**МИНИСТЕРСТВО
ЦИФРОВОГО РАЗВИТИЯ, СВЯЗИ
И МАССОВЫХ КОММУНИКАЦИЙ
РОССИЙСКОЙ ФЕДЕРАЦИИ**

Пресненская наб., д.10, стр.2, Москва, 123112
Справочная: +7 (495) 771-8000

26.09.2022 П25-1-05-200-59737
№

на от

Ассоциация банков России
119180, г. Москва,
ул. Большая Якиманка, д. 23

Министерство цифрового развития, связи и массовых коммуникаций Российской Федерации (далее – Министерство) в ответ на письмо Ассоциации банков России от 26.08.2022 № 02-05/811, поступившее из Аппарата Правительства Российской Федерации, по вопросу разъяснения положений Указа Президента Российской Федерации от 01.05.2022 № 250 «О дополнительных мерах по обеспечению информационной безопасности Российской Федерации» (далее – Указ) сообщает следующее.

В отношении предложения по возложению полномочий по обеспечению информационной безопасности на ответственное лицо (не на заместителя руководителя), находящееся под прямым подчинением руководителя. В соответствии с пунктом 1 действие Указа распространяется на федеральные органы исполнительной власти, высшие исполнительные органы государственной власти субъектов Российской Федерации, государственные фонды, государственные корпорации (компании) и иные организации, созданные на основании федеральных законов, стратегические предприятия, стратегические акционерные общества, а также на системообразующие организации российской экономики, в том числе не являющиеся субъектами критической информационной инфраструктуры Российской Федерации (далее – КИИ) и на юридических лиц, являющихся субъектами КИИ (далее – органы (организации).

Обращаем внимание, что согласно подпунктам «а» и «б» пункта 1 Указа руководителям органов (организаций) необходимо возложить на заместителя руководителя органа (организации) полномочия по обеспечению информационной безопасности органа (организации), в том числе по обнаружению, предупреждению и ликвидации последствий компьютерных атак и реагированию на компьютерные инциденты, а также необходимо создать в органе (организации) структурное подразделение, осуществляющее функции по обеспечению

информационной безопасности органа (организации), в том числе по обнаружению, предупреждению и ликвидации последствий компьютерных атак и реагированию на компьютерные инциденты, либо возложить данные функции на существующее структурное подразделение.

В соответствии с пунктом 11 Типового положения о заместителе руководителя органа (организации), ответственном за обеспечение информационной безопасности в органе (организации), утвержденного постановлением Правительства Российской Федерации от 15 июля 2022 г. № 1272 (далее – Положение), ответственный за обеспечение информационной безопасности в органе (организации), в том числе за обнаружение, предупреждение и ликвидацию последствий компьютерных атак, и реагирование на компьютерные инциденты (далее – ответственное лицо) осуществляет регулярный контроль текущего уровня (состояния) информационной безопасности в органе (организации), а также отвечает за реализацию мероприятий, направленных на поддержание и развитие уровня (состояния) информационной безопасности в органе (организации), в том числе с учетом появления новых угроз безопасности информации и современных способов и методов проведения компьютерных атак; осуществляет регулярное и своевременное информирование руководства органа (организации) о компьютерных инцидентах, текущем уровне (состоянии) информационной безопасности в органе (организации) и результатах практических учений по противодействию компьютерным атакам.

Таким образом, указанное предложение не может быть поддержано.

В то же время не поддерживается предложение по внесению изменений, направленных на установление требований к привлекаемой организации для обеспечения информационной безопасности. Так, в соответствии с подпунктом «в» пункта 1 Указа при принятии решения о привлечении организаций к осуществлению мероприятий по обеспечению информационной безопасности органа (организации), могут привлекаться исключительно организации, имеющие лицензии на осуществление деятельности по технической защите конфиденциальной информации.

Аналогичная позиция Министерства в отношении предложения по распространению требований Указа исключительно на значимые объекты КИИ, принадлежащие кредитным организациям, а также осуществлению мониторинга только значимых объектов КИИ.

При этом, порядок мониторинга информации, составляющей банковскую тайну, и способы и методы ее предоставления будут определены в соответствии с позицией, представленной Федеральной службой безопасности Российской Федерации (далее – ФСБ России), и доведены до всех субъектов КИИ.

Исходя из изложенного, предложения в части исключения обязанности по выполнению требования по предоставлению доступа ФСБ России к используемым информационным ресурсам Министерством не поддерживаются.

Не может быть поддержано предложение о внесении изменений в пункт 6 Указа в части отказа от использования средств защиты информации, 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, так как данные положения, прежде всего, направлены на обеспечение технологической независимости субъектов КИИ.

Одновременно отмечаем, что реализация требований Указа не вызвала затруднений у Банка ВТБ (ПАО), ОАО «Российский Сельскохозяйственный банк», ПАО «Промсвязьбанк», РОССИЙСКИЙ НАЦИОНАЛЬНЫЙ КОММЕРЧЕСКИЙ БАНК (ПАО), включенных в перечень ключевых органов (организаций), которым необходимо осуществить мероприятия по оценке уровня защищенности своих информационных систем с привлечением организаций, имеющих соответствующие лицензии ФСБ России и ФСТЭК России (распоряжение Правительства Российской Федерации от 22.06.2022 № 1661-р).

Обращаем ваше внимание, что, исходя из закрепленного пунктом 6.6 Положения о Министерстве цифрового развития, связи и массовых коммуникаций Российской Федерации, утвержденного постановлением Правительства Российской Федерации от 2 июня 2008 г. № 418, права «давать государственным органам, органам местного самоуправления, юридическим и физическим лицам разъяснения по вопросам, отнесенным к сфере ведения Министерства», настоящее письмо не содержит правовых норм или общих правил, конкретизирующих нормативные предписания, и не является нормативным правовым актом. Данное письмо носит информационно-разъяснительный характер по вопросам компетенции Министерства.

Директор Департамента
обеспечения кибербезопасности В.Н. Бенгин

Минцифры России
Документ подписан электронной подписью
СВЕДЕНИЯ О СЕРТИФИКАТЕ ЭП
Сертификат: 148122CD5AE762536F619E581F05E3A321BD7C
Владелец: Бенгин Владимир Николаевич
Действителен с 14-02-2022 до 14-05-2023