Ассоциация банков России
(Ассоциация «Россия»)

ПРЕЗИДЕНТ

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

от 12.08.2022 № 02-05/1769

На №_____от_____

Заместителю Председателя
Банка России

Г.А. Зубареву

Уважаемый Герман Александрович!

В Ассоциацию банков России обращаются кредитные организации по вопросам обеспечения информационной безопасности и защиты данных клиентов в связи с опубликованием Указа Президента Российской Федерации от 01.05.2022 № 250 «О дополнительных мерах по обеспечению информационной безопасности Российской Федерации» (далее – Указ).

1. В соответствии с абзацем 1 пункта 1 Указа требования по информационной безопасности распространяются на все субъекты критической информационной инфраструктуры (КИИ) Российской Федерации и не учитывают критерий значимости объектов КИИ. Такой подход создает избыточное регулирование и дополнительную нагрузку в виде исполнения мер, не соотносимых с возможными рисками. Принимая во внимание положительный опыт регулирования безопасности КИИ, установленный профильным Законом № 187-ФЗ[1] и подзаконными актами (в частности,

[1] Федеральный закон от 26.07.2017 № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации».

Приказом № 239[2]), предлагается распространять требования Указа только в отношении значимых объектов КИИ, которые на праве собственности, аренды или ином законном основании принадлежат субъектам КИИ. Такая модель, согласно концепции риск-ориентированного регулирования, будет соответствовать принципам адресности и обеспечит безопасность всей системы КИИ.

2. В соответствии с подпунктом «а» пункта 1 Указа на заместителя руководителя субъекта КИИ требуется возложить полномочия по обеспечению информационной безопасности, в том числе по обнаружению, предупреждению и ликвидации последствий компьютерных атак и реагированию на компьютерные инциденты. Кредитные организации отмечают, что на практике будет невозможно найти кандидатуру, которая будет одновременно соответствовать требованиям Закона № 395-1[3], предъявляемым к заместителям руководителя в кредитных организациях в части опыта работы и квалификации, и требованиям в части компетенций по информационной безопасности.

В этой связи для кредитных организаций предлагается установить требование по возложению полномочия по обеспечению информационной безопасности не на заместителя руководителя, а на ответственное лицо с прямым подчинением руководителю (единоличному исполнительному органу). Такой подход будет соответствовать действующим требованиям Положения № 716-П[4].

3. Ряд членов Ассоциации предлагает для кредитных организаций, входящих в группу компаний, разрешить передавать право на осуществление мероприятий по обеспечению информационной безопасности в рамках этой группы компаний другой организации, имеющей общего собственника. Учитывая глубокую интеграцию ИТ-инфраструктуры в рамках группы

---

[2] Приказ ФСТЭК России от 25.12.2017 № 239 «Об утверждении Требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации».

[3] Федеральный закон от 02.12.1990 № 395-1 «О банках и банковской деятельности».

[4] Положение Банка России от 08.04.2020 № 716-П «О требованиях к системе управления операционным риском в кредитной организации и банковской группе».

компаний, комплексное обеспечение кибербезопасности компаний группы одной компетентной организацией положительно повлияет на общий уровень защищенности и позволит повысить надежность проводимых мероприятий.

4. Ряд членов Ассоциации выражает обеспокоенность порядком реагирования на компьютерные инциденты, указанным в подпункте «г» пункта 1 Указа, в соответствии с которым субъект КИИ может привлекать исключительно аккредитованные государственной системой обнаружения, предупреждения и ликвидации последствий компьютерных атак (ГосСОПКА) организации. Учитывая тот факт, что в рамках реагирования на инциденты кредитные организации, как субъекты КИИ, обязаны передавать информацию о них в ГосСОПКА, сохранится ли текущий рекомендованный Банком России и предусмотренный протоколом о взаимодействии Банка России с ФСБ России порядок предоставления данных о компьютерных инцидентах посредством АСОИ ФинЦЕРТ, и не потребуется ли кредитным организациям организовывать дублирующий канал для непосредственной передачи данных в ГосСОПКА?

5. В соответствии с подпунктом «д» пункта 1 Указа организации, являющиеся субъектами КИИ, должны обеспечивать должностным лицам федеральной службы безопасности беспрепятственный доступ (в том числе удаленный) к принадлежащим им или используемым ими информационным ресурсам, доступ к которым обеспечивается через Интернет, в целях осуществления мониторинга защищенности информационных ресурсов. Порядок проведения мониторинга в соответствии с подпунктом «в» пункта 5 Указа утверждается ФСБ России.

Кредитные организации отмечают, что в соответствии со статьей 26 Закона № 395-1 они обязаны гарантировать тайну об операциях, о счетах и вкладах своих клиентов и корреспондентов. Справки по операциям, счетам и вкладам физических и юридических лиц выдаются кредитной организацией руководителям (должностным лицам) федеральных государственных органов по соответствующим запросам.

В этой связи кредитные организации не вправе предоставлять доступ к информации, составляющей банковскую тайну, в ходе мониторинга защищенности информационных ресурсов. Будет ли информация, составляющая банковскую тайну, выведена за периметр такого мониторинга, и правомерен ли будет отказ кредитной организации в предоставлении должностным лицам федеральной службы безопасности доступа, в том числе удаленного, к такой информации?

Дополнительно предлагается исключить обязанность по выполнению требования о предоставлении доступа ФСБ России к **используемым** информационным ресурсам, так как кредитная организация, не являясь владельцем такого ресурса, не всегда сможет повлиять на обеспечение третьим лицам доступа к нему для осуществления мониторинга информационной безопасности.

Учитывая положительный опыт отстаивания интересов банковского сообщества в межведомственном взаимодействии и глубокое понимание специфики функционирования информационных систем организаций финансового сектора, кредитные организации просят Банк России принять участие в разработке параметров удаленного доступа и порядка мониторинга информационных систем, утверждаемого ФСБ России.

Кроме того, члены Ассоциации отмечают, что в последнее время участились случаи применения к кредитным организациям помимо профильных норм, разработанных Банком России, общих норм по обеспечению информационной безопасности, в частности, в области защиты объектов КИИ. При этом Банк России не всегда привлекается к обсуждению требований нового регулирования, что снижает его качество в части учета особенностей участников финансового рынка. В этой связи кредитные организации крайне заинтересованы в том, чтобы Банк России в обязательном порядке привлекался для согласования требований к информационной безопасности и порядка их реализации.

6. В соответствии с пунктом 6 Указа субъектам КИИ с 01.01.2025 запрещается использовать средства защиты информации (СЗИ), странами происхождения которых являются иностранные государства, совершающие в отношении Российской Федерации, российских юридических лиц и физических лиц недружественные действия, либо производителями которых являются организации, находящиеся под юрисдикцией таких иностранных государств, прямо или косвенно подконтрольные им либо аффилированные с ними.

В соответствии с пунктом 2.7.2 ГОСТ Р 50922-2006[5] под термином «средство защиты информации» понимается техническое, программное, программно-техническое средство, вещество и (или) материал, предназначенные или используемые для защиты информации. Таким образом, под общее определение СЗИ подпадает широкий спектр средств, в том числе, например, встроенные средства операционных систем или функции телекоммуникационного оборудования.

Вместе с тем профильным регулированием (Закон № 187-ФЗ и Приказ № 239) требования к СЗИ устанавливаются только в отношении значимых объектов КИИ с учетом их категорий, термин СЗИ определяется также исключительно в применении к значимым объектам КИИ. Такой подход является основой нормативно-правового регулирования объектов КИИ и доказывает свою эффективность при обеспечении безопасности всей системы КИИ Российской Федерации.

В настоящее время кредитные организации испытывают значительную нагрузку на подразделения информационной безопасности, связанную в том числе с высоким уровнем киберагрессии, и при этом объективно вынуждены поддерживать высокие темпы импортозамещения. Полная замена действующих СЗИ, а также отсутствие сопоставимых аналогов, может увеличить риски потери информации и вызывает беспокойство участников рынка, которые также заинтересованы в обеспечении и сохранении высокого

---

[5] Национальный стандарт Российской Федерации «Защита информации. Основные термины и определения».

уровня защиты информации о российских гражданах, организациях и их операциях.

Члены Ассоциации в целях определения перечня приоритетных к проработке задач в сфере импортозамещения заинтересованы в получении разъяснений Банка России о средствах кредитных организаций, включаемых в понятие СЗИ в понимании Указа. В частности, учитывая сформировавшуюся концепцию регулирования КИИ, предусматривающую установление особых требований к информационной безопасности именно в отношении **значимых** объектов КИИ, правомерно ли исполнять требования Указа только для СЗИ, применяемых на **значимых** объектах КИИ кредитных организаций?

Кроме того, принимая во внимание значимость вопросов импортозамещения для банковского сообщества, кредитные организации просят Банк России во взаимодействии с Минцифры России и Минпромторгом России содействовать обеспечению финансового рынка аналогами текущих СЗИ и/или определить план перехода на использование СЗИ, не связанного с недружественными государствами, по мере появления аналогов на финансовом рынке.

Просим Вас рассмотреть вопросы, замечания и предложения кредитных организаций в части исполнения требований Указа и инициировать подготовку разъяснений в целях повышения прозрачности регулирования информационной безопасности в финансовом секторе.

С уважением,

Г.И. Лунтовский

Жижанов Г.В., 8-499-678-30-13