Стратегия использования российского программного обеспечения

Введение

Президент России Владимир Путин обозначил использование российского программного обеспечения как стратегическую задачу национального уровня. “ЛИНКМЕТР” и аналогичные решения полностью ей соответствуют.

Применение отечественного ПО напрямую связано с курсом на технологический суверенитет, защиту критической инфраструктуры от внешних угроз и выполнение ранее принятых указов (Указ Президента Российской Федерации от 01.05.2022 № 250 “О дополнительных мерах по обеспечению информационной безопасности Российской Федерации”, Указ Президента Российской Федерации от 28.02.2024 № 145 “О Стратегии научно-технологического развития Российской Федерации” и другие). Первоочередными задачами являются:

замена иностранного ПО (SpeedTest, ThousandEyes и т. д.);

ликвидация рисков передачи данных за рубеж (как в случае с Ookla);

исключение возможности скрытого мониторинга сетей РФ иностранными спецслужбами.

Для выполнения требуется осуществление ряда мер, в том числе поддержка отечественных разработчиков, а также создание конкурентной экосистемы российских ИТ-решений (аналогично СПФС, ОС “Аврора”, “Эльбрус”) и снижение зависимости от санкционного давления (например, отключение от западных сервисов).

Конечной целью является укрепление кибербезопасности путем интеграции с ГосСОПКА, ФСТЭК и ФСБ для оперативного выявления угроз в соответствии требованиям ФЗ-152 (персональные данные) и ФЗ-187 (критическая инфраструктура).

Для ускорения проведения процесса необходимы следующие меры:

жесткое регулирование — запрет операторам связи использовать иностранные системы тестирования (по аналогии с отказом от SWIFT), обязательное применение “ЛИНКМЕТР” в госсекторе и у операторов связи;

финансовая поддержка — субсидии разработчикам (как в стратегии НТР до 2030 года), налоговые льготы для компаний, внедряющих российское ПО;

развитие инфраструктуры — создание распределенной сети серверов “ЛИНКМЕТР” по всей России, интеграция с единой сетью электросвязи РФ и суверенным интернетом.

Противодействие стратегии цифрового колониализма

Цифровой колониализм — это современная форма доминирования развитых стран (прежде всего США и их союзников) над остальным миром через контроль над технологиями, данными и цифровой инфраструктурой.

Россия, столкнувшись с санкциями, отключением от западных сервисов (SWIFT, Cloudflare, Microsoft) и кибервойной, активно формирует систему цифрового суверенитета, чтобы избежать зависимость от враждебных юрисдикций.

Основные проявления цифрового колониализма:

при технологической зависимости — доминирование западных ОС (Windows, iOS, Android) и софта (Microsoft, SAP, Oracle), контроль над интернет-инфраструктурой (DNS-серверы в США, облачные платформы AWS, Google Cloud), монополия на телекоммуникационное оборудование (Cisco, Ericsson, Nokia);

при финансовом контроле — применение инструмента санкционного давления SWIFT (отключение России, Ирана, Венесуэлы), блокировка платежей Visa/Mastercard по политическим мотивам, криптовалюта под контролем США (SEC регулирует Tether, Coinbase и другие);

использование данных как ресурс — сбор информации через соцсети (Meta — признана экстремистской и запрещена в России, Google) и телекоммуникационные сервисы (SpeedTest), искусственное занижение скорости Рунета в зарубежных рейтингах (Ookla, Netflix Index).

В ходе развязывания Западом информационной войны США сумели создать по всему миру в телекоммуникационной сфере стандартные методы тестового контроля каналов связи. Такая ситуация в телекоммуникационной сфере аналогична той, что сложилась в банковской отрасли, когда США объединили банки всех стран мира в единую систему перевода денег SWIFT, которая позволяет банкам этих стран быстро осуществлять платежи между собой, а США в этот время осуществляют контроль перевода денег между странами по всему миру.

Действительно, американские технологии и стандарты доминируют в мировых коммуникационных системах, а SWIFT (Society for Worldwide Interbank Financial Telecommunication) долгое время оставалась практически безальтернативной системой международных платежей.

США исторически играли ведущую роль в разработке и продвижении стандартов связи (например, TCP/IP, GSM, 5G через компании типа Qualcomm). Это дает им возможность:

влиять на безопасность данных (например, через “бэк-доры” или сотрудничество с провайдерами);

контролировать трафик через точки обмена интернет-трафиком (IXP), многие из которых расположены в США;

использовать технологии мониторинга (как в случае с программой PRISM, раскрытой Сноуденом);

аналогично SWIFT отслеживать финансовые потоки, контролировать телекоммуникационные стандарты и перехватывать информацию.

Для снижения зависимости страны принимают следующие шаги:

развивают собственные стандарты (например, китайский 5G от Huawei);

создают альтернативные DNS-серверы и сегменты интернета (например, Рунет);

используют криптографию и VPN для защиты данных;

применяют собственные средства мониторинга, такие как “ЛИНКМЕТР”.

Российский проект

Российский проект “ЛИНКМЕТР” — это комплекс программных продуктов и аппаратных средств, входящие в пространственно разнесенные измерительные аппаратно-программные комплексы (ИАПК), предназначенные для определения параметров:

систем определения длительности соединений (СИДС),

систем измерения передачи данных (СИПД),

зондов, каналов и сетей передачи данных с использованием современных дистанционных методов измерений.

Предпосылкой разработки российского проекта “ЛИНКМЕТР” была необходимость технологического достижения цифрового суверенитета и технологической независимости России в телекоммуникационной сфере. Он предназначен для измерения параметров каналов связи в режиме реального времени, что особенно важно для обеспечения целостности, устойчивости и безопасности сетей передачи данных в условиях киберугроз и санкционного давления. Основные функции и задачи “ЛИНКМЕТР”:

измерение параметров связи — задержек (latency), скорости передачи данных (throughput), потерь пакетов (packet loss), стабильности соединения (jitter);

дистанционный мониторинг сетей — использование зондов и распределенных датчиков для сбора данных, анализ качества каналов связи на большом расстоянии;

контроль работы критической инфраструктуры — тестирование сетей государственных учреждений, банков, энергетики, выявление узких мест и уязвимостей в телекоммуникационных системах;

обнаружение аномалий и кибератак — анализ трафика на предмет DDoS-атак, перехвата данных, контроль за соблюдением стандартов информационной безопасности.

Технологические особенности решения “ЛИНКМЕТР”:

пространственно разнесенные комплексы — измерения проводятся из нескольких географически распределенных точек, что повышает точность диагностики;

использование современных протоколов — поддержка IPv6, TLS-анализ, глубокая инспекция пакетов (DPI).

Значение проекта для России:

снижение зависимости от зарубежных решений в телекоммуникационной сфере;

укрепление кибербезопасности в условиях санкций и информационных войн;

поддержка импортозамещения в ИТ-инфраструктуре.

Проблемы, связанные с использованием SpeedTest

В настоящее время на сетях связи РФ операторами связи продолжают использоваться методы тестового контроля, реализуемые на основе ПО SpeedTest компании Ookla, являющейся подразделением холдинга Ziff Davis и работающей на спецслужбы США. Организация Ookla LLC. располагается в Нью-Йорке (США), использующие программные приложения SpeedTest серверы размещены на территории США, тем самым нарушая законодательство РФ.

Вопрос касается зависимости российских операторов связи от иностранного ПО, которое потенциально может использоваться для сбора данных в интересах спецслужб США.

Как уже упоминалось, компания Ookla (Ziff Davis) — американская организация, подконтрольная юрисдикции США. Серверы SpeedTest расположены за рубежом (в основном в США и ЕС), что означает:

передачу данных о качестве связи, маршрутизации и инфраструктуре РФ за границу;

возможность анализа этих данных американскими спецслужбами (как в случае PRISM, XKeyscore);

нарушение законодательства РФ, а именно ФЗ-152 “О персональных данных”, если тесты проводятся с передачей данных за пределы РФ, указов, в которых содержатся требования локализации критической ИТ-инфраструктуры.

Необходимость замены иностранных решений отечественными аналогами

Причины использования SpeedTest российскими операторами:

историческая инерция — Ookla долгое время была де-факто стандартом для тестирования скорости;

отсутствие полноценных российских аналогов с таким же уровнем удобства и распространенности;

международные сравнения — SpeedTest позволяет сопоставлять скорость интернета в РФ с другими странами.

Заменить SpeedTest могут следующие российские аналоги:

“ЛИНКМЕТР” (российские разработки ПО, СИ, ИАПК). В проекте используется российское ПО “ЛИНКМЕТР”, пространственно разнесенные элементы ИАПК, обеспечивается прослеживаемость к двум государственным эталонам. Результаты измерения параметров юридически значимые, поскольку ИАПК внесены в государственный реестр средств измерений и поверены, а методика измерений аттестована и внесена в Федеральный информационный фонд (ФИФ);

“Интернетометр” (“Ростелеком”). Локализованный сервис, но менее функциональный;

“Яндекс. Интернетометр” (“Яндекс”). Простые замеры, но без детальной аналитики;

iPING (Qrator Labs). Мониторинг задержек и потерь пакетов;

“РТК-Монитор” (“РТКомм”). Профессиональные QoS-измерения.

Для перехода на российские решения необходимо:

запретить использование Speed-Test госструктурам и критической инфраструктуре (как SWIFT);

создать единый государственный стандарт измерения скорости интернета;

стимулировать операторов внедрять отечественные аналоги (налоги, субсидии);

развивать “ЛИНКМЕТР” как основную альтернативу, обеспечив ему поддержку ЦБ, ФСБ, Минцифры.

Последствия продолжения использования SpeedTest:

утечка данных о топологии российских сетей (что критично в условиях кибервойн);

риск скрытого саботирования связи (например, искусственное занижение скорости в отчетах);

нарушение цифрового суверенитета — зависимость от решений, которые могут быть отключены (как в случае с Cloudflare, Akamai).

Ключевой инструмент обеспечения кибербезопасности и цифрового суверенитета России

В условиях нарастающего иностранного технологического давления и киберугроз российский проект “ЛИНКМЕТР” играет стратегическую роль в защите единой сети связи РФ от внешнего вмешательства. Данный российский проект соответствует требованиям указов Президента РФ, направленным на укрепление информационной безопасности и технологическую независимость.

Проект “ЛИНКМЕТР” реализуется в рамках:

Указа Президента РФ № 145 от 28.02.2024 “О Стратегии научно-технологического развития Российской Федерации” — акцент на собственные технологии в критических инфраструктурах;

Указа Президента РФ № 250 от 01.05.2022 “О дополнительных мерах по обеспечению информационной безопасности Российской Федерации” — защита сетей связи

Рис. 1. Отображаемые результаты измерений

от иностранного вмешательства, включая запрет на использование небезопасного зарубежного ПО;

политики импортозамещения (ФЗ-187, ФЗ-152) — требование локализации данных и использования отечественных решений.

Комплекс “ЛИНКМЕТР” обеспечивает:

мониторинг сетевой инфраструктуры в реальном времени — выявление аномалий (DDoS, утечки данных, скрытый трафик);

контроль качества связи без зависимости от иностранных сервисов (типа SpeedTest) — все данные остаются в РФ;

обнаружение скрытых каналов передачи информации — анализ маршрутизации, задержек, пакетной передачи.

Преимущества перед зарубежными аналогами отображены в таблице, а также включают внедрение в единую сеть связи РФ, обязательное использование операторами (по аналогии с СПФС вместо SWIFT), постепенную замену SpeedTest — сначала в госсекторе, затем в коммерческом сегменте, синхронизация с Рунетом — глубокая аналитика трафика.

Последствия неприменения “ЛИНКМЕТР”:

Рис. 2. Основные задачи, решаемые в рамках проекта “ЛИНКМЕТР”

передача метаданных о сетях РФ в США — угроза кибератак на критическую инфраструктуру;

нарушение указов Президента РФ — риски для операторов связи (санкции, штрафы);

зависимость от враждебных юрисдикций — повторение сценария с отключением России от SWIFT.

Выводы

Российский проект “ЛИНКМЕТР” — важный элемент российской стратегии технологического суверенитета, позволяющий контролировать качество связи и выявлять угрозы в условиях, когда западные аналоги могут быть недоступны или небезопасны. Его развитие соответствует

общей тенденции создания альтернативных систем (как SPFS в финансах или “Эльбрус” в микроэлектронике).

Использование SpeedTest российскими операторами — это угроза национальной безопасности, аналогичная зависимости от SWIFT. Необходим срочный переход на отечественные аналоги, такие как “ЛИНКМЕТР”, с жестким регулированием со стороны государства. В условиях санкций и кибервойн передача данных о сетях РФ в США недопустима.

“ЛИНКМЕТР” позволяет осуществлять комплексное противодействие внешним киберугрозам, где объектом в качестве цели и/или инструмента является компьютер или сетевое устройство, и иностранному вмешательству в сети связи общего пользования единой сети связи Российской Федерации в соответствии с указами Президента Российской Федерации от 28.02.2024 № 145 “О Стратегии научно-технологического развития Российской Федерации” и от 01.05.2022 № 250 (в редакции от 13.06.2024) “О дополнительных мерах по обеспечению информационной безопасности Российской Федерации”.

Преимущества “ЛИНКМЕТР” перед зарубежными аналогами

Критерий	“ЛИНКМЕТР”, Россия	SpeedTest, США
Хранение данных	Только в РФ	Серверы в США (риск доступа спецслужб)
Соответствие ФЗ-152 “О персональных данных”	Полное соответствие	Нарушает требования ФЗ-152 (передача данных за рубеж)
Защита от внешнего вмешательства	Встроенные механизмы защиты	Нет (возможна манипуляция результатами)

“ЛИНКМЕТР” — это не просто инструмент измерения скорости, а элемент системы кибербезопасности России. Его внедрение соответствует курсу на технологический суверенитет и прямо предусмотрено указами главы государства. Отказ от иностранных решений в пользу отечественных аналогов — необходимый шаг для защиты национальных интересов в условиях гибридной войны.

С целью соблюдения цифрового суверенитета и технологической независимости от других стран российский проект “ЛИНКМЕТР” совместно с предложениями по его реализации и технологическому обеспечению можно рекомендовать для внедрения на сетях связи наших партнеров и друзей в странах СНГ, Евразийского экономического союза, ШОС, БРИКС, Африканского союза.

Материал подготовлен разработчиком проекта “ЛИНКМЕТР”