УДК 004.056.5:621.395.721.5

АППАРАТНО-ПРОГРАММНЫЙ КОМПЛЕКС SIMVAULT ДЛЯ БЕЗОПАСНОГО ХРАНЕНИЯ И УПРАВЛЕНИЯ ПРОФИЛЯМИ ESIM: РЕШЕНИЕ ПРОБЛЕМЫ УЯЗВИМОСТИ ЦИФРОВОЙ ИДЕНТИФИКАЦИИ

Андриянов А.А., Архипов И.С., Соколова А.С., Черненко Д.В.

Витебский государственный технологический университет, г. Витебск. Республика Беларусь (E-mail: Chernenko203509@gmail.com)

eSIM (embedded SIM – «встроенная SIM») – это цифровая программируемая SIM-карта, которая впаяна непосредственно в устройство (смартфон, планшет или умные часы) при производстве [1]. В отличие от привычной пластиковой SIM-карты, её нельзя вынуть или потрогать. Если раньше SIM-карту покупали у оператора, вставляли её в слот и пользовались связью, то с eSIM всё происходит полностью удалённо. Сканируется QR-код или скачиваются настройки оператора через приложение – и номер сразу появляется на телефоне. Физический пластик не нужен.

На материнской плате устройства распаян специальный чип eUICC. Он умеет хранить в себе несколько профилей разных операторов. Пользователь может переключаться между ними программно, без похода в салон связи.

Достоинства таких SIM – не нужен слот, можно хранить несколько номеров, удобно для путешествий, безопаснее для устройств. Но есть и недостатки. Сложно перенести в другой телефон, существует риск взлома, а также необходимость привязка к устройству [2].

Таким образом технология eSIM представляет собой программно-аппаратный модуль, впаянный в устройство, который выполняет функции традиционной SIM-карты. Несмотря на очевидные преимущества, массовое внедрение eSIM выявило ряд критических уязвимостей с точки зрения информационной безопасности [3] и удобства пользователя:

1. Уязвимость к SIM-свопингу. Перевыпуск eSIM злоумышленниками через оператора связи становится менее защищенным процессом по сравнению с физическим носителем.

2. Проблема одноразовых QR-кодов. Первичная активация eSIM требует сканирования QR-кода, который легко потерять или повредить, а его повторное получение не всегда возможно без обращения к оператору.

3. Офлайн-паралич. Восстановление или перенос номера на новое устройство требует обязательного доступа в интернет (облачный бэкап), что делает пользователя беспомощным при отсутствии сети.

4. Привязка к устройству и экосистеме. Существующие механизмы переноса (например, Apple-Android) ограничены и часто не работают между разными операционными системами без участия оператора.

Таким образом, актуальной научно-технической задачей является разработка метода и устройства, обеспечивающего физическую изоляцию eSIM-профилей от сети и их безопасный перенос между любыми устройствами.

В ответ на выявленные проблемы предлагается создание экосистемы SimVault, включающей аппаратный крипто-ключ и мобильное приложение-ассистент.

Ключевым элементом является чип Secure Element с уровнем защиты EAL6+, который используется для хранения криптографических ключей в банковских приложениях и платежных системах.

Secure Element – это специализированный микрочип, который можно представить, как «сейф в миниатюре». Он спроектирован так, чтобы хранить самые секретные данные

(криптографические ключи, пароли, биометрию) и выполнять криптографические операции в абсолютно изолированной и защищенной среде. [4]

Даже если злоумышленник получит полный физический доступ к устройству (например, украдет телефон), взломать Secure Element и извлечь из него данные чрезвычайно сложно и дорого.

Основные характеристики Secure Element являются:

1. Аппаратная изоляция: это отдельный чип со своим процессором, памятью (RAM, ROM) и криптоускорителем. Он не зависит от основной операционной системы мобильного устройства.

2. Защита от взлома: чип устойчив к физическим атакам (например, попыткам просканировать его электронным микроскопом, пережечь дорожки, заморозить). При попытке физического вскрытия данные мгновенно уничтожаются.

3. Безопасное исполнение кода: внутри чипа работает маленькая ОС (например, Java Card), которая может запускать только сертифицированные программы.

Совместно с Secure Element примеяется EAL6+ – один из самых высоких уровней применяемой в военной и космической промышленности, а также в системах особо важной критической инфраструктуры. Таким образом EAL6 – полуформальное проектирование и проверка устойчивости к высоким атакам. Это значит, что производитель не просто заявил, что чип защищен, а математически доказал архитектуру и проверил, что чип выдержит сложные методы взлома (анализ побочных каналов, манипуляции с напряжением и т.д.). EAL6+ применяется в платежных чипах банковских карт (Visa/MasterCard), чипах в заграничных паспортах нового поколения, а также аппаратно реализованных кошельках для криптовалют высокого уровня.

В разработанном проекте SimVault Secure Element с уровнем защиты EAL6+ используется для хранения токенов eSIM, чтобы злоумышленник не мог украсть номер, даже украв сам брелок.

Протокол работы системы SimVault включает три этапа:

1. Захват профиля. На исходном устройстве пользователь сканирует операторский QR-код или вводит активационный ключ. Приложение перехватывает токен SM-DP+ (Subscription Manager Data Preparation – сервер подготовки данных).

2. Шифрование и запись. Полученный токен шифруется ключом, привязанным к биометрии владельца (для исключения доступа при утере физического носителя). Зашифрованные данные передаются на аппаратный носитель SimVault (в форм-факторе стикера, брелока или карты) по защищенному NFC-каналу. Емкость носителя позволяет хранить до 15 профилей.

3. Активация. Для переноса номера владелец прикладывает метку SimVault к любому NFC-совместимому устройству (iOS/Android). Приложение-ассистент расшифровывает токен с использованием биометрического ключа и передает его в системный eUICC-чип целевого смартфона.

Ключевым научно-техническим преимуществом является то, что процесс не требует наличия физического SIM-слота на устройстве и работает с любыми современными смартфонами, поддерживающими eSIM.

Сравнение предлагаемого решения с существующими подходами демонстрирует его научно-техническую и потребительскую ценность:

1. Физические SIM-карты: Занимают слот, требуют механического извлечения (скрепка), одна карта = один номер, подвержены физической утере или порче.

2. Облачный бэкап оператора (Apple/Google Transfer): Требует подключения к интернету, уязвим для атак на облачную инфраструктуру, функционально ограничен рамками одной экосистемы (iOS → iOS, Android → Android).

3. Адаптеры типа eSIM.me: Являются ближайшим аналогом, но имеют принципиальное ограничение – они требуют наличия физического слота для SIM-карты. Это делает их бесполезными для устройств без слота (например, iPhone для рынка США).

4. SimVault (предлагаемое решение): Не требует SIM-слота, обеспечивает кроссплатформенный перенос (iOS ↔ Android), гарантирует аппаратную защиту от кражи номера и функционирует полностью офлайн. [5]

Для оценки экономической перспективности проекта SimVault требуется анализ рыночных трендов, себестоимости, модели монетизации и конкурентной среды.

Проект имеет высокий экономический потенциал при условии успешного решения технических задач и выхода на B2B-сегмент. Ниша криптозащищенных физических носителей для eSIM практически пуста, а тренд на отказ от физических SIM-слотов создает растущий спрос.

Себестоимость всех затрат, которые необходимо потратить на производство одного физического устройства учитывая заявленные $3–5 за чип при партии от 1000 шт. – это реалистичная цифра для оптовых закупок компонентов среднего ценового сегмента. Розничная цена – $25-35.

Таким образом валовая прибыль с единицы составит $20-30 (400-600%). Такой уровень прибыли позволяет закладывать в бюджет высокие расходы на маркетинг.

Уход производителей от физических SIM-слотов (первыми были американские iPhone, следом – Европа) создает дефицит физического контроля у пользователя. Существующие облачные решения от Apple и Google бесплатны, но привязаны к экосистеме и требуют интернета. SimVault играет на страхе остаться без связи в роуминге или при взломе аккаунта. Просто распечатанный QR-код в бумажнике мнется и теряется, и это небезопасно. SimVault оцифровывает этот носитель с высоким уровнем защиты.

Можно сделать вывод что представленный проект экономически состоятелен. Ключевым фактором успеха является скорость выхода на рынок, пока массовый пользователь не привык к неудобствам eSIM, и заключение B2B-партнерств с операторами связи, которые обеспечат масштабирование. Инвестиции на этапе исследования и разработки и сертификации (заявленный Q3-Q4 2026) окупятся за счет высокой маржинальности первой B2C-партии. Себестоимость аппаратной части (NFC + Secure Element) при оптовой партии составляет $3-5 при розничной цене $25-35.

Стратегия развития подразумевает выход на B2B-рынок и лицензирование технологии:

1. Корпоративный сектор. Интеграция с системами управления мобильными устройствами. Выдача корпоративных карт SimVault сотрудникам позволяет IT-отделу централизованно управлять корпоративной связью и удалённо стирать профили при увольнении.

2. Лицензирование технологии. Встраивание NFC-чипа SimVault в продукты партнеров: аппаратные криптокошельки, премиальные чехлы, тревел-аксессуары.

3. White-label для операторов. Продажа решения мобильным операторам под их брендом для предложения VIP-клиентам как премиум-аксессуара безопасности.

Заключение: Предлагаемый проект SimVault направлен на решение актуальной научно-технической проблемы – обеспечения суверенитета пользователя над его цифровым идентификатором (номером телефона) в эпоху тотальной виртуализации SIM-карт. Применение аппаратных криптографических модулей и протокола передачи данных через изолированный NFC-канал позволяет создать принципиально новый класс устройств, сочетающий удобство eSIM и безопасность физического носителя. Разработка находится на стадии исследования и разработки (Q3-Q4 2026) с планами запуска краудфандинговой кампании и пилотных B2B-проектов в 2027 году.

СПИСОК ИСПОЛЬЗОВАННОЙ ЛИТЕРАТУРЫ

1. European Union Agency for Cybersecurity (ENISA). Embedded SIM Ecosystem, Security Risks and Measures [Электронный ресурс] : Report. – March 2023. – Режим доступа: https://www.enisa.europa.eu/ (дата обращения: 19.03.2026).
2. GSMA. Remote SIM Provisioning (RSP) Technical Specification [Электронный ресурс] : Standard SGP.22 v2.4. – GSM Association, 2023. – Режим доступа: https://www.gsma.com/esim/ (дата обращения: 19.03.2026).
3. Motallebighomi, M. eSIMplicity or eSIMplification? Privacy and Security Risks in the eSIM Ecosystem / M. Motallebighomi, J. Veara, E. Bitsikas, A. Ranganathan // Proceedings of the 34th USENIX Security Symposium. – Seattle, 2025.
4. Urien, P. On Line Secure Elements: Deploying High Security Keystores and Personal HSMs / P. Urien // 2023 7th Cyber Security in Networking Conference (CSNet). – IEEE, 2023. – P. 23-26.
5. Kim, M. A Study of the Emerging Trends in SIM Swapping Crime and Effective Countermeasures / M. Kim, J. Suh, H. Kwon // 2022 IEEE/ACIS 7th International Conference on Big Data, Cloud Computing, and Data Science (BCD). – IEEE, 2022. – P. 240-245.