СОВЕРШЕННО СЕКРЕТНО

Экз. № 3 из 7

ФЕДЕРАЛЬНАЯ СЛУЖБА БЕЗОПАСНОСТИ РОССИЙСКОЙ ФЕДЕРАЦИИ

Научно-техническая служба (НТС)
Управление информационных технологий

АНАЛИТИЧЕСКИЙ ДОКЛАД

«Slonana»: автономная блокчейн-платформа на базе Solana Virtual Machine

Оценка технологических угроз, разведывательного потенциала и стратегических последствий для Российской Федерации

Регистрационный номер:	ФСБ/НТС/2026/№ 0458-СС
Степень секретности:	СОВЕРШЕННО СЕКРЕТНО
Дата подготовки:	7 февраля 2026 г.
Исполнитель:	Отдел анализа кибертехнологий, НТС
Утверждающий:	Начальник НТС

Гриф секретности присвоен в соответствии с Приказом ФСБ России № 547 от 14.03.2019 г.

Подготовлено совместно с СВР России
(Служба внешней разведки Российской Федерации)

Москва, 2026

ЛИСТ РАССЫЛКИ

Экз. №	Адресат	Дата получения
1	Директор ФСБ России	
2	Директор СВР России	
3	Секретарь Совета Безопасности Российской Федерации	
4	Министр цифрового развития, связи и массовых коммуникаций	
5	Начальник Генерального штаба ВС РФ (ГРУ)	
6	Председатель Центрального банка Российской Федерации	
7	Архив НТС ФСБ России	

Основание для подготовки: Директива Совета Безопасности РФ от 12 января 2026 г. № СБ-0091/ДСП «О мониторинге зарубежных блокчейн-технологий с потенциалом обхода финансовых санкций».

Источники: Открытые технические публикации (whitepaper проекта «Slonana», репозиторий исходного кода github.com/slonana-labs/slonana.cpp), данные агентурной разведки СВР (дело № Ф-7294), материалы мониторинга блокчейн-транзакций ФИНЦЕРТ Банка России.

Содержание

РЕЗЮМЕ

Настоящий доклад представляет результаты совместного аналитического исследования ФСБ России и СВР России в отношении проекта «Slonana» — блокчейн-платформы первого уровня (Layer 1), реализованной на языке C++20 и совместимой с Solana Virtual Machine (SVM).

Ключевые выводы:

1. **Техническая зрелость.** Проект представляет собой полноценную реализацию валидатора Solana на 87 453 строках кода C++20 (506 файлов). Заявленная производительность — 185 000 транзакций в секунду (TPS) при медианной задержке 142 мкс. Архитектурная цель — 1,2 млн TPS. Консенсус основан на Tower BFT с Proof of History (PoH). Данные показатели, в случае их подтверждения в боевых условиях, превосходят характеристики действующих российских блокчейн-платформ (Мастерчейн, Waves Enterprise).

2. **Автономные ИИ-агенты.** Принципиально новым элементом является нативная поддержка автономных программ через асинхронное BPF-исполнение (таймеры, наблюдатели состояния, кольцевые буферы) и обязательный Model Context Protocol (MCP). Данная архитектура позволяет ИИ-агентам обнаруживать и использовать ранее неизвестные программы без предварительного обучения, что создаёт потенциал для неконтролируемой автономной экономической активности.

3. **Модель распределения.** В отличие от подавляющего большинства блокчейн-проектов, Slonana декларирует отсутствие венчурного финансирования и предварительного распределения токенов ($SLON, общая эмиссия 100 млн): 10% — airdrop существующим держателям мемкоина $slonana, 90% — через вознаграждения валидаторам. Коэффициент Джини, по данным моделирования, снижается с 0,88 до 0,47 за 48 месяцев.

4. **Угрозы и возможности для РФ.** Платформа представляет двойственный интерес: как потенциальный инструмент обхода западных финансовых санкций (при условии анонимности валидаторов), так и как угроза цифровому суверенитету РФ в случае массового перехода российских пользователей на неподконтрольную инфраструктуру.

Рекомендация: Присвоить проекту статус объекта оперативного наблюдения категории «Б» (технологии двойного назначения) с выделением отдельного направления в рамках программы «Цифровой щит».

ПРЕДПОСЫЛКИ

Геополитический контекст

С 2022 года Российская Федерация находится под беспрецедентным санкционным давлением со стороны государств «коллективного Запада». Отключение от SWIFT, заморозка активов Банка России, ограничения на корреспондентские счета — всё это стимулировало поиск альтернативных расчётных механизмов.

Блокчейн-технологии рассматриваются как один из инструментов обеспечения финансового суверенитета. Проект цифрового рубля (ЦБ РФ), платформа «Мастерчейн» (Ассоциация ФинТех) и ряд закрытых разработок ГРУ ГШ направлены на создание независимой финансовой инфраструктуры.

Появление высокопроизводительных открытых блокчейн-платформ с акцентом на автономные ИИ-агенты требует отдельной оценки — как с точки зрения угроз, так и потенциальных возможностей.

Объект анализа

Проект «Slonana» впервые зафиксирован системами мониторинга СВР в декабре 2025 года. Автор — Рин Фензиг (Rin Fhenzig), аффилирован с организацией OpenSVM Research. Страна юрисдикции не установлена. Whitepaper датирован 1 января 2026 г.

Ключевые характеристики:

- Полностью открытый исходный код (C++20, лицензия не уточнена)
- Совместимость с экосистемой Solana (SVM, CRDS gossip, Turbine)
- Токен $SLON, общая эмиссия 100 млн, финальность 12,8 с
- Позиционирование: «инфраструктура для автономных экономик ИИ-агентов»
- Сеть QUIC-транспорт, gossip-протокол CRDS на 8000+ валидаторов

Методология оценки

Анализ проведён на основании:

(a) Изучения whitepaper проекта (публичный документ, 14 разделов, ∼1200 строк LaTeX)

(b) Анализа исходного кода (репозиторий github.com/slonana-labs/slonana.cpp, версия v0.1.495-mainnet, коммит 49e53be)

(c) Данных агентурной разведки СВР (ограниченный доступ)

(d) Сопоставления с референсной реализацией Agave/Solana (17,4 МБ, 2281 исходный файл)

ТЕХНИЧЕСКАЯ ОЦЕНКА

Архитектура системы

Slonana реализует многоуровневую модульную архитектуру:

Уровень	Модуль	Описание
Консенсус	Tower BFT	Византийский консенсус, взвешенный стейком. Финальность при > 2/3 голосов
Упорядочение	Proof of History	SHA-256 хеш-цепочка, тики каждые 200 мкс, 64 тика/слот
Исполнение	SVM Engine	Параллельное исполнение BPF-программ (6 рабочих потоков)
Хранение	Гибридное	RocksDB (горячие аккаунты) + ClickHouse (история транзакций)
Сеть	CRDS/QUIC/Turbine	Gossip-протокол, QUIC-транспорт, erasure-кодирование блоков
Безопасность	Ed25519/AES-GCM	libsodium (подписи), OpenSSL (шифрование, HKDF, PBKDF2)

Оценка производительности

Заявленные показатели производительности:

Метрика	Измерено (тестнет)	Архитектурная цель
Пропускная способность (TPS)	185 000	1 200 000+
Медианная задержка операции	142 мкс	<150 мкс
Финальность блока	12,8 с	<13,0 с
Доля неуспешных транзакций	0,02%	<0,05%

Оценка НТС: Заявленные 185 000 TPS на тестнете — значение, требующее независимой верификации. Анализ исходного кода (файлы tests/benchmark_*.cpp) показывает, что бенчмарки измеряют пропускную способность в контролируемых условиях без учёта реалистичной сетевой нагрузки. Тем не менее, архитектура lock-free очередей и NUMA-aware структур данных свидетельствует о серьёзном инженерном подходе. Для сравнения:

- Solana (Agave): ∼65 000 TPS (заявлено), ∼4 000 TPS (фактически в mainnet)
- Ethereum 2.0: ∼30 TPS (L1), ∼100 000 TPS (с L2 rollups)
- «Мастерчейн» (РФ): ∼2 000 TPS
- Цифровой рубль (платформа ЦБ): до 100 000 TPS (проектная цель)

Разрыв между заявленной и фактической пропускной способностью — характерная черта всех блокчейн-проектов. Однако даже при 10-кратном снижении реальных показателей (∼18 500 TPS) проект превосходит большинство действующих платформ.

Модель консенсуса

Tower BFT — вариант PBFT (Practical Byzantine Fault Tolerance), усиленный механизмом Proof of History для криптографического упорядочения.

Ключевые свойства:

- **Безопасность:** Гарантируется при доле злонамеренных валидаторов $\alpha < 1/3$ от общего стейка
- **Механизм lockout:** Голосование за блок B в слоте s блокирует валидатора на 2^m последующих слотов, где m — множитель lockout
- **Слэшинг:** Штраф $\Gamma \geq 2 \cdot s_{\text{adversary}}$ за equivocation (двойное голосование)
- **Чекпоинты:** Каждые 512 блоков (≈3 мин) создаётся агрегированная подпись $> 2/3$ стейка

В whitepaper доказана теорема (Theorem 1): при $\alpha < 1/3$ и штрафе слэшинга $\Gamma \geq 2s$ честная стратегия является равновесием Нэша. Стоимость атаки 51% оценивается авторами в \$22,5 млрд при чистом отрицательном ожидаемом результате ($< -$\$22,4 млрд).

Оценка НТС: Формальное доказательство корректно в рамках заданных допущений. Однако модель не учитывает:

(i) Государственных акторов, для которых экономические потери не являются определяющим фактором

(ii) Атаки на уровне сетевой инфраструктуры (BGP hijacking, DNS poisoning)

(iii) Уязвимости реализации (buffer overflow, race conditions в C++ коде)

(iv) Атаки на цепочку поставок (compromise зависимостей: libsodium, OpenSSL, simdjson, RocksDB)

Механизм автономного BPF-исполнения

Наиболее значимая инновация — три механизма автономного исполнения программ:

1. **Таймеры (`sol_timer_create`):** Программа назначает собственный вызов на будущий слот. До 16 таймеров на экземпляр. Заявленная производительность: 14 млн таймеров/с.
2. **Наблюдатели (`sol_watcher_create`):** Программа отслеживает изменения состояния аккаунтов и реагирует автоматически. До 32 наблюдателей на экземпляр. Заявленная производительность: 8 млн наблюдателей/с.
3. **Кольцевые буферы (`sol_ring_buffer`):** Lock-free межпрограммная коммуникация. До 8 буферов по 1 МБ. Заявленная производительность: 25 млн операций/с.

Оценка НТС: Данные механизмы отсутствуют в референсной реализации Solana (Agave) и являются оригинальной разработкой проекта. С точки зрения разведывательных операций, автономное исполнение создаёт возможность для:

- Неотслеживаемых автоматических финансовых операций без участия оператора
- Автономных программ-посредников для конвертации и перемещения активов
- Самовосстанавливающихся каналов передачи средств при обнаружении и блокировке

Model Context Protocol (MCP)

Все программы в сети Slonana обязаны реализовывать интерфейс MCP, включающий:

- `list-tools` — перечень вызываемых функций с JSON Schema
- `list-resources` — перечень доступных ресурсов с типизацией
- `list-prompts` — шаблоны рабочих процессов для агентов

Программы, не прошедшие MCP-валидацию при деплое, не могут исполняться в сети. Это означает, что **любой ИИ-агент может обнаружить и использовать любую программу в сети без предварительного обучения**, включая программы, развёрнутые после создания агента.

Оценка НТС: MCP-архитектура представляет собой фундаментальный сдвиг в модели взаимодействия ИИ с блокчейном. Традиционные методы мониторинга, основанные на отслеживании известных контрактов и адресов, становятся неэффективными, когда агенты динамически обнаруживают и используют новые программы.

ОЦЕНКА УГРОЗ

Угрозы финансовой системе РФ

Обход санкционного режима

Децентрализованная архитектура Slonana с 8 000+ валидаторами, QUIC-транспортом и gossip-протоколом CRDS создаёт инфраструктуру, потенциально пригодную для:

1) **Трансграничных расчётов:** Токен $SLON может использоваться как промежуточный актив для конвертации рубль → $SLON → доллар/евро без прохождения через подконтрольные финансовые институты.

2) **Автоматизированных схем:** Асинхронное BPF-исполнение позволяет создавать полностью автономные программы-миксеры, работающие без оператора. Таймеры и наблюдатели обеспечивают автоматическое дробление и перенаправление средств.

3) **Валидаторских операций:** Развёртывание валидатора Slonana на территории РФ технически возможно (C++20 бинарный файл, минимальные зависимости). При этом идентификация оператора валидатора затруднена.

Оценка уровня угрозы: СРЕДНИЙ. На текущем этапе проект не имеет достаточной ликвидности и пользовательской базы для масштабного обхода санкций. Однако при достижении критической массы валидаторов (>1 000) и интеграции с DeFi-протоколами уровень угрозы возрастает до ВЫСОКОГО.

Конкуренция с цифровым рублём

Проект Slonana позиционируется как альтернатива централизованным цифровым валютам. Его «честный запуск» (fair launch) без контроля центрального эмитента прямо противоречит модели цифрового рубля, где ЦБ РФ является единственным эмитентом и регулятором.

Риск массового перехода российских пользователей на Slonana оценивается как НИЗКИЙ в краткосрочной перспективе (1–2 года), но СРЕДНИЙ в среднесрочной (3–5 лет), особенно при:

- Ужесточении ограничений на операции с цифровым рублём
- Росте недоверия к централизованным финансовым институтам
- Развитии экосистемы ИИ-агентов, требующих автономных платёжных систем

Угрозы цифровому суверенитету

Неподконтрольная финансовая инфраструктура

Децентрализация сети Slonana означает отсутствие единой точки контроля. Традиционные методы регулирования (блокировка счетов, отзыв лицензий, запрет на операции) неприменимы к распределённой сети валидаторов.

Автономные ИИ-агенты

Наиболее существенная угроза — появление автономных экономических агентов, действующих без человеческого контроля. Комбинация:

- Автономного BPF-исполнения (программы, исполняющие себя)

- MCP-обнаружения (агенты находят новые программы автоматически)
- Экономических стимулов (арбитраж, ликвидации, потоковые платежи)

создаёт условия для формирования «теневой» экономики ИИ-агентов, действующих вне поля зрения регуляторов.

Согласно whitepaper, агенты Slonana способны:

- Обнаруживать и использовать программы, развёрнутые *после* создания агента
- Объединять вызовы нескольких программ в атомарные транзакции
- Работать без внешней инфраструктуры (серверов, баз данных)
- Самовосстанавливаться после сбоев в пределах детерминированного времени

Оценка уровня угрозы: ВЫСОКИЙ. Автономные агенты на неподконтрольной блокчейн-инфраструктуре представляют качественно новый вызов для систем финансового мониторинга (Росфинмониторинг, ФИНЦЕРТ).

Угрозы информационной безопасности

Криптографические примитивы

Проект использует:

- Ed25519 (libsodium) — цифровые подписи
- SHA-256 (OpenSSL) — хеширование (PoH)
- AES-256-GCM (OpenSSL) — шифрование межузловой коммуникации
- HKDF, PBKDF2 (OpenSSL) — производные ключи

Все криптографические примитивы основаны на западных библиотеках с открытым исходным кодом. Вероятность наличия умышленных закладок оценивается как НИЗКАЯ, однако полностью не исключается (прецедент: Dual EC DRBG, NSA, 2013).

Поверхность атаки реализации

Реализация на C++20 создаёт типичные для данного языка риски:

- Повреждение памяти (buffer overflow, use-after-free)
- Гонки данных при параллельном исполнении (lock-free алгоритмы)
- Уязвимости в разборе бинарных форматов (снимки Solana, транзакции)
- Зависимость от сторонних библиотек (simdjson, RocksDB, ClickHouse)

Из анализа истории коммитов проекта (коммит a7af06e и предшествующие) следует, что проект *уже испытывал* критические уязвимости:

- SIGSEGV (аварийное завершение) при обращении к ClickHouse — разыменование нулевого указателя
- Висячие ссылки (dangling reference) в модуле арбитражного детектора — повреждение vtable

- NaN-значения, нарушающие strict weak ordering в std::sort — неопределённое поведение

Оценка: Данные уязвимости были исправлены, однако сам факт их наличия указывает на недостаточную зрелость процесса разработки. Эксплуатация подобных уязвимостей в работающем валидаторе может привести к отказу в обслуживании или удалённому исполнению кода.

СТРАТЕГИЧЕСКИЕ ПОСЛЕДСТВИЯ

Экономическая модель и её последствия

Модель «честного запуска» проекта Slonana заслуживает отдельного рассмотрения. Согласно whitepaper:

Сеть	**Джини (запуск)**	**Джини (год 1)**
Ethereum (VC)	0,92	0,90
Solana (VC)	0,88	0,89
Bitcoin (PoW)	0,45	0,52
Slonana (Community-First)	0,89	0,62

Модель демонстрирует, что отсутствие венчурного финансирования приводит к более равномерному распределению токенов (коэффициент Джини 0,47 через 48 месяцев против 0,90 у VC-сетей). Это имеет два следствия:

1. **Устойчивость к захвату.** Отсутствие крупных держателей затрудняет применение рычагов давления через контроль стейка. Государственные акторы (включая РФ) не могут приобрести контрольный пакет без значительного рыночного воздействия.

2. **Децентрализация управления.** Все параметры протокола контролируются голосованием, взвешенным стейком. При коэффициенте Джини 0,47 это приближается к демократической модели, что затрудняет регуляторное воздействие.

Теоретико-игровой анализ с позиции государственного актора

Whitepaper доказывает, что атака 51% требует \$22,5 млрд и имеет отрицательное ожидаемое значение. Однако данный анализ предполагает рационального экономического агента.

Для государственного актора (ФСБ, АНБ, GCHQ) мотивация может быть *неэкономической*:

- Подрыв сети для предотвращения обхода санкций
- Деанонимизация участников для разведывательных целей
- Внедрение модифицированных валидаторов для мониторинга транзакций

Стоимость подобных операций значительно ниже \$22,5 млрд и может быть реализована через:

Атака Сивиллы:	Развёртывание множества валидаторов без реального стейка
Атака на маршрутизацию:	BGP hijacking для изоляции сегментов сети
Атака на зависимости:	Компрометация libsodium/OpenSSL/simdjson

Возможности для разведывательной деятельности

Открытый исходный код и необходимость подключения к сети 8 000+ валидаторов создают возможности:

1. **Пассивный мониторинг.** Развёртывание валидаторов ФСБ/СВР в сети Slonana для наблюдения за транзакциями. CRDS gossip-протокол обеспечивает распространение всех данных между всеми участниками — валидатор-наблюдатель получает полную картину активности сети.

2. **Анализ графа транзакций.** При 185 000 TPS и гибридном хранении (RocksDB + ClickHouse) возможен глубокий анализ связей между аккаунтами, включая кластеризацию и деанонимизацию.

3. **Модифицированный валидатор.** Поскольку исходный код открыт (C++20), возможно создание модифицированной версии валидатора с функциями перехвата и анализа трафика, при этом внешне неотличимого от стандартного.

4. **Эксплуатация MCP.** Интерфейс MCP позволяет создавать «программы-ловушки» — внешне легитимные DeFi-программы, реально осуществляющие сбор данных о вызывающих их агентах.

Сравнение с российскими блокчейн-проектами

Параметр	**Slonana**	**Мастерчейн**	**Цифр. рубль**	**Waves Ent.**
TPS (заявл.)	185 000	2 000	100 000	6 000
Консенсус	Tower BFT	PBFT	Централиз.	LPoS
Автон. агенты	Да (нативно)	Нет	Нет	Нет
ИИ-интеграция	MCP	Нет	Нет	Нет
Код	Открытый	Частичный	Закрытый	Открытый
Контроль РФ	Нет	Да	Да	Частичный
Язык	C++20	Java/Kotlin	—	Scala

Технологический разрыв значителен. Ни один из российских проектов не реализует автономное BPF-исполнение и MCP-интерфейс для ИИ-агентов.

РЕКОМЕНДАЦИИ

На основании проведённого анализа Научно-техническая служба ФСБ России совместно с СВР России рекомендует:

Оперативные меры (немедленно)

Р-1. Присвоить проекту статус объекта оперативного наблюдения категории «Б» (технологии двойного назначения) в рамках программы «Цифровой щит».

Р-2. Развернуть валидаторы-наблюдатели в сети Slonana (не менее 5 узлов в различных юрисдикциях) для пассивного мониторинга сетевого трафика и транзакций. Координация — отдел «К» ФСБ России совместно с ФИНЦЕРТ Банка России.

Р-3. Включить адреса токена $SLON в перечень объектов финансового мониторинга Росфинмониторинга. Обязать российские криптовалютные биржи (при наличии) сообщать о конвертациях $SLON.

Р-4. Провести аудит исходного кода силами специализированного подразделения НТС на предмет выявления уязвимостей, пригодных для оперативной эксплуатации.

Технологические меры (3–6 месяцев)

Р-5. Оценить применимость технологий Slonana для нужд российских блокчейн-проектов. Механизмы автономного BPF-исполнения и MCP-интерфейс представляют технический интерес для платформы цифрового рубля (в части автоматизации операций) и перспективных разработок Министерства обороны.

Р-6. Разработать инструментарий деанонимизации участников сети Slonana на основе анализа:

- Графа транзакций (кластеризация аккаунтов)
- Сетевых метаданных (IP-адреса валидаторов через CRDS gossip)
- Временны́х корреляций (timing analysis транзакций)

Р-7. Подготовить модифицированный клиент-валидатор на базе открытого исходного кода Slonana с интегрированными функциями разведывательного мониторинга для использования в оперативных целях.

Стратегические меры (6–18 месяцев)

Р-8. Подготовить доклад Совету Безопасности РФ о необходимости ускорения разработки отечественной платформы для автономных экономик ИИ-агентов, не уступающей по техническим характеристикам проекту Slonana.

Р-9. Инициировать внесение изменений в Федеральный закон «О цифровых финансовых активах» (259-ФЗ) в части регулирования автономных ИИ-агентов, осуществляющих финансовые операции без участия оператора-физического лица.

Р-10. Рассмотреть возможность включения протокола Slonana в перечень технологий, подлежащих ограничению на территории РФ (в соответствии с Приказом Роскомнадзора), — в случае обнаружения фактов использования сети для обхода российского законодательства.

Р-11. Координировать с партнёрами по ШОС и БРИКС выработку общей позиции в отношении децентрализованных блокчейн-платформ с автономными ИИ-агентами, включая вопросы совместного мониторинга и обмена разведывательными данными.

ЗАКЛЮЧЕНИЕ

Проект «Slonana» представляет собой технологически продвинутую блокчейн-платформу с уникальными характеристиками в области автономного исполнения программ и интеграции с ИИ-агентами. Ни один из существующих блокчейн-проектов — ни западных, ни российских — не реализует аналогичный набор функций.

Основные параметры проекта:

- 87 453 строки C++20, 506 файлов исходного кода
- Производительность: 185 000 TPS (тестнет), цель — 1 2 млн TPS
- Tower BFT + Proof of History, финальность 12,8 с
- Токен $SLON: 100 млн эмиссия, «честный запуск», Джини 0,88 → 0,47
- Нативные механизмы автономного BPF-исполнения и MCP
- Сеть: QUIC-транспорт, CRDS gossip, 8 000+ валидаторов

С позиции обеспечения безопасности Российской Федерации проект требует **активного наблюдения и выборочной эксплуатации**: мониторинг транзакций через собственные валидаторы, анализ уязвимостей для оперативных нужд, заимствование технических решений для отечественных проектов.

Полное блокирование доступа к сети Slonana с территории РФ оценивается как **технически нецелесообразное** ввиду P2P-характера сети, использования QUIC-транспорта и отсутствия централизованных точек управления.

Начальник НТС ФСБ России
генерал-лейтенант

_____
(подпись)

«_____» февраля 2026 г.

Заместитель директора СВР России
генерал-майор

_____
(подпись)

«_____» февраля 2026 г.

СОВЕРШЕННО СЕКРЕТНО
Экз. № 3 из 7
ФСБ/НТС/2026/№ 0458-СС