

Реквизиты внутреннего нормативного документа:

Номер документа: №55

Дата утверждения: 21 августа 2020 года

Орган утверждения: Совет директоров АО «Народный Банк Казахстана»

**Политика управления непрерывностью деятельности
в АО «Народный Банк Казахстана»
(сокращенная версия)**

Глава 1. Общие положения

1. Политика управления непрерывностью деятельности (далее – Политика) в АО «Народный Банк Казахстана» (далее – Банк) определяет подходы, принципы, стратегии в построении эффективной системы управления непрерывностью деятельности в Банке, а также определяет органы и подразделения Банка, ответственные за реализацию настоящей Политики.

2. Политика разработана в соответствии с Правилами формирования системы управления рисками и внутреннего контроля для банков второго уровня, утвержденными постановлением Правления Национального Банка Республики Казахстан от 12.11.2019 № 188, и внутренними документами Банка.

3. Требования Политики распространяются на все структурные подразделения Банка, а также рекомендуются к использованию дочерними организациями Банка. В целях реализации настоящей Политики Банк вправе обращаться к филиалам, представительствам и дочерним организациям с требованием о предоставлении необходимой информации и документов.

4. Политика подлежит пересмотру в случаях внесения изменений в законодательство Республики Казахстан, а также во внутренние процедуры, связанных с обеспечением непрерывности деятельности, которые могут повлечь за собой необходимость внесения соответствующих изменений в Политику.

Глава 2. Цели, задачи и принципы управления непрерывностью деятельности

5. Управление непрерывностью деятельности является составной частью операционного риск-менеджмента и включает Политику и процедуры, нацеленные на обеспечение непрерывности и своевременное восстановление определенных бизнес-процессов при Инцидентах.

6. Цели управления непрерывностью деятельности:

1) минимизация операционных, финансовых, правовых, репутационных и других финансовых последствий, вытекающих из Инцидентов;

2) формирование способности к обеспечению непрерывности деятельности Банка, удовлетворяющей изменяющимся потребностям бизнеса и соответствующей размерам, сложности, характеру, географии, значимости хозяйственной деятельности, культуре, взаимозависимостям и условиям деятельности Банка;

3) определение требований к процессам, соблюдение которых гарантирует, что мероприятия по обеспечению непрерывности деятельности будут продолжать удовлетворять потребности Банка в случае Инцидентов, которые могут повлиять на финансовую устойчивость Банка;

4) создание четко определенной системы поддержания постоянной способности Банка к управлению непрерывностью деятельности, выполнению принятых на себя обязательств перед депозиторами, кредиторами и другими клиентами в части своевременного обеспечения возможности осуществления расчетов, предупреждению и предотвращению возможного нарушения режима повседневного функционирования Банка, снижению последствий такого нарушения (в том числе размера финансовых потерь, потери деловой репутации);

5) сохранение уровня управления Банком, позволяющего обеспечить условия для принятия адекватных решений, их своевременную и полную реализацию в непредвиденных обстоятельствах.

7. Задачи управления непрерывностью деятельности включает (но не ограничиваясь):

1) соответствие текущей рыночной ситуации, стратегии, размеру, уровню сложности операций Банка;

2) обеспечение системы управления непрерывностью деятельности, включающей, но не ограничивающейся следующими компонентами:

- политикой управления непрерывностью деятельности Банка;
- процедурами управления непрерывностью деятельности Банка;
- системой управленческой информации;
- оценкой эффективности системы управления непрерывностью деятельности подразделением внутреннего аудита.

8. Основными принципами внедрения системы управления непрерывностью деятельности являются:

- непрерывность. Принцип функционирования системы управления непрерывностью деятельности, обеспечивающей постоянное функционирование комплекса организационных и технических мер и средств защиты без перерывов и сбоев;
- своевременность. Предполагает заблаговременное выявление угроз непрерывности деятельности Банка на основе анализа рисков, разработку эффективных мер противодействия и минимизации рисков. Требует адекватной оценки влияния рисков и угроз для достижения целей бизнес-процессов;
- экономическая целесообразность. Сопоставимость возможного ущерба затратам на обеспечение непрерывности (критерий «эффективность – стоимость»). Во всех случаях стоимость системы управления непрерывностью деятельности должна быть меньше размера возможного ущерба от реализации любых видов риска;
- централизация управления. Предполагает централизованное управление системой с учетом изменяющихся условий и имеющихся факторов риска и функционирование системы управления непрерывностью деятельности в Банке, филиалах Банка по единым нормативным, организационным и технологическим принципам.

§ 4. План обеспечения непрерывности и восстановления деятельности

9. План обеспечения непрерывности и восстановления деятельности является неотъемлемой частью процесса Управления непрерывностью деятельности, разрабатывается владельцами бизнес-процессов по отношению ко всем критическим бизнес-направлениям, согласовывается с Chief Continuity Officer и утверждается Правлением Банка.

10. План обеспечения непрерывности и восстановления деятельности филиалов разрабатывается по отношению ко всем критическим бизнес-направлениям, согласовывается с Chief Continuity Officer/Continuity Officer, Управлением операционных рисков.

11. Решение об активации Плана обеспечения непрерывности и восстановления деятельности принимается Председателем Правления Банка (или уполномоченным лицом, указанным в плане обеспечения непрерывности и восстановления деятельности) после консультации с заместителем Председателя Правления Банка, курирующим соответствующий блок (или другим уполномоченным лицом).

12. План обеспечения непрерывности и восстановления деятельности разрабатывается в соответствии с типовым Планом, указанным в приложении 2 к Политике, и должен содержать:

1) определение цели и области действия, которые понятны персоналу по управлению непрерывностью деятельности и задействованным работникам;

2) указание на связи с другими планами обеспечения непрерывности и восстановления деятельности или внутренними нормативными документами Банка и описывать метод получения доступа к ним;

3) альтернативные механизмы, позволяющие возобновить услуги в случае сбоя в работе бизнес-процессов;

4) определение перечня приоритетности восстановления бизнес-процессов Банка;

5) установление приоритетных целей в отношении критических бизнес-процессов, подлежащих восстановлению, уровня восстановления для каждого критического бизнес-процесса;

6) определение лиц и группы лиц, которых охватывает План; роли и ответственность отдельных лиц и их групп, обладающих полномочиями во время Инцидента и после него;

7) меры по минимизации риска потери репутации;

8) согласовывается с действиями внешних организаций;

9) содержит требования к минимальному объему ресурсов и поставщиков, необходимых в различные моменты времени для восстановления и аварийного предоставления критичных видов деятельности;

10) содержит последовательность действий по восстановлению и непрерывному предоставлению критичных видов деятельности, в том числе:

- схему вовлечения сторонних организаций в процесс восстановления;
- схему вовлечения контрагентов и заинтересованных лиц банка в процесс восстановления деятельности банка;

- последовательность и места восстановления критичных видов деятельности банка;

- сроки и места восстановления критичных информационно-технологических услуг, а также последовательность действий по их восстановлению, в том числе восстановление сетевой инфраструктуры в новом здании, восстановление базовой функциональности, приложений и баз данных, синхронизации, резервного копирования, телекоммуникаций;

- содержит метод документирования ключевой информации о ходе работ, принятых решениях и принятых мерах;

11) матрицу ответственности, содержащую сведения, в которых каждое детализированное мероприятие Плана связано с конкретными работниками, ответственными за его реализацию, в том числе, но не ограничиваясь, следующие сведения: порядок перераспределения функций, полномочий и обязанностей работников Банка на случай возникновения чрезвычайных ситуаций, в том числе право активации Плана.

13. Матрица ответственности составляется в соответствии с примером, указанным в приложении 3 к Политике:

1) Ф.И.О. и контактная информация лиц, ответственных за реализацию Плана;

2) процедуры построения эффективной внутренней координации и связи между различными работниками и подразделениями Банка, порядок доведения до сведения Совета директоров информации о ходе выполнения Плана и принимаемых Банком мероприятий;

3) способ активизации Плана, который должен обеспечивать его активизацию в кратчайшие сроки после Инцидента, руководство к действию и критерии определения полномочия лица для активации Плана;

4) процедуры принятия решения по активации плана уполномоченным лицом, контактную информацию лица (лиц), с которыми необходимо проконсультироваться перед принятием решения об активации Плана;

5) определение лица или группы лиц, которые должны быть проинформированы после принятия решения об активации Плана;

6) процедуры установления приоритетов, которые детализируют порядок принятия мер, а также случаи, когда каждая из мер должна быть выполнена; кто, куда и когда должен направиться; какие службы доступны, где и когда, в том числе каким образом Банк будет мобилизовать внешние ресурсы и ресурсы третьих сторон;

7) описание способа мобилизации Центра кризисного управления и Бригад восстановления, места сбора и альтернативных площадок на случай недоступности основной площадки; способа расформирования Центра кризисного управления и Бригад восстановления;

8) детальные инструкции для подразделений и работников Банка, содержащие описание действий, необходимых для поддержания или своевременного возобновления функционирования критических бизнес-процессов Банка;

9) процедуры работы в чрезвычайном режиме, в том числе восстановления работы нарушенных бизнес-процессов, а также порядок завершения работы в чрезвычайном режиме и возврата в режим повседневного функционирования;

10) контактная информация (в том числе для «внерабочего времени»); описание того, каким образом и при каких обстоятельствах Банк будет контактировать с работниками, их родственниками (друзьями) и контактными лицами при Инцидентах; либо ссылка на документ, представляющий подробную информацию;

11) указание лица, группы лиц, ответственных за: эвакуацию с места происшествия, мобилизацию эвакуационных бригад, оказанию первой медицинской помощи; непрерывную связь с работниками, клиентами, партнерами, уполномоченными государственными органами, аварийно-спасательными службами;

12) способы оповещения средств массовой информации, включая: стратегию представления информации, предпочтительные средства массовой информации; руководство или шаблон для составления заявления в средства массовой информации; либо ссылка на документ, представляющий подробную информацию;

13) процесс определения и установления приоритетности связей с заинтересованными сторонами; либо ссылка на документ, устанавливающий критерии определения приоритетов и выделения лица, ответственное за каждое заинтересованное лицо или группу лиц; комплекс мероприятий, которые в периоды кризисов обеспечивают своевременную, последовательную связь с внутренними, а также внешними субъектами рынка (Национальным Банком Республики Казахстан, Агентством Республики Казахстан по регулированию и развитию финансового рынка и др.) для поддержания общего доверия к Банку;

14) необходимые ресурсы в случае сбоя в работе бизнес-процессов, осуществляемых подразделениями для реализации возложенных на них задач и функций по направлениям деятельности Банка (квалифицированный персонал, помещения, программное обеспечение, информация, технологии, оборудование и иные ресурсы);

15) перечень мероприятий, необходимых для восстановления нормального функционирования Банка, нарушенного вследствие чрезвычайных ситуаций;

16) выявление подразделений (зависимых в том числе от внешних поставщиков услуг или иных третьих лиц), по которым необходимо скорейшее возобновление услуг;

17) определение протоколов коммуникаций с внутренними и внешними сторонами;

18) указание владельца Плана, определение лиц, ответственных за регулярный анализ, внесение поправок и поддержание актуальности Плана.

Глава 4. Перечень критичных событий и Инциденты, связанные с угрозой возникновения последствий, препятствующих бесперебойному функционированию Банка

14. Перечень критичных событий, связанных с угрозой возникновения последствий, препятствующих бесперебойному функционированию Банка, определяется по результатам проведенного анализа рисков непредвиденных обстоятельств. Анализ рисков непредвиденных обстоятельств позволяет оценить угрозы и уязвимость в критичных видах деятельности и используемых ими ресурсах.

15. Инциденты могут причинить значительный ущерб физической инфраструктуре, представлять угрозу жизни и здоровью людей, повлечь человеческие жертвы; Инциденты могут быть результатом широкого спектра событий:

1) природного характера (землетрясений, ураганов, селей, лавин, наводнений и других погодных явлений, эпидемий (пандемий));

2) техногенного характера (технологических вирусов, сбоев программно-технических средств, пожаров (взрывов), внезапных обрушений зданий и сооружений, выбросов сильнодействующих ядовитых, радиоактивных и биологически опасных веществ, сбоев инфраструктуры связи и телекоммуникаций, аварий на электроэнергетических и коммуникационных системах жизнеобеспечения, очистных сооружениях);

3) социально-политического характера (поджогов, террористических атак, забастовок (митингов), в том числе с участием работников Банка).

16. Анализ рисков непредвиденных обстоятельств позволяет оценить угрозы и уязвимость в критичных бизнес-процессах. В качестве угроз и рисков, которые могут появиться вследствие реализации Инцидентов, рассматриваются (но не ограничиваются):

1) недоступность работников;

2) недоступность технологий, в том числе информационных и коммуникационных технологий;

3) недоступность снабжения (воды, электричества);

4) отсутствие доступа к зданиям (помещениям);

5) недоступность ключевых поставщиков, контрагентов;

6) недоступность ключевой информации;

7) недоступность финансовых ресурсов.

17. Аналогичные угрозы существуют для деятельности филиала, расположенного в городе Алматы. Филиалы Банка, расположенные в других регионах Казахстана, могут быть также подвержены данным рискам иного уровня в силу географического многообразия, а также некоторым специфическим рискам, уровень которых и масштабы воздействия не повлияют значительно на деятельность Банка, и которые должны быть отражены в их планах обеспечения непрерывности и восстановления деятельности. Планы обеспечения непрерывности и восстановления деятельности филиалов Банка относятся к деятельности отдельных областных и региональных филиалов Банка и утверждаются решением Комитета по обеспечению непрерывности деятельности

18. Анализ рисков непредвиденных обстоятельств на деятельность Головного банка основывается на субъективной оценке вероятности реализации Инцидентов, ущерба/воздействия на деятельность Банка и расчета уровня рисков и может проводиться в соответствии с приложением 5 к Политике.

19. Результаты проведенного анализа рисков непредвиденных обстоятельств на деятельность отражаются в приложении 6 к Политике.

20. Анализ рисков непредвиденных обстоятельств на деятельность филиалов Банка проводится Continuity Officer в соответствии с приложением 5 к Политике и подлежит

ежегодному пересмотру в обязательном порядке и внепланово в случае значительных изменений.

21. Результаты проведенного анализа рисков непредвиденных обстоятельств на деятельность филиалов Банка отражаются в приложении 6 к Политике.

22. Chief Continuity Officer рассматривает и согласовывает результаты проведенного анализа рисков непредвиденных обстоятельств на деятельность Банка, филиалов и обеспечивает проведение анализа негативных событий и рисков, принимаемых Банком на консолидированной основе.

Глава 6. Мероприятия по обеспечению и поддержанию непрерывности деятельности

23. В целях обеспечения непрерывности осуществления критических бизнес-процессов, а также восстановления бизнес-процессов, не входящих в группу «Критические бизнес-процессы», смягчению последствий и уменьшению потенциального воздействия Инцидентов Банк применяет подходы, нацеленные на восстановление и продолжение его деятельности при нарушении нормального хода бизнес-процессов, путем разработки, выбора и использования стратегий обеспечения непрерывности деятельности ресурсами. При выборе и использовании стратегий обеспечения непрерывности деятельности ресурсами учитываются:

- 1) максимально допустимая продолжительность нарушения нормального хода критических бизнес-процессов;
- 2) затраты на реализацию стратегии;
- 3) последствия бездействий.

24. Стратегия по персоналу.

При определении минимального необходимого для восстановления и осуществления критичных бизнес-процессов количества персонала, как ресурса, устанавливаются:

- 1) необходимое для поддержания критичных бизнес-процессов количество работников;
- 2) необходимые навыки и компетенции данных работников для работы в аварийном режиме.

25. Банк использует различные подходы к обеспечению в периоды Инцидентов необходимым количеством персонала соответствующей квалификации, обладающего необходимыми навыками и знаниями. К таким подходам относятся:

- 1) использование доступного персонала для сверхурочной работы;
- 2) перебазирование существующего персонала из филиалов;
- 3) наем на работу ранее работавший в Банке персонал;
- 4) наем временного персонала;
- 5) наем нового персонала.

26. Защита навыков и знаний персонала Банка обеспечивается следующими способами:

- 1) документирование процедур осуществления критических бизнес-процессов;
- 2) обучение/переподготовка персонала по нескольким функциям;
- 3) применение наставничества и преемственности;
- 4) сохранение и управление знаниями, периодическое тестирование знаний.

27. Ответственность за разработку и реализацию стратегии по персоналу, учет стратегии при разработке внутренних нормативных документов Банка и обеспечение в периоды Инцидентов необходимым количеством персонала несет Департамент управления персоналом.

28. Стратегия по помещениям.

При определении минимального необходимого для восстановления и осуществления критичных бизнес-процессов количества помещений, как ресурса, устанавливаются:

- 1) основные и альтернативные площадки;
- 2) помещения, требующие повышенной защиты.

29. Банк в зависимости от масштабов Инцидентов использует различные подходы к обеспечению необходимыми альтернативными площадками при недоступности основной площадки. К таким подходам относятся:

- 1) ввод в эксплуатацию альтернативных площадок, в том числе Резервного центра Банка;
- 2) использование запасных помещений на основной площадке;
- 3) использование помещений филиалов;
- 4) использование альтернативных площадок, предоставленных государственными органами, финансовыми или другими организациями, в том числе временное размещение;
- 5) использование заранее согласованного специального размещения на площадках;
- 6) предоставленных третьими сторонами на основании договоров аренды при возникновении Инцидентов.

30. Выбор размещения альтернативных площадок основывается на анализе возможности воздействия Инцидента, выведшего из строя основную площадку, на альтернативную площадку и доступность (возможность ежедневного прибытия и убытия) альтернативной площадки для персонала.

31. Ответственность за реализацию стратегии по помещениям и обеспечение необходимыми альтернативными площадками в периоды Инцидентов несут:

- 1) Департамент ИТ инфраструктуры совместно с Департаментом безопасности в части обеспечения функционирования технологий альтернативных площадок, в том числе Резервного центра;
- 2) Департамент ресурсов в части организации использования альтернативных площадок, транспортного обслуживания собственным автопарком или, при его недоступности, приобретение услуг автобусных парков и такси, и совместно с владельцами бизнес-процессов в части обеспечения размещения на альтернативных площадках требуемого для восстановления деятельности количества персонала.

32. Стратегия по технологиям.

При определении минимально необходимых для восстановления и осуществления критичных бизнес-процессов технологий, как ресурса, устанавливаются:

- 1) информационно-технологические услуги, поддерживающие критичные бизнес-процессы;
- 2) телекоммуникационные услуги, поддерживающие критичные бизнес-процессы;
- 3) прочие технологии, поддерживающие критичные бизнес-процессы, в том числе охрана периметра, технологии инкассации.

33. В силу масштабов и характера деятельности Банка, сложности его операций особое внимание отведено вопросу, направленному на сохранение, замену или восстановление специализированных технологий или технологий, разработанных по индивидуальному заказу, предполагающих длительное время производственного цикла.

34. Применение стратегии по технологиям зависит от характера технологий и их связи с критическими бизнес-процессами и могут включать:

- 1) географическое распределение технологий для уменьшения концентрации рисков, т.е. поддержание технологий в различных местах, которые не попадут под воздействие Инцидента, выведшего из строя основные технологии, в том числе: «горячий резерв», «теплый резерв» и «холодный резерв»;
- 2) хранение более старого оборудования для замены или в качестве запасных частей на случай Инцидента;
- 3) организация договоренности с поставщиками технологий о хранении аварийных

запасов оборудования, программного обеспечения, доступного по первому требованию;

4) поддержание собственных аварийных запасов оборудования, программного обеспечения.

35. При выборе стратегии по информационным технологиям и телекоммуникационным системам принимаются во внимание следующие факторы:

1) размещение информационных технологий на нескольких альтернативных площадках (возможно наличие стратегии взаимного восстановления технологических систем, чтобы размеры систем, сети и хранилищ данных на каждой площадке позволяли обрабатывать объединенный трафик и выполнять работу других технологических систем в дополнение к своей собственной);

2) показатели целевого срока восстановления для автоматизированных информационных систем и приложений, обеспечивающих функционирование критических бизнес-процессов;

3) расположение и расстояние между площадками размещения технологии (тщательный анализ расстояния сетевых маршрутов между площадками, которое может оказать отрицательное воздействие на функционирование и восстановление технологических систем);

4) возможность использования удаленного доступа;

5) подключение к телекоммуникациям и дублирующая маршрутизация;

6) характер «обработки отказа» – необходимость вмешательства оператора для активации альтернативного ИТ-решения или автоматическая его активация.

36. Ответственность за выбор и реализацию стратегии по информационным технологиям и телекоммуникационным системам и обеспечение непрерывности функционирования технологий в периоды Инцидентов несут Департамент ИТ инфраструктуры и Департамент безопасности.

37. Стратегия по информации.

При определении минимальной необходимой для восстановления и осуществления критичных бизнес-процессов информации, как ресурса, устанавливаются:

1) информация, необходимая для выполнения критичных бизнес-процессов, включая внутренние документы Банка;

2) объем информации, требующей восстановления (целевая точка восстановления);

3) методы хранения, защиты и восстановления этой информации.

38. Банк использует различные подходы для обеспечения защиты и возможности восстановления информации, имеющей критическое значение для функционирования бизнес-процессов. Стратегия по информации распространяется на:

1) информацию в физической (печатной) форме;

2) информацию в виртуальной (электронной) форме.

39. Защита и обеспечение возможности восстановления информации может обеспечиваться, но не ограничивается, следующими методами:

1) резервное копирование в электронном виде;

2) резервное копирование на пленку;

3) микрофиши;

4) фотокопии;

5) создание нескольких экземпляров в момент подготовки;

6) сканирование и хранение в электронном виде.

40. При выборе и реализации стратегии по информации принимаются во внимание требования законодательства, внутренних нормативных актов, требования владельцев бизнес-процессов Банка, а также следующие критерии к информации: конфиденциальность, целостность, доступность, актуальность.

41. Ответственность за реализацию стратегии по информации и обеспечение восстановления критической информации в периоды Инцидентов несут:

1) Департамент ИТ инфраструктуры совместно с Департаментом безопасности и владельцами бизнес-процессов в части обеспечения хранения и восстановления информации в электронном виде и обеспечения конфиденциальности информации;

2) Департамент защиты информационных ресурсов совместно Департаментом безопасности и владельцами бизнес-процессов в части обеспечения хранения и восстановления информации в физической (печатной) форме и обеспечения конфиденциальности информации;

3) Владельцы бизнес-процессов в части формирования Перечня критической информации и формы хранения информации.

42. Стратегия по запасам.

При определении поставщиков, внешних услуг и снабжения, как ресурсов, необходимых для восстановления и осуществления критичных бизнес-процессов, устанавливаются поставщики, внешние услуги и снабжение, от которых зависит выполнение критичных бизнес-процессов.

При определении финансовых ресурсов, необходимых для восстановления и осуществления критичных бизнес-процессов, устанавливается объем финансовых ресурсов, потенциально доступный для исполнения плана обеспечения непрерывности и восстановления деятельности в случае возникновения непредвиденных обстоятельств.

43. Банк обеспечивает хранение резервных (аварийных) запасов, которые необходимы для осуществления непрерывного функционирования бизнес-процессов, путем применения одной или нескольких стратегий по запасам, таких как:

1) хранение резервных (аварийных) запасов на альтернативных площадках и складах;

2) организация договоренности с поставщиками о незамедлительной поставке в случае Инцидентов;

3) организация резервных (аварийных) запасов у поставщиков;

4) определение альтернативных/заменяющих запасов.

44. Для обеспечения непрерывности функционирования бизнес-процессов и поддержания бесперебойности поставок специализированных запасов Банк использует следующие стратегии обеспечения бесперебойности поставок:

1) увеличение количества поставщиков;

2) поощрение или предъявление к поставщикам требования о наличии подтвержденной способности к обеспечению непрерывности деятельности;

3) организация договорных соглашений с основными поставщиками;

4) определение альтернативных поставщиков, способных удовлетворить требования Банка.

45. Ответственность за реализацию стратегии по запасам и обеспечение бесперебойности поставок в периоды Инцидентов несет Департамент ресурсов: в части организации хранения резервных (аварийных) запасов и бесперебойности поставок; совместно с владельцами бизнес-процессов в части формирования и поддержания актуального перечня основных запасов, требуемых для непрерывного функционирования бизнес-процессов.

46. Подразделения ИТ-блока совместно с Департаментом ресурсов осуществляют контроль за достаточностью оснащения альтернативных площадок необходимыми ресурсами и технологиями путем проведения инвентаризации один раз в полгода. При этом, общий контроль по данному процессу возлагается на Управление операционных рисков.

47. При выборе мер управления рисками непредвиденных обстоятельств банк учитывает результаты анализа влияния на деятельность банка и определяет, в том числе внутренний порядок взаимодействия с внешними поставщиками, участвующими в восстановительных работах, с внешними контрагентами (вкладчиками, кредиторами), акционерами банка, с уполномоченным органом и иными органами власти, а также со средствами массовой информации и другими заинтересованными сторонами.

48. При выборе мер управления рисками непредвиденных обстоятельств банк учитывает, но не ограничивается следующими факторами:

- максимально приемлемый период простоя критичного вида деятельности;
- затраты на реализацию плана (планов) обеспечения непрерывности и восстановления деятельности;
- последствия непринятия мер;
- реалистичность рисков и величину потерь от их реализации;
- согласованность с установленными целями системы управления непрерывностью деятельности;
- согласованность с политикой и процедурами по управлению непрерывностью деятельности банка.

49. Банк определяет меры по поддержанию ключевых знаний и компетенций для обеспечения непрерывности своей деятельности. Меры включают, но, не ограничиваясь, следующее:

- регламентирование внутреннего порядка осуществления критичных видов деятельности;
- ведение списка дополнительных компетенций персонала, не использующихся в повседневной деятельности, для перераспределения функций в условиях нехватки работников;
- обучение персонала профессиональным навыкам, включая проведение кросс-функциональных тренингов.

50. Банк определяет меры по снижению влияния на предоставление критичных продуктов и услуг в связи с отсутствием основных помещений. Эти меры включают, но, не ограничиваясь, следующее:

- предоставление альтернативных помещений;
- перевод персонала в другие помещения банка;
- использование рабочих мест работников, выполняющих некритичную работу;
- работа на дому или в удаленных помещениях.

51. При выборе альтернативного помещения банк учитывает, но, не ограничиваясь, следующие особенности:

- защищенность помещения;
- доступ к помещению;
- близость от основного помещения;
- наличие необходимых коммуникаций.

52. Банк определяет меры по поддержанию работоспособности информационно-технологических и коммуникационных услуг, необходимых для обеспечения непрерывности деятельности.

53. Банк определяет меры по обеспечению целостности, доступности и конфиденциальности информации, необходимой для обеспечения непрерывности деятельности в случае критичного события.

54. Банк определяет перечень используемых ресурсов (включая материальное снабжение, финансовые ресурсы) и мероприятия по обеспечению их наличия, в том числе от внешних поставщиков и контрагентов и иных заинтересованных лиц в случае критичного события, который включает:

- хранение дополнительных ресурсов, в том числе технологического и телекоммуникационного оборудования, в складских помещениях;
- соглашения с поставщиком о срочной доставке (замене) ресурсов на складе;
- наличие альтернативных поставщиков ресурсов.

55. Для обеспечения эффективности системы управления непрерывностью деятельности Управление операционных рисков при необходимости (совместно с задействованными подразделениями) обеспечивает проведение проектов по самооценке процесса ОНД.

Самооценка проводится после завершения работ по оценке влияния на бизнес, тестирования, проведения корректирующих мероприятий (по завершению нескольких циклов), согласно решению Комитета по обеспечению непрерывности деятельности.

С учетом вышеизложенного, Банк уведомляет, что согласно пункту 3 статьи 61-5 Закона о банках, Банк обеспечивает гарантированный уровень непрерывности предоставления услуг клиентам, который устанавливается следующими внутренними правилами Банка (но не ограничиваясь):

- Правила по обеспечению непрерывности и восстановлению деятельности;
- Правила Homebank;
- Правила процесса управления событиями ИТ-инфраструктуры.