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 18.08.2022г. № 02-05/8111

На №_____от_____

Заместителю
Председателя Правительства
Российской Федерации

Д.Н. Чернышенко

Краснопресненская наб., д. 2,
Москва, 103274

Уважаемый Дмитрий Николаевич!

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).

Указ принят в целях повышения устойчивости и безопасности функционирования информационных ресурсов Российской Федерации и распространяется на широкий перечень лиц, относящихся к субъектам критической инфраструктуры (КИИ), к которым, в том числе, относятся кредитные организации.

На текущий момент Законом № 187-ФЗ[1] и Приказом № 239[2] установлены требования к обеспечению информационной безопасности на объектах КИИ, доказавшие свою эффективность на практике. Безопасность обеспечивается за счет установления требований по обеспечению безопасности значимых объектов КИИ с учетом их категорий. Категоризация и отделение значимых объектов от

[1] Федеральный закон от 26.07.2017 № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации».
[2] Приказ ФСТЭК России от 25.12.2017 № 239 «Об утверждении Требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации».

иных служит целям адресного регулирования для обеспечения безопасности всей системы КИИ в соответствии с принципом риск-ориентированного подхода и является основой нормативно-правового регулирования объектов КИИ в Российской Федерации.

Реализация указанного подхода позволяет при установлении регулирования выделять среди широкого круга объектов КИИ те виды, которые оказывают непосредственное влияние на важные для государства процессы, а также не распространять новые требования на программное обеспечение и оборудование, не оказывающее влияния на КИИ, что позволяет рационально использовать текущие ресурсы в условиях их острого дефицита.

Вместе с тем положения Указа применяют более широкий подход к регулированию КИИ, чем сложившийся на практике. В результате при реализации требований Указа возникает правовая неопределенность в части того, какие требования к информационной безопасности следует применять к объектам КИИ, которым не присвоена ни одна из категорий значимости. Кроме того, кредитными организациями отмечается избыточность некоторых требований, которые, по их мнению, не окажут значительного влияния на общий уровень безопасности КИИ, приведут к дополнительной нагрузке на службы информационной безопасности и усугубит существующий кадровый дефицит.

В настоящее время кредитные организации, как и многие другие субъекты КИИ, испытывают существенную нагрузку на подразделения информационной безопасности, связанную в том числе с высоким уровнем киберагрессии, и объективно вынуждены поддерживать высокие темпы импортозамещения. При этом разработанные Банком России комплексные требования к информационной безопасности кредитных организаций, а также жесткий контроль и надзор за их соблюдением позволяют говорить о банковском секторе как об одной из самых защищенных отраслей среди всех субъектов КИИ.

Члены Ассоциации крайне заинтересованы в получении разъяснений относительно порядка применения Указа, в том числе о возможности распространения его требований только в отношении значимых объектов КИИ, которые на праве собственности, аренды или ином законном основании

принадлежат кредитным организациям. Аналогичный подход применяется в Указе Президента Российской Федерации № 166[3], который также направлен на обеспечение безопасности КИИ Российской Федерации.

Кроме того, принимая во внимание значимость вопросов импортозамещения для банковского сообщества, кредитные организации просят Вас инициировать совместную работу Минцифры России, Минпромторга России и Банка России по содействию обеспечению финансового рынка аналогами текущих средств защиты информации (СЗИ) и/или определить план перехода на использование СЗИ, не связанного с недружественными государствами, по мере появления аналогов на отечественном рынке.

Члены Ассоциации также заинтересованы в систематическом привлечении Банка России к согласованию требований к информационной безопасности субъектов КИИ и порядка их реализации в целях учета специфики функционирования информационных систем организаций финансового сектора и синхронизации норм регулирования с профильным банковским регулированием в сфере кибербезопасности. В частности, по вопросу разработки параметров удаленного доступа и порядка мониторинга информационных систем, утверждаемого ФСБ России в соответствии с подпунктом «в» пункта 5 Указа.

Направляем Вам замечания и предложения кредитных организаций к требованиям Указа (в приложении) и просим оказать содействие в подготовке разъяснений в целях повышения прозрачности регулирования информационной безопасности в финансовом секторе.

Приложение: на 5 л. в 1 экз.

С уважением,

Г.И. Лунтовский

Жижанов Г.В., 8-499-678-30-13

---

[3] Указ Президента Российской Федерации от 30.03.2022 № 166 «О мерах по обеспечению технологической независимости и безопасности критической информационной инфраструктуры Российской Федерации».

Приложение

Замечания и предложения к требованиям Указа Президента Российской Федерации от 01.05.2022 № 250 «О дополнительных мерах по обеспечению информационной безопасности Российской Федерации» (далее – Указ)

1. 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[1], предъявляемым к заместителям руководителя в кредитных организациях в части опыта работы и квалификации, и требованиям в части компетенций по информационной безопасности.

В настоящее время требования к лицу, ответственному за информационную безопасность в кредитной организации, установлены пунктом 7.7 Положения № 716-П[2]. Согласно данным требованиям кредитная организация в целях управления риском информационной безопасности определяет во внутренних документах **должностное лицо** (лицо, его замещающее), ответственное за функционирование системы обеспечения информационной безопасности (**с прямым подчинением лицу, осуществляющему функции единоличного исполнительного органа кредитной организации, или его заместителю**) и не участвующее в совершении операций, сделок, организации бухгалтерского и управленческого учета, обеспечении функционирования информационных систем.

В этой связи с целью учета профильной специфики кредитные организации предлагают установить требование по возложению полномочий по обеспечению

---

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

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

информационной безопасности не на заместителя руководителя, а на ответственное лицо с прямым подчинением руководителю (единоличному исполнительному органу).

2. В соответствии с подпунктом «в» пункта 1 Указа предусматривается, что руководитель субъекта КИИ вправе принимать в случае необходимости решения о привлечении организаций к осуществлению мероприятий по обеспечению информационной безопасности. При этом привлекаться могут исключительно организации, имеющие лицензии на осуществление деятельности по технической защите конфиденциальной информации.

Вместе с тем требования к информационной безопасности, в том числе планирование, разработка, совершенствование и осуществление внедрения мероприятий по обеспечению безопасности, устанавливаются в части 3 статьи 9 Закона № 187-ФЗ[3] только в отношении значимых объектов КИИ. Таким образом, установление требований к привлекаемой организации для обеспечения информационной безопасности на «не значимых» объектах КИИ, к которым регулированием не предъявлены специальные требования по информационной безопасности, нецелесообразно и приведет к увеличению расходов на привлечение контрагентов. В этой связи кредитные организации просят распространить данное требование Указа исключительно на значимые объекты КИИ.

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

---

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

3. 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.

Представленное в статье 5 Закона № 187-ФЗ определение понятия «информационные ресурсы» аналогично определению понятия «объект критической информационной инфраструктуры», указанному в пункте 7 статьи 2 данного закона.

Целью проведения вышеуказанного мониторинга является проверка защищенности ресурсов. При этом в случае распространения данных положений на объекты КИИ, которым не присвоена ни одна из категорий значимости, требование будет предусматривать проведение мониторинга защищенности информационных ресурсов, в отношении которых законодательством в сфере КИИ не предусматривается специальных требований к обеспечению информационной безопасности. В этой связи кредитные организации предлагают проводить мониторинг только значимых объектов КИИ.

Кредитные организации также 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 по предоставлению 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.

4. Согласно подпункту «е» пункта 1 Указа руководитель субъекта КИИ обязан обеспечивать незамедлительную реализацию организационных и технических мер, решения о необходимости осуществления которых принимаются ФСБ России и ФСТЭК России в пределах их компетенции и направляются на регулярной основе с учетом меняющихся угроз в информационной сфере.

Полномочия ФСБ России и ФСТЭК России в области обеспечения безопасности КИИ поименованы в Законе № 187-ФЗ и распространяются в отношении значимых объектов КИИ. В частности, ФСТЭК России вправе устанавливать требования по обеспечению безопасности значимых объектов КИИ и требования к созданию систем безопасности таких объектов и обеспечению их функционирования. Также в соответствии с частью 2 статьи 11 Закона № 187-ФЗ государственные органы и российские юридические лица, выполняющие функции по разработке, проведению или реализации государственной политики и (или) нормативно-правовому регулированию в установленной сфере деятельности, по согласованию с ФСТЭК России, могут устанавливать дополнительные требования по обеспечению безопасности значимых объектов КИИ, содержащие особенности функционирования таких объектов в установленной сфере деятельности.

В этой связи, принимая во внимание действующий риск-ориентированный подход в регулировании (Закон № 187-ФЗ), предлагается рассмотреть возможность распространения требований Указа исключительно на значимые объекты КИИ, принадлежащие кредитным организациям.

5. 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[4] 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[5]) требования к СЗИ устанавливаются только в отношении значимых объектов КИИ, термин СЗИ определяется также исключительно в применении к значимым объектам КИИ.

Кредитными организациями в рамках осуществления деятельности используется программное обеспечение различного назначения, многое из которого не оказывает влияние на работоспособность объектов КИИ и КИИ в целом. Реализация указанных требований на все объекты КИИ будет препятствовать эффективному сосредоточению ресурса участников банковского рынка на наиболее важных и нужных для КИИ объектах. При этом отсутствие данных требований для «не значимых» объектов КИИ, по мнению кредитных организаций, не создаст рисков устойчивости и безопасности КИИ.

---

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

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