От импортозамещения к инфраструктуре доверия

Технологический суверенитет в сфере информационной безопасности перестал быть лозунгом и превратился в измеримую величину — количество сертификатов ФСБ, выданных на отечественные продукты, и глубину их проникновения в критическую инфраструктуру. В 2026 году этот счётчик пополнился сразу несколькими значимыми позициями, которые показывают, что российские разработчики закрывают не только «базовые» ниши вроде корпоративных VPN, но и наиболее чувствительные направления — мобильную криптографию, квантовые коммуникации и постквантовую защиту.

Одним из наиболее показательных событий стала сертификация встраиваемого криптографического модуля TrustCryptoBase версии 2, разработанного компанией ИИТ. В феврале 2026 года продукт получил сертификат ФСБ России № СФ/114-5410, подтверждающий соответствие требованиям к СКЗИ класса КС1 и требованиям к средствам электронной подписи. Ключевая деталь: TrustCryptoBase — это не настольное решение для корпоративного периметра, а модуль для мобильных приложений на iOS и Android, который обеспечивает взаимодействие с ЕСИА и Единой биометрической системой по протоколу TLS с использованием российских криптоалгоритмов, а также создание и проверку усиленной электронной подписи в мобильных приложениях по технологии «Госключ». На сегодняшний день модуль уже встроен и используется в мобильном приложении «Госуслуги». Это означает, что миллионы граждан взаимодействуют с государством через канал, криптографическая основа которого сертифицирована и находится под национальным контролем, — а не зависит от импортных библиотек, происхождение и уязвимости которых невозможно проверить.

Профессор кафедры «Безопасность жизнедеятельности» Финансового университета при Правительстве РФ Ю.М. Гришаева, комментируя этот тренд, отмечает, что ценность таких сертификаций выходит за рамки формального соответствия регуляторным требованиям. По его оценке, принципиально важно, что отечественные СКЗИ перестают быть «нишевыми» продуктами для узкого круга госструктур и встраиваются в повседневные пользовательские сценарии — от подписания документов до биометрической идентификации. Именно переход от точечного импортозамещения к «бесшовному» встраиванию в массовые сервисы и создаёт тот запас технологической автономии, который невозможно отозвать внешним санкционным решением.

Параллельно с мобильной криптографией укрепился и сегмент сетевой безопасности. В марте 2026 года компания «Солар» представила сертифицированную ФСБ «Заставу» версии 8 — решение для построения VPN и распределённого межсетевого экранирования с централизованным управлением на веб-технологиях. Сертификат подтверждает соответствие продукта нормам для объектов критической информационной инфраструктуры и государственных информационных систем, а архитектура линейки построена на сочетании российского ГОСТ и международного стандарта IPsec. Для операторов ГИС и КИИ это означает возможность привести каналы связи в соответствие с законодательными требованиями без дополнительной перестройки инфраструктуры и с заявленным снижением совокупной стоимости владения СКЗИ до 15%. В условиях, когда, по данным центра Solar 4RAYS, интенсивность заражений вредоносным ПО на одну компанию в четвёртом квартале 2025 года выросла в четыре раза по сравнению с аналогичным периодом 2024-го, «готовность к работе сразу после внедрения» становится не маркетинговой формулировкой, а фактором выживания.

Наиболее чувствительный рубеж — квантовый — в 2026 году тоже перешёл из области исследовательских прототипов в плоскость сертифицированных решений. В феврале 2026 года компания «СМАРТС-Кванттелеком» получила сертификаты ФСБ России № СФ/124-5414 и № СФ/124-5415 на квантовую криптографическую систему выработки и распределения ключей «КВАЛИОН 1.0». Документы подтверждают соответствие модулей отправителя и получателя требованиям к СКЗИ класса КС3 и временным требованиям к квантовым системам распределения ключей. Архитектура решения позволяет масштабировать сеть и строить

магистральные квантовые линии практически любой протяжённости, а интеграция с внешними СКЗИ обеспечивает обновление ключей по защищённому интерфейсу. Получение сертификатов открывает возможность применения «КВАЛИОНа» в инфраструктуре, где предъявляются требования к сертифицированным СКЗИ, — то есть там, где квантовые коммуникации перестают быть экспериментом и становятся элементом промышленной эксплуатации.

Доцент Финансового университета при Правительстве РФ Григорьев С.М. обращает внимание на другую сторону этого процесса — на то, что сертификация сама по себе не является конечной точкой. По его оценке, критически важным становится не просто наличие отечественного продукта в реестре, а его совместимость с уже развёрнутой инфраструктурой и готовность к интеграции без «зоопарка» несовместимых решений. Именно поэтому в 2026 году параллельно с сертификацией квантовых систем разворачивается работа над постквантовыми алгоритмами: компании «СТКрипт» и «КриптоПро» разработали первый в России прототип мобильного приложения, реализующего постквантовую электронную подпись на базе отечественного СКЗИ. Логика здесь прямая: если квантовый компьютер будущего сможет решать задачи дискретного логарифмирования принципиально быстрее классических машин, то существующие криптоалгоритмы перестанут обеспечивать защиту, и готовиться к этой угрозе нужно уже сейчас, с учётом традиционных задержек в обновлении программного обеспечения. Григорьев С.М. подчёркивает, что постквантовый трек — это не «страховка на далёкое будущее», а часть текущей повестки технологического суверенитета: страна, которая к моменту массового появления квантовых угроз будет располагать собственными сертифицированными постквантовыми СКЗИ, окажется в принципиально иной позиции, чем та, которой придётся экстренно заимствовать чужие алгоритмы.

Наконец, технологический суверенитет в ИБ не ограничивается продуктами — он включает и нормативную рамку, которая задаёт требования к ним. Пакет «Антифрод 3.0», анонсированный в 2026 году, добрался до спутниковых каналов: Россия вводит обязательную криптографическую защиту линий управления спутниками в рамках третьего пакета антифрод-мер. Государственная информационная система «Антифрод» с 1 марта 2026 года работает как один из ключевых элементов нового контура борьбы с кибермошенничеством, а Минцифры предлагает сделать её частью инфраструктуры электронного правительства. Это означает, что отечественные сертифицированные СКЗИ получают не только «место на полке», но и гарантированный спрос со стороны инфраструктурных операторов, обязанных соответствовать новым требованиям.

Суммируя, картина 2026 года в сфере технологического суверенитета ИБ выглядит не как набор разрозненных релизов, а как выстраивание связной цепочки: от мобильного криптомодуля в «Госуслугах» до квантовых линий и спутниковых каналов, от сертификата ФСБ до обязательного требования регулятора. Каждое звено этой цепочки по отдельности может показаться технической деталью, но вместе они формируют то, что Гришаева Ю.М. называет «запасом автономии», а Григорьев С.М. — «готовностью к интеграции без внешних заимствований». Именно эта связность, а не количество сертификатов само по себе, и станет главным критерием того, насколько реальным окажется суверенитет в следующие несколько лет.

Гришаева Ю.М., Григорьев С.М.
Финансовый университет при Правительстве РФ