ЦЕНТРАЛЬНЫЙ БАНК РОССИЙСКОЙ ФЕДЕРАЦИИ
(БАНК РОССИИ)

Методические рекомендации 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

26.10.2023 № 15-МР

Настоящие Методические рекомендации описывают действия кредитных организаций при выявлении компьютерных инцидентов, инцидентов защиты информации (далее – инциденты) на объектах критической информационной инфраструктуры (далее – КИИ) и взаимодействии с МВД России и ФСБ России в целях принятия процессуальных решений уполномоченными органами.

Перечень инцидентов, включающий критерии информирования и разработанный в целях реализации Федерального закона № 187-ФЗ[1], Положения Банка России № 683-П[2], Положения Банка России № 719-П[3], приведен в приложениях 11 и 18 к стандарту Банка России СТО БР БФБО-1.5-2023 «Безопасность финансовых (банковских) операций. Управление инцидентами, связанными с реализацией информационных угроз, и инцидентами операционной надежности. О формах и сроках взаимодействия Банка России с кредитными организациями, некредитными

[1] Пункт 1 части 2 статьи 9 Федерального закона от 26.07.2017 № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации».

[2] Абзац восьмой пункта 8 Положения 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] Абзац второй пункта 1.5 Положения Банка России от 04.06.2020 № 719-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».

финансовыми организациями и субъектами национальной платежной системы при выявлении инцидентов, связанных с реализацией информационных угроз, и инцидентов операционной надежности», принятому и введенному в действие приказом Банка России от 08.02.2023 № ОД-215 (далее – СТО БР БФБО-1.5-2023).

При выявлении инцидентов кредитная организация в соответствии с пунктом 1 части 2 статьи 9 Федерального закона № 187-ФЗ направляет в Банк России с использованием технической инфраструктуры Банка России уведомление, содержащее сведения о выявленном инциденте, по форме и в порядке, установленным СТО БР БФБО-1.5-2023, а также в Национальный координационный центр по компьютерным инцидентам (далее − НКЦКИ) по форме и в порядке, установленным приказом ФСБ России № 282[4], в соответствии с пунктом 3 Порядка, утвержденного приказом ФСБ России № 282[5].

В случае выявления инцидента, повлекшего неправомерную передачу (предоставление, распространение, доступ) персональных данных, кредитная организация в соответствии с частью 12 статьи 19 Федерального закона № 152-ФЗ[6] также информирует НКЦКИ[7] в порядке, установленном приказом ФСБ России № 77[8].

В ходе проведения технического анализа КИИ по факту выявленного инцидента кредитной организации рекомендуется обеспечить сохранение

---

[4] Приказ ФСБ России от 19.06.2019 № 282 «Об утверждении Порядка информирования ФСБ России о компьютерных инцидентах, реагирования на них, принятия мер по ликвидации последствий компьютерных атак, проведенных в отношении значимых объектов критической информационной инфраструктуры Российской Федерации».

[5] В случае если кредитной организацией ранее было принято решение направлять информацию об инцидентах в НКЦКИ посредством Автоматизированной системы обработки инцидентов ФинЦЕРТ Банка России, дополнительное информирование НКЦКИ о данных событиях не требуется.

[6] Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных».

[7] В случае если кредитной организацией ранее было принято решение направлять информацию об инцидентах в НКЦКИ посредством Автоматизированной системы обработки инцидентов ФинЦЕРТ Банка России, дополнительное информирование НКЦКИ в порядке, установленном указанным приказом ФСБ России, не требуется. Сведения передаются в Банк России по форме и в порядке, установленным СТО БР БФБО-1.5-2023.

[8] Приказ ФСБ России от 13.02.2023 № 77 «Об утверждении порядка взаимодействия операторов с государственной системой обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации, включая информирование ФСБ России о компьютерных инцидентах, повлекших неправомерную передачу (предоставление, распространение, доступ) персональных данных».

технических данных выявленного несанкционированного воздействия на КИИ, в том числе включающих в себя образы оперативной памяти, жестких дисков скомпрометированных объектов КИИ, информацию о сетевой активности с объектов КИИ.

Дополнительные рекомендации по применению организационных, технологических и технических подходов, связанных со сбором, обработкой, анализом и распространением (передачей) технических данных по выявленному инциденту, приведены в стандарте Банка России СТО БР ИББС-1.3-2016 «Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Сбор и анализ технических данных при реагировании на инциденты информационной безопасности при осуществлении переводов денежных средств», принятом и введенном в действие приказом Банка России от 30.11.2016 № ОД-4234.

По результатам реагирования на инциденты, вследствие которых возникли прямые и (или) непрямые потери, кредитная организация в соответствии с пунктом 7.6 Положения Банка России № 716-П[9] определяет суммы потерь в разрезе видов потерь согласно пункту 3.11 Положения Банка России № 716-П и пункту 4 приложения 5 к Положению Банка России № 716-П в целях установления суммы причиненного ущерба.

В случае выявления инцидентов в целях уголовно-правовой оценки действий злоумышленников кредитная организация обращается с заявлением в уполномоченные органы.

При подаче заявления в МВД России, помимо описания событий, связанных с несанкционированным переводом денежных средств со счетов организации, рекомендуется указать факт незаконного воздействия на КИИ и изменения компьютерной информации.

Обращение по факту выявления инцидентов подается очно в территориальное подразделение МВД России по месту нахождения юридического лица либо в исключительных случаях с использованием

---

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

сервиса приема обращений граждан и организаций, размещенного на официальном сайте МВД России[10] в информационно-телекоммуникационной сети «Интернет» (www.мвд.рф).

Помимо МВД России, кредитная организация обращается в ФСБ России с использованием сервиса приема обращений граждан и организаций, размещенного на официальном сайте ФСБ России в информационно-телекоммуникационной сети «Интернет» (fsb.ru), или очно в территориальные органы безопасности.

Настоящие Методические рекомендации согласованы с Генеральной прокуратурой Российской Федерации, МВД России и ФСБ России.

Заместитель Председателя
Банка России Г.А. Зубарев

[10] В открывшемся списке подразделений выбирается «БСТМ МВД России» для дальнейшего заполнения формы обращения.