УДК 321.01; 316.422.44; 004.056

Борис Н. Кривошеин[1], Иван А. Покровский[2]
[1]ООО НПП «Зелакс»
ул. Заводская, 1 Б, стр. 2, офис 1/2, Зеленоград, Москва, 124365, Россия
[2]Ассоциация разработчиков и производителей электроники
ул. Правды, 24, стр. 4, офис 322, Москва, 125124, Россия
[1]e-mail: bnk@bnkserv.com, https://orcid.org/0000-0002-9921-6682
[2]e-mail: pokrov@arpe.ru, https://orcid.org/0009-0001-7819-1607

ПОНЯТИЯ И КРИТЕРИИ ОЦЕНКИ ТЕХНОЛОГИЧЕСКОЙ НЕЗАВИСИМОСТИ И БЕЗОПАСНОСТИ ОБЪЕКТОВ КРИТИЧЕСКОЙ ИНФОРМАЦИОННОЙ ИНФРАСТРУКТУРЫ

DOI: http://dx.doi.org/10.26583/bit.2023.4.02

Аннотация. В статье представлен анализ понятий и терминов, использованных в Указе Президента Российской Федерации от 30.03.2022 № 166 «О мерах по обеспечению технологической независимости и безопасности критической информационной инфраструктуры Российской Федерации». Определены различия в понятиях технологического суверенитета и безопасности объектов инфраструктуры, различия между критериями оценки доверия программно-аппаратных комплексов и критериями российского происхождения. Предложены уточнения нормативной базы, которые позволят исключить разночтения понятий и противоречия в требованиях.

Ключевые слова: критическая информационная инфраструктура, технологический суверенитет, технологическая независимость, информационная безопасность, доверенные информационные системы, критерии российского происхождения, уровень локализации.
Для цитирования: КРИВОШЕИН Борис Н.; ПОКРОВСКИЙ Иван А. ПОНЯТИЯ И КРИТЕРИИ ОЦЕНКИ ТЕХНОЛОГИЧЕСКОЙ НЕЗАВИСИМОСТИ И БЕЗОПАСНОСТИ ОБЪЕКТОВ КРИТИЧЕСКОЙ ИНФОРМАЦИОННОЙ ИНФРАСТРУКТУРЫ. Безопасность информационных технологий, [S.l.], т. 30, № 4, с. 39–60, 2023. ISSN 2074-7136. URL: https://bit.spels.ru/index.php/bit/article/view/1561. DOI: http://dx.doi.org/10.26583/bit.2023.4.02.

Boris N. Krivoshein[1], Ivan A. Pokrovsky[2]
[1]LLC NPP «Zelaks»,
Zavodskaya str., 1B, building 2, office 1/2, Zelenograd, Moscow, 124365, Russia
Association of Developers and Manufacturers of Electronics,
24 Pravdy str., building 4, office 322, Moscow, 125124, Russia
[1]e-mail: bnk@bnkserv.com, https://orcid.org/0000-0002-9921-6682
[2]e-mail: pokrov@arpe.ru, https://orcid.org/0009-0001-7819-1607

Concepts and criteria for assessing the technological independence and security of critical information infrastructure facilities

DOI: http://dx.doi.org/10.26583/bit.2023.4.02

Abstract. The article presents an analysis of the concepts and terms used in the Decree of the President of the Russian Federation No. 166 dated 30.03.2022 "On measures to ensure the technological independence and security of the critical information infrastructure of the Russian Federation". Differences in the concepts of technological sovereignty and security of infrastructure facilities are identified, as well as differences between the criteria for assessing the trust of software and hardware complexes and the criteria of Russian origin. Clarifications of the regulatory framework are proposed, which will eliminate discrepancies in concepts and contradictions in requirements.

Keywords: critical information infrastructure, technological sovereignty, technological independence, information security, trusted information systems, criteria of Russian origin, localization level.
For citation: KRIVOSHEIN Boris N.; POKROVSKY Ivan A. Concepts and criteria for assessing the technological independence and security of critical information infrastructure facilities. IT Security (Russia), [S.l.], v. 30, no. 4,

p. 39–60, 2023. ISSN 2074-7136. URL: https://bit.spels.ru/index.php/bit/article/view/1561. DOI: http://dx.doi.org/10.26583/bit.2023.4.02.

Введение

Указ Президента РФ № 166 от 30.03.2022 г. «О мерах по обеспечению технологической независимости и безопасности критической информационной инфраструктуры Российской Федерации» использует ряд терминов, одни из которых чётко определены и стандартизованы в технической области, а другие – такого определения не имеют и требуют дополнительного толкования. Уже в названии мы видим понятия «Технологической независимости КИИ» и «Безопасности КИИ», с которых следует начать.

Термин «технологическая независимость» [1, 2] или «технологический суверенитет» [3, 4] происходит от понятия государственного суверенитета, как способности государства ставить собственные стратегические цели и достигать этих целей как внутри страны, так и в отношениях с другими государствами. Технологический суверенитет является одним из аспектов государственного суверенитета, а именно – способностью ставить и достигать цели в области технологического развития [5].

Определение «Технологическая независимость КИИ» требует пояснений, т.к. КИИ не является субъектом, который может иметь свои цели и задачи. Данное определение раскрывается, как способность государства самостоятельно управлять технологическим составом и процессами в критической информационной инфраструктуре.

Технологическая независимость в данном случае – это характеристика государства, его самостоятельности в принятии решений, управлении информационными системами и технологическими процессами. Уровень технологической независимости определяется наличием соответствующих инженерных и производственных кадров, компетенций и ресурсов, но необходимым условием является наличие собственных целей и стратегии их достижения. Без собственной технологической стратегии уровень независимости обнуляется при любых ресурсах, т.к. все они могут быть подчинены внешнему влиянию и целям других субъектов. Технологическая стратегия нужна для развития информационной инфраструктуры [6], но также она необходима для обеспечения устойчивости при противодействии внешним влияниям, особенно для КИИ. Таким образом это – проекция общих принципов государственного суверенитета в плоскости информационных технологий.

Суверенитет государства проявляется в реализации технологической стратегии через проекты с участием большого числа компаний с различными компетенциями. Для этого необходимы устойчивые связи, взаимопонимание и доверие между коллективами компаний и государством, устойчивые нормы юридических и финансово-экономических взаимоотношений. В рыночной экономике это предполагает наличие отраслевого сообщества, альтернативой является жесткое подчинение государственной иерархии.

Важно отметить, что оценивать технологическую независимость отдельных технологий или элементов имеет смысл, когда они влияют на устойчивость системы в целом с учётом существующих или возможных внешних и внутренних угроз. При этом приходится учитывать условия и причины возникновения угроз, которые могут быть вызваны как внешними воздействиями, так и ситуацией внутри страны.

Перечень критических технологий Российской Федерации (утв. Указом Президента РФ от 7 июля 2011 г. № 899) включает в себя:

- Технологии доступа к широкополосным мультимедийным услугам.
- Технологии информационных, управляющих, навигационных систем.

- Технологии и программное обеспечение распределенных и высокопроизводительных вычислительных систем.
- Технологии создания электронной компонентной базы и энергоэффективных световых устройств.

Владение перечисленными технологиями определяет возможности обеспечения устойчивости и развития КИИ так же, как всей отрасли информационных технологий и электроники. Владение технологиями включает в себя процессы разработки и производства технических решений, управления цепочками кооперации и каналами поставок, управления рисками и жизненными циклами технологий и информационных систем.

Повышение технологической независимости требует не только развития инженерных компетенций и производственных ресурсов [7], но также требует ограничений на использование закрытых технологий и безальтернативных, не замещаемых технических решений. При этом повышение независимости всегда ограничивает использование наиболее передовых технологий коммерческого сектора, которые в момент появления, как правило являются закрытыми, не имеют альтернативных поставщиков, что используется разработчиками для максимизации прибыли при отсутствии прямой ценовой конкуренции. Решение этого противоречия для государства требует разработки подходов, которые позволяют мотивировать компании на разработку и внедрение новых технологий, но не допускать злоупотребления технологической зависимостью заказчиков.

В настоящее время отсутствует нормативная база для оценки технологической независимости и управления уровнем независимости. Технологическая независимость государства, как субъекта, может быть определена через оценку процессов создания и управления жизненным циклом продукции в области критических технологий, в том числе технологий КИИ.

Понятие «Безопасность КИИ» – другая категория, имеющая чёткие регуляторные и технические определения [8]. В отличие от суверенитета и независимости, оно характеризует не субъект, обладающий собственными целями, а объект управления. Набор требований безопасности для объекта КИИ зависит от источников и факторов угроз [9]. Например, ГОСТ Р 70139-2022 «Центры обработки данных. Инженерная инфраструктура. Классификация» определяет требования к инженерной инфраструктуре ЦОД, в том числе – по обеспечению безопасности. Эти требования касаются не только информационной безопасности, и представлены четырьмя группами:

1. Обеспечение стойкости к внешним воздействиям и явлениям.
2. Обеспечение защиты имущества от нежелательных или несанкционированных физических воздействий.
3. Обеспечение защиты инженерных систем и ИТ-инфраструктуры от нежелательных или несанкционированных логических воздействий.
4. Обеспечение защиты (безопасности) персонала, посетителей и окружающей среды от нежелательных воздействий.

В каждой из перечисленных групп определён конкретный набор показателей, а также целевые значения этих показателей для присвоения ЦОД того или иного класса. В целом, только в областях информационной и функциональной безопасности приняты сотни международных, национальных и отраслевых стандартов, приказов федеральных служб и других нормативных документов, в которых даны технические определения и толкования всех используемых терминов.

Для обеспечения и оценки безопасности значимых объектов КИИ существует соответствующая им нормативная база. Для управления безопасностью КИИ в целом необходима в первую очередь систематизация и актуализация этой нормативной базы,

включая терминологию, источники и факторы угроз, требования безопасности (См. раздел 5. Список основных нормативных правовых актов и документов).

Возвращаясь к Указу № 166, рассмотрим, какие понятия и термины использованы в тексте, и как они связаны с заголовком Указа. В документе использованы следующие термины, в контексте возможности или желательности применения на значимых объектах КИИ:

- Иностранное программное обеспечение.
- Отечественная радиоэлектронная продукция и телекоммуникационное оборудование.
- Доверенные программно-аппаратные комплексы.

Определений этих терминов в тексте Указа нет, как и не использованы понятия «технологический независимости» и «безопасности», выведенные в заголовок.

1. Отечественная радиоэлектронная продукция и телекоммуникационное оборудование

Критерий «иностранное/отечественное» не используется в нормативных документах, регламентирующих безопасность, соответственно он введён в Указе № 166 в целях обеспечения технологической независимости. Рассмотрим эту связь.

Понятие «отечественное оборудование» кажется естественным и простым, но его использование в государственном регулировании вызывает значительные сложности [10]. В любой технически сложной электронной продукции используются в той или иной степени иностранные компоненты и технологии. Разработка и производство электронного оборудования включает более 20 основных технологических переделов, каждый из которых декомпозируется на десятки, иногда сотни технологий. Ни одна страна в мире не обладает полным набором технологий для разработки и производства современной электроники. Поэтому понятие отечественной и иностранной продукции можно определять по уровню добавленной стоимости, по составу технологических операций в производстве, по составу процессов проектирования и других процессов жизненного цикла продукции.

У электронной продукции, выпускаемой на предприятиях РФ, доля участия отечественных компаний в добавленной стоимости может быть совершенно разной – от минимальной, при крупноузловой сборке изделий из иностранных модулей, до преобладающей, в случае полного цикла проектирования на основе отечественных компонентов. Более того, «доля участия» отечественных компаний в количественном или денежном выражении не выглядит подходящим критерием для оценки технологической независимости. Если изделие содержит уникальные, не воспроизводимые в РФ иностранные компоненты, то прекращение их поставок или прав использования создаёт угрозу для всего жизненного цикла продукта. В некоторых случаях доля таких компонентов может быть незначительной в составе изделия, но без них невозможно дальнейшее производство и развитие «почти отечественного» оборудования.

Таким образом, критерий «отечественного происхождения» явно связан с понятием технологической независимости, но является слишком абстрактным и на практике должен быть раскрыт в виде конкретного набора измеряемых характеристик продукта [11]. В настоящий момент базовым документом, определяющим такие характеристики, является постановление Правительства РФ от 17 июля 2015 г. № 719 «О подтверждении производства промышленной продукции на территории Российской Федерации». В документе вводится отдельный набор требований для каждой товарной группы, при этом общим критерием является наличие у заявителя прав на конструкторскую, технологическую и программную документацию на соответствующую продукцию, а в

остальном используются принципиально разные подходы. Дополнительными условиями могут являться (список не исчерпывающий):

1. Соблюдение процентной доли иностранных комплектующих изделий для производства товара (пример – ТН ВЭД 26.20.40.150 – Устройства числового программного управления).

2. Набор заданного количества баллов, которые начисляются за применение отечественной ЭКБ и выполнение технологических операций на территории РФ (пример – ТН ВЭД 26.20.13-15 – Машины вычислительные электронные цифровые).

3. Наличие научно-производственной базы (собственной или контрактной), расположенной на территории РФ и необходимой для разработки и производства продукции, наличие на территории РФ сервисного центра, уполномоченного осуществлять ремонт, гарантийное и постгарантийное обслуживание продукции (пример – большинство товарных групп раздела 26.20 – Компьютеры и периферийное оборудование).

Условия 1 и 2 не имеют прямого отношения ни к безопасности, ни к технологической независимости, и направлены на контроль уровня локализации при производстве продукции. Безусловно, в этом есть экономический смысл, и такой же подход используется в Постановлении для большинства товарных групп, не только в области производства электроники.

Условие 3 направлено на контроль жизненного цикла продукта, от стадии разработки до эксплуатации. Смысл этого требования заключается в защите от угроз блокирования процессов производства, развития и сервисного обслуживания продуктов товарной группы. Тем не менее, требования о наличии у заявителя «научно-производственной базы» и «сервисного центра» выглядят слишком абстрактными без дальнейших уточнений, и не достаточными для каких-либо выводов о соответствии продукции целям технологической независимости.

Для радиоэлектронной продукции такие уточнения требований установлены Постановлением правительства РФ от 10 июля 2019 г. № 878 «О мерах стимулирования производства радиоэлектронной продукции на территории Российской Федерации при осуществлении закупок товаров, работ, услуг для обеспечения государственных и муниципальных нужд, о внесении изменений в постановление Правительства Российской Федерации от 16 сентября 2016 г. № 925 и признании утратившими силу некоторых актов Правительства Российской Федерации». Постановление вводит понятие «Реестр российской радиоэлектронной продукции», определяет правила формирования и ведения этого реестра (далее – Правила), а также порядок его использования при осуществлении закупок [12].

Из всей радиоэлектронной продукции Правила выделяют одну особую категорию – телекоммуникационное оборудование. По всем остальным видам продукции для включения в реестр достаточно заполнить формальную заявку со ссылкой на заключение Министерства промышленности и торговли РФ о подтверждении производства промышленной продукции на территории РФ, в соответствии с Постановлением № 719. В случае телекоммуникационного оборудования подтверждение его производства на территории РФ в рамках Постановления № 719 является необходимым, но не достаточным условием для его включения в реестр, поскольку предъявляются дополнительные требования к заявителю.

К таким требованиям относятся (из п.14 Постановления правительства РФ № 878, в сокращении):

г) заявитель является:

- *разработчиком программного обеспечения, используемого в телекоммуникационном оборудовании, и/или обладает исключительными правами на такое программное обеспечение…;*
- *правообладателем изобретения или полезной модели … либо ему предоставлено право использования в составе телекоммуникационного оборудования изобретения или полезной модели по договору;*
- *заявителем осуществляется модификация программного обеспечения самостоятельно либо на основании соответствующего договора со сторонней организацией с целью дальнейшего развития и улучшения качеств телекоммуникационного оборудования;*

д) заявитель является разработчиком конструкторской (включая архитектурное решение по разработке телекоммуникационного оборудования, схему принципиальную электрическую, шаблон печатных плат электронных блоков для телекоммуникационного оборудования), программной, эксплуатационной и технологической документации…;

е) заявитель имеет возможность осуществлять адаптацию и модификацию конструкторской документации. Заявителю принадлежат на праве собственности или на ином законном основании подлинники конструкторской, технологической и эксплуатационной документации (включая проектную, техническую и пользовательскую документацию);

ж) производство телекоммуникационного оборудования осуществляется на территории Российской Федерации…;

з) заявителем обеспечивается полный цикл тестового и сервисного сопровождения телекоммуникационного оборудования и программного обеспечения, используемого в его составе, на территории Российской Федерации;

и) в телекоммуникационном оборудовании применяются интегральные схемы российского производства первого и второго уровня…;

к) телекоммуникационное оборудование соответствует требованиям по уровню локализации производства…

По каждому пункту требований в Правилах приведён список документов, необходимых для подтверждения соответствия. В частности, по пункту *д)* необходимо предоставить свидетельства о выполнении всех этапов разработки, начиная с копии приказа о проведении ОКР, а также сведения о системе внутреннего контроля за разработкой программного обеспечения, о ключевых блоках и компонентах изделия, о правах владения средствами разработки и т.д.

Совокупность этих требований можно определить, как соответствие определенному уровню контроля жизненного цикла продукта субъектами, находящимися в Российской юрисдикции. В текущей редакции Правил такой термин не используется и подразумевается только два возможных уровня: 1 – продукт соответствует требованиям для включения в реестр, и 0 – не соответствует. Возможно, имеет смысл расширить диапазон возможных значений (как это сделано при определении Классов защиты, Уровней доверия и других характеристик, учитываемых при оценке объектов КИИ), а также обобщить этот подход на другие категории радиоэлектронной продукции. Большинство требований, сформулированных для телекоммуникационного оборудования, полностью применимы и для других категорий – компьютеров, ПАК, АСУ и т.д. Введение общих критериев позволит уйти от фрагментарного подхода в техническом регулировании и вводить требования к отдельным товарным группам только по специфическим для этой группы характеристикам, на основе общих правил.

Оценка уровня контроля жизненного цикла также должна обязательно учитывать санкционные риски, которые могут привести к прекращению поставок отдельных компонентов и материалов, отзыву прав на использование объектов интеллектуальной собственности, или созданию других условий, препятствующих производству и развитию продукта. Эти риски наиболее критичны в случае, когда не существует альтернатив для отдельных ключевых компонентов изделия (например – центрального или сетевого процессора), а каналы поставок и технической поддержки контролируются единственным иностранным производителем. Такие обстоятельства создают одиночную точку блокирования жизненного цикла изделия, и практически обнуляют его уровень контроля, независимо от других характеристик. Действующие правила формирования и ведения реестра РЭП не предусматривают такого анализа, а требования по проектированию на основе ключевых интегральных схем российского происхождения первого или второго уровня обходятся через набор порогового числа баллов за счёт других оцениваемых характеристик изделия, или через использование российских микросхем во вспомогательных модулях, которые не влияют на основной функционал, безопасность и технологическую независимость.

Таким образом, набор требований к контролю жизненного цикла продуктов и технологий, составляющих основу КИИ, позволяет управлять уровнем «Технологической независимости КИИ». Оценка уровня контроля жизненного цикла должна включать все стадии – от выполнения ОКР до эксплуатации изделий и комплексов на объектах КИИ. Действующая нормативная база предусматривает проведение таких оценок только для телекоммуникационного оборудования. Целесообразно распространить этот подход на все другие группы электронной продукции. Для системной оценки соответствия продукции и технологий КИИ целям технологической независимости необходимо разработать единую классификацию по уровням контроля жизненного цикла и методики оценки (сертификации) по каждому из уровней. Такой подход позволит регуляторам ссылаться в нормативных документах, определяющих требования к отдельным категориям изделий и систем в составе КИИ, на необходимый уровень контроля жизненного цикла, подтвержденный сертификатом соответствия.

2. Доверенные программно-аппаратные комплексы

Термин «доверенные программно-аппаратные комплексы» ранее не использовался в российской нормативно-правовой базе, однако его можно рассматривать, как составной термин, включающий понятия «доверие» и «программно-аппаратный комплекс» (ПАК).

Понятие «доверие» определено в контексте безопасности информационных технологий. ГОСТ Р ИСО/МЭК 15408-1-2012 «Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 1 – Введение и общая модель» определяет этот термин следующим образом (Раздел 3 – Термины и определения, п. 3.1.4):

Доверие – основание для уверенности в том, что объект оценки (ОО) отвечает конкретным функциональным требованиям безопасности (ФТБ).

В этом же стандарте определено понятие «доверенный продукт ИТ» (Раздел 3 – Термины и определения, п. 3.1.79):

Доверенный продукт ИТ – Продукт ИТ, отличный от ОО, для которого имеются свои функциональные требования, отличные от ОО, и который, как предполагается, реализует свои функциональные требования корректно. Примечание – примером доверенного продукта ИТ является продукт, который был отдельно оценен.

Указ президента РФ № 166 от 30.03.2022 г. «О мерах по обеспечению технологической независимости и безопасности критической информационной инфраструктуры Российской Федерации» в своём названии указывает на обеспечение безопасности КИИ, и понятие доверия в сочетании «доверенные программно-аппаратные комплексы» должно рассматриваться именно в этом контексте.

Термин «программно-аппаратные комплексы» (ПАК) является синонимом термина «аппаратно-программные комплексы» (АПК), при этом в нормативных документах используются оба этих термина без каких-либо смысловых различий. Определение ПАК введено Постановлением правительства РФ от 28.12.2022 № 2461:

«Программно-аппаратный комплекс» – комплекс технических и программных средств (программного обеспечения), работающих совместно для выполнения одной или нескольких специальных задач, являющийся электронной вычислительной машиной или специализированным электронным устройством (устройствами), функционально-технические характеристики которого (которых) определяются исключительно совокупностью программного обеспечения и технических средств и не могут быть реализованы при их разделении. Программно-аппаратный комплекс является самостоятельно используемым, законченным техническим изделием, имеющим серийный номер.

Ещё один близкий по смыслу термин – «программно-технический комплекс» (ПТК) используется в стандартах на автоматизированные системы (АС). ГОСТ Р 59853-2021 «Информационные технологии (ИТ). Комплекс стандартов на автоматизированные системы. Автоматизированные системы. Термины и определения» приводит следующее определение:

«Программно-технический комплекс автоматизированной системы; программно-технический комплекс АС; ПТК АС»: Совокупность совместно функционирующих технических, программных и информационных средств, предназначенных для выполнения определенного набора функций АС.

В этих определениях сложно увидеть смысловые различия, но формальные различия в формулировках есть. Для ПАК устанавливается связь программного обеспечения и технических средств, без которой (при разделении аппаратной и программной составляющей) характеристики ПАК не могут быть реализованы. Для ПТК такого ограничения нет, но сам этот термин введён только в контексте автоматизированных систем и не применим вне этого контекста. Кроме того, в составе ПТК упоминаются информационные средства, которых в определении ПАК нет.

Для трактовки взаимосвязей и различий терминов ПАК и ПТК обратимся к Приказу Министерства цифрового развития, связи и массовых коммуникаций Российской Федерации от 31.01.2023 № 62 «Об утверждении классификатора программно-аппаратных комплексов и Правил применения классификатора программно-аппаратных комплексов». Классификатор предназначен для формирования реестра российских программ для ЭВМ и баз данных в части ПАК.

Приказ вводит понятие «Раздел ПАК», отражающий определенную технологию или сферу применения ПАК, а также, внутри каждого раздела – «Класс ПАК» с присвоенным ему числовым обозначением (кодом), определяющий конкретное назначение ПАК и в некоторых случаях – дополнительные характеристики класса. Пункт 2 Правил применения классификатора (утв. этим же Приказом) гласит: *«Использование кода, не внесённого в Классификатор, не допускается»*.

Таким образом, Приказ вводит конечный формализованный список классов ПАК. Произвольный комплекс технических и программных средств может быть признан ПАК

только в том случае, если он соответствует по своему назначению одному из классов. Нужно ли понимать требование о том, что функционально-технические характеристики ПАК определяются исключительно совокупностью программного обеспечения и технических средств и не могут быть реализованы при их разделении, как техническую невозможность разделения аппаратной платформы и программного обеспечения ПАК без утраты функциональности? Введённая Приказом классификация даёт однозначно понять, что ответ на этот вопрос – нет. В качестве примера можем рассмотреть Класс 02.10 – Программно-аппаратные комплексы математического и имитационного моделирования, определенные, как *«Программно-аппаратные комплексы, предоставляющие возможность имитации (моделирования) процесса функционирования различных изделий и систем»*. Очевидно, что ПО математического и имитационного моделирования может быть установлено на широкий класс различных совместимых по характеристикам аппаратных платформ (серверов) и в свою очередь, эти же сервера могут использоваться и для другого, сходного по функциональности ПО. Для множества других классов выводы о технической возможности разделения аппаратной платформы и ПО аналогичные. Отсюда следует, что требование о невозможности разделения относится только к конкретному набору функционально-технических характеристик ПАК, который заявлен его разработчиком или производителем. Смысл в том, что эта совокупность характеристик не может рассматриваться по отдельности в отношении аппаратной платформы и в отношении ПО, а определена только для ПАК, как единого целого.

Продолжая сравнение определений ПАК и ПТК, отметим, что в области регулирования автоматизированных систем единственное отличие этих понятий – в привязке ПАК к определенной классификации. Если ПАК должен соответствовать одному из классов, то ПТК можно назвать произвольный комплекс, предназначенный для выполнения определенного набора функций АС. В абсолютном большинстве случаев классификатор ПАК уже включает классы, соответствующие различным видам автоматизированных систем. Например, для АСУТП введен класс ПАК 11.05 – Программно-аппаратные комплексы автоматизированного управления технологическими процессами. В этом случае можно сказать, что ПТК АСУТП (в определении ГОСТ Р 59853-2021) реализован, как ПАК класса 11.05 с набором информационных средств, специфичных для целевого технологического процесса. Этот же подход можно использовать для ПТК АС, которые имеют несколько различных наборов функций, соответствующих различным классам ПАК. В этом случае ПТК может включать в себя несколько ПАК различных классов, и возможно – дополнительное технологическое оборудование, не относящееся ни к одному из ПАК.

Таким образом, Указ № 166 с одной стороны определяет требования, которые направлены на контроль жизненного цикла продукции и в конечном итоге создают базу для технологической независимости, а с другой – использует термин «Доверенные ПАК», связанный с безопасностью КИИ и находящийся в области регулирования ФСТЭК России, а в части криптозащиты – ФСБ России.

В зоне ответственности ФСТЭК России находятся специальные требования безопасности, устанавливаемые в зависимости областей и условий применения оборудования или ПО. Следующими приказами ФСТЭК России уже введены требования для конкретных условий применения и типов оборудования:

- Приказ ФСТЭК России от 25 декабря 2017 г. № 239 «Требования по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации».

- Приказ ФСТЭК России от 2 июня 2020 г. № 76 «Требования по безопасности информации, устанавливающие уровни доверия к средствам технической защиты информации и средствам обеспечения безопасности информационных технологий».
- Приказ ФСТЭК России от 3 апреля 2018 г. № 55 «Положение о системе сертификации средств защиты информации».
- Приказ ФСТЭК России от 14 марта 2014 г. № 31 «Требования к обеспечению защиты информации в автоматизированных системах управления производственными и технологическими процессами на критически важных объектах, потенциально опасных объектах, объектах, представляющих повышенную опасность для жизни и здоровья людей и для окружающей природной среды».
- Приказ ФСТЭК России от 11 февраля 2013 года № 17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах».
- Приказ ФСТЭК России от 18 февраля 2013 г. № 21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных».
- Приказ ФСТЭК России от 27 октября 2022 г. № 187 «Об утверждении Требований по безопасности информации к средствам виртуализации».

В зависимости от области применения технических и программных средств и характеристик объекта защиты ФСТЭК устанавливает конкретный набор требований безопасности, которые могут быть подтверждены с определённым уровнем доверия. Этот подход полностью согласуется с определениями доверия и доверенного продукта ИТ по ГОСТ Р ИСО/МЭК 15408-1-2012.

3. Проблемы нормативно-правовой базы

Появление нового класса требований, направленного на контроль жизненного цикла критически важных продуктов и технологий, не вписывалось в сложившуюся структуру нормативно-правовой базы РФ. Со стороны регуляторов, отвечающих за контроль функциональной и информационной безопасности, критерий отечественного или иностранного происхождения продукта не соответствовал общепринятым принципам, целям и методам технического контроля. В зоне ответственности правительства РФ такой критерий присутствовал, но использовался в других целях, а именно – стимулирования производства продукции на территории РФ. Для большинства видов продукции измерение долей отечественных и иностранных комплектующих или начисление баллов за выполнение определенных операций на территории РФ является естественным подходом, позволяющим российским предприятиям увеличивать добавленную стоимость в выпускаемой продукции, а на уровне государства – поддерживать торговый баланс российской промышленности и развивать экономику в целом. Однако, оптимизация критериев и методик оценки российского происхождения продукции исключительно из соображений экономической эффективности, оказалась после введения санкций несостоятельной. Без учета технологической независимости через оценку контроля жизненного цикла продукта и его ключевых компонентов экономическое развитие оказывается неустойчивым. Оно обрывается зарубежными государственными регуляторами или решениями зарубежных корпораций, чьи технологии составляют основу выпускаемой в России продукции.

Дальнейшее уточнение требований к продукции не должно ограничиваться стимулированием производства, оно должно включать критерии безопасности и

технологический независимости в области критических технологий. Такие меры могут иметь негативный экономический эффект в краткосрочном плане, например, в отдельных случаях сдерживать планы развития цифровой инфраструктуры. В долгосрочной перспективе они будут и экономически более эффективны, чем действующие подходы, стимулирующие локализацию производства зарубежных разработок.

Структура требований должна включать в себя три пересекающихся набора критериев – безопасности, локализации и контроля жизненного цикла продукции. В настоящее время они не согласованы между собой – пересекаются, но не учитывают друг друга, рис. 1.

Рис. 1. Текущая структура требований к продукции КИИ
Fig. 1. Current structure of requirements for CII products

Это создает значительное увеличение бюрократической нагрузки и повышает уровень неопределенности в экспертизе и регулировании рынка, оставляет риски уязвимости инфраструктуры и неустойчивости экономического развития промышленности. Негативно влияет расширение требований безопасности и контроля жизненного цикла до полного набора требований по локализации, еще хуже подмена этих требований уровнем локализации. С другой стороны, нежелателен перенос всех требований безопасности и контроля жизненного цикла на продукцию, которая не имеет отношения к КИИ, и может оцениваться только по уровню локализации для допуска к государственным закупкам.

Требования контроля жизненного цикла в нормативной базе представлены эпизодически и разрозненно в положениях по отдельным группам продукции. В то же время, именно требования по контролю жизненного цикла являются наиболее универсальными для всех групп продукции. Поскольку они обеспечивают технологическую независимость, целесообразно рассматривать их в совокупности с требованиями безопасности, как общий набор Требований доверия. Тогда требования контроля жизненного цикла будут областью пересечения в регулировании безопасности и технологической независимости КИИ и в регулировании государственных закупок, общая структура требований будет иметь вид, представленный на рис. 2.

Рис. 2. Оптимизированная структура требований к продукции КИИ
Fig. 2. Optimized structure of CII product requirements

Систематизация требований предполагает дополнение понятия доверия, основанного на контроле требований безопасности, требованиями контроля жизненного цикла продукции, аналогичными требованиям к разработчикам и процессам разработки в действующих положениях ТОРП (Часть III Постановления правительства РФ № 878). Также общие требования по контролю жизненного цикла должны быть включены в регулирование рынка по уровню локализации по всем товарным группам продукции ИТ. Таким образом, контроль жизненного цикла окажется внутри области пересечения требований доверия и требований локализации продукции. Для продукции, ориентированной на рынки, не относящиеся к КИИ, достаточно будет получить подтверждение уровня локализации для доступа к закупкам, регулируемым ФЗ № 44 и № 223 без дополнительных проверок уровня безопасности. Продукция для КИИ может не соответствовать полному набору требований локализации в той части, которая не влияет на безопасность, например, в части происхождения пассивных компонентов и несущих конструкций.

Если требования по контролю жизненного цикла полностью перекрывают требования по уровню локализации (рис. 3), то процедура экспертизы по уровню локализации для оборудования КИИ может быть сокращена – продукция будет получать доступ ко всем рынкам государственных закупок по факту соответствия требованиям доверия. Если продукция не адресована КИИ, то проще пройти экспертизу на соответствие сокращенному набору требований по уровню локализации без обращения к регуляторам КИИ.

Рис. 3. Структура требований к продукции КИИ с общей оценкой по требованиям доверия
Fig. 3. The structure of requirements for CII products with a general assessment of the requirements of trust

В текущей структуре требований к продукции КИИ средства контроля жизненного цикла продукции представлены в виде дополнительных требований к отдельным товарным группам при подтверждении производства продукции на территории РФ. Кроме того, постановлениями Правительства РФ введены отдельные реестры российской

радиоэлектронной продукции и российского ПО (включая ПАК), для которых предусмотрены свои собственные требования по включения продукции в реестр для определенных категорий (для реестра РЭП в такую категорию было выделено телекоммуникационное оборудование). В результате при регистрации продуктов в реестрах определенный продукт может быть законно признан продукцией российского происхождения своей товарной группы и войти в общий реестр российской промышленной продукции по требованиям постановления Правительства РФ № 719, но при этом может не войти в реестр РЭП по требованиям постановления № 878.

С точки зрения контроля закупок предприятиями и организациями, находящимися в собственности или под контролем государства, появление дополнительных требований только осложнило осуществление таких закупок, так же, как и выход на рынок производителям определенных товарных групп.

Использование номенклатуры ТН ВЭД для определения требований к закупкам может быть оправдано для целей экономического стимулирования, но в области технического контроля такой подход не имеет смысла. Товары одной и той же группы могут закупаться для применения в составе значимых объектов КИИ, государственных ИС, или других критических технологий, а могут – для выполнения второстепенных функций, не имеющих никакого отношения к технологической независимости и безопасности.

В практике ФСТЭК возможность применения того и иного продукта в определенных условиях, связанных с видом инфраструктуры и степенью критичности или секретности обрабатываемой информации, всегда опиралось на соответствие объекта оценки набору измеряемых характеристик, как правило – с градацией по нескольким категориям (Классы защиты, уровни доверия, уровни контроля отсутствия недекларированных возможностей и т.д.). В случае новой категории требований к уровню контроля жизненного цикла продукта таких метрик не было, и в результате в области технического регулирования начал использоваться искусственный критерий – включение сведений об объекте оценки в один из реестров продукции. В частности, согласно Приказу ФСТЭК России от 2 июня 2020 г. № 76 «Требования по безопасности информации, устанавливающие уровни доверия к средствам технической защиты информации и средствам обеспечения безопасности информационных технологий», в числе условий для установления соответствия средства четвертому уровню доверия указаны:

- *Сведения об аппаратной платформе средства должны быть включены в единый реестр российской радиоэлектронной продукции;*
- *Сведения о процессорах или микросхемах, выполняющих функции; процессоров (микроконтроллеры), элементах памяти, сетевых картах, графических адаптерах аппаратной платформы средства должны быть включены в единый реестр российской радиоэлектронной продукции.*

В результате, вопросы экономического стимулирования, технического контроля, информационной и функциональной безопасности оказались, сведены вместе с вопросами технологической независимости к включению или не включению продукта в реестр РЭП без каких-либо градаций его соответствия требованиям (рис. 4).

Структура на рис. 4 демонстрирует условия для принятия двух видов решений – о применимости СЗИ или СВТ в составе КИИ, и о возможности закупки госпредприятиями и организациями товаров определенной товарной группы. Оба этих решения зависят от внесения записи о товаре в реестр российской промышленной продукции и/или реестр РЭП. Критерии включения в реестры, основанные на принципах экономического стимулирования, могут оказаться недостаточными для контроля безопасности и технологической независимости, но их расширение до уровня, необходимого в КИИ, может

создать государственным заказчикам необоснованные препятствия для закупок в других, не связанных с КИИ целях.

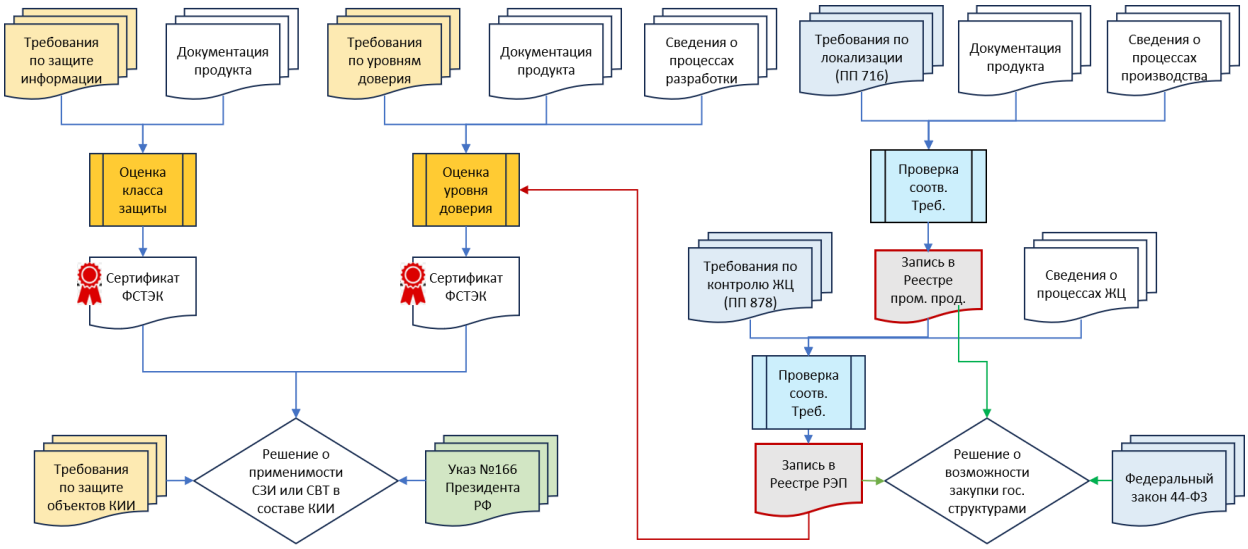

Рис. 4. Структура регулирования допуска СЗИ и СВТ к применению на объектах КИИ и при осуществлении государственных закупок
Fig. 4. The structure of regulation of the admission of SPI and SVT to use at CI facilities and in the implementation of public procurement

Решение возникающих, как следствие такого смешения, проблем у всех участников рынка определенно лежит в области пересмотра самого подхода, в котором понятия и категории из совершенно разных по своей природе направлений государственного, экономического и технического регулирования сведены к единому реестру «на все случаи жизни».

4. Предложения по развитию нормативно-правовой базы в целях управления уровнем технологической независимости КИИ

Развитие нормативной базы в целях управления технологической независимостью КИИ может опираться на зрелые, согласованные с национальными и международными стандартами подходы, которые используются ФСТЭК в области безопасности ИТ.

Нормативные документы ФСТЭК образуют систему с жёстко определенными связями, позволяющую для любой предметной области в зоне ответственности ФСТЭК однозначно определить совокупность требований безопасности. В отношении объектов КИИ регулируется, в частности, применение сертифицированных средств защиты информации (СЗИ) и средств вычислительной техники (СВТ). Приказ ФСТЭК № 239 «Об утверждении требований по обеспечению безопасности значимых объектов КИИ» от 25.12.2017 определяет эти требования, как соответствие классам защиты. Например, для объектов КИИ 1 категории (п. 29 а):

а) в значимых объектах 1 категории применяются средства защиты информации не ниже 4 класса защиты, а также средства вычислительной техники не ниже 5 класса.

Для объектов КИИ 2 и 3 категории Приказ № 239 также требует соответствия применяемых СВТ 5 классу защиты (п.29 б, в).

Связь классов защиты с уровнями доверия установлена приказом ФСТЭК № 76 от 02.06.2020 «Требования по безопасности информации, устанавливающие уровни доверия…» (п. 5):

Устанавливается следующее соответствие классов средств защиты информации и средств вычислительной техники уровням доверия:

средства защиты информации 4 класса и средства вычислительной техники 5 класса должны соответствовать 4 уровню доверия.

Рассмотрим подробнее требования, установленные Приказом для СЗИ и СВТ 4 уровня доверия, с точки зрения обеспечения технологической независимости. Приказ устанавливает три группы требований (п. 6):

1. Требования к разработке и производству средства.
2. Требования к проведению испытаний средства.
3. Требования к поддержке безопасности средства.

В каждой группе определены требования к составу и содержанию документации, подлежащей оценке, а также к процессам жизненного цикла изделия. Для стадии разработки и производства Приказ определяет необходимые процедуры (п. 7):

При разработке средства разработчиком должны быть выполнены процедуры, предусматривающие:

1) разработку модели безопасности средства;
2) проектирование архитектуры безопасности средства;
3) разработку функциональной спецификации средства;
4) проектирование средства;
5) разработку проектной (программной) документации;
6) выбор средств разработки, применяемых для создания средства;
7) управление конфигурацией средства;
8) разработку документации по безопасной разработке средства;
9) разработку эксплуатационной документации.

По каждой из перечисленных процедур разработчик должен предоставить комплект документов, подтверждающий полноту и качество выполненных работ с учётом заявленного уровня доверия. Наличие у заявителя такого комплекта документов позволяет провести объективную оценку по требованиям безопасности и тот же комплект документов может быть использован для оценки по критериям технологической независимости. Однако, последнее выходит за рамки определения доверия и в Приказе не рассматривается. Оценка доверия, согласно Требованиям, проводится только в отношении объекта (продукта) и технологических процессов его жизненного цикла, но не в отношении субъекта – разработчика. В результате, сертификацию по уровню доверия может получить продукт, представленный заявителем – посредником, который не является разработчиком, а лишь обладает необходимым комплектом документации от иностранной компании, заинтересованной в локализации производства и сопровождения своего продукта на территории РФ. Права компании-посредника, касающиеся порядка использования, распространения и модификации переданных ей объектов интеллектуальной собственности могут быть существенно ограничены, и оставаться под контролем иностранной компании, владеющей продуктом.

Примером системной оценки субъекта – заявителя по критериям технологической независимости может служить Постановление правительства РФ от 10 июля 2019 г. № 878 в части телекоммуникационного оборудования. Для присвоения статуса телекоммуникационного оборудования российского происхождения (ТОРП) его заявитель должен находиться в российской юрисдикции и контролироваться более, чем на 50%

российскими собственниками, а также подтвердить право владения на законном основании полным комплектом конструкторской, технологической, эксплуатационной и программной документации изделия (п. 14 ПП РФ № 878). Право владения в данном случае понимается, как право собственности либо право неограниченного использования всех видов проектной документации и заимствованных объектов интеллектуальной собственности на основе исключительной или открытой (свободной) лицензии.

В целях управления уровнем технологической независимости КИИ требования Приказа ФСТЭК № 76 могут быть совмещены с подходами ПП РФ № 878 в рамках нового нормативного документа, по следующим принципам:

- Комплект документов, предусмотренный Приказом № 76 для оценки уровня доверия по критериям безопасности, должен также использоваться для оценки по критериям технологической независимости КИИ. Наличие такого комплекта в любом случае необходимо для подтверждения уровня доверия СЗИ и СВТ, применяемых в КИИ.
- Оценка по критерию технологической независимости должна выполняться в отношении субъекта – заявителя и субъектов всей технологической цепочки, в рамках полного жизненного цикла продукта. Примером могут служить требования к подтверждению статуса ТОРП из ПП РФ № 878. Результатом оценки может являться сертификат соответствия продукта заявленному уровню контроля жизненного цикла российскими лицами.
- Требования приказа № 76, относящиеся к контролю безопасности ИТ, должны быть дополнены требованиями, обеспечивающими защиту жизненного цикла продукта от угроз, связанных с технологической зависимостью.

Последний в списке тезис поясним на примере. Одним из требований Приказа ФСТЭК России № 76 к проектной документации является (п. 12.1):

Для аппаратной платформы средства должен быть разработан (представлен) перечень аппаратных устройств (микросхем), которые влияют на выполнение функций безопасности и/или могут быть использованы для реализации угроз безопасности информации.

Далее (п. 12.2):

В случае отсутствия сведений о заимствованных компонентах средства должны быть спроектированы, реализованы и описаны в документации на средство меры защиты информации, направленные на блокирование эксплуатации возможных уязвимостей и реализуемых заимствованными элементами (компонентами) потенциально опасных возможностей.

В целях контроля жизненного цикла продукта аналогичные требования могут быть сформулированы следующим образом:

Для аппаратной платформы средства должен быть разработан (представлен) перечень компонентов (комплектующих изделий) и технологий, которые влияют на устойчивость жизненного цикла и/или могут быть использованы для реализации угроз процессам управления жизненным циклом.

В случае отсутствия сведений о заимствованных компонентах средства и/или технологиях должны быть разработаны и описаны меры защиты, направленные на блокирование угроз процессам управления жизненным циклом.

Примером угрозы жизненному циклу в этих определениях может являться наличие в составе устройства компонента с уникальными техническими характеристиками, контролируемого единственным иностранным поставщиком, а примером меры защиты – разработка альтернативной конфигурации аппаратной платформы, которая позволит продолжить выпуск и сопровождение продукта при реализации угрозы.

Дополнительным критерием при оценке угроз жизненному циклу и мер защиты может являться принадлежность компании-разработчика к странам, не входящим в список недружественных (см. Распоряжение Правительства РФ от 05.03.2022 № 430-р «Об утверждении перечня иностранных государств и территорий, совершающих недружественные действия в отношении Российской Федерации, российских юридических и физических лиц»). Ещё одним фактором, снижающим уровень риска, может быть наличие нескольких независимых поставщиков компонентов, совместимых с разработанной аппаратной платформой, в странах, не объявленных недружественными.

Присвоение статуса (уровня соответствия) СВТ по критериям технологической независимости может быть организовано на основе действующего, зрелого процесса ФСТЭК по оценке классов защиты информации и уровней доверия СЗИ и СВТ. Соответствие требованиям по контролю жизненного цикла может оцениваться в рамках единого процесса сертификации по уровням доверия, в дополнение к уже существующей процедуре оценки доверия в отношении функциональных требований безопасности, рис. 5.

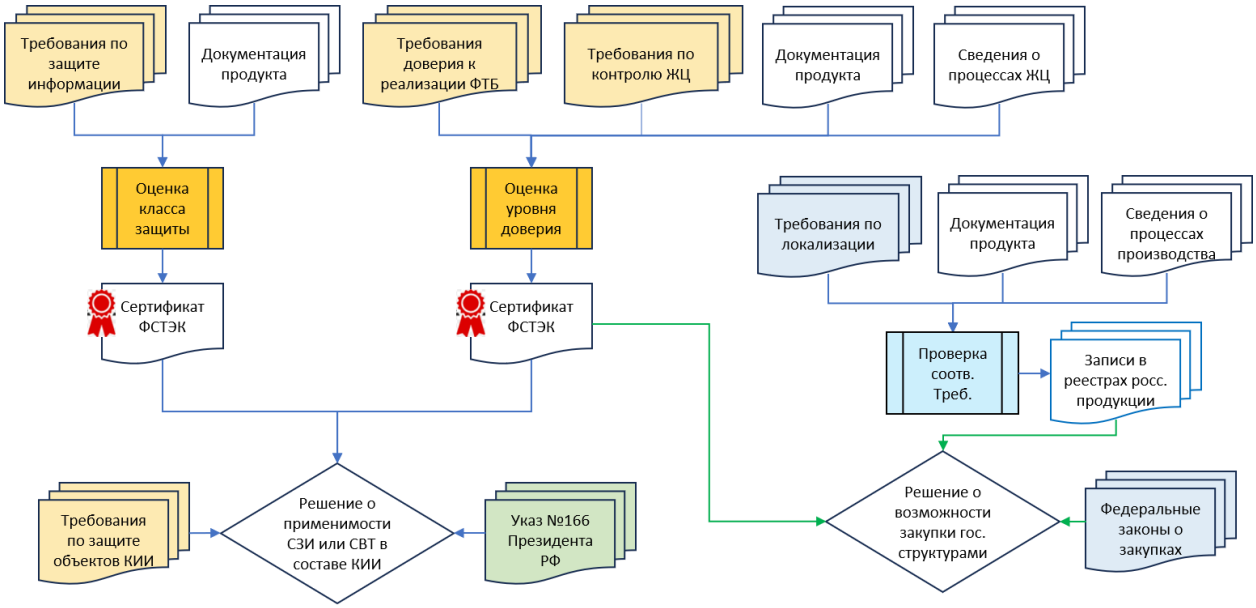

Рис. 5. Оптимизированная структура регулирования допуска СЗИ и СВТ к применению на объектах КИИ и при осуществлении государственных закупок
Fig. 5. The optimized structure of the regulation of the admission of SPI and SVT to use at CII facilities and in the implementation of the state. procurement

Получение сертификата соответствия необходимому уровню контроля жизненного цикла может являться достаточным условием для допуска продукции к закупкам, в тех случаях, когда требования по локализации для соответствующей товарной группы перекрываются требованиями по контролю жизненного цикла. В случаях, когда для товарной группы предусмотрены особые условия по локализации производства, наличие сертификата также может учитываться при включении в реестр, для исключения повторных проверок требований, уже подтверждённых при сертификации. Сертификаты уровня доверия, учитывающие требования по контролю жизненного цикла, могут использоваться не только в целях допуска оборудования к применению на объектах КИИ или к участию в гос. закупках, но и в других чувствительных областях применения – в государственных информационных системах, АСУ, системах обработки персональных данных и т.д. Для

каждой категории инфраструктуры или обрабатываемых данных может быть определён свой необходимый уровень сертификации, с учётом условий применения и критичности защищаемых технологий.

Предлагаемое решение также обеспечивает возможность отзыва выданного сертификата при изменении условий, которые могли повлиять на оценку при проведении сертификации. В части технологической независимости к таким условиям можно отнести изменение структуры собственников заявителя, замену ключевых аппаратных и/или программных компонентов, а также смену локации выполнения технологических операций, критичных для жизненного цикла продукта.

5. Список основных нормативных правовых актов и документов

1. Указ президента РФ «О мерах по обеспечению технологической независимости и безопасности критической информационной инфраструктуры Российской Федерации» от 30 марта 2022 г. № 166.
2. Указ Президента РФ "Об утверждении приоритетных направлений развития науки, технологий и техники в Российской Федерации и перечня критических технологий Российской Федерации" от 7 июля 2011 г. № 899.
3. ГОСТ Р ИСО/МЭК 15408-1-2012 «Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 1 – Введение и общая модель».
4. ГОСТ Р ИСО/МЭК 15408-2-2013 «Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 2 – Функциональные компоненты безопасности».
5. ГОСТ Р ИСО/МЭК 15408-3-2013 «Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 3 – Компоненты доверия к безопасности».
6. ГОСТ Р ИСО/МЭК 27000-2021 «Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Общий обзор и терминология».
7. ГОСТ Р ИСО/МЭК 27001-2021 «Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования».
8. ГОСТ Р ИСО/МЭК 27002-2021 «Информационные технологии. Методы и средства обеспечения безопасности. Свод норм и правил применения мер обеспечения информационной безопасности».
9. ГОСТ Р ИСО/МЭК 21827-2010 «Информационная технология. Методы и средства обеспечения безопасности. Проектирование систем безопасности. Модель зрелости процесса».
10. ГОСТ Р ИСО/МЭК ТО 19791-2008 «Информационная технология. Методы и средства обеспечения безопасности. Оценка безопасности автоматизированных систем».
11. ГОСТ Р ИСО/МЭК 27033-1-2011 «Информационная технология. Методы и средства обеспечения безопасности. Безопасность сетей. Часть 1. Обзор и концепции».
12. ГОСТ Р ИСО/МЭК 27033-2-2021 «Информационная технология. Методы и средства обеспечения безопасности. Безопасность сетей. Часть 2. Рекомендации по проектированию и реализации безопасности сетей».
13. ГОСТ Р ИСО/МЭК 27033-3-2014 «Информационная технология. Методы и средства обеспечения безопасности. Безопасность сетей. Часть 3. Эталонные сетевые сценарии».
14. ГОСТ Р ИСО/МЭК 27033-4-2021 «Информационная технология. Методы и средства обеспечения безопасности. Безопасность сетей. Часть 4. Обеспечение безопасности межсетевого взаимодействия с использованием шлюзов безопасности».
15. ГОСТ Р ИСО/МЭК 27033-5-2021 «Информационная технология. Методы и средства обеспечения безопасности. Безопасность сетей. Часть 5. Обеспечение безопасности межсетевого взаимодействия с помощью виртуальных частных сетей (ВЧС)».
16. ГОСТ Р 70139-2022 «Центры обработки данных. Инженерная инфраструктура. Классификация»
17. ГОСТ Р 59853-2021 «Информационные технологии (ИТ). Комплекс стандартов на автоматизированные системы. Автоматизированные системы. Термины и определения».

18. ГОСТ Р 51583—2014 «Защита информации. Порядок создания автоматизированных систем в защищенном исполнении. Общие положения».

19. ГОСТ Р 50739-95 «Средства вычислительной техники. Защита от несанкционированного доступа к информации. Общие технические требования».

20. Методический документ. Методика оценки угроз безопасности информации. *(Утвержден ФСТЭК России 5 февраля 2021 г.)*.

21. Положение о банке данных угроз безопасности информации *(Утверждено приказом ФСТЭК России от 16 февраля 2015 г. № 9)*.

22. Методический документ. Регламент включения информации об уязвимостях программного обеспечения и программно-аппаратных средств в банк данных угроз безопасности информации ФСТЭК России.

23. Требования по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации *(Утверждены приказом ФСТЭК России от 25 декабря 2017 г. № 239)*.

24. Требования по безопасности информации, устанавливающие уровни доверия к средствам технической защиты информации и средствам обеспечения безопасности информационных технологий *(Утверждены приказом ФСТЭК России от 2 июня 2020 г. № 76)*.

25. Положение о системе сертификации средств защиты информации *(Утверждено приказом ФСТЭК России от 3 апреля 2018 г. № 55)*.

26. Требования к обеспечению защиты информации в автоматизированных системах управления производственными и технологическими процессами на критически важных объектах, потенциально опасных объектах, объектах, представляющих повышенную опасность для жизни и здоровья людей и для окружающей природной среды. *(Утверждены приказом ФСТЭК России от 14 марта 2014 г. № 31)*.

27. Требования о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах *(Утверждены приказом ФСТЭК России от 11 февраля 2013 г. № 17)*.

28. Требования по безопасности информации к средствам виртуализации *(Утверждены приказом ФСТЭК России от 27 октября 2022 г. № 187)*.

29. Приказ ФСТЭК России «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных» с Приложением «Состав и содержание мер по обеспечению безопасности персональных данных, необходимых для обеспечения каждого из уровней защищенности персональных данных» от 18.02.2013 № 21 (в ред. от 14.05.2020).

30. Приказ Министерства цифрового развития, связи и массовых коммуникаций Российской Федерации «Об утверждении классификатора программно-аппаратных комплексов и Правил применения классификатора программно-аппаратных комплексов» от 31.01.2023 № 62.

31. Федеральный закон «О контрактной системе в сфере закупок товаров, работ, услуг для обеспечения государственных и муниципальных нужд» от 05.04.2013 № 44-ФЗ.

32. Федеральный закон «О закупках товаров, работ, услуг отдельными видами юридических лиц» от 18 июля 2011 г. № 223-ФЗ.

33. Постановление Правительства РФ «О подтверждении производства промышленной продукции на территории Российской Федерации» от 17 июля 2015 г. № 719.

34. Постановление правительства РФ «О мерах стимулирования производства радиоэлектронной продукции на территории Российской Федерации при осуществлении закупок товаров, работ, услуг для обеспечения государственных и муниципальных нужд, о внесении изменений в постановление Правительства Российской Федерации от 16 сентября 2016 г. № 925 и признании утратившими силу некоторых актов Правительства Российской Федерации» от 10 июля 2019 г. № 878.

35. Постановление Правительства РФ «Об установлении запрета на допуск программного обеспечения, происходящего из иностранных государств, для целей осуществления закупок для обеспечения государственных и муниципальных нужд» от 16 ноября 2015 г. № 1236.

36. Постановление Правительства РФ «О внесении изменений в постановление Правительства Российской Федерации от 16 ноября 2015 г. № 1236 и признании утратившими силу отдельных положений некоторых актов Правительства Российской Федерации» от 28.12.2022 № 2461.

Заключение

- Предлагаем нормативно разделить понятия и критерии оценки технологической независимости субъектов КИИ и безопасности объектов КИИ. Предлагаем также не смешивать их с экономическими критериями добавленной стоимости и локализации.
- В настоящее время нормативная база для оценки технологической независимости субъектов КИИ отсутствует. Предлагаем разработать требования к контролю жизненного цикла продуктов и технологий, составляющих объекты КИИ, в качестве критерия оценки технологической независимости субъекта КИИ. Для всех групп продукции и технологий КИИ установить единую классификацию по уровням контроля жизненного цикла и методики оценки по каждому из уровней. Включить в критерии оценки все стадии жизненного цикла – от выполнения ОКР до эксплуатации изделий и комплексов на объектах КИИ.
- В целях контроля соответствия ПАК и других продуктов в составе КИИ новому классу требований предлагаем ввести на законодательном уровне процедуру оценки соответствия требованиям к контролю жизненного цикла электронной продукции, по аналогии с действующими процедурами ФСТЭК России по оценке (сертификации) средств защиты информации и средств вычислительной техники. Ответственность за разработку нормативной базы, регламентирующей требования по контролю жизненного цикла продукции и технологий, возложить на федеральные службы (ФСТЭК России, ФСБ России, Росстандарт) в рамках их компетенций.
- Регулирование в плоскости экономических параметров добавленной стоимости и локализации, включая реестры российской продукции, предлагаем использовать в качестве меры дополнительного стимулирования к повышению уровня технологической независимости. При этом предлагаем исключить ссылки на реестры российской продукции из документов, регламентирующих оценки уровня безопасности объектов КИИ и технологической независимости субъектов КИИ.
- Чтобы исключить противоречия и разночтения в понятиях, которые используется для управления безопасностью КИИ, предлагаем подготовить пояснения к Указу президента РФ № 166 от 30.03.2022, в которых систематизировать действующую нормативную базу, гармонизировать терминологию, актуализировать и расширить перечень источников и факторов угроз.

СПИСОК ЛИТЕРАТУРЫ:

1. Сухарев О.С. Технологическая независимость России: способы обеспечения. Россия: общество, политика, история. 2023;(1(6)):24-39. DOI: https://doi.org/10.56654/ROPI-2023-1(6)-24-39.
2. Журиков Роман Н.; Щукин Илья С.; Юшков Ярослав Н. Обеспечение технологической независимости путем создания необходимых запасов ЭКБ как один из элементов ее доверенности. Безопасность информационных технологий, [S.l.], т. 30, № 3, с. 149–157, 2023. ISSN 2074-7136. DOI: http://dx.doi.org/10.26583/bit.2023.3.10. – EDN ZEGTRV.
3. Мусиенко Н.О., Лысов Д.А., Медведева В.Д., Кузина В.В. Обзор Указа президента РФ № 166 от 30.03.2022 «О мерах по обеспечению технологической независимости и безопасности критической информационной инфраструктуры Российской Федерации» в контексте создания системы информационной безопасности для значимых объектов критической информационной инфраструктуры. В сборнике: Информационная безопасность и защита персональных данных. Проблемы и пути их решения. Сборник материалов и докладов XV межрегиональной научно-практической конференции. Под общей редакцией О.М. Голембиовской. Брянск. 2023, с. 178–182. – EDN HXMEJL.
4. Петров М.Н., Филиппов Я.С. Технологический суверенитет: основные принципы концепции национальной научно-технологической безопасности. Вопросы инновационной экономики. 2023, т. 13, № 3, с. 1185–1198. DOI: https://doi.org/10.18334/vinec.13.3.118646. – EDN AIMDAX.
5. Афанасьев А.А. Технологический суверенитет: к вопросу о сущности. Креативная экономика. 2022, № 10, с. 3691–3708. DOI: https://doi.org/10.18334/ce.16.10.116406.

6. Ерженин Р.В. Модификация стратегии развития информационной системы планирования в условиях политики обеспечения технологического суверенитета. XXI век: итоги прошлого и проблемы настоящего плюс. 2022, т. 11, № 3(59), с. 81–87. DOI: https://doi.org/10.46548/21vek-2022-1159-0034.
7. Константинов И.Б., Константинова Е.П. Технологический суверенитет как стратегия будущего развития российской экономики. Вестник Поволжского института управления. 2022, т. 22, № 5, с. 12–22. DOI: https://doi.org/10.22394/1682-2358-2022-5-12-22.
8. Кузнецов С.А., Куликов И.А., Фоминых А.А. Сравнение КИИ и методов категорирования КИИ в РФ и США. Актуальные научные исследования в современном мире. 2021, № 6-1(74), с. 63–68. – EDN EFWCLF.
9. Ожиганова М.И., Егорова А.О., Миронова А.О., Головин А.А. Автоматизация выбора мер по обеспечению безопасности объекта КИИ соответствующей категории значимости при составлении модели угроз. Энергетические установки и технологии. 2021, т. 7, № 2, с. 130–135. – EDN CWQOZN.
10. Голикова В.В., Кузнецов Б.В. Что день грядущий нам готовит: по кому ударят санкционные ограничения на поставки импортного оборудования? Журнал Новой экономической ассоциации. № 3(60), с. 187–196, 2023. DOI: https://doi.org/10.31737/22212264_2023_3_187-196. – EDN UXYKHJ.
11. Смирнов Дмитрий О. Функциональная безопасность и недоверенная электронная компонентная база. Безопасность информационных технологий, [S.l.], т. 29, № 2, с. 128–143, 2022. ISSN 2074-7136. DOI: http://dx.doi.org/10.26583/bit.2022.2.10. – EDN ITCJXN.
12. Белоусова Н.Н., Плис Н.И. Состояние дел с производством гражданской продукции крупного предприятия ОПК радиоэлектронной промышленности: проблемные вопросы, требующие решения. Экономические и социально-гуманитарные исследования. 2022, № 2(34), с. 6–16. DOI: https://doi.org/10.24151/2409-1073-2022-2-6-16. – EDN BMPCTJ.

REFERENCES:

[1] Sukharev O.S. Technological Independence of Russia: Methods of Provision. Russia: Society, Politics, History. 2023;(1(6)):24-39. DOI: https://doi.org/10.56654/ROPI-2023-1(6)-24-39 (in Russian).
[2] Zhurikov Roman N.; Shchukin Ilya S.; Yushkov Yaroslav N. Ensuring technological independence by creating the necessary reserves of the electronic component base as one of the elements of its power of attorney. IT Security (Russia), [S.l.], v. 30, no. 3, p. 1491–57, 2023. ISSN 2074-7136. DOI: http://dx.doi.org/10.26583/bit.2023.3.10. – EDN ZEGTRV.
[3] Musienko N.O., Lysov D.A., Medvedeva V.D., Kuzina V.V. Review of the decree of the president of the Russian Federation no. 166 dated 30.03.2022 "On measures to ensure the technological independence and security of the critical information infrastructure of the Russian Federation" in the context of creating an information security system for significant objects of critical information infrastructure. In the collection: Information security and personal data protection. Problems and ways to solve them. Collection of materials and reports of the XV interregional scientific and practical conference. Under the general editorship of O.M. Golembiovskaya. Bryansk. 2023, p. 178–182 (in Russian). – EDN HXMEJL.
[4] Petrov M.N., Filippov Ya.S. Technological sovereignty: basic principles of the concept of national scientific and technological security. Voprosy innovatsionnoy ekonomiki. 2023, v. 13, no. 3, p. 1185–1198. DOI: https://doi.org/10.18334/vinec.13.3.118646 (in Russian). – EDN AIMDAX.
[5] Afanasyev, A.A. (2022) Technological sovereignty: a question of essence. Kreativnaya ekonomika. 16(10), p. 3691–3708. DOI: https://doi.org/10.18334/ce.16.10.116406 (in Russian).
[6] Yerzhenin R.V. Modification of the strategy for the development of the information planning system in the context of the policy of ensuring technological sovereignty. XXI century: results of the past and problems of the present plus. 2022, v. 11, no. 3(59), p. 81–87. DOI: https://doi.org/10.46548/21vek-2022-1159-0034 (in Russian).
[7] Konstantinov I.B., Konstantinova E.P. Technological sovereignty as a strategy for the future development of the russian economy. Bulletin of the Volga Institute of Management. 2022, v. 22, no. 5, p. 12–22. DOI: https://doi.org/10.22394/1682-2358-2022-5-12-22 (in Russian).
[8] Kuznetsov S.A., Kulikov I.A., Fominykh A.A. Comparison of critical infrastructure and methods of categoring critical infrastructure in Russian Federation AND USA. Current scientific research in the modern world. 2021, no. 6-1(74), p. 63–68 (in Russian). – EDN EFWCLF.
[9] Ozhiganova M.I., Egorova A.O., Mironova A.O., Golovin A.A. Automation of the selection of measures to ensure the safety of the KII facility of the significance category in modeling the threat. Power plants and technologies. 2021, v.7, no. 2, p. 130–135 (in Russian). – EDN CWQOZN.
[10] Golikova V.V., Kuznetsov B.V. What waits us tomorrow: What branches will be hit by supplies' sanctions of technological equipment to Russia? Journal of the New Economic Association. No. 3(60), p. 187–196, 2023. DOI: https://doi.org/10.31737/22212264_2023_3_187-196 (in Russian). – EDN UXYKHJ.

[11] Smirnov Dmitry O. Functional Security and an Untrusted Electronic Component Base. IT Security (Russia), [S.l.], v. 29, no. 2, p. 128–143, 2022. ISSN 2074-7136. DOI: http://dx.doi.org/10.26583/bit.2022.2.10 (in Russian). – EDN ITCJXN.

[12] Belousova N.N., Plis N.I. State of affairs with civil products' manufacturing at the large enterprise of defense industry complex of radioelectronic industry: problematic issues requiring solution. Economic and Socio-Humanitarian Studies. 2022, no. 2 (34), p. 6–16. DOI: https://doi.org/10.24151/2409-1073-2022-2-6-16 (in Russian). – EDN BMPCTJ.

Поступила в редакцию – 20 сентября 2023 г. Окончательный вариант – 20 октября 2023 г.
Received – September 20, 2023. The final version – October 20, 2023.