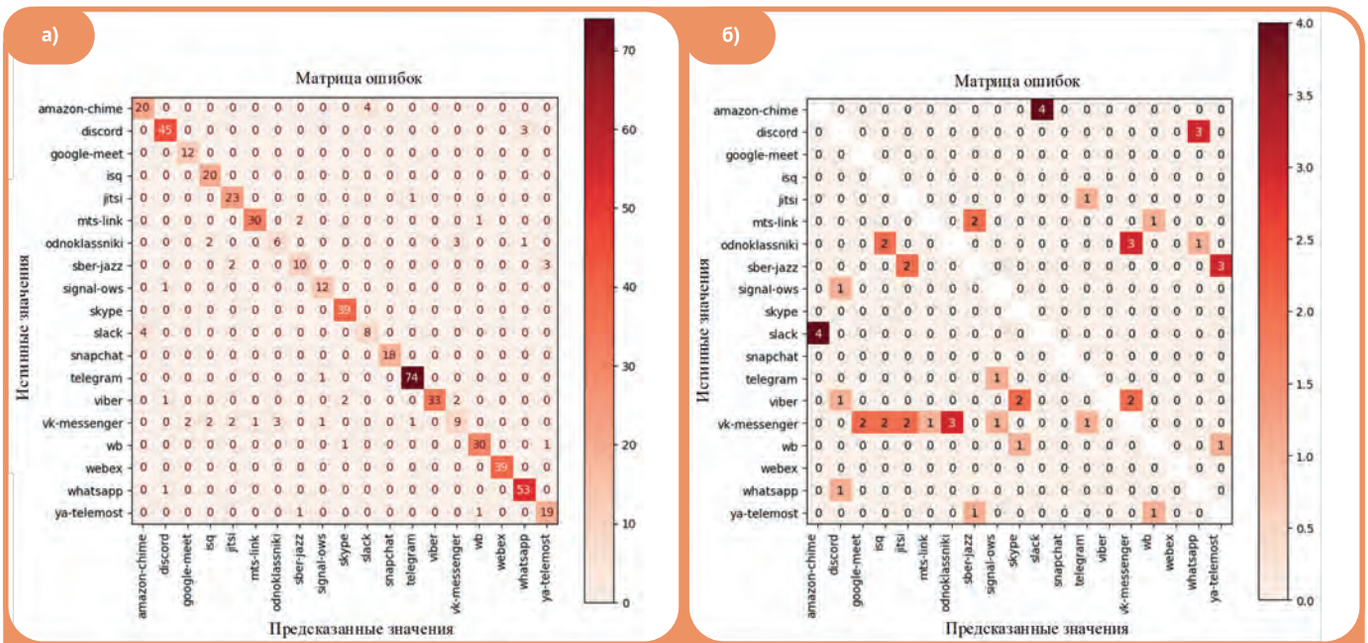


Рис. 8. Матрица неточностей – а) и матрица неточностей с удаленными диагональными элементами – б) при n_estimators=20 и max_depth=22.

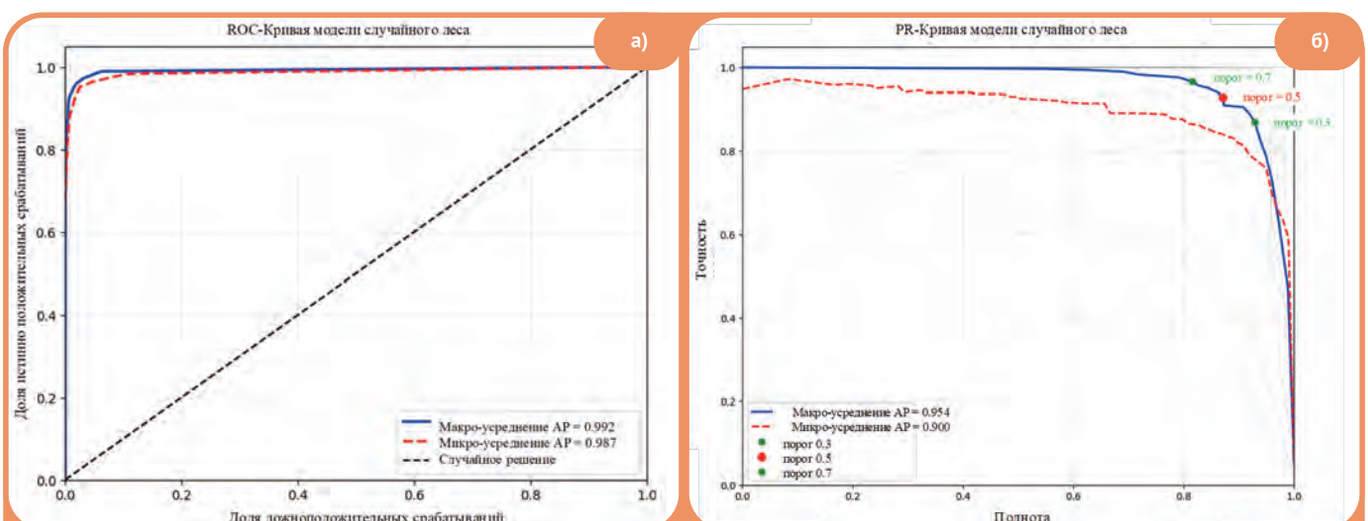


Рис. 9. ROC кривая – а) и PR кривая – б) при n_estimators=20 и max_depth=22.

Оценка полученных результатов анализа метрик модели позволяет сделать вывод о том, что предложенный способ накопления статистики достигает максимума точности на 8-ом пакете дуплексной сессии (в среднем по всем сервисам). На основании данного вывода и с учетом ранжирования признаков классификации формируется набор исходных данных – структурно-временные характеристики информационного обмена, содержащих статистику сессий, накопленную к 8-му пакету. В ходе исследования модели на обновленном наборе устанавливаются рациональные значения её параметров **(рисунок 7)**:

- *n_estimators=20;*
- *max_depth=22.*

На основании анализа матрицы ошибок **(рисунок 8)** рассчитываются основные метрики качества модели.

Кривая ROC (англ. Receiver Operating Characteristic) – график, иллюстрирующий производительность классификационной модели при всех возможных порогах классификации. Ось абсцисс данного графика представляет собой FPR, т.е. ложноположительную частоту, а ось ординат – TRP (recall), т.е. истинноположительную частоту. Показатель AUC (англ. Area Under the ROC Curve) – мера, суммирующая производительность модели одним числом, измеряя площадь под кривой ROC.

На **рисунке 9-а** отображены 2 зависимости: micro-average (микро-среднее) и macro-average (макро-среднее). Кривая ROC изначально используется в бинарной классификации. В условиях рассматриваемого эксперимента исследуются 19 классов и для того, чтобы построить ROC, требуется свести задачу к бинарной. С этой целью обычно используется стратегия OVR (англ. One-vs-Rest):

- берется «класс №1» против «остальных», производится расчёт и построение ROC;
- берется «класс №2» против «остальных», производится расчёт и построение ROC;
- и т.д.

В итоге образуется множество кривых. Отображать их на одном графике визуально не удобно, поэтому производится усреднение 2-мя способами:

1. *micro-average* (микро-среднее):
   - суть: выбираются показания для всех 19 классов и рассчитываются общие TP, FP, FN;
   - смысл: глобальная оценка точности;
   - в мультиклассовых задачах *micro-average* ROC зачастую совпадает с accuracy;

2. *macro-average* (макро-среднее):
   - суть: AUC рассчитывается для каждого класса отдельно и берётся среднее арифметическое;
   - смысл: все классы равнозначны, независимо от того сколько для него примеров в исходном наборе данных; в случае если модель плохо обучена на «маленьком» наборе, *macro-average* упадёт даже при высоком *micro-average*.

Анализ ROC на рисунке 9-а показывает, что исследуемая модель работает одинаково хорошо на всех классах. Иначе, если бы модель отлично «знала» Telegram и совсем «не знала» Whatsapp, кривая macro-average снизилась бы, тогда как micro-average осталась бы на прежнем уровне.

Зависимость метрик модели от количества обрабатываемых пакетов в дуплексном соединении при *n_estimators=20* и *max_depth=22* показана на **рисунке 10**.

3.4. ОБУЧЕНИЕ И ИССЛЕДОВАНИЕ МОДЕЛИ CATBOOST

В рамках эксперимента выполнено обучение и исследование модели CatBoost. Бустинг – это ансамблевый метод машинного обучения, целью которого является объединение нескольких слабых моделей предсказания для создания одной сильной. Градиентный бустинг CatBoost соединяет последовательно несколько классификаторов (как правило неглубоких деревьев) и обещает [6] качество классификации выше бэггинга случайного леса.

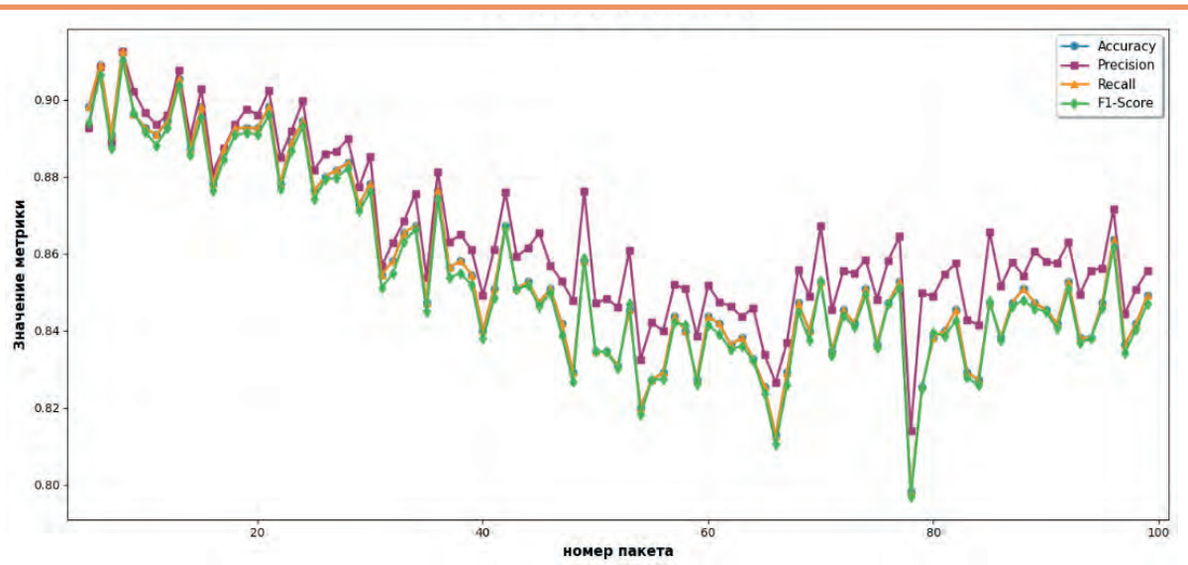


Рис. 10. Зависимость метрик модели от длительности наблюдения трафикапри n_estimators=20 и max_depth=22.

Результаты обучения модели на тестовых данных с зафиксированными параметрами с числом деревьев 149 представлены на **рисунке 11**. Результирующие метрики исследуемой модели приведены в **таблице 3**.

На основании анализа метрик модели CatBoost можно сделать следующие выводы:

- бустинг на деревьях не принес существенного выигрыша по качеству относительно базовой модели;
- в последующих экспериментах следует оценить производительность конечной модели и провести сравнение с результатом случайного леса (бэггинга на деревьях).

3.5. РЕЗУЛЬТАТЫ И ВЫВОДЫ

Результаты исследования базовой модели случайный лес позволяют сделать следующие выводы.

1. Метрики модели находятся на высоком уровне **(таблица 4)**.
2. Детализация по классам так же показывает хорошие результаты **(рисунок 5)**.
3. Зависимость метрик от секунды наблюдения трафика показывает, что первые 5 секунд обеспечивают качество порядка 88%, и далее оно постепенно увеличивается до 92% к 55 секунде. Отдельный интерес представляет пик качества на 1 секунде наблюдения трафика, который на 2-ой секунде стремительно деградирует. Возможная причина может заключаться в статистических свойствах установочных пакетов STUN или стартовых кодовых слов полезной нагрузки. Данная особенность подлежит дальнейшему исследованию.
4. Зависимость метрик от номера пакета в симплексном соединении показывает, что первые 15 пакетов обеспечивают качество порядка 92%, и далее с увеличением объема данных оно не демонстрирует устойчивого роста.

Примечание: Значение 15 – это не 15 пакетов в отдельном симплексе, а более сложная величина: статистика копится до достижения 100 пакетов хотя бы по одному из направлений, и потом от общего числа поступивших пакетов по обоим симплексам (то есть в дуплексе) берутся первые 15% пакетов, и производится расчет по каждому симплексу. Подобное усложнение реализовано для сохранения общности форматов с первой (посекундной) частью эксперимента.

5. Зависимость метрик от номера пакета в дуплексном соединении соответствует выявленной зависимости в симплексах. При этом рациональным значением количества пакетов для накопления статистики является 8 **(рисунок 10)** – далее происходит избыточное накопление статистики, и качество постепенно деградирует.
6. Дальнейшие направления исследований могут быть посвящены:

- изучению зависимости метрик модели от числа бинов в гистограмме (в настоящем эксперименте это значение зафиксировано на уровне 17);
- формированию обучающего набора данных большего размера и уточнению результатов в ходе кросс-валидационной проверки;

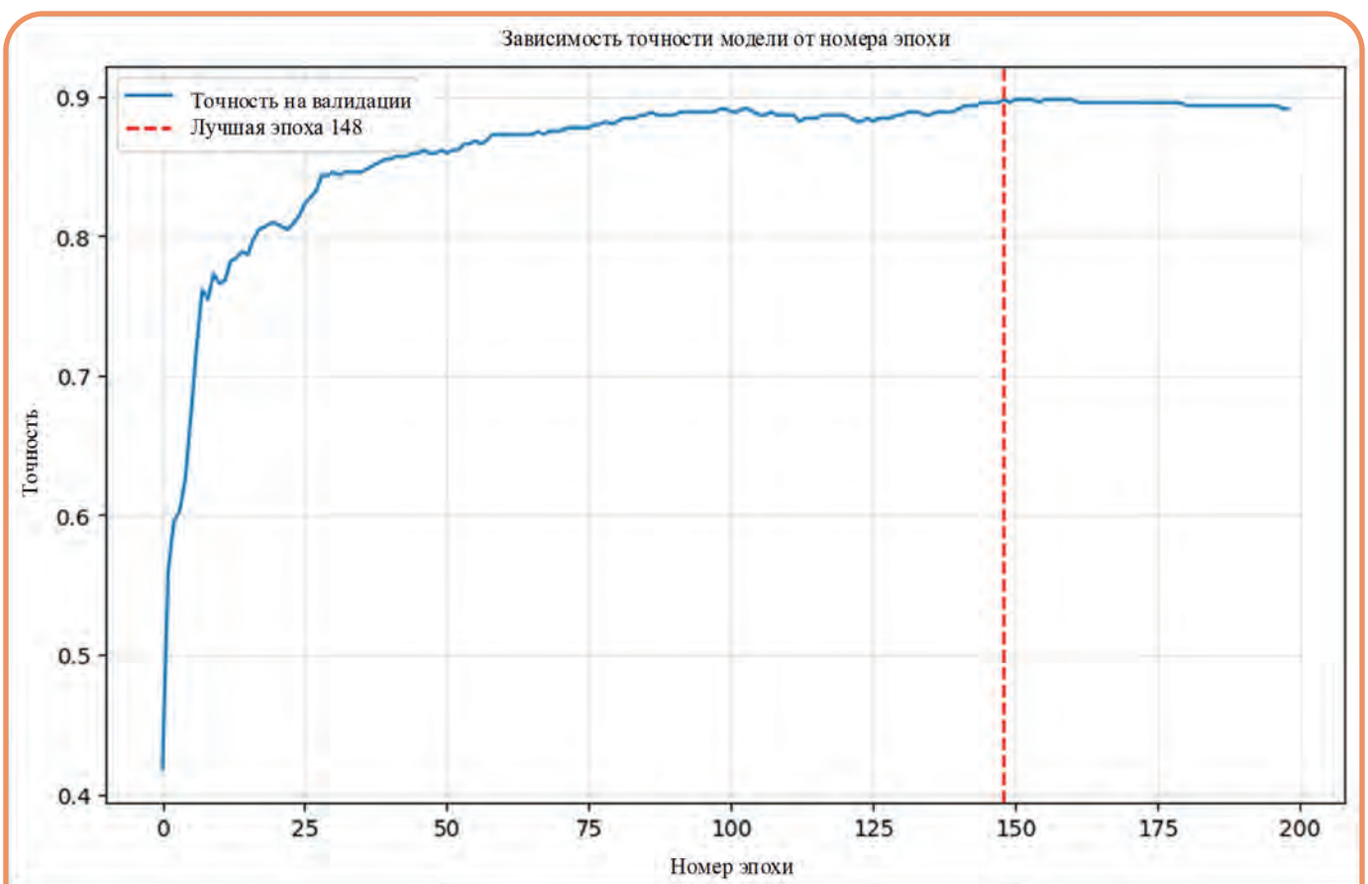


Рис. 11. Результаты обучение модели CatBoost с ранним остановом.

Табл. 3. Результирующие метрики модели CatBoost

№ п/п	Метрика	Значение
1.	accuracy	0.91
2.	precision	0.91
3.	recall	0.91
4.	F1-score	0.91

Табл. 4. Результирующие метрики модели Random Forest

№ п/п	Метрика	Значение
1.	accuracy	0.9082
2.	precision	0.9136
3.	recall	0.9082
4.	F1-score	0.9076

- изучению влияния исключения малоинформативных признаков из нижней части ранжированного списка на качество и быстродействие модели;
- классификации медиа трафика по последовательности STUN атрибутов, дополненных информацией о дельте времени между пакетами и длиной пакета.

4. ЗАКЛЮЧЕНИЕ

Из приведённого обзора отдельно взятого решения по классификации трафика сервисов мгновенного обмена сообщениями из состава DPI Engine TrACE TA можно сделать ряд выводов. Необходимо констатировать, что особенности современного этапа развития инфраструктуры сетевых сервисов в целом и функционирования цифровых сервисов мгновенного обмена сообщениями в российском сегменте сети Интернет в частности определяют для участников технического сообщества ряд вызовов. Проблема контроля доступа к ресурсам сети Интернет актуальна и имеет важное прикладное значение, особенно в условиях наблюдения анонимизированного на уровне протоколов трафика. Для решения известных проблем классификации широкое распространение получили технологии машинного обучения. Вместе с тем процессы разработки и внедрения ML решений для классификации сетевого трафика требуют подбора конкретных моделей и 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 классификации с одной стороны и производительности с другой.

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 не только для классификации трафика большинства современных сервисов мгновенного обмена сообщениями, но и для идентификации типов передаваемых пользовательских данных с возможностью определения фактов обмена текстовыми сообщениями, совершения аудио и видеозвонков, передачи файлов.

СПИСОК ЛИТЕРАТУРЫ

1. Полунин А.В. Особенности классификации сетевого трафика в российском сегменте сети Интернет. Документальная электросвязь, № 35, 2025г., стр. 25-30.
2. Гетьман А.И., Иконникова М.К. Обзор методов классификации сетевого трафика с использованием машинного обучения. Труды ИСП РАН, том 32, вып. 6, 2020г., стр. 137-154. DOI: 10.15514/ISPRAS–2020–32(6)–11.
3. Гетьман А.И., Иконникова М.К. Идентификация прозрачных, сжатых и шифрованных данных в сетевом трафике. Труды ИСП РАН, том 33, вып. 4, 2021 г., стр. 31-48. DOI: 10.15514/ISPRAS–2021–33(4)–3.
4. Шелухин О.И., Барков В.В., Полковников М.В. Классификация зашифрованного трафика мобильных приложений методом машинного обучения. Вопросы кибербезопасности, № 4(28), 2018 г., стр. 21-28. DOI: 10.21681/2311–3456–2018–4–21–28.
5. KNIME Analytics Platform. [Электронный ресурс] – Режим доступа: URL: https://www.knime.com/knime-analytics-platform (17.04.2026).
6. CatBoost. [Электронный ресурс] – Режим доступа: URL: https://habr.com/ru/companies/otus/articles/778714/?ysclid=ms76pfuxxo611623258 (21.05.2026).



ДМИТРИЙ ПЕТРОВ
генеральный директор
ООО «Комфортел»

ЭКОНОМИКА ОТКАЗОУСТОЙЧИВОСТИ ЦИФРОВОЙ ИНФРАСТРУКТУРЫ: РИСК-ОРИЕНТИРОВАННЫЙ ПОДХОД

АННОТАЦИЯ
Рост зависимости организаций от цифровой инфраструктуры требует перехода от традиционных подходов к обеспечению надежности к управлению непрерывностью цифровых сервисов. В статье предложен риск-ориентированный подход к оценке экономической эффективности инвестиций в отказоустойчивость, основанный на сопоставлении затрат на обеспечение цифровой устойчивости и потенциального ущерба от простоев. Практическая применимость подхода продемонстрирована на примере гостиничного комплекса. Предложенный подход может быть использован при проектировании и модернизации цифровой инфраструктуры организаций телекоммуникационной отрасли, банковского сектора и других отраслей.

КЛЮЧЕВЫЕ СЛОВА:
цифровая инфраструктура, цифровая устойчивость, отказоустойчивость, управление рисками, непрерывность бизнеса, SLA, RTO, RPO.

1. ОТ РЕЗЕРВИРОВАНИЯ К ЦИФРОВОЙ УСТОЙЧИВОСТИ

Цифровая экономика характеризуется высокой зависимостью бизнеса, органов государственной власти и общества от стабильной работы информационно-телекоммуникационной инфраструктуры. Нарушение доступности цифровых сервисов приводит не только к техническим сбоям, но и к финансовым потерям, остановке бизнес-процессов и снижению качества предоставляемых услуг.

По мере усложнения цифровой среды меняется и понимание отказоустойчивости. Если ранее основной задачей считалось резервирование отдельных элементов инфраструктуры, то сегодня приоритетом становится обеспечение непрерывности цифровых сервисов независимо от характера возникающих инцидентов [1, 2].

Под цифровой устойчивостью в настоящей работе понимается способность информационно-телекоммуникационной инфраструктуры обеспечивать непрерывную работу критически важных сервисов при возникновении технических, программных, организационных или кибернетических нарушений за счет комплекса инженерных, организационных и экономических мер.

Современная цифровая инфраструктура объединяет телекоммуникационные сети, облачные платформы, центры обработки данных, программные сервисы и средства информационной безопасности. Причинами инцидентов могут выступать ошибки программного обеспечения, некорректные обновления, человеческий фактор, кибератаки и нарушения в работе взаимосвязанных цифровых компонентов. Для распределённых и IoT-сред существенны также особенности архитектуры и управления нагрузкой [3, 4].

По мере усложнения инфраструктуры снижается эффективность простого наращивания резервов. Дополнительные элементы резервирования уже не обеспечивают пропорционального роста надежности, поскольку вероятность отказов определяется совокупностью взаимосвязанных технических, программных и организационных факторов [1, 3].

В этих условиях отказоустойчивость становится одним из ключевых инструментов обеспечения цифровой устойчивости, позволяющим управлять рисками нарушения непрерывности цифровых сервисов и принимать инвестиционные решения с учетом их экономической эффективности. В настоящей работе предлагается подход, основанный на сопоставлении стоимости резервирования и потенциального ущерба от нарушения непрерывности цифровых сервисов, что позволяет использовать количественные критерии при выборе архитектуры цифровой инфраструктуры [5].

2. ЭКОНОМИКА ОТКАЗОУСТОЙЧИВОСТИ: СТОИМОСТЬ ПРОСТОЯ И ПРИНЯТИЕ ИНВЕСТИЦИОННЫХ РЕШЕНИЙ

На начальном этапе инвестиции в резервирование обеспечивают значительное снижение рисков. Например, организация второго независимого канала связи существенно уменьшает вероятность полной потери доступа к сети. Однако дальнейшее повышение уровня доступности требует непропорционального роста затрат. Если достижение доступности 99,9 % обычно связано с умеренными инвестициями, то обеспечение уровня 99,99 % и особенно 99,999 % требует значительно больших расходов на оборудование, каналы связи, инженерную инфраструктуру и сопровождение. Поэтому решение о резервировании должно приниматься не исходя из максимально возможного уровня надежности, а на основе оценки его экономической эффективности и с учетом требований регуляторов.

Стоимость простоя как интегральный показатель риска
Ключевым критерием выбора архитектуры цифровой инфраструктуры является стоимость недоступности цифровых сервисов. Совокупный ущерб от инцидента определяется по формуле:
СП = ПВ + ШС + РП + ИВ,
где:
СП – совокупная стоимость простоя;
ПВ – прямые потери выручки;
ШС – штрафные санкции и компенсационные выплаты;
РП – репутационные потери;
ИВ – издержки восстановления работоспособности.

Предлагаемая модель учитывает как прямые финансовые потери, так и косвенные последствия нарушения непрерывности цифровых сервисов. Для операторов связи, банков, предприятий сферы услуг и других организаций репутационные потери и снижение доверия клиентов нередко оказываются сопоставимыми с прямым финансовым ущербом [2].

Современная практика управления непрерывностью бизнеса использует показатели:
- RTO (Recovery Time Objective) – максимально допустимое время восстановления цифрового сервиса;
- RPO (Recovery Point Objective) – максимально допустимый объем потери данных [6,7].

Использование этих показателей позволяет перейти от оценки надежности отдельных технических компонентов к оценке доступности цифровых сервисов, обеспечивающих выполнение критически важных бизнес-процессов.

Типовой алгоритм включает: определение критически важных цифровых сервисов, идентификацию возможных угроз, оценку вероятности возникновения инцидентов, расчет потенциального ущерба, выбор мероприятий по обеспечению цифровой устойчивости с учетом их экономической эффективности.

Рост числа киберинцидентов, использование облачных платформ и зависимость организаций от внешних поставщиков цифровых сервисов делают такой подход особенно актуальным. Независимо от причины инцидента – кибератаки, ошибки обновления программного обеспечения, сбоя облачной инфраструктуры или человеческого фактора – определяющим для организации остается влияние на непрерывность цифровых сервисов и связанные с этим финансовые последствия [3, 5].

3. ОЦЕНКА ЭКОНОМИЧЕСКОЙ ЭФФЕКТИВНОСТИ ОБЕСПЕЧЕНИЯ ЦИФРОВОЙ УСТОЙЧИВОСТИ (НА ПРИМЕРЕ ГОСТИНИЧНОГО КОМПЛЕКСА)

Практическая применимость предложенной методики проиллюстрирована на условном примере гостиничного комплекса, цифровая инфраструктура которого обслуживается оператором связи. Выбор объекта обусловлен высокой зависимостью гостиничного бизнеса от непрерывной работы информационно-телекоммуникационных сервисов.

Гостиничный комплекс использует взаимосвязанные цифровые сервисы – онлайн-бронирование, PMS, эквайринг, IP-телефонию, контроль доступа, видеонаблюдение и гостевой Wi-Fi. Нарушение их доступности способно затронуть обслуживание клиентов и операционные процессы; конкретный состав систем определяется используемой архитектурой объекта [2, 6].

ИСХОДНЫЕ ДАННЫЕ

В качестве расчетного примера рассматривается гостиничный комплекс, включающий пять объектов. Для целей моделирования принимаются исходные показатели, приведенные в **таблице 1**.

Табл. 1. Исходные данные расчетной модели

Метрика	Значение
Количество объектов	5
Годовая выручка	3,85 млрд руб.
Среднегодовая выручка одного объекта	770 млн руб.
Среднемесячная выручка одного объекта	64,167 млн руб.
Средняя загрузка	95 %

Поскольку гостиничный комплекс функционирует круглосуточно, средняя часовая выручка (Вч) одного объекта составляет:
Вч = 64 167 000 / 720 = 89 121 руб./час.

Предполагается, что 85 % бизнес-процессов зависят от бесперебойной работы цифровой инфраструктуры. Тогда прямые потери выручки (ПВч) при недоступности цифровых сервисов составят:
ПВч = 89 121 × 0,85 = 75 753 руб./час.

РАСЧЕТ СТОИМОСТИ ПРОСТОЯ

В качестве типового сценария рассматривается инцидент продолжительностью 4 часа.

Прямые потери выручки определяются как:
ПВ = 75 753 × 4 = 303 012 руб.

Помимо прямых потерь учитываются расходы на восстановление работоспособности, компенсационные выплаты и репутационные потери.

Совокупная стоимость простоя с учетом указанных компонентов представлена в **таблице 2**.

Все параметры расчётного примера являются условными допущениями и используются для демонстрации работы методики. При практическом применении значения должны определяться по данным бухгалтерского, операционного и технического учёта организации.

Табл. 2. Расчет совокупной стоимости простоя

Компонент ущерба	Значение
Прямые потери выручки	303 012 руб.
Компенсационные выплаты	80 000 руб.
Репутационные потери	224 500 руб.
Восстановление работоспособности	25 000 руб.
Совокупный ущерб	**632 512 руб.**

Для дальнейших расчетов значение округляется до 632,5 тыс. руб., а стоимость одного часа простоя (Спч) составляет:
Спч = 632 500 / 4 = 158 125 руб./час.

Полученные результаты показывают, что даже непродолжительная недоступность цифровых сервисов приводит к существенным финансовым потерям, сопоставимым со стоимостью мероприятий по обеспечению цифровой устойчивости.

ОЦЕНКА ЭКОНОМИЧЕСКОЙ ЭФФЕКТИВНОСТИ

В качестве типового решения рассматривается комплекс мероприятий, включающий резервный канал связи через независимого оператора, резервирование пограничного оборудования, автоматическое переключение на резервный маршрут, круглосуточный мониторинг инфраструктуры и регламентированные процедуры аварийного восстановления.

Стоимость такого решения составляет 35 тыс. руб. в месяц, или 420 тыс. руб. в год на один объект.

При предотвращении одного значимого инцидента в течение года экономический эффект определяется следующим образом:
Э = 632 500 – 420 000 = 212 500 руб./год.

Коэффициент возврата инвестиций для такого случая составляет:
ROI = (212 500 / 420 000) × 100 % = 50,6 %.
Срок окупаемости проекта составит:
420 000 / (632 500 / 12) ≈ 8 месяцев.

Следовательно, предотвращение даже одного значимого инцидента в течение года обеспечивает положительный экономический эффект и делает инвестиции в обеспечение цифровой устойчивости экономически оправданными.

ВЫБОР УРОВНЯ ЗАЩИТЫ

Экономически оправданный уровень защиты определяется сравнением годовой стоимости резервирования (TCOreserve) и ожидаемого ущерба от ИТ-инцидентов.

Годовая стоимость резервирования рассчитывается по формуле:
TCOreserve = CapEx / N + OpEx,
где CapEx – капитальные затраты на создание системы резервирования;
N – срок эксплуатации оборудования;
OpEx – ежегодные эксплуатационные расходы.

Потенциальный годовой ущерб определяется выражением:
ПУ = СП × К,
где СП – стоимость одного инцидента; К – ожидаемое количество инцидентов в течение года.

Например, если по статистике в год происходит два инцидента (К=2), то для одного объекта:
ПУ = 632 500 × 2 = 1 265 000 руб.

Сравнивая эту величину с годовой стоимостью резервирования (420 000 руб.), получаем экономический эффект 845 000 руб. и ROI > 201,2 %. Каждое предприятие должно определить пороговое значение Кпорог =ТСО/СП, выше которого резервирование экономически оправдано.
В нашем примере
Кпорог = 420 000/632 500 = 0,66,
то есть достаточно одного инцидента в 1,5 года для окупаемости.

Сопоставление совокупной годовой стоимости различных уровней защиты и соответствующих пороговых значений приведено в **таблице 3**.

Табл. 3. Расчет совокупной годовой стоимости обеспечения отказоустойчивости для типовых уровней защиты

Уровень защиты	Типовое решение	TCOreserve, руб./год	Кпорог
Базовый	Резервный канал связи	150 тыс.	0,24 (1 инцидент в 4 года)
Стандартный	Два независимых канала + резервное оборудование	420 тыс.	0,66 (1 инцидент в 1,5 года)
Повышенный	Автоматическое переключение + георезервирование	1,5 млн.	2,37 (2–3 инцидента в год)
Критический	Географически распределенная инфраструктура + резервный ЦД	6 млн.	9,49 (около 10 инцидентов в год)

*Срок эксплуатации оборудования (N) – 5 лет

Таким образом, выбор архитектуры обеспечения отказоустойчивости определяется сопоставлением совокупной стоимости резервирования (TCOreserve) и потенциального годового ущерба от ИТ-инцидентов. Если ожидаемые потери превышают стоимость обеспечения цифровой устойчивости, инвестиции в резервирование являются экономически оправданными.

Следует отметить, что подобный подход применим не только в гостиничной отрасли [5, 6]. Аналогичные принципы могут использоваться в банковском секторе, промышленности, здравоохранении, электронной коммерции и государственном управлении – везде, где непрерывность цифровых сервисов непосредственно влияет на финансовые результаты или выполнение социально значимых функций.

ЗАКЛЮЧЕНИЕ

Развитие цифровой экономики приводит к тому, что отказоустойчивость перестает быть исключительно технической характеристикой информационно-телекоммуникационной инфраструктуры и становится важным фактором устойчивости организаций. В этих условиях наращивание резервирования не всегда является экономически оправданным, что обусловливает переход к риск-ориентированному управлению цифровой устойчивостью.

Предложенная методика позволяет количественно оценивать целесообразность инвестиций в отказоустойчивость на основе сопоставления затрат на защитные мероприятия с ожидаемыми потерями от нарушения непрерывности цифровых сервисов. Такой подход создает основу для выбора уровня защиты с учетом не только технических требований, но и экономических последствий возможных ИТ-инцидентов.

Практическая применимость методики продемонстрирована на примере гостиничного комплекса. Расчеты показывают, что предотвращение одного значимого инцидента в течение года обеспечивает положительный экономический эффект: ROI превышает 50 %, а срок окупаемости составляет менее 8 месяцев.

Методика уже применяется в практической деятельности оператора связи «Комфортел»*. В частности, описанный подход был использован при оценке экономической эффективности обеспечения цифровой устойчивости гостиничного объекта. В настоящее время методика проходит практическое тестирование на других проектах, что позволяет уточнять расчетные параметры и оценивать возможности ее применения для различных типов объектов и отраслей.

Таким образом, предложенный подход может использоваться при проектировании и модернизации цифровой инфраструктуры организаций различных отраслей для экономического обоснования инвестиций в обеспечение ее устойчивости. Его дальнейшее практическое тестирование позволит сформировать накопленную базу расчетных параметров и повысить точность оценки экономической эффективности различных уровней защиты.

СПИСОК ЛИТЕРАТУРЫ

1. Путилов В. А., Маслобоев А. В., Быстров В. В. Методологическая база информационной поддержки управления безопасностью региональных критических инфраструктур // Труды Кольского научного центра РАН. Информационные технологии. 2021. Т. 12, № 5. С. 157–160. DOI: 10.37614/2307-5252.2021.5.12.014.
2. Борзаков Д. В. Цифровая трансформация комплаенс-менеджмента – стратегическое решение по обеспечению непрерывности бизнеса // Вестник ВГУ. Серия: Экономика и управление. 2021. № 3. С. 22–32. DOI: 10.17308/econ.2021.3/3523.
3. Воеводин В. А. Модель оценки функциональной устойчивости элементов информационной инфраструктуры для условий воздействия множества компьютерных атак // Информатика и автоматизация. 2023. Т. 22, № 3. С. 691–715. DOI: 10.15622/ia.22.3.8.
4. Глушак Е. В. Анализ отказоустойчивости в IoT-системах на основе туманных вычислений // Труды учебных заведений связи. 2026. Т. 12, № 2. С. 27–35. DOI: 10.31854/1813-324X-2026-12-2-27-35.
5. Татьянин М. Н. Выбор динамической модели управления рисками // Экономика и бизнес: теория и практика. 2024. № 10-2 (116). С. 101–104. DOI: 10.24412/2411-0450-2024-10-2-101-104.
6. ISO 22301:2019. Security and resilience – Business continuity management systems – Requirements.
7. ISO 22300:2021. Security and resilience – Vocabulary.

* ООО «Комфортел»
Оператор связи бизнес-класса
https://comfortel.pro/



АЛЕКСЕЙ БУНЬКОВ
руководитель Департамента перспективных исследований, правовой работы и обеспечения взаимодействия с экспертно-совещательными органами
АНО «ИРИ»



НАТАЛЬЯ САРАНКИНА
юрист-аналитик Департамента перспективных исследований, правовой работы и обеспечения взаимодействия с экспертно-совещательными органами
АНО «ИРИ»

РОССИЙСКИЙ РЫНОК ВИДЕОИГР И ИГРОВОГО ПО: АКТУАЛЬНЫЕ ТЕНДЕНЦИИ РАЗВИТИЯ

В последние годы видеоигры окончательно перестали восприниматься исключительно как развлечение и способ проведения досуга. Они стали перспективной отраслью инвестирования, профессиональным направлением спортивных соревнований (киберспорт), инструментом кадровой подготовки силовых структур (игры двойного назначения) и важным механизмом «мягкой силы», способным транслировать ценности и содействовать формированию современного образа страны.

По разным оценкам, объем российского рынка видеоигр в 2025 году достиг 200 млрд рублей[1]. При базовом сценарии его развития к 2030 году прогнозируется рост до 257 млрд рублей, при оптимистичном – до 327 млрд рублей, при консервативном – 203 млрд рублей[2].

Согласно исследованию Организации развития видеоигровой индустрии (ОРВИ)[3], Аналитического центра «НАФИ»[4] и видеоигрового холдинга ИФСИ, совокупная аудитория видеоигр составляет от 106 до 110 млн человек в возрасте 7 лет и старше (78–81% от численности населения РФ)[5].

В России продолжается работа по выработке государственного регулирования данного сектора экономики. В частности, принят Федеральный закон от 08.08.2024г. №330-ФЗ «О развитии креативных (творческих) индустрий в Российской Федерации», включивший деятельность по разработке ПО, компьютерных игр и видеоигр в перечень креативных индустрий[6].

Определенные меры по дальнейшему развитию отрасли закладываются в рамках поручений Президента Российской Федерации[7, 8], а также правительственных и ведомственных нормативных правовых актов.

Тем не менее, по доле рынка в денежном выражении Россия занимает лишь 2-3% от мирового рынка[9], по данным экспертов, озвученным на отраслевой конференции-выставке Play Port Fest 2025[10]. Это создает огромное поле для роста, развития собственных студий и экспорта контента, подчеркивает необходимость продолжения государственной и частной поддержки индустрии видеоигр и игрового ПО, а также политики импортозамещения ПО.

Согласно опросу представителей российской игровой индустрии, проведенному в 2025 году АНО «ИРИ»[11] совместно с профильными организациями, рынок видеоигр демонстрирует готовность к дальнейшему росту[12]. Для этого необходимы более доступные меры поддержки, активное продвижение на внешние рынки и развитие объединений, способных представлять

[1] https://rg.ru/2025/09/20/videoigrovoj-rynok-rossii-dostig-200-mlrd-rublej.html
[2] https://strategy.ru/research/research/analiz-rossiyskogo-i-mirovogo-rynkov-videoigr-77/
[3] https://forgamedev.ru/
[4] https://nafi.ru/
[5] https://gaminginrussia.forgamedev.ru/
[6] Федеральный закон от 08.08.2024 г. № 330-ФЗ «О развитии креативных (творческих) индустрий в Российской Федерации» // Российская газета. 2024. № 182.
[7] http://kremlin.ru/acts/assignments/orders/73070
[8] http://www.kremlin.ru/acts/assignments/orders/72053
[9] https://rg.ru/2025/09/20/videoigrovoj-rynok-rossii-dostig-200-mlrd-rublej.html
[10] https://playport.org/fest?ysclid=mshbmyryv6877951642
[11] https://ири.рф/
[12] https://apriori.games/dev-support/

интересы индустрии. Некоторые запросы со стороны отрасли уже выполнены. Например, в августе 2025 года АПРИОРИ[13] заключила меморандумы с крупнейшими китайскими игровыми компаниями об экспорте продукции, информационном сотрудничестве и нетворкинге[14].

АНО «ИРИ» в рамках своей деятельности на конкурсной основе распределяет государственные субсидии на создание и продвижение социально значимого интернет-контента, в том числе компьютерных игр. В частности, поддержка осуществляется путем проведения конкурса прототипов игр[15]. Данный инструмент позволяет получить участникам конкурса финансирование на создание демоверсии (до 15 млн рублей) или вертикального среза (до 7,5 млн рублей) – упрощенных или неполных версий игры, которые демонстрируют общую концепцию и ключевые элементы игры, либо полноценно реализованных фрагментов игры, доведенных до финального качества.

В конкурсах участвовать могут не только юридические лица и индивидуальные предприниматели, но и физические лица, что критически важно для инди-разработчиков, создающих игры самостоятельно, без финансовой или иной поддержки издателей, корпораций или больших игровых студий.

Консолидированные усилия государства, бизнеса и иных участников игровой отрасли по поддержке индустрии сопровождаются системной аналитической работой отраслевых организаций.

В рамках вышеупомянутого исследования «Поддержка игровой индустрии в России и за рубежом»[16] экспертами было опрошено более 200 представителей российской игровой индустрии – от независимых студий до крупных игроков рынка. В частности, были выявлены самые востребованные меры поддержки: помощь в продвижении (52,8%), налоговые льготы (47,2%) и гранты на разработку (45,1%).

Кроме того, основными барьерами развития индустрии **(рис. 1)** названы: жесткие требования (58%), сложность документации (57%) и непрозрачность процедур (44,4%).

Также участники индустрии показывают высокий интерес к экспорту контента – 58,8% **(рис. 2)**.

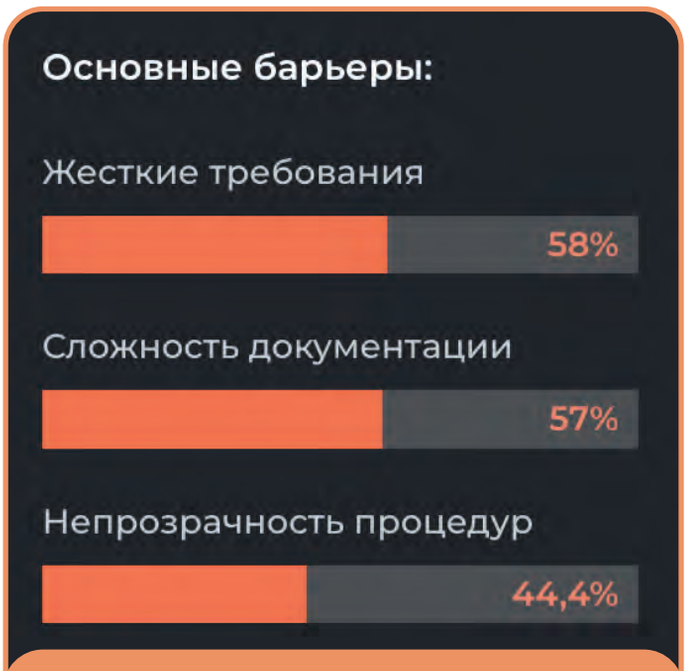


Рис. 1 Основные барьеры развития игровой индустрии в России по результатам проведенного исследования
Источник: https://apriori.games/dev-support/

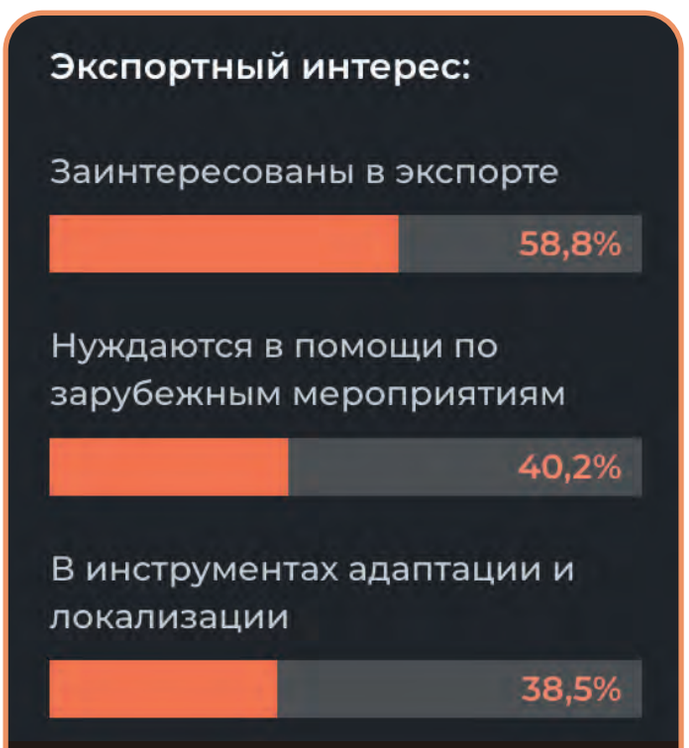


Рис. 2 Наиболее востребованные меры поддержки Российской игровой индустрии, связанные с экспортом
Источник: https://apriori.games/dev-support/

[13] https://apriori.games/
[14] https://apriori.games/news/memorandum_china/
[15] https://ири.рф/contests/otbor-prototipov-igr-2026/
[16] https://apriori.games/dev-support/

РАЗВИТИЕ ИКТ-ИНФРАСТРУКТУРЫ

В рамках исследования[17] была проведена оценка соответствия существующих в Российской Федерации мер поддержки запросам индустрии. На сегодняшний день в России действует многоуровневая система поддержки разработчиков видеоигр, реализуемая как через государственные органы (Минцифры России), так и через отраслевые и частные структуры (АПРИОРИ, РВИ[18], VK[19], 1С[20] и др.), а также с привлечением институтов развития (РФРИТ[21], ИРИ, РЭЦ[22], АСИ[23]).

Для выявления лучших практик и возможных направлений развития национальной поддержки геймдева в рамках исследования были проанализированы меры, применяемые в ведущих странах мира, включая Австрию, Канаду, Великобританию, Китай, США, Казахстан и другие **(рис. 3)**. В частности, были выявлены лучшие меры поддержки и страны-лидеры по ним. Анализ зарубежных практик показывает, что успешные страны сочетают финансовые стимулы с поддержкой рекламы, маркетинга и экспорта, а также с развитием инфраструктуры и подготовкой кадров.

По итогам исследования стало ясно, что ключевыми направлениями для развития индустрии видеоигр и игрового ПО должны стать выработка национальной стратегии игровой индустрии, запуск региональных кластеров и акселераторов, системная работа с экспортом, правовая защита и снятие барьеров при международных расчетах.

В отдельных регионах и макрорегионах России прорабатываются проекты создания центров компетенций для оказания экспертной поддержки компаниям по вопросам участия в различных конкурсных мероприятиях.

В ходе еще одного исследования «ИТ-ландшафт российской игровой индустрии», проведенного АНО «ИРИ», АПРИОРИ и Фондом «Сколково», был проведен опрос 140 представителей индустрии.

В рамках исследования было установлено, что отечественные студии активно работают с широким спектром платформ, жанров и форматов. На рынке сохраняется спрос на локальные и международные каналы дистрибуции игрового контента, а разработчики активно сочетают несколько каналов для расширения охватов аудитории.

Исследование также показало значительный потенциал для расширения локальных и open-source решений в области игровых сервисов, инфраструктурных инструментов, ИИ-технологий, а также облачных и хостинг-платформ для задач геймдева.

Не менее важным выводом исследования является установление факта высокой зависимости студий от зарубежных решений: 56,6% разработчиков используют движок Unity, 39,7% - Unreal Engine. Таким образом, выявляется необходимость развития собственного

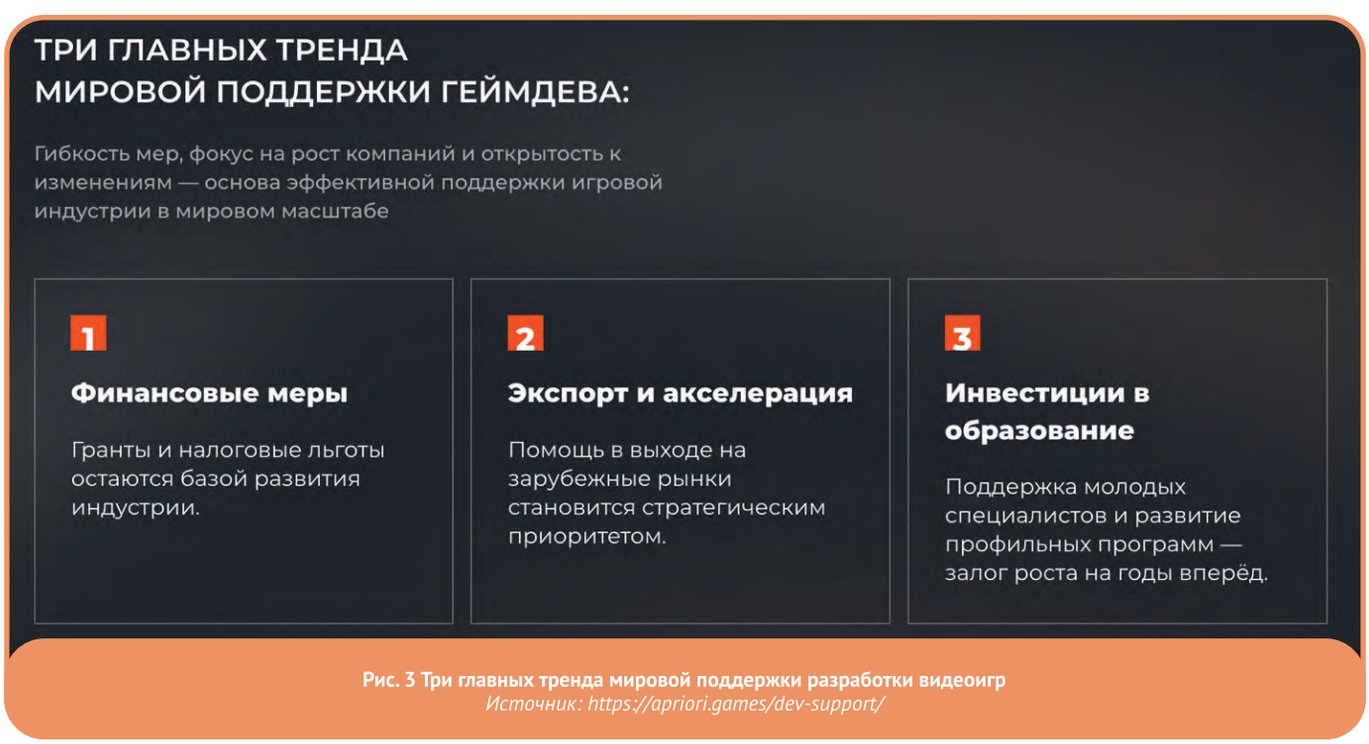


Рис. 3 Три главных тренда мировой поддержки разработки видеоигр
Источник: https://apriori.games/dev-support/

[17] https://apriori.games/dev-support/
[18] https://forgamedev.ru/
[19] https://vk.company/ru/
[20] https://1c.ru/
[21] https://rfrit.ru/
[22] https://www.exportcenter.ru/
[23] https://asi.ru/

программного обеспечения, обеспечивающего импортонезависимость российских решений.

Продолжающееся развитие инструментов разработки с помощью ИИ было отмечено в качестве одного из ключевых трендов отрасли игровых сервисов в исследовании «Развитие новых коммуникационных интернет-технологий в России и в мире в 2025 году», подготовленном ПАО «Ростелеком» совместно с АНО «ИРИ» и Фондом развития интернет-инициатив (ФРИИ)[24]. При этом установлено, что российские студии активно осваивают ИИ, но сохраняется зависимость от зарубежных ИИ-платформ[25].

Таким образом, очевидна необходимость точечного наращивания поддержки локальных разработок с ориентированием на фактические приоритеты и запросы индустрии.

В 2026 году АНО «ИРИ» опубликована книга «Компьютерные игры и метавселенные»[26], в которой представлен масштабный обзор современного состояния рынка видеоигр, анализ его структуры и инфраструктуры, а также основных трендов отрасли.

Большинство из рассмотренных в книге вопросов и предлагаемых решений представляют особую актуальность, так как регуляторные подходы по данным аспектам еще продолжают формироваться.

Так, например, в книге проведен сравнительный анализ мирового опыта возрастной маркировки (Австралия, Германия, Китай, Южная Корея, США (ESRB), Европа (PEGI)). В России в настоящее время рассматривается несколько инициатив по маркировке видеоигр (проект Минэкономразвития, QR-коды от Р.А.Д.И.[27], «зеленая маркировка» от ОРВИ), однако на законодательном уровне маркировка не регулируется.

Не менее важным вопросом остаются меры борьбы с игровой зависимостью, манипулятивным дизайном интерфейса игровых сервисов, защита несовершеннолетних пользователей. В настоящее время фиксируется тенденция роста претензий к владельцам игровых платформ в связи с недостаточным обеспечением детской безопасности (например, иск к Genshin Impact[28], к Roblox[29] в США, почти двухлетняя блокировка Roblox в Турции[30]).

Актуальность представляют и рассмотренные в книге видеоигры двойного назначения. Изучение зарубежного опыта демонстрирует широкое использование киберспорта и игр для рекрутинга в армию, повышения навыков бойцов, отработки командного взаимодействия.

В приведенном выше совместном исследовании АНО «ИРИ» и ПАО «Ростелеком» отмечено, что игровые технологии все активнее начинают применяться за пределами индустрии развлечений, в том числе для профессионального образования (так называемые «серьезные игры»), промышленного дизайна, инжиниринга и целей реального сектора экономики.

Полагаем, что указанные направления развития видеоигр требуют дополнительной проработки, в том числе в части распространения на них мер поддержки игровой индустрии.

Подводя итог, следует отметить, что российская игровая индустрия продолжает свой рост несмотря на беспрецедентное внешнее давление, благодаря системной работе государства, институтов развития и профессионального сообщества.

Так, например, за период 2022-2025гг. АНО «ИРИ» поддержано 47 игровых проектов на общую сумму свыше 4,6 млрд рублей. Всего в релиз при поддержке АНО «ИРИ» вышло 33 игры.

Вместе с тем, проведенные аналитические исследования показывают, что потенциал отрасли не раскрыт полностью. Зависимость от зарубежного ПО, затруднения в доступе к стимулирующим механизмам и сохраняющиеся барьеры для экспорта требуют дальнейшей выработки необходимых мер поддержки. Ключевыми векторами развития могут стать: системная работа по импортозамещению и переход к импортонезависимости игрового ПО, расширение региональной инфраструктуры (кластеры, акселераторы), а также создание национальной стратегии продвижения российских игр на внешние рынки.

У российского геймдева есть все предпосылки, чтобы занять достойное место в глобальной игровой индустрии. Для этого необходимо выстраивание гибкой, прозрачной и доступной системы поддержки, которая будет оперативно реагировать на запросы разработчиков и иных участников отрасли и помогать им конкурировать на глобальном уровне, сохраняя и транслируя российский культурный код и обеспечивая технологический суверенитет страны.

[24] https://www.company.rt.ru/projects/digital_economy_rf/ncit/files/Development_NCIT_Russia_world_2026.pdf
[25] https://www.comnews.ru/content/241457/2025-09-25/2025-w39/1009/rossii-80-igrovykh-studiy-ispolzuyut-ii-pri-razrabotke-igr
[26] https://ири.рф/reports/kompyuternye-igry-i-metavselennye/
[27] https://radi-videoigr.ru/
[28] https://www.ftc.gov/news-events/news/press-releases/2025/01/genshin-impact-game-developer-will-be-banned-selling-lootboxes-teens-under-16-without-parental
[29] https://variety.com/2025/digital/news/roblox-sued-louisiana-attorney-general-sexual-exploitation-1236489936/
[30] https://www.gamermarkt.com/blog/roblox-unblocked-turkey-680-day-ban-lifted-2026/



МАРИЯ БОЛЬШАКОВА
заместитель генерального директора
РСС



ВЛАДИМИР ГОРЖАЛЦАН
советник директора
АНО «Координационный центр национального домена сети Интернет»

35 ЛЕТ РЕГИОНАЛЬНОМУ СОДРУЖЕСТВУ В ОБЛАСТИ СВЯЗИ:

СТРАТЕГИЧЕСКИЕ ОРИЕНТИРЫ ЦИФРОВОГО РАЗВИТИЯ И УКРЕПЛЕНИЕ МЕЖГОСУДАРСТВЕННОГО СОТРУДНИЧЕСТВА

В июне 2026 года Региональное содружество в области связи (РСС) отметило 35-летие со дня основания. Юбилейные мероприятия, проведенные в Санкт-Петербурге при поддержке Петербургского международного экономического форума, объединили руководителей администраций связи, экспертов телекоммуникационных компаний и международных организаций. Ключевыми векторами работы Содружества на современном этапе определены обеспечение цифровой безопасности, гармонизация нормативно-правового регулирования и развитие трансграничной инфраструктуры, что подтверждается активным и предметным участием в заседаниях РСС Координационного центра доменов .RU/.РФ как давнего партнера организации.

03 июня 2026 года ровно в полдень пушечный выстрел прозвучал с Государева бастиона Петропавловской крепости в Санкт-Петербурге. Право произвести полуденный выстрел было предоставлено Алексею Бородину, Генеральному директору Регионального содружества в области связи – старейшей и самой авторитетной международной организации электросвязи в регионе Центральная Евразия – по случаю 35-летия РСС.

17 декабря 1991 года, в дни, когда на карте мира возникали новые независимые государства, руководители администраций связи одиннадцати стран – Азербайджана, Армении, Беларуси, Казахстана, Кыргызстана, Молдовы, России, Таджикистана, Туркменистана, Узбекистана и Украины – подписали в Москве Соглашение о создании Регионального содружества в области связи. Это был один из первых международных договоров, заключенных на постсоветском пространстве, – и далеко не последний, но по значимости – один из самых важных для отрасли. Политические бури того времени не разрушили того, что десятилетиями строилось как единая телекоммуникационная структура: руководители отрасли нашли в себе мудрость и волю сохранить связность сетей, обеспечить непрерывность связи и создать механизм для согласования действий на принципах добровольности, взаимоуважения и суверенности. Так родилось Содружество – первый отраслевой союз новых государств, ставший со временем авторитетной межгосударственной организацией, признанной и Международным союзом электросвязи, и Всемирным почтовым союзом.

Тридцать пять лет – возраст зрелости. За эти годы РСС прошло путь от экстренной координации транзита вызовов и согласования тарифов до формирования стратегических направлений цифрового развития целого региона. Менялись технологии, лидеры, поколения специалистов – но неизменной оставалась суть: РСС создавалось как инструмент практического сотрудничества, и именно эта прагматичность обеспечила ему долговечность. Сегодня структура Содружества охватывает все ключевые направления – от регулирования радиочастотного спектра и спутниковых орбит до почтовой связи, от координации международного сотрудничества до развития информационного общества и цифровой трансформации.

В этой структуре особую роль сегодня играют два вспомогательных (рабочих) органа РСС, совместное заседание которых стало одной из центральных вех юбилейного года: Комиссия РСС по регулированию телекоммуникаций и Совет операторов электросвязи и инфокоммуникаций РСС. Каждый из них выполняет свою незаменимую функцию. Комиссия – это площадка регуляторов, где вырабатываются согласованные подходы к правилам игры на рынке связи, тарифной политике, взаиморасчетам, развитию сетей. Совет операторов – голос бизнеса, прямой диалог компаний, которые строят сети, предоставляют услуги и ежедневно сталкиваются с технологическими и коммерческими реалиями. Их совместные заседания – не формальность, а механизм, при котором регуляторная мысль встречается с инженерной и рыночной практикой, а

решения рождаются не в вакууме кабинетов, а на стыке реальных потребностей и государственной политики.

4 июня 2026 года в Мариинском дворце Санкт-Петербурга состоялось 01/49-е совместное заседание Комиссии РСС по регулированию телекоммуникаций и Совета операторов электросвязи и инфокоммуникаций РСС. С приветственным словом к участникам обратился Председатель Совета операторов, генеральный директор РУП «Белтелеком» Александр Кенда, подчеркнувший, что повестка дня отражает самые актуальные вызовы, стоящие перед отраслью в регионе. В работе заседания приняли участие эксперты ведущих телекоммуникационных компаний, представители администраций связи государств – участников Содружества, а также профильных ведомств и международных организаций. Заседание прошло в рамках серии юбилейных мероприятий РСС, проходивших в Санкт-Петербурге с 3 по 5 июня, в рамках программы Петербургского международного экономического форума.

Повестка заседания отличалась редкой широтой и одновременно четкой практической фокусировкой. Одной из ключевых тем стала борьба с мошенничеством в сфере электросвязи – проблема, которая затрагивает каждого абонента и каждого оператора в регионе. Социальная инженерия, подмена номеров, мошеннические звонки и SMS превратились в транснациональное явление, требующее координированного реагирования, и на заседании обсуждались конкретные шаги по усилению межгосударственного взаимодействия: обмен информацией об инцидентах, согласование технических мер противодействия, разработка моделей угроз.

Не менее значимой стала дискуссия о тарифах на услуги связи в роуминге. Вопрос «справедливого роуминга» – обеспечения максимально выгодных условий для граждан, перемещающихся между странами Содружества, – давно находится в фокусе внимания РСС. При Совете операторов и Комиссии по регулированию телекоммуникаций уже действует специальная Рабочая группа по вопросам роуминга, в фокусе работы которой: подходы к снижению стоимости роуминга, гармонизации тарифных моделей и координации действий с Евразийской экономической комиссией, которая ведет параллельную работу в этом направлении для государств – членов Евразийского экономического союза.

Отдельным блоком повестки стало обсуждение развития передовых технологий. Перспективы внедрения сетей 5G и подготовки к технологиям 6G в странах региона, развитие технологии Direct-to-Device, обеспечивающей прямую спутниковую связь с пользовательскими устройствами, – все эти темы требуют согласованной работы по управлению радиочастотным спектром, согласованию технических стандартов и формированию единых требований к оборудованию. На заседании обсуждались также вопросы развития искусственного интеллекта и центров обработки данных, что отражает растущую роль цифровой инфраструктуры как фундамента экономического развития.

Трансграничные инфраструктурные проекты – еще одно направление, в котором РСС традиционно играет роль координатора. Развитие магистральных сетей, обеспечение их устойчивости и пропускной способности, согласование маршрутов и параметров качества – все это требует постоянного диалога между операторами и регуляторами стран, через территории которых проходят транзитные маршруты. На заседании были рассмотрены конкретные проекты и предложены механизмы их ускоренной реализации.

Кибербезопасность и модели угроз заняли в повестке особое место. Операторы связи все чаще сталкиваются с целенаправленными атаками на инфраструктуру, попытками перехвата трафика и нарушениями работы сетей. На заседании обсуждались вопросы создания региональных механизмов обмена информацией об инцидентах, координации действий при масштабных сбоях и развития компетенций специалистов. Обсуждались также вопросы анализа интернет-трафика и развития доменного бизнеса – направления, в котором РСС сотрудничает с Координационным центром доменов .RU/.РФ, являющимся давним партнером и теперь уже участником Содружества.

Значимым элементом повестки стало выступление советника директора Координационного центра доменов .RU/.РФ Владимира Горжалцана. Он представил доклад, посвященный противодействию мошенническим схемам с использованием доменных имен, и обозначил комплексный многоуровневый подход к минимизации подобных рисков.

В своем выступлении В. Горжалцан акцентировал внимание на российском опыте защиты национальной доменной инфраструктуры и анонсировал изменения в регулировании доменной отрасли, вступающие в силу с 1 сентября 2026 года. Также были презентованы собственные проекты Координационного центра в сфере информационной безопасности – «Доменный патруль» и «Нетоскоп».

«Рунет сегодня развивается не в изоляции, а под влиянием глобальных трендов и вызовов. В санкционных условиях Россия сталкивается с необходимостью искать собственные национальные ответы. В этой связи решать задачи по снижению рисков от мошеннических атак мы планируем путем укрепления безопасности национальной доменной экосистемы, а также представляя свой опыт и отстаивая национальную позицию на региональных и глобальных международных мероприятиях», – подчеркнул спикер.

Заседание 4 июня не было единственным событием юбилейных дней в Санкт-Петербурге. 5 июня 2026 года в Мариинском дворце прошло 65/32-е совместное заседание Совета глав администраций связи – участников РСС и Координационного совета государств – участников СНГ по информатизации при РСС.

Директор Координационного центра доменов .RU/.РФ Андрей Воробьев направил в адрес Содружества официальное поздравление, отметив:
«С удовлетворением отмечаем, что все цели Содружества выполняются на высоком профессиональном и организационном уровне, а заслуженный авторитет Содружества в международном сообществе общепризнан. Координационный центр доменов .RU/.РФ гордится своим участием в работе Содружества и старается вносить свой посильный вклад в его работу».

В Ротонде дворца состоялась торжественная церемония памятного гашения почтовых марок, выпущенных Российской Федерацией и Республикой Беларусь к 35-летию РСС. Руководители делегаций администраций связи Беларуси, Казахстана, Кыргызстана, России, Таджикистана, Туркменистана, Узбекистана и Генеральный директор РСС поставили на конверты с марками оттиски штемпеля и свои подписи. Почта России доставила эти юбилейные конверты в министерства связи стран Содружества – символический жест, соединивший традицию почтовой связи с цифровой эпохой. Позднее, в августе 2026 года в Чолпон-Ате, состоялась и церемония гашения марки, выпущенной ОАО «Кыргыз почтасы», – и этот совместный выпуск администраций связи марок в честь юбилея Содружества стал еще одним проявлением солидарности, которую РСС укрепляет на протяжении трех с половиной десятилетий.

В рамках мероприятий юбилейного года проходят церемонии вручения наград за вклад в развитие Содружества: ими были отмечены главы администраций связи, председатели и члены вспомогательных (рабочих) органов РСС, эксперты, трудовые коллективы, представители операторов связи, научно-исследовательских институтов, учебных заведений и международных организаций. Это была не просто дань уважения – это признание того, что РСС построено людьми, и именно люди – их профессионализм, преданность делу, готовность к диалогу – являются главным ресурсом Содружества.

35-летие РСС – это не только повод оглянуться назад. Юбилейный год насыщен событиями, которые задают ориентиры на будущее. В сентябре 2026 года, в рамках III Международного технологического конгресса в конгрессно-выставочном центре «Патриот-Экспо» в Московской области, состоится Юбилейный форум РСС «35 лет вместе: Цифровое будущее единого пространства». Форум станет ядром тематического кластера «Связь и телеком» и охватит ключевые направления деятельности Содружества: состоятся тематические секции по цифровой трансформации почтовой отрасли, электросвязи и ИКТ, международной информационной безопасности и искусственному интеллекту, стратегическая сессия по развитию международного сотрудничества.

Все эти события складываются в единую картину. РСС сегодня – это не исторический раритет, а живой, динамично развивающийся институт, способный отвечать на вызовы времени. Состоявшееся 01/49-е совместное заседание Комиссии по регулированию телекоммуникаций и Совета операторов электросвязи и инфокоммуникаций наглядно это подтвердило: повестка была не протокольной, а содержательной; обсуждения – не формальными, а предметными; решения – не декларативными, а ориентированными на практическую реализацию. Именно так – через конкретные шаги, через согласование позиций, через обмен опытом – РСС строило свою работу все 35 лет.

За этими десятилетиями стоят сотни заседаний, тысячи экспертов – уже не только из стран и предприятий региона, но из зарубежных компаний – лидеров отрасли, десятки согласованных позиций на международных площадках, сотни научно-исследовательских работ, программы подготовки кадров, совместные проекты по развитию сетей и защите спектра. Но главное – за этими десятилетиями стоит непрерывная связность: связность сетей, связность людей, связность стран. В мире, где технологии меняются быстрее, чем законодательства успевают адаптироваться, а геополитические сдвиги бросают вызовы институтам, казавшимся незыблемыми, РСС остается островком стабильности и предсказуемости – не потому, что оно сопротивляется изменениям, а потому что умеет меняться, сохраняя свою суть.

Юбилейный год продолжается, продолжается и кропотливая работа членов и участников Содружества. Впереди – большие конференции и конгрессы, новые заседания и новые решения. Но уже сейчас можно сказать: 35-летие РСС встречает организация, которая не просто состоялась, но и уверенно смотрит вперед.



АНАТОЛИЙ КОРСАКОВ
генеральный директор
ООО «Трамплин Электроникс»

ТРАНСФЕР ТЕХНОЛОГИЙ: В КАКОЙ МОМЕНТ «ЧУЖОЕ» СТАНОВИТСЯ «СВОИМ»?

Геополитические события последних лет стали вызовом для российской микроэлектроники: до сих пор большая часть производимых в России процессоров и контроллеров относится к категориям 90-65 нм и выше[1]. При этом, есть огромный спрос на современные чипы, которые в России пока не производятся. 99% всей IT-инфраструктуры до сих пор работает на процессорах Intel и AMD. Но даже оставшийся 1% российских центральных процессорных устройств (ЦПУ) не до последней песчинки построен на российских компонентах и производится не на территории России и даже процессорная архитектура может быть разработана не в России. Так в какой момент происходит отделение российского производства от зарубежного, особенно в контексте трансфера технологий, которыми все мы так или иначе пользуемся?

ГЕОПОЛИТИЧЕСКАЯ НЕОБХОДИМОСТЬ В ОБМЕНЕ ТЕХНОЛОГИЯМИ

За последние 30 лет Россия прошла сложный путь в контексте общемировых тенденций глобализации. Многие российские предприятия стали частью мировой экономики и производственных процессов, внутри которых сложно и дорого, а зачастую просто невозможно построить всё от и до в одной стране. С 2022 года наша страна в глобальном смысле, включая разные отрасли от микроэлектроники до малого бизнеса, оказалась в новой реальности, к которой мало кто был готов. То время, когда можно было проектировать инфраструктурные решения на любых технологических стеках, на любых комплектующих из любых технологических юрисдикций, безнадежно прошло и уже никогда не вернется. Особенно остро это почувствовала отрасль микроэлектроники, где влияние глобализации колоссально. По сути, мы оказались в некоторой степени изоляции, потому что международные конфликты и наличие уникальных технологий в руках определенных игроков оказали негативное влияние на мировую отрасль в целом — сегодня ни одна страна не может самостоятельно с нуля создать процессор 3-10 нм. Для этого обязательно нужно кооперироваться и поддерживать дружеские отношения с другими государствами.

Постепенно все крупные страны или объединения стран приходят к тому, что без технологического суверенитета невозможно говорить о цифровой и технологической независимости и безопасности. Всем нужны:

- своя независимая архитектура;
- свои производственные возможности;
- защищенные цепочки поставок.

В марте 2022 года вышло распоряжение Правительства Российской Федерации о перечне иностранных государств, совершающих в отношении Российской Федерации, российских юрлиц и физических лиц недружественные действия[2]. И если мы говорим о доверенности и суверенности, надо руководствоваться этим постановлением, а также Указом Президента Российской Федерации № 166 от 30 марта 2022 года «О мерах по обеспечению технологической независимости и безопасности критической информационной инфраструктуры Российской Федерации»[3] и Распоряжением Правительства Российской Федерации № 20-р от 17.01.2020 «О стратегии развития электронной промышленности Российской Федерации на период до 2030 года»[4]. Именно эти документы показывают всю неоднозначность геополитической обстановки и четко указывают на то, что дружественные страны должны поддерживать друг друга в том числе и при обмене технологиями. Ведь на момент глобального разделения на «свой-чужой» страны и компании подошли с разным промышленным, производственным и научным потенциалом. Эта разность достижений диктует необходимость трансфера технологий из дружественных юрисдикций, если мы не хотим оказаться за бортом перспективных решений. То, что раньше было относительно просто, условно доступно и хорошо, начиная с покупки готовой топологии и заканчивая проектированием сложных функциональных блоков, перестало быть таким простым и доступным. Эти технологии в Россию просто не продадут.

[1] По данным «Анализа рынка процессоров и контроллеров в России» от BusinesStat в 2025 году выпуск процессоров и контроллеров сократился на 12% до 7,5 млн штук. При этом, большая часть производимых в стране процессоров и контроллеров относится к категориям 90-65 нм и выше. https://marketing.rbc.ru/articles/16334/

[2] Распоряжение Правительства Российской Федерации от 5 марта 2022 № 430-р Об утверждении перечня иностранных государств и территорий, совершающих недружественные действия в отношении Российской Федерации, российских юридических и физических лиц: https://mid.ru/ru/foreign_policy/official_documents/1861789/

[3] http://www.kremlin.ru/acts/bank/47688

[4] http://publication.pravo.gov.ru/document/0001202001220017

А конечный заказчик ориентируется на тот технологический уровень, который был неограниченно доступен до 2022 года, и, соответственно, требует от производителей, в том числе микроэлектроники, решений, которые сопоставимы по производительности, энергопотреблению, цене тому, что было ранее. И тут на помощь производителям и разработчикам приходит трансфер технологий, который на сегодня стал остро необходимым.

ТРАНСФЕР ТЕХНОЛОГИЙ: ОПРЕДЕЛЕНИЕ И ЭТАПЫ

Трансфер технологий – это процесс передачи и адаптирование технологий, соответствующих прав на них от владельцев технологии к принимающей стороне, которая в этом случае становится контрибьютором и, в том числе, может создавать свои решения на основе данной технологии.

Трансфер технологий состоит из двух больших слотов:

1. Юридический процесс лицензирования. Это очень важно, ведь недружественные страны используют все доступные рычаги воздействия для подрыва суверенитета России, в том числе в микроэлектронике. Ошибочный выбор компании-партнера может привести к тому, что российские компании в одночасье лишаются лицензий на технологии, средства проектирования и поддержку. При любой попытке сделать что-то на основе этой технологии — международной судебный иск, лишение технической поддержки, запрет на производство.
2. Собственно технологический трансфер. Это освоение и глубина разработки лицензированных технологий, вопросы построения производства и встраивания собственных решений в существующую индустрию.

Что же в этих условиях вызывает доверие? Какие критерии доверия можно выделить в трансфере технологий?

Во-первых, это возможность и доказательство прямого лицензирования технологии и прозрачных финансовых взаимодействий. Допустим, если мы покупаем архитектурную лицензию, то мы покупаем это напрямую у правообладателя по понятным и законным финансовым каналам и можем, грубо говоря, в любой момент предъявить платежку, а также доказать тем самым факт передачи прав на технологию у компании-покупателя.

Во-вторых, глубина освоения компетенций, например, по данной конкретной архитектуре для каких-то конкретных микропроцессоров или микроконтроллеров. Соответственно, это дает возможность продемонстрировать, что компания имеет собственную топологию, собственные наработки, и доказать, что теперь это и их собственные технологии, на основе которых выстроены собственные изделия и решения. Такие компании могут с легкостью доказать, что в полной мере освоили технологию, научились ее дорабатывать, привнося что-то новое.

В-третьих, жизненный цикл и техподдержка. Умеет ли компания контролировать жизненный цикл своих изделий, закрывать их уязвимости? В этом случае крайне важна быстрота реагирования на запросы конечных потребителей: насколько разработчик и производитель гарантируют заказчику работоспособность своих продуктов.

И, в-четвертых, экосистема. Лицензировать возможно всё, что угодно — любую технологию или продукт. Но невозможно лицензировать экосистему, по крайней мере пока этого не делают. Сейчас мы видим, как многие крупные компании в России, такие как Вконтакте, Яндекс, Сбер, НТЦ ИТ Роса работают над созданием собственной экосистемы, вкладывают в это деньги, привлекают студентов, сотрудничают с разработчиками программного обеспечения (ПО). Развитие экосистемы — длительный и очень ресурсоемкий процесс. Это борьба за вендоров ПО, за кадры, за студентов, даже за разработчиков игр, которые должны поверить в процессорную архитектуру, увидеть ее перспективы и согласиться тратить на нее свое время и деньги. Но экосистема — это необходимое условие для развития микропроцессорной архитектуры, без которого она «не взлетит» и не получит массового применения.

Все эти факторы в совокупности дают выбранной модели технологического трансфера гарантированную воспроизводимость всей технологической базы. Между покупкой конечного изделия с иностранным решением и трансфером технологий лежит принципиальная разница. Купить готовое решение — это, условно говоря, купить рыбу. А провести трансфер технологий — это не просто купить удочку, но и научиться ей эффективно пользоваться и делать новые удочки. ООО «Трамплин Электроникс»[5] идет именно этим путем: для нас важно не просто производить процессоры, а осваивать опыт, развивать компетенции, строить собственные технологии разработки и производства.

ОПЫТ КОМПАНИИ ТРАМПЛИН ЭЛЕКТРОНИКС

Бизнес-модель «Трамплин Электроникс» построена на трансфере технологий. Задачей компании было провести трансфер технологий и дать рынку производительный и энергоэффективный процессор, который может конкурировать с Intel и AMD. В качестве партнера мы выбрали компанию из дружественной страны и официально купили лицензию на процессорную архитектуру LoongArch. Это решение было продиктовано несколькими причинами:

- собственная система исполнения команд (ISA);
- развитая экосистема;
- готовые процессорные линейки с доказанной производительностью;

[5] https://tramplin.group/

- возможность стабильного производства без санкционных рисков;
- долларонезависимые бесперебойные поставки.

Для Трамплин Электроникс важнейшей задачей было не просто взять готовое решение, но пройти весь инженерный путь, развить компетенции команды инженеров и получить процессор, адаптированный под российский рынок и запросы бизнеса и КИИ. Так появилась платформа «Иртыш» - семейство процессоров и систем на кристалле (СнК) с уже развитой партнерской сетью и готовыми программными и аппаратными решениями. Трамплин Электроникс были не первые, кто проявил интерес к этой процессорной архитектуре: компании Базальт СПО и Хи-Квадрат, Норси-Транс разрабатывали ПО и ПАК на LoongArch еще с 2023 года. Компания Трамплин Электроникс располагает штатом инженеров с опытом в разработке процессоров более 15 лет, полным комплектом технической документации и набором готовых инструментов для создания программ, включающим библиотеки кода, документацию и компиляторы (SDK), собственным дизайн-центром, стендами разбраковки и техподдержкой. За полтора года была создана линейка серверных процессоров Иртыш **(см. табл. 1)**.

Табл. 1. Технические характеристики процессоров Иртыш

Параметры	Иртыш С616	Иртыш С632	Иртыш С664
Пиковая тактовая частота	2.2 ГГц	2.1 ГГц	2.0 ГГц
Количество ядер/потоков	16/32	32/64	64/128
Количество чипов на подложке	1	2	4
Ядро процессора	64-разрядное суперскалярное ядро LA664; Поддерживает систему инструкций LoongArch; Поддерживает 128/256-битные векторные инструкции; Внеочередное исполнение команд до 6 за такт; 4 блока с фиксированной точкой, 4 векторных блока и 4 блока доступа.		
Производительность	844.8 ГФлопс@2.2 ГГц	1612.8 ГФлопс@2.1 ГГц	3072 ГФлопс@2.0 ГГц
Межпроцессорная шина	LCL PCIe мультиплексирование		
Модуль безопасности	Собственная разработка в соответствии с требованиями российских регуляторов		
КЭШ	Каждое ядро содержит L1 инструкций: 64KB L1 данных: 64KB L2: 256KB L3: 32MB	Каждое ядро содержит L1 инструкций: 64KB L1 данных: 64KB L2: 25KB L3: 64MB	Каждое ядро содержит L1 инструкций: 64KB L1 данных: 64KB L2: 256KB L3: 128MB
Память	4 канала 72-битной DDR4-3200	4 канала 72-битной DDR4-3200 8 каналов 72-битной DDR4-3200	4 канала 72-битной DDR4-3200 8 каналов 72-битной DDR4-3200
Ввод-вывод (I/O)	4 канала PCIe x16 (64 линии)*	8 каналов PCIe x16 (128 линий)*	8 каналов PCIe x16 (128 линий)*
Прочие I/O	SPI UART I2C GPIO	SPI UART I2C GPIO	SPI UART I2C GPIO
Управление питанием	Поддержка динамического отключения тактовых сигналов основных модулей; поддержка динамического изменения частоты основных доменов; поддержка динамической регулировки напряжения основного домена питания.		
Типовое потребление	100-120Вт	180-200Вт	250-300Вт

*в максимальной комплектации. Точное количество линий зависит от конечной конфигурации платформы

«Трамплин Электроникс» прошел весь инженерный путь трансфера и адаптации технологии и в случае, если на территории Российской Федерации появятся технологические возможности изготовления микроэлектроники с техпроцессом 12 нм и меньше, компания будет готова производить процессоры «Иртыш» здесь — в России. Уже сейчас совместно с НИУ МИЭТ и АО ЗНТЦ готовится один из важных этапов производства процессоров — корпусирование. Основная цель сотрудничества трех российских компаний разработка и развитие в РФ технологий полного цикла корпусирования высокопроизводительных микросхем и многопроцессорных модулей мирового уровня с применением метода flip-chip монтажа кристаллов с количеством выводов более 10 тыс. шт. в корпусах типов BGA, LGA[6].

ОТ ТРАНСФЕРА К СУВЕРЕНИТЕТУ. ПОЧЕМУ ВАЖНО НЕ ПРОСТО КУПИТЬ, А ОСВОИТЬ?

В условиях постоянного санкционного давления и высокой геополитической турбулентности трансфер технологий из дружественных стран становится не просто удобным инструментом, а стратегической необходимостью. Он позволяет сократить инновационный цикл, избежать «изобретения велосипеда» и получить тактическое технологическое преимущество в кратчайшие сроки.

Однако важно четко осознавать фундаментальный риск: сам факт получения доступа к зарубежным разработкам, патентам или оборудованию еще не гарантирует технологического суверенитета. Механическое копирование, работа с «черными ящиками» или простая отверточная сборка создают лишь иллюзию независимости, которая может рухнуть при первом же изменении внешнеполитического курса даже самых лояльных партнеров.

Истинно отечественной технология становится только в одном случае: когда она проходит цикл глубокого инженерного освоения. Это означает не просто умение эксплуатировать чужое решение, а полное понимание лежащих в его основе физических и конструкторских принципов. Это способность адаптировать технологию под доступные отечественные материалы и, что критически важно, **возможность воспроизвести ее на любой российской фабрике, соответствующей требованиям**, независимо от внешних поставок комплектующих.

Без этого фундаментального этапа трансфер технологий превращается в технологическую зависимость нового типа. И главное последствие такого подхода — стагнация человеческого капитала. Только в процессе глубокой адаптации, обратного инжиниринга и локализации рождаются новые компетенции, формируется современная инженерная школа и удерживаются кадры высочайшей квалификации.

Таким образом, трансфер технологий из дружественных стран должен рассматриваться не как конечная цель, а как стартовая площадка. Превратив заимствованное знание в собственную, глубоко проработанную инженерную практику, Россия обеспечит себе не просто тактическую выживаемость в условиях санкций, а создаст прочный фундамент для будущих, уже собственных технологических прорывов.

[6] https://tramplin.group/news_ru

ОБЕСПЕЧЕНИЕ ДОВЕРИЯ И БЕЗОПАСНОСТИ ПРИ ИСПОЛЬЗОВАНИИ ИКТ



АЛЕКСАНДР ФЕФИЛОВ
руководитель
учебно-методического направления
ГК «ИнфоТеКС»



НАТАЛИЯ КАБАКОВА
старший специалист
по информационной безопасности
ГК «ИнфоТеКС»



НАТАЛЬЯ КИСЕЛЕВА
контент-менеджер
ГК «ИнфоТеКС»

ПРАКТИЧЕСКАЯ ПОДГОТОВКА ПЕРСОНАЛА К КИБЕРИНЦИДЕНТАМ: ВОЗМОЖНОСТИ СОВРЕМЕННЫХ КИБЕРУЧЕНИЙ

В последние три года наблюдается взрывной рост числа кибератак и их интенсивности на российские компании. Согласно аналитике[1], собранной специалистами «Перспективного мониторинга» (входит в ГК «ИнфоТеКС»), с 2023 года фиксируется стабильное увеличение количества APT-инцидентов[2]. Основной удар нацелен на критически важные отрасли — телеком, ИТ-провайдеров, финансовый и государственный секторы.

Растет и число атак, совершенных при помощи социальной инженерии или фишинга[3]. В 2025 году фишинг стал основным способом первоначального проникновения, на него пришлось 64% всех зафиксированных эпизодов. При этом до 90% успешных атак на корпоративную инфраструктуру начинаются именно с письма или сообщения сотруднику. В 2026 году значительно возрастает количество фишинговых атак через мессенджеры и фальшивые чаты.

[1] Ландшафт киберугроз — https://amonitoring.ru/article/Ландшафт%20киберугроз.pdf
[2] APT-инциденты — сложные целевые кибератаки, которые обычно отличаются длительным присутствием злоумышленников в инфраструктуре, использованием нескольких этапов атаки и стремлением оставаться незамеченными.
[3] Фишинг — вид социальной инженерии, выполняемый с использованием технических средств, при котором злоумышленник под видом доверенного источника (человека, организации и др.) воздействует на жертву с целью вынудить выдать информацию или выполнить определенные действия.

В связи с этим подготовка персонала к нештатным ситуациям, вызванным вредоносной активностью нарушителей и APT-группировок, приобретает первостепенное значение.

Одной из эффективных форм подготовки или совершенствования навыков специалистов, способных своевременно обнаруживать компьютерные атаки и уверенно реагировать на них, ликвидируя последствия компьютерных инцидентов, являются практические занятия в формате киберучений.

ПОДГОТОВКА СПЕЦИАЛИСТОВ ИБ-СЛУЖБ И ИТ-ПОДРАЗДЕЛЕНИЙ

В учебных программах подготовки или повышения квалификации специалистов зачастую доминируют теория и изучение актуальных нормативно-правовых актов, при этом слабо отрабатываются прикладные навыки. Полученные знания помогают сформировать базовое понимание угроз, однако сами по себе не готовят сотрудников к действиям в условиях реального инцидента.

При реальных атаках от специалиста требуется способность быстро принимать правильные решения, соблюдать установленный регламент реагирования, осуществлять взаимодействие с рабочей группой и не допускать ошибок под давлением обстоятельств.

Киберучения — это практический формат тренировки, при котором участники действуют в условиях, максимально приближенных к реальной обстановке во время компьютерной атаки (КА). Тренировки проходят в цифровой среде. Участники противостоят виртуальному нарушителю, владеющему различными техниками и тактиками атак. Тренировки дают возможность оценить, насколько специалист или группа способны противостоять КА. Основой для проведения киберучений являются киберполигоны — интерактивные тренировочные платформы для подготовки специалистов в сфере информационной безопасности (ИБ).

Киберполигон Ampire, разработанный компанией «Перспективный мониторинг», поддерживает проведение учений для различных категорий пользователей. Платформа реализует как индивидуальный, так и групповой форматы тренировок и лабораторных работ. Форма проведения киберучений может быть различной — как онлайн, так и офлайн. Цель тренировки — отработка навыков защиты информационной системы от вредоносных воздействий, реализуемых внешними и внутренними нарушителями.

Платформа Ampire в рамках подготовки специалистов предоставляет возможность использования современных технических средств защиты от киберугроз, таких как, например, системы обнаружения вторжений, аналитические системы продуктовой линейки ViPNet TDR (ГК «ИнфоТеКС»), имеющие доступ к непрерывно обновляющимся экспертным данным и базам решающих правил. Киберполигон Ampire сочетает в себе возможности интеграции дополнительных средств защиты информации, кастомизации тренировочных шаблонов и создания уникальных тренировочных сценариев на базе цифрового двойника ИТ-инфраструктуры данной организации. Таким образом, киберполигон Ampire является тренировочной платформой, соответствующей современным реалиям и актуальным требованиям к подготовке специалистов по ИБ и ИТ в области защиты информации.

Специалистам по ИБ и сотрудникам ИТ-департаментов занятия на киберполигоне позволяют отрабатывать навыки обнаружения КА и их регистрации, расследования компьютерных инцидентов (КИ), анализа журналов событий и восстановления инфраструктуры, а также отрабатывать алгоритмы взаимодействия между подразделениями.

Киберполигон позволяет развернуть виртуальную инфраструктуру организации и безопасно воспроизводить различные сценарии кибератак. В отличие от тренировок в рабочей среде, использование киберполигона исключает риск нарушения работы реальных информационных систем и позволяет многократно воспроизводить один и тот же сценарий, изменяя его сложность, масштаб и состав участников.

Проведение занятий в формате командных учений специалистов нескольких подразделений позволяет проверить уровень подготовки сотрудников и выявить слабые места в процессах реагирования, распределении ролей и взаимодействии между подразделениями. В результате организация получает возможность устранить выявленные недостатки до того, как столкнется с действиями реального злоумышленника.

Специалисты по информационной безопасности регулярно проходят киберучения в той или иной форме. Если они являются сотрудниками организаций, входящих в перечень КИИ[4] со значимыми объектами, то их обязанность — не реже одного раза в год проводить тренировки по отработке плана реагирования[5].

Использование киберполигона Ampire при подготовке специалистов по ИБ позволяет применять функционал моделирования угроз и векторов атак, комбинировать различные уязвимости и последствия в целях

[4] Критическая информационная инфраструктура
[5] Приказ ФСБ России от 25.12.25 № 457, который вступил в силу с 30 января 2026 года

всесторонней подготовки персонала в области противодействия КА **(рис. 1, 2)**. Практический опыт проведения ежемесячных киберучений со специалистами департамента информационных технологий одного из регионов на протяжении года показал, что регулярные киберучения позволяют достичь высоких результатов, значительно снижающих риски компьютерных инцидентов: сокращается время на обнаружение КА и анализ событий ИБ, принятие решений, реагирование на КИ и восстановление работоспособности инфраструктуры.

Киберучения также помогают специалистам по ИБ отработать взаимодействие с системой ГосСОПКА[6]. Организации обязаны передавать в систему сведения о КА и КИ[7] через Национальный координационный центр по компьютерным инцидентам (НКЦКИ) с использованием утвержденной формы. В киберполигоне Ampire для регистрации доступно заполнение карточек инцидентов как в упрощенном варианте, так и по форме НКЦКИ.

Наиболее подходящий для специалистов ИТ и ИБ формат киберучений — CSIRT (Computer Security Incident Response Team). CSIRT представляет собой группу экспертов, которая оценивает, документирует и реагирует на КИ, чтобы обеспечить быстрое восстановление защищаемой инфраструктуры и не допустить в будущем подобных инцидентов.

Командный формат Red Team и индивидуальный Red Team Labs помогают подготовке специалистов к предупреждению кибератак в форме offensive security[8]. Участники таких киберучений действуют на стороне атакующей команды, исследуя уязвимости информационной инфраструктуры. В формате Red Team они проходят полный цикл исследования инфраструктуры, в формате Red Team Labs участники тренировок развивают навыки, связанные с тестированием на проникновение и исследованием защищённости, выполняя набор последовательных практических заданий.

ОБУЧЕНИЕ СОТРУДНИКОВ НЕПРОФИЛЬНЫХ ПОДРАЗДЕЛЕНИЙ

Точкой вхождения злоумышленника в периметр организации может стать любой сотрудник, имеющий корпоративный доступ к инфраструктуре. Таким сотрудником может быть не только администратор сети, но и бухгалтер или менеджер.



Рис. 1 — Участники Кибербитвы среди регионов Дальнего Востока на форуме «ИнфоХаб 2026»

[6] https://gossopka.ru/
[7] Приказ ФСБ России от 25 декабря 2025 г. № 546
[8] Подход Offensive Security (наступательная кибербезопасность) направлен на заблаговременное обнаружение и устранение уязвимостей в информационных системах, играет ключевую роль в защите предприятий, предоставляя целый спектр методов и стратегий для борьбы с угрозами. Источник: https://www.anti-malware.ru/analytics/Technology_Analysis/Offensive-Security



Рис. 2 — Киберучения на Форуме ГосСОПКА 2026, организованном НКЦКИ

Согласно исследованиям «Перспективного мониторинга», мошенники в 2026 году переходят от массовых обезличенных рассылок к контекстным сценариям, дополненным персональными данными из ранее опубликованных утечек, что повышает успешность сценариев атак.

Для защиты ресурсов от КА, начинающихся с фишинга и других методов социальной инженерии, необходимо повышать уровень цифровой грамотности сотрудников организации, знакомить их с основами информационной безопасности. Практические занятия, имитирующие реальную фишинговую атаку, представляются наиболее эффективной формой обучения. Так, в течение трех лет сотрудники «Перспективного мониторинга» оказывали одной из коммерческих организаций услуги анализа защищенности организации методом социальной инженерии. В 2023 году по фишинговой ссылке прошли 63% испытуемых, в 2024-м — 33%, в 2025-м — 8%. Учитывая, что после проведения фишинговой рассылки с испытуемыми проводился разбор ситуации, результаты наглядно демонстрируют повышение уровня цифровой грамотности в организации.

Еще одним инструментом для обучения сотрудников являются лабораторные работы, доступные на модуле Ampire Junior, в рамках которого реализованы сценарии, направленные на распознавание фишинга, соблюдение правил цифровой гигиены, защиту персональных данных и корректные действия при работе с цифровыми устройствами. Курс повышения квалификации непрофильных сотрудников организации проводится в виде теоретических, практических занятий и лабораторных работ.

ОБУЧЕНИЕ ТОП-МЕНЕДЖМЕНТА

Топ-менеджмент коммерческих организаций и руководство органов государственной власти — постоянная цель для злоумышленников при планировании и проведении кибератак. Нарушители могут использовать их как точку вхождения в инфраструктуру организации, применяя методы социальной инженерии. Учитывая, что руководители имеют большое количество доступов в инфраструктуре организации или департамента органа государственной власти, успех такой атаки может нанести значительный ущерб — например, крупную утечку данных. Так, в апреле 2026 года стало известно о пяти крупных инцидентах в государственном секторе, в результате которых оказались скомпрометированы 159 млн записей[9]. Данные из утечек позволяют злоумышленникам формировать убедительные сценарии атак.

Личность руководителя организации также может использоваться для фишинговых атак на сотрудников. С начала 2024 года в России стали фиксироваться случаи мошеннических схем, сочетающих социальную инженерию и дипфейки[10] в схемах FakeBoss[11]. Число атак с использованием дипфейков в финансовом секторе РФ в 2024 году выросло на 13 %, до 5,7 тыс. случаев[12]. В 2025 году схема FakeBoss стала самой популярной в атаках с использованием подделки личности, продемонстрировав десятикратный рост.

[9] https://safe.cnews.ru/news/line/2026-05-05_perspektivnyj_monitoring
[10] Дипфейк (от англ. deepfake) — это синтетический медиаконтент (изображение, видео или аудио), созданный с помощью искусственного интеллекта и машинного обучения. В таких подделках с помощью нейросетей подменяется лицо, мимика, жесты или голос человека, чтобы он выглядел так, как будто делает или говорит то, чего на самом деле не происходило.
[11] FakeBoss (ложный руководитель) — мошенническая схема, в которой злоумышленник выдает себя за руководителя или ключевого сотрудника.
[12] https://iz.ru/1773345/oksana-belkina/odinakovy-s-lica-v-rossii-vyroslo-cislo-atak-s-primeneniem-dipfeikov

В 2026 году потенциально под риском находятся руководители более чем 40 тыс. российских компаний[13], а ежедневно сценарии атак на топ-менеджеров могут затрагивать более миллиона сотрудников.

При этом принцип минимальных привилегий, применяемый департаментом ИБ в организации, не всегда достаточен, так как ограничивает свободу действий руководителя, необходимую для выполнения его обязанностей.

В связи с этим руководителям организаций любого уровня и профиля необходимо владеть основами информационной безопасности и цифровой грамотности. Платформа Ampire позволяет пройти обучение основам цифровой грамотности в формате индивидуальных лабораторных работ, которые могут проводиться на регулярной основе.

Помимо повышения собственной цифровой грамотности руководителя, большое значение имеет его участие в совместных комплексных тренировках с сотрудниками всех подразделений организации. Комплексные учения позволяют выявить проблемные места в безопасности организации и отработать способность руководителей принимать решения для ликвидации последствий компьютерных атак.

КОМАНДНО-ШТАБНЫЕ КИБЕРУЧЕНИЯ

Для проверки готовности организации в целом к реагированию на КА предназначены командно-штабные учения (КШУ) по информационной безопасности. В отличие от технических тренировок, где основное внимание уделяется поиску и устранению уязвимостей или отражению атак, здесь оценивается способность компании действовать как единый механизм. Такие учения позволяют проверить не только технические средства защиты, но и процессы принятия решений, взаимодействие между подразделениями, соблюдение внутренних регламентов и готовность руководства действовать в условиях дефицита времени и неопределенности. На практике именно организационные ошибки, например, несогласованность действий, отсутствие коммуникации или затянутое принятие решений нередко становятся причиной серьезных последствий инцидента.

В настоящее время проведение комплексных киберучений стало распространенной практикой в сфере информационной безопасности. Такие киберучения — наследники военных командно-штабных учений, но только в сфере ИБ. Руководители обучаются вместе со своими подчиненными и сами выступают в роли обучаемых. При этом руководство осуществляет контроль, направляет работу заместителей (помощников), штаба руководства киберучениями, а также обучаемых для достижения поставленных целей, полной и качественной отработки всех задач.

В КШУ принимают участие представители руководящего состава и органов управления, специалисты подразделений по обеспечению ИБ, подразделений ИТ, администраторы безопасности, системные и сетевые администраторы, специалисты отделов обеспечения безопасности значимых объектов КИИ, а также другие сотрудники организации, так или иначе задействованные в процессе ликвидации КА. По мере развития сценария участники получают вводные о происходящих событиях: сообщения о подозрительной активности, обращения пользователей, информацию о возможной утечке данных, требования злоумышленников или запросы со стороны регуляторов и партнеров. На основании этой информации команды принимают управленческие решения, распределяют задачи между подразделениями и действуют в соответствии с утвержденными процедурами.

Киберполигон Ampire позволяет дополнить проведение КШУ реализацией практических работ в безопасной виртуальной среде, моделируя корпоративную инфраструктуру, действия злоумышленников и развитие инцидента без риска для реальных информационных систем организации. Сценарии могут быть адаптированы под отрасль, особенности инфраструктуры и уровень подготовки участников, а также включать как распространенные угрозы — например, фишинг или программы-вымогатели, — так и сложные многоэтапные атаки. Благодаря гибкой настройке формата тренировки учения могут проводиться как для отдельных подразделений, так и для всей организации с одновременным участием нескольких команд.

Эффект КШУ наиболее заметен при их систематическом и регулярном проведении. Повторяющиеся тренировки позволяют не только поддерживать навыки сотрудников, но и проверять эффективность изменений, внесенных после предыдущих учений: обновленных регламентов, новых технических средств защиты, перераспределения ролей или изменения процессов взаимодействия. Многие организации проводят такие учения ежегодно, а при существенных изменениях инфраструктуры, внедрении новых информационных систем или изменении требований регуляторов — чаще.

ВЫВОДЫ

Рост количества и сложности кибератак показывает, что обеспечить защиту организации исключительно техническими средствами уже невозможно. Даже при наличии современных средств защиты значительная часть успешных атак начинается с действий сотрудников или развивается из-за несвоевременного реагирования на инцидент. Поэтому формирование практических навыков безопасной работы, регулярное обучение цифровой грамотности должны стать частью комплексной стратегии организации в области обеспечения ИБ.

Практическая подготовка в виде киберучений позволяет проверить готовность организации к реальным угрозам. КШУ помогают выявить слабые места в технической защите, процессах взаимодействия и принятия решений, а также отработать действия всех участников — от рядовых сотрудников до руководства. Регулярное проведение таких комплексных учений повышает устойчивость организации к современным угрозам.

https://tass.ru/ekonomika/27606893



МАКСИМ ОРЛОВ
начальник отдела развития проектов
АО «ИВК»

ОДНОЮНИТОВАЯ КРЕЙТОВАЯ МОДУЛЬНАЯ СИСТЕМА ДЛЯ КРИТИЧЕСКОЙ ИНФОРМАЦИОННОЙ ИНФРАСТРУКТУРЫ

ВВЕДЕНИЕ

Тысячи российских организаций и предприятий, владеющих критической информационной инфраструктурой (КИИ), решают сегодня задачу по переводу своего компьютерного парка на технологически независимое, санкционно устойчивое отечественное оборудование. Этим обусловлен рост спроса на вычислительную технику на базе процессоров «Эльбрус». Однако российский рынок предложений практически не в полной мере покрывает потребности в гибкой комплектации, возможности кастомизации и расширения таких систем представлены крайне слабо. Особенно остро ощущается дефицит устройств с графическими ускорителями. Найти готовое решение в формате крейта[1], сочетающее, например, процессор «Эльбрус-2С3» и дискретный графический ускоритель, необходимый для выполнения специфических задач, сегодня фактически нереально.

Специалисты АО «ИВК»[2] решили эту проблему, создав компактную версию конструктива. Это первый в России программно-аппаратный комплекс (ПАК), сочетающий процессор архитектуры «Эльбрус-2С3» и графическую подсистему, которая представлена дискретным ускорителем уровня Radeon[3], выполненным в виде сменного модуля MXM 3.0 (Type A). Устройство работает под управлением операционной системы «Альт 8 СП»[4] разработки «ИВК» со встроенными средствами защиты, сертифицированной ФСТЭК России (№3866)[5].

ОДНОЮНИТОВАЯ КРЕЙТОВАЯ МОДУЛЬНАЯ СИСТЕМА

ПАК **(рис. 1)** построен по модульному принципу и фактически представляет собой «конструктор». Модульный принцип предполагает, что функции компьютера реализуются унифицированными модулями – конструктивно и функционально законченными электронными блоками. Это платы-носители, процессорные модули, блоки питания и корпусные решения. Комбинируя модули, можно выбрать нужные компоненты из набора подсистем и оперативно собрать изделие, адаптируя его к индивидуальным потребностям заказчика.

Ключевой аспект разработок компании основан на преимущественном применении российской элементной базы, прежде всего, процессоров «Эльбрус-2С3» и «Байкал-М». Сейчас компания расширяет спектр решений, разработав с нуля модули на процессорах от поставщиков из дружественных стран - например, на китайских процессорах Loongson 3A6000[6].



Рис. 1. Одноюнитовая крейтовая модульная система

[1] Крейт (от англ. crate — ящик) — это специализированный металлический каркас-шасси, предназначенный для установки стандартных электронных плат расширения, модулей управления и блоков питания. Крейты обеспечивают модули питанием, заземлением и объединяют их в общую информационную сеть (шину). Применяется в промышленной автоматизации (АСУ ТП), серверных системах, телекоммуникационном оборудовании, медицинской и специальной технике.
[2] https://ivk.ru/
[3] https://www.amd.com/en/products/graphics/workstations.html
[4] https://altsp.su/
[5] https://reestr.fstec.ru/reg3
[6] https://www.loongson.cn/EN/product/show?id=11

Корпус

Корпус ПАКа — это компактный одноюнитовый (1U) металлический крейт, который может монтироваться в стандартные 19-дюймовые стойки или шкафы. Это позволяет заказчикам увеличить плотность размещения вычислительных ресурсов и таким образом сэкономить пространство в ЦОДе или серверной.

Внутри крейта также находится тыльный модуль — плата разработки АО «ИВК», расширяющая функциональность изделия дополнительными интерфейсами.

Вычислитель

Сегодня, когда разработчики вычислительной техники для промышленных и бортовых вычислительных систем вынуждены действовать в условиях неопределенности, целесообразно применять технологию COM Express[7], которая позволяет создавать высокоэффективные вычислители в компактных форм-факторах.

Основная идея технологии COM Express состоит в разделении вычислительной системы на две составные части — стандартизованную (процессорный модуль) и специализированную (плата-носитель). Процессорный модуль объединяет процессор, микросхемы или модули системной памяти, BIOS, флеш-память и часть подсистемы ввода-вывода. На уровне платы-носителя реализованы необходимые внешние соединители, а также дополнительная функциональность: например, интерфейсы/соединители для установки плат расширения и др.

Разделение вычислителя на два компонента — процессорный модуль и плату-носитель — дает возможность создавать набор гибких решений. Например, имея в арсенале 4 процессорных модуля и 5 плат-носителей, разработчик может создавать 20 комбинаций из этих изделий и быстро собирать вычислители для 20 разных задач, не разрабатывая каждый с нуля.

Процессорные модули

Процессорный модуль ПМ-2У **(рис. 2)** представляет собой «компьютер на модуле». Он предназначен для установки в плату-носитель, совместимую с современной высокоскоростной системной шиной COM Express.

Процессорный модуль, установленный в плату-носитель, может использоваться в составе встраиваемых и бортовых вычислителей, систем промышленной автоматизации, сбора и отображения информации, работающих в тяжелых условиях эксплуатации (вибраций, ударов, широкого диапазона рабочих и предельных температур).

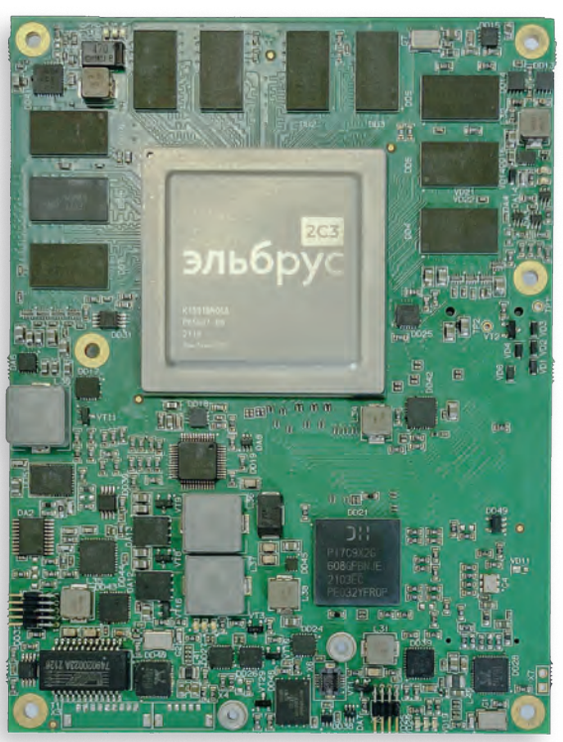


Рис. 2. Процессорный модуль ПМ-2У

[7] Форм-фактор COM Express - «компьютер-на-модуле» - представляет собой высокоинтегрированный и компактный компьютер, который можно использовать в различных приложениях.

Благодаря единому стандарту COM вычислитель можно быстро модернизировать для нового поколения процессоров: достаточно заменить COM-модуль на новый, не прибегая к перепроектированию всей системы.

Интересным решением является модуль ПМ-2У, отличающийся интеграцией процессора «Эльбрус-2С3» с оперативной памятью 16 ГБ DDR4-3200. При работе под управлением операционной системы «Альт 8 СП» задействуются возможности встроенной 3D графики. Модуль включен в Единый реестр радиоэлектронной продукции Минпромторга России[8].

Платы-носители

Платы-носители предназначены для установки процессорного модуля, совместимого с системной шиной COM Express Type 6, и выполняют функции ввода-вывода, первичной обработки информации, а также обеспечивают взаимодействие процессорного модуля с внешними устройствами.

Платы-носители разработки и производства АО «ИВК» для обеспечения критической информационной инфраструктуры (КИИ) включены в Единый реестр радиоэлектронной продукции Минпромторга России: COM-E6v2[9], COM-E6v3[10], COM-E6v4[11] и CPCI-6[12].

Рассмотрим назначение и особенности, разработанных и производимых АО «ИВК» плат-носителей.

Плата-носитель COM-E6v2

Плата-носитель COM-E6v2 **(рис. 3)** предназначена для применения в составе интеллектуальных вычислительных систем в качестве платы-носителя для встраиваемых процессорных модулей на основе процессоров «Эльбрус» (e2k), Loongson (LoongArch) и решений на архитектуре x86. Это готовое аппаратное решение с широкими функциональными возможностями и большим набором интерфейсов ввода-вывода, имеющее в своем составе в том числе четыре изолированных Serial- и два изолированных CAN-интерфейса.

Плата-носитель COM-E6v3

Плата форм-фактора COM Express Type 6 Basic **(рис. 4)**, позволяющая устанавливать процессорные модули типоразмеров Compact и Basic, совместима с процессорными модулями на базе ЦП «Эльбрус» (e2k), Loongson (LoongArch) и решений на архитектуре x86. Расширение функциональности доступно посредством установки двух модулей PCI Express Mini Card в два разъема miniPCIe, а для подключения твёрдотельных накопителей данных предназначены два разъема SATA и один mSATA. Плата оснащена набором высокоскоростных интерфейсов ввода-вывода, в том числе 4 портами Gigabit Ethernet. Плата-носитель COM-E6v3 обладает высокими характеристиками надежности и предназначена для работы в жестких условиях эксплуатации с воздействием вибраций, ударных нагрузок и широкого диапазона температур.



Рис. 3. Плата-носитель COM-E6v2



Рис. 4. Плата форм-фактора COM Express Type 6 Basic

[8] https://gisp.gov.ru/goods/#/product/3997053
[9] https://gisp.gov.ru/goods/#/product/4629450
[10] https://gisp.gov.ru/goods/#/product/4629281
[11] https://gisp.gov.ru/goods/#/product/4629287
[12] https://gisp.gov.ru/goods/#/product/4630079

Плата-носитель COM-E6v4

Плата-носитель COM-E6v4 **(рис. 5)** предназначена для установки процессорного модуля, совместимого с системной шиной COM Express Type 6, а также выполняет функции ввода-вывода, первичной обработки информации и обеспечивает взаимодействие процессорного модуля с внешними устройствами. Изделие предназначено для применения в составе интеллектуальных вычислительных систем в качестве платы-носителя для встраиваемого процессорного модуля на основе процессоров e2k («Эльбрус»), Loongson и x86, реализуя готовое аппаратное решение с широкими функциональными возможностями и большим набором интерфейсов ввода-вывода (четыре слота miniPCIe и один слот M.2 SATA).

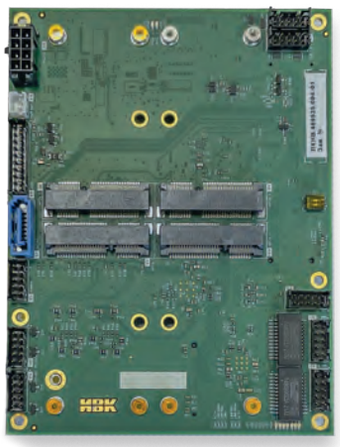


Рис. 5. Плата-носитель COM-E6v4

Плата-носитель CPCI-6

Плата-носитель COM Express Type 6 **(рис. 6)** в форм-факторе CompactPCI 6U 8HP может применяться в составе интеллектуальных вычислительных систем с широкими функциональными возможностями и большим набором интерфейсов ввода-вывода. Предназначена для совместной работы с процессорными модулями ПМ-2У и ПМ-2У-Б на базе отечественных процессоров «Эльбрус-2С3» и «Байкал-М», а также с процессорными модулями Loongson и решений на архитектуре x86. Плата-носитель оснащена лицевой панелью с портами HDMI (1 шт.), Gigabit Ethernet (2 шт.), USB 3.0 (1 шт.), USB 2.0 (1 шт.), DisplayPort (4 шт.), RS-232 (1 шт.).

Для подключения накопителей данных на печатной плате установлены 1 разъем mPCIe/mSATA и 1 разъем M.2 2242 B-Key SATA.

Также на плате-носителе есть разъем MXM Type A для подключения графического ускорителя.

Расширение функциональных возможностей системы осуществляется установкой тыльного RTM модуля.

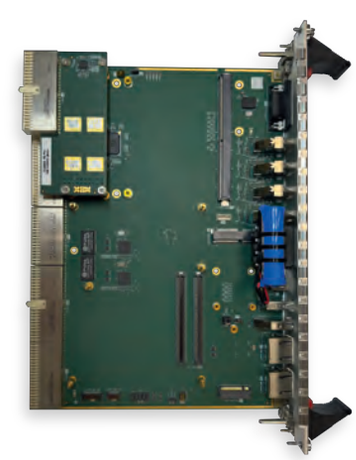


Рис. 6. Плата-носитель COM Express Type 6 в форм-факторе CompactPCI 6U 8HP

ЗАКЛЮЧЕНИЕ

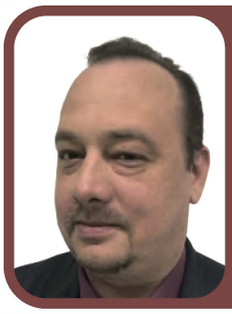
На сегодняшний день крейт АО «ИВК» полностью готов к промышленной эксплуатации. Комплектация (установка платы-носителя: COM-E6v2, COM-E6v3, COM-E6v4 или CPCI-6, также процессорного модуля с процессорами «Эльбрус», «Байкал» или Loongson) может варьироваться в зависимости от пожеланий заказчика.

ПАК может применяться в промышленности, на транспорте, в топливно-энергетическом комплексе, в организациях ВПК. ПАК идеально подходит для оснащения диспетчерских центров, особенно там, где требуется высокая надежность, длительный жизненный цикл и поддержка сложных конфигураций вывода изображения.

Также крейт подходит для оснащения конструкторских, технологических и инженерных и расчетных подразделений во всех отраслях промышленности, которые занимаются научно-техническими, конструкторскими и расчетными работами, реверс-инжинирингом, архитектурным и строительным моделированием.

Еще одна перспективная сфера применения крейта – системы работы с генеративным ИИ, построения больших языковых моделей (LLM), обработка сложных многопоточных задач.

Все эти применения реализуются на объектах КИИ, поэтому здесь не должна использоваться вычислительная техника на базе Windows/Intel. Крейтовая система АО «ИВК» позволяет создать закрытый контур обработки данных. Данные SCADA, видеонаблюдения, связи и др. обрабатываются внутри одного защищенного устройства на доверенном процессоре. Таким образом, решение АО «ИВК» содействует выполнению государственных решений и задач обеспечения импортозамещения и импортонезависимости, а также укреплению суверенитета Российской Федерации.



ЕВГЕНИЙ ГРОМЫХИН
директор представительства
ООО «Сигнатек» в г.Москве

ИМИТАТОР ТС ОРМ «ИМПУЛЬС 374». РЕАЛИЗАЦИЯ НОВЫХ НПА. СЕРТИФИКАЦИЯ.

СТАТЬЯ ДОСТУПНА В ПЕЧАТНОЙ ВЕРСИИ ЖУРНАЛА



ОЛЕГ ИВАНОВ
менеджер продуктов
квантового направления компании
АО «ИнфоТеКС»

VIPNET QRNG КВАНТОВЫЙ ГЕНЕРАТОР СЛУЧАЙНЫХ ЧИСЕЛ: ОБЗОР АРХИТЕКТУРЫ, ПРИНЦИПОВ РАБОТЫ И СРАВНИТЕЛЬНЫЙ АНАЛИЗ

АННОТАЦИЯ
Статья посвящена обзору квантовых генераторов случайных чисел в России и в мире, отечественному продукту ViPNet QRNG (Quantum Random Number Generators)[1] и его сравнению с ведущими зарубежными решениями в области физических датчиков случайных чисел. Автор рассматривает физические принципы генерации истинной случайности, архитектурные особенности современных генераторов случайных чисел, алгоритмы постобработки и статистического контроля качества случайных последовательностей. Выполнено сравнение российского продукта ViPNet QRNG с решениями ID Quantique[2], Quantinuum[3], QuintessenceLabs[4] и другими генераторами случайных чисел по принципу работы, производительности, области применения и уровню интеграции в криптографические системы. Показано, что отечественные квантовые генераторы являются перспективной платформой построения доверенной криптографической инфраструктуры и могут использоваться совместно с системами квантового распределения ключей.

ВВЕДЕНИЕ

Случайные числа являются фундаментальным элементом широкого класса информационных, вычислительных и измерительных систем. Они применяются не только для решения задач информационной безопасности, но и в моделировании физических процессов, статистическом анализе, машинном обучении, численных методах, телекоммуникациях, испытаниях технических систем, финансовом моделировании, робототехнике и других областях, где требуется формирование непредсказуемых и статистически независимых последовательностей. В связи с расширением сферы применения цифровых технологий возрастают требования к качеству, скорости и надежности источников случайных чисел.

Традиционно для получения случайных последовательностей широко используются программные генераторы псевдослучайных чисел, реализующие заданные математические алгоритмы. Несмотря на возможность формирования последовательностей с высокими статистическими характеристиками, такие генераторы являются детерминированными: значения на каждом последующем шаге определяются текущим внутренним состоянием системы и параметрами используемого алгоритма. Поэтому область их применения и качество генерируемых последовательностей во многом зависят от свойств математической модели, периода генерации, структуры алгоритма и способа формирования начального состояния.

Альтернативой детерминированным методам являются аппаратные генераторы случайных чисел, использующие физические процессы в качестве источника энтропии. В качестве таких процессов могут применяться тепловые и электрические шумы, шумы полупроводниковых приборов, нестабильность частоты генераторов, процессы радиоактивного распада и другие физические явления. Использование реальных физических источников позволяет сформировать последовательности, характеристики которых определяются не только алгоритмом обработки, но и статистическими свойствами наблюдаемого физического процесса.

Особое место среди аппаратных источников случайности занимают квантовые генераторы случайных чисел. Их функционирование основано на фундаментальных вероятностных свойствах квантовых процессов, результат отдельных измерений которых не может быть заранее детерминирован классическими моделями. В зависимости от архитектуры генератора в качестве источника случайности могут использоваться результаты измерения квантовых состояний фотонов, процессов фотодетектирования, фазовых флуктуаций лазерного излучения и других квантовых явлений. Это создает принципиальную основу для получения физически обусловленных случайных последовательностей.

Современные квантовые генераторы случайных чисел характеризуются не только высокой степенью непредсказуемости, но и возможностью формирования значительных объемов случайных данных в режиме реального времени.

[1] https://infotecs.ru/products/vipnet-qrng/
[2] https://www.idquantique.com/
[3] https://www.quantinuum.com/
[4] https://www.quintessencelabs.com/

Благодаря этому они представляют интерес для широкого спектра практических и научных задач: проведения численного моделирования методом Монте-Карло[5], формирования выборок для статистических исследований, обучения и тестирования алгоритмов искусственного интеллекта, стохастической оптимизации, моделирования сложных физических и экономических процессов, генерации случайных параметров в телекоммуникационных системах, проведения испытаний и тестирования аппаратно-программных комплексов.

Развитие датчиков и генераторов случайных чисел является важным направлением совершенствования современной вычислительной техники. Расширение областей применения случайных последовательностей формирует потребность в источниках, сочетающих высокую скорость генерации, статистическое качество, надежность, воспроизводимость заданных характеристик и возможность интеграции с различными аппаратно-программными системами. В этом контексте исследование принципов построения и характеристик квантовых генераторов случайных чисел представляет интерес как с точки зрения развития технологий формирования случайности, так и с позиции их применения в широком спектре научных, инженерных и информационных задач.

ЭВОЛЮЦИЯ ГЕНЕРАТОРОВ СЛУЧАЙНЫХ ЧИСЕЛ

Развитие генераторов случайности можно условно разделить на три поколения.

Первое поколение основано исключительно на программных алгоритмах (Linear Congruential Generator, Mersenne Twister, Xoshiro и др.) Они отличаются высокой скоростью работы, но обладают полностью детерминированной природой.

Второе поколение использует физические источники шума: тепловой шум резисторов, дробовой шум электронных компонентов, джиттер генераторов тактовой частоты и другие процессы. Хотя такие устройства обеспечивают более высокую энтропию, многие процессы подвержены внешним воздействиям и могут содержать корреляции.

Третье поколение представлено квантовыми генераторами случайных чисел, использующими процессы, фундаментально описываемые законами квантовой механики **(рис. 1)**. Именно к этой категории относится ViPNet QRNG.

ПРИНЦИПЫ ПОСТРОЕНИЯ И РАБОТЫ КВАНТОВОГО ГЕНЕРАТОРА СЛУЧАЙНЫХ ЧИСЕЛ.

Несмотря на разнообразие аппаратных реализаций можно выделить несколько типов квантовых генераторов случайных чисел (КГСЧ), представленных на **рисунке 2**.

Рассмотрим квантовый генератор случайных чисел ViPNet QRNG. Принцип работы основывается на детектировании квазиоднофотонного светодиодного излучения и его последующей математической обработке. Квантовая природа данного процесса не позволяет предсказывать получаемую последовательность чисел даже после сколь угодно точных измерений системы.

В качестве источника квазиоднофотонного излучения применяется полупроводниковый светодиод. Светодиод работает в непрерывном режиме, что повышает темп поступления фотонов на детектор. Квазиоднофотонное излучение светодиода формируется за счёт работы его специальной схемы питания.

Путь прохождения квазиоднофотонного излучения от светодиода к фотодетектору максимально короткий и недоступен для перехвата, наблюдения или воздействия извне.

Квазиоднофотонное светодиодное излучение детектируется с помощью SiPM-матрицы (кремниевые фотоумножители) — это многоканальные полупроводниковые фотоприемники, состоящие из множества соединенных в единую плату микропикселей (кремниевых лавинных фотодиодов), которые работают



Рис 1. Отличия квантового генератора случайных чисел от классического генератора случайных чисел



Рис. 2. Типы квантовых генераторов случайных чисел

[5] https://ru.wikipedia.org/wiki/Метод_Монте-Карло

в режиме Гейгера и способны регистрировать отдельные фотоны. Эффективность детектирования фотонов матрицей составляет от 10 до 30%. Использование SiPM-матрицы позволяет увеличить темп поступления фотонов в отличие от одиночного лавинного фотодетектора. Это возможно за счет условной развязки мертвого времени - это минимальный промежуток времени после регистрации фотона, в течение которого отдельная микроячейка (пиксель) матрицы полностью или частично теряет чувствительность и не может зарегистрировать следующий фотон.

Электрический сигнал с SiPM-матрицы поступает на микросхему широкополосного усилителя, где с малыми искажениями усиливается до уровня, пригодного для обработки элементами цифрового тракта.

Усиленный сигнал поступает на вход микросхемы компаратора напряжений, формирующий на выходе поток случайных по времени появления импульсов, который подается для дальнейшей обработки на вход программируемой логической интегральной схемы (далее – ПЛИС).

В ПЛИС осуществляется математическая обработка потока импульсов и формирование случайной последовательности чисел. В итоге на информационном выходе формируется последовательность случайных чисел, в которой вероятность появления 0 и 1 равна ½.

Данная последовательность случайных чисел дополнительно защищена криптографическим способом за счёт применения режима гаммирования (в соответствии с ГОСТ 34.13-2018[6], алгоритм «Кузнечик»[7]).

Итоговая генерируемая последовательность случайных чисел выдается потребителю по каналу информационного обмена шины PCIe через разъём интерфейса M.2. На **рисунке 3** представлен внешний вид ViPNet QRNG.

Технические характеристики продукта ViPNet QRNG:
1. Форм-фактор — M.2, разъем с ключами M+B совместимость с разъёмами хоста высотой от 4 мм;
2. Габариты — 80 x 23 x 15.9 мм;
3. Максимальное энергопотребление — до 3 Вт по цепи питания +3.3В;
4. Интерфейс подключения через переходную плату — PCI Express Gen1.0 x 1 (пропускная способность 2.5 Гбит/с);
5. Источник энтропии — квантовый;
6. Номинальная скорость формирования случайных чисел — 170 Мбит/с;
7. Диапазон рабочих температур — +10…+35°C.

ЗАРУБЕЖНЫЕ АНАЛОГИ

На мировом рынке существует несколько компаний, являющихся лидерами разработки квантовых генераторов случайных чисел.



Рис. 3. ViPNet QRNG производства компании «ИнфоТеКС»

Наиболее известной является ID Quantique (Швейцария), выпускающая линейку устройств Quantis QRNG. Эти генераторы основаны на регистрации отдельных фотонов и широко используются в научных исследованиях, банковском секторе и системах квантового распределения ключей.

Компания QuintessenceLabs (Австралия) разрабатывает высокопроизводительные генераторы случайности, ориентированные на центры обработки данных, облачные платформы и государственные организации. Особенностью решений является встроенная оценка энтропии в реальном времени.

Компания Quantinuum (Великобритания – США) предлагает облачные сервисы генерации квантовой случайности, использующие квантовые вычислительные процессоры и квантовые измерения.

Кроме того, крупные производители микропроцессоров (Intel, AMD, Apple) внедряют аппаратные генераторы энтропии в состав процессоров, однако большинство таких решений относится к аппаратным TRNG (True Random Number Generator) и не всегда использует квантовые физические процессы.

[6] https://files.stroyinf.ru/Data2/1/4293732/4293732952.pdf?ysclid=mtiojr44ed899221795
[7] https://ru.wikipedia.org/wiki/Кузнечик_(шифр)

Зарубежные аналоги ViPNet QRNG

Модель / Основные характеристики	ID Quantique Quantis QRNG (Швейцария)	QuintessenceLabs QRNG (Австралия)	Quantinuum QRNG (Великобритания/США)	Toshiba QRNG (Япония)	Infineon OPTIGA™ QRNG (Германия)
					
	Основан на измерении одиночных фотонов и их квантовых свойств	Использует квантовый шум полупроводникового лазера и расширенный контроль энтропии	Облачный и аппаратный QRNG на базе квантовых вычислений и квантовых измерений	Основан на квантовом фазовом шуме лазера и гомодинном детектировании	Интегрированный QRNG для встраиваемых систем и микроконтроллеров
Источник энтропии	Измерение одиночных фотонов	Квантовый шум лазера	Квантовые вычисления и квантовые измерения	Квантовый фазовый шум лазера	Квантовые эффекты в полупроводниках
Тип реализации	Аппаратный (настольный/в стойку)	Аппаратный (настольный/серверный)	Аппаратный и облачный сервис	Аппаратный (настольный)	Встраиваемый (чип/модуль)
Скорость генерации	До 1 Гбит/с	До 20 Гбит/с	До 1 Гбит/с (аппаратный) Облачный сервис – по запросу	До 1 Гбит/с	До 1 Мбит/с
Интерфейсы	USB, Ethernet, оптика	USB, Ethernet, PCIe, оптика	API, Ethernet, облачный API	USB, Ethernet	SPI, I²C
Оценка энтропии	Встроенная (онлайн)	Расширенная оценка (min-entropy, онлайн)	Встроенная (сертифицированная)	Встроенная (онлайн)	Встроенная (онлайн)
Соответствие стандартам	NIST SP 800-90B/C, AIS 31, FIPS 140-2	NIST SP 800-90B/C, AIS 31, FIPS 140-2/3	NIST SP 800-90B/C, ISO/IEC 19790	NIST SP 800-90B, FIPS 140-2	NIST SP 800-90B, Common Criteria EAL5+
Основное применение	Криптография, QKD, научные исследования	ЦОД, облака, финансы, правительственные системы	Облачные сервисы, квантовые вычисления, исследования	Криптография, телекоммуникации, финансы	IoT, встраиваемые системы, устройства безопасности
Особенности	Высокая надёжность, широкое применение в QKD-системах	Высокая производительность, расширенный мониторинг энтропии	Интеграция с квантовыми компьютерами и облачной платформой	Компактность, стабильность, низкое энергопотребление	Интеграция в чипы, низкое энергопотребление, для массового рынка

Рис. 4. Зарубежные аналоги ViPNet QRNG

Сравнение зарубежных аналогов представлено на **рисунке 4**.

ПРЕИМУЩЕСТВА И ОГРАНИЧЕНИЯ

Основными преимуществами ViPNet QRNG являются использование фундаментальной квантовой случайности, аппаратная реализация, совместимость с отечественной криптографической инфраструктурой и возможность применения в критически важных информационных системах.

К ограничениям можно отнести более узкую область коммерческого распространения по сравнению с международными аналогами и ограниченную публичную информацию о технической реализации, что затрудняет независимое сравнение отдельных характеристик (например, архитектуры источника энтропии или производительности).

Развитие QRNG связано с увеличением скорости генерации, миниатюризацией устройств, внедрением фотонных интегральных схем и расширением областей применения — от центров обработки данных и облачных сервисов до мобильных устройств и интернета вещей. Для отечественных решений перспективными направлениями являются интеграция с системами квантового распределения ключей, сертификация по национальным требованиям и применение в государственной и критической информационной инфраструктуре.

ЗАКЛЮЧЕНИЕ

Квантовые генераторы случайных чисел представляют собой перспективное направление развития современных средств формирования случайных последовательностей. ViPNet QRNG демонстрирует возможность практической реализации источника квантовой случайности в виде специализированного аппаратно-программного решения. Потенциал подобных устройств не ограничивается задачами информационной безопасности. Высокоскоростные источники случайных чисел могут использоваться при статистическом моделировании и вычислениях методом Монте-Карло, формировании случайных выборок для алгоритмов искусственного интеллекта и машинного обучения, проведении испытаний и тестирования цифровых систем, моделировании физических процессов, стохастической оптимизации, а также в различных телекоммуникационных и вычислительных системах.

Совершенствование данных устройств позволит обеспечить современные вычислительные и информационные системы надежным источником физически обусловленной случайности и расширить возможности применения случайных последовательностей в научных исследованиях, инженерных расчетах и перспективных цифровых технологиях.

Перспективы дальнейшего развития квантовых генераторов случайных чисел связаны прежде всего с увеличением скорости формирования случайных последовательностей, повышением стабильности работы устройств, совершенствованием методов контроля и оценки энтропии, снижением аппаратных ограничений и расширением возможностей интеграции с вычислительными платформами. Особое значение приобретает создание компактных и высокопроизводительных источников случайности, способных непосредственно взаимодействовать с современными процессорами, микроконтроллерами, системами связи и специализированными вычислительными комплексами.



АЛЕКСАНДР МОИСЕЕНКО
менеджер по продукту
ООО «Айдеко»

МНОГОУРОВНЕВАЯ ЗАЩИТА ПЕРИМЕТРА В МЕЖСЕТЕВЫХ ЭКРАНАХ СЛЕДУЮЩЕГО ПОКОЛЕНИЯ (NGFW)

Как система предотвращения вторжений (IPS – Intrusion Prevention System), межсетевой экран веб-приложений (WAF – Web Application Firewall), DNS Security (модуль защиты системы доменных имён) и TLS-инспекция работают в одной точке сети – и почему важно понимать путь каждого потока трафика.

Ideco – российский разработчик решений сетевой безопасности с 2005 года. Данные технологии реализованы в продукте Ideco NGFW Novum, детальное описание доступно на сайте производителя.

ВВЕДЕНИЕ. НЕ КОНВЕЙЕР, А НЕСКОЛЬКО ТРАКТОВ ОБРАБОТКИ

В описаниях межсетевых экранов следующего поколения (NGFW – Next-Generation Firewall) многоуровневую защиту часто изображают как последовательный конвейер: трафик входит с одной стороны, проходит через межсетевой экран, IPS, антивирус, контент-фильтр – и выходит «очищенным» с другой. Такая схема удобна для маркетинговых материалов, но плохо отражает реальную работу устройства.

На практике всё зависит от конкретного потока. DNS-запрос к системе доменных имён (Domain Name System), исходящее HTTPS-соединение – защищённый обмен веб-данными по HTTP поверх TLS (Transport Layer Security), произвольный транзитный трафик и обращение к опубликованному веб-приложению обрабатываются разными механизмами. У каждого из них свой объект анализа, свои профили и свои журналы.

КЛЮЧЕВОЙ ПРИНЦИП:
созданный профиль безопасности сам по себе не получает трафик.

Он должен быть назначен правилу, через которое фактически проходит соединение. Именно из-за этого возникают «бумажные» конфигурации: модуль куплен, включён и виден в интерфейсе, но конкретный поток идёт мимо него. В этой статье мы разбираем четыре типовых тракта обработки трафика на примере Ideco NGFW и показываем, какие механизмы задействованы на каждом из них.

Четыре типовых сценария прохождения трафика и задействованные в них механизмы приведены в **таблице 1**. Количество механизмов и внешних проверок, которые могут участвовать в обработке каждого из этих потоков, показано на **рисунке 1**.

Табл. 1. Типовые сценарии прохождения трафика и механизмы, которые их обрабатывают

Сценарий	Задействованные механизмы
Разрешение внешнего доменного имени	DNS-служба NGFW, DNS Security
Исходящий HTTP(S)-доступ	Межсетевой экран, Контроль приложений, IPS, TLS-инспекция, Контент-фильтр, веб-антивирус, ICAP
Другой транзитный трафик	Межсетевой экран, Контроль приложений, IPS, TLS/SSL-инспекция
Обращение к опубликованному веб-приложению	Правила доступа, Обратный прокси, WAF

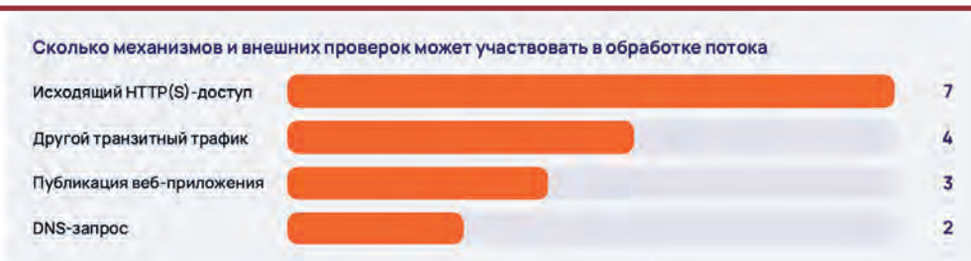


Рис. 1. Количество механизмов и внешних проверок, участвующих в обработке каждого потока

МЕХАНИЗМЫ ЗАЩИТЫ. КАЖДЫЙ МЕХАНИЗМ ВИДИТ СВОЁ

Механизмы NGFW различаются объектом анализа: межсетевой экран оперирует параметрами соединения, IPS – признаками атак в сетевом и прикладном трафике, контент-фильтр – URL (адресами веб-ресурсов) и параметрами веб-запросов. Понимание того, что именно доступно каждому механизму, – основа корректной настройки политики безопасности. Объекты анализа и назначение основных механизмов защиты NGFW приведены в **таблице 2**.

ПОЧЕМУ НОМЕР ПОРТА БОЛЬШЕ НИЧЕГО НЕ ЗНАЧИТ.

Через TCP 443 сегодня могут работать корпоративный SaaS (Software as a Service) – программный сервис, доступный пользователю через сеть без локального развёртывания серверной части, файлообменник, мессенджер, средство удалённого доступа или инструмент обхода ограничений. DPI (Deep Packet Inspection, глубокий анализ пакетов) позволяет распознавать прикладные протоколы и приложения по содержимому и признакам трафика. Контроль приложений использует результаты этого анализа в политике – вместо устаревшей фильтрации «по портам».

ВАЖНО: объединение механизмов в NGFW не означает, что они используют один движок или выполняются строго друг за другом. Это отдельные компоненты со своими объектами анализа, профилями и журналами – но с общими пользователями, группами, сетевыми объектами и единым интерфейсом управления.

ЧЕТЫРЕ ТРАКТА ОБРАБОТКИ ТРАФИКА.

Каждый поток проходит свой путь внутри NGFW. На **рисунке 2** показано, какие механизмы могут участвовать в обработке соединения в каждом из четырёх трактов.

ТРАНЗИТНЫЙ ТРАФИК. МЕЖСЕТЕВОЙ ЭКРАН, DPI И IPS

МЕЖСЕТЕВОЙ ЭКРАН С УЧЁТОМ СОСТОЯНИЯ.

Для транзитного трафика применяются правила FORWARD – правила обработки транзитного трафика, проходящего через NGFW, – с учётом состояния сессии (stateful inspection). Правило не только разрешает или запрещает соединение по адресам, портам, зонам, пользователям и GeoIP – оно же подключает к потоку дополнительные профили безопасности: Контроль приложений и IPS. Если профиль создан, но не назначен правилу, через которое реально идёт поток, – он не работает.

DPI И КОНТРОЛЬ ПРИЛОЖЕНИЙ – НЕ ОДНО И ТО ЖЕ.

DPI анализирует признаки прикладного протокола в трафике и определяет, какое приложение работает в соединении – независимо от номера порта.

Контроль приложений использует результаты DPI в политике: разрешает, ограничивает или блокирует распознанное приложение для конкретных пользователей и групп.

Табл. 2. Объекты анализа и назначение механизмов защиты NGFW

Механизм	Объект анализа	Назначение
Межсетевой экран	Адреса, порты, протоколы, зоны, состояние соединения, пользователи, группы, GeoIP	Разрешает или запрещает соединение, применяет профили безопасности
Контроль приложений	Признаки прикладного протокола и приложения (результаты DPI)	Применяет политику к распознанному приложению
IPS	Сетевой и прикладной трафик, протокольные признаки и сигнатуры	Регистрирует или блокирует атаки и аномалии
TLS-инспекция	TLS-соединение и расшифрованное содержимое	Делает содержимое доступным для остальных механизмов фильтрации
Контент-фильтр	Домены, URL и параметры веб-запросов	Управляет доступом к веб-ресурсам
DNS Security	Запросы на разрешение доменных имён	Блокирует резолвинг опасных доменов до установления соединения
Веб-антивирус	Объекты в поддерживаемом веб-тракте	Проверяет файлы на вредоносное содержимое
WAF	Входящие HTTP- и HTTPS-запросы к опубликованным приложениям	Обнаруживает и блокирует атаки на веб-приложение

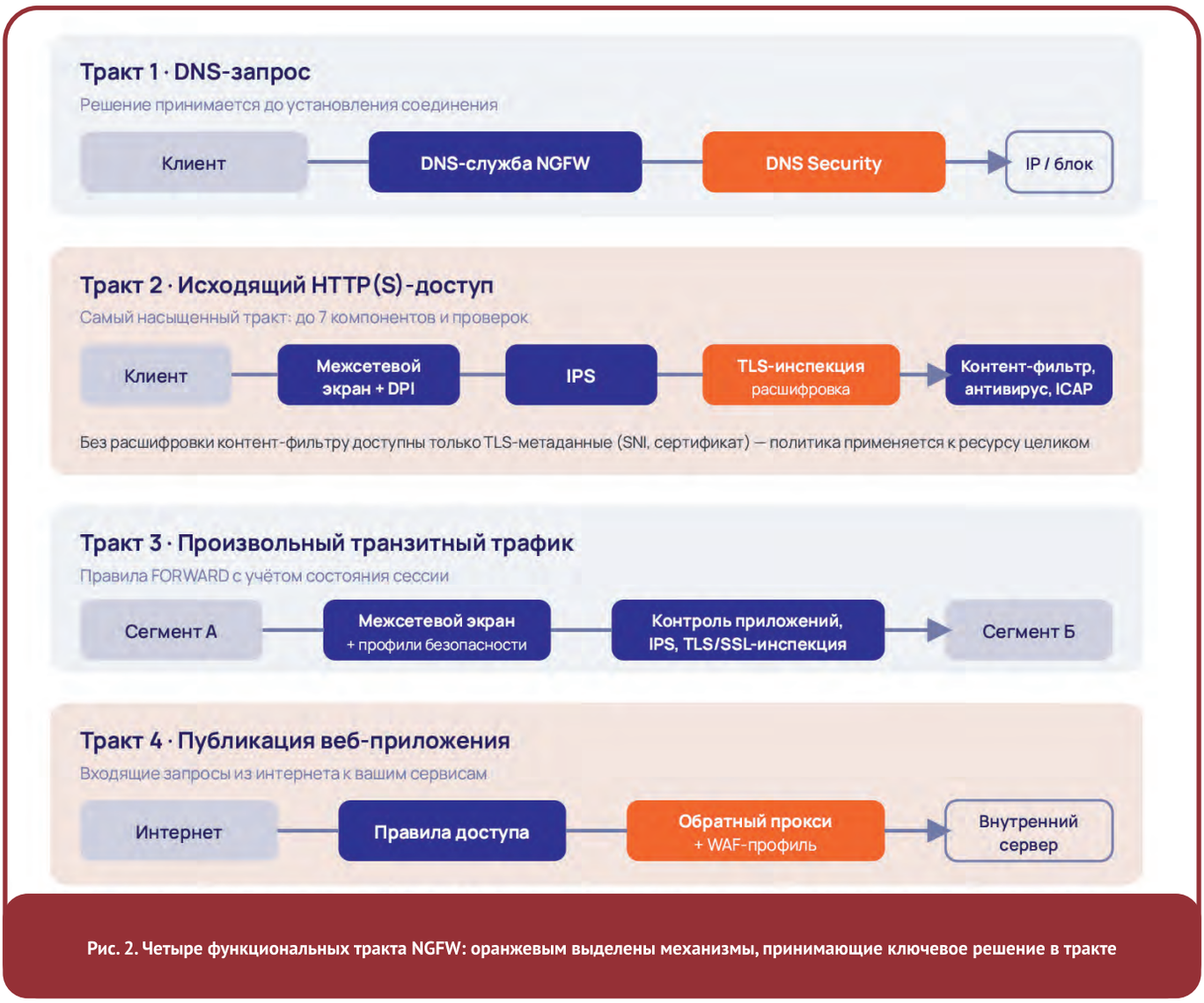


Рис. 2. Четыре функциональных тракта NGFW: оранжевым выделены механизмы, принимающие ключевое решение в тракте

IPS: ЧТО ЛОВИТ И ЧЕГО НЕ ОБЕЩАЕТ.
Система предотвращения вторжений (IPS) в NGFW анализирует сетевой и прикладной трафик по сигнатурам и протокольным признакам.

Профиль IPS определяет набор сигнатур и действие при срабатывании: журналирование, пропуск или блокировка.

IPS выявляет:
- эксплуатацию известных уязвимостей;
- сканирование сети и протокольные аномалии;
- обращения к известной вредоносной инфраструктуре.

ЧЕСТНОЕ ОГРАНИЧЕНИЕ.
IPS не гарантирует обнаружение атак с использованием ранее неизвестных уязвимостей (zero-day) и не заменяет EDR – средства обнаружения и реагирования на конечных устройствах – или анализ подозрительных объектов в изолированной среде («песочнице»). Это один из уровней эшелонированной защиты, а не универсальный детектор.

ЧТО МЕНЯЕТ ШИФРОВАНИЕ.
Без TLS-инспекции, контроля приложений и IPS доступны только параметры соединения, незашифрованные протоколы и часть TLS-метаданных. Полный URL запрашиваемого ресурса, HTTP-заголовки, тело запроса и защищённое содержимое остаются невидимыми. При этом перенос TLS-сервиса на нестандартный порт не гарантирует обход проверки: если профиль расшифровки охватывает соответствующий трафик, он будет расшифрован и на нестандартном порту.

ВЫВОД ДЛЯ АДМИНИСТРАТОРА: проверяйте не список включённых модулей, а фактически сработавшее правило для конкретного соединения – назначенные профили, счётчики и журналы.

HTTPS-ТРАКТ.
TLS-ИНСПЕКЦИЯ: ЧТО ОТКРЫВАЕТ РАСШИФРОВКА
NGFW завершает защищённое соединение клиента (включая TLS 1.3), устанавливает отдельную TLS-сессию с внешним сервером и выдаёт клиенту динамически сформированный сертификат, подписанный локальным удостоверяющим центром NGFW.

Корневой сертификат необходимо добавить в доверенное хранилище устройств – в доменной среде это делается централизованно через групповые политики.

Различия в видимости HTTPS-трафика без расшифровки и при использовании TLS-инспекции приведены в **таблице 3**.

КОНТЕНТ-ФИЛЬТР ≠ ВЕБ-АНТИВИРУС.
Первый управляет доступом к веб-ресурсам и передачей контента, второй проверяет объекты на вредоносное содержимое. Наличие одного механизма не заменяет другой.

КАК ВНЕДРЯТЬ БЕЗ ИНЦИДЕНТОВ.
Глобальное включение TLS-инспекции «одним переключателем» может нарушить работу отдельных приложений и сервисов, вызвать ошибки сертификатов и увеличить нагрузку на NGFW. Особенно это касается приложений с жёсткой привязкой к определённому сертификату или открытому ключу (certificate pinning), для которых может потребоваться настройка исключений.

Поэтому TLS-инспекцию целесообразно внедрять поэтапно. Рекомендуемый порядок:
1. Пилотная группа пользователей.
2. Ограниченный набор категорий и приложений.
3. Анализ ошибок сертификатов.
4. Формирование исключений.
5. Поэтапное расширение охвата.

HTTP/3 использует транспортный протокол QUIC поверх UDP, поэтому такой трафик не проходит обычный HTTPS-тракт на TCP. Если контроль веб-трафика обязателен, QUIC и HTTP/3 необходимо ограничить политикой – тогда браузеры с поддержкой отката переходят на TCP, а приложения без такого механизма могут потребовать отдельных исключений.

DNS-ТРАКТ.
DNS SECURITY: БЛОКИРОВКА ДО СОЕДИНЕНИЯ
DNS Security принимает решение до установления соединения. Если пользователь переходит по фишинговой ссылке, вредоносная программа обращается к серверу командования и управления (C2) или пытается определить IP-адрес домена, автоматически созданного алгоритмом генерации доменных имён (DGA, Domain Generation Algorithm) – запрос блокируется ещё до получения IP-адреса.

Анализ учитывает не только репутацию, но и аномалии DNS-трафика: структуру субдоменов, частоту запросов, типы записей. Канал к аналитической платформе защищён (DNS-over-TLS), внутренние зоны обрабатываются локально (**рис. 3**).

DNS Security работает, только если запрос проходит через NGFW: когда NGFW используется как DNS-сервер или когда включён перехват пользовательских DNS-запросов – тогда все запросы принудительно направляются на DNS-службу NGFW, даже если на устройстве настроен другой резолвер. Ограничения тоже честные: соединения по IP обходят DNS, а проверка домена не заменяет анализ последующего трафика.

Табл. 3. Видимость HTTPS-трафика: без расшифровки политика применяется только к ресурсу целиком

Что видит NGFW	Без расшифровки	С TLS-инспекцией
Домен (SNI) и поля сертификата	✓ да	✓ да
Полный URL конкретной страницы	– нет	✓ да
HTTP-метод и заголовки запроса	– нет	✓ да
MIME-тип передаваемого контента	– нет	✓ да
Файлы для проверки веб-антивирусом	– нет	✓ да

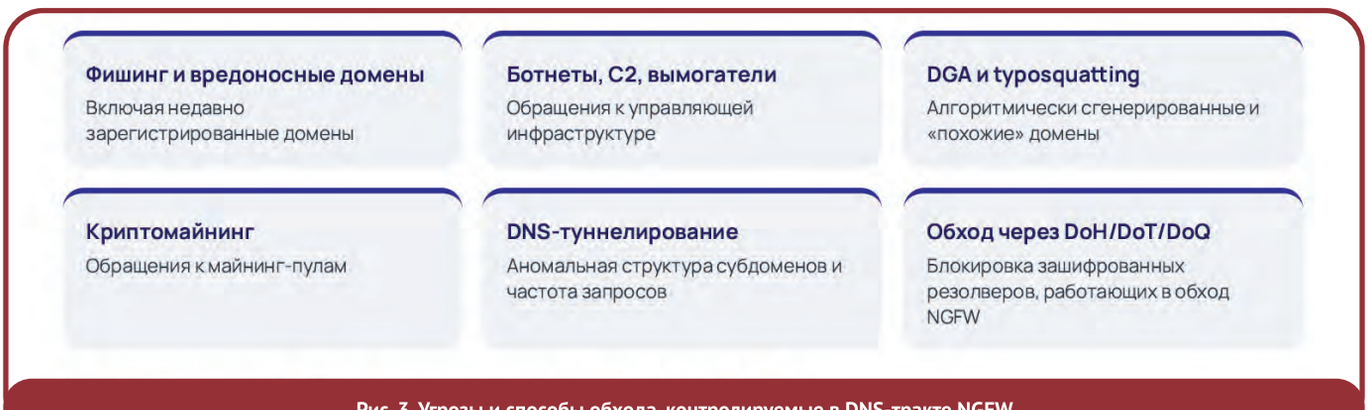


Рис. 3. Угрозы и способы обхода, контролируемые в DNS-тракте NGFW

ПУБЛИКАЦИЯ ПРИЛОЖЕНИЙ.
WAF: ЗАЩИТА ВХОДЯЩИХ ЗАПРОСОВ

WAF защищает не исходящий веб-доступ пользователей, а входящие HTTP(S)-запросы к опубликованным приложениям: выявляет типовые инъекции, межсайтовый скриптинг (XSS – внедрение сценария, выполняемого в браузере пользователя), обращения к чувствительным файлам, сканирование и протокольные аномалии. Ключевое условие – приложение должно быть опубликовано через обратный прокси с выбранным WAF-профилем. Обычный DNAT (Destination Network Address Translation) только перенаправляет входящее соединение на внутренний сервер и не включает WAF.

РЕЖИМ «ТОЛЬКО ОБНАРУЖЕНИЕ».

Подозрительные запросы журналируются, но не блокируются. С него разумно начинать для нового или изменившегося приложения: изучить профиль штатных запросов и настроить исключения.

РЕЖИМ «ОБНАРУЖЕНИЕ И БЛОКИРОВКА».

Запросы журналируются и блокируются. Включается после анализа ложных срабатываний – когда профиль штатного трафика приложения понятен.

ГРАНИЦЫ ПРИМЕНИМОСТИ.

WAF не знает бизнес-логику приложения, не исправляет уязвимый код и не заменяет безопасную разработку. Авторизация, разграничение прав и защита бизнес-операций реализуются в самом приложении.

ДИАГНОСТИКА.
ТИПОВЫЕ РАЗРЫВЫ В ЗАЩИТЕ И КАК ИХ НАЙТИ

Самые опасные пробелы возникают не из-за отсутствия модуля, а из-за того, что трафик идёт мимо него. Проверку полезно начинать не со страницы настроек, а с одного конкретного соединения: источник, назначение, протокол, сработавшее правило и события в журналах.

Наиболее характерные разрывы в конфигурации и точки их проверки приведены в **таблице 4**.

Табл. 4. Семь типовых «слепых зон» конфигурации и точки их проверки

Что предполагалось защитить	Типовой разрыв	Что проверить
Транзитное соединение	Профиль создан, но не подключён к правилу, разрешающему поток	Фактически сработавшее правило, назначенные профили, счётчики и журналы
Пользовательские DNS-запросы	Клиент использует другой резолвер или зашифрованный DNS-канал	DNS-настройки клиента, перехват обычного DNS, политика DoH/DoT/DoQ, журнал DNS
HTTPS-соединение	Трафик не расшифровывается или попадает в исключение	Профиль TLS-инспекции, доверие к корневому сертификату, исключения, журнал ошибок
Полные URL и параметры HTTP	Применяется только фильтрация по TLS-метаданным	Фактический режим HTTPS-фильтрации и доступность расшифрованного содержимого
Загружаемые файлы	Антивирус включён, но не получает объект	Доступность веб-антивируса в выбранном контексте, правило веб-фильтрации, результат проверки
Веб-трафик через HTTP/3	Клиент продолжает использовать QUIC	Политика QUIC/HTTP/3 и фактический переход соединения на TCP
Опубликованное приложение	Настроен WAF-профиль, но публикация выполнена через DNAT	Правило Обратного прокси, выбранный WAF-профиль, журнал WAF

ПРАВИЛЬНЫЙ ВОПРОС ПРИ АУДИТЕ КОНФИГУРАЦИИ – не «какие модули включены?», а «по какому тракту проходит конкретный поток, какой механизм его получает и какие данные доступны ему на этом этапе?»

ИТОГИ.
ЦЕННОСТЬ ЕДИНОЙ ПЛАТФОРМЫ

Многоуровневая защита в NGFW – это не один универсальный конвейер, а сочетание нескольких функциональных трактов. Каждый механизм решает свою задачу на своём этапе.

Роли отдельных механизмов в эшелонированной защите периметра обобщены в **таблице 5**.

ЧТО ДАЁТ ОБЪЕДИНЕНИЕ В ОДНОЙ ТОЧКЕ:

- политики используют общих пользователей, группы и сетевые объекты;
- разные уровни контроля настраиваются в одном интерфейсе;
- события можно сопоставлять внутри продукта или передавать во внешнюю SIEM (Security Information and Event Management) – систему централизованного сбора и анализа событий информационной безопасности;
- меньше отдельных точек включения в сеть и независимых контуров управления.

Но единый интерфейс не отменяет необходимость понимать путь трафика. Ошибочная привязка профиля, обход ожидаемого DNS- или веб-тракта и публикация через неподходящий механизм оставят слепую зону независимо от числа включённых модулей.

Табл. 5. Роли механизмов в эшелонированной защите периметра

Механизм	Вклад в эшелонированную защиту
DNS Security	Останавливает обращение к опасному домену до установки соединения
Межсетевой экран	Определяет допустимые направления трафика
Контроль приложений	Классифицирует прикладные протоколы и сервисы
IPS	Ищет признаки атак в разрешённых соединениях
TLS-инспекция	Открывает защищённое содержимое для подключённых механизмов
Контент-фильтр	Управляет веб-доступом
Веб-антивирус	Проверяет передаваемые объекты
WAF	Отдельно защищает опубликованные приложения через Обратный прокси

МЕРОПРИЯТИЯ АДЭ

17 МАРТА 2026 ГОДА

ИТОГОВЫЙ ДОКУМЕНТ 24-Й ЕЖЕГОДНОЙ КОНФЕРЕНЦИИ «ОБЕСПЕЧЕНИЕ ДОВЕРИЯ И БЕЗОПАСНОСТИ ПРИ ИСПОЛЬЗОВАНИИ ИКТ»

17 марта 2026 года в Москве состоялась 24-я ежегодная конференция «Обеспечение доверия и безопасности при использовании ИКТ», организованная общественно-государственным объединением «Ассоциация документальной электросвязи» (далее - АДЭ).

В работе конференции приняли участие более 150 специалистов, представляющих органы государственной власти, операторские компании связи, системных интеграторов, разработчиков оборудования и программного обеспечения, контент-провайдеров, регистраторов, а также преподаватели и студенты профильных вузов **(рис. 1)**. Программный комитет конференции сгруппировал основные направления деятельности АДЭ в сфере развития национальной ИКТ-инфраструктуры и обеспечения доверия и безопасности при её использовании в 6 тематических круглых столов, в рамках которых с докладами и предложениями выступили более 50 представителей отрасли ИКТ. АДЭ выражает благодарность членам программного комитета конференции за проделанную работу.

Конференцию открыл председатель Исполнительного комитета АДЭ А.В. Иванюк, ведущий первого круглого стола **«ОТКРЫТИЕ. ПРИОРИТЕТНЫЕ НАПРАВЛЕНИЯ ДЕЯТЕЛЬНОСТИ АДЭ В 2026 ГОДУ»**. На заседании руководители органов государственной власти и отраслевых компаний обсуждали актуальные задачи нормативного правового и нормативного технического регулирования обеспечения доверия и безопасности при использовании ИКТ, а также задачи АДЭ по содействию их реализации **(рис. 2)**.

Ведущий: Иванюк А.В., АДЭ.



Рис. 1. Участники конференции



Рис. 2. Заседание круглого стола № 1 «Открытие. Приоритетные направления деятельности АДЭ в 2026 году»

Выступили: Ивашко А.М., ФСБ России; Гайфутдинов Э.А., Администрация Президента России; Люкманов А.Р., МИД России; Ширяев К.В., Роскомнадзор; Воробьев А.А., КЦ доменов .RU/.РФ; Бадаев А.Ш., Айдеко.

На заседании круглого стола сформулированы следующие предложения:

1. Подчеркнуть значимость деятельности АДЭ и её рабочих групп в части организации взаимодействия органов государственной власти, отраслевого сообщества и бизнеса, а также экспертной проработки актуальных вопросов нормативного регулирования, обеспечения доверия и безопасности при использовании ИКТ
2. Рекомендовать использование площадки АДЭ и наработок Ассоциации для развития экспертного взаимодействия, обсуждения актуальных вопросов отрасли ИКТ и распространения выработанных подходов и практик.
3. В рамках деятельности АДЭ при координирующей роли государства и участии профильных Регуляторов для обеспечения технологической независимости Российской Федерации оказывать содействие в продвижении российских ИКТ-решений, в том числе на зарубежные рынки.

В рамках **КРУГЛОГО СТОЛА № 2 «ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ ОКАЗАНИЯ ИНФОКОММУНИКАЦИОННЫХ УСЛУГ С ИСПОЛЬЗОВАНИЕМ ИНТЕРНЕТ-ТЕХНОЛОГИЙ»** обсуждались результаты деятельности рабочей группы АДЭ по нормированию обеспечения безопасности при развитии функциональности услуг связи с использованием Интернет-технологий на примере виртуальных АТС и технологии M2M **(рис. 3)**.

Ведущий: Антипкин Р.Б., РГ АДЭ по СОРМ.
Выступили: Мацкевич А.Ю., МТС; Ярошенко И.А., Т2 Мобайл; Васильев А.В., ЛУВ; Маршак М.А., НТЦ СОТСБИ; Гулькина Д.Н., НТЦ СОТСБИ; Горовенко А.В., Минцифры России.

Выступающими отмечено, что своевременный запуск обсуждения в рамках рабочей группы АДЭ вопросов реализации услуг виртуальных автоматических телефонных станций (ВАТС), нумерации, сертификации цифровых сервисных платформ ВАТС и требований СОРМ к ним, позволил прийти к согласованному пониманию представителями отрасли роли и места ВАТС на сети связи общего пользования включая, в том числе функции, задачи и оказываемые услуги.



Рис. 3. Заседание круглого стола № 2
«Обеспечение безопасности оказания инфокоммуникационных услуг с использованием интернет-технологий»

Выступающие доложили о результатах деятельности рабочей группы АДЭ по подготовке проектов нормативно-правовых актов в части регулирования виртуальных АТС. Рабочей группой АДЭ были подготовлены проекты приказов: «Об утверждении Требований к применению оборудования систем коммутации, включая программное обеспечение, обеспечивающего выполнение установленных действий при проведении оперативно-разыскных мероприятий при использовании виртуальных телефонных станций» (далее – правила применения ВАТС) и «Об утверждении Требований к применению оборудования реализующего функции коммутации и управления услугами. Часть I. Требования к применению виртуальных телефонных станций» (далее – правила применения оборудования СОРМ при использовании ВАТС).

Участниками круглого стола отмечена необходимость проработки вопросов нормативного правового регулирования отношений, возникающих при использовании технологии «от устройства к устройству» (M2M, machine-to-machine), поскольку в настоящее время отсутствуют чётко определённые подходы в данной сфере. Подчеркнута актуальность выработки согласованных решений, направленных на уточнение действующего законодательства с учётом особенностей M2M-сервисов и интересов участников рынка и государства. Обсудили наиболее распространённые и актуальные проблемы, возникающие при использовании технологии M2M.

На заседании круглого стола сформулированы следующие предложения:

1. Поддержать согласование подготовленных в рамках рабочей группы АДЭ проектов нормативных правовых актов, в том числе:
   - правила применения ВАТС;
   - правила применения оборудования СОРМ при использовании ВАТС.
2. Исполнительной дирекции АДЭ выслать проекты правил применения ВАТС и правил применения оборудования СОРМ при использовании ВАТС в Минцифры России для возможного использования в работе как согласованную позицию отраслевого сообщества.
3. В рамках рабочей группы АДЭ продолжить обсуждение вопросов регулирования M2M.

В рамках **КРУГЛОГО СТОЛА № 3 «КООРДИНАЦИЯ УСТОЙЧИВОГО И БЕЗОПАСНОГО ФУНКЦИОНИРОВАНИЯ НАЦИОНАЛЬНОЙ ДОМЕННОЙ ЗОНЫ»** обсуждались приоритетные задачи Координационного центра национальных доменов по комплексному обеспечению устойчивого и безопасного функционирования национальной доменной зоны и её развитию **(рис. 4)**.

Ведущий: Воробьев А.А., КЦ доменов .RU/.РФ.
Выступили: Рогдев А.Н., ТЦИ; Морозов Е.Н., MSK-IX; Мирошников Б.Н., ГК Гарда; Хаазе И., ЭластикХостинг.

В ходе круглого стола участниками было отмечено, что приоритетными задачами развития национального доменного пространства Российской Федерации являются повышение устойчивости инфраструктуры доменной зоны, совершенствование механизмов противодействия злоупотреблениям, а также развитие взаимодействия с государственными и отраслевыми структурами.

Отдельное внимание было уделено вступающим в силу с 1 сентября 2026 года изменениям в регулировании доменного рынка. Участники подчеркнули значимость внедрения обязательной идентификации администраторов доменных имен с использованием единой системы идентификации и аутентификации для всех операций с доменами. Отмечено, что данный механизм позволит повысить прозрачность операций, снизить возможности злоупотреблений, а также укрепить доверие пользователей и международного сообщества к российской доменной зоне.



Рис. 4. Заседание круглого стола № 3 «Координация устойчивого и безопасного функционирования национальной доменной зоны»

Также участники обсудили вводимый специальный порядок регистрации и обслуживания доменных имен государственных организаций, включая механизм резервирования доменных имен после прекращения их использования. Подчёркнута важность данной меры для предотвращения неправомерного использования доменных имен и повышения устойчивости цифровой инфраструктуры государственного сектора.

В ходе дискуссии отдельно отмечена эффективность реализуемых мер по противодействию компьютерным инцидентам, в том числе в рамках проекта «Доменный патруль». Участники подчеркнули высокий уровень оперативности реагирования на фишинговые атаки и необходимость дальнейшего совершенствования соответствующих механизмов.

На заседании круглого стола сформулированы следующие предложения:

1. Поддержать реализацию мер, направленных на повышение устойчивости и безопасности функционирования национальной доменной зоны Российской Федерации.
2. Поддержать развитие нормативного регулирования в части регистрации и обслуживания доменных имен государственных организаций, включая механизмы резервирования доменных имен. Рассмотреть возможность использования площадки АДЭ для обсуждения проектов подзаконных актов по указанному направлению.
3. Продолжить совершенствование механизмов противодействия использованию доменной инфраструктуры в целях фишинга, мошенничества и иных противоправных действий, в том числе за счёт развития взаимодействия с государственными и отраслевыми структурами.

В рамках **КРУГЛОГО СТОЛА № 4 «НОРМИРОВАНИЕ УРОВНЯ ДОВЕРИЯ ДЛЯ ТКО»** обсуждалась выработка критериев, требований и методик проверки доверенного телекоммуникационного оборудования (ТКО) с точки зрения контроля и управления функциональностью **(рис. 5)**.

Ведущий: Хасин Е.В., Минцифры России.
Выступили: Стариков П.П., ФГАНУ ЦИТиС; Ерёменко В.А., МТС; Лачинов А.Р., ВымпелКом; Трещиков В.Н., Т8; Середин Н.Е., АНО «ТКО»; Иванюк А.В., АДЭ.

В рамках круглого стола обсуждались подходы к формированию и нормированию уровня доверия к телекоммуникационному оборудованию и программно-аппаратным средствам. Участниками круглого стола отмечено, что понятие доверия является комплексным и требует структурированного подхода, включающего разделение доверия к производителю и доверия к процессам разработки и производства. Подчёркнуто, что основными критериями доверия являются обеспечение управляемости и контролируемости функционирования программно-аппаратных комплексов (ПАК) при их использовании.

В ходе обсуждения отмечено, что действующая система контроля и учёта оборудования (включая реестры и механизмы сертификации) в целом сформирована и требует дальнейшего развития, а не радикального пересмотра. Также отмечено, что при формировании требований к доверию необходимо учитывать реальную структуру телекоммуникационной инфраструктуры, включая использование как отечественных, так и уже внедренных зарубежных компонентов.

Отдельное внимание было уделено вопросам управления инфраструктурой сетей связи. Участники подчеркнули, что наличие защищённой системы управления является одним из ключевых элементов обеспечения доверия и должно предусматривать контроль доступа, применение криптографических механизмов и мониторинг состояния оборудования.

Отмечено также, что необходим переход к вероятностной оценке рисков и формированию измеримых критериев доверия, основанных на способности системы сохранять управляемость и контроль функциональности.



Рис. 5. Заседание круглого стола № 4 «Нормирование уровня доверия для ТКО»

На заседании круглого стола сформулированы следующие предложения:

1. Продолжить в рамках профильного комитета АДЭ разработку методологических подходов к определению и нормированию уровня доверия к телекоммуникационному оборудованию.
2. При формировании требований к доверию учитывать реальную инфраструктуру связи и риски изменения поставщиков.
3. Считать ключевыми критериями доверия обеспечение управляемости и контроль функционирования ПАК.

В рамках **КРУГЛОГО СТОЛА № 5 «НОРМАТИВНОЕ РЕГУЛИРОВАНИЕ ДОВЕРЕННЫХ ПАК»** обсуждалась реализация соглашения между Минпромторгом России и АДЭ, включая вопросы актуального нормативного правового и нормативного технического регулирования требований к доверенности программно-аппаратных комплексов, порядок подтверждения соответствия и возможности АДЭ по содействию реализации государственной политики в области обеспечения технологической независимости **(рис. 6)**.

Ведущий: Мардер С.Н., Минпромторг России.
Выступили: Иванюк А.В., АДЭ; Гоголев Д.В., НПО «КИС»; Хасин Е.В., Минцифры России; Трушкин К.А., МЦСТ; Панышев Д.О., РТК-ЦОД.

Участники обсудили практические аспекты внедрения существующих требований к уровню доверия в отраслевую инфраструктуру и подчеркнули необходимость комплексного взаимодействия регуляторов, производителей, операторов связи и разработчиков решений. Особое внимание было уделено синхронизации новых нормативных требований с действующими процессами перехода на отечественные решения.

Отдельно была выделена роль государственных реестров как инструмента прозрачности и контроля доверенных решений и необходимость дальнейшего развития такого подхода, правил включения в реестры, актуализацию сведений в них и повышение достоверности оценки производителей и поставщиков.

Выступающие обратили внимание на существующий разрыв между нормативными требованиями и фактической готовностью рынка: часть производителей не располагает достаточными ресурсами для полного соблюдения новых требований, особенно в части документирования процессов разработки, прослеживаемости компонентов и подтверждения происхождения технологической базы. В этой связи была подчеркнута целесообразность поэтапного внедрения новых требований.

Отдельный блок дискуссии был посвящён критериям оценки доверия. Подчёркнуто, что уровень доверия должен определяться не только происхождением оборудования, а также такими характеристиками, как управляемость и контроль функциональностью, прозрачность архитектуры, и наличие защищённых механизмов обновления и сопровождения.

Кроме того, участники пришли к выводу о необходимости формирования единых методических подходов к оценке доверия, обеспечивающих сопоставимость результатов и единообразное применение требований на рынке.

На заседании круглого стола сформулированы следующие предложения:

1. На площадке АДЭ продолжить разработку предложений в нормативную базу регулирования доверенных ПАК с учётом необходимости синхронизации с программами перехода на отечественные решения.
2. Считать целесообразным дальнейшее развитие государственных реестров доверенных решений, в том числе унификацию критериев включения, актуализацию данных и повышение достоверности оценки производителей и поставщиков.
3. Поддержать подход поэтапного внедрения требований к доверенным ПАК с установлением адаптационного периода для участников рынка.
4. Отметить важность разработки единых унифицированных критериев оценки доверия, применимых для различных категорий телекоммуникационного оборудования и программно-аппаратных комплексов.



Рис. 6. Заседание круглого стола № 5 «Нормативное регулирование доверенных ПАК»

В рамках **КРУГЛОГО СТОЛА № 6 «СОДЕЙСТВИЕ РАЗРАБОТКЕ И ВНЕДРЕНИЮ ПАК ДЛЯ ОТРАСЛИ ИКТ»** обсуждались нормативные, технологические и процедурные аспекты содействия разработке и внедрению программно-аппаратных комплексов для отрасли ИКТ с использованием ресурсов АДЭ. Рассматривались как отдельные проекты, так и обеспечение комплексного подхода к решению взаимосвязанных задач.

Ведущий: Иванюк А.В., АДЭ.
Выступили: Торбенко Е.Б., ФСТЭК России; Раевский А.Н., НКЦКИ; Смирнов А.В., Базальт СПО; Пименов А.В., МЦСТ; Семилетов Д.А., Альтэл; Кадомский В.С., НТЦ ИТ РОСА.

На заседании круглого стола обсудили вопросы развития отечественных программно-аппаратных комплексов для отрасли ИКТ, подчеркнув, что их создание и внедрение требует комплексного подхода, выходящего за рамки задач импортозамещения. Было отмечено, что необходима системная модель взаимодействия между регуляторами, разработчиками программного обеспечения, производителями оборудования и операторами связи. В ходе дискуссии подтверждено, что нормативная база для внедрения доверенных отечественных решений последовательно формируется, однако ключевой задачей остаётся её адаптация к практическим потребностям отрасли и совершенствование механизмов применения.

Участники указали, что на рынке уже сформирован базовый набор российских решений, включая операционные системы, платформы виртуализации и средства управления инфраструктурой. Вместе с тем одной из основных проблем остаётся отсутствие устойчивой кооперации между разработчиками ПАК и производителями прикладного программного обеспечения, что приводит к недостаточной совместимости их продуктов. Подчёркнуто, что отсутствие достаточного количества подтверждённых технологических партнёрств является серьёзным барьером для масштабного внедрения ПАК, особенно в сфере КИИ. Также отмечена необходимость постоянного обновления технологических стеков, модернизации внедрённых решений и поддержания их совместимости с новыми поколениями оборудования. В этой связи участники подчеркнули важность перехода к непрерывной модели сопровождения ПАК на всём жизненном цикле.

В ходе круглого стола также обсуждались вопросы кадрового обеспечения отрасли, включая роль базовой кафедры АДЭ в подготовке специалистов для работы с отечественными программно-аппаратными комплексами. Была отмечена необходимость повышения значимости вовлечения ИТ-компаний в деятельность базовых кафедр в рамках оценки участия бизнеса в образовательной деятельности.

В ходе обсуждения также поднимались вопросы формирования единых подходов к оценке доверия, сертификации и развитию отраслевых стандартов.

На заседании круглого стола сформулированы следующие предложения:

1. Рассмотреть на площадке АДЭ вопросы совершенствования подходов к моделированию актуальных угроз и нарушителей с учётом практики выявления современных рисков информационной безопасности.
2. Подчеркнуть актуальность дальнейшего совершенствования нормативной базы в сфере разработки и внедрения отечественных ПАК с учётом практических потребностей отрасли.
3. Обратить внимание на целесообразность формирования единых стандартов оценки ПАК, включая унифицированные требования к архитектуре и прозрачные процедуры подтверждения соответствия.
4. Отметить важность формирования долгосрочных механизмов государственной и отраслевой поддержки внедрения отечественных ПАК в ИКТ-инфраструктуре.
5. Активнее использовать ресурсы АДЭ в части содействия разработке и внедрению программно-аппаратных комплексов для отрасли ИКТ.
6. Пригласить отраслевые организации принять участие в целевом наборе студентов по магистерской программе «Доверенные программно-аппаратные средства для обеспечения безопасности КИИ» на базовой кафедре АДЭ в МТУСИ.



Рис. 7. Заседание круглого стола № 6 «Содействие разработке и внедрению ПАК для отрасли связи»

9 ОКТЯБРЯ 2025 ГОДА

СОГЛАШЕНИЕ О СОТРУДНИЧЕСТВЕ МЕЖДУ МИНПРОМТОРГОМ РОССИИ И АДЭ

На XXV ежегодной конференции общественно-государственного объединения «Ассоциация документальной электросвязи» (далее — АДЭ, Ассоциация) «Состояние и перспективы развития ИКТ-инфраструктуры» было подписано соглашение между Министерством промышленности и торговли Российской Федерации и самой Ассоциацией об эффективном информационном, организационном, экспертно-аналитическом сотрудничестве сторон **(рис. 1)**.

Соглашение, подписанное заместителем министра промышленности и торговли Василием Шпаком и председателем Исполнительного комитета АДЭ Александром Иванюком, направлено на создание условий для устойчивого развития и популяризации сферы архитектурного проектирования российских процессоров, в том числе применения таких процессоров российскими и зарубежными производителями в составе производимой радиоэлектронной продукции.

Основными приоритетами совместной деятельности стали два ключевых направления:

- **Методологическое направление.** Включает в себя подготовку предложений по: совершенствованию нормативного регулирования радиоэлектронной отрасли; научно-техническому развитию сферы архитектурного проектирования российских процессоров; продвижению архитектур российских процессоров; предложений по актуализации действующих и разработке новых межгосударственных стандартов и национальных стандартов Российской Федерации.
- **Просветительское направление.** Включает в себя взаимодействие с производителями радиоэлектронной продукции, разработчиками программного обеспечения для подготовки предложений по вопросам развития и популяризации сферы архитектурного проектирования российских процессоров и разработке и реализации образовательных программ.



Рис. 1. Соловьев Иван Константинович (слева) и Иванюк Александр Викторович (справа) на подписании Соглашения о сотрудничестве

Минпромторг России
от 09.10.2025 № с268/11

СОГЛАШЕНИЕ О СОТРУДНИЧЕСТВЕ
между Министерством промышленности и торговли Российской Федерации и общественно-государственным объединением «Ассоциация документальной электросвязи»

г. Москва «9» октября 2025 г.

Министерство промышленности и торговли Российской Федерации в лице заместителя Министра промышленности и торговли Российской Федерации Шпака Василия Викторовича, действующего на основании доверенности от 11 сентября 2025 г. № АА-101952/11, и

общественно-государственное объединение «Ассоциация документальной электросвязи», в лице Председателя Исполнительного комитета Иванюка Александра Викторовича, действующего на основании Устава,

именуемые в дальнейшем «Стороны», заключили настоящее Соглашение о нижеследующем:

1. ПРЕДМЕТ СОГЛАШЕНИЯ

Предметом настоящего Соглашения является установление в пределах компетенции Сторон и в соответствии с законодательством Российской Федерации эффективного информационного, организационного, экспертно-аналитического сотрудничества Сторон в целях создания условий для устойчивого развития и популяризации сферы архитектурного проектирования российских процессоров, в том числе применения таких процессоров российскими и зарубежными производителями в составе производимой радиоэлектронной продукции.

2. ОСНОВНЫЕ НАПРАВЛЕНИЯ СОТРУДНИЧЕСТВА

2.1. В целях реализации настоящего Соглашения Стороны в соответствии с законодательством Российской Федерации в пределах компетенции осуществляют сотрудничество по следующим направлениям:

2.1.1. «Методологическое направление»:

подготовка предложений по совершенствованию нормативного регулирования радиоэлектронной отрасли в сфере архитектурного проектирования российских процессоров;

подготовка предложений, направленных на научно-техническое развитие сферы архитектурного проектирования российских процессоров;

подготовка предложений по продвижению архитектур российских процессоров на территории Российской Федерации, государств-членов Евразийского экономического союза и иных международных рынках;

подготовка предложений по актуализации действующих и разработке новых межгосударственных стандартов и национальных стандартов Российской Федерации, учитывающих перспективные международные требования, к радиоэлектронной продукции в части архитектур российских процессоров.

2.1.2. «Просветительское направление»:

взаимодействие с производителями радиоэлектронной продукции, разработчиками программного обеспечения, субъектами критической информационной инфраструктуры, образовательными учреждениями по вопросу развития и популяризации сферы архитектурного проектирования российских процессоров;

подготовка предложений по организации, проведению и участию в мероприятиях, направленных на развитие и популяризацию сферы архитектурного проектирования российских процессоров;

подготовка предложений по разработке и реализации образовательных программ, включая стажировки, производственные и исследовательские практики, обеспечивающих формирование и применение в практической деятельности знаний и компетенций, необходимых для внедрения и эксплуатации архитектур российских процессоров;

подготовка предложений по разработке и реализации программ дополнительного профессионального образования, содействующих обеспечению формирования и применения в практической деятельности знаний и компетенций, необходимых для внедрения и эксплуатации архитектур российских процессоров.

2.2. Перечень направлений сотрудничества может дополняться и уточняться по согласованию Сторон в пределах компетенции в соответствии с законодательством Российской Федерации.

3. ФОРМЫ СОТРУДНИЧЕСТВА

3.1. В целях реализации настоящего Соглашения Стороны в пределах компетенции и в соответствии с законодательством Российской Федерации осуществляют сотрудничество в следующих формах:

обмен информацией (посредством направления Сторонами писем, организации встреч представителей Сторон) и документами, относящимися к сфере сотрудничества Сторон в рамках настоящего Соглашения;

совместное участие в организации и проведении мероприятий, в том числе семинаров, конференций, выставок, форумов, а также заблаговременное информирование Сторонами друг друга о планируемых к проведению мероприятиях;

участие Сторон (по приглашению) в мероприятиях по вопросам развития радиоэлектронной отрасли в сфере архитектурного проектирования российских процессоров.

3.2. Сотрудничество Сторон может осуществляться в иных согласованных формах, обеспечивающих реализацию настоящего Соглашения, в пределах компетенции и в соответствии с законодательством Российской Федерации.

4. КОНФИДЕНЦИАЛЬНОСТЬ

4.1. Стороны в процессе реализации настоящего Соглашения обеспечивают в установленном законодательством Российской Федерации порядке защиту сведений, составляющих государственную, коммерческую, служебную и иную охраняемую законом тайну.

4.2. Информация, которую одна из Сторон относит к конфиденциальной и сообщила об этом другой Стороне, является конфиденциальной для другой Стороны.

4.3. Передача информации третьим лицам осуществляется с письменного согласия Стороны, предоставившей эту информацию.

4.4. Конфиденциальная информация может быть предоставлена третьим лицам в соответствии с законодательством Российской Федерации или в рамках судебного (арбитражного, третейского) разбирательства.

5. ПРОЧИЕ УСЛОВИЯ

5.1. Настоящее Соглашение не является предварительным договором в соответствии со статьей 429 Гражданского кодекса Российской Федерации, рамочным договором в соответствии со статьей 429.1 Гражданского кодекса Российской Федерации или договором простого товарищества в соответствии со статьей 1041 Гражданского кодекса Российской Федерации, не влечет возникновения юридических, финансовых, имущественных обязательств, а неисполнение его положений не может являться основанием для возникновения ответственности Сторон.

5.2. Стороны признают, что настоящее Соглашение не может рассматриваться как создающее благоприятные условия для деятельности отдельного хозяйствующего субъекта (хозяйствующих субъектов), которые могут иметь своим результатом ограничение конкуренции или ущемление интересов иных хозяйствующих субъектов.

5.3. Стороны обязуются не выступать с публичными заявлениями без предварительного согласования с другими Сторонами по вопросам сотрудничества в рамках настоящего Соглашения.

5.4. Любая реклама, относящаяся к сотрудничеству Сторон в рамках настоящего Соглашения, должна быть согласована заранее между Сторонами.

5.5. Любые изменения и дополнения в настоящее Соглашение могут вноситься по взаимному согласию Сторон путем подписания дополнительных соглашений.

5.6. Настоящее Соглашение заключено на неопределенный срок и вступает в силу со дня его подписания Сторонами. Каждая из Сторон вправе в одностороннем порядке расторгнуть настоящее Соглашение, письменно уведомив об этом другую Сторону не позднее чем за 2 (два) месяца до предполагаемой даты расторжения.

5.7. Настоящее Соглашение составлено в 2 (двух) экземплярах, имеющих одинаковую силу, по одному экземпляру для каждой из Сторон.

6. РЕКВИЗИТЫ И ПОДПИСИ СТОРОН

Министерство промышленности и торговли Российской Федерации	Общественно-государственное объединение «Ассоциация документальной электросвязи»
Адрес местонахождения: 125039, г. Москва, Пресненская наб., д. 10, стр. 2	Адрес местонахождения: 103375, г. Москва, ул. Тверская, д.7
ИНН 7705596339/КПП 770301001 ОГРН 1047796323123	ИНН 7710041879/КПП 771001001 ОГРН 1037739282129
Заместитель Министра промышленности и торговли Российской Федерации	Председатель Исполнительного комитета
_____ / В.В. Шпак /	_____ /А.В. Иванюк/

ЧЛЕНЫ АДЭ

ПО СОСТОЯНИЮ НА 30 СЕНТЯБРЯ 2026 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
- Комфортел
- Консорциум "Телекоммуникационное оборудование"
- Координационный центр доменов .RU/.РФ
- Космическая связь
- Манго Телеком
- 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
- Научно-производственный центр «Электронные вычислительно-информационные системы»
- НИИ Интеграл
- НоваКард
- Новофон-ОС
- Норси-Транс
- НТЦ ИТ РОСА
- НТЦ Модуль
- НТЦ Протей
- НТЦ СОТСБИ
- Пенсионный фонд Российской Федерации
- Позитив Текнолоджиз
- Российская Академия Наук
- Российская телевизионная и радиовещательная сеть (РТРС)
- Ростелеком
- Санкт-Петербургский государственный университет телекоммуникаций им. проф. М.А.Бонч-Бруевича
- СИГНАЛТЕК
- Сигнатек
- Системы и Решения
- Специальные технологии
- СТАРТЕЛЕКОМ
- Стек Софт
- Т2 Мобайл
- Т8
- Телепорт
- Телкор
- ТехАргос
- Т-Мобайл
- Трамплин Электроникс
- Труконф
- УК Гарда
- Фастком
- 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
- Эра Технологий
- ЭР-Телеком Холдинг
- Яндекс