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 14.03.2024 № 02-05/248

На №_____от_____

Директору Департамента
информационной безопасности
Банка России

В.А. Уварову

Уважаемый Вадим Александрович!

Ассоциация банков России в дополнение к письму от 11.03.2024 № 02-05/238 направляет поступившие вопросы и предложения кредитных организаций по тематике обеспечения информационной безопасности и импортозамещения (в приложении).

Просим Вас рассмотреть поступившие вопросы и предложения кредитных организаций и направить ответы и комментарии к ним в адрес Ассоциации.

Приложение: на 5 л. в 1 экз.

И.о. Президента А.А. Войлуков

Жижанов Г.В., 8-499-678-30-13

Приложение

Вопросы и предложения кредитных организаций по тематике информационной безопасности

1. Согласно пункту 1.9 Положения № 762-П[1] перевод денежных средств осуществляется банками по распоряжениям плательщиков в электронном виде или на бумажных носителях. Согласно пункту 1.26 Положения № 762-П распоряжение плательщика на перевод денежных средств в электронном виде должно быть подписано электронной подписью, аналогом собственноручной подписи и (или) удостоверяется кодами, паролями и иными средствами, позволяющими подтвердить, что распоряжение составлено плательщиком или уполномоченным на это лицом. Требования к обеспечению защиты информации при осуществлении переводов денежных средств установлены Положениями № 683-П[2] и № 821-П[3]. Учитывая требования указанных нормативных правовых актов, кредитные организации просят сообщить:

- может ли банк использовать телекоммуникационный канал связи «электронная почта» для получения распоряжений клиента на перевод денежных средств в электронной форме, подписанных электронной подписью?
- применимы ли в случае получения распоряжения на перевод денежных средств в электронной форме с применением электронной почты меры по обеспечению защиты информации, указанные в Положениях № 683-П и № 821-П?

---

[1] Положение Банка России от 29.06.2021 № 762-П «О правилах осуществления перевода денежных средств».

[2] Положение Банка России от 17.04.2019 № 683-П «Об установлении обязательных для кредитных организаций требований к обеспечению защиты информации при осуществлении банковской деятельности в целях противодействия осуществлению переводов денежных средств без согласия клиента».

[3] Положение Банка России от 17.08.2023 № 821-П «О требованиях к обеспечению защиты информации при осуществлении переводов денежных средств и о порядке осуществления Банком России контроля за соблюдением требований к обеспечению защиты информации при осуществлении переводов денежных средств».

2. В соответствии с Методическими рекомендациями № 14-МР[4] возможным способом информирования ФСБ России о компьютерных инцидентах и компьютерных атаках, а также о результатах по реагированию и принятию мер по ликвидации последствий компьютерных инцидентов и атак является передача соответствующей информации в Банк России с использованием технической инфраструктуры Банка России – Автоматизированной системы обработки инцидентов ФинЦЕРТ Банка России (АСОИ ФинЦЕРТ) – с последующим направлением Банком России полученной информации в Национальный координационный центр по компьютерным инцидентам (НКЦКИ).

При этом согласно Методическим рекомендациям № 15-МР[5] в случае выявления компьютерных инцидентов и атак кредитная организация в целях уголовно-правовой оценки действий злоумышленников обращается с заявлением в уполномоченные органы (МВД России и ФСБ России) с использованием сервиса приема обращений граждан и организаций или очно в их территориальные подразделения.

Действующее законодательство, в частности Уголовно-процессуальный кодекс Российской Федерации, не обязывает лицо (независимо от того, является оно потерпевшим или свидетелем) обращаться в правоохранительные органы с заявлением о возбуждении уголовного дела по факту действий злоумышленников. Такое обращение всегда является правом лица.

В этой связи члены Ассоциации просят разъяснить, обязана ли кредитная организация, которой реализовано информирование регуляторов о компьютерных инцидентах и атаках с помощью АСОИ ФинЦЕРТ,

---

[4] Методические рекомендации Банка России от 26.10.2023 14-МР «По выполнению кредитными и некредитными финансовыми организациями мероприятий по обеспечению безопасности критической информационной инфраструктуры Российской Федерации в части информирования федерального органа исполнительной власти, уполномоченного в области обеспечения функционирования государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации, о компьютерных инцидентах, результатах мероприятий по реагированию на них и принятии мер по ликвидации последствий компьютерных атак».

[5] Методические рекомендации Банка России от 26.10.2023 № 15-МР «По взаимодействию кредитных организаций с МВД России и ФСБ России в целях принятия процессуальных решений при проведении компьютерных атак в отношении объектов критической информационной инфраструктуры».

дополнительно обращаться с заявлением об инцидентах в МВД России и ФСБ России или такое обращение является ее правом?

3. В соответствии со статьей 57.5-1 Закона № 86-ФЗ[6] кредитные организации обязаны обеспечить переход на преимущественное использование российского программного обеспечения, отечественных радиоэлектронной продукции и телекоммуникационного оборудования, в том числе в составе программно-аппаратных комплексов (ПАК), на принадлежащих им значимых объектах критической информационной инфраструктуры Российской Федерации (КИИ). Банк России согласовывает планы мероприятий по переходу на преимущественное использование российского программного обеспечения, отечественных радиоэлектронной продукции и телекоммуникационного оборудования, в том числе в составе ПАК (далее – План мероприятий), и заявки на закупку иностранных ИТ-решений.

Кредитные организации просят разъяснить следующие вопросы:

- требование по переходу на преимущественное использование отечественных решений распространяется исключительно на значимые объекты КИИ?
- для подтверждения проведенного категорирования объектов КИИ достаточно факта включения данных объектов в Реестр КИИ, подтвержденного уведомлением от ФСТЭК России?
- кредитные организации, которые не имеют в своей инфраструктуре значимые объекты КИИ, могут не согласовывать с Банком России Планы мероприятий и закупку иностранных ИТ-решений?
- кредитным организациям при осуществлении перехода необходимо руководствоваться сроками, установленными в Постановлении № 1912[7]?

---

[6] Федеральный закон от 10.07.2002 № 86-ФЗ «О Центральном банке Российской Федерации (Банке России)».

[7] Постановление Правительства Российской Федерации от 14.11.2023 № 1912 «О порядке перехода субъектов критической информационной инфраструктуры Российской Федерации на преимущественное применение доверенных программно-аппаратных комплексов на принадлежащих им значимых объектах критической информационной инфраструктуры Российской Федерации».

4. В соответствии с пунктом 21 Правил категорирования объектов КИИ[8] субъект КИИ не реже чем один раз в 5 лет, а также в случае изменения показателей критериев значимости объектов КИИ или их значений осуществляет пересмотр установленных категорий значимости или решений об отсутствии необходимости присвоения указанным объектам таких категорий. Согласно статье 57.5-1 Закона № 86-ФЗ Банк России осуществляет согласование Планов мероприятий кредитных организаций.

Кредитные организации просят сообщить, в какой срок в случае присвоения одному из объектов КИИ категории значимости необходимо разработать и согласовать с Банком России План мероприятий?

5. 25 июля 2024 года вступает в силу Закон № 369-ФЗ[9], который вносит существенные изменения в процедуры антифрода в кредитных организациях. Важным элементом системы противодействия мошенничеству становится сверка реквизитов операции с информацией, содержащейся в базе данных о случаях и попытках осуществления переводов денежных средств без добровольного согласия клиента (далее – АС «Фид-Антифрод»). Осуществление кредитной организацией перевода по содержащимся в АС «Фид-Антифрод» реквизитам без реализации механизма двухдневного периода «охлаждения» влечет за собой обязанность по возмещению клиенту суммы перевода.

В этой связи при проверке факта добросовестного исполнения кредитной организацией требований Закона № 369-ФЗ и вынесении решения о возмещении суммы перевода определяющее значение будет иметь время совершения операции по реквизитам, содержащимся в АС «Фид-Антифрод», по сравнению с временем информирования Банком России кредитных организаций о включении данного реквизита в базу данных.

---

[8] Утверждены Постановлением Правительства Российской Федерации от 08.02.2018 № 127 «Об утверждении Правил категорирования объектов критической информационной инфраструктуры Российской Федерации, а также перечня показателей критериев значимости объектов критической информационной инфраструктуры Российской Федерации и их значений».

[9] Федеральный закон от 24.07.2023 № 369-ФЗ «О внесении изменений в Федеральный закон «О национальной платежной системе».

В настоящее время показатель, который мог бы использоваться для такого сравнения, отсутствует. Содержащееся в записи каждого реквизита в АС «Фид-Антифрод» поле «date», в котором отображаются дата и время последней актуальной операции без согласия по данному реквизиту, не может использоваться для указанных целей. Информация о новом реквизите в АС «Фид-Антифрод» становится доступна кредитным организациям существенно позже значения, указанного в поле «date», так как требуется дополнительное время для внесения реквизита в базу данных, отправки информации в кредитные организации и ее загрузки в системы антифрода.

В этой связи члены Ассоциации предлагают рассмотреть возможность введения дополнительного поля для реквизитов в АС «Фид-Антифрод»: дата и время вступления в силу каждой записи о реквизите, которые должны отражать реальное время появления информации о данном реквизите у кредитных организаций. К операциям без согласия, совершенным ранее этой даты и времени, не должны применяться период «охлаждения» и, соответственно, обязанность по возмещению суммы перевода денежных средств.