УДК 004.056.5 https://doi.org/10.33619/2414-2948/120/12

ДОВЕРЕННЫЕ ПРОГРАММНО-АППАРАТНЫЕ КОМПЛЕКСЫ

©Турянская К. А.*, SPIN-код: 4864-3898, Петербургский государственный университет путей сообщения Императора Александра I, г. Санкт-Петербург, Россия, kristina.turianskaia@gmail.com*

TRUSTED HARDWARE AND SOFTWARE SYSTEMS

©Turianskaya K., *SPIN-код: 4864-3898, Petersburg State Transport University of Emperor Alexander I, St. Petersburg, Russia, kristina.turianskaia@gmail.com*

Аннотация. Анализируются предпосылки и особенности внедрения доверенных программно-аппаратных комплексов (ДПАК) в Российской Федерации в контексте обеспечения информационной безопасности критической инфраструктуры. Рассматриваются нормативно-правовые основы регулирования применения ДПАК, в том числе Постановление Правительства РФ № 1912 от 14 ноября 2023 года. Уточняются требования к отечественным решениям, включающим использование российской радиоэлектронной продукции, сертифицированного программного обеспечения и компонентов информационной безопасности. Представлена классификация ДПАК на общесистемные и функциональные, обозначены ключевые направления их развития, а также проблемы сертификации и стандартизации. Отдельное внимание уделяется анализу рынка доверенных ПАК, динамике его роста и перспективам консолидации производителей. Делается вывод о необходимости комплексного государственного регулирования, расширения нормативной базы и подготовки квалифицированных специалистов для успешного завершения перехода к использованию отечественных решений к 2030 году.

Abstract. Analyzes the prerequisites and specific features of implementing trusted hardware and software systems (THSS) in the Russian Federation in the context of ensuring the security of critical information infrastructure. The study examines the regulatory framework governing the use of THSS, including the Resolution of the Government of the Russian Federation No. 1912 of November 14, 2023. The requirements for domestic solutions are clarified, such as the use of Russian-made electronic components, certified software, and information security modules. The classification of THSS into general-purpose and functional types is presented, along with key directions of their development, as well as current challenges of certification and standardization. Special attention is given to the analysis of the THSS market, its growth dynamics, and prospects for industry consolidation. The article concludes that comprehensive state regulation, expansion of the legal framework, and the training of qualified specialists are essential for the successful transition to domestic solutions by 2030.

Ключевые слова: доверенные программно-аппаратные комплексы; критическая информационная инфраструктура; информационная безопасность; нормативно-правовое регулирование; импортозамещение; отечественная радиоэлектронная продукция; сертификация; стандартизация; рынок программно-аппаратных комплексов.

Т. 11. №11 2025
https://doi.org/10.33619/2414-2948/120

Keywords: trusted hardware and software systems; critical information infrastructure; information security; regulatory framework; import substitution; domestic electronics; certification; standardization; hardware and software systems market.

В экономике России в последнее десятилетие можем наблюдать стремительный рост технологий и, в том числе, — увеличение количества радиоэлектронных средств, используемых в самых разных сферах: от тяжелой промышленности до повседневной жизни. При этом с расширением применения радиоэлектронных систем возникают новые вызовы, особенно в области информационной безопасности, которая испытывает некоторые проблемы. Разработка доверенных программно-аппаратных комплексов (ДПАК) отечественного производства — пример одного из самых срочных вызовов для ИТ-рынка в данный момент. Изучение вопроса начнем с Постановления Правительства Российской Федерации от 14 ноября 2023 г №1912 «О порядке перехода субъектов критической информационной инфраструктуры Российской Федерации на преимущественное использование доверенных программно-аппаратных комплексов на значимых объектах критической информационной инфраструктуры».

В документе установлено, что: 1. переход субъектов критической информационной инфраструктуры Российской Федерации на преимущественное применение доверенных программно-аппаратных комплексов на принадлежащих им значимых объектах критической информационной инфраструктуры Российской Федерации осуществляется до 1 января 2030 г. в соответствии с Правилами, утвержденными настоящим постановлением; 2. с 1 сентября 2024 г. не допускается использование субъектами критической информационной инфраструктуры Российской Федерации на принадлежащих им значимых объектах критической информационной инфраструктуры Российской Федерации программно-аппаратных комплексов, приобретенных субъектами критической информационной инфраструктуры Российской Федерации с 1 сентября 2024 г. и не являющихся доверенными программно-аппаратными комплексами [1].

Использование данных комплексов, приобретенных после указанной в Постановлении даты (1 сентября 2024 г.), для всех остальных субъектов становится под запретом. Рассмотрим, что представляют собой доверенные программно-аппаратные комплексы. Понятие «доверенный ПАК» (ДПАК) включает в себя комплексы или системы, которые состоят из отечественной радиоэлектронной продукции с требуемым уровнем локализации российских комплектующих и программного обеспечения. Кроме того, доверенные ПАК должны соответствовать следующим требованиям (согласно Постановлению, указанному выше) [1]: обязательно их присутствие в реестре Минпромторга; программное обеспечение внутри программно-аппаратного комплекса должно быть российским; компоненты, отвечающие за информационную безопасность, должны быть сертифицированы ФСТЭК.

При этом сам факт включения ПАКа в реестр Минцифры не делает его автоматически отечественным с точки зрения законодательства о закупках. Программно-аппаратный комплекс должен в целом соответствовать критериям доверенности, таким как технологическая независимость, длительный жизненный цикл и функциональная насыщенность. Дополнительно существуют рекомендации АО «НПО КИС», разработанные в конце 2023 года, но их выполнение пока носит добровольный характер.

По словам Валерия Андреева, заместителя генерального директора по развитию АО «ИВК» ключевыми отличиями ПАКов для критической информационной инфраструктуры от обычных автоматизированных рабочих мест являются технологическая независимость и

Т. 11. №11 2025
https://doi.org/10.33619/2414-2948/120

длительный жизненный цикл. В данном контексте важно не просто присутствие ПАКа в реестре Минпромторга или Минцифры, а его реальная технологическая автономность как в программной, так и в аппаратной частях. Также эксперт отмечает, что большую роль играет срок эксплуатации, который в случае доверенных ПАКов, может составлять 15 и даже 25 лет (https://goo.su/SWWBNaR).

Выделяют два класса доверенных ПАК (в соответствии с классификацией Федерального агентства по техническому регулированию и метрологии) [3]:

общесистемные — когда функционально-технические характеристики ДПАК не зависят от целевого объекта (например, это комплексы для передачи, хранения и управления данными, обеспечения информационной безопасности, для задач машинного обучения и инженерного проектирования).

функциональные — соответственно, функционально-технические характеристики связаны с целевым объектом (включают такие типы, как доверительные ПАКи для мониторинга, диагностики и защиты).

В соответствии с Федеральным законом от 26.07.2017 №187-ФЗ (ред. от 10.07.2023) «О безопасности критической информационной инфраструктуры Российской Федерации» [3] критическая информационная инфраструктура — это объекты критической информационной инфраструктуры (информационные системы, информационно-телекоммуникационные сети и автоматизированные системы управления субъектов КИИ), а также сети электросвязи, используемые для организации взаимодействия таких объектов. Из этого следует, что объекты КИИ напрямую влияют на организацию работы в критически важных областях. В соответствии с этим, развитие доверенных ПАКов идет в нескольких направлениях — инфраструктурные, сетевые, специализированные сегменты и сектор информационной безопасности.

Лидером по востребованности и количеству доверенных ПАКов является сегмент информационной безопасности. Второе место у инфраструктурного сегмента (решения для виртуализации, хранения данных и СУБД), поскольку в КИИ он занимает порядка 80%.

На рынке программно-аппаратных комплексов присутствуют не только крупные корпорации, предоставляющие комплексные решения, но и небольшие стартапы, которые могут закрыть потребности в узких областях. Мы считаем, такое разнообразие игроков существенно важным, так как это позволяет проводить работу оперативнее, ориентируясь на более точечные запросы рынка.

Критически важно, чтобы ПАКи обеспечивали виртуализацию, управление и мониторинг, а также соответствовали требованиям безопасности. Согласны с мнением, что жизнеспособными останутся только те производители, которые предоставляют высокий уровень клиентского сервиса и проверяют совместимость с программным обеспечением.

В настоящее время производителям приходится сталкиваться с проблемой сертификации и отсутствием контролирующего органа для доверенных ПАКов. В связи с этим необходимо расширять нормативную базу и подходить к вопросам регулирования комплексно. На данный момент комитет 167 проработал основные термины, определения и классификацию ПАКов, а также разработал соответствие между национальными стандартами и классификатором Минцифры (https://goo.su/SWWBNaR).

При этом констатируем факт, что рынок доверенных программно-аппаратных комплексов пока небольшой и только набирает обороты. Но эксперты отмечают, что в период ближайших 3-5 лет объем рынка может вырасти кратно [4].

Динамика регистрации за последние два года значительно ускорилась. Особенно в ключевых реестрах Минцифры РФ и Минпромторга РФ. Безусловно, ключевую роль здесь

Т. 11. №11 2025
https://doi.org/10.33619/2414-2948/120

играет необходимость обновления инфраструктуры у заказчиков. Также рынок активно ориентируется на перечень приоритетных решений от Минцифры РФ. Если в 2023 г максимальный рост наблюдался в сегменте обработки больших данных, то в 2024 г на первый план вышли решения для маршрутизации и коммутации. Кроме того, существенно увеличилось количество комплексов для управления технологическими процессами. Предполагаем, что в районе пяти лет российский рынок ждет череда слияний и поглощений. Это должно привести к консолидации производителей и снижению хаоса в отрасли. Кроме того, встает вопрос о подготовке сертифицированных специалистов для работы с доверенными ПАКами. Отметим, что на данный момент отдельной сертификации для таких специалистов не требуется, однако обучение работе с ПАКами проводится как самими производителями, так и профильными учебными центрами.

Подводя итог, отметим, что программно-аппаратные комплексы, использующиеся в критически важных системах, требуют строгого контроля и соответствия установленным стандартам. Создание Минпромторгом перечня доверенных ПАК — инициатива, направленная на формирование конкретной и прозрачной системы контроля за качеством радиоэлектронной продукции. Это необходимый шаг для повышения уровня доверия со стороны потребителей, а также для защиты стратегических информационных систем от потенциальных угроз и негативных факторов. Поддержка создания доверенных ПАКов со стороны государства позволяет сделать оптимистичный прогноз и рассчитывать на высокие темпы и системный подход. Что является необходимым условием, чтобы завершить переход на отечественные решения к 2030 г.

Список литературы:

1. Постановление Правительства Российской Федерации от 14.11.2023 №1912 «О порядке перехода субъектов критической информационной инфраструктуры Российской Федерации на преимущественное применение доверенных программно-аппаратных комплексов на принадлежащих им значимых объектах критической информационной инфраструктуры Российской Федерации». https://goo.su/wL6ak

2. Федеральное агентство по техническому регулированию и метрологии (Росстандарт). Технический комитет по стандартизации ТК 167 «Программно-аппаратные комплексы для критической информационной инфраструктуры и программное обеспечение для них». Заседание технического комитета ТК 167, 30.05.2024 : протокол (или материалы заседания). https://goo.su/e11hgM

3. Ст. 2. Основные понятия, используемые в настоящем Федеральном законе // Федеральный закон от 26.07.2017 №187-ФЗ (ред. от 07.04.2025) «О безопасности критической информационной инфраструктуры Российской Федерации». https://goo.su/gia6hV0

4. Федорова В. Сети заПАКовали: Переход госструктур, банков и телека на доверенные ПАКи окажется непростым // Коммерсантъ. 20.05.2024. https://goo.su/UHkcBJ

References:

1. Postanovlenie Pravitel'stva Rossiiskoi Federatsii ot 14.11.2023 №1912 «O poryadke perekhoda sub"ektov kriticheskoi informatsionnoi infrastruktury Rossiiskoi Federatsii na preimushchestvennoe primenenie doverennykh programmno-apparatnykh kompleksov na prinadlezhashchikh im znachimykh ob"ektakh kriticheskoi informatsionnoi infrastruktury Rossiiskoi Federatsii». https://goo.su/wL6ak

2. Federal'noe agentstvo po tekhnicheskomu regulirovaniyu i metrologii (Rosstandart). Tekhnicheskii komitet po standartizatsii TK 167 «Programmno-apparatnye kompleksy dlya kriticheskoi informatsionnoi infrastruktury i programmnoe obespechenie dlya nikh». Zasedanie tekhnicheskogo komiteta TK 167, 30.05.2024 : protokol (ili materialy zasedaniya). https://goo.su/e11hgM

3. St. 2. Osnovnye ponyatiya, ispol'zuemye v nastoyashchem Federal'nom zakone // Federal'nyi zakon ot 26.07.2017 №187-FZ (red. ot 07.04.2025) «O bezopasnosti kriticheskoi informatsionnoi infrastruktury Rossiiskoi Federatsii». https://goo.su/gia6hV0

4. Fedorova V. Seti zaPAKovali: Perekhod gosstruktur, bankov i teleka na doverennye PAKi okazhetsya neprostym // Kommersant". 20.05.2024. https://goo.su/UHkcBJ

Поступила в редакцию
01.10.2025 г.

Принята к публикации
09.10.2025 г.

Ссылка для цитирования:

Турянская К. А. Доверенные программно-аппаратные комплексы // Бюллетень науки и практики. 2025. Т. 11. №11. С. 100-104. https://doi.org/10.33619/2414-2948/120/12

Cite as (APA):

Turianskaya, K. (2025). Trusted Hardware and Software Systems. *Bulletin of Science and Practice, 11*(11), 100-104. (in Russian). https://doi.org/10.33619/2414-2948/120/12