Ассоциация банков России
(Ассоциация «Россия»)

119180, Москва, ул. Большая Якиманка, д.23
www.asros.ru
asros@asros.ru
т. 8-(495)-785-29-90

от 15.06.2020 № 02-05/419

На № _____ от _____

Министру цифрового развития,
связи и массовых коммуникаций
Российской Федерации

М.И. Шадаеву

Пресненская наб., д.10, стр.2,
г. Москва, 123112

Уважаемый Максут Игоревич!

В Ассоциацию банков России обращаются кредитные организации в связи с публичным обсуждением проекта указа Президента Российской Федерации «О мерах по обеспечению информационной безопасности в экономической сфере при использовании программного обеспечения и оборудования на объектах критической информационной инфраструктуры» и проекта постановления Правительства Российской Федерации «Об утверждении требований к программному обеспечению и оборудованию, используемому на объектах критической информационной инфраструктуры и порядка перехода на преимущественное использование российского программного обеспечения и оборудования» (далее – Проекты).

Ассоциация банков России поддерживает общий курс на импортозамещение, которое позволяет стимулировать национальное производство, развивать отдельные сектора и отрасли экономики, а также в целом укрепляет независимость и безопасность страны. При этом члены Ассоциации просят при доработке Проектов учесть особенности функционирования кредитных организаций и специфику нормативного правового регулирования банковского сектора со стороны Банка России и иных регуляторов.

В настоящее время к кредитным организациям применяются одни из самых строгих требований в российской экономике к обеспечению бесперебойности деятельности и защите информации клиентов. Внедрение всех финтех-инноваций последних лет в банковском секторе (Единая биометрическая система, Система быстрых платежей и т.д.) сопровождается жесткими условиями со стороны регуляторов по обеспечению кибербезопасности. Безусловно такой подход сохранится и для будущих внедрений.

По мнению участников рынка, несмотря на направленность Проектов на повышение информационной безопасности критической информационной инфраструктуры (КИИ), реализация их в текущей редакции создаст риски масштабных перебоев функционирования объектов КИИ, так как на практике

требования Проектов по объективным причинам сложно выполнимы (а в отдельных случаях практически невыполнимы) в части предлагаемых сроков и возможности замещения многих видов иностранного программного обеспечения (ПО) и ИТ-оборудования. Такие риски возникают в том числе из-за следующих причин:

1. В Проектах не учитываются текущее состояние предложения на рынке ИТ, объективно достижимые пределы его увеличения в указанные сроки, степень зрелости некоторых участников рынка, а также конкурентоспособность их продукции в сравнении с мировыми аналогами. К сожалению, число областей с насыщенным предложением качественного отечественного ПО и оборудования относительно невелико. Формально аналогичные по классу российские и иностранные программные продукты зачастую отличаются по набору специализированного функционала, возможности интеграции и эргономичности, причем не в пользу российского ПО. Замена ПО на российское не должна приводить к снижению уровня надежности функционирования банковской системы.

Замещение иностранного ИТ-оборудования российским еще более осложнено в связи с отсутствием у отечественных производителей современных технологий производства радиоэлектроники и его элементно-компонентной базы. Так, кредитные организации активно используют иностранное ИТ-оборудование, аналоги которого отсутствуют у российских производителей.

2. Одновременная реализация в крайне сжатые сроки масштабных проектов по замещению иностранного ПО и ИТ-оборудования в большом числе компаний требует наличия у производителей достаточных мощностей и компетенций для удовлетворения спроса. В настоящее время, по оценке экспертов, рынок ПО и оборудования не готов для решения масштабной задачи форсированного одновременного перехода на отечественные аналоги в значительном количестве кредитных организаций. Производителям придется в условиях сжатых сроков осуществлять настройку и доработку ПО и оборудования под потребности кредитных организаций, что влечет за собой риски сбоев, ошибок и инцидентов кибербезопасности. При этом Проектами не предусмотрены механизмы прямого государственного воздействия и поддержки ИТ-производителей в целях ускоренного стимулирования развития отрасли и удовлетворения повышенного спроса.

3. Проекты требуют одномоментного замещения всего ПО и ИТ-оборудования, информации о котором нет в соответствующих реестрах. При этом под замену попадает даже российское ПО, не включенное в реестр, в том числе собственной разработки. Такой подход, по мнению ИТ-специалистов, считается крайне опасным и может повлечь серьезные нарушения бесперебойности функционирования информационных систем, особенно у кредитных организаций, обладающих сложными интегрированными ИТ-системами со сложными взаимосвязями и необходимостью поддерживать доступность всех сервисов в режиме «365/24/7». Кроме того, во многих случаях подобное замещение просто не имеет смысла, поскольку использование в кредитных организациях ПО собственной разработки полностью удовлетворяет бизнес-потребностям,

соответствует всем жестким требованиям в области информационной безопасности и позволяет предлагать клиентам продукты и услуги по наименьшей цене в кратчайшие сроки.

4. Сроки, установленные в Проектах, предполагают наличие у всех субъектов КИИ достаточных временных, трудовых и финансовых ресурсов для замещения ПО и оборудования абсолютно на всех объектах КИИ, то есть в составе всех автоматизированных систем, информационных систем и информационно-телекоммуникационных сетей. Не учитывается тяжелая экономическая ситуация, вызванная пандемией коронавирусной инфекции, увеличивающаяся финансовая нагрузка на банки, связанная с предоставлением помощи ряду клиентов, сложность ряда корпоративных информационных систем и жизненные циклы объектов КИИ. Отсутствуют меры государственной поддержки процессов перехода на отечественное ПО и оборудование (например, налоговые льготы, льготное кредитование и т.п.).

По приблизительным оценкам, кредитные организации должны будут разово потратить **более 700 млрд руб.** на процедуру замещения (с учетом сжатых сроков сумма может еще больше возрасти). Средние сроки замещения с учетом непрерывности деятельности и постоянной транзакционной нагрузкой кредитных организаций составят **не менее 3 лет** при наличии готовых образцов и **5-7 лет** с учетом процессов поиска, выбора, тестирования, доработки, бюджетирования, открытия проекта, заключения договора и прочих необходимых мероприятий.

Помимо этого, механизмы, заложенные в Проектах, негативным образом скажутся на развитии конкуренции на российском рынке ПО и оборудования, а также на стимулах для совершенствования продукции и создания новых образцов. Новые правила приведут к монопольному положению некоторых компаний, стагнации и отставанию отечественного производства ПО и ИТ-оборудования и, как следствие, вынужденной закупке субъектами КИИ некачественных продуктов по завышенным ценам.

В Проектах также не учитывается принятая в нормативных правовых актах категоризация объектов КИИ по категории значимости. Федеральный закон от 26.07.2017 № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации» устанавливает требования по информационной безопасности только для значимых объектов КИИ. В соответствии с Приказом ФСТЭК России от 30.07.2018 № 131 «Об утверждении требований по безопасности информации, устанавливающие уровни доверия к средствам технической защиты информации и средствам обеспечения безопасности информационных технологий» (далее – Приказ ФСТЭК России № 131) установлены дифференцированные требования в зависимости от категории значимости объекта КИИ. При этом даже для самого высокого уровня значимости (первого) требования по безопасности **вступают с 01.01.2028 года**, а для третьего уровня значимости новые требования по безопасности вообще не устанавливаются. В свою очередь, Проекты устанавливают требования **для всех объектов КИИ**, что приведет к существенным неоправданным издержкам и ряду упомянутых выше негативных последствий, включая сбои в работе ИТ-систем, у соответствующих субъектов КИИ.

Опасения также вызывает тот факт, что в условиях снижения доходов бизнеса и населения финансирование замещения ПО и оборудования в конечном итоге будет перенесено на потребителей услуг субъектов КИИ, что может выразиться в увеличении стоимости некоторых банковских продуктов и услуг.

Таким образом, исполнение требований Проектов в установленные жесткие сроки создает существенные риски для бесперебойной работы кредитных организаций и защиты информации их клиентов, а сами Проекты требуют существенной переработки с учетом приведенных выше аргументов. В этой связи Ассоциация банков России предлагает при доработке Проектов рассмотреть возможность внесения в них следующих поправок:

1. Перенести сроки вступления в силу требований Проектов на 4 года (на 01.01.2025 и 01.01.2026 соответственно).
2. Уточнить область применения Проектов, распространив их положения исключительно на значимые объекты КИИ, относящиеся к первой категории значимости.
3. Допустить применение ПО собственной разработки кредитных организаций, не включенное в соответствующий реестр.
4. Разработать меры государственной поддержки российских производителей ПО и оборудования, которые позволили бы им в необходимые сроки удовлетворить спрос на продукцию, а также активно внедрять инновации в производство.
5. Разработать и утвердить порядок рассмотрения и принятия решений уполномоченным государственным органом заявления кредитной организации о праве использования ПО собственной разработки, легализации ПО и оборудования иностранной разработки, для которых отсутствует российский аналог.

Представители Ассоциации банков России также выражают заинтересованность принять участие в мероприятиях по доработке Проектов.

С уважением,

И.о. Президента А.А. Войлуков

Жижанов Г.В.
8-499-678-30-13, zgv@asros.ru