

УТВЕРЖДЕНО

Постановление Правления  
Национального банка  
Республики Беларусь

31.12.2019 № 552

## СТАНДАРТ ПРОВЕДЕНИЯ РАСЧЕТОВ

СПР 7.01-2020 "Банковская  
деятельность. Информационные  
технологии. Обеспечение  
непрерывности функционирования  
и восстановление  
работоспособности участника  
платежной системы. Общие  
требования"

### ГЛАВА 1 ОБЩИЕ ПОЛОЖЕНИЯ

1. Настоящий стандарт проведения расчетов (далее – стандарт) устанавливает общие требования к обеспечению непрерывности функционирования и восстановления работоспособности участника платежной системы при осуществлении платежей и проведении расчетов.

2. Настоящий стандарт применяется к отношениям, связанным с выполнением участниками платежных систем мероприятий по обеспечению непрерывной работы и восстановлению работоспособности в случае возникновения кризисной (сбойной) ситуации.

3. В настоящем стандарте используются следующие термины и их определения:

кризисная (сбойная) ситуация – чрезвычайное происшествие, приводящее к нарушению процесса функционирования платежной системы вследствие отказов в работе программно-технических комплексов, средств телекоммуникаций (далее – СТ), систем жизнеобеспечения;

обеспечивающие системы – системы, предназначенные для обеспечения физической и технической защиты, безопасных условий работы персонала в зданиях и помещениях, в которых расположена программно-техническая инфраструктура автоматизированных систем, используемых для осуществления платежей и проведения расчетов;

платежная система – совокупность участников платежной системы, оператора платежной системы, платежных инструментов и (или) средств платежа, правил платежной системы, программно-технических и

телекоммуникационных средств, обеспечивающих осуществление перевода денежных средств (электронных денег);

план обеспечения непрерывной работы и восстановления работоспособности участника платежной системы (далее – ПОНРВ) – документ, содержащий комплекс организационных и программно-технических мероприятий, которые должны выполняться до, во время и после возникновения кризисной (сбойной) ситуации;

применение программных и программно-технических средств по назначению – использование программных и программно-технических средств в соответствии с назначением, указанным изготовителем в эксплуатационных документах;

программно-технический комплекс (далее – ПТК) – программно-технические средства (далее – ПТС), объединенные в комплекс для реализации задач автоматизированной системы;

ПТС – совокупность программных и технических средств (далее – ТС);

программное средство (далее – ПС) – объект, состоящий из программ, процедур, правил, а также при необходимости сопутствующих им документации и данных, относящихся к функционированию программного средства;

средства телекоммуникаций – совокупность программных, программно-технических, технических и коммуникационных средств и каналов связи, предназначенных для приема и передачи информации;

системы жизнеобеспечения – системы и процессы создания и поддержания условий пригодности среды в зданиях и помещениях для бесперебойного функционирования ПТК и работы персонала;

техническая документация – документация на автоматизированную систему (далее – АС), определяющая технические требования к АС, технические и организационные решения по созданию (развитию) и функционированию АС;

учтенная копия программного обеспечения, технической документации – копия, взятая на учет держателем подлинников программного обеспечения и (или) технической документации для внесения изменений в подлинники при проведении модернизации программного обеспечения и (или) технической документации;

эксплуатационная документация – документация, предназначенная для использования при эксплуатации АС, определяющая правила и порядок действий пользователей при ее функционировании;

участник платежной системы (участник) – Национальный банк, банки и небанковские кредитно-финансовые организации, зарегистрированные в соответствии с законодательством, и другие организации, допущенные к

участию в платежной системе в соответствии с правилами платежной системы.

Термины "автоматизированная система", "документация на автоматизированную систему" используются в значениях, определенных в ГОСТ 34.003–90 "Информационная технология. Комплекс стандартов на автоматизированные системы. Автоматизированные системы. Термины и определения".

Термины "безотказность", "восстановление", "отказ", "работоспособное состояние", "резервирование" используются в значениях, определенных в ГОСТ 27.002–89 "Надежность в технике. Основные понятия. Термины и определения".

Термин "подлинник" используется в значении, определенном в ГОСТ 28388–89 "Системы обработки информации. Документы на магнитных носителях данных. Порядок выполнения и обращения".

Термин "технические средства" используется в значении, определенном в ГОСТ 15971–90 "Системы обработки информации. Термины и определения".

Термин "информационный ресурс" используется в значении, определенном в Законе Республики Беларусь от 10 ноября 2008 г. № 455-3 "Об информации, информатизации и защите информации".

## ГЛАВА 2

### ОБЩИЕ ТРЕБОВАНИЯ К ОРГАНИЗАЦИИ НЕПРЕРЫВНОЙ РАБОТЫ УЧАСТНИКА И ВОССТАНОВЛЕНИЮ ЕГО РАБОТОСПОСОБНОСТИ

4. Выполнение участником установленных требований к подключению (отключению) к (от) работе (работы) в платежной системе подтверждается документами, выдаваемыми оператором платежной системы в соответствии с установленной им правилами.

5. Непрерывная работа участника осуществляется в соответствии с действующими в платежной системе национальными и международными стандартами в области информационной безопасности, включая построение и поддержку защищенных сетей и систем, защиту данных пользователей, поддержку программы управления уязвимостями, внедрение строгих мер контроля доступа, осуществление регулярного мониторинга и тестирования сетей, поддержку политики информационной безопасности.

6. Работоспособность используемых участником при осуществлении платежей и проведении расчетов АС обеспечивается работоспособностью всех используемых участником ПТС и СТ, обеспечивающих осуществление платежей и проведение расчетов. Участником

предпринимаются меры, чтобы нарушение в работе ПТС и СТ участника не приводило к существенному нарушению или прекращению работы платежной системы.

7. Непрерывность работы и минимизация времени восстановления работоспособности деятельности участника обеспечивается следующими мероприятиями:

- разработка и применение организационно-методических документов;
- разработка и выполнение политики информационной безопасности;
- повышение качества разработки, сопровождения ПС и развития АС;
- создание условий по обеспечению надежности функционирования АС и СТ;

- управление безопасностью и надежностью доступа к используемым информационным ресурсам;

- эффективное управление информационными ресурсами;

- качество управления системами жизнеобеспечения;

- создание условий для успешной работы персонала.

8. Надежное, безопасное осуществление платежей и проведение расчетов обеспечивается достаточным количеством персонала с соответствующим уровнем квалификации, а также достаточным количеством финансовых и материальных ресурсов. При этом личная безопасность персонала, а также установленный порядок обеспечения принятия решений и использования эффективных схем оповещения в кризисных (сбойных) ситуациях имеют степень первостепенной важности.

9. В целях обеспечения надежного, безопасного функционирования участника, а также минимизации негативного воздействия кризисной (сбойной) ситуации на работу платежной системы разрабатывается ПОНРВ участника.

10. При разработке ПОНРВ участника кризисные (сбойные) ситуации категорируются. Присвоение категорий кризисной (сбойной) ситуации осуществляется по одному или нескольким признакам:

- масштаб кризисной (сбойной) ситуации;

- размер наносимого ущерба при реализации выхода из кризисной (сбойной) ситуации;

- причины возникновения кризисной (сбойной) ситуации;

- время реакции и восстановления работоспособности;

- уровень оповещения руководства участника и (или) принятия им решений.

Основными причинами возникновения кризисной (сбойной) ситуации в функционировании участника являются:

- стихийные бедствия (землетрясение, наводнение, ураган и т.д.);

- чрезвычайные ситуации (пожар, затопление, отравления ядовитыми

веществами и т.д., включая террористический акт или его угрозу, возникновение, распространение и объявление в Республике Беларусь эпидемии смертельно опасного заболевания);

технологические ошибки;

отказ систем жизнеобеспечения и обеспечивающих систем;

отказ ПТС и СТ, а также ошибки в системных, специальных и (или) прикладных ПС;

ошибки персонала, вызванные неправильными действиями случайного или умышленного характера;

массированные атаки со стороны злоумышленников с использованием вредоносного ПО и (или) ПТС;

нарушение требований к информационной безопасности в АС, используемых для осуществления платежей и проведения расчетов.

11. Объектами ПОНРВ являются:

организационно-методическое и документационное обеспечение (локальные правовые акты и эксплуатационная документация, описывающие технологический процесс осуществления платежей и проведения расчетов);

АС с входящими в их состав информационными ресурсами, используемыми для осуществления платежей и проведения расчетов;

иная программно-техническая инфраструктура АС, используемая для осуществления платежей и проведения расчетов (функционирующие ПТС и СТ);

обеспечивающие системы и системы жизнеобеспечения;

персонал, эксплуатирующий, обслуживающий и сопровождающий ПТС и СТ, обеспечивающие осуществление платежей и проведение расчетов, и обслуживающий системы жизнеобеспечения, а также использующий информационные ресурсы АС при выполнении должностных обязанностей;

здания и помещения, в которых расположена программно-техническая инфраструктура АС и СТ, используемых для осуществления платежей и проведения расчетов, и работает персонал участника.

12. Мероприятия по восстановлению работоспособности участника в соответствии с ПОНРВ ограничиваются временными рамками и фиксируются в соответствии с локальными правовыми актами участника. Восстановление работоспособности участника начинается в пределах операционного дня, когда была обнаружена кризисная (сбойная) ситуация.

Время восстановления участника устанавливается в каждой платежной системе в зависимости от установленных категорий кризисных (сбойных) ситуаций.

13. Для сокращения времени восстановления работоспособности участника при работе с документацией предусматривается:

- наличие подлинников организационно-методических документов и эксплуатационной документации;

- наличие рабочих экземпляров организационно-методических документов и эксплуатационной документации на резервных рабочих местах и (или) резервных центрах;

- хранение подлинников документов отдельно от рабочих экземпляров;

- поддержание локальных правовых актов, организационно-методических документов и эксплуатационной документации в актуальном состоянии;

- обеспечение персонала рабочими экземплярами организационно-методических документов и эксплуатационной документации.

14. Для осуществления непрерывной работы и восстановления работоспособности АС участника обеспечивается:

- разработка и поддержание в актуальном состоянии описания технологического процесса используемых АС, ПТК и (или) СТ;

- наличие учтенных рабочих и резервных копий ПС;

- наличие резервного вычислительного центра;

- хранение резервных копий используемых ПС в территориально удаленных зданиях и помещениях;

- сохранность эксплуатируемых информационных ресурсов;

- использование сертифицированных и лицензионных ПС, а также ПС, соответствующих требованиям, установленным в стандартах проведения расчетов;

- установление порядка разработки, сопровождения (внесения изменений), хранения и эксплуатации ПС.

15. Для минимизации времени восстановления программно-технической инфраструктуры АС участника обеспечивается выполнение следующих требований по:

- управлению порядком функционирования и восстановления АС, ПТС и СТ;

- определению критически значимых АС, ПТС и СТ;

- резервированию критически значимых ПТС и СТ;

- контролю работоспособности резервных ПТС и СТ;

- техническому обслуживанию ПТС и СТ на постоянной основе (комплекс работ по поддержанию ТС в работоспособном состоянии);

- организации дежурства специалистов по техническому сопровождению (при необходимости).

16. При работе с персоналом участника учитываются требования по: подбору и подготовке персонала необходимой квалификации;

учету мотивации персонала к положительным результатам работы; управлению переподготовкой и повышением квалификации персонала;

проведению аттестации персонала и выполнению рекомендаций по результатам аттестации;

организации прохождения медицинского осмотра персонала (медицинское освидетельствование) и выполнению рекомендаций по его результатам;

созданию резерва и организации замещения персонала (в соответствии со схемой замещения);

обеспечению снижения текучести кадров.

17. Для сокращения времени восстановления работоспособности систем жизнеобеспечения и обеспечивающих систем участника выполняются следующие требования:

соблюдение установленных правил и процедур эксплуатации зданий и помещений, систем жизнеобеспечения и обеспечивающих систем;

ограничение и контроль доступа в здания и помещения, используемые для осуществления платежей и проведения расчетов;

оборудование зданий и помещений соответствующими системами оповещения о пожаре, пожарной сигнализации, автоматического пожаротушения, схемами эвакуации из зданий и помещений;

проведение профилактических мероприятий по поддержанию систем жизнеобеспечения и обеспечивающих систем в работоспособном состоянии с учетом сезонных нагрузок.

18. Восстановительные работы при кризисных (сбойных) ситуациях проводятся с оказанием минимального влияния на график (регламент) функционирования платежной системы, для чего участником предусматриваются дополнительные возможности осуществления платежей и проведения расчетов в основном и (или) резервном режимах функционирования платежной системы.

### ГЛАВА 3

## ОБЩИЕ ТРЕБОВАНИЯ К ОБЕСПЕЧЕНИЮ БЕЗОТКАЗНОСТИ РАБОТЫ ПРОГРАММНО-ТЕХНИЧЕСКОЙ ИНФРАСТРУКТУРЫ АС УЧАСТНИКА

19. Безотказность работы ТС, ПТС, СТ участника достигается за счет проведения мероприятий, направленных на предупреждение нарушения их работоспособности и минимизацию времени их восстановления при возникновении кризисных (сбойных) ситуаций.

20. Участник разрабатывает локальные правовые акты по обеспечению управления, использования и взаимодействия ПТС и СТ, входящих в состав АС, используемых для осуществления платежей и проведения расчетов, в которых также определяется перечень работ по сопровождению, обслуживанию и эксплуатации указанных АС участника, используемых для осуществления платежей и проведения расчетов.

21. Участник определяет и утверждает перечень ТС, ПТС и СТ, а также создает их резерв, включающий комплектующие изделия и детали в количестве, достаточном для восстановления работоспособности данных ТС, ПТС, СТ и функционирования каналов связи.

22. Участником обеспечивается доступность резервных ТС, ПТС, СТ, каналов связи, комплектующих изделий и деталей в течение всего операционного дня персоналу участника, обеспечивающему проведение восстановительных работ.

23. Временная защита ТС, ПТС и СТ от сбоев в работе электрической сети обеспечивается путем использования источников бесперебойного питания, резервированием питания и (или) использования автономного генератора мощностью, достаточной для поддержания работоспособности ТС, ПТС и СТ, обеспечивающих проведение расчетов, не менее 45 минут с целью завершения технологического этапа работы ПТК и сохранения информации.

24. Для защиты ТС от воздействия окружающей среды участник обеспечивает поддержание температурно-влажностного режима, установленного в технической документации производителя соответствующих ТС.

25. Повышение уровня безотказной работы ПТС, ТС, СТ и каналов связи обеспечивается за счет проведения их периодического технического обслуживания и тестирования в соответствии с требованиями технической документации производителя ПТС, ТС и СТ, но не реже одного раза в год по утвержденному участником графику.

Участник разрабатывает порядок проведения периодического технического обслуживания и тестирования ТС, ПТС, СТ и каналов связи (дата проведения технического обслуживания, перечень работ и т.д.), а также учета всех обнаруженных в ходе выполнения работ дефектов.

Порядок проведения периодического технического обслуживания и тестирования включает в себя проведение периодического контроля (проверки) резервных ПТК, ПС, ПТС, СТ, каналов связи и параметров их настроек.

26. В процессе периодического технического обслуживания ПТС, ТС и СТ персонал участника проводит внешний и внутренний осмотр ПТС, ТС



и СТ, проверяет параметры настроек работоспособности ПТС, ТС и СТ и тестирует взаимодействие ПТС, ТС и СТ.

Подробное описание работ, проводимых при периодическом техническом обслуживании и тестировании ПТС, ТС и СТ, участник отражает в технической документации и (или) договорах на оказание соответствующих услуг при привлечении сторонних организаций. Внутренний осмотр ПТС и ТС может не проводиться, если это влечет нарушение порядка их гарантийного обслуживания или не предусмотрено технической документацией производителя.

В рамках работ по техническому обслуживанию и тестированию эксплуатируемых ПТС участник проводит плановые проверки на отсутствие компьютерных вирусов и вредоносных программ с соблюдением частоты и содержание проверок в соответствии с проводимой участником политикой информационной безопасности.

27. В случае кризисной (сбойной) ситуации в функционировании ТС, ПС, ПТС, СТ и каналов связи восстановление его работоспособности проводится в соответствии с технической документацией производителя ТС, ПС, ПТС, СТ и каналов связи (поставщика телекоммуникационных услуг) и (или) документами участника по восстановлению работоспособности ТС, ПС, ПТС, СТ и каналов связи и завершается проведением их тестирования.

Факт кризисной (сбойной) ситуации в функционировании ТС, ПС, ПТС, СТ и каналов связи (дата и время возникновения и устранения, причины, меры по недопущению в дальнейшем и т.д.) фиксируется в соответствии с разработанным участником порядком. Учету подлежат все факты кризисной (сбойной) ситуации в функционировании ТС, ПС, ПТС, СТ и каналов связи.

28. Участник проводит регулярный анализ сбоев в функционировании ТС, ПТС, СТ и каналов связи и обнаруженных в ходе их периодического технического обслуживания и тестирования дефектов.

На основании результатов проведенного анализа формируется план корректирующих мероприятий для предупреждения в дальнейшем кризисных (сбойных) ситуаций и устранения причин выявленных дефектов, а также минимизацию времени восстановления при возникновении кризисных (сбойных) ситуаций.

29. Доступ к ТС, ПТС и СТ, используемым при осуществлении платежей и проведении расчетов, и в помещения, где расположены данные ТС, ПТС и СТ, а также технический архив ПС, используемых при функционировании АС, ограничивается в соответствии с локальными правовыми актами участника.

30. Участник разрабатывает порядок учета ПТК и оборудования СТ, используемых для осуществления платежей и проведения расчетов. При проведении мероприятий по учету ПТК и оборудования СТ, используемых для осуществления платежей и проведения расчетов, учитывается следующая информация:

наименование ПТК или оборудования СТ;

дата ввода в эксплуатацию ПТК или оборудования СТ;

данные персонала, ответственного за эксплуатацию ПТК или оборудования СТ;

данные персонала, ответственного за техническую поддержку ПТК или оборудования СТ (при наличии информации);

состав ТС и их размещение;

состав ПС;

перечень технической и эксплуатационной документации;

основной и резервный каналы связи (для СТ);

перечень резервного оборудования с указанием места его размещения.

31. В комплект технической и эксплуатационной документации СТ входят схемы подключения и расположения (с указанием мест хранения информации об актуальных сетевых адресах, параметрах маршрутизации и конфигурационных файлах).

32. Перед вводом в эксплуатацию разрабатываемых (поставляемых) ПС участник проводит проверку их работоспособности и отсутствия вредоносного программного обеспечения либо производитель (поставщик) ПС документально подтверждает участнику их работоспособность (самостоятельно или в составе ПТК) и отсутствие вредоносного программного обеспечения.

33. В комплект разрабатываемых (поставляемых) ПС входит эксплуатационная документация на данное ПС.

34. Участник определяет порядок учета и хранения ПС (подлинников, дубликатов и рабочих копий на машинных носителях) и их использования в производстве. Данные процедуры выполняются участником до введения ПС в эксплуатацию. Учет и хранение данных ПС на машинных носителях осуществляется участником в своем техническом архиве в соответствии с требованиями ГОСТ 28388–89 "Системы обработки информации. Документы на магнитных носителях данных. Порядок выполнения и обращения" в помещениях основного и резервного вычислительных центров участника.

Участник в течение всего операционного дня обеспечивает доступность персоналу, обеспечивающему функционирование указанных ПС, рабочих копий ПС на машинных носителях, эксплуатационной

документации, а также документации по восстановлению работоспособности ПС.

Перед передачей ПС из технического архива в эксплуатацию машинный носитель с ПС проверяется на отсутствие вредоносного программного обеспечения и на работоспособность на оборудовании, используемом для тестирования ПС.

35. Для осуществления платежей и проведения расчетов участник использует основной и резервный каналы связи. Помимо использования собственных каналов связи допускается их аренда у поставщиков телекоммуникационных услуг.

Участник самостоятельно или с привлечением поставщика телекоммуникационных услуг осуществляет контроль доступности и мониторинг загрузки каналов, а также обеспечивает автоматическое переключение между основным и резервным каналами связи в случае возникновения кризисной (сбойной) ситуации.

36. Участник обеспечивает пропускную способность оборудования СТ и каналов связи, достаточную для осуществления платежей и проведения расчетов в режимах, установленных в платежной системе. При этом пропускная способность основного канала связи обеспечивает передачу сообщений, необходимых для проведения платежей и осуществления расчетов, в объеме не менее 120 % от пикового количества в час, переданных, через данный канал связи за предшествующий месяц, для резервного канала связи – не менее среднего количества сообщений в час, переданных через основной канал связи в течении операционного дня за предшествующий месяц.

37. При подключении через поставщика телекоммуникационных услуг информация о контактных телефонах служб технической поддержки поставщика телекоммуникационных услуг доводится до персонала участника.

38. В случае использования услуг арендованного центра обработки данных или поставщика облачных решений участник обеспечивает наличие документов, подтверждающих, что используемый для оказания услуги центр обработки данных:

обеспечивает защиту информации, распространение и (или) предоставление которой ограничено, имеет аттестацию и использует сертифицированные средства защиты информации в соответствии с требованиями законодательства об информации, информатизации и защите информации;

имеет серверное оборудование и оборудование хранения данных, удовлетворяющее требованиям по надежности и резервированию технических средств на уровне не ниже 2 (N+1);

имеет (предоставляет) защищенные каналы связи для удаленного администрирования, а также для соединения с иными защищаемыми (аттестованными) объектами. Защищенные каналы связи организовываются с использованием сертифицированных систем защиты информации (средств криптографической защиты информации), соответствующих требованиям законодательства об информации, информатизации и защите информации;

имеет внедренную систему управления (менеджмента) информационной безопасности, имеющей сертификат соответствия требованиям ISO 27001;

соответствует требованиям стандарта безопасности данных индустрии банковских платежных карточек PCI DSS для среды банковских платежных карточек;

имеет платформу виртуализации и компоненты виртуализации сети, имеющей сертификат соответствия и поддерживающей функции:

контроля и разделения доступа к ресурсам системы виртуализации и физическим ресурсам;

разделения системы управления и обработки данных;

разделения потоков информации виртуальных машин;

ограничения на использование физических ресурсов;

регистрации событий;

использования (встраивания) систем защиты информации производителей, отличных от производителя системы виртуализации.

## ГЛАВА 4

### ОБЩИЕ ТРЕБОВАНИЯ К ОБЕСПЕЧЕНИЮ РАБОТОСПОСОБНОСТИ СИСТЕМ ЖИЗНЕОБЕСПЕЧЕНИЯ УЧАСТНИКА

39. В состав систем жизнеобеспечения участника входят следующие основные системы:

электроснабжения;

кабельные системы вычислительных сетей, связи и автоматизации;

вентиляции и кондиционирования;

теплоснабжения, водоснабжения и канализации;

оповещения о пожаре, пожарной сигнализации, автоматического пожаротушения, мониторинга за техническими средствами противопожарной защиты.

40. Участник определяет перечень процедур, необходимых для восстановления работоспособности систем жизнеобеспечения, выполняемых при возникновении кризисных (сбойных) ситуаций.

41. Действия, выполняемые персоналом по восстановлению работоспособности систем жизнеобеспечения участника, описываются в локальных правовых актах участника (с учетом планов гражданской обороны, предупреждения и ликвидации чрезвычайных ситуаций), а также в относящихся к ПОНРВ и детализирующих его локальных правовых актах по переходу систем жизнеобеспечения в аварийный режим функционирования и возврату в штатный режим.

42. Система электроснабжения участника, обеспечивающая функционирование АС, ПТК, ПТС и СТ, организовывается с использованием выделенной линии питания, защищенной от перенапряжения специальными устройствами и не связанной с системой электропитания осветительного и другого электрооборудования.

Использование местных нагревательных и отопительных приборов, питаемых теплоносителями, выполняется в соответствии с требованиями изготовителя по их использованию.

43. Участник проводит мероприятия, направленные на бесперебойное обеспечение электричеством критически значимых объектов, ПТС и СТ, функционирования систем жизнеобеспечения и создания условий труда персонала. К указанным мероприятиям относятся следующие:

оборудование ПТС и СТ, обеспечивающих осуществление платежей и проведение расчетов, источниками бесперебойного питания достаточной мощности, обеспечивающей работу указанных ПТС и СТ не менее 45 минут;

организация двух независимых входов подачи электроэнергии в здание участника от двух подстанций;

установка, наладка и периодическая проверка работоспособности автономной дизель-генераторной установки (при ее наличии).

44. Выбор здания, в которых размещены служебные и вспомогательные помещения, используемые участником для обеспечения осуществления платежей и проведения расчетов, производится с учетом обязательного обеспечения системами холодного и горячего водоснабжения, канализации и водостоков, противопожарного водоснабжения.

45. Системы отопления, вентиляции, кондиционирования воздуха и пожарной безопасности зданий участника организуются в соответствии с требованиями, предъявляемыми для их проектирования и модернизации.

## ГЛАВА 5

ОБЩИЕ ТРЕБОВАНИЯ К ОБЕСПЕЧЕНИЮ РАБОТОСПОСОБНОСТИ  
ОБЕСПЕЧИВАЮЩИХ СИСТЕМ УЧАСТНИКА

46. К обеспечивающим системам относятся:  
ТС и системы охраны зданий и помещений;  
автоматизированная система контроля и управления доступом в здания и помещения;  
система видеонаблюдения.

47. Участник определяет перечень процедур, необходимых для восстановления работоспособности обеспечивающих систем, выполняемых при возникновении кризисных (сбойных) ситуаций.

48. Действия, выполняемые персоналом по восстановлению работоспособности обеспечивающих систем участника, описываются в локальных правовых актах участника (с учетом планов гражданской обороны, предупреждения и ликвидации чрезвычайных ситуаций).

49. Использование обеспечивающих систем участника проводится с соблюдением требований по:

обеспечению безопасности работы персонала;

обеспечению безопасности зданий и помещений, в которых размещены ПТК, ПТС и СТ, обеспечивающие осуществление платежей и проведение расчетов;

обеспечению ограничения доступа в помещения, в которых размещены ПТК, ПТС и СТ, обеспечивающие осуществление платежей и проведение расчетов, включая видеосъемку и хранение информации о посещениях данных помещений, в соответствии с применяемой политикой безопасности;

недопущению несанкционированного доступа к системам жизнеобеспечения.

## ГЛАВА 6

ОБЩИЕ ТРЕБОВАНИЯ К ОБЕСПЕЧЕНИЮ СОХРАННОСТИ  
ИНФОРМАЦИОННЫХ РЕСУРСОВ УЧАСТНИКА

50. При организации работы с информационными ресурсами участника обеспечивается выполнение следующих требований:

проведение классификации, идентификации и документированного учета всех основных информационных ресурсов;

использование для работы с информационными ресурсами лицензионных и сертифицированных ПС;

разделение информационных ресурсов по среде использования (среда

разработки, среда тестирования и производственная среда);

распределение зон ответственности при эксплуатации, сопровождении и обслуживании информационных ресурсов;

управление процедурами создания эталонных и рабочих копий информационных ресурсов, а также их резерва с соблюдением принципа территориального разделения при хранении эталонных и резервных копий информационных ресурсов;

соблюдение порядка ввода и вывода информационных ресурсов из эксплуатации и их последующего уничтожения;

соблюдение порядка гарантированного уничтожения информации и ПС с устройств их хранения;

соблюдение порядка физического уничтожения носителей при выведении информационных ресурсов из эксплуатации.

51. При размещении резервных ТС и ПС на резервном вычислительном центре участника обеспечивается доступ к информационным ресурсам в соответствии с применяемой политикой информационной безопасности, а также минимизируется вероятность их уничтожения вследствие кризисных (сбойных) ситуаций.

52. В состав информационных ресурсов, подлежащих хранению, входят:

совокупность документированной информации, включающей базы данных, другие совокупности взаимосвязанной информации в АС, обеспечивающей осуществление платежей и проведение расчетов;

структуры баз данных;

протоколы обработки информации, включая кризисные события и действия персонала;

входная и выходная информация об осуществляемых платежах и проводимых расчетах.

53. Информационные ресурсы, подлежащие хранению, хранятся в создаваемом участником архиве. В случае отсутствия у участника возможности организации архива для обеспечения данного требования он может привлечь поставщика данных услуг, если соответствующие требования платежной системы это позволяют.

54. Участник разрабатывает порядок восстановления информационных ресурсов в случае нарушения их целостности.

55. В течение всего операционного дня персоналу, обеспечивающему функционирование АС участника, обеспечивается доступность архивов, эксплуатационной документации и локальных правовых актов по восстановлению целостности информационных ресурсов.

56. С целью исключения возможности несанкционированного доступа к информационным ресурсам участником проводятся мероприятия по ограничению доступа к информационным ресурсам.

## ОБЩИЕ ТРЕБОВАНИЯ К ПЕРСОНАЛУ УЧАСТНИКА

57. Техническое обеспечение непрерывной работы АС, ПТК, ПТС и СТ, используемых при осуществлении платежей и проведении расчетов, а также доступ к информационным ресурсам, используемым при возникновении кризисных (сбойных) ситуаций для восстановления работоспособности АС, ПТК, ПТС и СТ, осуществляется персоналом участника в соответствии с возложенными на него должностными обязанностями.

58. Мероприятия по техническому обеспечению процесса осуществления платежей и проведения расчетов в соответствии с должностными обязанностями выполняются персоналом участника, обладающим достаточной для их выполнения квалификацией и имеющим образование, соответствующее профилю выполняемых обязанностей.

59. Участник определяет резервный персонал, временно обеспечивающий эксплуатацию, сопровождение и обслуживание АС, ПТК, ПТС и СТ, используемых при осуществлении платежей и проведении расчетов, в случае нетрудоспособности и (или) недоступности персонала, выполняющего данные функции на постоянной основе согласно своим должностным обязанностям.

60. Участник разрабатывает и утверждает схему замещения персонала, обеспечивающего эксплуатацию, сопровождение и обслуживание АС, ПТК, ПТС и СТ, используемых при осуществлении платежей и проведении расчетов.

61. Персонал участника проходит подготовку (инструктаж) по вопросам использования информационных ресурсов, применяемых в процессе осуществления платежей и проведения расчетов.

62. При изменении состава информационных ресурсов, АС, ПТК, ПТС и СТ, используемых при осуществлении платежей и проведении расчетов, участником не реже одного раза в три года обеспечивается проведение переподготовки (повышение квалификации) персонала, осуществляющего техническое обеспечение процесса осуществления платежей и проведения расчетов.

63. Сведения о подготовке (инструктаже) и переподготовке (повышении квалификации) персонала, обеспечивающего эксплуатацию, сопровождение и обслуживание АС, ПТК, ПТС и СТ, учитываются в личных делах персонала участника.



## ГЛАВА 8

## ОБЩИЕ ТРЕБОВАНИЯ К ПЛАНУ ОБЕСПЕЧЕНИЯ НЕПРЕРЫВНОЙ РАБОТЫ И ВОССТАНОВЛЕНИЯ РАБОТОСПОСОБНОСТИ УЧАСТНИКА

64. Проведение мероприятий по восстановлению непрерывной работы, связанных с возникновением кризисных (сбойных) ситуаций, осуществляется участником в соответствии с ПОНРВ, утвержденным локальным правовым актом.

Оформление ПОНРВ участника может осуществляться в виде иерархически упорядоченных организационно-методических документов, регулирующих обеспечение непрерывной работы участника, а также восстановление в установленные сроки его работоспособности после устранения кризисной (сбойной) ситуации.

65. В ПОНРВ участника входят:

- перечень объектов ПОНРВ участника;
- описание порядка функционирования участника в штатном режиме;
- определение и классификация кризисных (сбойных) ситуаций;
- сценарии возникновения и развития кризисных (сбойных) ситуаций в различные промежутки времени;
- оценка возможных потерь (ущерба) в результате возникновения кризисной (сбойной) ситуации;
- описание порядка функционирования в нештатном режиме;
- схемы оповещения и принятия решений;
- описание действий по восстановлению функционирования участника;
- описание действий по возврату функционирования участника в штатный режим;
- описание мероприятий, выполняемых после возврата к функционированию в штатном режиме;
- порядок рассмотрения кризисной (сбойной) ситуации;
- распределение ответственности персонала участника;
- определение порядка тестирования (испытаний) и пересмотра ПОНРВ участника.

66. При классификации кризисных (сбойных) ситуаций может учитываться участником характер кризисной (сбойной) ситуации: умышленная (возникает в результате выполнения злоумышленниками в определенные промежутки времени заранее обдуманных и спланированных действий) или случайная (возникает как результат объективных причин случайного характера, халатности, небрежности и форс-мажорных обстоятельств).

67. Участник определяет и поддерживает в актуальном состоянии перечень объектов ПОНРВ, который охватывает все критически значимые ПТК, используемые участником для осуществления платежей и проведения расчетов. В состав указанных ПТК входят ПТК, обеспечивающие:

функционирование АС участника, используемых для осуществления платежей и проведения расчетов в платежной системе;

взаимодействие участника с обслуживаемыми клиентами и пользователями информации;

резерв для восстановления функционирования основных ПТК.

68. Проведение мероприятий по восстановлению работоспособности участника в соответствии с ПОНРВ участника ограничивается установленными в платежной системе временными рамками. Время восстановления определяется в каждой платежной системе в зависимости от установленных категорий кризисных (сбойных) ситуаций.

Мероприятия по восстановлению работоспособности участника в соответствии с ПОНРВ подлежат учету в соответствии с локальными правовыми актами участника.

Осуществление мероприятий по восстановлению работоспособности участника начинаются в пределах того же операционного дня. При возникновении масштабных кризисных (сбойных) ситуаций в рамках платежной системы восстановление работоспособности участника начинается в пределах одного операционного дня после нейтрализации угрозы и восстановления функционирования платежной системы.

69. С целью минимизации влияния проведения участником восстановительных работ при кризисных (сбойных) ситуациях участник обеспечивает возможность осуществления платежей и проведения расчетов в основном и резервном режимах функционирования платежной системы.

70. Участник определяет порядок распределения между персоналом полномочий по принятию решений и ответственности за их выполнение, при организации проводимых мероприятий в кризисных (сбойных) ситуациях (возможно несколько сценариев с описанием организационных мероприятий).

71. Схема оповещения распределяет между персоналом участника обязанности по оповещению заинтересованного персонала участника и других организаций о возникновении кризисной (сбойной) ситуации, действий по восстановлению функционирования участника, действий по возврату функционирования в штатный режим.

Схема оповещения включает в себя требования к срокам и способам информирования потребителей услуг участника о возникновении кризисной (сбойной) ситуации и планируемых сроках восстановления функционирования участника, а также о возможных альтернативных способах осуществления платежей и проведения расчетов.

72. В ПОНРВ участника включаются ссылки на локальные правовые акты, техническую и эксплуатационную документацию, в которых установлены требования к:

- обеспечению информационной безопасности АС, используемых для осуществления платежей и проведения расчетов;

- структуре используемых информационных ресурсов;

- схемам технологического процесса взаимодействия ПТС и СТ при осуществлении платежей и проведении расчетов;

- периодическому техническому обслуживанию ПТС и СТ и составу работ, выполняемых в процессе его проведения;

- процедурам обеспечения непрерывной работы и восстановления работоспособности отдельных ПТК и альтернативных вариантов (мест) деятельности участника;

- перечню персонала участника, а также к работникам сторонних организаций, привлекаемых к решению возникающих кризисных (сбойных) ситуаций, и способам их оповещения;

- процедурам перехода к осуществлению платежей и проведению расчетов в резервном режиме;

- системам жизнеобеспечения и обеспечивающим системам;

- персоналу участника;

- к наличию учтенных и (при необходимости) рабочих копий организационно-методических документов для их целевого применения персоналом;

- обеспечению персонала участника необходимыми актуальными организационно-методическими документами ПОНРВ на своих рабочих местах;

- распределению обязанностей по приобретению, сопровождению, эксплуатации и архивированию ПС.

Описание структуры используемых информационных ресурсов и схемы технологического процесса взаимодействия ПТС и СТ содержит состав и конфигурацию ПТС и СТ, включая ПТК, ПС, ТС, и описание функционирования ПТК, а также схемы их взаимодействия.

Состав персонала участника, а также работников сторонних организаций, привлекаемых к решению возникающих кризисных (сбойных) ситуаций, и способы их оповещения позволяют минимизировать время восстановления работоспособности участника.

Процедуры перехода участника к осуществлению своих функций в резервном режиме содержат условия, при которых может приниматься решение о необходимости перехода к осуществлению платежей и проведению расчетов в резервном режиме, и основания для такого перехода. Процедуры включают порядок введения резервного режима и

порядок возврата в штатный режим функционирования, а также определяют перечень персонала, уполномоченного принимать данные решения.

Процедурами предусматривается обязательный возврат к функционированию на штатных ПТС и СТ после восстановления их работоспособности.

Порядок осуществления контроля исполнения ПОНРВ описывает процедуры и периодичность проведения контроля, а также включает перечень ответственного за его проведение персонала участника.

73. В ПОНРВ может включаться положения (документы), описывающие мероприятия по:

- ограничению доступа к информационным ресурсам участника;
- проведению копирования и архивирования ПС и данных;
- осуществлению контроля исполнения ПОНРВ.

В ПОНРВ может включаться документ, содержащий требования к порядку взаимодействия персонала участника, обслуживающего и сопровождающего ПТС и СТ при возникновении кризисных (сбойных) ситуаций, в котором взаимоувязаны вопросы классификации кризисных (сбойных) ситуаций, причины их возникновения и учтены требования настоящего стандарта.

74. Участник обеспечивает возможность осуществлять работы по восстановлению функционирования ПТС и СТ (ПТК), предусмотренные ПОНРВ, адекватные источнику и масштабам кризисной (сбойной) ситуации, затратам времени и видам ресурсов на восстановление функционирования, включающие:

использование соответствующих схем оповещения заинтересованных в обеспечении непрерывной работы участника и восстановления его работоспособности;

использование нескольких технологий передачи информации (система передачи финансовой информации Национального банка, факс, электронная почта, мобильная связь) в соответствии с установленными в платежной системе правилами;

использование резервных вычислительных центров, резервных центров обработки данных на случай невозможности восстановления функционирования платежной системы на основном вычислительном центре участника;

резервирование критически значимых компонентов АС;

резервирование СТ, наличие резервного канала связи для основного канала связи (если каналы арендуются, то желательно – у двух разных поставщиков телекоммуникационных услуг);

резервное копирование и хранение на разных территориях используемых участником сертифицированных и лицензионных ПС;

резервное копирование и хранение на разных территориях информационных ресурсов;

обеспечение бесперебойного энергоснабжения критически значимых компонентов АС;

защищенность силовых линий и каналов связи;

обеспечение ограничения доступа к информационным ресурсам;

использование средств информационной безопасности;

определение и поддержание в актуальном состоянии перечня и порядка взаимозаменяемости персонала;

наличие и обеспечение процедуры проведения отдельных определенных в платежной системе расчетов при выходе из строя СТ и каналов связи.

75. Не реже одного раза в год участник проводит тренировку (тестирование, контроль) действий, предусмотренных ПОНРВ. Данная тренировка воспроизводит один или несколько отдельных сценариев возникновения и развития кризисной (сбойной) ситуации в функционировании участника. Информацию по результатам тренировки ПОНРВ участник отражает в утверждаемом руководителем участника акте с отражением в нем полученных итогов, сделанных выводах, установленных несоответствий, предложениях по проведению корректирующих мероприятий и внесению изменений в ПОНРВ и локальные правовые акты участника.

76. Участник обеспечивает выполнение работ по регулярному пересмотру ПОНРВ.

Полный пересмотр ПОНРВ участник проводит в следующих случаях:  
при изменении перечня решаемых задач или конфигурации ПТК, обеспечивающих осуществление платежей и проведение расчетов, приводящем к изменению технологии обработки информации;

при получении неудовлетворительных (отрицательных) результатов тренировок (тестирования, контроля);

после урегулирования критических (сбойных) ситуаций.

Частичный пересмотр ПОНРВ участник проводит при изменении:

конфигурации ПТК, обеспечивающих осуществление платежей и проведение расчетов, не изменяющей технологии обработки информации; состава персонала, а также его должностных обязанностей.

Профилактический пересмотр ПОНРВ участник проводит ежегодно для поддержания ПОНРВ участника в актуальном состоянии или для оценки эффективности и корректности ПОНРВ в случае необходимости.

Информацию о результатах пересмотра ПОНРВ участник отражает в протоколе пересмотра ПОНРВ или путем утверждения новой редакции ПОНРВ.

## ГЛАВА 9

### ОБЩИЕ ТРЕБОВАНИЯ К ОРГАНИЗАЦИИ РЕЗЕРВНЫХ ВЫЧИСЛИТЕЛЬНЫХ ЦЕНТРОВ

77. Под резервным вычислительным центром участника понимают помещения, в которых размещены АС, ПТК, ПТС и СТ для осуществления платежей и проведения расчетов в резервном режиме в случае полной или частичной неработоспособности основных АС, ПТК, ПТС и СТ.

78. Участник обеспечивает информационную и техническую совместимость АС, ПТК, ПТС и СТ основного и резервного вычислительных центров, обеспечивающую их полную взаимозаменяемость.

79. Территориальная удаленность помещений резервного вычислительного центра участника от помещений основного вычислительного центра участника составляет не менее трех километров, если иное не предусмотрено требованиями, установленными в платежной системе.

80. Помещения резервного вычислительного центра участника оборудуются системами жизнеобеспечения. Энергопитание РВЦ участника обеспечивается с использованием резервирования энерговодвда, источников бесперебойного питания, дизель-генераторов.

81. Между резервным вычислительным центром участника и основным или резервным вычислительными центрами платежной системы участник организует отдельный канал связи. Допускается использование данного канала связи в качестве резервного канала связи для основных ПТС и СТ.

82. Между основным и резервным вычислительными центрами участника связь организуется без использования физических каналов связи с основным и резервным вычислительными центрами платежной системы. Организованный канал связи обеспечивает возможность осуществления платежей и проведение расчетов при возникновении кризисных (сбойных) ситуаций, приведших к частичному выходу из строя основных АС, ПТК, ПТС и СТ.

83. При организации резервного вычислительного центра участник обеспечивает выполнение требований к:

- организации непрерывной работы и восстановлению работоспособности;

- обеспечению безопасности работы с информационными ресурсами;

- обеспечению работоспособности обеспечивающих систем и систем жизнеобеспечения;

- обеспечению сохранности информационных ресурсов.

84. Участник контролирует работоспособность резервного вычислительного центра путем планового перехода на его использование вместо основного вычислительного центра не реже одного раза в полгода.

85. Процедуры перехода с основного на резервный вычислительный центр и обратно участник определяет в ПОНРВ.