АППАРАТ СОВЕТА ФЕДЕРАЦИИ
ФЕДЕРАЛЬНОГО СОБРАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
**ПРАВОВОЕ УПРАВЛЕНИЕ**

ул. Б.Дмитровка, д. 26, Москва, 103426 Тел. (495) 692-69-74

23 ноября 2022 г. № 5.1-04/3088@

Председателю Комитета
Совета Федерации
по экономической политике

**А.В.КУТЕПОВУ**

**Уважаемый Андрей Викторович!**

В связи с Вашим письмом от 20 октября 2022 года № 3.6-14/4005@ направляется подготовленный в Правовом управлении Аппарата Совета Федерации информационный правовой материал, который может быть использован при подготовке к проведению заседания "круглого стола" на тему "О ходе реализации Указа Президента Российской Федерации от 30 марта 2022 года № 166 "О мерах по обеспечению технологической независимости и безопасности критической информационной инфраструктуры Российской Федерации" в части импортозамещения зарубежного программного обеспечения и оборудования".

Приложение: файл (11 л.).

Заместитель
Руководителя Аппарата
Совета Федерации —
начальник Правового
управления

ДОКУМЕНТ ПОДПИСАН
ЭЛЕКТРОННОЙ ПОДПИСЬЮ
Сертификат 00E711E918297C0E28F8C396702C2B3497
Владелец **Егорова Екатерина Юрьевна**
Действителен с 01.04.2022 по 24.06.2023

Е.Ю. ЕГОРОВА

Шебаршина Анастасия Романовна
8-495-697-83-54

АППАРАТ СОВЕТА ФЕДЕРАЦИИ
ФЕДЕРАЛЬНОГО СОБРАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
**ПРАВОВОЕ УПРАВЛЕНИЕ**

103426, Москва, Б.Дмитровка, 26 Тел. 692-69-74

**К вопросу об импортозамещении зарубежного программного обеспечения и оборудования в области обеспечения безопасности критической информационной инфраструктуры Российской Федерации**

Стратегия национальной безопасности Российской Федерации, утвержденная Указом Президента Российской Федерации от 2 июля 2021 года № 400 (далее – Стратегия), является базовым документом стратегического планирования, определяющим национальные интересы и стратегические национальные приоритеты Российской Федерации, цели и задачи государственной политики в области обеспечения национальной безопасности и устойчивого развития Российской Федерации на долгосрочную перспективу. В Стратегии, в частности, выделяются такие направления, как информационная безопасность и научно-технологическое развитие.

В части информационной безопасности Стратегией отмечается, что быстрое развитие информационно-коммуникационных технологий сопровождается повышением вероятности возникновения угроз безопасности граждан, общества и государства.

Достижение цели обеспечения информационной безопасности осуществляется путем реализации государственной политики, направленной на решение следующих задач, в частности:

совершенствование средств и методов обеспечения информационной безопасности на основе применения передовых технологий, включая технологии искусственного интеллекта и квантовые вычисления;

обеспечение приоритетного использования в информационной инфраструктуре Российской Федерации российских информационных технологий и оборудования, отвечающих требованиям информационной безопасности, в том числе при реализации национальных проектов (программ) и решении задач в области цифровизации экономики и государственного управления.

В условиях перехода мировой экономики на новую технологическую основу лидерство в развитии науки и технологий становится одним из ключевых факторов повышения конкурентоспособности и обеспечения национальной безопасности.

Достижение цели научно-технологического развития Российской Федерации осуществляется путем решения следующих задач, в частности:

выработка и реализация на федеральном, региональном, отраслевом и корпоративном уровнях согласованной политики, обеспечивающей переход российской экономики на новую технологическую основу;

создание условий и стимулов для повышения заинтересованности российского бизнеса в развитии научной, научно-технической и инновационной деятельности;

ускоренное внедрение в промышленное производство результатов научных исследований для обеспечения полного научно-производственного цикла в соответствии с приоритетами социально-экономического, научного и научно-технологического развития Российской Федерации;

совершенствование системы фундаментальных научных исследований как важнейшей составляющей устойчивого развития Российской Федерации;

модернизация и развитие научной, научно-технической и инновационной инфраструктуры;

привлечение к работе в России ученых мирового уровня и молодых талантливых исследователей, создание и развитие на территории Российской Федерации центров международного сотрудничества в области науки и технологий;

развитие системы отбора, подготовки и адресной поддержки молодых российских ученых и специалистов в области научной, научно-технической и инновационной деятельности;

обеспечение передачи знаний и технологий между оборонным и гражданским секторами экономики;

формирование внутреннего спроса на российскую наукоемкую и инновационную продукцию, в первую очередь со стороны государственных заказчиков, государственных компаний и компаний с государственным участием.

Федеральный закон от 26 июля 2017 года № 187-ФЗ "О безопасности критической информационной инфраструктуры Российской Федерации" (далее – Федеральный закон № 187-ФЗ) регулирует отношения в области обеспечения безопасности критической информационной инфраструктуры Российской Федерации в целях ее устойчивого функционирования при проведении в отношении ее компьютерных атак.

Безопасность критической информационной инфраструктуры представляет собой состояние защищенности критической информационной инфраструктуры, обеспечивающее ее устойчивое функционирование при проведении в отношении ее компьютерных атак. В

свою очередь, критическая информационная инфраструктура – это объекты критической информационной инфраструктуры, а также сети электросвязи, используемые для организации взаимодействия таких объектов. Под объектами критической информационной инфраструктуры понимаются информационные системы, информационно-телекоммуникационные сети, автоматизированные системы управления субъектов критической информационной инфраструктуры.

Особенности применения Федерального закона № 187-ФЗ к сетям связи общего пользования определяются Федеральным законом от 7 июля 2003 года № 126-ФЗ "О связи" и принимаемыми в соответствии с ним нормативными правовыми актами Российской Федерации.

Государственная система обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации представляет собой единый территориально распределенный комплекс, включающий силы и средства, предназначенные для обнаружения, предупреждения и ликвидации последствий компьютерных атак и реагирования на компьютерные инциденты. В целях статьи 5 Федерального закона № 187-ФЗ под информационными ресурсами Российской Федерации понимаются информационные системы, информационно-телекоммуникационные сети и автоматизированные системы управления, находящиеся на территории Российской Федерации, в дипломатических представительствах и (или) консульских учреждениях Российской Федерации.

Средствами, предназначенными для обнаружения, предупреждения и ликвидации последствий компьютерных атак и реагирования на компьютерные инциденты, являются технические, программные, программно-аппаратные и иные средства для обнаружения (в том числе для поиска признаков компьютерных атак в сетях электросвязи, используемых

для организации взаимодействия объектов критической информационной инфраструктуры), предупреждения, ликвидации последствий компьютерных атак и (или) обмена информацией, необходимой субъектам критической информационной инфраструктуры при обнаружении, предупреждении и (или) ликвидации последствий компьютерных атак, а также криптографические средства защиты такой информации.

Согласно Федеральному закону № 187-ФЗ федеральный орган исполнительной власти, уполномоченный в области обеспечения функционирования государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации[1], организует в установленном им порядке обмен информацией о компьютерных инцидентах между субъектами критической информационной инфраструктуры, а также между субъектами критической информационной инфраструктуры и уполномоченными органами иностранных государств, международными, международными неправительственными организациями и иностранными организациями, осуществляющими деятельность в области реагирования на компьютерные инциденты.

Министерство цифрового развития, связи и массовых коммуникаций Российской Федерации утверждает по согласованию с Федеральной службой безопасности Российской Федерации, порядок, технические условия установки и эксплуатации средств, предназначенных для поиска признаков компьютерных атак в сетях электросвязи, используемых для

[1] Указом Президента Российской Федерации от 22 декабря 2017 года № 620 "О совершенствовании государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации" функции возложены на Федеральную службу безопасности Российской Федерации

организации взаимодействия объектов критической информационной инфраструктуры[2].

В целях учета значимых объектов критической информационной инфраструктуры Федеральная служба по техническому и экспортному контролю (ФСТЭК России) ведет реестр значимых объектов критической информационной инфраструктуры в установленном им порядке[3].

Указом Президента Российской Федерации от 30 марта 2022 года № 166 "О мерах по обеспечению технологической независимости и безопасности критической информационной инфраструктуры Российской Федерации" (далее – Указ Президента Российской Федерации № 166) установлено, что:

с 31 марта 2022 года заказчики (за исключением организаций с муниципальным участием), осуществляющие закупки в соответствии с Федеральным законом от 18 июля 2011 года № 223-ФЗ "О закупках товаров, работ, услуг отдельными видами юридических лиц" (далее – заказчики), не могут осуществлять закупки иностранного программного обеспечения, в том числе в составе программно-аппаратных комплексов (далее – программное обеспечение), в целях его использования на принадлежащих им значимых объектах критической информационной инфраструктуры Российской Федерации, а также закупки услуг, необходимых для использования этого программного обеспечения на таких объектах, без согласования возможности осуществления закупок с федеральным органом исполнительной власти, уполномоченным Правительством Российской Федерации;

---

[2] Приказ Минкомсвязи России от 17 марта 2020 года № 114 "Об утверждении Порядка и Технических условий установки и эксплуатации средств, предназначенных для поиска признаков компьютерных атак в сетях электросвязи, используемых для организации взаимодействия объектов критической информационной инфраструктуры Российской Федерации"

[3] Приказ ФСТЭК России от 6 декабря 2017 года № 227 "Об утверждении Порядка ведения реестра значимых объектов критической информационной инфраструктуры Российской Федерации"

с 1 января 2025 года органам государственной власти, заказчикам запрещается использовать иностранное программное обеспечение на принадлежащих им значимых объектах критической информационной инфраструктуры.

В соответствии с Указом Президента Российской Федерации № 166 Правительство Российской Федерации постановлением от 22 августа 2022 года № 1478 утвердило:

требования к программному обеспечению, в том числе в составе программно-аппаратных комплексов, используемому органами государственной власти, заказчиками, осуществляющими закупки в соответствии с Федеральным законом "О закупках товаров, работ, услуг отдельными видами юридических лиц" (за исключением организаций с муниципальным участием), на принадлежащих им значимых объектах критической информационной инфраструктуры Российской Федерации;

Правила согласования закупок иностранного программного обеспечения, в том числе в составе программно-аппаратных комплексов, в целях его использования заказчиками, осуществляющими закупки в соответствии с Федеральным законом "О закупках товаров, работ, услуг отдельными видами юридических лиц" (за исключением организаций с муниципальным участием), на принадлежащих им значимых объектах критической информационной инфраструктуры Российской Федерации, а также закупок услуг, необходимых для использования этого программного обеспечения на таких объектах;

Правила перехода на преимущественное использование российского программного обеспечения, в том числе в составе программно-аппаратных комплексов, заказчиками, осуществляющими закупки в соответствии с Федеральным законом "О закупках товаров, работ, услуг отдельными видами юридических лиц" (за исключением организаций с муниципальным

участием), на принадлежащих им значимых объектах критической информационной инфраструктуры Российской Федерации.

Кроме того, Правительству Российской Федерации необходимо реализовать комплекс мероприятий, направленных на обеспечение преимущественного применения субъектами критической информационной инфраструктуры отечественных радиоэлектронной продукции и телекоммуникационного оборудования на принадлежащих им значимых объектах критической информационной инфраструктуры, в том числе:

определить сроки и порядок перехода субъектов критической информационной инфраструктуры на преимущественное применение доверенных программно-аппаратных комплексов на принадлежащих им значимых объектах критической информационной инфраструктуры;

обеспечить внесение в законодательство Российской Федерации изменений в соответствии с Указом Президента Российской Федерации № 166;

обеспечить создание и организацию деятельности научно-производственного объединения, специализирующегося на разработке, производстве, технической поддержке и сервисном обслуживании доверенных программно-аппаратных комплексов для критической информационной инфраструктуры;

организовать подготовку и переподготовку кадров в сфере разработки, производства, технической поддержки и сервисного обслуживания радиоэлектронной продукции и телекоммуникационного оборудования;

создать систему мониторинга и контроля в названной сфере.

Следует отметить, что Указом Президента Российской Федерации от 14 апреля 2022 года № 203 "О Межведомственной комиссии Совета Безопасности Российской Федерации по вопросам обеспечения

технологического суверенитета государства в сфере развития критической информационной инфраструктуры Российской Федерации" в целях выполнения возложенных на Совет Безопасности Российской Федерации задач по выработке мер, направленных на обеспечение безопасности критической информационной инфраструктуры Российской Федерации, а также по координации деятельности федеральных органов государственной власти, органов государственной власти субъектов Российской Федерации, других государственных органов, органов местного самоуправления и организаций (далее – органы и организации) при реализации мероприятий по обеспечению технологической независимости объектов критической информационной инфраструктуры, оснащению таких объектов отечественной радиоэлектронной продукцией, техническим оборудованием, программно-аппаратными комплексами, включая программное и информационное обеспечение, образована Межведомственная комиссия Совета Безопасности Российской Федерации по вопросам обеспечения технологического суверенитета государства в сфере развития критической информационной инфраструктуры Российской Федерации.

На указанную Комиссию возлагаются такие функции, как:

оценка уровня технологической независимости объектов критической информационной инфраструктуры от иностранных технологий в области создания и производства отечественной продукции, выработка предложений и рекомендаций федеральным органам исполнительной власти по импортозамещению в данной области и развитию критической информационной инфраструктуры;

анализ эффективности деятельности органов и организаций по выполнению решений Совета Безопасности, направленных на обеспечение технологического суверенитета государства в сфере

развития критической информационной инфраструктуры (далее - технологический суверенитет);

прогнозирование, выявление и оценка внутренних и внешних угроз национальной безопасности в следующих сферах: развитие информационных технологий, сетей электросвязи и информационно-телекоммуникационных сетей; развитие и поддержка производства отечественной продукции; развитие промышленности и оборонно-промышленного комплекса в части, касающейся обеспечения технологического суверенитета;

координация деятельности органов и организаций при решении оперативных, среднесрочных и долгосрочных задач по обеспечению национальной безопасности в области развития информационных технологий, производства средств связи, радиопромышленности и электронной промышленности, а также расширения международного сотрудничества в указанной области.

Стратегическая сессия об импортозамещении программного обеспечения в отраслях состоялась 13 сентября 2022 года, по итогам которой Правительством Российской Федерации приняты, в частности, следующие решения и даны поручения[4]:

Минцифры России надлежит обеспечить согласование с заинтересованными федеральными органами исполнительной власти и внесение в Правительство Российской Федерации проекта федерального закона "О внесении изменений в отдельные законодательные акты Российской Федерации" (устанавливающего требования по преимущественному использованию всеми субъектами критической

---

[4] Поручение Правительства Российской Федерации (о решениях по итогам стратегической сессии по вопросу "Презентация импортозамещенных решений, отобранных центрами компетенций для масштабирования в отраслях"), текст документа приведен в соответствии с публикацией на сайте http://government.ru по состоянию на 23 сентября 2022 года

информационной инфраструктуры отечественных программно-аппаратных комплексов, программного обеспечения, телекоммуникационного оборудования и радиоэлектронной продукции (с учетом их готовности к массовому внедрению) на принадлежащих им значимых инфраструктурных объектах, а также уточняющего полномочия отраслевых ведомств в части отнесения информационных систем к значимым объектам критической информационной инфраструктуры);

Минпромторгу России и Минцифры России необходимо представить в Правительство Российской Федерации предложения о механизмах разработки и внедрения российских PLM-систем в составе финансирования, выделяемого промышленным лидерам на разработки новой продукции.

Правовое управление
Аппарата Совета Федерации

Исполнители:
отдел гражданского права: А.Р.Шебаршина;
отдел административного, уголовного и процессуального права: Б.А.Ельцов