ЦЕНТРАЛЬНЫЙ БАНК РОССИЙСКОЙ ФЕДЕРАЦИИ
(БАНК РОССИИ)

У К А З А Н И Е

«9» января 2024 г. № 6653-У

г. Москва

МИНИСТЕРСТВО ЮСТИЦИИ РОССИЙСКОЙ ФЕДЕРАЦИИ
ЗАРЕГИСТРИРОВАНО
Регистрационный № 78331
от "29" мая 2024 г.

О внесении изменений в Положение Банка России от 27 октября 2020 года № 738-П «О порядке обеспечения бесперебойности функционирования платежной системы Банка России»

На основании пункта 14 части 1 и части 9 статьи 20 Федерального закона от 27 июня 2011 года № 161-ФЗ «О национальной платежной системе»:

1. Внести в Положение Банка России от 27 октября 2020 года № 738-П «О порядке обеспечения бесперебойности функционирования платежной системы Банка России»[1] следующие изменения:

1.1. Абзац первый пункта 1.2 после слов «приостановления их оказания» дополнить словами «в соответствии с критериями, указанными в пункте 3.7 настоящего Положения».

---

[1] Зарегистрировано Минюстом России 21 декабря 2020 года, регистрационный № 61663, с изменениями, внесенными Указанием Банка России от 22 сентября 2022 года № 6254-У (зарегистрировано Минюстом России 29 сентября 2022 года, регистрационный № 70276).

1.2. В пункте 1.4:

в подпункте 1.4.2 слова «включая правовые риски» заменить словами «правовых рисков, рисков информационной безопасности»;

в подпункте 1.4.4 слово «организовывать» заменить словом «организовать».

1.3. Пункт 1.6 признать утратившим силу.

1.4. Абзац второй пункта 2.1 после слов «руководителями ПУРиН,» дополнить словами «структурным подразделением Банка России, ответственным за определение требований к защите информации в ПС, структурным подразделением Банка России, ответственным за организацию и осуществление контроля за соблюдением требований к защите информации в ПС,».

1.5. В пункте 2.2:

в абзацах девятом и десятом слова «работниками подразделения» заменить словами «работниками структурного подразделения Банка России»;

дополнить абзацами следующего содержания:

«работниками структурного подразделения Банка России, ответственного за определение требований к защите информации в ПС (далее – работники, определяющие требования к защите информации);

работниками структурного подразделения Банка России, ответственного за организацию и осуществление контроля за соблюдением требований к защите информации в ПС (далее – работники, осуществляющие контроль за соблюдением требований к защите информации).

Работники структурных подразделений Банка России, выполняющие функции, указанные в абзацах девятом, десятом, одиннадцатом, четырнадцатом и пятнадцатом настоящего пункта, назначаются организационно-распорядительными документами Банка России.»;

абзац третий подпункта 2.2.1 признать утратившим силу;

в подпункте 2.2.2:

в абзаце четвертом слова «согласовывает КИР» заменить словами «согласовывает ключевые индикаторы рисков (далее – КИР)»;

абзац пятый дополнить словами «, за исключением плана ОНиВД ОПКЦ внешней платежной системы»;

абзац шестой изложить в следующей редакции:

«принимает решения о применении мер реагирования, направленных на обеспечение непрерывности функционирования ПС в условиях инцидента (далее – ответные меры), приводящего к приостановлению оказания одной или нескольких УПИ более чем на два часа, в том числе о реализации соответствующей последовательности действий плана ОНиВД (далее – сценарий плана ОНиВД), а также принимает решения о реагировании на инциденты, воздействие которых требует перехода на оказание УПИ с использованием резервного комплекса программных и (или) технических средств;»;

в подпункте 2.2.4:

абзац двадцать первый изложить в следующей редакции:

«принимать решения о применении ответных мер, включая активацию сценариев плана ОНиВД в отношении инцидентов, приводящих к нарушению надлежащего оказания УПИ в ПС, за исключением решений, отнесенных к компетенции курирующего руководителя Банка России, руководителей ПУРиН;»;

в абзаце двадцать втором слова «Председателя Банка России или» исключить;

абзац восемнадцатый подпункта 2.2.5 изложить в следующей редакции:

«принимать решения о применении ответных мер, за исключением решений, отнесенных к компетенции курирующего руководителя Банка России, владельца бизнес-процесса»;

абзац восьмой подпункта 2.2.10 признать утратившим силу;

абзацы двадцать третий – двадцать седьмой подпункта 2.2.12 изложить в следующей редакции:

«организовать проведение оценки соответствия текущего уровня защиты информации объектов информационной инфраструктуры ОПКЦ внешней платежной системы, обеспечивающих функционирование ПС, уровням, определенным пунктом 6.7 раздела 6 национального стандарта Российской Федерации ГОСТ Р 57580.1-2017 «Безопасность финансовых (банковских) операций. Защита информации финансовых организаций. Базовый состав организационных и технических мер» (утвержден приказом Федерального агентства по техническому регулированию и метрологии от 8 августа 2017 года № 822-ст (М., ФГУП «Стандартинформ», 2017) и введен в действие 1 января 2018 года) (далее – ГОСТ Р 57580.1-2017), согласно методике оценки соответствия защиты информации, определенной в разделе 6 национального стандарта Российской Федерации ГОСТ Р 57580.2-2018 «Безопасность финансовых (банковских) операций. Защита информации финансовых организаций. Методика оценки соответствия» (утвержден приказом Федерального агентства по техническому регулированию и метрологии от 28 марта 2018 года № 156-ст (М., ФГУП «Стандартинформ», 2018) и введен в действие 1 сентября 2018 года) (далее – ГОСТ Р 57580.2-2018).

В части организации взаимодействия Банка России, ОПКЦ внешней платежной системы и участников ПС по обеспечению БФПС риск-координатор СБП внешней платежной системы должен контролировать выполнение мероприятий по информированию Банка России и участников ПС о приостановлении и восстановлении оказания УПИ.

В части осуществления контроля за соблюдением ОПКЦ внешней платежной системы порядка обеспечения БФПС риск-координатор СБП внешней платежной системы должен:

обеспечивать разработку и поддержание в актуальном состоянии документов ОПКЦ внешней платежной системы, определяющих деятельность ОПКЦ внешней платежной системы по обеспечению БФПС в части СБП,

соответствующих требованиям настоящего Положения по обеспечению БФПС;

направлять владельцу бизнес-процесса на рассмотрение документы, определяющие деятельность ОПКЦ внешней платежной системы по обеспечению БФПС в части СБП, и заключение о соответствии;»;

дополнить абзацем следующего содержания:

«контролировать соблюдение требований документов, определяющих деятельность ОПКЦ внешней платежной системы по обеспечению БФПС в части СБП, работниками ПУРиН внешней платежной системы.»;

дополнить подпунктами 2.2.13 и 2.2.14 следующего содержания:

«2.2.13. Работники, определяющие требования к защите информации, должны:

проводить мониторинг уровня риска информационной безопасности в ПС на основе КИР 6, КИР 7, КИР 8 и КИР 9, определенных в приложении 2 к настоящему Положению;

предоставлять риск-координаторам бизнес-процесса результаты мониторинга уровня риска информационной безопасности в ПС в части КИР 6, КИР 7, КИР 8 и КИР 9 для включения в ежегодный отчет об управлении рисками в ПС;

разрабатывать и предоставлять риск-координаторам бизнес-процесса сценарии плана ОНиВД в отношении инцидентов защиты информации в ПС.

2.2.14. Работники, осуществляющие контроль за соблюдением требований к защите информации, должны:

организовать контроль за соблюдением требований к защите информации в ПС;

организовать проведение оценки соответствия текущего уровня защиты информации объектов информационной инфраструктуры Банка России, обеспечивающих функционирование ПС, уровням, определенным пунктом 6.7 раздела 6 ГОСТ Р 57580.1-2017, согласно методике оценки соответствия защиты информации, определенной в разделе 6 ГОСТ Р 57580.2-2018;

проводить мониторинг уровня риска информационной безопасности в ПС на основе КИР 10, КИР 11, определенных в приложении 2 к настоящему Положению;

предоставлять риск-координаторам бизнес-процесса результаты мониторинга уровня риска информационной безопасности в ПС в части КИР 10 и КИР 11 для включения в ежегодный отчет об управлении рисками в ПС;

разрабатывать и предоставлять риск-координаторам бизнес-процесса сценарии плана ОНиВД в отношении инцидентов защиты информации в ПС в части КИР 10 и КИР 11;

организовывать применение в отношении инцидентов защиты информации в ПС в части КИР 10 и КИР 11, реализовавшихся при выполнении бизнес-процесса, ответных мер;

информировать структурное подразделение Банка России, ответственное за определение требований к защите информации в ПС, и риск-координаторов бизнес-процесса о выявленных инцидентах защиты информации в ПС в случае, если нарушения пороговых значений КИР 10 и КИР 11 приводят к инцидентам защиты информации в ПС.».

1.6. В пункте 3.2:

абзац первый подпункта 3.2.1 после слова «осуществляться» дополнить словами «не реже одного раза в год»;

в подпункте 3.2.3.1:

в абзаце втором слова «хотя бы» заменить словом «ни»;

абзацы четвертый и пятый изложить в следующей редакции:

«доля недополученных распоряжений в СБП превысила 10 процентов от значения суточной медианы распоряжений, исполненных с использованием СБП за предыдущий календарный месяц;

доля распоряжений, исполненных с использованием СБП более чем за тридцать секунд, до момента восстановления надлежащего оказания УПИ

превысила 10 процентов от значения суточной медианы распоряжений, исполненных с использованием СБП за предыдущий календарный месяц.»;

в подпункте 3.2.3.2:

в абзаце втором слова «хотя бы» заменить словом «ни»;

абзацы четвертый и пятый изложить в следующей редакции:

«доля недополученных распоряжений в СБП превысила 5 процентов от значения суточной медианы распоряжений, исполненных с использованием СБП за предыдущий календарный месяц;

доля распоряжений, исполненных с использованием СБП более чем за тридцать секунд, до момента восстановления надлежащего оказания УПИ превысила 5 процентов от значения суточной медианы распоряжений, исполненных с использованием СБП за предыдущий календарный месяц.»;

в подпункте 3.2.3.3:

в абзаце втором слова «хотя бы» заменить словом «ни»;

абзацы четвертый и пятый изложить в следующей редакции:

«доля недополученных распоряжений в СБП превысила 1 процент от значения суточной медианы распоряжений, исполненных с использованием СБП за предыдущий календарный месяц;

доля распоряжений, исполненных с использованием СБП более чем за тридцать секунд, до момента восстановления надлежащего оказания УПИ превысила 1 процент от значения суточной медианы распоряжений, исполненных с использованием СБП за предыдущий календарный месяц.»;

в подпункте 3.2.3.4:

в абзаце втором слова «хотя бы» заменить словом «ни»;

абзацы четвертый и пятый изложить в следующей редакции:

«доля недополученных распоряжений в СБП превысила 0,5 процента от значения суточной медианы распоряжений, исполненных с использованием СБП за предыдущий календарный месяц;

доля распоряжений, исполненных с использованием СБП более чем за тридцать секунд, до момента восстановления надлежащего оказания УПИ

превысила 0,5 процента от значения суточной медианы распоряжений, исполненных с использованием СБП за предыдущий календарный месяц.»;

абзацы четвертый и пятый подпункта 3.2.3.5 изложить в следующей редакции:

«доля недополученных распоряжений в СБП превысила 0,1 процента от значения суточной медианы распоряжений, исполненных с использованием СБП за предыдущий календарный месяц;

доля распоряжений, исполненных с использованием СБП более чем за тридцать секунд, до момента восстановления надлежащего оказания УПИ превысила 0,1 процента от значения суточной медианы распоряжений, исполненных с использованием СБП за предыдущий календарный месяц.»;

дополнить подпунктами 3.2.3.6 и 3.2.3.7 следующего содержания:

«3.2.3.6. Расчет недополученных распоряжений в СБП должен осуществляться ОПКЦ внешней платежной системы по формуле:

$K = \sum_{j=1}^{M}(P_j - C_j)$,

где:

P_j – количество распоряжений, ожидаемых для исполнения в СБП в j-й минуте. Рассчитывается на основании средних значений в аналогичном j-й минуте периоде времени за последний месяц;

C_j – количество исполненных распоряжений в СБП в j-й минуте;

M – продолжительность негативных (неблагоприятных) последствий инцидента или оценка продолжительности воздействия риска, в минутах.

3.2.3.7. Шкала оценки воздействия риска, предусмотренная в подпункте 3.2.3 настоящего пункта, также применяется в целях оценки негативных (неблагоприятных) последствий инцидента.»;

абзац третий подпункта 3.2.6 изложить в следующей редакции:

«план ОНиВД должен состоять из сценариев, каждый из которых регламентирует деятельность ПУРиН, подразделений Банка России, обеспечивающих функционирование ПС, или подразделения, руководителем

которого является владелец бизнес-процесса, в пределах их компетенции при обеспечении надлежащего оказания УПИ.»;

подпункты 3.2.7–3.2.9 изложить в следующей редакции:

«3.2.7. Самооценка должна проводиться в сроки, установленные организационно-распорядительным документом Банка России (далее – плановая самооценка), или по решению владельца бизнес-процесса (далее – внеплановая самооценка).

3.2.8. Внеплановая полная самооценка должна проводиться в отношении всех значимых рисков при внесении изменений в бизнес-процесс по решению владельца бизнес-процесса и должна быть завершена не позднее истечения 6 месяцев со дня принятия указанного решения.

3.2.9. Внеплановая частичная самооценка отдельных значимых рисков (отдельного значимого риска) должна проводиться по решению владельца бизнес-процесса и должна быть завершена не позднее истечения 4 месяцев со дня:

возникновения события, реализация которого привела к приостановлению (прекращению) оказания УПИ и описание которого в профиле рисков не предусмотрено либо негативные последствия от реализации которого превышают негативные последствия, предусмотренные для этого инцидента в профиле рисков;

установления по результатам проводимого мониторинга уровней значимых рисков факта превышения текущими значениями КИР пороговых значений КИР, указанных в приложении 2 к настоящему Положению; выявления значимого риска в ПС, для которого уровень присущего риска до применения способов управления рисками в ПС может превысить или превысил уровень допустимого риска.»;

в абзаце первом подпункта 3.2.10 слово «самооценки» заменить словами «плановой самооценки, внеплановой полной самооценки и внеплановой частичной самооценки отдельных значимых рисков (отдельного значимого риска)».

1.7. Пункт 3.3 дополнить подпунктом 3.3.4 следующего содержания:

«3.3.4. В целях мониторинга уровня риска информационной безопасности в ПС должны быть предусмотрены следующие дополнительные мероприятия:

оценка соответствия текущего уровня защиты информации объектов информационной инфраструктуры Банка России, обеспечивающих функционирование ПС, уровням, определенным пунктом 6.7 раздела 6 ГОСТ Р 57580.1-2017, согласно методике оценки соответствия защиты информации, определенной в разделе 6 ГОСТ Р 57580.2-2018;

оценка соответствия текущего уровня защиты информации объектов информационной инфраструктуры ОПКЦ внешней платежной системы, обеспечивающих функционирование ПС, уровням, определенным пунктом 6.7 раздела 6 ГОСТ Р 57580.1-2017, согласно методике оценки соответствия защиты информации, определенной в разделе 6 ГОСТ Р 57580.2-2018;

оценка выполнения требований к защите информации, обязательных для ОПКЦ внешней платежной системы в соответствии с Положением Банка России от 25 июля 2022 года № 802-П «О требованиях к защите информации в платежной системе Банка России» (зарегистрировано Минюстом России 25 ноября 2022 года, регистрационный № 71124) (далее – Положение Банка России № 802-П);

оценка выполнения требований, обязательных для работников структурных подразделений Банка России.».

1.8. В пункте 3.4:

абзац седьмой изложить в следующей редакции:

«определение требований для участников ПС, являющихся кредитными организациями, в части управления риском информационной безопасности участника ПС;»;

дополнить абзацами следующего содержания:

«определение требований к защите информации ОПКЦ внешней платежной системы в соответствии с Положением Банка России № 802-П;

определение требований к защите информации, обязательных для работников структурных подразделений Банка России.

В целях управления значимыми рисками могут применяться дополнительные меры реагирования при условии, что их применение обеспечивает снижение уровня воздействия от реализации значимого риска или снижение вероятности реализации значимого риска.».

1.9. Главу 3 дополнить пунктами 3.6–3.8 следующего содержания:

«3.6. В случае если действующая СУР не обеспечила три и более раза в течение календарного года возможность восстановления оказания УПИ в сроки, определенные в пункте 1.2 настоящего Положения (при приостановлении их оказания), в СУР должны быть внесены изменения.

3.7. Критериями отнесения риск-событий, реализовавшихся при оказании УПИ, к риск-событиям приостановления оказания УПИ являются:

в части сервиса срочного перевода и (или) сервиса несрочного перевода – непоступление в операционный и платежный клиринговый центр ПС, функции которого выполняет Банк России, в течение периода времени, превышающего 15 минут, ни одного распоряжения, направленного участником ПС для исполнения с использованием сервиса срочного перевода и (или) сервиса несрочного перевода в рамках операционного дня, в котором предоставлялись сервис срочного перевода и (или) сервис несрочного перевода в соответствии с графиком функционирования ПС с учетом периодов и (или) сеансов;

в части СБП – превышение доли недополученных распоряжений в СБП 0,5 процента от значения суточной медианы распоряжений, исполненных с использованием СБП за предыдущий календарный месяц.

3.8. Приостановление оказания УПИ в связи с проведением технологических и (или) регламентных работ, предусмотренных организационно-распорядительными документами Банка России, не относится к событиям приостановления оказания УПИ.».

1.10. Абзац первый пункта 4.2 изложить в следующей редакции:

«4.2. Выявление сведений об инцидентах должно проводиться на основании информации о нарушении надлежащего оказания УПИ, полученной от работников ПУРиН, работников ПУРиН внешней платежной системы и работников структурных подразделений Банка России, а также сведений, направляемых ОПКЦ внешней платежной системы в Банк России в соответствии с пунктом 1.5 Положения Банка России от 17 августа 2023 года № 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» (зарегистрировано Минюстом России 6 декабря 2023 года, регистрационный № 76286).».

1.11. В пункте 4.3:

абзацы четвертый и пятый изложить в следующей редакции:

«наименование одного или нескольких бизнес-процессов Банка России, в ходе которых произошел инцидент;

наименование одного или нескольких бизнес-процессов Банка России, на которые инцидент оказал влияние;»;

абзац десятый изложить в следующей редакции:

«мероприятия по устранению неблагоприятных последствий инцидента с указанием планируемой и фактической продолжительности проведения данных мероприятий;»;

дополнить абзацами следующего содержания:

«ПУРиН, ПУРиН внешней платежной системы, подразделения Банка России, обеспечивающие функционирование ПС, осуществляют хранение сведений об инцидентах в специализированной автоматизированной системе не менее 5 лет с даты получения указанных сведений.

Регистрация инцидентов защиты информации ОПКЦ внешней платежной системы должна дополнительно предусматривать фиксацию

реализованных компьютерных атак, фактов (индикаторов) компрометации объектов информационной инфраструктуры ОПКЦ внешней платежной системы, а также проведенной претензионной работы с учетом мер, определенных подпунктом 7.4.2 пункта 7.4 раздела 7 национального стандарта Российской Федерации ГОСТ Р 57580.4-2022 «Безопасность финансовых (банковских) операций. Обеспечение операционной надежности. Базовый состав организационных и технических мер» (утвержден приказом Федерального агентства по техническому регулированию и метрологии от 22 декабря 2022 года № 1549-ст (М., ФГБУ «Институт стандартизации», 2023) и введен в действие 1 февраля 2023 года) (далее – ГОСТ Р 57580.4-2022) и подпунктом 8.3.2.4 пункта 8.3 раздела 8 национального стандарта Российской Федерации ГОСТ Р 57580.3-2022 «Безопасность финансовых (банковских) операций. Управление риском реализации информационных угроз и обеспечение операционной надежности. Общие положения» (утвержден приказом Федерального агентства по техническому регулированию и метрологии от 22 декабря 2022 года № 1548-ст (М., ФГБУ «РСТ», 2023) и введен в действие 1 февраля 2023 года) (далее – ГОСТ Р 57580.3-2022).

ОПКЦ внешней платежной системы устанавливает во внутренних документах состав сведений для регистрации инцидентов защиты информации с учетом сведений об инцидентах защиты информации, направляемых ОПКЦ внешней платежной системы в Банк России.».

1.12. Абзац первый пункта 4.4 изложить в следующей редакции:

«4.4. Оценка влияния на БФПС каждого инцидента должна проводиться в срок не позднее окончания рабочего дня, следующего за днем возникновения (выявления) инцидента, а также в срок не позднее окончания рабочего дня, следующего за днем устранения последствий инцидента (восстановления надлежащего оказания УПИ).».

1.13. Пункт 4.6 дополнить абзацами следующего содержания:

«Применение ответных мер в отношении инцидентов защиты информации ОПКЦ внешней платежной системы должно осуществляться с учетом мер, определенных подпунктами 7.4.3 и 7.4.4 пункта 7.4 раздела 7 ГОСТ Р 57580.4-2022.

Оценка влияния на БФПС инцидентов защиты информации ОПКЦ внешней платежной системы должна включать в себя проведение анализа причин и последствий реализации инцидентов защиты информации.».

1.14. В подпункте 5.2.2 пункта 5.2:

абзац первый после слова «инцидентах» дополнить словами «(за исключением инцидентов защиты информации)»;

дополнить абзацем следующего содержания:

«Взаимодействие Банка России и ОПКЦ внешней платежной системы в части обмена информацией об инцидентах защиты информации ОПКЦ внешней платежной системы осуществляется с использованием технической инфраструктуры (автоматизированной системы) Банка России или резервного способа взаимодействия (при технической невозможности использования технической инфраструктуры (автоматизированной системы) Банка России), информация о которых размещается на официальном сайте.».

1.15. Абзац второй пункта 7.1 изложить в следующей редакции:

«В соответствии с решением Совета директоров Банка России (протокол заседания Совета директоров Банка России от 22 декабря 2023 года № ПСД-49) пункты 3.3 и 4.3 настоящего Положения и приложение 2 к настоящему Положению (за исключением подпункта 2.3 пункта 2 приложения 2 к настоящему Положению) вступают в силу с 1 октября 2024 года, пункты 4.4 и 4.5 настоящего Положения и подпункт 2.3 пункта 2 приложения 2 к настоящему Положению вступают в силу с 1 октября 2026 года.».

1.16. В приложении 2:

в пункте 2:

дополнить абзацами следующего содержания:

«индикатор эффективности противодействия информационным угрозам в ПС (КИР 6);

индикатор несанкционированных операций в СБП (КИР 7);

индикатор уровня соответствия защиты информации объектов информационной инфраструктуры Банка России, обеспечивающих функционирование ПС (КИР 8);

индикатор уровня соответствия защиты информации объектов информационной инфраструктуры ОПКЦ внешней платежной системы (КИР 9);

индикатор эффективности применяемых в ПС мер технологического контроля поступающих электронных сообщений (КИР 10);

индикатор качества управления уязвимостями в ПС (КИР 11).»;

в подпункте 2.1:

абзац первый изложить в следующей редакции:

«2.1. КИР 1 должен рассчитываться по каждому из инцидентов, повлекших приостановление оказания УПИ, как период времени с момента возникновения инцидента, приведшего к приостановлению оказания УПИ в результате первого из возникших инцидентов, и до момента восстановления оказания всех УПИ.»;

в абзаце четвертом слова «устранения последствий последнего инцидента» заменить словами «восстановления оказания УПИ»;

абзац первый подпункта 2.2 изложить в следующей редакции:

«2.2. КИР 2 должен рассчитываться по каждому из инцидентов, повлекших приостановление оказания УПИ, как период времени между двумя последовательно произошедшими инцидентами с момента восстановления оказания УПИ, приостановленных в результате первого инцидента, и до

момента возникновения события, приведшего к приостановлению оказания УПИ в результате следующего инцидента.»;

в абзаце первом подпункта 2.4 слова «ОПКЦ внешней платежной системы» исключить;

в абзаце пятом подпункта 2.5 слово «рабочий» исключить;

дополнить подпунктами 2.6–2.11 следующего содержания:

«2.6. КИР 6 должен рассчитываться в зависимости от размера активов участника ПС.

2.6.1. Для банка – участника ПС, размер активов которого составляет менее 500 миллиардов рублей на начало текущего отчетного года, КИР 6 должен рассчитываться ежегодно как количество событий списания денежных средств с банковских счетов участников ПС и клиентов Банка России без их согласия, за исключением случаев, предусмотренных законодательством Российской Федерации или комплексным договором банковского обслуживания.

В случае если значение КИР 6 более либо равно 2, произошло нарушение порогового уровня КИР 6.

2.6.2. Для банка – участника ПС, размер активов которого составляет 500 миллиардов рублей и более на начало текущего отчетного года, КИР 6 должен рассчитываться ежегодно как количество событий списания денежных средств с банковских счетов участников ПС и клиентов Банка России без их согласия, за исключением случаев, предусмотренных законодательством Российской Федерации или комплексным договором банковского обслуживания.

В случае если значение КИР 6 более либо равно 1, произошло нарушение порогового уровня КИР 6.

2.7. КИР 7 должен рассчитываться ежеквартально как отношение суммы денежных средств, относительно которых участниками СБП получены уведомления от их клиентов о списании денежных средств с банковских счетов клиентов без их согласия за оцениваемый квартал, за исключением случаев, предусмотренных законодательством Российской Федерации, к

общей сумме денежных средств, списанных с банковских счетов клиентов участников СБП посредством осуществления перевода денежных средств с использованием СБП.

В случае если значение КИР 7 более 0,005 процента, произошло нарушение порогового уровня КИР 7.

2.8. КИР 8 должен рассчитываться не реже одного раза в два года на основе результатов оценки соответствия текущего уровня защиты информации объектов информационной инфраструктуры Банка России, обеспечивающих функционирование ПС, уровням, определенным пунктом 6.7 раздела 6 ГОСТ Р 57580.1-2017, согласно методике оценки соответствия защиты информации, определенной в разделе 6 ГОСТ Р 57580.2-2018.

В случае если числовая итоговая оценка соответствия защиты информации, рассчитываемая в соответствии с пунктом 7.10 раздела 7 ГОСТ Р 57580.2-2018, менее 0,85 процента, произошло нарушение порогового уровня КИР 8.

2.9. КИР 9 должен рассчитываться не реже одного раза в два года на основе результатов оценки соответствия текущего уровня защиты информации ОПКЦ внешней платежной системы уровням, определенным пунктом 6.7 раздела 6 ГОСТ Р 57580.1-2017, согласно методике оценки соответствия защиты информации, определенной в разделе 6 ГОСТ Р 57580.2-2018.

В случае если уровень соответствия ниже уровня, установленного пунктом 20 Положения Банка России № 802-П, произошло нарушение порогового уровня КИР 9.

2.10. КИР 10 должен рассчитываться как количество случаев успешного прохождения в ПС технологического контроля электронных сообщений, не подлежащих обработке, в результате инцидентов.

В случае если значение КИР 10 больше 0, произошло нарушение порогового уровня КИР 10.

2.11. КИР 11 должен рассчитываться как количество повторно выявленных по результатам ежегодного тестирования на проникновение уязвимостей, имеющих высокий или критический уровень опасности уязвимости, предусмотренный подпунктом 5.2.18 пункта 5.2 раздела 5 национального стандарта Российской Федерации ГОСТ Р 56545-2015 «Защита информации. Уязвимости информационных систем. Правила описания уязвимостей» (утвержден приказом Федерального агентства по техническому регулированию и метрологии от 19 августа 2015 года № 1180-ст (М., ФГУП «Стандартинформ», 2015) и введен в действие 1 апреля 2016 года).

В случае если значение КИР 11 больше 0, произошло нарушение порогового уровня КИР 11.»;

абзац третий пункта 3 после слов «подразделений Банка России» дополнить словами «, в состав которых входят ПУРиН,».

1.17. В приложении 4:

в пункте 2:

в абзаце первом слово «Подготовка» заменить словами «Идентификация значимых рисков должна осуществляться не реже одного раза в год. Подготовка»;

дополнить абзацем следующего содержания:

«Идентификация ОПКЦ внешней платежной системы риска информационной безопасности в ПС должна включать в себя идентификацию области применения процесса управления риском информационной безопасности, присущим шагам (операциям) бизнес-процесса, выполняемым ОПКЦ внешней платежной системы, идентификацию риска информационной безопасности, присущего шагам (операциям) бизнес-процесса, выполняемым ОПКЦ внешней платежной системы, а также моделирование угроз безопасности информации с учетом мер, определенных подпунктом 7.2.2 пункта 7.2 раздела 7 ГОСТ Р 57580.4-2022 и подпунктами 8.2.2.3 и 8.2.2.4 пункта 8.2 раздела 8 ГОСТ Р 57580.3-2022.»;

пункт 5 дополнить подпунктом 5.3 следующего содержания:

«5.3. Оценка ОПКЦ внешней платежной системы риска информационной безопасности в ПС должна включать в себя оценку степени возможности реализации и степени тяжести последствий инцидентов защиты информации с учетом мер, определенных подпунктом 8.2.2.5 пункта 8.2 раздела 8 ГОСТ Р 57580.3-2022.».

1.18. В приложении 6:

пункт 3 дополнить абзацами следующего содержания:

«АС и подразделения Банка России, в которых используются данные из ПС, а также мероприятия по информированию указанных подразделений Банка России о переходе ПС на резервный комплекс программных средств;

мероприятия по переходу на резервный комплекс программных и (или) технических средств (при совмещении в ПС функций оператора платежной системы и операционного, и (или) платежного клирингового, и (или) расчетного центров).»;

абзац пятый пункта 7 изложить в следующей редакции:

«При реализации рисков, последствия которых требуют перехода на оказание УПИ с использованием резервного комплекса программных и (или) технических средств, решение о переходе принимается курирующим руководителем Банка России.»;

дополнить пунктом 13 следующего содержания:

«13. План ОНиВД ОПКЦ внешней платежной системы должен включать в себя мероприятия по переходу на резервный комплекс программных и (или) технических средств оператора УПИ в случае приостановления оказания ОПКЦ внешней платежной системы УПИ в ПС.».

2. Настоящее Указание подлежит официальному опубликованию и в соответствии с решением Совета директоров Банка России (протокол заседания Совета директоров Банка России от 22 декабря 2023 года

№ ПСД-49) вступает в силу с 1 октября 2024 года, за исключением подпункта 1.12 пункта 1 настоящего Указания.

Подпункт 1.12 пункта 1 настоящего Указания вступает в силу с 1 октября 2026 года.

Председатель
Центрального банка
Российской Федерации Э.С. Набиуллина