ФЕДЕРАЛЬНОЕ СОБРАНИЕ РОССИЙСКОЙ ФЕДЕРАЦИИ
**КОМИТЕТ СОВЕТА ФЕДЕРАЦИИ
ПО ЭКОНОМИЧЕСКОЙ ПОЛИТИКЕ**

ул. Б.Дмитровка, д. 26, Москва, 103426

4 марта 2025 г. № 3.6-09/979@

РЕКОМЕНДАЦИИ
«круглого стола» на тему «О мерах по обеспечению технологической безопасности и безопасности критической информационной инфраструктуры на объектах топливно-энергетического комплекса»

28 января 2025 года Совет Федерации

Комитет Совета Федерации по экономической политике 28 января 2025 года провел «круглый стол» на тему «О мерах по обеспечению технологической безопасности и безопасности критической информационной инфраструктуры на объектах топливно-энергетического комплекса».

В мероприятии приняли участие сенаторы Российской Федерации, представители федеральных органов исполнительной власти, государственных органов власти субъектов Российской Федерации, государственных и коммерческих организаций.

ТЭК является стратегической основой экономики России, обеспечивая энергетическую независимость, стабильность социально-экономического развития и национальную безопасность. В условиях цифровой трансформации отрасли вопросы защиты её инфраструктуры от внутренних и внешних угроз приобретают первостепенное значение. Безопасность ТЭК — это не только вопрос бесперебойной подачи энергии, но и гарантия суверенитета России. Нарушение работы объектов комплекса может привести к техногенным катастрофам, экономическим потерям и социальной дестабилизации.

Цифровая трансформация ТЭК является одним из ключевых инструментов повышения эффективности отрасли. Технологии виртуальных поисковых и

разведочных работ, дистанционное зондирование земли и геоинформационные системы на основе 3D-моделирования активно используются для разведки различных видов ископаемых энергоресурсов. Перевод в цифровую среду бизнес-процессов позволяет существенно сократить трудозатраты и снизить временные издержки, повысить клиентоориентированность.

В целях обеспечения информационной безопасности ТЭК Президент Российской Федерации В.В. Путин в 2022 году подписал Указ «О мерах по обеспечению технологической независимости и безопасности критической информационной инфраструктуры Российской Федерации». Согласно документу, с 31 марта 2022 года запрещено приобретать иностранное программное обеспечение (далее – ПО), в том числе в составе программно-аппаратных комплексов (далее – ПАК), для объектов критической информационной инфраструктуры (далее – КИИ) без согласования с уполномоченным органом исполнительной власти. Запрет распространяется и на закупки услуг, необходимых для использования такого софта. С 1 января 2025 года операторы КИИ и стратегические предприятия должны полностью отказаться от средств защиты информации, разработанных в недружественных государствах.

В последние годы российские энергокомпании стали более активно использовать отечественные программные решения. С 2020 года по начало 2023 года доля российского ПО в закупках софта предприятиями сектора ресурсоснабжения выросла с 60% до 80%. Соответственно, доля западных решений стремительно сокращается.

Тренд обусловлен государственными мерами по достижению технологического суверенитета, а также стимулированием использования продукции российских программистов на фоне продолжающейся цифровой трансформации отрасли. В 2020 году Минцифры России актуализировало Методические рекомендации по цифровой трансформации государственных корпораций и компаний с государственным участием. Документ содержит рекомендации по разработке стратегий цифровой трансформации, перечень ключевых показателей эффективности (далее – КПЭ) и

Мунянов Данзан Дорджиевич
8-(495)692-61-12

расчётные методы к ним, рекомендации по модели финансирования стратегий и порядок государственного мониторинга разработки и реализации стратегий.

Правительством Российской Федерации сформированы финансовые инструменты государственной поддержки процессов цифровой трансформации в компаниях:

1) льготное кредитование компаний, реализующих проекты по цифровой трансформации и внедряющих ИТ-решения. Размер льготной ставки по кредиту: от 1 до 5 % (до 3% для аккредитованных ИТ-организаций; размер кредита для реализации проекта: минимальный – 5 млн рублей, максимальный – 5 млрд рублей; размер кредита для реализации программы (совокупности проектов): минимальный – 500 млн рублей, максимальный – 10 млрд рублей);

2) льготный лизинг на внедрение цифровых технологий и платформенных решений на основе программно-аппаратных комплексов. Максимальный срок лизингового договора составляет 5 лет; стоимость проекта не ограничена; аванс лизингополучателя по договору лизинга – от 0%; итоговая ставка по лизингу зависит от доли оборудования отечественного производства в объёме сделки. Максимальные преференции имеют проекты с долей отечественного оборудования от 70% и выше, в этом случае федеральным бюджетом финансируется до 80% объёма сделки. При использовании в рамках сделки менее 70% льготный лизинг предоставляется с привлечением средств федерального бюджета в объёме до 40% от объема сделки;

3) грантовая поддержка проектов по разработке и внедрению цифровых решений.

Тем не менее, по-прежнему, остаются ниши, в которых преобладают решения иностранных разработчиков, например - средства защиты от DDoS-атак высокой интенсивности (1Тб/с и выше); высокопроизводительные горизонтально масштабируемые средства защиты приложений от таргетированных атак; средства высокопроизводительной криптографии для защиты каналов связи и др.

Участниками мероприятия отмечено, что отдельные крупные проекты ТЭК реализуются на единых комплексных ПАК от иностранных компаний. В настоящее

Мунянов Данзан Дорджиевич
8-(495)692-61-12

время отечественные аналоги используемых ПАК отсутствуют. В связи с чем экономические потери федерального бюджета в случае остановки производственных процессов и досрочного перехода на доверенные ПАК будут существенно выше, нежели потери от возможного кибер-инцедента. Полная замена действующих ПАК на проектах при появлении доступных технических решений потребует остановки производства на срок до 12 месяцев.

Имеет место формирование устойчивой тенденции выявления намеренно заложенных «уязвимостей» и не декларированного функционала и возможностей (НДВ) в микросхемах зарубежного производства. Растёт уровень технологической сложности топологических решений и уменьшение технического процесса производства зарубежных микросхем и их подложек, что, в некоторых случая, делает невозможным их реверс-инжиниринг для установления областей чипа с аппаратными НДВ. Известная и реализуемая практика противодействия функционирования НДВ интеграцией наложенных средств – электронных модулей Радиоэлектронные аппаратуры (далее – РЭА) и Электротехнического оборудования (далее – ЭТО), в полной мере не обеспечивает требуемого уровня нивелирования потенциальных угроз в зарубежных микросхемах. При всех вышеописанных технологических рисках и опасности, отказ от использования зарубежных микросхем в ближайшие 10-15 лет по-прежнему невозможен в силу ряда широкого спектра объективных технологических и производственных причин. При всех имеющихся рисках и проблемах, сопутствующих применению зарубежных микросхем даже в проприетарных схемотехнических и топологических решениях РЭА/ЭТО необходим комплексный подход в реализации эффективного мониторинга и нивелирования возможности активации НДВ на аппаратном уровне, с декомпозиций вплоть до физических параметров управляющих сигналов в цепях РЭА/ЭТО.

В связи с вышеизложенным, участники «круглого стола» **рекомендуют:**

1. Правительству Российской Федерации

1) проработать вопрос дополнения Правил перехода субъектов критической информационной инфраструктуры Российской Федерации на преимущественное

Мунянов Данзан Дорджиевич
8-(495)692-61-12

применение доверенных программно-аппаратных комплексов на принадлежащих им значимых объектах критической информационной инфраструктуры Российской Федерации, утвержденные постановлением Правительства от 14.11.2023 г. № 1912 (далее – Правила), понятием «доверенная зона», включающим в себя комплекс программно-аппаратных средств обеспечения безопасности КИИ (антивирусное ПО, межсетевое экранирование, сканер уязвимостей и т.п.), построенный на доверенных отечественных решениях;

2) рассмотреть возможность дополнения Правил положениями, предусматривающими возможность установления в отношении отдельных крупных проектов ТЭК индивидуальных сроков замещения ПАК в случае, если критерии присвоения категории ОКИИ не относятся к политической (и) или оборонной сфере, а сам объект размещен внутри «доверенной зоны», исключающей возможность удаленного подключения из сети Интернет. При этом указанные индивидуальные сроки замещения должны допускать продление эксплуатации действующих и уже закупленных ПАК на объектах КИИ до окончания плановых сроков службы оборудования, но не более чем до 01.01.2040;

3) проработать возможность внесения изменений в действующее законодательства в части расширения понятия «Доверенный» на системы, элементы и РЭА, радиоэлектронной продукции (далее – РЭП), ЭТО, а также ПО;

4) проработать вопрос разработки нормативных правовых актов об унифицировании объектов профильного регулирования ФСБ России, ФСТЭК России и действующих федеральных законов в части понятия «Доверенный» РЭА, РЭП, ЭТО, ПАК, ПО критической инфраструктуры и КИИ.

2. Министерству промышленности и торговли Российской Федерации проработать вопрос внесения изменений в постановление Правительства Российской Федерации от 14.11.2023 г. № 1912 в части предоставления возможности субъектам КИИ использования на принадлежащих им значимых объектах КИИ программно-аппаратных комплексов (далее – ПАК), приобретенных до 1 сентября 2024 года и не являющихся доверенными, до окончания их срока полезной эксплуатации, при

Мунянов Данзан Дорджиевич
8-(495)692-61-12

условии исполнения требований законодательства Российской Федерации в сфере информационной безопасности, с последующем замещением таких ПАК на доверенные.

3. Министерству промышленности и торговли Российской Федерации совместно с Министерством цифрового развития, связи и массовых коммуникаций Российской Федерации проработать вопрос формирования и реализации финансовых мер государственной поддержки, направленных на стимулирование разработки и внедрения систем автоматизации производств (АСУП, АСУ ТП и пр.), построенных на базе открытых технологий и открытых архитектур, а также на снижение технологической зависимости от проприетарных решений.

4. Министерству цифрового развития, связи и массовых коммуникаций Российской Федерации совместно с Министерством промышленности и торговли Российской Федерации и иными заинтересованными федеральными органами исполнительной власти рассмотреть возможность внесения изменений в Порядок формирования и утверждения перечня особо значимых проектов, а также контроля и мониторинга их реализации (далее – Порядок) в части включения дополнительного критерия подбора проектов отраслевых решений/ПО (приложение № 9 к Порядку) – «Применение открытых технологий и открытой архитектуры».

Председатель комитета

ДОКУМЕНТ ПОДПИСАН
ЭЛЕКТРОННОЙ ПОДПИСЬЮ

Сертификат 37671DDD911EB5FF633A3BE512BEE99E
Владелец **Кутепов Андрей Викторович**
Действителен с 04.12.2024 по 27.02.2026

А.В. Кутепов

Мунянов Данзан Дорджиевич
8-(495)692-61-12